NSFOCUS Firewall Products

Web Configuration Guide

NSFOCUS Technologies, Inc.

Document version: 6W600-20230111

Preface

This Web configuration guide describes the software features for the NSFOCUS firewall products and provides Web configuration examples for these features.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

About the Web configuration guide

The NSFOCUS firewall products Web configuration guide describes the software features for the Dahua firewall products. This guide also provides Web configuration examples to help you apply the software features to different network scenarios.

To obtain software version information for a device, use the display version command in any view on the device. The configuration guides use the R8560P29 versions as examples to illustrate feature configuration. For information about feature changes in other software versions, see the release notes for your device.

Overview

Log in to the Web interface

Web browser requirements

As a best practice, use the following Web browsers:

- Google Chrome 40 or higher.
- Mozilla Firefox 19 or higher.
- Internet Explorer 10 or higher.

To access the Web interface, you must use the following browser settings:

- Accept the first-party cookies (cookies from the site you are accessing).
- To ensure correct display of webpage contents after software upgrade or downgrade, clear data cached by the browser before you log in.
- Enable active scripting or JavaScript, depending on the Web browser.
- If you are using a Microsoft Internet Explorer browser, you must enable the following security settings:
    - Run ActiveX controls and plug-ins.
    - Script ActiveX controls marked safe for scripting.

Log in to the Web interface for the first time

As a best practice, change the login password after the first successful login for security purposes.

The device supports user login through HTTP and HTTPS. By default, HTTPS is enabled.

Use the following default settings for the first login.

Item	Setting
IP address of the device management interface	192.168.0.1/24
Username	admin
Password	admin
User role	network-admin

To log in to the Web interface:

1. Use an Ethernet cable to connect the configuration terminal to an Ethernet port on the device.
2. Assign the login host an IP address in the same subnet as the device.
3. Open the browser, and then enter login information:
   a. In the address bar, enter the IP address of the device **https://192.168.0.1**.
   b. On the login page, enter the default username (**admin**) and password (**admin**).
   c. Click **Login**.
4. Change the login information:

After you click **Login**, a dialog box automatically opens to force you to change the default password. To ensure system security, configure a new password that is complex enough. Then, click **OK** in the dialog box to log in to the Web interface.

To change the device IP address, go to the **Network** > **Interface Configuration** > **Interfaces** page.

To add new user accounts and assign access permissions to different users, go to the **System** > **Administrators** > **Administrators** page.

Log out of the Web interface

- For security purposes, log out of the Web interface immediately after you finish your tasks.
- You cannot log out by directly closing the browser.
- The device does not automatically save the configuration when you log out of the Web interfac prevent the loss of configuration when the device reboots, you must save the configuration.

1. Use one of the following methods to save the current configuration.
   - Click the **Save** icon  in the upper-right corner of the Web interface.
   - Go to the **System** > **Maintenance** > **Configuration Management** page to save the configuration.
2. Click **Logout** icon  in the upper-right corner of the Web interface.

Use the Web interface

Web interface layout

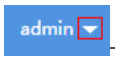
Figure 1 Web interface layout

1) Banner and admin section	2) Navigation pane	3) Work pane

As shown in Figure 1, the Web interface contains the following areas:

Area	Description
(1) Banner and admin section	Contains the following items: • Basic information, including the company logo, device name, and information about the current login user.

Area	Description

	• Basic management icons:
	  ◦ **Admin icon**  —Click this icon to change the login password.
	  ◦ **Save icon**  —Click this icon to save the configuration.
	  ◦ **Help icon**  —Click this icon to access the online help.
	  ◦ **Logout icon**  —Click this icon to log out.

(2) Navigation pane	Contains menus of all features and functionalities.
(3) Wok pane	Displays information and provides an area for you to configure features. Depending on the content in this pane, the webpages include the following types: • **Table page**—Displays entries in a table (see "Use a table page"). • **Configuration page**—Contains parameters for you to configure a feature or function (see "Use a configuration page").

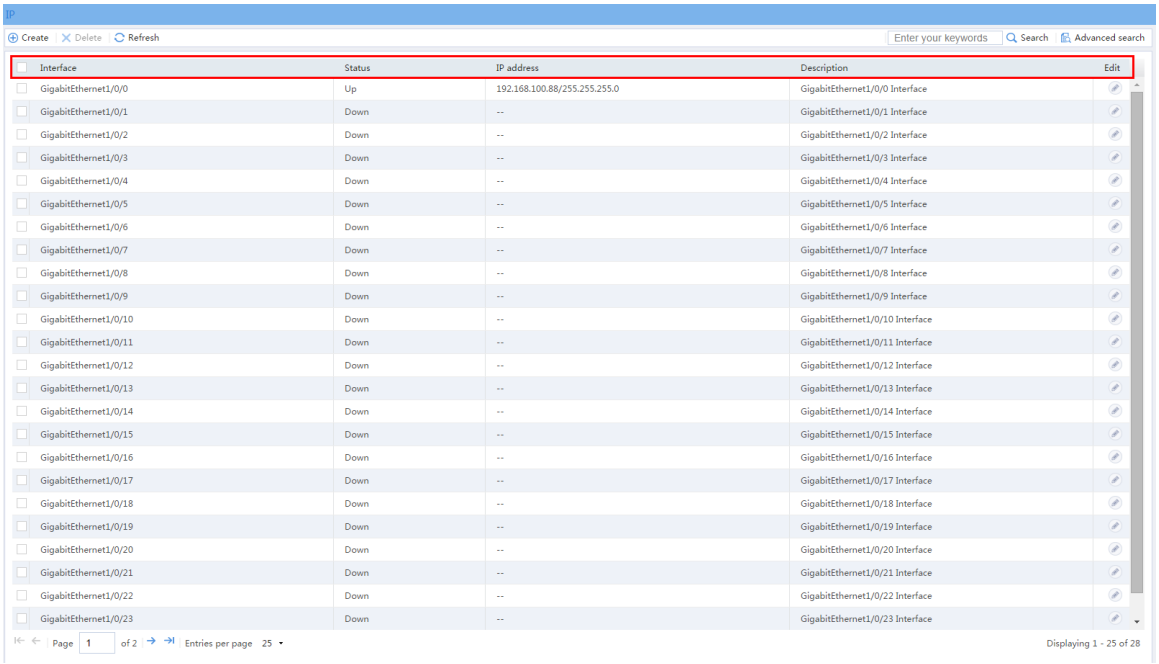
Types of webpages

Webpages include table and configuration pages. This section provides basic information about these pages.

Use a table page

As shown in Figure 2, a table page displays entries in a table. To sort entries by a field in ascending or descending order, click the field. For example, click **Interface** to sort entries by interface.

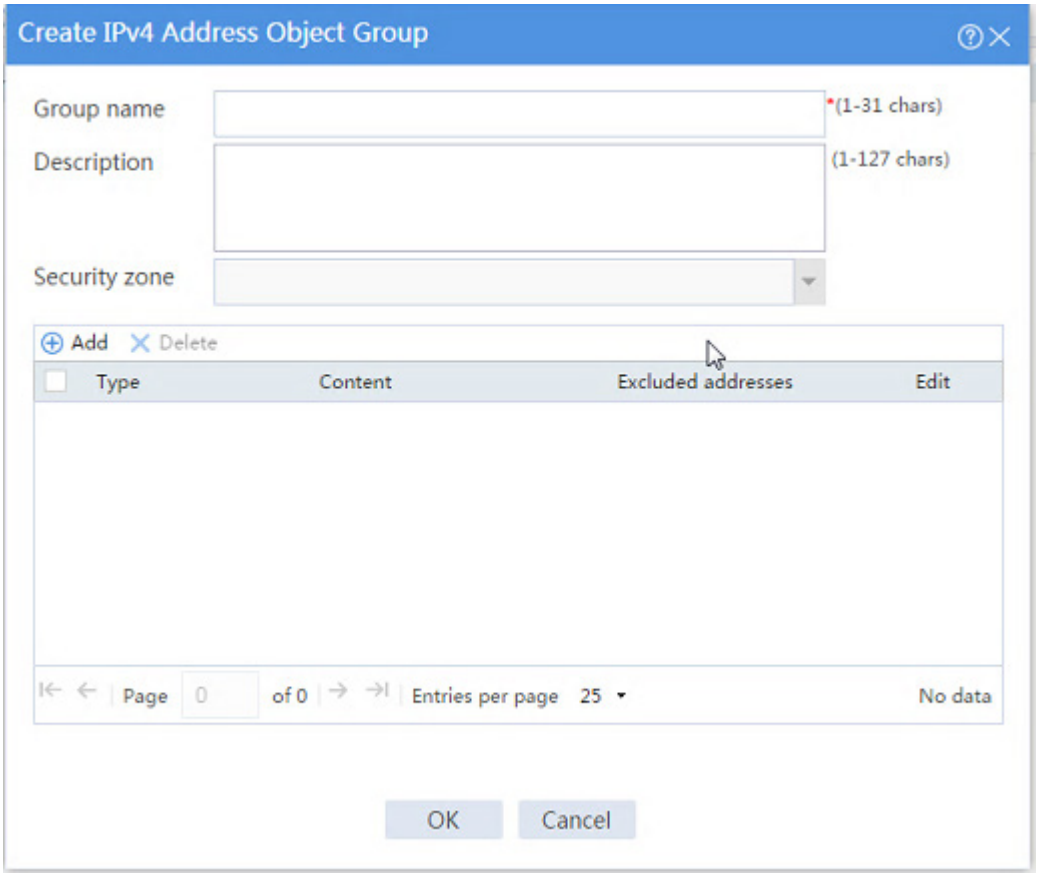
Figure 2 Sample table page



Use a configuration page

As shown in Figure 3, one configuration page contains all parameters for a configuration task. If a parameter must be configured on another page, the configuration page typically provides a link. You do not need to navigate to the destination page.

Figure 3 Sample configuration page



Perform basic tasks

This section describes the basic tasks that must be frequently performed when you configure or manage the device.

Save the configuration

Typically, settings take effect immediately after you create them. However, the system does not automatically save the settings to the configuration file. They are lost when the device reboots.

To prevent settings from being lost, use one of the following methods to save the configuration:

- Click the **Save** icon  in the upper-right corner of the Web interface.
- Go to the **System** > **Maintenance** > **Configuration Management** page, and then click **Save running configuration**.

Reboot the device

Reboot is required for some settings (for example, IRF) to take effect.

To reboot the device:

1. Save the configuration.
2. Click the **System** tab.
3. In the navigation pane, select **Maintenance** > **Reboot**.

The **Reboot** page opens.

4. Click **Reboot the device**.

Feature navigator

Menu items and icons available to you depend on the user roles you have. By default, you can use any user roles to display information. To configure features, you must have the **network-admin** or **context-admin** user role.

After you log in with the **network-admin** or **context-admin** user role, click each top menu on the banner and admin section to open a navigator table. Use the navigator tables to navigate to the pages for the tasks you want to perform.

For example:

- To change the default device name, go to the **System** > **Maintenance** > **Settings** > **Device Info** page.

- To delete an IPv4 ACL, go to the **Objects** > **ACLs** > **IPv4 ACLs** page.

Quick start

This help contains the following topics:

Introduction

To ensure high security, security devices by default can communicate only with the network devices or endpoints connected to the management interfaces. For the security devices to communicate with other devices, you must add the connecting interfaces of the security devices to security zones and configure security policies to permit traffic. This page will help you complete required configurations when you first use your security device.

Basic settings for the security device

Change the default password

When you first access the Web interface of the security device, you can use the default administrator account (username and password are both **admin**) to log in. After you successfully log in, immediately change the default password as a best practice to avoid illegal logins and ensure security for the device and network.

Configure interface IP addresses

By default, only the management interface of the security device has an IP address configured for login management. To enable the security device to forward service packets, you must configure IP addresses for service interfaces. For more information about interface configuration, see the interface help.

Add security zone members

The security device discards packets between two interfaces that are not in any security zone. For the security device to correctly process received packets, you must add the device's interfaces to security zones. The security device has five predefined security zones, which are **Local**, **Management**, **Trust**, **Untrust**, and **DMZ**. The **Local** zone represents the security device itself. You cannot add interfaces to the **Local** zone. The **Management** zone holds the management interface. As a best practice, do not add service interfaces to the **Management** zone. You can add service

interfaces to the **Trust**, **Untrust**, and **DMZ** zones. You can also create security zones as needed. For more information about security zones, see the security zone help.

Configure a security policy

The security device uses the security policies applied to security zone pairs to control packet forwarding. By default, the security device forwards packets only between the **Management** and **Local** zones. That is, the device or endpoint connected to the interface in the **Management** zone can access the security device, and all other packets accessing the security device will be discarded. For the security device to forward these packets correctly, you must configure security policies to permit valid packets and discard invalid packets between specific zone pairs.

A device might need to exchange packets with the security device itself for some services, such as OSPF, tunnel, VPN, DHCP, and NAT. To correctly process these packets, you need to configure a security policy to permit packets between the security zone of the device and the **Local** zone of the security device.

For more information about security policies, see the security policy help.

Dashboard

This help contains the following topics:

Introduction

The **Dashboard** page clearly displays key information, data, and various states of the device in graphical widgets. It provides a pre-defined tab and allows you also to define tabs as needed. The pre-defined tab displays information about the basic modules and allows you to add other modules as required. To view information about the modules important to you conveniently, for example, modules in the operation monitor, traffic monitor, threat monitor, or filtering monitor, you can define a tab and add and display information about the modules on the tab.

Support for the modules depends on the device model.

Operation monitor

Operation monitor provides device operating status information.

Device status

The **Device Status** widget displays the CPU usage, memory usage, and CF card usage. To display detailed information and set the alarm thresholds, click the **Details** icon.

Alarm thresholds include CPU usage alarm thresholds and free-memory alarm thresholds. Set alarm thresholds as required.

System logs

The **System Logs** widget displays the system log messages of and above the error level. To display detailed information about log messages of all levels, click the **Details** icon. You can use the information for device status analysis and troubleshooting.

System traffic statistics

The **System Traffic Statistics** widget displays the inbound and outbound traffic statistics during a period of time in a line chart. You can use the chart to analyze traffic distribution over time on the network.

To display detailed traffic statistics on interfaces, click the **Details** icon.

To set traffic statistics parameters and filter the statistics result, click the **Set** icon.

System session statistics

The **System Sessions** widget displays statistics on the number of sessions established during the past hour. To display statistics about sessions established during the past hour, the past day, or past 30 days, click the **Details** icon.

To enable top 10 ranking and view the ranking result, click the following buttons:

- **Enable top 10 ranking**—Enables the device to collect statistics based on services and sort the statistics by source or destination address.
- **View top 10 ranking**—Displays the top 10 ranking result. You can select the time period (past hour, past day, or past 30 days) and the sort criterion (source or destination address).

Session establishment rate statistics

The **Session Establishment Rate Statistics** widget displays session establishment rate statistics during the past hour. To display session establishment rate statistics during the past hour, the past day, or past 30 days, click the **Details** icon.

To enable top 10 ranking and view the ranking result, click the following buttons:

- **Enable top 10 ranking**—Enables the device to collect statistics based on services and sort the statistics by source or destination address.
- **View top 10 ranking**—Displays the top 10 ranking result. You can select the time period (past hour, past day, or past 30 days) and the sort criterion (source or destination address).

Deny session statistics

The **Deny Sessions Statistics** widget displays statistics on the number of deny sessions. To display the statistics during the past hour, the past day, or past 30 days, click the **Details** icon.

To enable top 10 ranking and view the ranking result, click the following buttons:

- **Enable top 10 ranking**—Enables the device to collect statistics based on services and sort the statistics by source or destination address.
- **View top 10 ranking**—Displays the top 10 ranking result. You can select the time period (past hour, past day, or past 30 days) and the sort criterion (source or destination address).

System information

The **System Info** widget displays device information, for example, the device name, device model, software version, and IRF mode.

Internet access monitoring

The **Internet Access Monitoring** widget displays Internet access information, including the application type, website address, and transferred files. To display detailed Internet access information and audit user behaviors, click the **Details** icon.

License information

The **License Info** widget displays license information about features. To display detailed license information, including the license type, status, and validity period, click the **Details** icon.

Interface information

The **Interface Information** widget displays the current state and detailed information for each interface on the device. To view the interface states on the simulated device panel, click the **View device panel** button.

Traffic monitor

Traffic monitor displays traffic ranking statistics for the most recent monitoring interval. The top 10 is displayed by default.

Real-time application ranking

By default, the real-time application ranking widget displays the top 10 applications by percentage of the application's traffic rate to the total traffic rate in a list.

The real-time application ranking list contains the following fields:

- Application.
- Downlink traffic rate.
- Uplink traffic rate.
- Total rate.
- Percentage.

To customize the widget to display real-time application ranking list, click the **Set** icon  in the top-right corner of the widget and configure either of the following functions:

- **Auto refreshing**—Select the **Auto refresh** option, enter the refresh interval in the **Refresh interval** field, and then click **OK**.
- **Real-time traffic data collection**—Select the **Enable real-time traffic data collection** option and click **OK**. To view traffic details in real time, select the **Display real-time traffic details** option. To view the traffic data of the application used by different users in real time, click an application in the **Application** column in the real-time application ranking list.

Threat monitor

Security status

This widget displays the risk factor and security event distribution. To view detailed statistics analysis, click the data in the **Security Event Distribution** graph.

Top 10 hosts at risk

This widget displays compromised host information, including hostname, risk level, and attack events. To view detailed risk analysis for a host, click the hostname.

Application analysis center

This help contains the following topics:

Introduction

The application analysis center displays the statistics for the following widgets:

- **Application Usage**.

- **User Activity**.
- **Source IP Activity**.
- **Destination IP Activity**.
- **Security Policy Usage**.
- **Source Security Zones**.
- **Destination Security Zones**.
- **Threat Activity**.

Each widget displays the statistics based on the following aspects:

- **Bytes**—Displays the traffic distribution by bytes.
- **Sessions**—Displays session statistics. You can obtain information about which applications, users, and IP addresses have established or occupied a large number of sessions.
- **Threats**—Displays threat statistics.
- **URLs**—Displays Web access statistics.
- **Files**—Displays file filtering statistics.

Restrictions and guidelines

If the device updates to a version that supports the application analysis center feature from one that does not, the device performs application analysis only on the data after update.

Configure the application analysis center

Configure global settings

The **Application Analysis Center** page provides the following global conditions for statistics collection that take effect for all widgets.

Select a context

To display context-based statistics, select a context from the **Context** list. To display the statistics for all contexts, select **All** from the list.

Specify the time range

To display the statistics in a time range, select the time range from the **Time range** list, or click **Custom** from the list and customize the time range as required.

Select widgets

To customize the widgets displayed on the page, click **Select module** and select the desired widgets from the list.

Add global filters

To add a filter to filter the statistics, click **Filters** in the **Global filters** field, select a filter type, and configure the filter as required.

To remove a filter, hover the mouse over the filter and click the icon at the right of the filter. To remove all filters, hover the mouse over the **Global filters** field, and click the icon at the right end of the field.

Customize the settings for each widget

You can configure the following settings that take effect only for the specified widget.

View more data

By default, each widget displays only top 10 entries. To view more data, click the icon in the top-right corner of each section.

Add analyzer filters

To add filters for a widget only, click the icon in the top-right corner of each section, and then set the filters as required.

Switch between analysis aspects

To obtain the statistics for an analysis aspect, select the analysis aspect on the top of each section. The following aspects are supported in the current software version: **Bytes**, **Session**, **Threats**, **URLs**, and **Files**. After you select an analysis aspect, the system ranks the statistics based on the analysis aspect. For example, if you select **Bytes** for **Application Usage**, the **Application Usage** section will rank the applications based on the traffic in graphs and tables.

Display data in graphs and tables

The page supports display data in graphs and tables for each widget.

The types of graphs include treemaps (), area graphs (), line graphs (), and histograms (). Support for types of graphs varies by widget.

To display the statistics in a type of graph, click the graph icon in the top-right corner of each section. Only area graphs support the drill down functionality. Drill down is a capability that enables you to view statistics from a general view to a more specific view by clicking the mouse. For example, for the **Application Usage** widget, you can click the E-Mail area in the area graph. Then, the area graph will display information only about the Email's subcategories, such as 126 Mail and 163 Mail. To view information about a specific Email subcategory, click the subcategory area, like 126 Mail area.

By default, a table displays only top 10 entries. To view more data, click **Miscellaneous** and select **View more data** from the list.

The non-numeric columns allow for more actions, such as adding an application name as a widget-specific filter or adding it as a global filter. To bring up the action menu for an item in a non-numeric column, hover the mouse over the item, click the icon.

Application usage

The **Application Usage** section displays application usage statistics based on different aspects. You can customize the settings for applications accordingly.

Area graphs provide visibility to the applications with the top bandwidth usages, and provide the drill down capability to present the detailed application statistics.

User activity

The **User Activity** section displays user statistics based on different aspects. You can customize the settings for users accordingly.

Source IP activity

The **Source IP Activity** section displays source IP statistics based on different aspects. You can customize the settings for source IPs accordingly.

Destination IP activity

The **Destination IP Activity** section displays destination IP statistics based on different aspects. You can customize the settings for destination IPs accordingly.

Source security zones

The **Source Security Zones** section displays statistics of source security zones based on different aspects. You can customize the settings for source security zones accordingly.

Destination security zones

The **Destination Security Zones** section displays statistics of destination security zones based on different aspects. You can customize the settings for destination security zones accordingly.

Security policy usage

The **Security Policy Usage** section displays security policy matching count. You can customize the settings for security policies accordingly.

Threat activity

The **Threat Activity** section displays statistics of the threat events. You can customize the settings for threat defense accordingly.

Blacklist logs

This help contains the following topics:

Introduction

After you enable blacklist logging, the device outputs logs in the following situations:

- A blacklist entry is manually added.
- A blacklist entry is dynamically added by the scanning attack detection feature.
- A blacklist entry is manually deleted.
- A blacklist entry ages out.

A blacklist log records the following information:

- Source IP address of the blacklist entry.
- Remote IP address of the DS-Lite tunnel.
- VPN instance (VRF) name.
- Reason for adding or deleting the blacklist entry.

- Aging time for the blacklist entry.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage blacklist logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Blacklist Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Blacklist Logs**.

3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

- To continue the export, click **Yes**.
- To stop the export process, click **No**.

Single-packet attack logs

This help contains the following topics:

Introduction

If logging is enabled for single-packet attack events, the device outputs a log when a packet with a specific signature is detected.

By default, log aggregation for single-packet attack events is enabled. The device aggregates multiple logs generated during a period of time and outputs one log. Logs that are aggregated must have the following attributes in common:

- Security zone where the attacks are detected.
- Attack type.
- Attack prevention action.
- Source and destination IP addresses.
- VPN instance (VRF) to which the victim IP address belongs.

You can disable log aggregation for single-packet attack events on the **System** > **Log Settings** > **Attack Defense Log Settings** page. As a best practice, do not disable log aggregation if single-packet attacks frequently occur. A large number of logs will consume the display resources.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage single-packet attack logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Single-Packet Attack Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.

2. In the navigation pane, select **Security Logs** > **Single-Packet Attack Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

- To continue the export, click **Yes**.
- To stop the export process, click **No**.

Scanning attack logs

This help contains the following topics:

Introduction

If logging is enabled for scanning attack events, the device outputs a log when a scanning attack is detected.

If IP sweep and port scan attacks reach the scanning thresholds at the same time, the device output a log only for the IP sweep attack.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage scanning attack logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Scanning Attack Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Scanning Attack Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

     – To continue the export, click **Yes**.

     – To stop the export process, click **No**.

Flood attack logs

This help contains the following topics:

Introduction

If logging is enabled for flood attack events, the device outputs a log when a flood attack is detected.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage flood attack logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Flood Attack Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Flood Attack Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

     – To continue the export, click **Yes**.

     – To stop the export process, click **No**.

Threat logs

This help contains the following topics:

Introduction

The **Threat Log List** page displays the logs generated by the IPS module and the anti-virus module. These logs help administrators customize IPS profiles and anti-virus profiles to improve network security.

When configuring an IPS profile or anti-virus profile, you can enable the logging function. The IPS module and anti-virus module can then generate logs for matching packets.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.
- When querying logs of a time range, this page displays the logs of the first day by default. You can click **Previous Day** or **Next Day** to view the logs of a specific date.

Configuration guidelines

Viewing threat log details

To view details of a log, click the **Details** icon  in the **Details** column. In the **Threat Log Details** window, the threat name in the **Threat information** area and the fields in the **Packet Details** area may be incompletely displayed. To view the complete content, you can use the following methods:

- Hover over the content.
- Click **Copy**. On the window that opens, obtain the complete content.

Downloading capture files

After the intrusion prevention system executes the packet capture action, the device generates logs. With hard disks installed, you can click **Download** of a log to obtain the captured file for threat analysis. To enable the device to cache IPS captured packets, execute the **`ips capture-cache`** *`number`* command in system view.

Adding to whitelist

If false alarms exist in the threat logs, you can click the **Add to whitelist** icon  of a log to add the detected IPS signature ID and URL to the whitelist. The whitelist feature permits packets matching the whitelist to pass through, reducing false alarms.

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Threat Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Threat Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

     – To continue the export, click **Yes**.

     – To stop the export process, click **No**.

URL filtering logs

This help contains the following topics:

Introduction

The **URL Filtering Log List** page displays the logs generated by the URL filtering module. These logs help administrators customize URL filtering profiles to control users' website access behaviors.

You can enable logging in a URL filtering profile. The URL filtering module can then generates logs for packets that match the URL filtering profile.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage URL filtering logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **URL Filtering Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **URL Filtering Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

     – To continue the export, click **Yes**.

     – To stop the export process, click **No**.

File filtering logs

This help contains the following topics:

Introduction

The **File Filtering Log List** page displays the logs generated by the file filtering module. These logs help administrators customize file filtering profiles to reduce the risks of information leakage and transfer of virus-infected files on the company network.

When configuring a file filtering profile, you can enable logging in file filtering rules. The file filtering module generates logs for files that match file filtering rules with the logging option enabled.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage file filtering logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **File Filtering Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **File Filtering Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

     – To continue the export, click **Yes**.

     – To stop the export process, click **No**.

Security policy logs

This help contains the following topics:

Introduction

This feature enables the system to generate a security policy log entry for each packet matching a security policy rule, helping administrators audit user behaviors and perform network troubleshooting.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage security policy logs

Import logs

1. Client the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Security Policy Logs**.
3. Click the **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Client the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Security Policy Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is

Item	Description
	required when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

     The system supports exporting a maximum of 65000 logs to one log file.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.
     - To continue the export, click **Yes**.
     - To stop the export process, click **No**.

IPCAR logs

This help contains the following topics:

Introduction

The IPCAR logs can be displayed only when you select **Alarm** as the action for the connection establishment rate limit configuration (see **Policies** > **Active Defense** > **Threat Intelligence** > **Request Limit** > **Public Network Protection** or **Internal Network Protection**).

A log is exported to the **IPCAR Logs** page when the rate of new connections sourced from or destined for an IP address exceeds the connection rate threshold.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage IPCAR logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **IPCAR Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password is the one set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **IPCAR Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required when you view the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page

Item	Description
	displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

     The system supports exporting a maximum of 65000 logs to one log file.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.
     - To continue the export, click **Yes**.
     - To stop the export process, click **No**.

Sandbox logs

Introduction

The sandbox logs record the sandbox inspection results, including the basic information of packets and inspected files, and threats found in these files.

For more information about the values for the threat family and threat action fields, see "Appendix."

Restrictions and guidelines

The detailed information of sandbox logs is displayed only in JSON format.

The field value in the appendix varies by the software version of the sandbox.

Appendix

Table 1 Value for the threat family field

ID	Threat family
0	Others
1	Viruses

ID	Threat family
2	Trojans
3	Worms
4	Backdoors
5	Ransomware
6	Downloader
7	Malicious advertisements
8	Malicious scripts
9	Macro viruses
10	Malicious files with vulnerabilities
11	Phishing
12	Riskware
13	Shell software
14	Heuristic behaviors
15	Digital currency
16	Botnets
17	APT intelligence
18	Malicious DGA domain names

Table 2 Value for the threat act field

ID	Threat action
1	Enable autorun after the device starts.
2	Inject to other processes remotely.
3	Reduce the firewall security level or add whitelist entries.
4	Bypass User Account Control (UAC) to obtain the administrator privilege.
5	Disable the system protection mechanism.
6	Detect whether the antivirus software is installed or running in the system.
7	Detect whether the file runs in the sandbox or is debugged by the debugger.
8	Delete local files.
9	DLL hijacking or image hijacking.
10	Replace the file to be an EXE file or a DLL file.
11	The file uses a name similar to a key process for counterfeiting.
12	Infect the existing PE files.
13	Load the driver.
14	Modify the security policies of the IE browser.
15	Add or modify a Windows account.
16	Add or modify a Windows service.
17	Suspicious network connection.
18	Create a suspicious process and release a suspicious file.

ID	Threat action
19	Release an executable program.
20	Automatic shutdown, automatic restart or automatic logout.
21	The PE file execution releases a script file.
22	Modify the hosts file.
23	Hook the key functions of the program.
24	Promote the privilege of the program.
25	The script file uses the PowerShell.
26	Malicious network behaviors of the script file.
27	Access sensitive files, such as the files storing the browser username and password.
28	Using the Android software consumes the call charge.
29	Malicious advertisements on the Android software.
30	The Android software steals user privacy.
31	File faking
32	Modify the file hidden attribute.
33	Malicious network behaviors of an executable file.
34	Malicious shortcut files
35	Suspicious macro viruses
200	Viruses

ID	Threat action
201	Spyware
202	Worms
203	Backdoors
204	Ransomware
205	Downloader
206	Malicious advertisements
207	Malicious scripts
208	Malicious files with vulnerabilities
209	Virus generator
210	Shell software
211	Heuristic behaviors
212	Riskware
213	Phishing
214	Macro viruses
215	Other threat types

NAT logs

This help contains the following topics:

Introduction

NAT logs record NAT session information, including translation information and access information.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage NAT logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **NAT Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **NAT Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

     – To continue the export, click **Yes**.

     – To stop the export process, click **No**.

SSL VPN user access logs

This help contains the following topics:

Introduction

When an SSL VPN user logs in or logs out, the device outputs a log. The log information includes login or logout time, username, login IP address, SSL VPN context, login or logout result, and reason for the failure. You can view the logs for detailed user login or logout information to help with device management and maintenance.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage SSL VPN user access logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **SSL VPN User Access Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **SSL VPN User Access Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

     The system supports exporting a maximum of 65000 logs to one log file.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.
     - To continue the export, click **Yes**.
     - To stop the export process, click **No**.

SSL VPN access resource logs

This help contains the following topics:

Introduction

When an SSL VPN user accesses internal resources, the device outputs corresponding log messages. The log information includes login time, username, login IP address, SSL VPN context, resource type, access resource, resource port number, and access result. You can view the logs to get detailed resource access information to help with resource access control and management.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage SSL VPN access resource logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **SSL VPN Access Resource Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **SSL VPN Access Resource Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

     The system supports exporting a maximum of 65000 logs to one log file.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.
     - To continue the export, click **Yes**.
     - To stop the export process, click **No**.

Terminal logs

Introduction

Terminal identification logs

Terminal identification logs record detailed information about identified terminals, including terminal ID, IP address, access interface, and MAC address.

Traffic abnormality logs

Traffic abnormality logs are recorded when the highest bandwidth of a terminal is higher than the bandwidth upper limit or the lowest bandwidth is lower than the bandwidth lower limit during a one-minute interval.

Load balancing logs

Introduction

Inbound link LB logs

This page displays logs about traffic scheduled by inbound link LB and GLB. You can use the logs to obtain the scheduling results and analyze scheduling failure reasons.

You can click **Export to Excel** on the page to export the logs.

Outbound link LB logs

This page displays logs about traffic scheduled by outbound link LB. You can use the logs to obtain the scheduling results and analyze scheduling failure reasons.

You can click **Export to Excel** on the page to export the logs.

Transparent DNS proxy logs

This page displays logs about traffic scheduled by transparent DNS proxies. You can use the logs to obtain the scheduling results and analyze scheduling failure reasons.

You can click **Export to Excel** on the page to export the logs.

Application audit logs

Introduction

This page displays the Internet access behaviors of users. According to the users' Internet access behaviors, you can adjust the application audit and management policy to regulate the users' Internet access behaviors.

The application audit log displaying function takes effect after the logging function is enabled in the application audit policy. When packets match the policy, logs are output to the application audit logs page.

Click **Details** on the page to view details of the Internet access behaviors.

Restrictions and guidelines

If a user does not belong to any user groups, the user group field in the application audit log displays the username.

If a user belongs to only one user group and the user group has been used by an audit policy, the user group field displays the user group name. If the user group is not used by any audit policy, the user group field displays the username.

If a user belongs to multiple user groups, the user group field displays the name of a user group randomly selected from the multiple user groups.

Only one log operation (import, export, or delete) is allowed at a time.

Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Configure application audit logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select any item under **Application Audit Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select any item under **Application Audit Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

     The system supports exporting a maximum of 65000 logs to one log file.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.
     - To continue the export, click **Yes**.
     - To stop the export process, click **No**.

System logs

This help contains the following topics:

Introduction

The system logs page records the log messages generated while the device system is running. The system log messages help with system troubleshooting and maintenance. By viewing system log messages, you can know about the device running process, analyze network conditions, and locate the failures.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage system logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Device Logs** > **System Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Device Logs** > **System Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

     The system supports exporting a maximum of 65000 logs to one log file.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.
     - To continue the export, click **Yes**.
     - To stop the export process, click **No**.

Configuration logs

This help contains the following topics:

Introduction

This page displays configuration operations performed on the device. You can use the information to track operations of administrators, audit administrator behavior, and troubleshoot the device.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage configuration logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Device Logs** > **Configuration Logs**.
3. Click **Import**.
4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Device Logs** > **Configuration Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required

Item	Description
	when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.
   - **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

     The system supports exporting a maximum of 65000 logs to one log file.
   - **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.
8. Perform one of the following tasks as required:
   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.
     - To continue the export, click **Yes**.
     - To stop the export process, click **No**.

Traffic logs

Introduction

This page displays traffic information on a per-flow basis. Administrators can apply appropriate bandwidth limit policies according to traffic logs.

For traffic logs to be displayed, you must enable session statistics collection on the **System** > **Session Aging Time Settings** > **Advanced Setting** page.

Restrictions and guidelines

- Only one log operation (import, export, or delete) is allowed at a time.
- Only one user can perform a log operation at a time. When you import, export, or delete logs, make sure no one else is performing a log operation.

Manage traffic logs

Import logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Device Logs** > **Traffic Logs**.
3. Click **Import**.

4. In the dialog box that opens, click **Yes**.
5. Select a log file, and enter the password for the log file. The password was set when the file was exported.

Export logs

1. Click the **Monitor** tab.
2. In the navigation pane, select **Device Logs** > **Traffic Logs**.
3. Click **Advanced search**.
4. On the page that opens, specify the search criteria to display the logs to be exported.
5. Click **Export**.
6. On the page that opens, configure the log export settings.

Table 1 Log export configuration items

Item	Description
Set password	Enter a password for encrypting the log files. This password is required when you view or import the exported log files.
Log range	Specify the range of logs to be exported. Options are: • **All results**—Exports all logs that satisfy the search criteria. The page displays the total number of logs to be exported. • **Day on the current page**—Exports logs of the day indicated by the **Time** field on the current page. You can define the ending page to decrease the number of logs to be exported.

7. Select one of the following export methods.

- **Export to one file**—Exports logs to one file. When a small number of logs are to be exported, select this method.

  The system supports exporting a maximum of 65000 logs to one log file.

- **Export to files**—Exports logs to multiple files. If more than 65000 logs are to be exported, select this method.

8. Perform one of the following tasks as required:

   - If you have selected **Export to one file**, click **OK** in the dialog box that opens.
   - If you have selected **Export to files**, specify the number of logs to be exported to each file and click **OK** in the dialog box that opens.

     When a log export to one file is complete, a dialog box opens, asking you whether to continue exporting the remaining logs to a new file.

     – To continue the export, click **Yes**.

     – To stop the export process, click **No**.

TopN traffic

This help contains the following topics:

Introduction

The device analyzes traffic statistics and generates the following types of traffic ranking reports that display the traffic ranking results in bar chart, pie chart, and list:

- **TopN Users**.
- **TopN Applications**.
- **TopN Source Addresses**.
- **TopN Destination Addresses**.
- **TopN Contexts**.

On each of the preceding report configuration page, you can customize conditions such as the time range and the traffic direction for statistics collection. Then, you can generate the report and export the report as needed.

TopN users

Perform this task to generate the topN users traffic report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 1 Statistics collection condition configuration items for the topN users traffic report

Item	Description
Traffic direction	Select the traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of users to display.

3. Click **Start**.
4. Click a user on the topN users traffic report to view the application usage statistics for the user.

5. To export the topN users traffic report, click **Export report**.

TopN applications

Perform this task to generate the topN applications traffic report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 2 Statistics collection condition configuration items for the topN applications traffic report

Item	Description
Traffic direction	Select the traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Query object	Enter the source IP address whose application usage traffic statistics will be collected.
Ranked by	Select the ranked object. Options are:

Item	Description
	• **Application category**. • **Application**.
Show Top	Enter the number of applications to display.

3. Click **Start**.
4. Click an application on the topN applications traffic report and select **Source address** to view the topN source addresses that used the application.
5. Click an application on the topN applications traffic report and select **User** to view the topN users for the application.
6. To export the topN applications traffic report, click **Export report**.

TopN source addresses

Perform this task to generate the topN source addresses traffic report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 3 Statistics collection condition configuration items for the topN source addresses traffic report

Item	Description
Traffic direction	Select the traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Application category	Select the application category.
Application	Select an application in the designated application category. The device will rank the source IP addresses by the amount of traffic they spent on the application.
Show Top	Enter the number of source IP addresses to display.

3. Click **Start**.
4. Click a source IP address on the topN source addresses traffic report to view the topN applications accessed by the source IP address.
5. To export the topN source addresses traffic report, click **Export report**.

TopN destination addresses

Support for this feature depends on the device model.

Perform this task to generate the topN destination addresses traffic report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 4 Statistics collection condition configuration items for the topN destination addresses traffic report

Item	Description
Traffic direction	Select the traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Application category	Select the application category.
Application	Select an application in the designated application category. The device will rank the destination IP addresses by the amount of traffic they spent on the application.

Item	Description
Show Top	Enter the number of destination IP addresses to display.

3. Click **Start**.
4. Click a destination IP address on the topN destination addresses traffic report to go to the **TopN applications** page to view detailed application traffic.
5. To export the topN destination addresses traffic report, click **Export report**.

TopN contexts

Support for this feature depends on the device model.

Perform this task to generate the topN contexts traffic report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 5 Statistics collection condition configuration items for the topN contexts traffic report

Item	Description
Traffic direction	Select the traffic direction. Options are: • **Upstream**. • **Downstream**.

Item	Description
	• **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of contexts to display.

3. Click **Start**.

4. To export the topN contexts traffic report, click **Export report**.

Security policy hit analysis

Introduction

The **Policy Hit Analysis** page displays security policies that have not matched any packets in bar charts, pie charts, and lists. You can specify filtering criteria to view specific analysis statistics.

View policy hit analysis statistics

1. Click **Monitor** > **Statistics** > **Security Policy Hit Analysis**.

   The page that opens displays security policy hit analysis statistics.

2. To edit a security policy, click the policy name.

3. To filter statistics, click **Statistics collection settings**. On the page that opens, specify the filtering criteria and then click **Start**.

Table 1 Policy hit analysis filtering criteria

Item	Description
Type	Select the security policy type. Options include: • IPv4. • IPv6.
Statistics collection period	Select a time range. Options include: • Today.

Item	Description
	• Last 7 days. • Last 30 days. • Last 12 months. • Custom.
List display	Specify the number of security policies to be displayed.

TopN threats

This help contains the following topics:

Introduction

The device analyzes detected threat events (including IPS events and anti-virus events) and generates the following types of threat ranking reports:

- **TopN Users**.
- **TopN Applications**.
- **TopN Threat Types**.
- **TopN Attackers**.
- **TopN Attacked Targets**.
- **TopN Threat Names**.

These threat ranking reports help administrators customize IPS profiles and anti-virus profiles to improve network security.

On each of the preceding report configuration page, you can customize conditions such as the time range for statistics collection and the number of items to display. Then, you can generate the report and export the report as needed.

TopN users

The **TopN Users** page displays the topN users by the number of threats they are involved in.

Perform this task to generate the topN users threat report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 1 Statistics collection condition configuration items for the topN users threat report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of users to display.

3. Click **Start**.

4. To export the topN users threat report, click **Export report**.

TopN applications

The **TopN Applications** page displays the topN applications by the number of threats they are involved in.

Perform this task to generate the topN applications threat report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.

2. Configure the statistics collection conditions.

Table 2 Statistics collection condition configuration items for the topN applications threat report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of applications to display.

3. Click **Start**.

4. To export the topN applications threat report, click **Export report**.

TopN threat types

The **TopN Threat Types** page displays the topN types of the most common threats detected by the device.

Perform this task to generate the topN threat types threat report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 3 Statistics collection condition configuration items for the topN threat types threat report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of threat types to display.

3. Click **Start**.
4. To export the topN threat types threat report, click **Export report**.

TopN attackers

The **TopN Attackers** page displays the IP addresses of the topN attackers by the number of attacks they launched.

Perform this task to generate the topN attackers threat report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 4 Statistics collection condition configuration items for the topN attackers threat report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Threat type	Select the types of threats for statistics collection. Options are: • **IPS**. • **Anti-virus**. • **All**.
Show Top	Enter the number of attackers to display.

3. Click **Start**.

4. Click an attacker IP address on the topN attackers threat report and select **Threat name** to view the topN threats launched by the attacker.
5. Click an attacker IP address on the topN attackers threat report and select **Attacked target** to view the topN attacked targets for the attacker.
6. To export the topN attackers threat report, click **Export report**.

TopN attacked targets

The **TopN Attacked Targets** page displays the IP addresses of the topN attacked targets by the number of threats they are involved in.

Perform this task to generate the topN attacked targets threat report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 5 Statistics collection condition configuration items for the topN attacked targets threat report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

Item	Description
Threat type	Select the types of threats for statistics collection. Options are: • **IPS**. • **Anti-virus**. • **All**.
Show Top	Enter the number of attacked targets to display.

3. Click **Start**.
4. Click an attacked target IP address on the topN attacked targets threat report and select **Threat name** to view the topN threats targeted at the attacked target.
5. Click an attacked target IP address on the topN attacked targets threat report and select **Attacker** to view the topN attackers for the attacked target.
6. To export the topN attacked targets threat report, click **Export report**.

TopN threat names

The **TopN Threat Names** page displays the topN most common threats detected by the device.

Perform this task to generate the topN threat names threat report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 6 Statistics collection condition configuration items for the topN threat names threat report

Item	Description
Threat type	Select the types of threats for statistics collection. Options are: • **IPS**. • **Anti-virus**. • **All**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Attack category	Select **All**, **Attacker**, or **Attacked target**.
Show Top	Enter the number of threats targets to display.

3. Click **Start**.
4. Click a threat on the topN threat names threat report and select **Attacker** to view the topN attackers for the threat.
5. Click a threat on the topN threat names threat report and select **Attacked target** to view the topN attacked target for the threat.
6. To export the topN threat names threat report, click **Export report**.

TopN URL filtering statistics

This help contains the following topics:

Introduction

The device analyzes users' Web resource access behaviors and generates the following types of URL filtering reports that display statistics in bar chart, pie chart, and list:

- **TopN Users**.
- **TopN URL Categories**.
- **TopN Websites**.
- **TopN Source Addresses**.
- **TopN Destination Addresses**

These reports help administrators customize URL filtering profiles to control users' Web resource access behaviors.

On each of the preceding report configuration page, you can customize conditions such as the time range for statistics collection and the number of items to display. Then, you can generate the report and export the report as needed.

TopN users

Perform this task to generate the topN users URL filtering report and export the report. The topN users URL filtering report displays the topN users by website access count.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 1 Statistics collection condition configuration items for the topN users URL filtering report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of users to display.

3. Click **Start**.
4. To export the topN users URL filtering report, click **Export report**.

TopN URL categories

Perform this task to generate the topN URL categories URL filtering report and export the report. The topN URL categories URL filtering report displays the topN URL categories with the largest number of visit count.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 2 Statistics collection condition configuration items for the topN URL categories URL filtering report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of URL categories to display.

3. Click **Start**.
4. To export the topN URL categories URL filtering report, click **Export report**.

TopN websites

Perform this task to generate the topN websites URL filtering report and export the report. The topN websites URL filtering report displays the topN websites with the largest number of visit count.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 3 Statistics collection condition configuration items for the topN websites URL filtering report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of websites to display.

3. Click **Start**.
4. To export the topN websites URL filtering report, click **Export report**.

TopN source addresses

Perform this task to generate the topN source addresses URL filtering report and export the report. The topN source addresses URL filtering report displays the topN source addresses with the largest number of website visit count.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 4 Statistics collection condition configuration items for the topN source addresses URL filtering report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of source IP addresses to display.

3. Click **Start**.
4. To export the topN source addresses URL filtering report, click **Export report**.

TopN destination addresses

Perform this task to generate the topN destination addresses URL filtering report and export the report. The topN destination addresses URL filtering report displays the topN destination addresses for users' Web resource access behaviors.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 5 Statistics collection condition configuration items for the topN destination addresses URL filtering report

Item	Description
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Show Top	Enter the number of destination IP addresses to display.

3. Click **Start**.
4. To export the topN destination addresses URL filtering report, click **Export report**.

TopN file filtering statistics

Introduction

The **TopN File Filtering Statistics** page displays the file filtering statistics in a bar char, pie chart, and list. The statistics help administrators customize file filtering profiles to reduce the information leakage and virus infection risks on the company network.

Attack defense statistics

Introduction

Attack defense statistics

The attack defense statistics page displays the following attack defense statistics: attack types, attack times, and the number of dropped packets caused by each attack.

Client verification statistics

The client verification statistics page displays the following statistics for IP entries protected by client verification:

- Client verification type.
- VRF to which the protected IP belongs.
- Protected IP address.
- Port.
- Type of the protected IP address.
- Number of packets destined for the protected IP address.
- Number of request packets that passed client verification.

Blacklist statistics

The blacklist statistics page displays the following blacklist entry statistics:

- VRF.
- IP address added to the blacklist entry.
- DS-Lite tunnel peer address.
- Type of the blacklist entry.
- Remaining aging time of the blacklist entry.
- Number of dropped packets that match the blacklist entry.

Server load balancing statistics

Introduction

Virtual server statistics

Table 1 shows the information displayed on the virtual sever statistics page.

Table 1 Virtual server statistics

Item		Description
Virtual server name		Virtual server for which the statistics information is displayed.
State		Virtual server state: • Available. • Unavailable. • Disabled.
Connection count	Active	Number of active connections for the virtual server.
	New	Average number of connections established with the virtual server per second.
Bandwidth (Kbps)	Outbound	Outbound bandwidth of the virtual server.
	Inbound	Inbound bandwidth of the virtual server.

Server farm statistics

Real-time statistics

Table 2 shows the information displayed on the sever farm statistics page.

Table 2 Server farm statistics

Item		Description
Server farm name		Server farm for which the statistics information is displayed.
State		Server farm state: • Available. • Unavailable.
Total real servers		Total number of real servers in the server farm.
Available real servers		Number of available real servers in the server farm.
Connection count	Active	Number of active connections for the server farm.
	New	Average number of connections established with the server farm per second.
Bandwidth (Kbps)		Total bandwidth of the server farm.

Trends

This page displays the server farm statistics over time.

You can specify the server farm scope and statistics duration in the **Statistics conditions** section to display the following information:

- Traffic trend.
- Visit count trend.
- Active connection count trend.
- Stability trend.

Real server statistics

Real-time statistics

Table 3 shows the information displayed on the real sever statistics page.

Table 3 Real server statistics

Item	Description
Real server name	Real server for which the statistics information is displayed.
State	Virtual server state: • Available. • Unavailable. • Service slow offline. • Service disabled. • Probe failed. • Ramp-up phase of slow online. • Busy. • Unknown.

Item		Description
IPv4 address		IPv4 address of the real server.
IPv6 address		IPv6 address of the real server.
Connection count	Active	Number of active connections for the real server.
	New	Average number of connections established with the real server per second.
Bandwidth (Kbps)	Outbound	Outbound bandwidth of the real server.
	Inbound	Inbound bandwidth of the real server.

Trends

This page displays the real server statistics over time.

You can specify the real server scope and statistics duration in the **Statistics conditions** section to display the following information:

- Traffic trend.
- Visit count trend.
- Active connection count trend.
- Stability trend.
- HTTP delay trend.

URL visit statistics

The URL visit statistics shows the statistics of URLs accessed by users in a bar chart, pie chart, or list.

The administrator can set statistics conditions to rank URLs by virtual server or statistics node. Table 4 shows the statistics conditions.

Table 4 URL visit statistics conditions

Item	Description
Virtual server name	Counts the total number of URL accesses to a virtual server.
Statistics node name	Counts the total number of URL accesses to an HTTP statistics node that belongs to the specified virtual server.
Statistics period	Specifies the time period for collecting the total number of URL accesses.

Click **Start** to enable the device to collect URL visit statistics and rank URL accesses based on the specified statistics conditions.

HTTP protection statistics

The HTTP protection statistics page shows attack record statistics and attack rankings in a bar chart or a list to help you understand the protection results of protection policies.

Attack records

The **Attack Records** tab displays information about attack traffic matching a protection policy, including attack duration, source IP address, URL, virtual server name, cookie name, protection action, attack times, and context.

Attack ranking

You can set statistics conditions to rank attack traffic. Table 5 shows the supported statistics conditions.

Table 5 Attack traffic statistics conditions

Item	Description
Ranking	Specifies the top N ranking: Top 5 or Top 10.
Count by	Specifies the counting type: • Source IP address. • URL.
Duration	Specifies the duration for collecting attack traffic statistics.

Click **Start** to enable the device to collect attack traffic statistics and rank attack traffic based on the specified statistics conditions.

Protection logs

The protection log page displays information about traffic matching a protection policy, including attack duration, source IP address, URL, virtual server name, cookie name, and context.

Outbound link load balancing statistics

Introduction

Link statistics

The link statistics page displays the following information:

- Link name.
- Link state.
- IPv4 output interface.
- IPv6 output interface.
- Active connection count.
- New connection count.
- Inbound bandwidth.
- Outbound bandwidth.

Click the **Details** icon to view detailed information about the link, including the traffic size, packet count, link bandwidth, connection counts, output interface rate, output interface, statistics collection time, and packet loss ratio.

Link group statistics

The link group statistics page displays the following information:

- Link group name.
- Bandwidth.
- Active connection count.
- Total connection count.
- Inbound traffic size.
- Outbound traffic size.
- Inbound packet count.
- Outbound packet count.
- Number of dropped packets.

Click the **Details** icon to view detailed information about each link in the link group, including the link name, active connection count, maximum connection count, connection rate, and maximum connection rate.

Transparent DNS proxy statistics

Introduction

DNS server

Table 1 shows the information displayed on the DNS server statistics page.

Table 1 DNS server statistics

Item	Description
DNS server name	DNS server for which the statistics information is displayed.
Received requests	Number of DNS request packets received by the DNS server.
Dropped requests	Number of DNS request packets dropped by the DNS server.
Received responses	Number of DNS response packets received by the DNS server.
Sent responses	Number of DNS response packets sent by the DNS server.
Dropped responses	Number of DNS response packets dropped by the DNS server.

DNS server pool

Table 2 shows the information displayed on the DNS server pool statistics page.

Table 2 DNS server pool statistics

Item	Description
DNS server pool name	DNS server pool for which the statistics information is displayed.
Received requests	Total number of DNS request packets received by the DNS server pool.
Dropped requests	Total number of DNS request packets dropped by the DNS server pool.
Received responses	Number of DNS response packets received by the DNS server pool.
Sent responses	Total number of DNS response packets sent by the DNS server pool.
Dropped responses	Total number of DNS response packets dropped by the DNS server pool.

Connection rate ranking

Introduction

This feature allows you to rank source or destination IP addresses by connection rate over a time period and then display the Top N rank. The time period can be **Recent 5 min**, **Recent 15 min**, **Recent 1 hour**, **Recent 1 day**, **Recent 1 week**, or **Recent 30 days**. The value range for N is 10 to 500.

TopN traffic trends

This help contains the following topics:

Introduction

The device analyzes traffic statistics and generates the following types of traffic trend reports in line chart:

- **User Traffic Trend**.
- **Application Category Traffic Trend**.
- **Source IP Address Trend**.
- **Destination IP Address Trend**.

- **Application Traffic Trend**.
- **Context Traffic Trend**.
- **Traffic Policy Traffic Trend**.
- **Device Traffic Distribution by Volume Or Rate**.
- **Device Traffic Distribution Over Time**.

These reports help you understand the traffic trends, the peak traffic periods, and the off-peak traffic periods.

On each of the preceding report configuration page, you can customize conditions such as the time range and data range for statistics collection. Then, you can generate the report and export the report as needed.

User traffic trend

Perform this task to generate the user-based traffic trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 1 Statistics collection condition configuration items for the user-based traffic trend report

Item	Description
User	Select **Top 5 users** to collect statistics only for the top 5 users. Select **Specify users** and specify the users for statistics collection.

Item	Description
Traffic direction	Select a traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Application category	Select an application category from the list.
Application	Select an application for statistics collection.

3. Click **Start**.
4. To export the user-based traffic trend report, click **Export report**.

Application category traffic trend

Perform this task to generate the application category-based traffic trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 2 Statistics collection condition configuration items for the application category-based traffic trend report

Item	Description
Application category	Select **Top 5 application categories** to collect statistics only for the top 5 application categories. Select **Specify application categories** and specify the application categories for statistics collection.
Traffic direction	Select a traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Query object	Enter the host IP address for statistics collection in the **Host IP address** field.

3. Click **Start**.
4. To export the application category-based traffic trend report, click **Export report**.

Source IP address trend

Perform this task to generate the source IP address-based traffic trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 3 Statistics collection condition configuration items for the **source IP address-based traffic trend report**

Item	Description
Source IP address	Select **Top 5 source IPs** to collect statistics only for the top 5 source IP addresses. Select **Specify source IPs** and specify the source IP addresses for statistics collection.
Traffic direction	Select a traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Application category	Select an application category from the list.
Application	Select an application for statistics collection.

3. Click **Start**.
4. To export the source IP address trend report, click **Export report**.

Destination IP address trend

Perform this task to generate the destination IP address-based traffic trend report and export the report.

Support for this function depends on device model.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 4 Statistics collection condition configuration items for the **destination IP address-based traffic trend report**

Item	Description
Source IP address	Select **Top 5 destination IPs** to collect statistics only for the top 5 destination IP addresses. Select **Specify destination IPs** and specify the destination IP addresses for statistics collection.
Traffic direction	Select a traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

Item	Description
Application category	Select an application category from the list.
Application	Select an application for statistics collection.

3. Click **Start**.
4. To export the destination IP address trend report, click **Export report**.

Application traffic trend

Perform this task to generate the application-based traffic trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 5 Statistics collection condition configuration items for the application-based traffic trend report

Item	Description
Application	Select **Top 5 applications** to collect statistics only for the top 5 applications. • Select **Specify applications** and specify the applications for statistics collection.
Traffic direction	Select a traffic direction. Options are: • **Upstream**.

Item	Description
	• **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.
Query object	Enter the host IP address for statistics collection in the **Host IP address** field.

3. Click **Start**.
4. To export the application-based traffic trend report, click **Export report**.

Context traffic trend

Perform this task to generate the context-based traffic trend report and export the report.

Support for this function depends on device model.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 6 Statistics collection condition configuration items for the context-based traffic trend report

Item	Description
Context	Select **Top 5 contexts** to collect statistics only for the top 5 contexts. • Select **Specify contexts** and specify the contexts for statistics collection.
Traffic	Select a traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the context-based traffic trend report, click **Export report**.

Traffic policy traffic trend

Perform this task to generate the traffic policy-based traffic trend report and export the report. The report displays the policy hit traffic trend of traffic policies so you can optimize the traffic policies as needed.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 7 Statistics collection condition configuration items for the traffic policy-based traffic trend report

Item	Description
Traffic policy	Select **Top 5 traffic policies** to collect statistics only for the top 5 traffic policies with the largest policy hit traffic volumes. • Select **Specify traffic policies** and specify the traffic policies for statistics collection.
Traffic type	Select a traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the traffic policy-based traffic trend report, click **Export report**.

Device traffic distribution by volume or rate

Perform this task to generate the device traffic distribution by volume or rate report and export the report. The report displays the device traffic volume or traffic rate trend, which helps you customize traffic management policies.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 8 Statistics collection condition configuration items for the **device traffic distribution by volume or rate report**

Item	Description
Analyzed object	Select an analyzed object. Options are: • Traffic volume. • Traffic rate.
Traffic direction	Select a traffic direction. Options are: • **Upstream**. • **Downstream**. • **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.

4. To export the device traffic distribution by volume or rate report, click **Export report**.

Device traffic distribution over time

Perform this task to generate the device traffic distribution over time report and export the report. The report helps you learn the distribution of the peak traffic periods and off-peak traffic periods and customize traffic management policies as needed.

Procedure

1. Click **Stats conditions** in the top left corner of the page.

2. Configure the statistics collection conditions.

Table 9 Statistics collection condition configuration items for the **device traffic distribution over time report**

Item	Description
Time unit	Select the time unit for the device traffic distribution over time report. Options are: • **Hourly per day**. • **Daily per month**. • **Daily per week**.
Traffic direction	Select a traffic direction. Options are: • **Upstream**. • **Downstream**.

Item	Description
	• **Bidirectional**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.

4. To export the device traffic distribution over time report, click **Export report**.

Security policy hit trend analysis

Introduction

The **Security Policy Hit Trend** page displays the hit trends of security policies. You can specify filtering criteria to view statistics about the specified policies or the Top 5 policies with the most hit times.

View security policy hit trends

1. Click **Monitor** > **Trends** > **Security Policy Hit Trend**.

   The page that opens displays security policy hit trends.

2. To filter statistics, click **Statistics collection settings**. On the page that opens, specify the filtering criteria and then click **Start**.

Table 1 Policy hit trend filtering criteria

Item	Description
Policy range	Select the security policies to be displayed. Options include: • **Top 5 policies by hit count**—Specify the five security policies with the most hit times. • **Specified policies**.
Policy type	Select the policy type. Options include: • IPv4.

Item	Description
	• IPv6.
Time range	Select a time range for the analysis from the menu at the top right corner. Options include: • Today. • Last 7 days. • Last 30 days. • Last 12 months. • Custom.

TopN threat trends

This help contains the following topics:

Introduction

By analyzing the trends of detected threat events in various perspectives, the device generates the following types of threat trend reports to help illustrate the peak periods during which threats are most likely to happen and the time periods highly risky threats are most likely to happen:

- **User Threat Trend**.
- **Application Threat Trend**.
- **Threat Type Threat Trend**.
- **Attacker Threat Trend**.
- **Attacked Target Threat Trend**.
- **Threat ID Threat Trend**.

These reports help administrators adjust security policies to effectively protect the company network against threats.

On each of the preceding report configuration page, you can customize conditions such as the time range and data range for statistics collection. Then, you can generate the report and export the report as needed.

User threat trend

Perform this task to generate the user-based threat trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 1 Statistics collection condition configuration items for the user-based threat trend report

Item	Description
User	Select **Top 5 users** to collect statistics only for the top 5 users. Select **Specify users** and specify the users for statistics collection.
Threat type	Select the threat types. Options are: • **IPS**. • **Anti-virus**. • **All**.
Time range	Select a time range from the list. Options are:

Item	Description
	• **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the user-based threat trend report, click **Export report**.

Application threat trend

Perform this task to generate the application-based threat trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 2 Statistics collection condition configuration items for the application-based threat trend report

Item	Description
Application	Select **Top 5 applications** to collect statistics only for the top 5 applications. • Select **Specify applications** and specify the applications for statistics collection.
Time range	Select a time range from the list. Options are:

Item	Description
	• **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the application-based threat trend report, click **Export report**.

Threat type threat trend

Perform this task to generate the threat type-based threat trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 3 Statistics collection condition configuration items for the threat type-based threat trend report

Item	Description
Threat type	Select a threat type. Options are: • **IPS**. • **Anti-virus**.
Time range	Select a time range from the list. Options are:

Item	Description
	• **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the threat type-based threat trend report, click **Export report**.

Attacker threat trend

Perform this task to generate the attacker-based threat trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 4 Statistics collection condition configuration items for the attacker-based threat trend report

Item	Description
Attacker	Select **Top 5 attackers** to collect statistics only for the top 5 attackers. • Select **Specify attackers** and specify the attackers for statistics collection.
Threat type	Select the threat types. Options are:

Item	Description
	• **IPS**. • **Anti-virus**. • **All**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the attacker-based threat trend report, click **Export report**.

Attacked target threat trend

Perform this task to generate the attacked target-based threat trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 5 Statistics collection condition configuration items for the attacked target-based threat trend report

Item	Description
Attacked target	Select **Top 5 attacked targets** to collect statistics only for the top 5 attacked targets. • Select **Specify attacked targets** and specify the attacked targets for statistics collection.
Threat type	Select the threat types. Options are: • **IPS**. • **Anti-virus**. • **All**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the attacked target-based threat trend report, click **Export report**.

Threat ID threat trend

Perform this task to generate the threat ID-based threat trend report and export the report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 6 Statistics collection condition configuration items for the threat ID-based threat trend report

Item	Description
Threat ID	Select **Top 5 threat IDs** to collect statistics only for the top 5 threats. Select **Specify threat IDs** and specify the IDs of the threats for statistics collection.
Threat type	Select a threat type. Options are: • **IPS**. • **Anti-virus**.
Attack type	Select the attack types. Options are: • **Attacker**. • **Attacked target**. • **All**.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the threat ID-based threat trend report, click **Export report**.

TopN URL filtering trends

This help contains the following topics:

Introduction

The device analyzes users' Web resource access behaviors and generates the following types of URL filtering trend reports:

- **User URL Filter Trend**.

☐URL Category URL Filter Trend.

☐Website URL Filter Trend.

☐Source Address URL Filter Trend.

☐Destination Address URL Filter Trend.

These reports help you learn the trend of users' Web resource access behaviors, the peak Web resource access periods, and the most visited websites and website categories.

On each of the preceding report configuration page, you can customize conditions such as the time range and data range for statistics collection. Then, you can generate the report and export the report as needed.

User URL filter trend

Perform this task to generate the user-based URL filtering trend report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 1 Statistics collection condition configuration items for the user-based URL filtering trend report

Item	Description
User	Select **Top 5 users** to collect statistics only for the top 5 users. Select **Specify users** and specify the users for statistics collection.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the user-based URL filtering trend report, click **Export report**.

URL category URL filter trend

Perform this task to generate the URL category-based URL filtering trend report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 2 Statistics collection condition configuration items for the URL category-based URL filtering trend report

Item	Description
URL category	Select **Top 5 URL categories** to collect statistics only for the top 5 URL categories. Select **Specify URL categories** and specify the URL categories for statistics collection.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the URL category-based URL filtering trend report, click **Export report**.

Website URL filter trend

Perform this task to generate the website-based URL filtering trend report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 3 Statistics collection condition configuration items for the website-based URL filtering trend report

Item	Description
Website	Select **Top 5 websites** to collect statistics only for the top 5 websites. Select **Specify websites** and specify the websites for statistics collection.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the website-based URL filtering trend report, click **Export report**.

Source address URL filter trend

Perform this task to generate the source address-based URL filtering trend report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 4 Statistics collection condition configuration items for the source address-based URL filtering trend report

Item	Description
Source address	Select **Top 5 source addresses** to collect statistics only for the top 5 source IP addresses. Select **Specify source addresses** and specify the source IP addresses for statistics collection.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the source address-based URL filtering trend report, click **Export report**.

Destination address URL filter trend

Perform this task to generate the destination address-based URL filtering trend report.

Procedure

1. Click **Stats conditions** in the top left corner of the page.
2. Configure the statistics collection conditions.

Table 5 Statistics collection condition configuration items for the destination address-based URL filtering trend report

Item	Description
Destination address	Select **Top 5 destination addresses** to collect statistics only for the top 5 destination IP addresses. Select **Specify destination addresses** and specify the destination IP addresses for statistics collection.
Time range	Select a time range from the list. Options are: • **Today**. • **Past week**. • **Past month**. • **Custom**.

3. Click **Start**.
4. To export the destination address-based URL filtering trend report, click **Export report**.

TopN file filtering trends

Introduction

The **File Type Trend** page allows you to generate a trend report for the types of files transferred over a specific time range. You can use the information to customize file filtering profiles to reduce the information leakage and virus infection risks on the company network.

Link trend

Introduction

This page displays the link statistics over time.

You can specify the link scope and statistics duration in the Statistics conditions section to display the following information:

- Traffic trend.
- Bandwidth usage trend.
- Packet loss ratio.
- Delay.
- New connection count trend.
- Active connection count trend.
- RST packet count trend.
- Application-based traffic percentage.
- Stability.
- Real-time link quality.

Routing policy trends

This help contains the following topics:

Introduction

This page allows you to view match ratio statistics for traffic classes in routing policies.

You can specify the statistics duration on the **Statistics conditions** page to display class match ratio statistics for IPv4 and IPv6 routing policies, respectively.

Virtual server trend

Introduction

This page displays the virtual server statistics over time.

You can specify the virtual server scope and statistics duration in the **Statistics conditions** section to display the following information:

- Traffic trend.
- Visit count trend.
- Active connection count trend.

Server farm trends

Introduction

This page displays the server farm statistics over time.

You can specify the server farm scope and statistics duration in the **Statistics conditions** section to display the following information:

- Traffic trend.
- Visit count trend.
- Active connection count trend.
- Stability trend.

Real server trend

Introduction

This page displays the real server statistics over time.

You can specify the real server scope and statistics duration in the **Statistics conditions** section to display the following information:

- Traffic trend.
- Visit count trend.
- Active connection count trend.
- Stability trend.
- HTTP delay trend.

Domain Requested Times Trend

Introduction

This page provides administrators with intuitive statistics about DNS requests for specified domain names within a selected time span.

You can specify the domain name scope and statistics duration in the **Statistics conditions** section to display the trend graph for DNS requests.

URL visit trends

Introduction

The URL visit trends allow the administrator to obtain user online information by viewing URL visit peak times and visit count.

The administrator can set statistics conditions to view URL visit trends for virtual servers, statistics nodes, and visit sources.

Table 1 Common filter option

Item	Description
Statistics object	Select a statistics object: • Virtual server • Statistics node • Visit source

Table 2 Filter options for virtual server statistics object

Item	Description
Query scope	Select the query scope for the virtual server statistics object: • Top 5 virtual servers: Collects URL visit trend statistics for the top 5 virtual servers by URL visit count. • Specify virtual servers: Collects URL visit trend statistics for the specified virtual servers.

Item	Description
Virtual server name	Specify the names of the virtual servers for which the URL visit trend statistics are collected. This parameter is available only when you select **Specify virtual servers** for **Query scope**.

Table 3 Filter options for statistics node statistics object

Item	Description
Virtual server name	Specify a virtual server. The URL visit trend statistics are collected for the HTTP statistics nodes that belong to the virtual server.
Query scope	Select the query scope for the statistics node statistics object: • Top 5 statistics nodes: Collects URL visit trend statistics for the top 5 statistics nodes of the specified virtual server by URL visit count. • Specify statistics nodes: Collects URL visit trend statistics for the specified statistics nodes of specified virtual server.
Statistics node name	Specify the names of the statistics nodes for which the URL visit trend statistics are collected. This parameter is available only when you select **Specify statistics nodes** for **Query scope**.

Table 4 Filter options for visit source statistics object

Item	Description
Virtual server name	Specify a virtual server. The URL visit trend statistics are collected for the visit sources that belong to the virtual server.
Statistics node name	Specify the name of the statistics node accessed by the visit

Item	Description
	source.
Query scope	Select the query scope for the visit source statistics object: • Top 5 visit sources: Collects URL visit trend statistics for the top 5 visit sources by URL visit count. • Specify visit sources: Collects URL visit trend statistics for the specified visit sources.
Visit source name	Specify the source address object group names or source IP addresses for which the URL visit trend statistics are collected. This parameter is available only when you select **Specify visit sources** for **Query scope**.

Click **Start** to enable the device to collect URL access statistics based on the specified statistics conditions.

Online SSL VPN users trend

Introduction

The online SSL VPN users trend feature allows the administrator to perform statistics about the number of online SSL VPN users on the device in a specific time range. Then, an online SSL VPN users trend graph will be displayed based on the statistics. The administrator can view the user number peak and valley time periods in the specified time range.

View online SSL VPN users trend

1. Click the **Monitor** tab.
2. In the navigation pane, select **Trends** > **Online SSL VPN Users Trend**.
3. Click **Statistics conditions**, select a statistics time range in the **Date and time** section, and then click **Start statistics**.

Table 1 Online SSL VPN users trend configuration item

Item	Description
Time range	Select a time range for the trend statistics. Options include: • Today. • Past week. • Past month. • Past year.

Item	Description
	• Custom.

Botnet analysis

This help contains the following topics:

Introduction

The device analyses all security logs related to botnets and supports displaying information about hosts that might be zombie hosts, including IP and name of hosts, and peer hosts. This feature helps you identify and locate zombie hosts, and then take prevention actions.

Support for this feature depends on the device model.

Asset security

This help contains the following topics:

- Introduction
- Restrictions and guidelines
- Configure asset security
- Appendix

Introduction

The device analyses health status of downstream hosts and supports displaying the number of compromised hosts and security event distribution in graphs and tables. You can view a summary on the security status of downstream hosts, and a detailed security analysis report for a single host. Thus, you can take prevention actions based asset security information.

Restrictions and guidelines

- Support for this feature depends on the device model.
- The detailed security analysis report for a single host displays only the statistics over the past half year.
- The device generates detailed security analysis reports only for the hosts at the **Controlled** risk level or higher.

Configure asset security

1. Click the **Monitor** tab.
2. In the navigation pane, select **Asset Security**.

   The page displays security summary of hosts on the **Hosts at risk** tab. For information about risk levels, see "Appendix."
3. To view the detailed security analysis report for a single host, click the host name in the table.

Appendix

Table 1 Risk level description

Risk level	Description
Vulnerable	A vulnerability exists on a host.
Attacked	Malicious attacks are present and not blocked. For example, a host might be attacked by DDoS attacks, SQL injection attacks, worm attacks, Web shells, or has received ransomware or bots.
Controlled	Communication exists between an infected host and a C&C server.
Spread	An infected host has sent threats to other hosts.
Damaged	A file on an infected host has been leaked, or an infected host has been attacked by ransomware or has been forced to run mining software.

Threat case management

Introduction

Threat case management is used to manage and classify the threat logs generated by the device. The device provides an alarm resource pool to store threat logs and allows users to add the logs to cases for ease of log management.

To manage threat cases:

1. Click the **Monitor** tab.
2. In the navigation pane, select **Security Logs** > **Threat Logs**. Select the target logs, and then click **Add to alarm resource pool**.
3. In the navigation pane, select **Threat Case Management**. Click the **Alarm Resource Pool** tab to view logs for threat analysis.
4. To add logs to a case, select the target logs, and click **Add to case** to add the selected logs to a case.

You can perform the following threat log management tasks on the **Cases** tab:

- To archive a case, you can perform either of the following tasks:
    - Select the case, and then click the **Edit** icon for the case entry. In the dialog box that opens, select **Archived** from the **Status** field.
    - Select the case, and then click **Logs** in the case entry. In the dialog box that opens, click **Archive**. Then, click **Yes** to confirm your operation.
- To view the details of a case, click **Logs** in the case entry. In the dialog box that opens, you can also view the details of a log by clicking the **Details** icon in the log entry.

- To edit a case, click the **Edit** icon  for the case entry. In the dialog box that opens, edit the status of the case or remove logs from the case as needed.

Report settings

Introduction

The device can collect and analyze data of various services to generate the following types of reports:

- **Summary report**—Displays summarized service statistics collected over a time range.
- **Comparison report**—Provides comparison of service statistics collected over two time ranges that contain the same number of days.
- **Intelligent report**—Provides intelligent analysis of users' work efficiency, data leakage, and turnover risks based on their network access behaviors.
- **Comprehensive report**—Illustrates the overall device operational and network security status based on analysis of critical service statistics.

Session list

This help contains the following topics:

Introduction

The **Session List** page records the detailed information of each data flow, including the 5-tuple information of the data flow and the matching security policy and application. The page also provides the session suspend function. To suspend a session, click **Normal** in the **Status** Column. Any packets in the suspended session will be dropped.

The value for the master/backup status of a session includes the following:

- **Master**—The session is created on the current device.
- **Backup**—The session is synchronized from the other device.

Restrictions and guidelines

You can export a maximum of 1000 sessions by clicking **Export CLI Output**.

LB session information

Introduction

Table 1 shows TCP connection information for Layer 7 server load balancing.

Table 1 LB session information

Item	Description
Client-side client IP	Client-side client IP address used to establish TCP connections to the device.
Client-side client port	Client-side client port number used to establish TCP connections to the device.
Client-side server IP	Client-side server IP address used to establish TCP connections to the device.
Client-side server port	Client-side server port number used to establish TCP connections to the device.
Server-side client IP	Server-side client IP address used to establish TCP connections to the server.
Server-side client port	Server-side client port number used to establish TCP connections to the server.
Sever-side server IP	Server-side server IP address used to establish TCP connections to the server.
Sever-side server port	Server-side server port number used to establish TCP connections to the server.
Client-side connection	State of a TCP connection between the client and the device:

Item	Description
state	• CLOSED • LISTENING • SYN_SENT • SYN_RECEIVED • ESTABLISHED • CLOSE_WAIT • FIN_WAIT_1 • CLOSING • LAST_ACK • FIN_WAIT_2 • TIME_WAIT
Server-side connection state	State of a TCP connection between the device and the server: • CLOSED • LISTENING • SYN_SENT • SYN_RECEIVED • ESTABLISHED • CLOSE_WAIT • FIN_WAIT_1 • CLOSING • LAST_ACK • FIN_WAIT_2 • TIME_WAIT

User information center

Introduction

This page displays Internet access behaviors of users, including visited applications, visited websites, email, and file transfer. You can use the information for auditing purposes.

You can click a user to view detailed information about the user's Internet access behaviors, including Internet access statistics and traffic analysis for visited applications and websites.

DNS cache information

Introduction

A DNS cache entry records the mapping between a domain name and an IP address. Table 1 shows the DNS cache information.

Table 1 DNS cache information

Item	Description
Domain name	Domain name.
Type	IP type: • IPv4 • IPv6
Cached data	IP address corresponding to the domain name.
Lifetime	Aging time for DNS cache entries, in minutes.

IPv4 online users

Introduction

The IPv4 online user list displays information about all online IPv4 users. The displayed information includes the device interface through which a user accesses the network, IPv4 address of a user, login time of a user, and so on.

First navigate to the **Network** > **Security Access** > **IP Access** > **IP Authentication** page, and enable IP authentication on an IPv4 interface. When a user accesses the interface and passes authentication, you can view information about this user on the current page.

IPv6 online users

Introduction

The IPv6 online user list displays information about all online IPv6 users. The displayed information includes the device interface through which a user accesses the network, IPv6 address of a user, login time of a user, and so on.

First navigate to the **Network** > **Security Access** > **IP Access** > **IP Authentication** page, and enable IP authentication on an IPv6 interface. When a user accesses the interface and passes authentication, you can view information about this user on the current page.

MAC authentication online users

Introduction

The MAC authentication online user list displays information about all MAC authentication online users. On the list, you can view the access interface, MAC address, authorization VLAN, and login time, and so on of each online user. Additionally, you can forcibly log off online users as an administrator.

For this page to display information about a user, the following operations must be performed:

1. Enable MAC authentication globally and on the user's access interface on the **Network** > **Security Access** > **MAC Access** > **MAC Authentication** page.
2. The user accesses the interface and passes MAC authentication successfully.

Terminal status

This help contains the following topics:

Introduction

Terminal heat map

The terminal heat map offers a visual representation of the state of each terminal in each network segment. The terminal state can be normal, abnormal, or unreachable. You can search terminals by terminal state or block state. You can click the IP address of a terminal to block the terminal. The blocked terminal cannot access the network until the block duration expires or you unblock it.

The terminal heat map uses different colors to represent different states.

- **Unused (Gray)**—The device does not detect the traffic from the terminal that uses the IP address.
- **Normal (Green)**—The device has detected the traffic from the terminal, and the traffic is between the bandwidth lower limit and the bandwidth upper limit.
- **Abnormal (Orange)**—The terminal is in abnormal state, which includes the following situations:

    - **Poorly connected**—The traffic from the terminal is below the bandwidth lower limit.
    - **Illegally used**—The IP address of the terminal is used by another illegal terminal. The device detects this situation when terminal information changes.
- **Unreachable (Red)**—The device detected the traffic from the terminal and then cannot detect the traffic. This state transitions to the **Unused** state after being kept for seven days.
- **Blocked (Purple)**—The IP address of the terminal is administratively blocked.

Terminal information

This section displays information about and states of all terminals for monitoring purposes. By monitoring the MAC address, manufacturer, and model information of a terminal, you can prevent its IP address from being illegally used or prevent it from being illegally replaced. You can also click **Unblocked** or **Blocked** to block or unblock a terminal.

Restrictions and guidelines

The block function can be used only after you click **Enable globally** on the **Policies** > **Attack Defense** > **Blacklist** page.

Security policy

This help contains the following topics:

Introduction

A security policy defines a set of filtering criteria for identifying traffic. The filtering criteria include the following types: source security zone, destination security zone, source IP address and source MAC address, destination IP address, user, application, terminal, service, VRF, and time range. The device matches packets against the security policies and takes the action stated in the policy on the matched packets. Packets that match no security policies are discarded. A policy matches all packets if no criteria are specified for the policy.

Security policy name

You can configure multiple security policies, each of which must be uniquely identified by its name and type.

Security policy filtering criteria

The filtering criteria include the following types: source security zone, destination security zone, source IP address and source MAC address, destination IP address, user, application, terminal, service, VRF, and time range.

A packet is considered matched if it matches all the criterion types in a policy. Each criterion type includes one or more criteria, and a packet matches a criterion type if it matches any criterion of the type.

Security policy matching order

The device matches packets against security policies in the order the policies were created. Follow the depth-first order during policy creation to create policies with stricter match criteria first.

Security policies in the **Policies** > **Security Policies** > **Security Policies** page are displayed in the policy creation order. Policies created first come first in the list. You can move the policies to change the policy matching order.

Policy matching acceleration

This feature accelerates security policy matching to enhance connection establishment and packet forwarding performance, especially for a device using multiple policies to match packets from multiple users.

Matching of security policies switched from object policies is accelerated by default. You need to activate rule matching acceleration if a policy is modified or newly added or if the acceleration feature is deactivated for certain reasons. The following methods are available for activating policy matching acceleration:

- **Manual activation**—Activates security policy matching acceleration immediately after you click Activate. You can perform manual activation after a policy is modified or the acceleration feature is deactivated.
- **Automatic activation**—Enables the system to detect security policy changes at specific intervals and activate security policy matching acceleration automatically if any change has been made. If there are 100 or less security policies, the interval is 2 seconds. If there are over 100 security policies, the interval is 20 seconds.

Security policy group

Security policy grouping allows users to enable, disable, delete, and move security policies in the same security policy group in batches. You can specify a security policy group for each security policy or specify a range of security policies for each security policy group.

A security policy takes effect only when both the security policy and its security policy group are enabled.

Import and export

This feature allows the fast migration of security policy configurations. You can export the specific or all security policy settings and perform incremental import.

When importing a file, follow these restrictions and guidelines:

- If a configuration item (a time range for example) in the imported file has the same name as an existing item, the imported item will overwrite the existing one.
- The import process terminates if a policy fails to be imported, but the policies that have been imported are not affected and cannot be rolled back.
- Make sure the file is in CFG format.

Restrictions and guidelines

Restrictions and guidelines: Security policies

- You can move security policies to change their matching order among policies of the same type.
- A newly added security policy is listed below the existing security policies of the same type.
- If a security policy uses an object group that has no objects, the security policy cannot match any packets. For more information, see the online help for object groups.
- If policy matching acceleration fails to be activated by clicking Activate, the matching of policies that have been accelerated is not affected.
- You also need to activate policy matching acceleration if the objects in an object group used by a security policy change.
- The aging time configured for a security policy takes precedence over the aging times configured in **Session Aging Time Set**.
- When inter-VLAN bridge forwarding is configured, the statistics collection feature collects statistics only about packets discarded by the security policy. Statistics about permitted packets are not collected.
- Only IPv4 security policies support using source MAC addresses as the filtering criteria.
- Before configuring content security for a non-default context, make sure content security settings have been activated for the default context. To activate content security settings for a context, click **Submit** on the security policy page of the context.

Restrictions and guidelines: Security policy groups

- If you specify a security policy group for a security policy, the policy will be added to the security policy group as its last policy.
- If you remove the first security policy from a security policy group, the policy will be placed before the policy group. If you remove any other security policy from the security policy group, the policy will be placed after the policy group.
- You cannot move a security policy group that does not contain any policies or move a security policy group before or after an empty security policy group.
- You cannot move a security policy group to a place between policies in another security policy group.
- If you move a security policy to a place before or after a security policy group, the policy joins the group automatically.

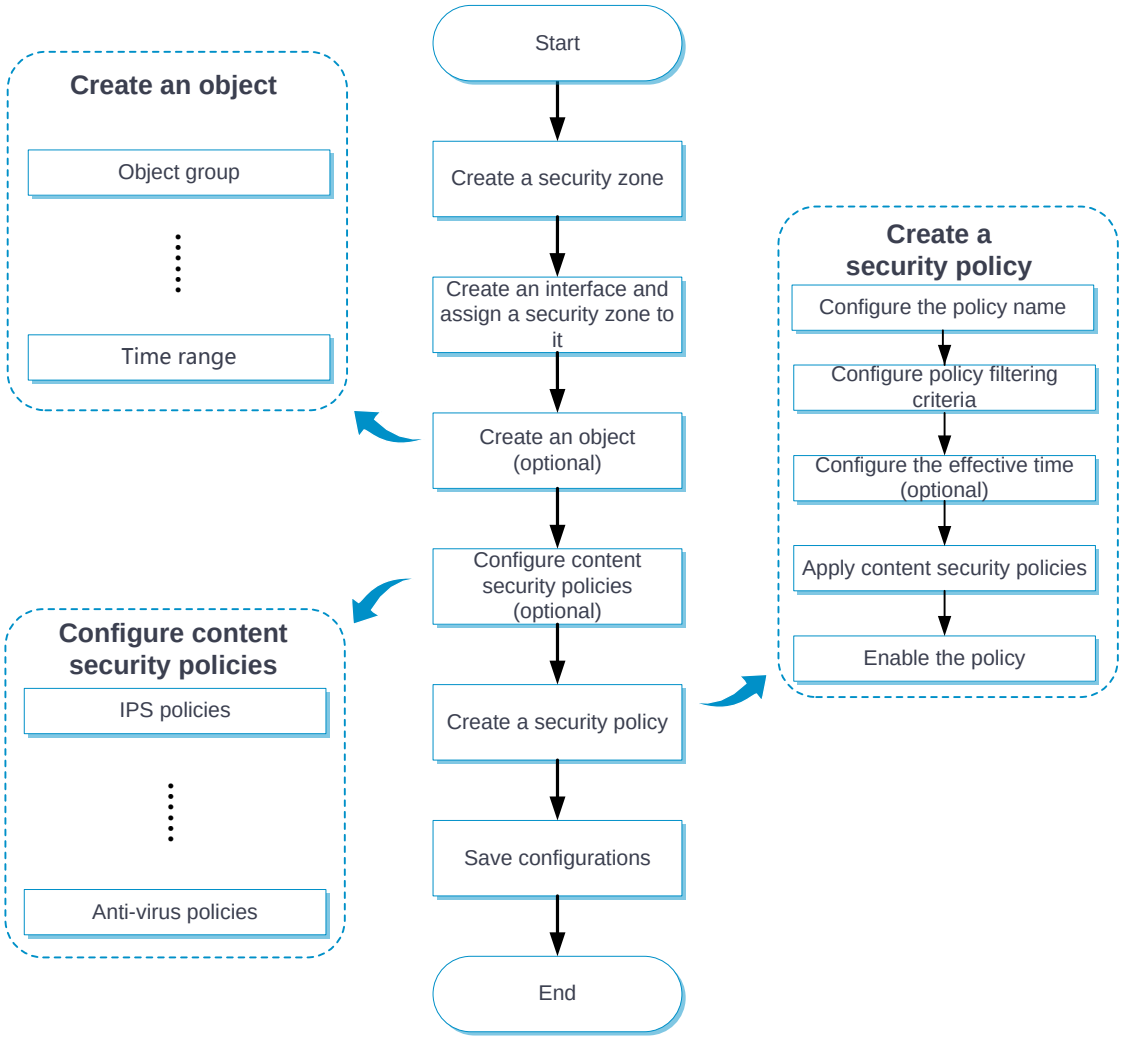
Restrictions and guidelines: Import and export

- You can export only user-defined applications, terminals, and security zones. Predefined applications, terminals, and security zones cannot be exported.
- The file to be imported can contain only security settings available for export.
- When exporting security zone and VRF settings, their binding relations with interfaces are not exported. You must configure interface binding for imported security zones and VRFs.
- The export operation exports only security policy settings and does not export settings about objects used by the security policy.
- Only one user can perform importing or exporting at a time.

Configure security policies

Configure a security policy as shown in Figure 1.

Figure 1 Security policy configuration procedure



Create a security policy

1. Select **Policies** > **Security Policies** > **Security Policies**.

2. Click **Create** and then select **Create a policy**.

3. Create a security policy.

Table 1 Security policy configuration items

Item	Description
Name	Enter a name for the security policy. Security policies of the same type cannot have the same name.
Auto naming	Select whether to enable the system to automatically name the security policy. With this feature enabled, you can specify only one source security policy and one destination security policy.
Source zone	Specify a source security zone as a filtering criterion.
Destination zone	Specify a destination security zone as a filtering criterion.
Type	Specify the security policy type. Options include: • IPv4. • IPv6.
Policy group	Specify a security policy group for the security policy.
Description	Configure a description for the security policy.
Action	Specify the security policy action. Options include: • **Permit**—Allows matched packets to pass. • **Deny**—Discards matched packets.
Source IP/MAC address	Specify a source IP/MAC address as a filtering criterion. Only IPv4 security policies support using source MAC addresses for packet filtering.
Destination address	Specify a destination IP address as a filtering criterion.
Service	Specify a service as a filtering criterion.

Item	Description
Application	Specify an application or application group as a filtering criterion.
Terminal	Specify a terminal or terminal group as a filtering criterion.
User	Specify a user or user group as a filtering criterion.
Time range	Specify the time range during which the security policy rule is in effect.
VRF	Configure the security policy rule to take effect on packets of the specified VRF.
Content security	Configure Deep Packet Inspection (DPI) services for matched packets.
Logging	Enable logging for matched packets.
Match counting	Enable statistics collection for matched packets.
Statistics collection period	Specify the statistics collection period. Options include **Permanent** and **Custom**.
Session aging	Set the aging time for stable sessions created for packets matching the security policy. If the aging time is not configured, stable sessions use the aging time configured on the **System** > **Session Aging Time Set** > **Protocol Session Aging Set** page.
Persistent session aging	Set the aging time for persistent sessions created for packets matching the security policy. If the aging time is not configured, stable sessions use the aging time configured on the **System** > **Session Aging Time Set** > **Protocol Session Aging Set** page.
Policy status	Select whether to enable this policy.
Redundancy analysis	Select whether to access the **Redundancy Analysis** page after the policy creation.

4. Click **OK**.
5. For the security policy to take effect immediately, click **Activate**.

Insert a security policy

1. Select **Policies** > **Security Policies** > **Security Policies**.
2. To insert a security policy to the place before or after all existing security policies, click **Insert** and select **First** or **Last**. To insert a security policy to the place before or after a specific policy, select the target policy, click **Insert**, and then select **Before** or **After**.
3. Configure the policy to be inserted and then click **OK**. For more information, see Table 1.

   The inserted policy will be displayed on the **Security Policies** page.
4. For the security policy to take effect immediately, click **Activate**.

Create a security policy group

1. Select **Policies** > **Security Policies** > **Security Policies**.
2. Click **Create** and then select **Create a policy group**.
3. Create a security policy group.

Table 2 Security policy group configuration items

Item	Description
Name	Enter a name for the security policy group.

Item	Description
Description	Configure a description for the security policy group.
Type	Specify the security policy group type. Options include: • IPv4. • IPv6.
Start policy	Specify the name of the start policy of a policy range in which all the security policies will be add to the group.
End policy	Specify the name of the end policy of a policy range in which all the security policies will be added to the group. Make sure the end policy is listed below the start policy and policies in the specified policy range do not belong to any other policy groups.

4. Click **OK**.

Security policy redundancy analysis

This help contains the following topics:

- Introduction
- Restrictions and guidelines
- Perform redundancy analysis

Introduction

This feature allows the system to compare the filtering criteria of existing security policies and identify redundant policies for users to simplify the configuration. Redundant security policies do not take effect because no packets can match the policies. A security policy is considered redundant in the following conditions:

- The security policy uses the same filtering criteria as a policy created earlier.
- The security policy uses filtering criteria that are covered by a policy created earlier.

To avoid effect on the network, perform this task when the traffic load is light. As a best practice, perform redundancy analysis right after you complete configuring security policies.

The system performs redundancy analysis again automatically if a security policy is modified from the page.

Restrictions and guidelines

- This feature analyzes only enabled security policies.
- This feature analyzes a maximum of 100 security policies at a time. If more than 100 security policies exist on the device, modify or delete the discovered redundant policies and then perform redundancy analysis again.
- Redundancy analysis consumes CPU resources. As a best practice, perform redundancy analysis when the traffic load is light.

Perform redundancy analysis

1. Select **Policies** > **Security Policies** > **Redundancy Analysis**.
2. Click **Start** to start a redundancy analysis.

   Redundant security policies will be displayed in the list in the order these policies were created.
3. Modify or delete redundant security policies.
   - To modify a redundant policy, click the **Edit** icon for the policy.
   - To delete a redundant policy, select the policy, and then click **Delete**.

Security policy hit analysis

Introduction

The Policy Hit Analysis page displays security policies that have not matched any packets in the policy creation order. Policies created first come first in the list.

A security policy is not hit if either of the following conditions exists:

- No packets match the filtering criteria specified for the policy.
- The policy is redundant because another security policy with less strict filtering criteria were created earlier than the policy.

Restrictions and guidelines

Match counting or statistics collection must be enabled for security policies for the system to perform policy hit analysis.

Perform policy hit analysis

1. Select **Policies** > **Security Policies** > **Policy Hit Analysis**.
2. View, modify, or delete security policies that have not matched any packets.

Table 1 Policy hit analysis configuration items

Item	Description
Time range	Select a time range for the analysis from the menu at the top right corner. Options include: • Today. • Last 3 days. • Last 7 days. • Last 30 days. • Last 3 months. • Last 6 months. • Last 12 months. • Last 3 years.
Edit	To modify a security policy, click the **Edit** icon for the policy.
Delete	To delete a security policy, select the policy and then click **Delete**.

3. After policy modification or deletion, click **Activate** to have the security policy configurations take effect immediately.

Security policy optimization

This help contains the following topics:

Introduction

About policy optimization

This feature enables the system to discover potential risks in security policies configured with application filtering criteria and enables users to optimize content security settings to lower the risks.

You can use this feature to optimize the existing security policies or to analyze application security risks to provide reference for precise security policy configuration. To analyze application risks for

future reference, configure a security policy with loose filtering criteria and then perform policy optimization.

Operating mechanism

Policy optimization operates as follows:

1. Identifies application information in the permitted traffic.
2. Compares the configured content security settings with the recommended settings in the application signature database. The database contains information about the recommended content security settings for each application.
3. Evaluates the security condition of the security policies based on the comparison result.

The feature scores the overall security condition and provides detailed security risk analysis for each security policy configured with application filtering criteria. Table 1 shows the information on the **Policy Optimization** page.

Table 1 Policy Optimization page information

Item	Description
Overall security score	Score for the overall security condition of all the security policies. A higher score represents a securer condition.
Security policy name	Name of the security policy.
Type	Security policy type. Options include: • IPv4. • IPv6.
Security level	Security level, in the range of 1 to 5. A higher value represents higher risks.

Item	Description
Total traffic	Total matching traffic for the security policy.
Application	Applications identified from the permitted traffic.
Traffic	Traffic amount and percentage for each application.
Security risks	Security risks of all identified applications.
Status	Security policy optimization status: • **Unsolved**—Indicates that the security policy has not been optimized. • **Solved**—Indicates that the security policy has been optimized but there still are security risks in the security policy.

Optimization methods

This feature provides the following optimization methods:

- **Automatic batch optimization**—Enables the system to optimize content security settings for all the security policies with security risks as recommended in the application signature database.
- **Manual optimization**—Enables users to optimize content security settings for a security policy as needed.

Table 2 shows the security risks and the corresponding content security measures.

Table 2 Security risks and the corresponding content security measures

Security risks	Content security measures
Vulnerability	IPS, anti-virus
Malware-vehicle	IPS, anti-virus
Data-loss	File filtering, data filtering
Bandwidth-consuming	URL filtering You can also specify the maximum bandwidth to lower the risk. For more information, see the online help for bandwidth management.
Misoperation	URL filtering
Tunneling	IPS
Evasive	URL filtering
Productivity-loss	URL filtering You can also specify the maximum bandwidth to lower the risk. For more information, see the online help for bandwidth management.

Restrictions and guidelines

- This feature analyzes security risks only in packets permitted by security policies.
- When a large number of security policies exist, policy optimization might consume a lot of CPU resources. Please use this feature when the network is not busy.
- You cannot add new security policies during automatic batch optimization.

- Automatic batch optimization stops if a master/backup switchover or memory threshold alert occurs during the optimization process. Policies that have been optimized will not be restored. To restart the optimization, click the **Auto batch optimization** button after the master/backup switchover finishes or the memory usage drops below the threshold.

Perform policy optimization

Prerequisites

Before you perform policy optimization, make sure statistics collection is enabled and security policies configured with application filtering criteria exist.

Automatic batch optimization

1. Click **Policies** > **Security Policies** > **Policy Optimization**.
2. Click **Auto batch optimization** to start an automatic batch optimization.

Manual policy optimization

1. Click **Policies** > **Security Policies** > **Policy Optimization**.
2. Click the button in the **Action** field for the security policy to be modified.
3. In the window that opens, change content security settings as needed.

Table 3 Manual policy optimization configuration items

Item	Description
Security policy name	Name of the security policy.
Application	Select the applications for which you are to modify the content security settings.
Traffic	Traffic amount for each application.
Severity level	Risk severity level in the range of 1 to 5. A higher value represents higher risks.
Security risks	Security risks of the identified applications.
Content security	Select content security measures for the selected applications. By default, the field displays content security settings configured for the security policy. If no content security settings are configured, the field displays the default content security settings.
Optimization action	Select whether to generate a new security policy. Options include: • **Generate a new policy**—Enables the system to retain the existing security policy and generate a new security policy with the configured settings. The new security policy will be placed before the existing policy and have a higher priority in packet matching. • **Optimize the existing policy**—Enables the system to modify the content security settings of the existing policy.
Auto optimization	Enables users to optimize the security policy as recommended.

4. Click **OK**.

Attack defense

This help contains the following topics:

Introduction

As an important network security feature, attack defense detects attacks by inspecting arriving packets and takes prevention actions.

Attack defense policy

An attack defense policy contains a set of attack detection and prevention action configuration. Prevention actions include logging, packet dropping, blacklisting, and client verification. The device supports the following attack defense policies:

- Scanning attack defense policy.
- Flood attack defense policy.
- Single-attack defense policy.

Apply an attack defense policy to a security zone to inspect packet received in the security zone.

Scanning attack detection and prevention

Scanning is a preintrusion activity used to prepare for intrusion into a network. The scanning allows the attacker to find a way into the target network and to disguise the attacker's identity.

Attackers use scanning tools to probe a network, find vulnerable hosts, and discover services that are running on the hosts. Attackers can use the information to launch attacks.

The device can detect and prevent the IP sweep (address scanning) and port scanning attacks. If an attacker performs port scanning from multiple hosts to the target host, distributed port scan attacks occur.

Apply a scanning attack defense policy to the security zone that is connected to the external network. Scanning attack detection inspects the incoming packet rate of connections to the target system. If a source initiates connections at a rate equal to or exceeding the pre-defined threshold, the device can take the following actions:

- Output logs.
- Drop subsequent packets from the IP address of the attacker.
- Add the attacker's IP address to the IP blacklist.

You can specify a detection sensitivity level for a scanning attack defense policy. The threshold values and detection periods are fixed for detection sensitivity levels **high**, **medium**, and **low**. To customize the threshold and the detection period, set the detection level to **User-defined**.

If the prevention action is adding attacker's IP address to the IP blacklist, you must enable the blacklist feature on the security zone to which the scanning attack defense policy is applied.

Flood attack detection and prevention

An attacker launches a flood attack by sending a large number of forged requests to the victim in a short period of time. The victim is too busy responding to these forged requests to provide services for legal users, and a DoS attack occurs.

Apply a flood attack defense policy to the security zone that is connected to the external network to protect internal servers. Flood attack detection monitors the rate at which connections are initiated to the internal servers. With flood attack detection enabled, the device is in attack detection state. When the packet receiving rate from an IP address or packet sending rate to an IP address reaches or exceeds the source or destination IP-based threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure flood attack detection and prevention for a specific IP address. For non-specific IP addresses, the device uses the global attack prevention settings.

An appropriate threshold can effectively prevent attacks. The system provides the threshold learning feature to automatically learn the global threshold. This feature allows the device to learn the global threshold based on the traffic flows in the network as follows:

1. Monitors the packet sending rate in the network.
2. Calculates the global threshold based on the peak rate learned within the threshold learning duration.

The threshold learning feature includes the following modes:

- **One-time learning**—The device performs threshold learning only once.
- **Periodic learning**—The device performs threshold learning at intervals. The most recent learned threshold always takes effect.

The threshold learning learns the threshold of all types of flood attacks. You can enable auto application of the learned threshold.

If the network traffic statistics is not known yet, use the default settings of the flood attack prevention parameters first, and then adjust the threshold based on the threshold learning result.

Single-packet attack detection and prevention

Single-packet attacks are also known as malformed packet attacks. An attacker typically launches single-packet attacks by using the following methods:

- An attacker sends defective packets to a device, which causes the device to malfunction or crash.
- An attacker sends normal packets to a device, which interrupts connections or probes network topologies.
- An attacker sends a large number of forged packets to a target device, which consumes network bandwidth and causes denial of service (DoS).

Apply the single-packet attack defense policy to the security zone that is connected to the external network. Single-packet attack detection inspects incoming packets based on the packet signature. If an attack packet is detected, the device can take the following actions:

- Output logs.
- Drop attack packets.

The device supports detecting both well-known single-packet attacks and attack packets with user-defined signatures.

Attack detection exemption

The attack defense policy uses the ACL to identify exempted packets. The policy does not check the packets permitted by the ACL. You can configure the ACL to identify packets from trusted servers. The exemption feature reduces the false alarm rate and improves packet processing efficiency.

If an ACL is used for attack detection exemption, only the following match criteria in the ACL permit rules take effect:

- Source IP address.
- Destination IP address.
- Source port.
- Destination port.
- Protocol.
- VRF.
- Non-first fragments.

Client verification

The client verification feature protects servers against TCP, DNS, DNS reply, HTTP, and SIP flood attacks. The device enabled with client verification is located between the client and the protected server, and verifies the connection initiated by the client.

IP addresses protected by client verification can be manually added or automatically learned:

- You can manually add protected IP addresses. The device performs client verification when it receives the first packet destined for a protected IP address.

- The client verification can automatically add victims' IP addresses to the protected IP list when collaborating with flood attack detection. Make sure client verification is specified as the flood attack prevention action.

The device directly forwards packets from trusted IP addresses.

TCP client verification

The TCP client verification feature protects TCP servers against the following flood attacks:

- SYN.
- ACK.
- SYN-ACK.
- FIN.
- RST.

TCP client verification can operate in the following modes:

- **Safe reset**—Enables unidirectional TCP proxy for packets only from TCP connection initiators. The unidirectional TCP proxy is sufficient for most scenarios because attacks are often seen from clients.
- **SYN cookie**—Enables bidirectional TCP proxy for TCP clients and servers.

The safe reset mode functions as follows:

1. After receiving a SYN packet destined for a protected server, the TCP proxy sends back a SYN ACK packet with an invalid sequence number.
2. If the TCP proxy receives an RST packet from the client, the client is verified as legitimate.
3. The TCP proxy adds the client's IP address to the trusted IP list. The client initiates the connection again and the TCP proxy directly forwards the TCP packets to the server.

The safe reset mode requires that TCP clients comply with the TCP protocol suite. The TCP proxy will deny a legitimate client to access the server if the client does not comply with the TCP protocol suite. With client verification, the TCP connection establishment takes more time than normal TCP connection establishment.

SYN cookie mode requires two TCP connections to be established as follows:

1. After receiving a SYN packet from a client to a protected server, the TCP proxy sends back a SYN ACK packet with the window size 0. If the client responds with an ACK packet, the client is verified as legitimate. The proxy device establishes a TCP connection with the client.
2. The TCP proxy device establishes a connection with the server through a new three-way handshake that has a different window size. This connection uses a different sequence number from the connection between the client and proxy device.

In SYN cookie mode, the TCP proxy is the server proxy that communicates with clients and the client proxy that communicates with server. Choose this mode when the following requirements are met:

- The TCP proxy device is deployed on the key path that passes through the ingress and egress of the protected server.
- All packets exchanged between clients and server pass through the TCP proxy device.

DNS client verification

The DNS client verification feature protects DNS servers against DNS flood attacks. It is configured on the device where packets from the DNS clients to the DNS servers pass through. The device with DNS client verification feature configured is called a DNS client authenticator.

The DNS client verification functions as follows:

1. Upon receiving a UDP DNS query destined for a protected server, the DNS client authenticator responds with a DNS truncate (TC) packet. The DNS truncate packet requires the client to initiate a query in a TCP packet.

2. When the authenticator receives a DNS query in a TCP SYN packet to port 53 from the client, the authenticator responds with a SYN-ACK packet that contains an incorrect sequence number.
3. When the authenticator receives a RST packet from the client, the authenticator verifies the client as legitimate.
4. The authenticator adds the client's IP address to the trusted IP list and forwards the trusted client's subsequent packets to the server.

The DNS client verification feature requires that DNS clients comply with the TCP/IP protocol suite. The DNS client authenticator will deny a legitimate client to access the server if the client does not comply with the TCP protocol suite. With client verification, the DNS connection establishment takes more time than normal TCP connection establishment.

DNS reply source verification

The DNS reply source verification feature protects DNS clients from DNS reply flood attacks. The device with DNS reply source verification feature configured is called a DNS reply authenticator.

The DNS reply source verification functions as follows:

1. Upon receiving a UDP DNS reply destined for a protected client, the DNS reply authenticator sends back a DNS query packet with the locally generated query ID and port number.
2. After receiving the DNS query, a valid DNS server responds with a DNS reply that contains a new query ID and destination port.
3. The DNS reply authenticator verifies the query ID and destination port in the reply. If the query ID and destination port are the same as the query ID and port number the authenticator has sent, the DNS server passes verification. The authenticator will forward subsequent packets from the server.

HTTP client verification

The HTTP client verification feature protects HTTP servers against HTTP flood attacks. It is configured on the device where HTTP GET or POST request packets from the HTTP clients to the HTTP servers pass through. A device with HTTP client verification feature configured is called an HTTP client authenticator.

The HTTP client authenticator uses HTTP GET requests to verify the HTTP client as follows:

1. Upon receiving a SYN packet destined for a protected HTTP server, the HTTP client authenticator performs TCP client verification in SYN cookie mode. If the client passes the TCP client verification, a TCP connection is established between the client and the authenticator.
2. When the authenticator receives an HTTP GET packet from the client, it performs the first redirect verification. The authenticator records the client information and responds with an HTTP Redirect packet. The HTTP Redirect packet contains a redirect URI and requires the client to terminate the TCP connection.
3. After receiving the HTTP Redirect packet, the client terminates the TCP connection and then establishes a new TCP connection with the authenticator.
4. When the authenticator receives the HTTP GET packet, it performs the second redirection verification. The authenticator verifies the following information:
    - The client has passed the first redirection verification.
    - The URI in the HTTP GET packet is the redirect URI.
5. If the client passes the second redirection verification, the authenticator adds its IP address to the trusted IP list, and responds a Redirect packet. The Redirect packet contains the URI that the client originally carried and requires the client to terminate the TCP connection.
6. The authenticator directly forwards the trusted client's subsequent packets to the server.

The HTTP client authenticator uses HTTP POST requests to verify the HTTP client as follows:

1. Upon receiving a SYN packet destined for a protected HTTP server, the HTTP client authenticator performs TCP client verification in SYN Cookie mode. If the client passes the TCP client verification, a TCP connection is established between the client and the authenticator.
2. When the authenticator receives an HTTP POST request from the client, it performs the redirect verification. The authenticator records the client information and responds with an HTTP Redirect packet. The HTTP Redirect packet contains a redirect URI and the Set-Cookie header, and requires the client to terminate the TCP connection.
3. After receiving the HTTP Redirect packet, the client terminates the TCP connection and then establishes a new TCP connection with the authenticator.
4. When the authenticator receives the HTTP POST request, it performs the timeout verification. The authenticator verifies the following information:
    - The client has passed the redirection verification.
    - The HTTP POST request contains a valid cookie.
5. If the client passes the timeout verification, the authenticator adds its IP address to the trusted IP list, and responds with an HTTP Timeout packet. The Timeout packet contains the URI that the client originally carried and requires the client to terminate the TCP connection.
6. The authenticator directly forwards the trusted client's subsequent packets to the server.

SIP client verification

The SIP client verification feature protects SIP servers against SIP flood attacks.

The device with SIP client verification feature configured is called a SIP client authenticator. The SIP client verification process is as follows:

1. Upon receiving a UDP INVITE packet destined for a protected server, the SIP client authenticator sends back an OPTIONS packet with a branch value.

2. After receiving the OPTIONS packet, the client sends a reply to the SIP client authenticator.
3. When receiving the reply, the SIP client authenticator verifies the branch value in the reply. If the branch value in the reply packet is the same as the branch value in the OPTIONS packets that the SIP client authenticator has sent, the client passes verification. The authenticator will forward subsequent packets from the client.

A legitimate SIP client might not pass the client verification if packets sent by the SIP client do not contain complete header information due to fragmentation.

Blacklist

The blacklist feature is an attack prevention method that filters packets by IP addresses or address object groups in blacklist entries. Compared with ACL-based packet filtering, IP blacklist filtering is simpler and provides effective screening at a faster speed.

Blacklist entries can be manually added or dynamically learned:

- You can manually add an IP blacklist entry. These entries do not age out by default. You can set an aging time for each entry.
- The device can automatically add IP blacklist entries when collaborating with scanning attack detection. Each dynamically learned IP blacklist entry has an aging time, which is user configurable. Make sure adding the attacker's IP address to the IP blacklist is specified as the scanning attack prevention action.

Whitelist

This feature exempts packets sourced from the subnets specified in the whitelisted address object group from attack detection. Packets from the whitelisted address are directly forwarded whether they are attack packets or not.

The whitelist can contain only one address object group. The address object group can only be manually added to or deleted from the whitelist.

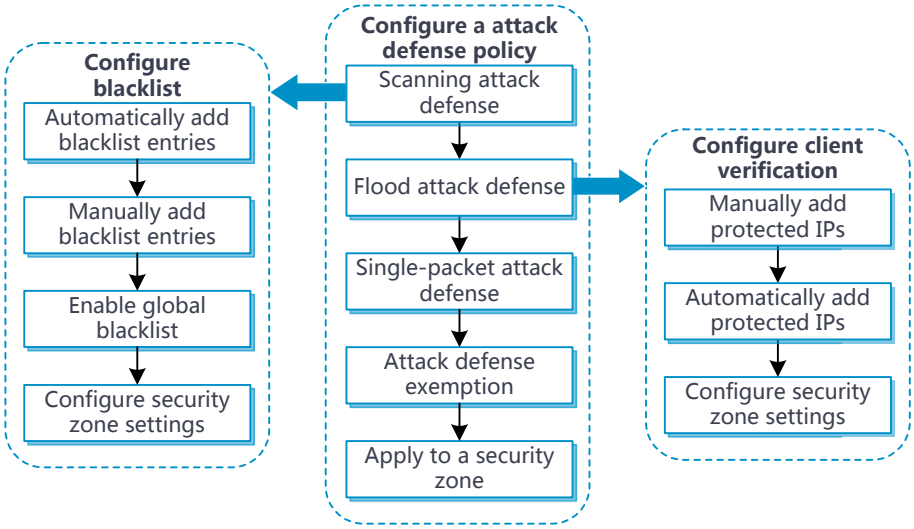
Restrictions and guidelines

- If a device has multiple service cards, the threshold value in a flood attack policy is card specific. The global threshold of the device is the product of multiplying the threshold value by the service card quantity.
- The client verification action in the attack defense policy takes effect only when the client verification is enabled in the security zone.
- Adjust the threshold according to the application scenarios. If the number of packets sent to a protected server is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.
- If the specified ACL does not exist or does not contain a rule, attack detection exemption does not take effect.
- If an ACL is used for attack detection exemption, only the following match criteria in the ACL permit rules take effect:
    - Source IP address.
    - Destination IP address.
    - Source port.
    - Destination port.
    - Protocol.
    - VRF.
    - Non-first fragments.

- The threshold learning feature learns the thresholds of the following attacks only on the default ports:
  - DNS flood attacks.
  - DNS response flood attacks.
  - SIP flood attacks.
  - HTTP flood attacks.
- Once you set the source IP-based threshold to **0** for a flood attack type, the device does not apply the source IP-based learning result to this attack type even if learning result automatic application is enabled. You cannot manually apply the source IP-based learning result to this attack type, neither. The same restriction applies when you set the destination IP-based threshold to **0**.

Configure attack defense and prevention

Figure 1 Attack defense and prevention configuration procedure



Configure an attack defense policy

Before you configure attack defense and prevention, create an attack defense policy. Specify the attack detection criteria and prevention actions in the policy based on the network security requirements.

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Attack Defense Policies**.
3. Click **Create**.
4. Create an attack defense policy.

Table 1 Configuration items for an attack defense policy

Item	Description
Policy name	Enter the name of an attack defense policy. Valid characters include letters, digits, underscores (_), and hyphens (-).
Apply to	Select a security zone to which the attack defense policy is applied. A security zone can have only one attack defense policy applied. An attack defense policy can be applied to multiple security zones. The list includes the default security zone and security zones that have been configured on the **Network** > **Security Zones** page.

To create a scanning attack defense policy, click the **Scanning Attack Defense** tab and configure the policy as described in Table 2.

Table 2 Configuration items for a scanning attack defense policy

Item	Description
Detection sensitivity	Scanning attack detection level: • **Close**—Disables the scanning attack defense. • **Low**—Specifies the low level. This level provides basic scanning attack detection and has a low false alarm rate, but many scanning attacks cannot be detected. • **Medium**—Specifies the medium level. Compared with the high and low levels, this level has medium false alarm rate and attack detection accuracy. • **High**—Specifies the high level. This level can detect most of the scanning attacks, but has a high false alarm rate. Some packets from active hosts might be considered as attack packets. • **User-defined**—Specifies the user-defined level. You can set a threshold for scanning attack prevention. Configure the following parameters as needed: • **Enable port scan attack prevention**—This feature is enabled when **Detection sensitivity** is set to **Low**, **Medium**, or **High**. You can determine whether to enable this feature when **Detection sensitivity** is set to **User-defined**. • **Threshold (packets)**—Threshold that triggers port scanning attack prevention. The value is 100000 for the low detection sensitivity level, 40000 for the medium detection sensitivity level, and 5000 for the high detection sensitivity level. You can specify a threshold when **Detection sensitivity** is set to **User-defined**. This parameter is not displayed when **Detection sensitivity** is disabled. • **Enable address scan attack prevention**—This feature is enabled when **Detection sensitivity** is set to **Low**, **Medium**, or **High**. You can determine whether to enable this feature when **Detection sensitivity** is set to **User-defined**. • **Threshold (packets)**—Threshold that triggers address scanning attack prevention. The value is 100000 for the low detection sensitivity level, 40000 for the medium detection sensitivity level, and 5000 for the high detection sensitivity level. You can specify a threshold when **Detection sensitivity** is set to **User-defined**. This parameter is not displayed when **Detection sensitivity** is disabled. • **Detection period**—Scanning attack detection cycle. The detection period is 10 seconds when **Detection sensitivity** is set to **Low**, **Medium**, or **High**. You can specify a detection cycle when **Detection sensitivity** is set to **User-defined**. This parameter is not displayed when **Detection sensitivity** is disabled.

Item	Description
Actions	Prevention actions against scanning attacks. • **Generate logs**. • **Drop attack packets**. • **Add attackers' IP addresses to blacklist**. • **Age out after** *n* **minutes**—Aging time for the dynamically added blacklist entries. This parameter is available only when **Add attackers' IP addresses to blacklist** is selected. Prevention actions are not available when **Detection sensitivity** is disabled.

To create a flood attack defense policy, click the **Flood Attack Defense Settings** tab. To configure global parameters for the attack defense policy, see Table 3. To configure IP-specific flood attack defense, see Table 5.

Table 3 Configuration items for flood attack defense global settings

Item	Description
Attack type	Flood attack types: • **ACK**—Specifies the ACK flood attack type. An ACK packet is a TCP packet only with the ACK flag set. Upon receiving an ACK packet from a client, the server must search half-open connections for a match. An ACK flood attacker sends a large number of ACK packets to the server. This causes the server to be busy searching for half-open connections, and the server is unable to process packets for normal services. • **DNS**—Specifies the DNS flood attack type. The DNS server processes and replies all DNS queries that it receives. A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries. • **DNS reply**—Specifies the DNS reply flood attack type. The DNS server processes and replies all DNS replies that it receives. A DNS reply flood attacker sends a large number of forged DNS replies. This attack consumes the bandwidth and resources of the DNS

Item	Description
	server, which prevents the server from processing and replying legal DNS replies. • **FIN**—Specifies the FIN flood attack type. FIN packets are used to shut down TCP connections. A FIN flood attacker sends a large number of forged FIN packets to a server. The victim might shut down correct connections, or be unable to provide services because it is busy searching for matching connections. • **HTTP**—Specifies the HTTP flood attack type. Upon receiving an HTTP GET or POST request, the HTTP server performs complex operations, including character string searching, database traversal, data reassembly, and format switching. These operations consume a large amount of system resources. An HTTP flood attacker sends a large number of HTTP GET or POST requests that exceed the processing capacity of the HTTP server, which causes the server to crash. • **HTTP slow**—Specifies the HTTP slow flood attack type. When an attacker holds a large number of HTTP concurrent connections to the HTTP server, the system resources of the server are occupied by these connections. As a result, the server cannot process normal services. • **ICMP**—Specifies the ICMP flood attack type. An ICMP flood attacker sends ICMP request packets, such as ping packets, to a host at a fast rate. Because the target host is busy replying to these requests, it is unable to provide services. • **ICMPv6**—Specifies the ICMPv6 flood attack type. An ICMPv6 flood attacker sends ICMPv6 request packets, such as ping packets, to a host at a fast rate. Because the target host is busy replying to these requests, it is unable to provide services. • **RST**—Specifies the RST flood attack type. RST packets are used to abort TCP connections when TCP connection errors occur. An RST flood attacker sends a large number of forged RST packets to a server. The victim might shut down correct connections, or be unable to provide services because it is busy searching for matching connections. • **SIP**—Specifies the SIP flood attack type. After receiving a SIP INVITE packet from a SIP client, the server must allocate resources to establish and trace the session with the SIP client. A SIP flood attacker sends a large number of fake INVITE request packets at a rate exceeding the processing capacity of the SIP server, which causes the server to crash. • **SYN**—Specifies the SYN flood attack type. A SYN flood attacker exploits the TCP three-way handshake characteristics and makes the victim unresponsive to legal users. An attacker sends a large number of SYN packets with forged source addresses to a server. This causes the server to open a large number of half-open connections and respond to the requests. However, the server will

Item	Description
	never receive the expected ACK packets. The server is unable to accept new incoming connection requests because all of its resources are bound to half-open connections. • **SYN-ACK**—Specifies the SYN-ACK flood attack type. Upon receiving a SYN-ACK packet, the server must search for the matching SYN packet it has sent. A SYN-ACK flood attacker sends a large number of SYN-ACK packets to the server. This causes the server to be busy searching for SYN packets, and the server is unable to process packets for normal services. • **UDP**—Specifies the UDP flood attack type. A UDP flood attacker sends UDP packets to a host at a fast rate. These packets consume a large amount of the target host's bandwidth, so the host cannot provide other services.
Src Threshold (pps)	Enter a global source IP-based threshold that triggers flood attack prevention. The value range is 0 to 1000000. The default value is 40000 for ACK flood attack detection and 10000 for other types of flood attack detection. With global flood attack detection configured, the device is in attack detection state. When the receiving rate of the packets originated from an IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. If you set this parameter to **0**, the system does not perform source IP-based flood attack detection.
Dest Threshold (pps)	Enter a global destination IP address-based threshold that triggers flood attack prevention. The value range is 0 to 1000000. The default value is 40000 for ACK flood attack detection and 10000 for other types of flood attack detection. With global flood attack detection configured, the device is in attack detection state. When the sending rate of packets to an IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. The global destination IP-based threshold applies to global flood attack detection. Adjust the threshold according to the application scenarios. If the number of packets sent to a protected server is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold. If you set this parameter to **0**, the system does not perform destination IP-based flood attack detection.
Logging	Enable logging for flood attack events. Log messages are sent to the log system.

Item	Description
Detect All IPs	Enable global flood attack detection.
Client verification	Enable client verification. The device automatically adds the victim IP addresses to the protected IP list, and provides proxy services for protected IP addresses.
Packet drop	Use packet dropping as the prevention action. The device drops subsequent attack packets destined for the victim IP addresses.
Target ports	A comma-separated list of up to 32 port number items, for example, 1-10,80. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. The port number is in the range of 1 to 65535. The device performs flood attack detection only on packets destined for the target ports. The target port setting applies to global flood attack detection and IP address-specific flood attack detection with no port specified. If IP address-specific flood attack detection is configured with specific ports, the device detects flood attacks on these ports for the specified IP address. This parameter is available only for DNS, DNS reply, HTTP, HTTP slow, and SIP flood attack types.
Concurrent connections	Enter a threshold for allowed concurrent HTTP connections. The default is 5000. HTTP slow attack detection is triggered when the number of HTTP concurrent connections reaches the threshold. This parameter is available only for the HTTP slow attack type.
Content-Length	Enter a threshold for the length of the **Content-Length** filed in the HTTP packet header. The value default is 10000. This parameter is available only for the HTTP slow attack type.
Payload length	Enter a threshold for the HTTP packet payload. The default is 50. An HTTP packet is an abnormal packet if its **Content-Length** field value is greater than the specified threshold and its payload is shorter than the specified length. This parameter is available only for the HTTP slow attack type.

Item	Description
Abnormal packets	Enter a threshold for abnormal packets. The default is 10. This parameter is available only for the HTTP slow flood attack type.
Detection cycle	Set an attack detection period. The device takes prevention actions when the number of received abnormal packets exceeds the threshold within the detection period. This parameter is available only for the HTTP slow flood attack type.
Blacklist	Select whether to use blacklisting as an attack prevention action. If the blacklist feature is enabled in the security zone to which the attack defense policy applies, the device drops packets from the blacklisted IP addresses. This parameter is available only for the HTTP slow flood attack type.
Blacklist aging time	Set an aging time of dynamic blacklist entries, in seconds. The default is 10. This parameter is available only when blacklisting is used as a prevention action for the HTTP slow flood attack.
Set threshold learning	Configure threshold learning parameters as shown in Table 4. Before configuring the threshold learning feature on the Edit page, you must complete the configuration of the attack defense policy first.
Apply learned threshold	Use the learned thresholds as the thresholds for flood attack prevention. This setting takes effect only on attack types that are enabled with **Detect All IPs** and have the threshold learning result.

Table 4 Configuration items for threshold learning

Item	Description
Threshold learning	As a best practice, enable threshold learning to provide a reference for threshold setting.

Item	Description
Learning duration	Duration of threshold learning. The system calculates the thresholds for different attacks based on the peak rate learned within the threshold learning duration.
Learning mode	The following modes are available: • **One-time learning**—The device performs threshold learning only once. • **Periodic learning**—The device performs threshold learning at intervals.
Auto apply	Automatically apply the most recent thresholds that the device has learned. This parameter takes effect only on attack types that are enabled with **Detect All IPs** and have the threshold learning result.
Tolerance	Threshold learning tolerance value that increases the learned threshold to a larger value before threshold application. This mechanism enables the threshold learning feature to promptly respond to traffic fluctuation.

To add protected IP addresses against flood attacks, click **Create** in the **Protected IP** area on the **Flood Attack Defense Settings** tab.

Table 5 Configuration items for IP-specific flood attack defense

Item	Description
IP version	Select an IP version, IPv4 or IPv6.
IP address	Enter an IP address to be protected. The protected IPv4 address cannot be 255.255.255.255 or 0.0.0.0. The protected IPv6 address cannot be a multicast address or **::**.
Attack type	For more information, see Table 3.
VRF	VRF to which the protected IP address belongs. You can select an existing VRF or create a new one. The newly created VRF will be

Item	Description
	displayed on the **Network** > **VRF** page.
Dest Threshold (pps)	Set the destination IP-based threshold that triggers flood attack prevention. The default value is 40000 for ACK flood attack detection and 10000 for other types of flood attack detection.

Threshold	Set thresholds for HTTP slow attack defense. The following methods are available:
	• **Global settings**—Select this option to use the global threshold settings in the **Global settings** area.
	• **User-defined**—Select this option and specify thresholds. The default threshold settings are as follows:
	  ◦ The number of concurrent connections is 5000.
	  ◦ The value of the **Content-Length** field is 10000.
	  ◦ The payload length is 50.
	  ◦ The number of abnormal packets is 10.
	This parameter is available only for the HTTP slow flood attack type.

Target ports	Specify ports to be protected. The device detects packets that are destined for the specified ports. The following methods are available: • **Global settings**—Select this option to use the global settings. By default, the global settings protect well-known ports specific to protocols. For example, the HTTP flood attack prevention protects port 80. • **User-defined**—Select this option to specify a port or a comma-separated list of port number items, for example, 1-10,80. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. This parameter is available only for DNS, DNS reply, HTTP, HTTP slow, and SIP flood attack types.
Detection cycle	Set an attack detection period. The following methods are available: • **Global settings**—Select this option to use the global detection period set in the **Global settings** area. • **User-defined**—Select this option and set a detection period. If no detection period is specified, the global detection period applies. This parameter is available only for the HTTP slow attack type.

Item	Description

Action	Specify prevention actions against the flood attack. The following methods are available:
	• **Global settings**——Select this option to use the global prevention actions in the **Global settings** area.
	• **User-defined**——Select this option and specify prevention actions.
	  ◦ **Logging**—Use logging as the prevention action. Flood attack events are logged and log messages are sent to the log system.
	  ◦ **Packet drop**—Use packet dropping as the prevention action. The device drops subsequent attack packets destined for the victim IP addresses.
	  ◦ **Client verification**—Use client verification as the prevention action. The device automatically adds the victim IP addresses to the protected IP list, and provides proxy services for protected IP addresses.

Blacklist	Select whether to use blacklisting as an attack prevention action. The device automatically blacklists the packet source IP address when an attack is detected. If the blacklist feature is enabled in a security zone, the device drops packets from the blacklisted IP address. This parameter is available only for the HTTP slow attack type.
Aging time	Set an aging time of the dynamic blacklist entry, in seconds. The default is 10. This parameter is available only when the blacklisting action is selected for the HTTP slow flood attack.

Table 6 Configuration items for well-known single packet attack defense

Item	Description
Attack type	Specify a well-known single packet attack type: • **IP fragment**—An attacker sends the victim an IP datagram with an offset smaller than 5, which causes the victim to malfunction or crash. • **IP impossible**—An attacker sends IP packets whose source IP

Item	Description
	address is the same as the destination IP address, which causes the victim to malfunction. • **Teardrop**—An attacker sends a stream of overlapping fragments. The victim will crash when it tries to reassemble the overlapping fragments. • **Tiny fragment**—An attacker makes the fragment size small enough to force Layer 4 header fields into the second fragment. These fragments can pass the packet filtering because they do not hit any match. • **IP option abnormal**—An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets. • **Smurf**—An attacker broadcasts an ICMP echo request to target networks. These requests contain the victim's IP address as the source IP address. Every receiver on the target networks will send an ICMP echo reply to the victim. The victim will be flooded with replies, and will be unable to provide services. Network congestion might occur. • **Traceroute**—An attacker uses traceroute tools to probe the topology of the victim network. • **Ping of death**—An attacker sends the victim an ICMP echo request larger than 65535 bytes that violates the IP protocol. When the victim reassembles the packet, a buffer overflow can occur, which causes a system crash. • **Large ICMP**—An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack. • **Large ICMPv6**—An attacker sends large ICMPv6 packets to crash the victim. Large ICMPv6 packets can cause memory allocation error and crash the protocol stack. • **TCP invalid flags**—An attacker sends packets with invalid TCP flags to the target host, which can cause the target system to crash. • **TCP null flag**—An attacker sends TCP packet with no flags to the target host, which can cause the target system to crash. • **TCP all flags**—An attacker sends TCP packet with all flags set to the target host, which can cause the target system to crash. • **TCP SYN-FIN**—An attacker sends TCP packet with both SYN and FIN flags set to the target host, which can cause the target system to crash. • **TCP FIN only flag**—An attacker sends TCP packet with only the FIN

Item	Description
	flag set to the target host, which can cause the target system to crash. • **TCP Land**—An attacker sends the target a large number of TCP SYN packets with the source and destination IP addresses same as the IP of the target. The half connection resources on the target will run out and the target cannot operate correctly. • **WinNuke**—An attacker sends Out-Of-Band (OOB) data to the TCP port 139 (NetBIOS) on the victim that runs Windows system. The malicious packets contain an illegal Urgent Pointer, which causes the victim's operating system to crash. • **UDP Bomb**—An attacker sends a malformed UDP packet. The length value in the IP header is larger than the IP header length plus the length value in the UDP header. When the target system processes the packet, a buffer overflow can occur, which causes a system crash. • **UDP snork**—An attacker sends a UDP packet with destination port 135 (the Microsoft location service) and source port 135, 7, or 19. This attack causes an NT system to exhaust its CPU. • **UDP fraggle**—An attacker sends a large number of packets with source UDP port 7 and destination UDP port 19 (UDP chargen port) to a network. These packets use the victim's IP address as the source IP address. Replies will flood the victim, resulting in DoS. • **IPv6 ext header abnormal**—An attacker sends IPv6 packets with disordered or repeated IPv6 extension headers to the target. • **IPv6 ext header exceed**—An attacker sends IPv6 packets with IPv6 extension headers exceeding the upper limit to the target. In abnormal IPv6 extension header and IPv6 extension header exceeded attack detection, the device examines the ESP header and headers before it. Headers after the ESP header are not examined.
Logging	Enable logging for the single-packet attack events. Log messages are sent to the log system.
Packet drop	Use packet dropping as the prevention action. The device drops subsequent attack packets destined for the victim IP addresses.
Threshold (bytes)	Maximum length of safe ICMP or ICMPv6 packets, in bytes. • 28 to 65534 for ICMP packets. • 48 to 65534 for ICMPv6 packets.

To create a single-packet attack defense policy to detect packets with user-defined signatures, access the **Custom Single-Packet Attack Defense** page, and then click **Create**.

Table 7 Configuration items for a single-packet attack defense policy with user-defined packet signatures

Item	Description
Signature	Packet signatures: • **IP option**—Specifies attack packets with a specific IP option. • **ICMP**—Specifies ICMP attack packets. • **ICMPv6**—Specifies ICMPv6 attack packets • **IPv6 extension header**—Specifies attack packets with IPv6 extension headers.
Value	Signature value in the range of 0 to 255. This value indicates the IP option code, or the type value in ICMP packets, ICMPv6 packets, or IPv6 extension headers.
Logging	Enable logging for the single-packet attack events. Log messages are sent to the log system.
Packet drop	Use packet dropping as the prevention action. The device drops subsequent attack packets destined for the victim IP addresses.

Table 8 Attack detection exemption configuration items

Item	Description
IPv4 exemption	IPv4 ACL for attack detection exemption. You can select an existing IPv4 ACL or create a new IPv4 ACL. The created ACL will be displayed on the **Objects** > **ACLs** > **IPv4 ACLs** page. If the specified ACL does not exist or does not contain a rule, attack

Item	Description
	detection exemption does not take effect.
IPv6 exemption	IPv6 ACL for attack detection exemption. You can select an existing IPv6 ACL or create a new IPv6 ACL. The created ACL will be displayed on the **Objects** > **ACLs** > **IPv6 ACLs** page. If the specified ACL does not exist or does not contain a rule, attack detection exemption does not take effect.

5. Click **OK**.

Configure protected IP addresses

IP addresses protected by client verification can be manually added or automatically learned. The device can automatically add victims' IP addresses to the protected IP list when client verification collaborates with flood attack detection. The device directly forwards packets from trusted IP addresses. Make sure client verification is specified as the flood attack prevention action.

The **Protected IP Addresses** page displays protected IP addresses manually added and automatically learned.

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Protected IP Addresses**.
3. Click **Create**.
4. Configure protected IP addresses.

Table 9 Configuration items for protected IP addresses

Item	Description
Protocol	Protocol type for client verification: • **TCP**—Specifies TCP client verification. • **DNS**—Specifies DNS client verification. • **DNS reply**—Specifies DNS client source verification. • **HTTP**—Specifies HTTP client verification. • **SIP**—Specifies SIP client verification.
VRF	VRF to which the protected IP address belongs. You can select an existing VRF or create a new one. The newly created VRF will be displayed on the **Network** > **VRF** page.
IP version	Select an IP version, IPv4 or IPv6.
IP address	Protected IP address. All connection requests destined for this address are verified by the client verification feature. The attacker sends TCP connection requests, DNS queries, DNS replies, HTTP GET requests, HTTP POST requests, or SIP UDP INVITE requests to the protected IP. The protected IPv4 address cannot be or 255.255.255.255 or 0.0.0.0. The protected IPv6 address cannot be a multicast address or **::**.
Port number	Number of a protected port. By default, DNS client verification protects port 53, HTTP client verification protects port 80, SIP client verification protects port 5060, and TCP client verification protects all ports.

5. Click **OK**.

Configure the blacklist feature

The blacklist feature is an attack prevention method that filters packets by IP addresses or address object groups in blacklist entries.

Blacklist entries can be manually added or dynamically learned. The device can automatically add IP blacklist entries when the blacklist feature collaborates with scanning attack detection. Make sure adding the attacker's IP address to the IP blacklist is specified as the scanning attack prevention action. Each dynamically learned IP blacklist entry has an aging time, which is configured on the **Policies** > **Attack Defense** >**Attack Defense Policies** > **Scanning Attack Defense** page.

Configure the IP blacklist

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Blacklist**.
3. Click **Create**.
4. Add an IP blacklist entry.

Table 10 IP blacklist configuration items

Item	Description
VRF	VRF to which the blacklist belongs. You can select an existing VRF or create a new one. The newly created VRF will be displayed on the **Network** > **VRF** page.
IP version	Select an IP version, IPv4 or IPv6.
Match field	Packet field to compare with the criterion: • Source IP address. • Destination IP address.
IP address	IP address in the blacklist entry. Packets sourced from or destined to the IP address will be dropped.
DS-Lite tunnel peer address	IPv6 address of the B4 element of the DS-Lite tunnel that transmits packets from the blacklisted IPv4 address. This parameter is available when **IPv4** is selected for **IP version**, and

Item	Description
	Source IP is selected for the match field.
Aging time (sec)	Aging time of the blacklist entry. If you do not set the aging time, the blacklist entry never ages out. You must delete it manually.

5. Click **OK**. The **IP Blacklist** page displays the newly added IP blacklist.
6. Click **Enable globally**. The IP blacklist takes effect on all security zones.

Configure the address object group blacklist

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Blacklist**.
3. Click the **Address Object Group Blacklist** tab.
4. Click **Add**.
5. Add an address object group blacklist entry.

Table 11 Address object group blacklist configuration items

Item	Description
Object group type	Select a type of address object groups, IPv4 or IPv6.
Object group name	Enter the name of an address object group.

6. Click **OK**. The **Address Object Group Blacklist** page displays the newly added address object group blacklist.
7. Click **Enable globally**. The address object group blacklist takes effect on all security zones.

Configure the whitelist

The whitelist feature exempts packets sourced from the IP addresses specified in the whitelisted address object group from attack detection.

An address object group can only be manually added to or deleted from the whitelist. To configure an address object group, access the **Objects** > **Object Groups** page.

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Whitelist**.
3. Click **Create**.
4. Add an address object group to the whitelist.

Table 12 Whitelist configuration items

Item	Description
Object group type	Select an IP version, IPv4 or IPv6.
Object group name	You can select an existing address object group or create a new one. The newly created address object group will be displayed on the **Objects** > **Object Groups** page.

5. Click **OK**.

Configure security zone settings

The client verification configuration includes adding protected IP addresses and enabling client verification on security zones.

The blacklist configuration includes enabling the blacklist feature and adding blacklist entries. The blacklist feature can be globally enabled or on a per security zone basis. If the blacklist feature is globally enabled, all security zones are enabled with the blacklist feature. To enable the global blacklist feature, access the **Policies** > **Attack Defense** > **Blacklist** page.

The whitelist configuration includes enabling the whitelist feature and adding whitelist entries. The whitelist feature can be globally enabled or on a per security zone basis. If the whitelist feature is globally enabled, all security zones are enabled with the whitelist feature. To enable the global whitelist feature, access the **Policies** > **Attack Defense** > **Whitelist** page.

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Security Zone Settings**.
3. Enable the client verification, blacklist, or whitelist feature on a security zone.

Table 13 Security zone configuration items

Item	Description
Security zone	Select a security zone. You can create a new security zone on the **Network** > **Security Zones** page.
TCP verification	TCP client verification setting on the a security zone: • **Disable**—Disables TCP client verification. • **SYN Cookie**—Enables bidirectional TCP proxy for TCP client verification.

Item	Description
	• **Safe Reset**—Enables unidirectional TCP proxy for TCP client verification.
DNS verification	Enable or disable DNS client verification on a security zone.
DNS reply source verification	Enable or disable DNS reply source verification on a security zone.
HTTP verification	Enable or disable HTTP client verification on a security zone.
SIP verification	Enable or disable SIP client verification on a security zone.
Blacklist	Enable or disable the blacklist feature on a security zone.
Whitelist	Enable or disable the whitelist feature on a security zone.

4. Click **Apply**.

Risk analysis

This help contains the following topics:

- Introduction
- Configure risk analysis

Introduction

This feature scans devices in an IPv4 or IPv6 address range to find whether specific TCP or UDP ports are opened on these devices. You can enhance the device security based on the scan result.

Configure risk analysis

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Risk Analysis**.
3. Select an address type. Options are IPv4 and IPv6.
4. Configure an IP address range.
5. Select or enter TCP port numbers.
6. Select or enter UDP port numbers.
7. Click **Scan**.

   During the scanning progress, you can minimize the scanning progress window and perform operations on other pages.

8. Click **OK** when the device finishes the scan task.

   To access the risk analysis page from other pages, select **Go to the risk analysis page** on the scanning progress window, and then click **OK**.

9. To view risk analysis results, select one or more entries in the **Scanning records** area, and then click **Search**.

Blacklist

This help contains the following topics:

Introduction

The blacklist feature is an attack prevention method that filters packets by IP addresses or address object groups in blacklist entries. Compared with ACL-based packet filtering, IP blacklist filtering is simpler and provides effective screening at a faster speed.

Blacklist entries can be manually added or dynamically learned:

- You can manually add an IP blacklist entry. These entries do not age out by default. You can set an aging time for each entry.
- The device can automatically add IP blacklist entries when collaborating with scanning attack detection. Each dynamically learned IP blacklist entry has an aging time, which is user configurable. Make sure adding the attacker's IP address to the IP blacklist is specified as the scanning attack prevention action.

Configure the blacklist

The blacklist feature is an attack prevention method that filters packets by IP addresses or address object groups in blacklist entries.

IP blacklist entries when the blacklist feature collaborates with scanning attack detection. Make sure adding the attacker's IP address to the IP blacklist is specified as the scanning attack prevention action.

Configure the IP blacklist

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Blacklist**.
3. Click **Create**.
4. Add an IP blacklist entry.

Table 1 IP blacklist configuration items

Item	Description
VRF	VRF to which the blacklist belongs. You can select an existing VRF or create a new one. The newly created VRF will be displayed on the **Network** > **VRF** page.
IP address	IP address in the blacklist entry. Packets sourced from or destined to the IP address will be dropped.
Match field	Packet field to compare with the criterion: • Source IP address. • Destination IP address.
IP address	IP address in the blacklist entry. Packets sourced from or destined to the IP address will be dropped.
DS-Lite tunnel peer address	IPv6 address of the B4 element of the DS-Lite tunnel that transmits packets from the blacklisted IPv4 address. This parameter is available when **IPv4** is selected for **IP version**, and **Source IP** is selected for the match field.
Aging time (sec)	Aging time of the blacklist entry. If you do not set the aging time, the

Item	Description
	blacklist entry never ages out. You must delete it manually.

5. Click **OK**. The **IP Blacklist** page displays the newly added IP blacklist.
6. Click **Enable globally**. The IP blacklist takes effect on all security zones.

Configure the address object group blacklist

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack Defense** > **Blacklist**.
3. Click the **Address Object Group Blacklist** tab.
4. Click **Add**.
5. Add an address object group blacklist entry.

Table 2 Address object group blacklist configuration items

Item	Description
Object group type	Select a type of address object groups, IPv4 or IPv6.
Object group name	Enter the name of an address object group.

6. Click **OK**. The **Address Object Group Blacklist** page displays the newly added address object group blacklist.
7. Click **Enable globally**. The address object group blacklist takes effect on all security zones.

Connection limit

This help contains the following topics:

Introduction

The connection limit feature enables the device to collect statistics and limit the number of established connections. It helps protect internal network resources and better allocate system resources.

Connection limit policies

The device supports both IPv4 and IPv6 connection limit policies. You can apply a configured connection limit policy globally or to an interface to limit the number of user connections.

The connection limit policy applied to an interface takes effect only on the specified connections on the interface. The connection limit policy applied globally takes effect on all the specified connections on the device.

Different connection limit policies can be applied to individual interfaces as well as globally on the device. In this case, the device matches connections against these policies in the order of the policy on the inbound interface, the global policy, and the policy on the outbound interface. New connections are limited as long as the number of connections reaches the smallest upper connection limit defined by these policies.

Connection limit rules

To use a connection limit policy, you need to add limit rules to the policy. Each rule defines a range of connections and the criteria for limiting the connections. Connections in the range will be limited based on the criteria. The following criteria are available:

- **Connection limits**—Limit the number of matching connections. When the number of matching connections reaches the upper limit, the device accepts or rejects new connections depending on the action you configured. If the action is to reject new connections, the device does not accept new connections until the number of connections drops below the lower limit due to connection aging. The device will send logs when the number of connections exceeds the upper limit. The device will send logs when the number of connections drops below the lower limit only if the action is to reject new connections.
- **Connection establishment rate limit**—Limits the number of connections established per second. When the connection establishment rate reaches the upper limit, the device accepts or rejects new connections depending on the action you configured and records logs.

Connections that do not match any limit rules are not limited.

In each connection limit rule, an ACL is used to define the connection range. Only the user connections that match the ACL are limited. In addition, the rule also uses the following filtering methods to further limit the connections:

- **Source IP**—Limits user connections by source IP address.

- **Destination IP**—Limits user connections by destination IP address.
- **Service port**—Limits user connections by service (transport layer protocol and service port).

You can select more than one filtering method, and the selected methods take effect at the same time. For example, if you specify both **Destination IP** and **Service port**, the user connections using the same service and destined to the same IP address are limited. If you do not specify any filtering methods in a limit rule, all user connections in the range are limited.

When a connection limit policy is applied, the device compares connections with all limit rules in the policy in ascending order of rule IDs. As a best practice, specify a smaller range and more filtering methods in a rule with a smaller ID.

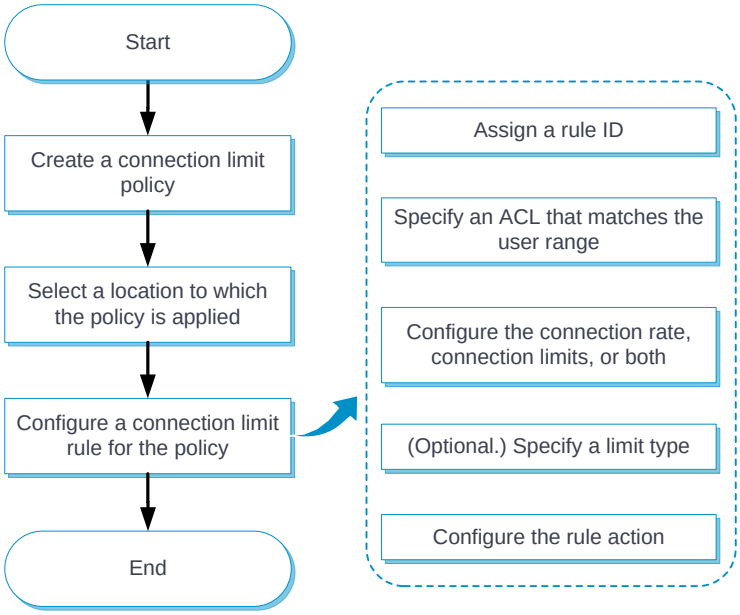
Restrictions and guidelines

- For devices supporting service modules, the connections are limited on a per-service module basis.
- A connection limit policy takes effect only on new connections. It does not take effect on existing connections.
- On an IRF fabric where session synchronization is enabled, connection limit policies applied to a subordinate device do not take effect on sessions switched from the master device.
- An ACL can only be used once in a connection limit policy and can be used in multiple connection limit policies.

Configure connection limit

Configure connection limit as shown in Figure 1.

Figure 1 Connection limit configuration procedure



The upper limit must be greater than the number of CPU cores on the device. As a best practice, set the upper limit to a value greater than 32.

uRPF

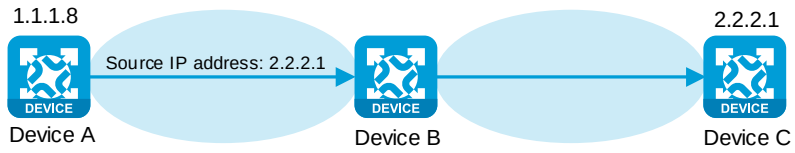
This help contains the following topics:

Introduction

Unicast Reverse Path Forwarding (uRPF) protects a network against source address spoofing attacks, such as DoS and DDoS attacks.

Attackers send packets with a forged source address to access a system that uses IP-based authentication, in the name of authorized users or even the administrator. Even if the attackers or other hosts cannot receive any response packets, the attacks are still disruptive to the attacked target.

Figure 1 Source address spoofing attack



As shown in Figure 1, an attacker on Device A sends the server (Device B) requests with a forged source IP address 2.2.2.1 at a high rate. Device B sends response packets to IP address 2.2.2.1 (Device C). Consequently, both Device B and Device C are attacked. If the administrator disconnects Device C by mistake, the network service is interrupted.

Attackers can also send packets with different forged source addresses or attack multiple servers simultaneously to block connections or even break down the network.

uRPF can prevent these source address spoofing attacks. It checks whether an interface that receives a packet is the output interface of the FIB entry that matches the source address of the packet. If not, uRPF considers it a spoofing attack and discards the packet.

uRPF check modes

uRPF supports strict and loose modes.

Strict uRPF check

To pass strict uRPF check, the source address of a packet and the receiving interface must match the destination address and output interface of a FIB entry. In some scenarios (for example, asymmetrical routing), strict uRPF might discard valid packets.

Strict uRPF is often deployed between a PE and a CE.

Loose uRPF check

To pass loose uRPF check, the source address of a packet must match the destination address of a FIB entry. Loose uRPF can avoid discarding valid packets, but might let go attack packets.

Loose uRPF is often deployed between ISPs, especially in asymmetrical routing.

uRPF extended functions

Using the default route in uRPF check

When a default route exists, all packets that fail to match a specific FIB entry match the default route during uRPF check and thus are permitted to pass. To avoid this situation, you can disable uRPF from using any default route to discard such packets. If you allow using the default route, uRPF permits packets that only match the default route.

By default, uRPF discards packets that can only match a default route. Typically, you do not need to use the default route for uRPF check on a PE device because it has no default route pointing to the CE. If you enable uRPF on a CE interface and the CE interface has a default route pointing to the PE, use the default route for uRPF check.

Link layer check (only supported by IPv4 uRPF)

Strict uRPF check can further perform link layer check on a packet. It uses the next hop address in the matching FIB entry to look up the ARP table for a matching entry. If the source MAC address of the packet matches the MAC address in the matching ARP entry, the packet passes strict uRPF check. Link layer check is applicable to ISP devices where a Layer 3 Ethernet interface connects a large number of PCs.

Loose uRPF does not support link layer check.

Using an ACL for uRPF check exemption

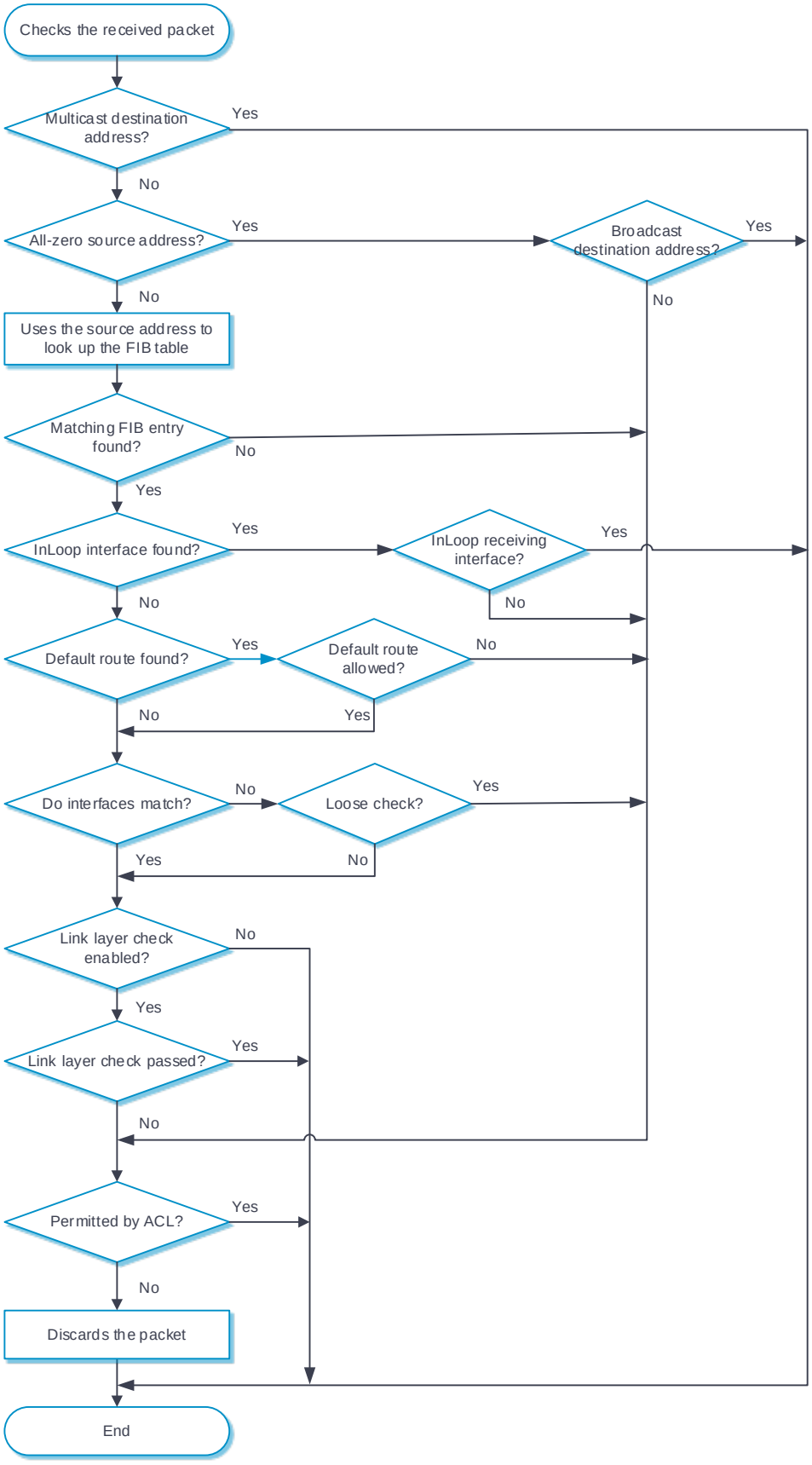
To identify specific packets as valid packets, you can use an ACL to match these packets. Even if the packets do not pass uRPF check, they are still forwarded.

uRPF operation

IPv4 uRPF operation

The following figure shows how IPv4 uRPF works.

Figure 2 IPv4 uRPF work flow


Checks the received packet
Multicast destination address?
Yes
No
All-zero source address?
Yes
Broadcast destination address?
Yes
No
No
Uses the source address to look up the FIB table
Matching FIB entry found?
No
Yes
InLoop interface found?
Yes
InLoop receiving interface?
Yes
No
No
Default route found?
Yes
Default route allowed?
No
No
Yes
Do interfaces match?
No
Loose check?
Yes
Yes
No
Link layer check enabled?
No
Yes
Link layer check passed?
Yes
No
Permitted by ACL?
Yes
No
Discards the packet
End

2. uRPF checks address validity:
    - uRPF permits a packet with a multicast destination address.
    - For a packet with an all-zero source address, uRPF permits the packet if it has a broadcast destination address. (A packet with source address 0.0.0.0 and destination address 255.255.255.255 might be a DHCP or BOOTP packet and cannot be discarded.) uRPF proceeds to step 7 if the packet has a non-broadcast destination address.
    - uRPF proceeds to step 2 for other packets.
3. uRPF checks whether the source address matches a unicast route:
    - If yes, uRPF proceeds to step 3.
    - If no, uRPF proceeds to step 7. A non-unicast source address matches a non-unicast route.
4. uRPF checks whether the matching route is to the host itself:
    - If yes, the output interface of the matching route is an InLoop interface. uRPF checks whether the receiving interface of the packet is an InLoop interface. If yes, it does not check the packet. If no, it proceeds to step 7.
    - If no, uRPF proceeds to step 4.
5. uRPF checks whether the matching route is a default route:
    - If yes, uRPF checks whether the default route is allowed. If yes, it proceeds to step 5. If no, it proceeds to step 7.
    - If no, uRPF proceeds to step 5.
6. uRPF checks whether the receiving interface matches the output interface of the matching FIB entry:
    - If yes, uRPF proceeds to step 6.

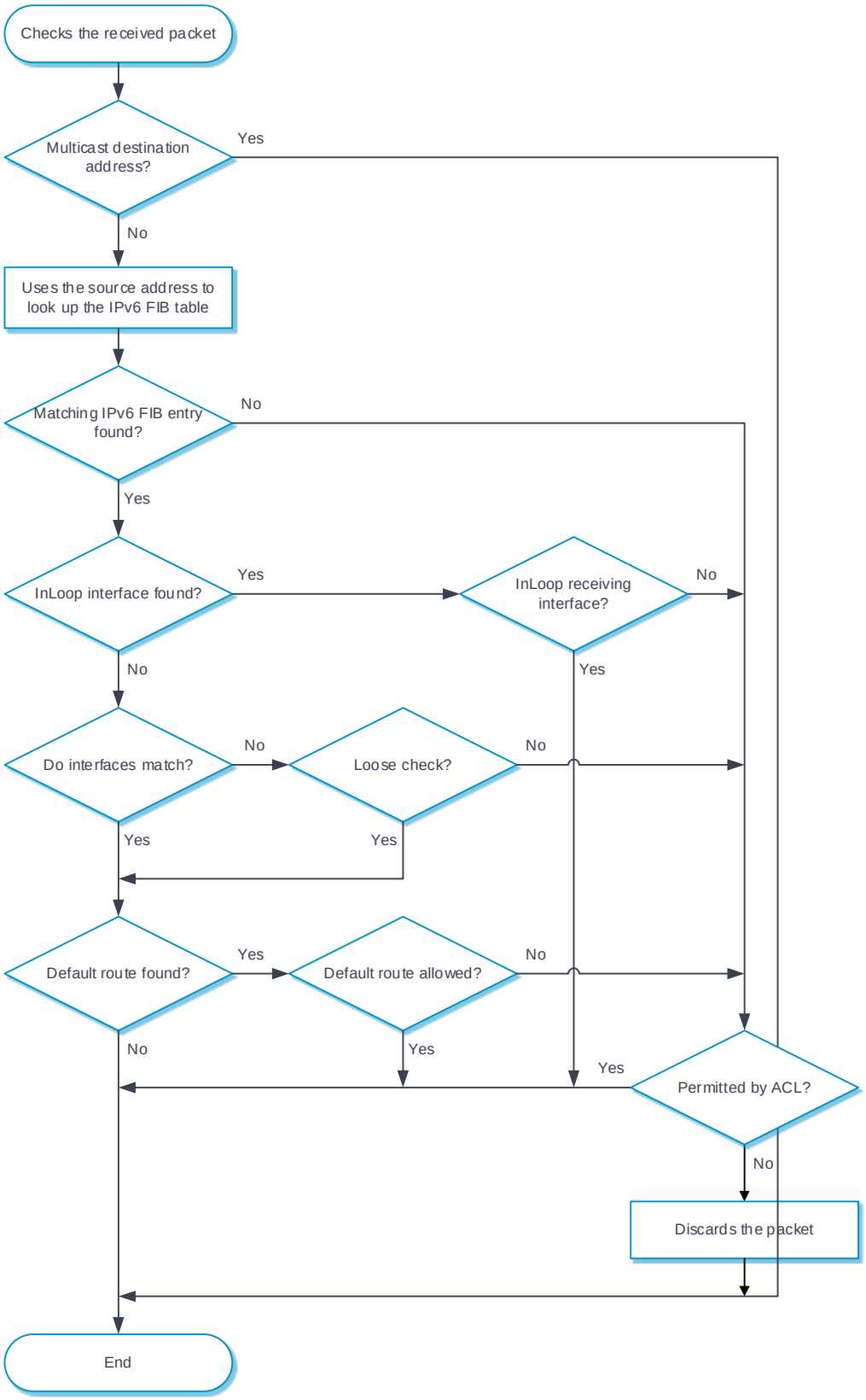
- If no, uRPF checks whether the check mode is loose. If yes, it proceeds to step 7. If no, it proceeds to step 6.

7. uRPF checks whether link layer check is configured:
   - If no, the packet passes the check.
   - If yes, uRPF uses the next-hop address of the FIB entry to look up the ARP table for a matching entry. Then it checks whether the MAC address of the matching ARP entry is identical with the source MAC address of the packet. If yes, the packet passes the check. If no, uRPF proceeds to step 7.
8. uRPF checks whether the packet is permitted by the ACL:
   - If yes, the packet is forwarded. Such a packet is suppressed from being dropped.
   - If no, the packet is discarded.

IPv6 uRPF operation

The following figure shows how IPv6 uRPF works.

Figure 3 IPv6 uRPF work flow

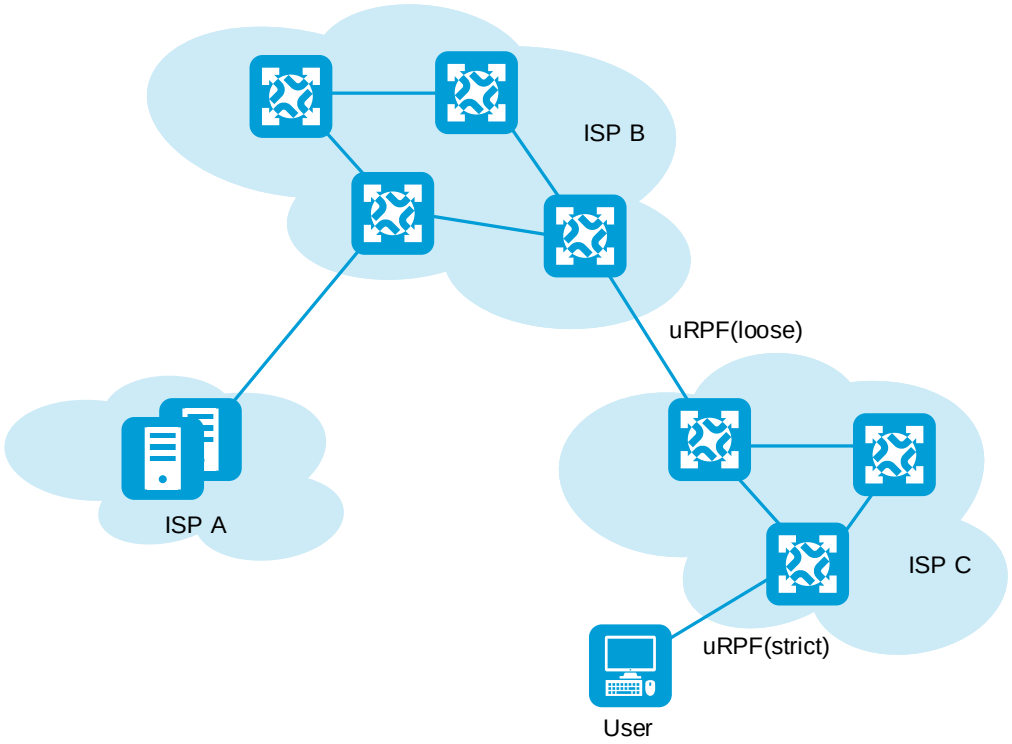


2. IPv6 uRPF checks whether the received packet carries a multicast destination address:
    - If yes, IPv6 uRPF permits the packet.
    - If no, IPv6 uRPF proceeds to step 2.
3. IPv6 uRPF checks whether the source address matches a unicast route:
    - If yes, IPv6 uRPF proceeds to step 3.
    - If no, IPv6 uRPF proceeds to step 6. A non-unicast source address matches a non-unicast route.
4. IPv6 uRPF checks whether the matching route is to the host itself:
    - If yes, the output interface of the matching route is an InLoop interface. IPv6 uRPF checks whether the receiving interface of the packet is an InLoop interface. If yes, IPv6 uRPF permits the packet. If no, IPv6 uRPF proceeds to step 6. If the source address is a link-local address and is the receiving interface address, also proceeds to step 6.
    - If no, IPv6 uRPF proceeds to step 4.
5. IPv6 uRPF checks whether the receiving interface matches the output interface of the matching FIB entry:
    - If yes, IPv6 uRPF proceeds to step 5.
    - If no, IPv6 uRPF checks whether the check mode is loose. If yes, it proceeds to step 5. If no, it proceeds to step 6.
6. IPv6 uRPF checks whether the matching route is a default route:
    - If yes, IPv6 uRPF checks whether the default route is allowed. If yes, the packet is forwarded. If no, IPv6 uRPF proceeds to step 6.
    - If no, the packet is forwarded.
7. IPv6 uRPF checks whether the packet is permitted by the IPv6 ACL:

- If yes, the packet is forwarded. Such a packet is suppressed from being dropped.
- If no, the packet is discarded.

uRPF network application

Figure 4 Network diagram



strict uRPF check is configured between an ISP network and a customer network. Loose IPv6 uRPF check is configured between ISPs.

For special packets or users, you can configure ACLs.

Restrictions and guidelines

Do not select **Allow using default route for uRPF check** for loose uRPF check. Otherwise, uRPF might fail to work.

Configure uRPF

Configure IPv4 uRPF

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack defense** > **uRPF** > **IPv4 uRPF**.
3. Click **Create**.
4. Configure IPv4 uRPF.

Table 1 IPv4 uRPF configuration items

Item	Description
Security zone	Select a security zone to which IPv4 uRPF is applied. The list contains the default security zone and security zones that have been configured on the **Network** > **Security Zones** page.
Check mode	• **Strict**—Strict uRPF check. To pass strict uRPF check, the source address and receiving interface of a packet must match the destination address and output interface of a FIB entry. • **Loose**—Loose uRPF check. To pass loose uRPF check, the source address of a packet must match the destination address

Item	Description
	of a FIB entry.
Check exemption	Select an ACL that suppresses packet dropping. You can select an existing IPv4 ACL or create a new one. The created ACL is displayed on the **Objects** > **ACLs** > **IPv4 ACLs** page.
Allow using default route for uRPF check	Select whether to allow using the default route for uRPF check.
Enable link layer check	Select whether to enable link layer check.

5. Click **OK**.

Configure IPv6 uRPF

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Attack defense** > **uRPF** > **IPv6 uRPF**.
3. Click **Create**.
4. Configure IPv6 uRPF.

Table 2 IPv6 uRPF configuration items

Item	Description
Security zone	Select a security zone to which IPv6 uRPF is applied. The list contains the default security zone and security zones that

Item	Description
	have been configured on the **Network** > **Security Zones** page.
Check mode	• **Strict**—Strict IPv6 uRPF check. To pass strict IPv6 uRPF check, the source address and receiving interface of a packet must match the destination address and output interface of an IPv6 FIB entry. • **Loose**—Loose IPv6 uRPF check. To pass loose IPv6 uRPF check, the source address of a packet must match the destination address of an IPv6 FIB entry.
Check exemption	Select an ACL that suppresses packet dropping. You can select an existing IPv6 ACL or create a new one. The created ACL is displayed on the **Objects** > **ACLs** > **IPv6 ACLs** page.
Allow using default route for uRPF check	Select whether to allow using the default route for uRPF check.

5. Click **OK**.

IPCAR

Introduction

This feature limits the number of connections established per second to prevent DDoS attacks from degrading device performance.

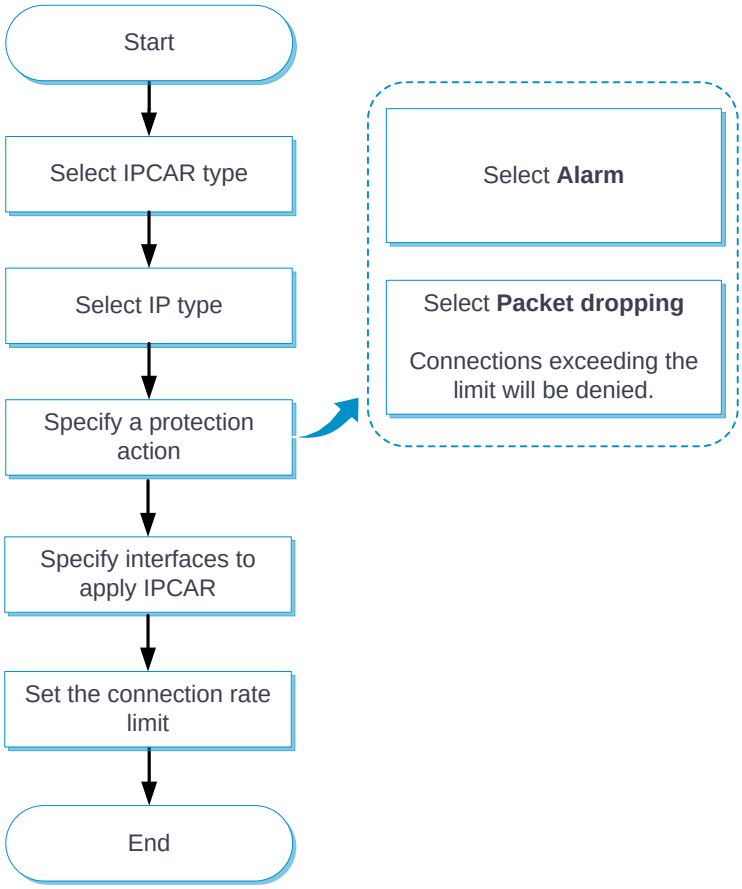
The device supports the following types of IPCAR protection:

- **Public network protection**—Limits the number of connections from the public network to the internal network based on destination IP address.
- **Internal network protection**—Limits the number of connections from the internal network to the public network based on source IP address.

Configure IPCAR

Configure IPCAR as shown in Figure 1.

Figure 1 IPCAR configuration procedure



NAT

This help contains the following topics:

Introduction

Network Address Translation (NAT) translates an IP address in the IP packet header to another IP address. Typically, NAT is configured on gateways to enable private hosts to access external networks and external hosts to access private network resources such as a Web server.

Dynamic NAT

Dynamic NAT uses an address pool to translate addresses. It applies to the scenario where a large number of internal users access the external network.

- NO-PAT

  Not Port Address Translation (NO-PAT) translates a private IP address to an IP public address. The public IP address cannot be used by another internal host until it is released.

  NO-PAT supports all IP packets.

- PAT

  Port Address Translation (PAT) translates multiple private IP addresses to a single public IP address by mapping the private IP address and source port to the public IP address and a unique port. PAT supports TCP and UDP packets, and ICMP request packets.

  A NAT address group is a set of address ranges. The source address in a packet destined for an external network is translated into an address in one of the address ranges.

NAT Server

The NAT Server feature maps a public address and port number to the private IP address and port number of an internal server. This feature allows servers in the private network to provide services for external users. The following table describes the address-port mappings between an external network and an internal network for NAT Server.

Table 1 Address-port mappings for NAT Server

External network	Internal network
One public address	One private address
One public address and one public port number	One private address and one private port number
One public address and *N* consecutive public	• One private address and one private port

External network	Internal network
port numbers	number • *N* consecutive private addresses and one private port number • One private address and *N* consecutive private port numbers
N consecutive public addresses	• One private address • *N* consecutive private addresses
N consecutive public addresses and one public port number	• One private address and one private port number • *N* consecutive private addresses and one private port number • One private address and *N* consecutive private port numbers
One public address and one public port number	One internal server group
One public address and *N* consecutive public port numbers	
N consecutive public addresses and one public port number	
Public addresses matching an ACL	One private address
	One private address and one private port
Public addresses in an address object group	One private address
	One private address and one private port

You can add multiple internal servers to an internal server group for load sharing so that these servers provide the same service for external hosts. The NAT device chooses one internal server based on the weight and number of connections of the servers to respond to a request from an external host to the public address of the internal server group.

Static NAT

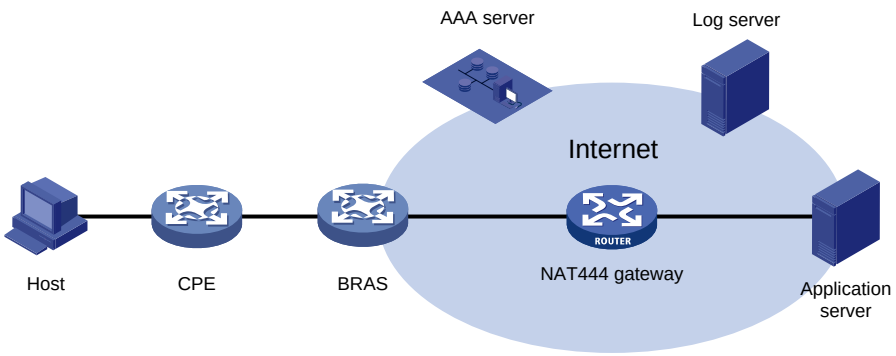
Static NAT creates a fixed mapping between a private address and a public address. It supports connections initiated from internal users to external network and from external users to the internal network. Static NAT applies to regular communications.

NAT444

NAT444 provides carrier-grade NAT by unifying the NAT444 gateway, AAA server, and log server. NAT444 introduces a second layer of NAT on the carrier side, with few changes on the customer side and the application server side. With port block assignment, NAT444 supports user tracking. It has become a preferred solution for carriers in transition to IPv6.

Figure 1 shows architecture of the NAT444 solution.

Figure 1 NAT444 solution architecture



Devices in this architecture provide services as follows:

- CPE—Performs customer-side address translation.
- BRAS—Provides endpoint access services and incorporates with the AAA server for authentication, authorization, and accounting.
- NAT444 gateway—Performs carrier-grade address translation.
- AAA server—Provides authentication, authorization, and accounting services.
- Log server—Records user access information and responds to user information queries.

NAT444 is a PAT translation based on port ranges. It maps multiple private IP addresses to one public IP address and uses a different port block for each private IP address. For example, the private IP address 10.1.1.1 of an internal host is mapped to the public IP address 202.1.1.1 and port block 10001 to 10256. When the internal host accesses public hosts, the source IP address 10.1.1.1 is translated to 202.1.1.1, and the source ports are translated to ports in the port block 10001 to 10256.

Static NAT444

The NAT gateway computes a static port block mapping before address translation. The mapping is between a private IP address and a public IP address with a port block.

When an internal user initiates a connection to the external network, the system performs the following operations:

- Locates a static mapping based on the private IP address of the user and obtains the public IP address and the port block in the mapping.
- Selects a public port number in the port block.
- Translates the private IP address to the public IP address and assigns the selected public port number.

The NAT gateway uses private IP addresses, public IP addresses, a port range, and a port block size to compute static mappings:

1. Divides the port range by the port block size to get the number of available port blocks for each public IP address.

   This value is the base number for mapping.
2. Sorts the port blocks in ascending order of the start port number in each block.
3. Sorts the private IP addresses and the public IP addresses separately in ascending order.
4. Maps the first base number of private IP addresses to the first public IP address and its port blocks in ascending order.

For example, the number of available port blocks of each public IP address is **m**. The first **m** private IP addresses are mapped to the first public IP address and the **m** port blocks in ascending order. The next **m** private IP addresses are mapped to the second IP address and the **m** port blocks in ascending order. The other static port block mappings are created by analogy.

Dynamic NAT444

Dynamic NAT444 integrates functionalities of dynamic NAT and static NAT444. When an internal user initiates a connection to the external network, the dynamic NAT444 operates as follows:

1. Uses ACLs to implement translation control. It processes only packets that match an ACL permit rule.
2. Creates a mapping from the internal user's private IP address to a public IP address and a port block.
3. Translates the private IP address to the public IP address, and the source ports to ports in the selected port block for subsequent connections from the private IP address.
4. Withdraws the port block and deletes the dynamic port block mapping when all connections from the private IP address are disconnected.

Dynamic port block mapping supports port block extending. If the ports in the port block for a private address are all occupied, dynamic port block mapping translates the source port to a port in an extended port block.

NAT advanced settings

PAT mapping modes

The following PAT mapping modes are supported:

- **Endpoint-Independent Mapping (EIM)**—Uses the same IP and port mapping (EIM entry) for packets from the same source IP and port to any destinations. EIM allows external hosts to initiate connections to the translated IP addresses and ports of internal hosts. It allows internal hosts behind different NAT gateways to access each other.
- **Address and Port-Dependent Mapping (APDM)**—Uses different IP and port mappings for packets from the same source IP and port to different destination IP addresses and ports. APDM allows an external host to initiate connections to an internal host only under the condition that the internal host has previously accessed the external host. It is secure, but it does not allow internal hosts behind different NAT gateways to access each other.

NAT DNS mappings

With NAT DNS mappings, a user in the internal network can access internal servers by using their domain names when the DNS server is located on the public network. The NAT DNS mapping works in conjunction with NAT server mappings. A NAT DNS mapping maps the domain name of an internal server to the public IP address, public port number, and protocol type of the internal server. A NAT server mapping maps the public IP and port to the private IP and port of the internal server.

The DNS reply from the external DNS server contains only the domain name and public IP address of the internal server in the payload. The NAT interface might have multiple NAT server mappings with the same public IP address but different private IP addresses. DNS ALG might find an incorrect internal server by using only the public IP address. If a NAT DNS mapping is configured, DNS ALG can obtain the public IP address, public port number, and protocol type of the internal server by using the domain name. Then it can find the correct internal server by using the public IP address, public port number, and protocol type of the internal server.

NAT hairpin

NAT hairpin allows internal hosts to access each other through NAT. The source and destination IP address of the packets are translated on the interface connected to the internal network. NAT hairpin works in conjunction with NAT Server, outbound dynamic NAT, or outbound static NAT. To provide service correctly, you must configure NAT hairpin on the same interface module as its collaborative NAT feature.

NAT hairpin includes C/S and P2P modes:

- **C/S**—Allows internal hosts to access internal servers through NAT addresses. The destination IP address of the packet going to the internal server is translated by matching the NAT Server configuration. The source IP address is translated by matching the outbound dynamic or static NAT entries.
- **P2P**—Allows internal hosts to access each other through NAT. The internal hosts first register their public addresses to an external server. Then, the hosts communicate with each other by using the registered IP addresses. To configure the P2P mode, you must configure outbound PAT on the interface connected to the external network and enable the EIM mapping mode.

NAT global settings

On a WAN network where two output interfaces of the NAT device are in the same security zone, if the link of one interface fails, traffic is switched to the link of the other interface. The NAT device retains old session entries after link switchover. Internal users cannot access the external network because the NAT device uses old session entries to match the user traffic. To avoid this issue, enable NAT session recreation to ensure availability of NAT services. The device will recreate NAT sessions when user traffic arrives.

Restrictions and guidelines

General restrictions and guidelines

- A NAT address group cannot be used by both PAT and NO-PAT modes.
- As a best practice, configure inbound static NAT with outbound dynamic NAT, NAT Server, or outbound static NAT to implement bidirectional NAT.
- If you perform all the translation methods on an interface, the NAT rules are sorted in the following descending order:
  a. NAT Server.
  b. Static NAT.
  c. NAT444 static port block mapping.
  d. Dynamic NAT.
- When you add address ranges to a NAT address group, make sure address ranges do not overlap.

Restrictions and guidelines: Dynamic NAT

You can configure multiple outbound dynamic NAT rules on an interface.

- A NAT rule with an ACL takes precedence over a rule without any ACL.

- If two ACL-based dynamic NAT rules are configured, the rule with the higher ACL number has higher priority.

Restrictions and guidelines: Static NAT

- When you specify object groups for a static mapping, follow these restrictions and guidelines:
    - The public or private IPv4 address object group can contain only one IPv4 address object.
    - The quantity of IPv4 addresses in the private IPv4 address object group cannot be larger than that in the public IPv4 address object group.
    - The object in the public IPv4 address object group cannot be an address range.
    - An address object cannot have excluded addresses. Otherwise, the mapping does not take effect.
    - Changes on an address object takes effect directly on the mapping that uses the object. Please edit address objects with caution.
- You must specify a VRF if you deploy outbound static NAT in VPN networks. The specified VRF must be the VRF to which the NAT interface belongs.
- When you specify an ACL, follow these restrictions and guidelines:
    - If you do not specify an ACL, the source addresses of all outgoing packets and the destination addresses of all incoming packets are translated.
    - If you specify an ACL and do not specify the reverse address translation, the source addresses of outgoing packets permitted by the ACL are translated. The destination addresses of packets are not translated for connections actively initiated by external hosts to the internal hosts.
    - If you specify both an ACL and the reverse address translation, the source addresses of outgoing packets permitted by the ACL are translated. If packets of connections actively initiated by external hosts to the internal hosts are permitted by ACL reverse matching, the destination addresses are translated. ACL reverse matching works as follows:
        - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.

- Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Restrictions and guidelines: NAT Server

- When you configure a load shared NAT server mapping, you must make sure a user uses the same public address and public port to access the same service on an internal server. For this purpose, make sure value *N* in the following mappings is equal to or less than the number of servers in the internal server group:
  - One public address and *N* consecutive public port numbers are mapped to one internal server group.
  - *N* consecutive public addresses and one public port number are mapped to one internal server group.
- An internal server with a larger weight receives a larger percentage of connections in the internal server group.
- You must specify a VRF if you configure NAT server mappings in VPN networks. The specified VRF must be the VRF to which the NAT interface belongs.
- When you configure object group-based NAT server mappings, object groups for matching public addresses can only be IPv4 address object groups configured with subnets, IP address ranges, or host addresses. The IPv4 address object groups cannot have excluded IPv4 addresses.

Configure NAT

NAT can be performed in the inbound or outbound direction.

- **Inbound NAT**—Performs address translation for packets received on an interface, as shown in Figure 2.
- **Outbound NAT**—Performs address translation for packets sent out of an interface, as shown in Figure 3.

Figure 2 Inbound NAT

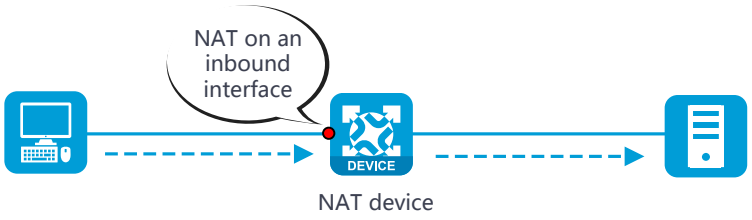
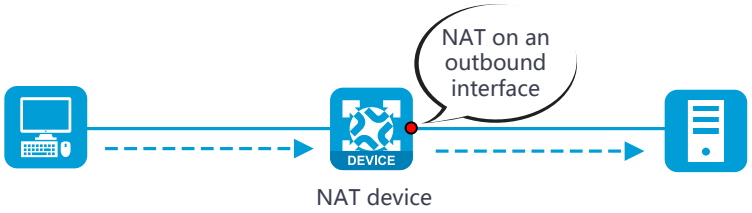


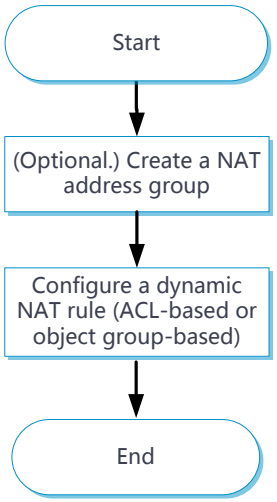
Figure 3 Outbound NAT



Configure dynamic NAT

Only outbound dynamic NAT is supported in the current software version. You can configure ACL-based outbound dynamic NAT or object group-based outbound dynamic NAT. Figure 4 shows the configuration procedure for dynamic NAT.

Figure 4 Dynamic NAT configuration procedure



Procedure

1. (Optional.) Create a NAT address group.
   a. Click the **Objects** tab.
   b. In the navigation pane, select **Object Groups** > **NAT Address Groups**.
   c. Click **Create**.
   d. Create a NAT address group as shown in Table 2.

Table 2 Configuration items for a NAT address group

Item	Description
Address group ID	Enter the ID of a NAT address group.
Address group name	Enter the name of the NAT address group.
VRRP group	Specify a VRRP group for high availability purposes. The master device in the VRRP group uses the virtual IP address and virtual MAC address to answer ARP requests. Support for the VRRP group feature depends on the device model.

Item	Description
Port range	Specify a port range for address translation.
Address probe	Select NQA templates to probe the availability of addresses in the NAT address group for outbound address translation.
Address group members	Add IP address ranges to the NAT address group. The NAT address group uses these IP address ranges to translate source IP addresses of the packets sent to the external network.

e. Click **OK**.

2. Configure ACL-based dynamic NAT.

a. Click the **Policies** tab.

b. In the navigation pane, select **Interface NAT** > **IPv4** > **Dynamic NAT**.

c. Click the **Outbound Dynamic NAT (ACL-Based)** tab.

d. Click **Create**.

e. Create an ACL-based outbound dynamic NAT rule, as shown in Table 3.

Table 3 Configuration items for ACL-based outbound dynamic NAT

Item	Description
Interface	Interface to which the NAT rule is applied. Outbound dynamic NAT is typically configured on the interface connected to the external network.
ACL	ACL for packet matching. If you specify an ACL, NAT translates the source IP addresses of outgoing packets permitted by the ACL. If you do not specify an ACL, NAT translates all packets.
Source address after NAT	Select the NAT address for address translation: • **NAT address group**—IP addresses in the NAT address group are used for address translation. • **Easy IP**—The IP address of the specified interface is used for address translation.

Item	Description
	An address group cannot be used by both PAT and NO-PAT modes.
VRF	VRF to which the source addresses belong after translation. The default setting is Public network. You must specify this parameter if you deploy outbound dynamic NAT for VPNs. The specified VRF must be the VRF to which the specified interface belongs.
Translation mode	Dynamic NAT translation mode: • **PAT**—Uses the IP addresses in the address group or the IP address of the interface to translate IP addresses of the matching packets. Source ports in the matching packets are also translated. • **NO-PAT**—Uses the IP addresses in the address group to translate IP addresses of the matching packets. Source ports in the matching packets are not translated.
Port preservation	Try to preserve port number for PAT. This option is available only when the translation mode is set to PAT.
Allow reverse NAT	Enable reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the external network to the internal network. This option is available only when the translation mode is set to NO-PAT.
Enable this rule	Enable this NAT rule.

f. Click **OK**.

3. Configure object group-based dynamic NAT.

a. Click the **Policies** tab.

b. In the navigation pane, select **Interface NAT** > **IPv4** > **Dynamic NAT**.

c. Click the **Outbound Dynamic NAT (Object Group-Based)** tab.

d. Click **Create**.

e. Create an object group-based outbound dynamic NAT rule, as shown in Table 4.

Table 4 Configuration items for object group-based outbound dynamic NAT

Item	Description
Rule name	Enter the name of a NAT rule.
Rule description	Enter the description of the NAT rule.
Output interface	Interface to which the NAT rule is applied. Outbound dynamic NAT is typically configured on the interface connected to the external network.
Source IP	Source IP address object group for the NAT rule. You can configure multiple source IP address object groups for a NAT rule. Each source IP object group is an independent packet match criterion.
Destination IP	Destination IP address object group for the NAT rule. You can configure multiple destination IP address object groups for a NAT rule. Each destination IP object group is an independent packet match criterion.
Service	Service object group for the NAT rule. You can configure multiple service object groups for a NAT rule. Each service object group is an independent packet match criterion. If you configure service object groups, source IP object groups, and destination object groups for a NAT rule, only packets with matching service type, source IP address, and destination IP address are translated.
Action	Dynamic NAT translation mode: • **PAT**—Uses the IP addresses in the address group or the IP address of the interface to translate IP addresses of the matching packets. Source ports in the matching packets are also translated. • **NO-PAT**—Uses the IP addresses in the address group to translate IP addresses of the matching packets. Source ports in the matching packets are not translated. • **Easy IP**—Uses the IP address of the specified interface for address translation. • **No translation**—Does not translate matching packets.

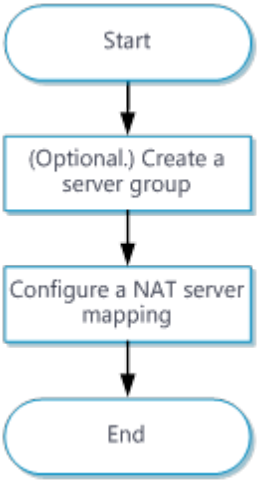
Item	Description
Source address after NAT	NAT address group for source address translation. An address group cannot be used by both PAT and NO-PAT modes.
Port reservation	Try to preserve port number for PAT. This option is available only when the translation mode is set to PAT.
Allow reverse NAT	Enable reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the external network to the internal network. This option is available only when the translation mode is set to NO-PAT.
Enable this rule	Enable this NAT rule.

f. Click **OK**.

Configure NAT Server

Configure the NAT Server feature as shown in Figure 5.

Figure 5 NAT Server configuration procedure



Procedure

1. (Optional.) Create a server group.
   a. Click the **Policies** tab.
   b. In the navigation pane, select **Interface NAT** > **IPv4** > **NAT Servers** > **NAT Server Groups**.
   c. Click **Create**.
   d. Create a server group.
   e. Click **OK**.
2. Configure a NAT server rule.
   a. Click the **Policies** tab.
   b. In the navigation pane, select **Interface NAT** > **IPv4** > **NAT Servers** > **Policy Configuration**.
   c. Click **Create**.
   d. Create a NAT server rule, as shown in Table 5.

Table 5 NAT server configuration items

Item	Description
Rule name	Enter the name of a NAT server rule.
Interface	Interface to which the NAT server rule is applied. The NAT server rule is typically configured on the interface connected to the external network.
Protocol type	Specify a protocol type. If you do not specify a protocol type, the configuration applies to packets of all protocols.
Mapping	Select an address-port mapping. For more information, see Table 1.
Mapping description	Mapping description for identification when a large number of NAT mappings exist.
Public IP	Public IP address that the server advertises to the external network.
Public port	Public port number or port range, depending on the mapping method. When you specify a port range, make sure the end port is greater than the start port.
Public port VRF	VRF to which the advertised public IP addresses belong. The default setting is Public network.
Server IP	Private IP address or address range, depending on the mapping method. In the address range, the end address must be greater than the start address. The number of addresses in the range must equal the number of ports in the public port range.
Server port	Private port number or port range, depending on the mapping method. When you specify a port range, make sure the end port is higher than the start port.
Server VRF	VRF to which the NAT server belongs. The default setting is Public network.
ACL for packet matching	If you specify an ACL, NAT translates packets permitted by the ACL. If you do not specify an ACL, NAT translates all packets.
VRRP group	Specify a VRRP group for high availability purposes.

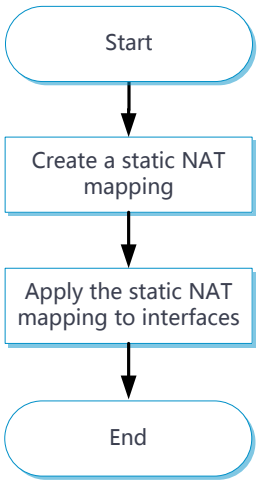
Item	Description
	The master device in the VRRP group uses the virtual IP address and virtual MAC address to answer ARP requests. Support for the VRRP group feature depends on the device model.
Allow reverse NAT	Allow reverse address translation. Reverse address translation applies to connections actively initiated by internal servers to the external network. It translates the private IP addresses of the internal servers to their public IP addresses. This option is available only when the mapping type is set to One single public address with one single or no public port.
Enable this rule	Enable this NAT server rule.

e. Click **OK**.

Configure static NAT

Only outbound static NAT is supported in the current software version. Configure static NAT as shown in Figure 6.

Figure 6 Static NAT configuration procedure



Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Interface NAT** > **IPv4** > **Static NAT** > **Policy Configuration**.
3. Click **Create**.
4. Create a static NAT mapping.

Table 6 Static NAT configuration items

Item	Description
Translation method	Select an address translation method: • **One-to-one**—Performs address translation from a private IP address to a public IP address. • **Net-to-net**—Performs address translation from a private network to a public network • **Address object group**—Performs address object group-based address translation.
Private address	Private IP address. The parameter setting depends on the translation method. If address object group-based translation method is selected, you must specify an IPv4 address object group.
Public VRF	VRF to which the public IP address belongs. The default setting is Public network.
Private VRF	VRF to which the private IP address belongs. The default setting is Public network.
Public address	Public IP address. The parameter setting depends on the translation method. If address object group-based translation method is selected, you must specify an IPv4 address object group.
ACL	Specify an ACL to define the destination IP addresses that internal hosts can access.
VRRP group	Specify a VRRP group for high availability purposes. The master device in the VRRP group uses the virtual IP address and virtual MAC address to answer ARP requests.

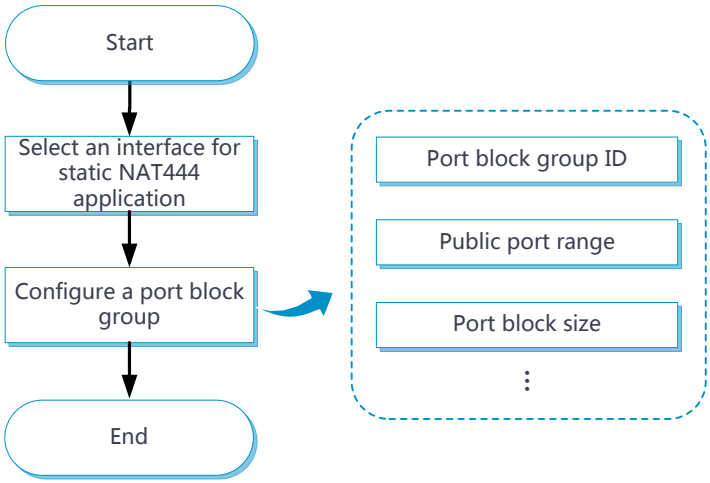
Item	Description
	Support for the VRRP group feature depends on the device model.
Allow reverse NAT	Allow reverse address translation. Reverse address translation applies to connections actively initiated by external hosts to the internal host. It uses the mapping to translate the destination address for packets of these connections if the packets are permitted by ACL reverse matching.
Enable this rule	Enable this static NAT rule.

5. Click **OK**.
6. Click the **Policies** tab.
7. In the navigation pane, select **Interface NAT** > **IPv4** > **Static NAT** > **Apply Policy**.
8. Select one or multiple interfaces.
9. Click **Enable**.

Configure static NAT444

Configure static NAT444 as shown in Figure 7.

Figure 7 Static NAT444 configuration procedure



Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Interface NAT** > **IPv4** > **Static NAT444**.
3. Click **Create**.
4. Select an interface.
5. Select or create a port block group.
6. Click **OK**.

Configure advanced NAT settings

Configure NAT DNS mappings

1. Click the **Policies** tab.
2. In the navigation pane, select **Interface NAT** > **IPv4**.
3. Click the **NAT DNS Mappings** tab.
4. Click **Create** to add a new mapping entry for a domain name to the internal server.

Table 7 NAT DNS mapping configuration items

Item	Description
Domain name	Specify a domain name for the internal server.
Internal server running protocol	Select a running protocol for the internal server: • **TCP**. • **UDP**.
Public IP	Specify a public IP address for the internal server.
Public port number	Specify a public port number for the internal server.

5. Click **OK**.

Configure NAT Hairpin

1. Click the **Policies** tab.
2. In the navigation pane, select **Interface NAT** > **IPv4**.
3. Click the **NAT Hairpin** tab.
4. Select an interface.
5. Click **Enable** to enable NAT Hairpin on the selected interface.

Configure general settings

1. Click the **Policies** tab.
2. In the navigation pane, select **Interface NAT** > **IPv4**.
3. Click the **General Settings** tab.
4. Select **Nat session reconstruction under double exists**.
5. Click **Apply** to enable NAT session reconstruction under double exists.

Configure PAT mode

1. Click the **Policies** tab.
2. In the navigation pane, select **Interface NAT** > **IPv4**.
3. Click the **General Settings** tab.
4. Select a PAT mapping mode. Options include **APDM** and **EIM**.
5. Click **Apply**.

Policy-based NAT

This help contains the following topics:

Introduction

Policy-based NAT contains a set of NAT rules to identify and translate matching packets. The packet match criteria include source security zone, destination security zone, source IP address, destination IP address, and service.

Policy-based NAT supports the following types of rules, which are applicable to different scenarios:

- **NAT44 rule**—Used for NAT translation between IPv4 networks.
- **NAT64 rule**—Used for NAT translation between IPv4 networks and IPv6 networks.
- **NAT66 rule**—Used for NAT translation between IPv6 networks.

Policy-based NAT supports the following translation modes:

- **Source address translation**—Translates the source IP address and source port of the packets. The NO-PAT and PAT modes are supported. For more information about NO-PAT and PAT, see "NAT."
- **Destination address translation**—Translates the destination IP address and destination port of the packets. Policy-based NAT supports translating different destination IP addresses and destination ports of the matching packets to the same IP address and port.

- **Bidirectional translation**—Translates the source IP address, source port, destination IP address, and destination port of the packets. The source address translation supports NO-PAT and PAT modes. The destination address translation supports translating different destination IP addresses and destination ports of the matching packets to the same IP address and port.

Restrictions and guidelines

- By default, the NAT rules in policy-based NAT are sorted in descending order of their configuration order. You can rearrange NAT rules to change their priorities. A rule has a higher priority than rules listed after it.
- A NAT address group cannot be used by both PAT and NO-PAT modes.
- If a packet matches both a policy-based NAT rule and an interface NAT rule, the packet is translated as follows:
  - For source and destination address translation method:
    - If the translation methods of the policy-based NAT rule and the interface NAT rule are the same, the device translates the packet by using the policy-based NAT rule.
    - If the translation methods of the policy-based NAT rule and the interface NAT rule are different, the device translates the packet by using the two rules.
  - If the translation method of the policy-based NAT rule is bidirectional, the device translates the packet by using the policy-based NAT rule, and the interface NAT rule does not take effect.
- When you add address ranges to a NAT address group, make sure address ranges do not overlap.
- The address object group used by a NAT rule cannot contain a host name or address object group.
- When you create or copy a policy-based NAT rule:
  - If you check the **Automatically generate security policy** check box, the device automatically generates a security policy based on the original packet configuration.

- If you make changes to the original packet configuration after checking the box, click **Refresh** to generates a security policy based the new configuration.

Configure policy-based NAT

NAT can be performed in the inbound or outbound direction.

- **Inbound NAT**—Performs address translation for packets received in a security zone, as shown in Figure 1.
- **Outbound NAT**—Performs address translation for packets sent out of a security zone, as shown in Figure 2.

Figure 1 NAT on an inbound security zone

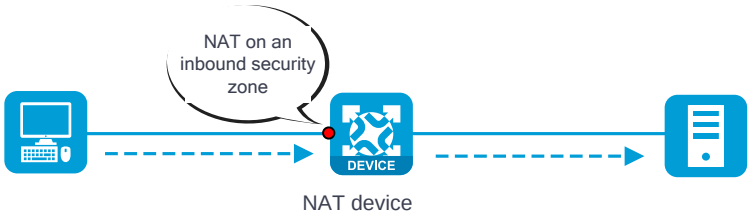
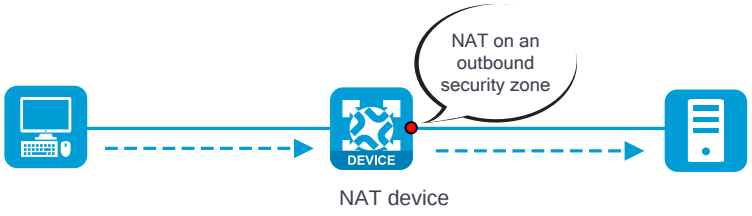


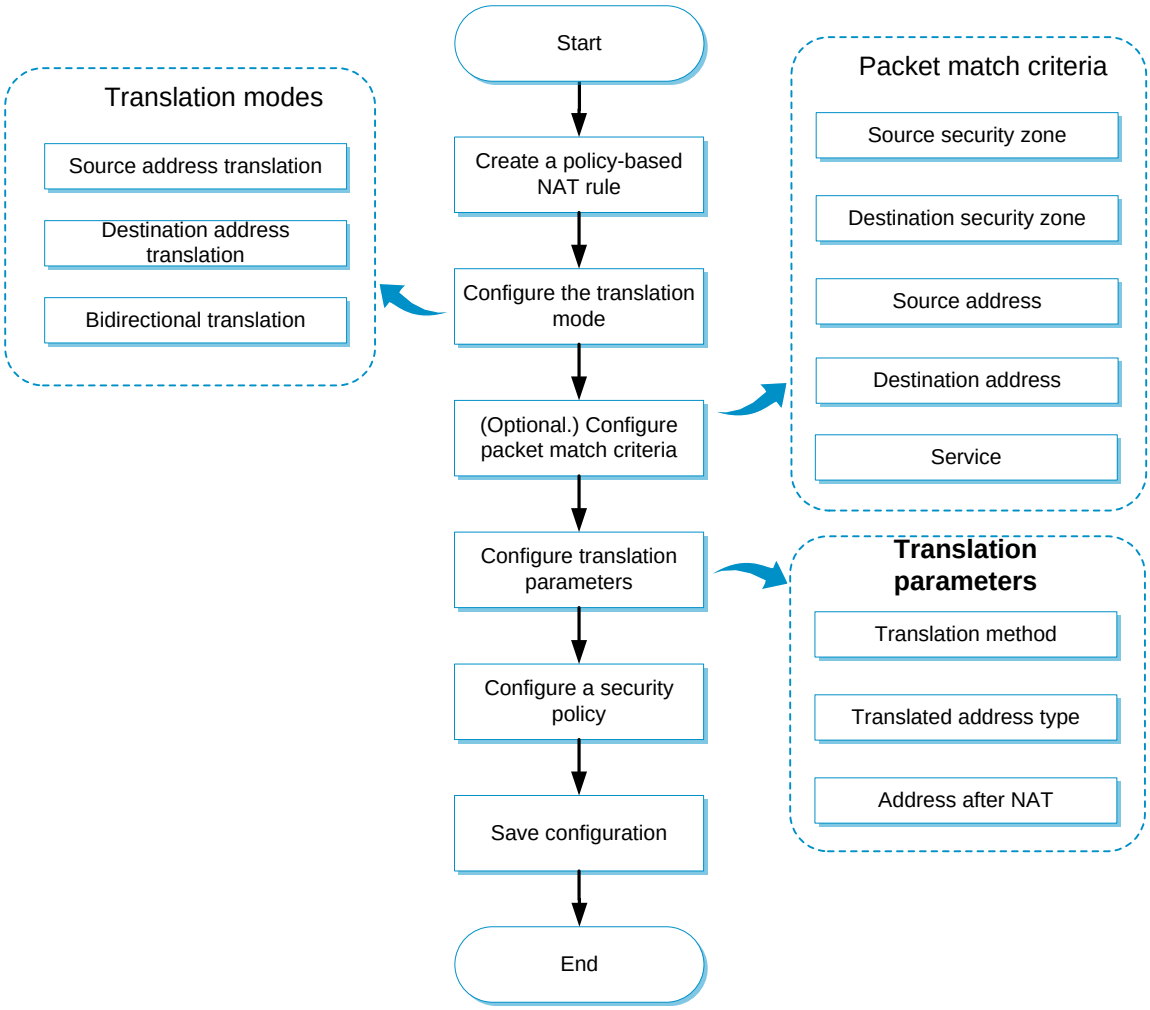
Figure 2 NAT on an outbound security zone



Configuration flowchart

Policy-based NAT supports packet match criteria including security zone, address object group, and service object group. Policy-based NAT supports source address translation, destination address translation, and bidirectional translation. Figure 3 shows the configuration flowchart.

Figure 3 Policy-based NAT configuration flowchart



Configure a policy-based NAT44 rule

Procedure

1. (Optional.) Create a security zone. (Details not shown.)
2. (Optional.) Create an address object group. (Details not shown.)
3. (Optional.) Create a service object group. (Details not shown.)
4. (Optional.) Create a NAT address group.
   a. Click the **Objects** tab.
   b. In the navigation pane, select **Object Groups** > **NAT Address Groups**.
   c. Click **Create**.
   d. Create a NAT address group.
   e. Click **OK**.
5. Create a policy-based NAT44 rule.
   a. Click the **Policies** tab.
   b. In the navigation pane, select **Policy-Based NAT**.
   c. Click **Create**.
   d. Create a policy-based NAT rule, and select the rule type as NAT44.
   e. Click **OK**.

Table 1 Configuration items for policy-based NAT44 rules

Item		Description
Rule name		Enter the name of a policy-based NAT44 rule. Chinese characters are supported.
Rule description		Enter the description of the policy-based NAT44 rule.
Original packets	Src zone	Select source security zones for packet match.

Item			Description
		Dst zone	Select destination security zones for packet match.
		Source IP	Select a source IP address, IP subnet, or address object group for packet match.
		Destination IP	Select a destination IP address, IP subnet, or address object group for packet match.
		Service	Select a service object group for packet match.
Source address translation	Translation method		Select a source address translation method: • **Dynamic IP+port**—Uses the PAT method to translate both the source IP addresses and source ports of packets. • **Dynamic IP**—Uses the NO-PAT method to translate only the source IP addresses of packets. • **Static IP**—Translates the source IP addresses of packets to a fixed IP address. • **No translation**—This rule and rules with lower priority than this rule are not used for source address translation.
	Address		Select a NAT address type for source address translation: • **Address object group**—Uses IP addresses in an address object group for source address translation. • **NAT address group**—Uses IP addresses in a NAT address group for source address translation. • **IP address**—Uses a fixed IP address for source address translation. • **Network address**—Uses IP addresses on a network for source address translation. • **Easy IP**—Uses the outgoing interface IP address of the device for source address translation.
	Source IP after NAT		Select a NAT address for source address translation.

Item		Description
	Allow reverse NAT	Enable reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the external network to the internal network. This option is available only when the translation mode is set to **Dynamic IP**.
	User original port preferentially	Preferentially use the original port for PAT. When the original port has been allocated, another port is used. This option is available only when the translation mode is set to **Dynamic IP+port**.
Destination address translation	Translation method	Select a destination address translation method: • **Static IP**—Translates the destination IP addresses of packets to a fixed IP address. • **Address object group**—Translates the destination IP addresses of packets to addresses in an address object group. • **No translation**—This rule and rules with lower priority than this rule are not used for source address translation.
	Destination IP after NAT	Set the destination IP address after translation.
	Port after NAT	Set the destination port after translation.
VRF before NAT	Specify a VRF used to match the VRF to which the packet belongs.	
VRF after NAT	Specify a VRF used to replace the VRF to which the matching packets belong.	
Enable this rule	Enable this policy-based NAT44 rule.	
Counting	Enable the counting of times that the policy-based NAT44 rule is matched.	

Configure a policy-based NAT64 rule

Procedure

1. (Optional.) Create a security zone. (Details not shown.)
2. (Optional.) Create an address object group. (Details not shown.)
3. (Optional.) Create a service object group. (Details not shown.)
4. Create a policy-based NAT64 rule.
   a. Click the **Policies** tab.
   b. In the navigation pane, select **Policy-Based NAT**.
   c. Click **Create**.
   d. Create a policy-based NAT rule, and select the rule type as NAT64.
   e. Click **OK**.

Table 2 Configuration items for policy-based NAT64 rules

Item		Description
Rule name		Enter the name of a policy-based NAT64 rule. Chinese characters are supported.
Rule description		Enter the description of the policy-based NAT64 rule.
Original packets	Src zone	Select source security zones for packet match.
	Source IP	Select a source IP address, IP subnet, or address object group for packet match.
	Destination IP	Select a destination IP address, IP subnet, or address object group for packet match.
	Service	Select a service object group for packet match.

Item		Description
Source address translation	Translation method	Select a source address translation method: • **Dynamic IP+port**—Uses the PAT method to translate both the source IP addresses and source ports of packets. • **Dynamic IP**—Uses the NO-PAT method to translate only the source IP addresses of packets. • **Static IP**—Translates the source IP addresses of packets to a fixed IP address. • **Prefix translation**—Uses IPv6 prefixes to translate the source IP addresses of packets.
	Source IP after NAT	Select a NAT address for source address translation. This option is available only when the translation method is **Dynamic IP+port**, **Dynamic IP**, or **Static IP**.
	Prefix translation	Select a prefix translation type: • **General prefix**—Uses the general prefix for source address translation. • **IVI prefix**—Uses the IVI prefix for source address translation. • **NAT64 prefix**—Uses the NAT64 prefix for source address translation. This option is available only when the translation method is **Prefix translation**.
	IPv6 prefix	Configure the IPv6 address prefix for the prefix translation method. This option is available only when the prefix translation type is **General prefix** or **NAT64 prefix**.
	Prefix length	Configure the IPv6 prefix length. This option is available only when the prefix translation type is **General prefix** or **NAT64 prefix**.
Destination address translation	Translation method	Select a destination address translation method: • **Prefix translation**—Uses the IPv6 prefixes for destination address translation.

Item		Description
		• **NAT server mapping**—Translates the destination IP addresses and destination port numbers of packets to a fixed destination IP address and destination port number. • **Static translation**—Translates the destination IP addresses of packets to a fixed IP address.
	Prefix translation	Select a prefix translation type: • **General prefix**—Uses the general prefix for source address translation. • **IVI prefix**—Uses the IVI prefix for source address translation. • **NAT64 prefix**—Uses the NAT64 prefix for source address translation. This option is available only when the translation method is **Prefix translation**.
	IPv6 prefix	Configure the IPv6 address prefix for the prefix translation method. This option is available only when the prefix translation type is **General prefix** or **IVI prefix**.
	Prefix length	Configure the IPv6 prefix length. This option is available only when the prefix translation type is **General prefix** or **IVI prefix**.
	Destination IP after NAT	Set the destination IP address after translation.
	Port after NAT	Set the destination port after translation. This option is available only when the translation method is **NAT server mapping**.
VRF before NAT	Specify a VRF used to match the VRF to which the packet belongs. The VRF is bound to the ingress port.	
VRF after NAT	Specify a VRF used to replace the VRF to which the matching packets belong. The VRF is bound to the egress port.	

Item		Description
Enable this rule	Enable this policy-based NAT64 rule.	
Counting	Enable the counting of times that the policy-based NAT64 rule is matched.	

Configure a policy-based NAT66 rule

Procedure

Procedure

1. (Optional.) Create a security zone. (Details not shown.)
2. (Optional.) Create an address object group. (Details not shown.)
3. (Optional.) Create a service object group. (Details not shown.)
4. Create a policy-based NAT66 rule.
   a. Click the **Policies** tab.
   b. In the navigation pane, select **Policy-Based NAT**.
   c. Click **Create**.
   d. Create a policy-based NAT rule, and select the rule type as NAT66.
   e. Click **OK**.

Table 3 Configuration items for policy-based NAT66 rules

Item	Description
Rule name	Enter the name of a policy-based NAT66 rule. Chinese characters are supported.

Item			Description
Rule description			Enter the description of the policy-based NAT66 rule.
Original packets		Src zone	Select source security zones for packet match.
		Dst zone	Select destination security zones for packet match.
		Source IP	Select a source IP address, IP subnet, or address object group for packet match.
		Destination IP	Select a destination IP address, IP subnet, or address object group for packet match.
		Service	Select a service object group for packet match.
Source address translation	Translation method		Select a source address translation method: • **Dynamic IP+port**—Uses the PAT method to translate both the source IP addresses and source ports of packets. • **Dynamic IP**—Uses the NO-PAT method to translate only the source IP addresses of packets. • **Static IP**—Translates the source IP addresses of packets to a fixed IP address • **NPTV6**—Uses the NPTV6 method to translate the prefixes in the source IPv6 addresses of packets to the configured prefix. To use this method, you must configure packet match rules for original packets. • **No translation**—This rule and rules with lower priority than this rule are not used for source address translation.
	Source IP after NAT		Select a NAT address for source address translation.
	IPv6 prefix		Configure the IPv6 address prefix for the prefix translation method. This option is available only when the prefix translation method is **NPTV6**.

Item		Description
	Prefix length	Configure the IPv6 prefix length. This option is available only when the prefix translation method is **NPTV6**.
Destination address translation	Translation method	Select a destination address translation method: • **Translation**—Translates the destination IP addresses of packets to a fixed IP address. • **NPTV6**—Uses the NPTV6 method to translate the prefixes in the destination IPv6 addresses of packets to the configured prefix. • **No translation**—This rule and rules with lower priority than this rule are not used for destination address translation.
	Destination IP after NAT	Set the destination IP address after translation.
	Port after NAT	Set the destination port after translation.
	IPv6 prefix	Configure the IPv6 address prefix for the prefix translation method. This option is available only when the translation method is **NPTV6**.
	Prefix length	Configure the IPv6 prefix length. This option is available only when the translation method is **NPTV6**.
VRF before NAT	Specify a VRF used to match the VRF to which the packet belongs. The VRF is bound to the ingress port.	
VRF after NAT	Specify a VRF used to replace the VRF to which the matching packets belong. The VRF is bound to the egress port.	
Enable this rule	Enable this policy-based NAT66 rule.	
Counting	Enable the counting of times that the policy-based NAT66 rule is matched.	

NAT66

Introduction

IPv6-to-IPv6 Network Address Translation (NAT66) translates an IPv6 address in the IPv6 header to another IPv6 address. NAT66 is configured on edge devices of IPv6 networks to allow private users to access external networks and external users to access private network resources such as a Web server.

NAT66 prefix translation

NAT66 prefix translation, also known as IPv6-to-IPv6 Network Prefix Translation (NPTv6), replaces the IPv6 prefix in an IPv6 address of the packet header with another IPv6 prefix. NAT66 prefix translation supports the following translation methods:

- **Source address translation**—Translates prefixes in source IPv6 addresses when users in the internal network access the external network.
- **Destination address translation**—Translates prefixes in destination IPv6 addresses when users in the external network access servers in the internal network.

NAT66 prefix translation uses the IPv6 prefix as the packet match criterion.

Restrictions and guidelines

Restrictions and guidelines: NAT66 prefix translation

- Source prefix translation rules on different interfaces do not support mapping different internal prefixes to the same external prefix.
- Destination prefix translation rules on different interfaces do not support mapping the same external prefix to different internal prefixes.
- Each source or destination prefix translation rule on one interface must be unique.

Configure NAT66

NAT66 can be performed in the inbound or outbound direction.

- Inbound NAT—Performs address translation for packets received on an interface, as shown in Figure 1.
- Outbound NAT—Performs address translation for packets to be sent out of an interface, as shown in Figure 2.

Figure 1 Inbound NAT

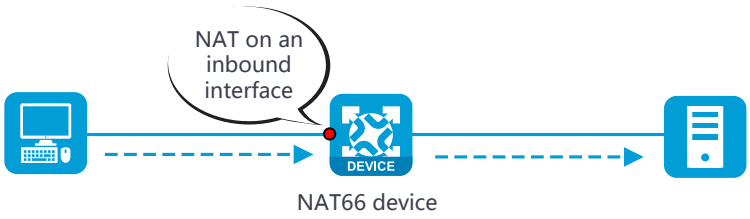
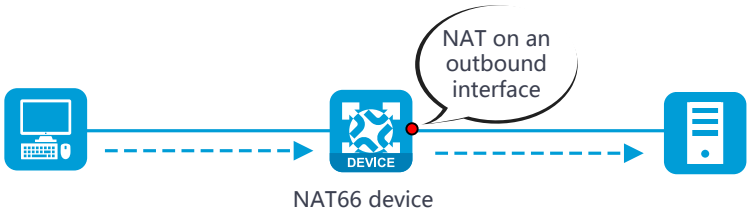


Figure 2 Outbound NAT



Configure NAT66 prefix translation

1. Click the **Policies** tab.
2. In the navigation pane, select **Interface NAT** > **IPv6** > **NAT66 Prefix Translation**.
3. Click **Create**.
4. Configure a NAT66 prefix translation rule as shown in Table 1.

Table 1 Configuration items for NAT66 prefix translation

Item	Description
Interface	Interface to which the NAT66 prefix translation rule is applied.
Translation method	Select one of the following translation methods: • **Source address translation**—Translates the source IP address of packets to be sent out of the interface. • **Destination address translation**—Translates the destination IP address of packets received on the interface.
PAT	PAT used to translate the source port in the matching packets. The option is available only when the translation method is source address translation.
Protocol type	Specify a protocol type. If you do not specify this option, translation is performed on packets of all protocols.

Item	Description
	The option is available only when the translation method is destination address translation.
IPv6 prefix/prefix length before NAT	IPv6 prefix and prefix length for packet match. • For source address translation, the IPv6 address prefix and prefix length are used to identify the matching source IPv6 address in the packet header. • For destination address translation, the IPv6 address prefix and prefix length are used to identify the matching destination IPv6 address in the packet header.
Port before NAT	Specify a port number used to match the source port in the packet header. The option is available only when the protocol type is 6 (TCP) or 17 (UDP).
IPv6 prefix/prefix length after NAT	Ipv6 prefix and prefix length used to replace the prefix in the source or destination Ipv6 address of the matching packets. Ipv6 prefix length before and after the translation must be the same.
Port after NAT	Specify a port number used to replace the source port number of matching packets. The option is only available when the protocol type is 6 (TCP) or 17 (UDP).

5. Click **OK**.

PAT translation mode

Introduction

Port Address Translation (PAT) is a Dynamic NAT translation mode. PAT translates multiple private IP addresses to a single public IP address by mapping the private IP address and source port to the public IP address and a unique port.

PAT supports the following mapping modes:

- **Address and Port-Dependent Mapping (APDM)**—Uses different IP and port mappings for packets from the same source IP and port to different destination IP addresses and ports. APDM allows an external host to initiate connections to an internal host only under the condition that the internal host has previously accessed the external host. It is secure, but it does not allow internal hosts behind different NAT gateways to access each other.
- **Endpoint-Independent Mapping (EIM)**—Uses the same IP and port mapping (EIM entry) for packets from the same source IP and port to any destinations. EIM allows external hosts to initiate connections to the translated IP addresses and ports of internal hosts. It allows internal hosts behind different NAT gateways to access each other.

Application audit

This help contains the following topics:

Introduction

This feature parses personal information from user packets and must be used for legitimate purposes.

Based on application recognition (APR), application audit audits and records Internet access behaviors of users by identifying behaviors and behavior contents of applications.

Basic concepts

Application behaviors

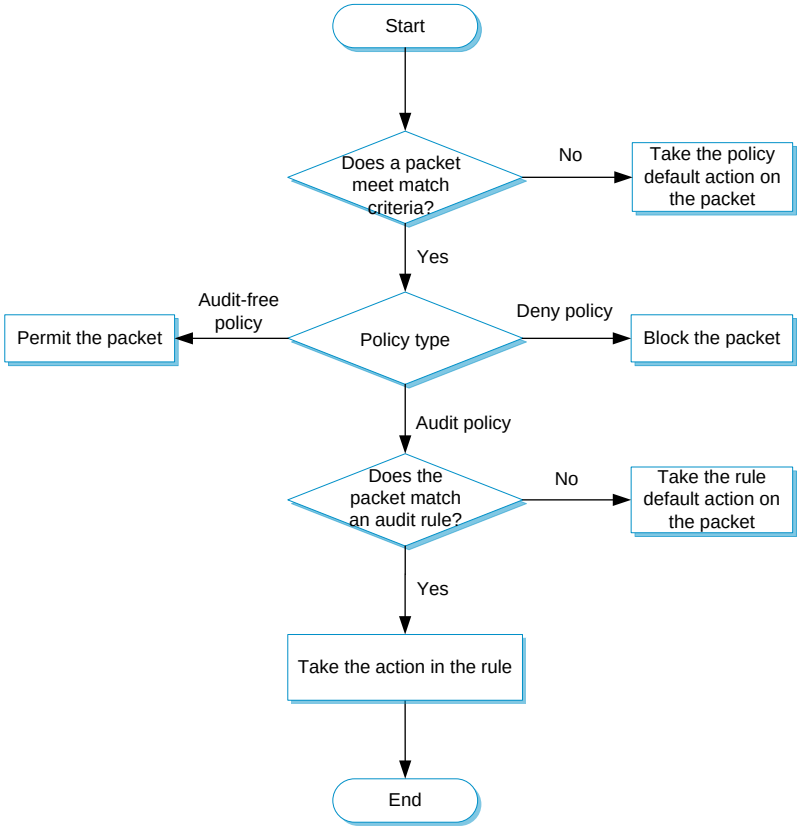
Applications and programs are characterized by different behaviors. For example, IM applications are characterized by login and message sending. FTP is characterized by file upload and file download.

Behavior contents

A behavior content is the content of a behavior. For example, the content of a login behavior is the account information. The content of an FTP file upload behavior is the file name. You can match behavior contents by using a string or a number.

Application audit process

Figure 1 Application audit process



Application audit policy

Different audit policies process matching packets differently.

Policy types

Application audit policies have the following types:

- **Audit policy**—Audits packets that meet match criteria in the policy.
- **Audit-free policy**—Does not audit packets that meet match criteria in the policy.

- **Deny policy**—Drops packets that meet match criteria in the policy.

Policy matching

Multiple application audit policies can exist on a device. The device compares a packet with policies in their configuration order. When a match is found, the match process ends. If no match is found, the device applies the default action to the packet.

You can view the configuration order of policies on the **Audit Policy** page. The configuration order is the creation order if no polices are moved. You can change the configuration order of a policy by moving the policy. As a best practice to audit packets more accurately, observe the depth-first principle when creating policies. Always create a policy with a smaller audit scope before a policy with a larger audit scope.

Match criteria

Multiple match criteria can be configured in an application audit policy. A policy is matched if all match criteria in the policy are matched.

The following match criteria are available:

- Source and destination security zones.
- Source and destination IP addresses.
- Users/user groups.
- Applications/application groups.
- Services.
- Time ranges.

One match criterion can contain multiple match values. For example, you can configure multiple address object groups for a source IP address match criterion. A match criterion is matched if any of its match values is matched.

Audit rule

Audit rules can be configured for an audit policy to perform more granular control on user behaviors and to generate audit logs.

The following rule match modes are available:

- **in-order**—The device compares packets with audit rules in ascending order of rule ID. When a packet matches a rule, the device stops the match process and performs the action defined in the rule.
- **all**—The device compares packets with audit rules in ascending order of rule ID.
    - If a packet matches a rule with the permit action, all subsequent rules continue to be matched.

      The device takes the action with higher priority on matching packets. The deny action has higher priority than the permit action.
    - If a packet matches a rule with the deny action, the device stops the match process and performs the deny action.

If a packet does not match any audit rule, the devices takes the default action for audit rules on the packet.

Email protection can be configured in a rule. The device detects incoming emails, counts emails based on recipients, and protects recipients from attacks. Specifically, you can configure the following functions:

- **Limit email sending**—Prevents users from sending emails to users of a different domain. For example, the user at user1@abc.com cannot receive emails from the user at user2@123.com.
- **Prevent email bombing**—Protects recipients from being overwhelmed by large numbers of emails from the same sender during a short period of time.

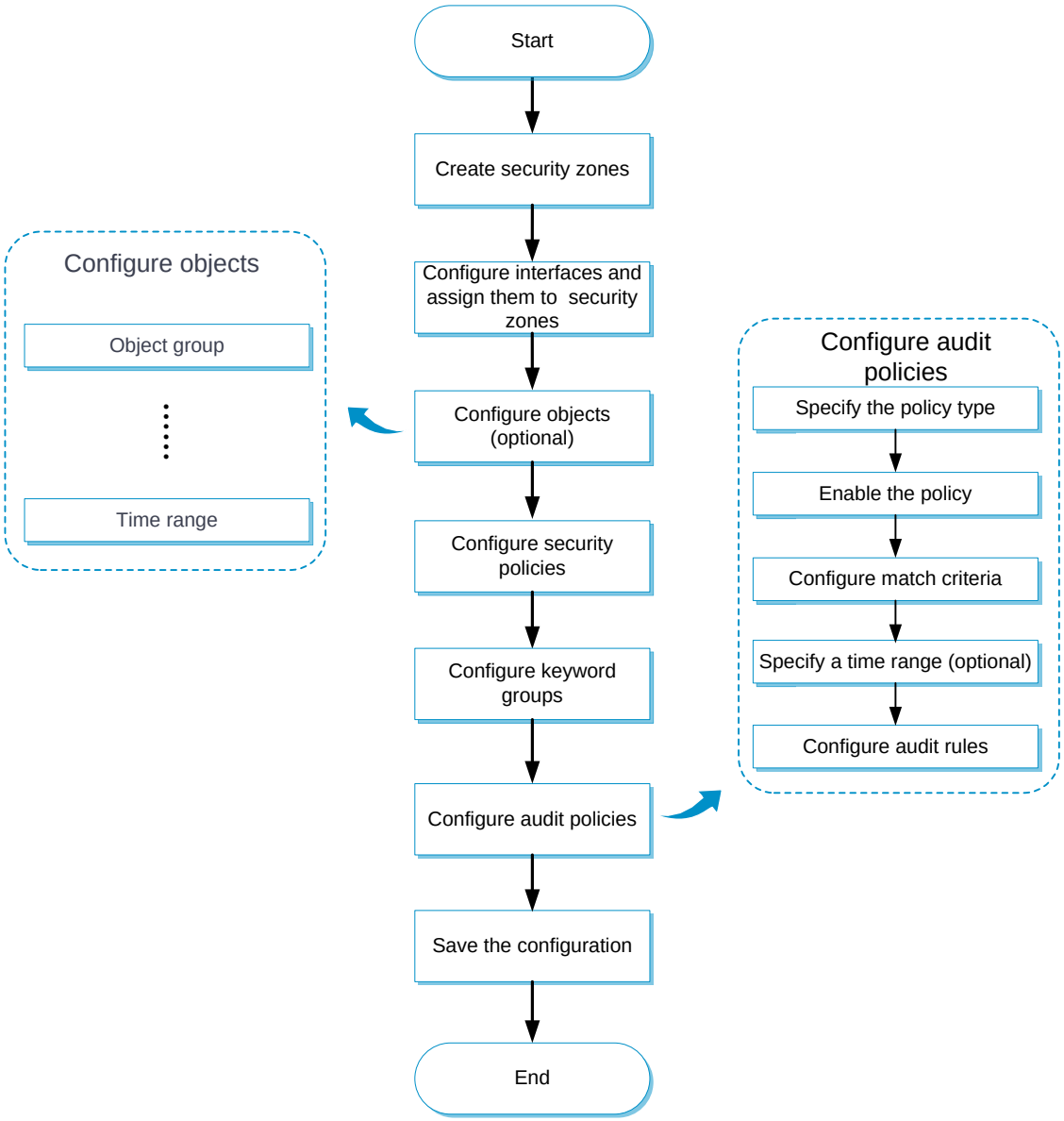
Restrictions and guidelines

By default, an audit policy configuration change takes effect 40 seconds after the change is performed. To make the change take effect immediately, click the **Submit** button. A configuration change indicates creating, editing, deleting, enabling, or disabling an audit policy. Activating configuration causes transient DPI service interruption. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.

Configure application audit

Figure 2 shows the configuration procedure for application audit.

Figure 2 Application audit configuration procedure



Before configuring application audit, configure security policies to allow traffic to flow through the device. For information about configuring security policies, see "Security Policy Help."

Configure a keyword group

1. Select **Policies** > **Application Audit** > **Keyword Groups**.

2. Click **Create** in the **Keyword Group** page.

3. Create a keyword group.

Table 1 Keyword group configuration items

Item	Description
Name	Enter a name for the keyword group.
Description	Enter a description for the keyword group, which helps the administrator identify the keyword group.
Keyword	Enter keywords to be audited. Keywords are separated by carriage returns.

4. Click **OK**. The new keyword group appears in the **Keyword Group** page.

Configure an application audit policy

1. Select **Policies** > **Application Audit** > **Audit Policies**.

2. Click **Create** in the **Audit Policy** page.

3. Create an application audit policy.

Table 2 Application audit policy configuration items

Item	Description
Name	Enter a name for the application audit policy.
Type	Select the application audit policy type: Audit, Audit-free, and Deny.

Item	Description
Enable	Enable the policy to make it take effect.
Source security zone	Specify a source security zone as a match criterion.
Destination security zone	Specify a destination security zone as a match criterion.
Source IP address	Specify a source IP address object group as a match criterion.
Destination IP address	Specify a destination IP address object group as a match criterion.
Service	Specify a service object group as a match criterion.
User	Specify a user as a match criterion.
Application	Specify an application or application group as a match criterion.
Time range	Specify a time range during which the policy is in effect.
Audit rule	Configure an audit rule to perform refined auditing on the behaviors and behavior contents of applications. This item can be configured only for an Audit-type policy.
Rule ID	Enter a rule ID.
Application	Select the applications to be audited.
Behavior	Select the behaviors to be audited.
Behavior content	Select the behavior contents to be audited.
Match type	Specify the behavior content type: • **Keyword**. • **Number**.
Keyword	Operator used when behavior contents are matched: • For keyword-type behavior contents: **Include**, **Exclude**,

Item	Description
	Equal, **Unequal**. • For number-type behavior contents: **Equal**, **Unequal**, **Greater**, **Less**, **Greater-equal**, **Less-equal**.
Email protection	Select **Enable** to configure the **Limit email sending** and **Prevent email bombing** functions.
Limit email sending	Select **Enable** to prevent users from sending emails to users of a different domain.
Prevent email bombing	Configure this function to protect recipients from being overwhelmed by large numbers of emails from the same sender during a short period of time. • **Detection time**—The specified maximum number of emails can be received from the same user during this time. • **Email count**—The maximum number of emails that can be received from the same user during the detection time.
Action	Select an action to take on packets matching audit rules: **Permit** or **Deny**.
Logging	Select **Enabled** or **Disabled** to enable or disable generation of logs.

4. Click **OK**. The new application audit policy appears in the **Audit Policy** page.
5. To make the new application audit policy take effect immediately, click the **Submit** button. By default, a new audit policy takes effect 40 seconds after it is created.

Bandwidth management

This help contains the following topics:

Introduction

Bandwidth management provides fine-grained control over traffic that flows through the device by using information such as source and destination IP addresses and usernames.

Bandwidth management is used in the following scenarios:

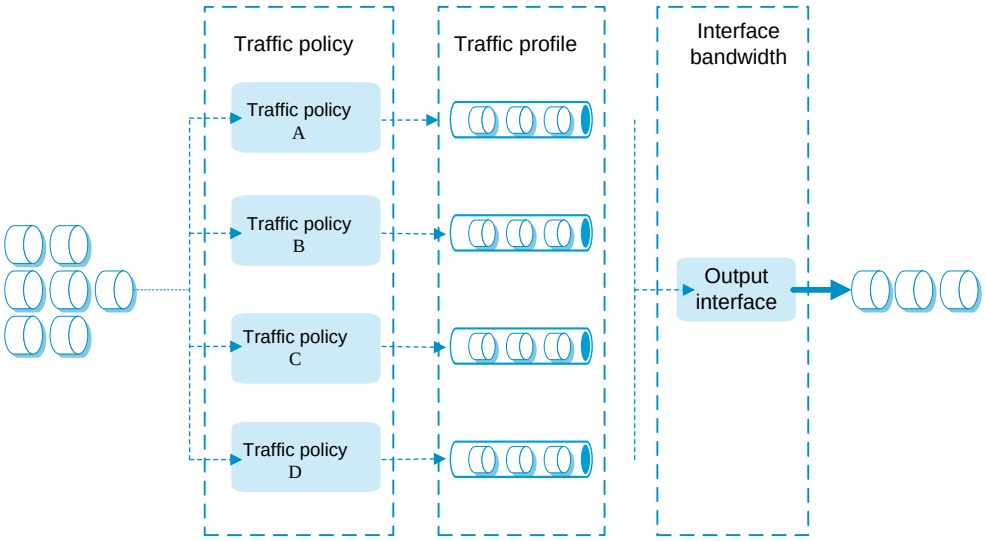
- Enterprise intranet users need far more bandwidth than the amount of bandwidth leased from an ISP. This creates a bandwidth bottleneck at the intranet egress.
- The P2P traffic on the intranet egress consumes a majority of the bandwidth resources. As a result, bandwidth cannot be guaranteed for key services.

Bandwidth management allows you to deploy traffic policies on the network egress for different traffic types. Bandwidth management improves bandwidth efficiency and guarantees bandwidth for key services when congestion occurs.

Bandwidth management process

Bandwidth management is implemented through traffic policies. You can configure traffic profiles and traffic policies in a traffic policy. A traffic profile specifies the guaranteed bandwidth and maximum bandwidth. A traffic policy specifies match criteria to match packets and the traffic profile to apply to matching packets.

Figure 1 Bandwidth management process



The bandwidth management process is as follows:

2. If a packet matches a traffic policy, the interface processes the packet according to the traffic profile (if any) specified for the traffic policy.

   If no traffic profile is specified for the traffic policy, the packet is forwarded without bandwidth management.

3. The traffic profile processes the packet according to its settings.

4. The packet is limited by the interface bandwidth of the output interface.

Traffic rule

Multiple traffic policies can be configured. In a traffic policy, you can define the match criteria to match packets and specify the traffic profile to apply to matching packets. The device matches traffic policies in their order of appearance on the device. When a traffic policy is matched, the matching process ends and the device applies the traffic profile for the traffic policy to the traffic. If no traffic policy is matched, the device forwards the traffic.

You can configure the following match criteria in a traffic policy:

- Source and destination security zones.
- Source and destination IP addresses.
- Users.

One match criterion can contain multiple match values. For example, you can configure multiple address object groups for a source IP address match criterion. A match criterion is matched if any of its match values is matched.

Traffic policies support policy nesting, which allows a traffic policy to have a parent traffic policy. A maximum of four nesting levels are supported. The following rules apply when the device matches a traffic policy with a parent traffic policy:

- The parent traffic policy is first matched. After the parent traffic policy is matched, the child traffic policy is matched. If the parent traffic policy is not matched, the child traffic policy is ignored and the matching process fails.
- If both parent and child traffic policies are matched, the traffic profile for the child traffic policy is executed before the traffic profile for the parent traffic policy is executed. If both parent and child traffic policies are about the same parameter, the smaller value for an upper-limit

parameter or the larger value for a lower-limit parameter is applied. If only the parent traffic policy is matched, the traffic profile for the parent traffic policy is applied.

Traffic profile

A traffic profile defines bandwidth resources that can be used by a traffic type. The interface bandwidth can be allocated among multiple traffic profiles. You can configure the following parameters in a traffic profile:

Table 1 Parameters in a traffic profile

Item	Description
Rate limit mode	You can limit the traffic rate in one of the following ways: • Limit the upstream bandwidth and downstream bandwidth separately. • Limit the upstream bandwidth and downstream bandwidth as a whole.
Reference mode	A traffic profile can be referenced by multiple traffic policies in one of the following ways: • **Exclusive**—Each rule that uses the profile can reach the bandwidth limits and connection limits specified in the profile. • **Shared**—All rules that use the profile share the bandwidth limits and connection limits specified in the profile.
Total guaranteed bandwidth	Guarantees the total minimum bandwidth for key services when congestion occurs.
Total maximum bandwidth	Controls the total maximum bandwidth for non-key services to prevent them from consuming a large amount of bandwidth.
Bandwidth allocation among	Allocates the total maximum bandwidth dynamically and

Item	Description
IP addresses	evenly among online IP addresses.
Per-IP or per-user guaranteed bandwidth	Guarantees the minimum bandwidth per IP address or per user to provide for bandwidth management at finer granularity.
Per-IP or per-user maximum bandwidth	Controls the maximum bandwidth allowed per IP address or per user to provide for bandwidth management at finer granularity.
Connection limits	Limits the total connection count, total connection rate, per-user/per-IP connection count, and per-user/per-IP connection rate.
Per-IP traffic quota	Limits the monthly traffic quota per IP address. After you configure this function, you can view traffic statistics on the **Per-IP traffic statistics** tab.
Monthly traffic quota	Per-IP monthly traffic quota.
Forwarding priority	When an interface is congested with packets of multiple traffic profiles, packets with higher priority are sent first. Packets with the same priority have the same chance of being forwarded.
DSCP marking	Modifies the DSCP value in packets. Network devices can classify traffic by using DSCP values and provide different treatment for packets according to the modified DSCP values.
TCP MSS	Specifies the TCP maximum segment size.
Bandwidth check	Enables the device to detect the amount of bandwidth consumed by traffic in real time by source IP address.
Static thresholds	Specifies the maximum bandwidth threshold and minimum bandwidth threshold. When the device detects that the traffic rate exceeds the maximum bandwidth threshold or falls below the minimum bandwidth threshold, it outputs logs to the log host by using the fast log output feature.
Dynamic threshold learning	Enables the device to dynamically learn the bandwidth threshold.

Item	Description
	Enable this option if you do not know the traffic rates in the network. The device will derive the maximum and minimum bandwidth thresholds from multiplying the learned bandwidth threshold by the maximum and minimum tolerance values. The derived maximum and minimum bandwidth thresholds have higher priority than the static thresholds.
Learning duration	Specifies the learning duration in minutes. After dynamic threshold learning is enabled, the device learns the traffic rates during the specified duration and calculates an average value as the learned bandwidth threshold. As a best practice to ensure the device can learn the traffic of a whole day, set the learning duration to be longer than 1440 minutes (24 hours). If the learning duration is modified while the device is learning, the device will learn the traffic again based on the new learning duration.
Bandwidth tolerance	Specifies the bandwidth tolerance values. The device derives the maximum and minimum bandwidth thresholds from multiplying the learned bandwidth threshold by the maximum and minimum bandwidth tolerance values. If you do not care about the minimum bandwidth threshold, you can specify only the maximum bandwidth tolerance value. If you do not care about the maximum bandwidth threshold, you can specify only the minimum bandwidth tolerance value.

Restrictions and guidelines

- The maximum bandwidth for a child traffic policy must be smaller than or equal to that for its parent traffic policy.
- The guaranteed bandwidth for a child traffic policy must be smaller than or equal to that for its parent traffic policy.
- The traffic profiles cannot be the same for the child and parent traffic policies.

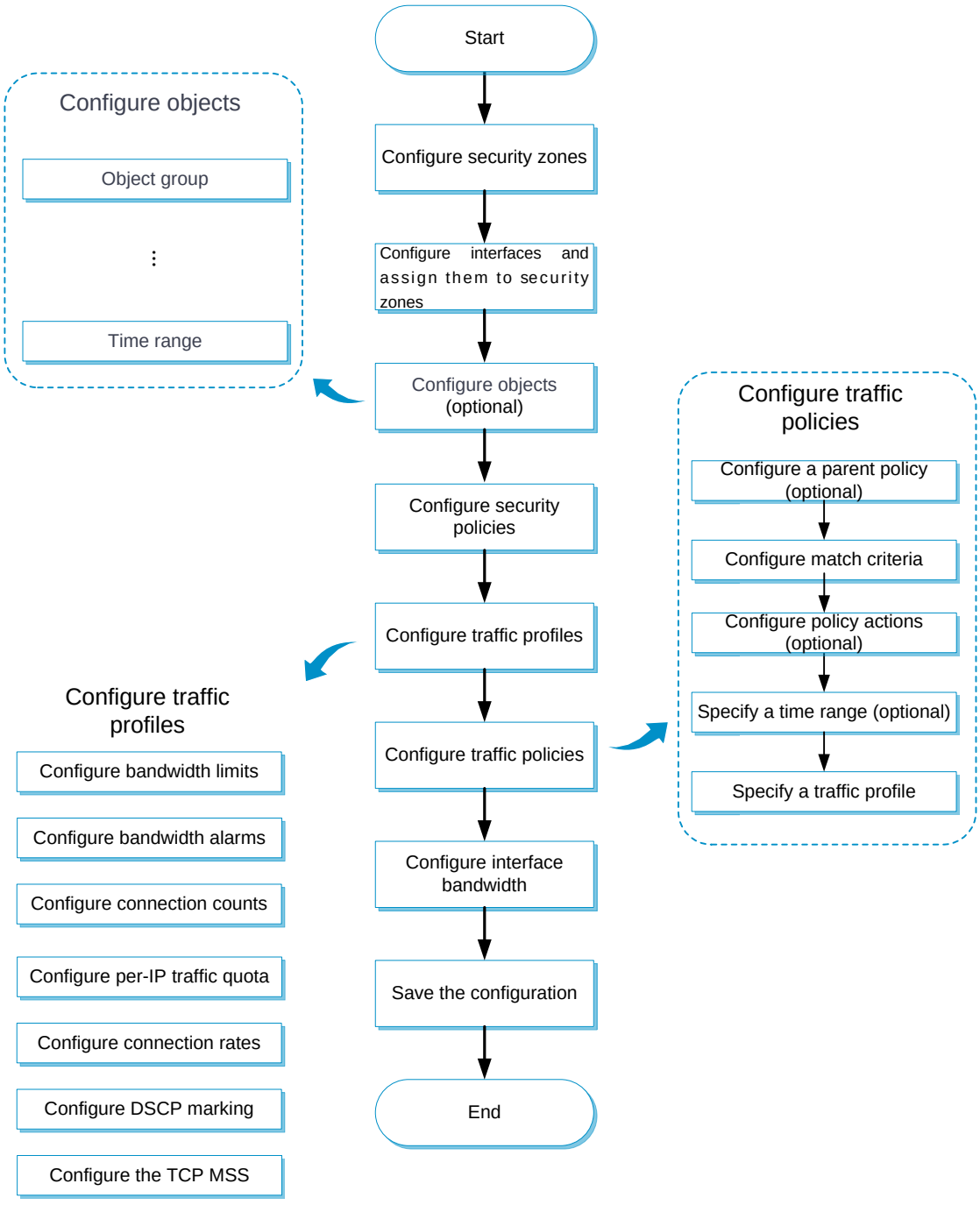
- If a traffic policy has a child traffic policy, the device performs bandwidth check and dynamic threshold learning only for the child traffic policy.
- An interface with small default expected bandwidth might experience traffic loss if the following conditions exist:
    - There is a large amount of traffic on the interface.
    - The interface uses the default expected bandwidth.

    To avoid traffic loss, implicitly set the expected bandwidth to a large value for such an interface. For example, you can set the expected bandwidth of a tunnel interface to a value greater than 64 kbps (the default) if there is a large amount of traffic on the interface.
- If a traffic policy to be copied has child traffic policies, only the parent traffic policy is copied.
- The traffic policy created by copying a traffic policy is placed next to the copied traffic policy.
- You can specify a parent traffic policy only when creating a traffic policy. You cannot add or modify a parent traffic policy for an existing traffic policy.
- The rate limit modes of the child and parent traffic policies must be the same.
- A parent traffic policy does not support dynamic and even allocation for maximum bandwidth.
- The all-OSI-layer protocol flow control function takes effect only on IPv6 packets.
- After the all-OSI-layer protocol flow control function is disabled, bandwidth management is performed on traffic of Layer 4 protocols and upper layer protocols.

Configure bandwidth management

Figure 2 shows the configuration procedure for bandwidth management.

Figure 2 Bandwidth management configuration procedure



Before configuring bandwidth management, configure security policies to allow traffic to flow through the device. For information about configuring security policies, see "Security Policy Help."

Configure a traffic profile

1. Select **Policies** > **Bandwidth Management** > **Traffic Profiles**.
2. Click **Create** on the **Traffic Profile** tab.
3. Create a traffic profile.

Table 2 Traffic profile configuration items

Item	Description
Name	Enter a name for the traffic profile.
Rate limit mode	Select **Limit uplink and downlink separately** or **Limit uplink and downlink**.
Reference mode	Select **Exclusive** or **Shared**.
Total uplink maximum bandwidth	Set the total uplink maximum bandwidth.
Total uplink guaranteed bandwidth	Set the total uplink guaranteed bandwidth.
Total downlink maximum bandwidth	Set the total downlink maximum bandwidth.
Total downlink guaranteed bandwidth	Set the total downlink guaranteed bandwidth.
Forwarding priority	Set the forwarding priority. A greater priority value means a higher priority.
Bandwidth allocation among IP addresses	Select this option to allocate the total maximum bandwidth dynamically and evenly among online IP addresses.
Per-IP uplink maximum bandwidth	Set the per-IP uplink maximum bandwidth.

Item	Description
Per-IP downlink maximum bandwidth	Set the per-IP downlink maximum bandwidth.
Per-user uplink maximum bandwidth	Set the per-user uplink maximum bandwidth.
Per-user downlink maximum bandwidth	Set the per-user downlink maximum bandwidth.
Enable bandwidth check	Enable the device to detect the amount of bandwidth consumed by traffic in real time by source IP address.
Static threshold-Maximum	Set the maximum static threshold.
Static threshold-Minimum	Set the minimum static threshold.
Enable dynamic threshold learning	Enable the device to dynamically learn bandwidth thresholds.
Learning duration	Set the learning duration.
Learning tolerance-Maximum	Set the maximum bandwidth tolerance value. The device derives the maximum bandwidth threshold from multiplying the learned bandwidth threshold by the maximum bandwidth tolerance value.
Learning tolerance-Minimum	Set the minimum bandwidth tolerance value. The device derives the minimum bandwidth threshold from multiplying the learned bandwidth threshold by the minimum bandwidth tolerance value.
Total connection count	Set the total connection count.
Per-IP/Per-user connection count	Set the per-IP/per-user connection count.
Total connection rate	Set the total connection rate.
Per-IP/Per-user connection	Set the per-IP/per-user connection rate.

Item	Description
rate	
Monthly traffic quota	Set the per-IP monthly traffic quota.
Mark DSCP priority	Set the DSCP priority to be marked for packets.
TCP MSS	Set the TCP MSS.

4. Click **OK**. The new traffic profile appears on the **Traffic Profile** page.

Configure a traffic policy

1. Select **Policies** > **Bandwidth Management** > **Traffic Policies**.
2. Click **Create** on the **Traffic Policy** page.
3. Create a traffic policy.

Table 3 Traffic policy configuration items

Item	Description
Name	Enter a name for the traffic policy.
Parent policy	Specify a parent policy.
Source security zone	Specify a source security zone as a match criterion.
Destination security zone	Specify a destination security zone as a match criterion.
Source IP address	Specify a source IP address object group as a match criterion.

Item	Description
Destination IP address	Specify a destination IP address object group as a match criterion.
User	Specify an identity user or user group as a match criterion.
Application	Specify an application or application group as a match criterion.
Service	Specify a service object group as a match criterion.
Time range	Specify a time range during which the policy is in effect.
DSCP priority	Specify a DSCP priority as a match criterion.
IPv6 flow label	Specify an IPv6 flow label as a match criterion.
IPv6 extension header	Specify an IPv6 extension header as a match criterion.
Terminal	Specify a terminal or terminal group as a match criterion.
Action	Specify an action for the policy: • **Rate limit**—Limits the rate of matching packets by referencing a traffic profile. • **Not rate limit**—Does not limit the rate of matching packets. • **Block**—Blocks matching packets.
Traffic profile	Specify a traffic profile.

4. Click **OK**. The new traffic policy appears on the **Traffic Policy** page.
5. To perform bandwidth management on traffic of Layer 3 protocols and upper layer protocols, enable **All-OSI-layer protocol flow control** at the upper right corner of the page. By default, bandwidth management is performed on traffic of Layer 4 protocols and upper layer protocols.

Configure interface bandwidth

1. Select **Policies** > **Bandwidth Management** > **Interface Bandwidth**.
2. Click **Create** on the **Interface Bandwidth List** page.
3. Create an interface bandwidth entry.

Table 4 Interface bandwidth configuration items

Item	Description
Interface name	Select an interface.
Expected bandwidth	Specify the expected bandwidth value.

4. Click **OK**. The new interface bandwidth entry appears on the **Interface Bandwidth List** page.

Load balancing common configuration

This help contains the following topics:

- Configure common settings
  - Configure a link
  - Configure a sticky group
  - Configure an SNAT address pool
  - Configure proximity
  - Configure ISP information
  - Configure a region
  - Advanced configuration

Configure common settings

Configure a link

A link is a physical link provided by an ISP. A link can be used in outbound link load balancing, inbound link load balancing, and transparent DNS proxy.

Procedure

1. Select **Policies** > **Load Balancing** > **Common Configuration** > **Links**.

2. Click **Create** on the **Link** page.

3. Create a link.

Table 1 Link configuration items

Item	Description
Link name	Enter a link name, case insensitive.
Next hop config method	Select a next hop configuration method: • Manual • Automatic
Next hop IPv4 address	Specify an outbound next hop IPv4 address. The IPv4 address cannot be an IPv4 address of any interface on the device, loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.
Next hop IPv6 address	Specify an outbound next hop IPv6 address. The IPv6 address cannot be an IPv6 address of any interface on the device, loopback address, multicast address, link-local address, or all-zero address.
Outgoing interface	Specify an outgoing interface for the link. The outgoing interface must be an interface whose IP address can be dynamically obtained.
Link cost for proximity calculation	Specify the link cost for proximity calculation.
Link feature	Enable or disable the link feature.
VRF	Specify the VPN instance to which the link belongs.
VRF inheritance	Enable or disable VRF inheritance. When VRF inheritance is enabled, a link without a VPN instance specified inherits the VPN instance of the virtual server. When VRF inheritance is disabled, a link without a VPN instance specified belongs to the public network.
Description	Enter a description for the link.

Table 2 Advanced link configuration items

Item	Description
Weight	Specify the link weight. For the weighted round robin and weighted least connections algorithms, a greater value means a higher priority to be referenced.
Priority	Specify the priority of the link in a link group. If the number of links with the highest priority is less than the minimum number, links with lower priority are selected to meet the minimum number or until no links are available. You can configure the maximum number and minimum number from **Policies** > **Load Balancing** > **Link Load Balancing** > **Outbound Link Load Balancing** > **Link Group**.
Link group	Select an existing link group or create a link group.
Probe method	Specify a probe template used to detect the health and availability of the link. You can also configure this parameter for a link group on the **Link Group** page. The probe template configured for a link has higher priority over that configured for a link group. You can select an existing probe template or create a probe template.
Success criteria	Specify the health monitoring success criteria for the link. • **All probes succeed**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least n probes succeed**—Health monitoring succeeds when a minimum of the specified number of health monitoring methods succeed. When the specified number of health monitoring methods is greater than the number of health monitoring methods on the device, health monitoring succeeds if all health

Item	Description
	monitoring methods succeed.
Total bandwidth-Bandwidth ratio	Specify the bandwidth ratio. The bandwidth ratio is the percentage of the current bandwidth to the total maximum bandwidth. When the traffic exceeds the maximum expected bandwidth multiplied by the bandwidth ratio of a link, new traffic (traffic that does not match any sticky entries) is not distributed to the link. If you do not set this parameter, the maximum value that can be set applies.
Total bandwidth-Bandwidth recovery ratio	Specify the bandwidth recovery ratio. When the traffic drops below the maximum expected bandwidth multiplied by the bandwidth recovery ratio of the link, the link participates in scheduling again. The bandwidth recovery ratio of a link must be smaller than or equal to the bandwidth ratio of the link.
Inbound bandwidth-Bandwidth ratio	Specify the inbound bandwidth ratio. The inbound bandwidth ratio is the percentage of the current inbound bandwidth to the maximum inbound bandwidth. When the traffic exceeds the maximum expected bandwidth multiplied by the bandwidth ratio of a link, new traffic (traffic that does not match any sticky entries) is not distributed to the link. If you do not set this parameter, the maximum value that can be set applies.
Inbound bandwidth-Bandwidth recovery ratio	Specify the inbound bandwidth recovery ratio. When the traffic drops below the maximum expected bandwidth multiplied by the bandwidth recovery ratio of the link, the link participates in scheduling again. The bandwidth recovery ratio of a link must be smaller than or equal to the bandwidth ratio of the link.
Outbound bandwidth-Bandwidth ratio	Specify the outbound bandwidth ratio. The inbound bandwidth ratio is the percentage of the current inbound bandwidth to the maximum inbound bandwidth. When the traffic exceeds the maximum expected bandwidth multiplied by the bandwidth

Item	Description
	ratio of a link, new traffic (traffic that does not match any sticky entries) is not distributed to the link. If you do not set this parameter, the maximum value that can be set applies.
Outbound bandwidth-Bandwidth recovery ratio	Specify the outbound bandwidth recovery ratio. When the traffic drops below the maximum expected bandwidth multiplied by the bandwidth recovery ratio of the link, the link participates in scheduling again. he bandwidth recovery ratio of a link must be smaller than or equal to the bandwidth ratio of the link.
Maximum bandwidth-Expected bandwidth	Specify the total maximum expected bandwidth. The value 0 means that the total maximum expected bandwidth is not limited. In addition to being used for link protection, the total maximum expected bandwidth is used for remaining bandwidth calculation in the bandwidth algorithm, maximum bandwidth algorithm, and dynamic proximity algorithm.
Maximum bandwidth-Expected inbound bandwidth	Specify the inbound maximum expected bandwidth. The value 0 means that the inbound maximum expected bandwidth is not limited. In addition to being used for link protection, the inbound maximum expected bandwidth is used for remaining bandwidth calculation in the bandwidth algorithm, maximum bandwidth algorithm, and dynamic proximity algorithm.
Maximum bandwidth-Expected outbound bandwidth	Specify the outbound maximum expected bandwidth. The value 0 means that the outbound maximum expected bandwidth is not limited. In addition to being used for link protection, the outbound maximum expected bandwidth is used for remaining bandwidth calculation in the bandwidth algorithm, maximum bandwidth algorithm, and dynamic proximity algorithm.
QoS-Connections	Specify the maximum number of connections allowed on the link. The value 0 means that the number of connections allowed on a link is not limited.

Item	Description
QoS-Connections per second	Specify the maximum number of connections per second allowed on the link. The value 0 means that the number of connections per second allowed on a link is not limited.
QoS-Bandwidth	Specify the total maximum bandwidth allowed on the link. The value 0 means that the total bandwidth allowed on a link is not limited.
QoS-Inbound bandwidth	Specify the inbound maximum bandwidth allowed on the link. The value 0 means that the inbound bandwidth allowed on a link is not limited.
QoS-Outbound bandwidth	Specify the outbound maximum bandwidth allowed on the link. The value 0 means that the outbound bandwidth allowed on a link is not limited.

4. Click **OK**. The new link appears on the **Link** page.

Configure a sticky group

A sticky group uses a sticky method to distribute similar sessions to the same real server or link according to sticky entries. The sticky method applies to the first packet of a session. Other packets of the session are distributed to the same real server or link.

Procedure

1. Select **Policies** > **Load Balancing** > **Common Configuration** > **Sticky Groups**.
2. Click **Create** on the **Sticky Group** page.
3. Create a sticky group.

Table 3 Sticky group configuration items

Item	Description
Stick group name	Enter a name for the sticky group, case insensitive.
Type	Select a group type: • Address and port • Payload • HTTP-Content • HTTP-Cookie • HTTP-Header • SSL • RADIUS • SIP • HTTP-Passive • UDP-Passive • TCP-Payload
Aging	Specify whether to age out sticky entries: **Yes** or **No**.
Aging time	Specify the timeout time for sticky entries. For sticky groups of the HTTP cookie type, the following rules apply: • If the sticky method is cookie insert or cookie rewrite, a timeout timer of 0 indicates session persistency. • If the sticky method is cookie get, a timeout timer of 0 indicates the timeout time for the sticky entries is 0 seconds.
Override limits	Enable or disable the function of ignoring the limits for sessions that match sticky entries. After this function is enabled, the device ignores the following limits for sessions that match sticky entries: • Bandwidth and connection parameters on real servers or links. • LB connection limit policies on virtual servers.

Item	Description
Stickiness-over-busyness	Enable or disable the stickiness-over-busyness function. This function enables the device to assign client requests to real servers based on sticky entries, regardless of whether the real servers are busy. When this function is disabled, the device assigns client requests to only real servers in normal state.
Match Across Virtual Servers	Enable or disable sticky entry matching across virtual servers. If you enable this function, traffic not matching any sticky entries on the virtual server will be matched against sticky entries on another virtual server. This parameter is supported only by the address and port and RADIUS sticky methods.
Match Across Services	Enable or disable sticky entry matching across services. If you enable this function, traffic not matching any sticky entries on the virtual server will be matched against sticky entries on another virtual server with the same IP address. This parameter is supported only by the address and port and RADIUS sticky methods.
Description	Enter a description for the sticky group.

Table 4 Address and port sticky method configuration items

Item	Description
IPv4	Select an IPv4 address/port sticky method: • Source address • Source address/port • Destination address • Destination address/port • Source address/Destination address • Source/Destination address/port
IPv6	Select an IPv6 address/port sticky method:

Item	Description
	• Source address • Source address/port • Destination address • Destination address/port • Source address/Destination address • Source/Destination address/port

Table 5 Payload sticky method configuration items

Item	Description
Offset	Specify the offset value of the HTTP payload based on the start of the HTTP packet.
Start string	Specify the regular expression that marks the start of the HTTP payload. The string cannot contain question marks (?).
Length/End string	Specify the length and end string of the HTTP payload. • **Length**—Specify the length of the HTTP payload. The value 0 indicates any length. • **End string**—Specify the regular expression that marks the end of the HTTP payload. The string cannot contain question marks (?).

Table 6 HTTP entity sticky method configuration items

Item	Description
Offset	Specify the offset value of the entity based on the start of the HTTP packet.
Start string	Specify the regular expression that marks the start of the entity. The string

Item	Description
	cannot contain question marks (?).
Length/End string	Specify the length and end string of the HTTP entity. • **Length**—Specify the length of the HTTP entity. The value 0 indicates any length. • **End string**—Specify the regular expression that marks the end of the HTTP entity. The string cannot contain question marks (?).

Table 7 HTTP cookie sticky method configuration items

Item	Description
Cookie stickiness	Select a cookie sticky method: • **Cookie insert**—Inserts the **Set-Cookie** field to the HTTP response packets sent by the server. • **Cookie rewrite**—Rewrites the **Set-Cookie** field in the HTTP response packets sent by the server. • **Cookie get**—Gets the **Set-Cookie** field in the HTTP response packets sent by the server.
Cookie name	Specify an HTTP cookie by its name, case sensitive.
Cookie domain name	Specifies a domain name indicating the hosts to which the cookie will be sent. If you do not specify this option, the cookie will be sent to only the host where it is created. Suppose a client can visit hosts **example.com**, **www.example.com**, and **www.corp.example.com**. If you specify **example.com**, the client includes the cookie when sending HTTP requests to any of the three hosts. If you specify **www.corp.example.com**, the client includes the cookie only when sending HTTP requests to **www.corp.example.com**. This parameter is supported only by the cookie insert sticky method.
Cookie path	Specifies a path to which the cookie will be sent. If you do not specify a path, the cookie will be sent to every path (the root directory / applies) of the specified domain name.

Item	Description
	This parameter limits the scope of the cookie to the specified path. Suppose a client can visit folders **www.example.com/a** and **www.example.com/b**. If you specify domain name **www.example.com** and path **/a**, the client includes the cookie only when sending HTTP requests to www.example.com/a. This parameter is supported only by the cookie insert sticky method.
HTTPOnly	Enable this option to prevent the cookie from being accessed by scripts. If you disable this option, the cookie can be accessed by scripts. The option prevents attackers from obtaining cookie information by using scripts. This option is supported only by the cookie insert and cookie rewrite sticky methods.
Secure	Enable this option to transmit the cookie over only HTTPS connections. If you disable this option, the cookie can be transmitted over any connections. This option is supported only by the cookie insert and cookie rewrite sticky methods.
Check all packets	Enable or disable checking for all packets. • If the sticky method is cookie get, use this parameter to get cookies from all HTTP response packets. If this parameter is not configured, the device gets only the Set-Cookie from the first response packet of a connection. • If the sticky method is cookie rewrite, use this parameter to rewrite cookies in all HTTP response packets. If this parameter is not configured, the device rewrites only the Set-Cookie in the first response packet of a connection. • If the sticky method is cookie insert, use this parameter to insert cookies to all HTTP response packets. If this parameter is not configured, the device inserts only the Set-Cookie to the first response packet of a connection.
Secondary cookie	Specify the name of the secondary cookie, a case-sensitive. The name cannot contain brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), or horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127. Only the cookie get sticky method supports this parameter. The device locates the secondary cookie in the URI when it fails to locate the specified cookie in the HTTP request packet header.
Offset	Specify the offset value of the cookie based on the start of the HTTP packet. Only the cookie get sticky method supports this parameter.

Item	Description
Start string	Specify the regular expression that marks the start of the cookie. The string cannot contain question marks (?). Only the cookie get sticky method supports this parameter.
Length/End string	Specify the length and end string of the cookie. • **Length**—Specify the length of the cookie. The value 0 indicates any length. • **End string**—Specify the regular expression that marks the end of the HTTP cookie. The string cannot contain question marks (?). Only the cookie get sticky method supports this parameter.

Table 8 HTTP header sticky method configuration items

Item	Description
Header stickiness	Select a header sticky method: • **URL**—HTTP URL based sticky method. • **Host**—HTTP host based sticky method. • **Method**—HTTP Request-Method based sticky method. • **Version**—HTTP version based sticky method. • **Name**—HTTP header name based sticky method.
Header name	Specify the HTTP header name. This parameter appears only if you have selected the HTTP header name based sticky method.
Offset	Specify the offset value of the HTTP header based on the start of the HTTP packet.
Start string	Specify the regular expression that marks the start of the HTTP header. The string cannot contain question marks (?).
Length/End string	Specify the length and end string of the HTTP header. • **Length**—Specify the length of the HTTP header. The value 0 indicates

Item	Description
	any length. • **End string**—Specify the regular expression that marks the end of the HTTP header. The string cannot contain question marks (?).

Table 9 SSL sticky method configuration items

Item	Description
SSL stickiness	Specify the SSL sticky method based on SSL session ID. This sticky method applies only to HTTPS request packets and requires specifying an SSL server policy for the virtual server.

Table 10 RADIUS sticky method configuration items

Item	Description
RADIUS attribute	Specify the RADIUS attribute sticky method. This sticky method applies only to RADIUS packets. The value 1 indicates the User-Name attribute. The value 8 indicates the Framed-IP-Address attribute.

Table 11 SIP sticky method configuration items

Item	Description
SIP stickiness	Specify the SIP sticky method based on the call ID in the header of SIP messages. All SIP messages with same call ID are assigned to the same real server.

Table 12 HTTP-passive sticky method configuration items

Item	Description
Check all packets	Enable or disable checking for all packets. This parameter determines whether or not to generate sticky entries from all HTTP response packets. If this parameter is not configured, the device generates sticky entries only from the first response packet of a connection.

Request configuration	Enable the device to obtain the specified string from HTTP requests for matching HTTP-passive sticky entries.
	
	The HTTP-passive sticky method requires both the request and response configuration for generating sticky entries. With the HTTP-passive sticky method configured, the device obtains the specified string in the HTTP response based on the response configuration, and generates a sticky entry. For all subsequent HTTP requests, the device obtains the specified string based on the request configuration. If the string matches the sticky entry, the device forwards the HTTP request according to the sticky entry.
	
	Follow these guidelines when you configure the request and response:
	
	• An HTTP-passive sticky group allows the device to obtain a maximum of four strings from HTTP response packets and a maximum of four strings from HTTP request packets.
	
	• Suppose the device obtains n strings from HTTP response packets. The strings can further generate 2^n-1 strings by combining the method IDs in the response configuration. Any of the 2^n-1 strings can be used to match the string obtained using the request configuration.
	
	• Suppose the device obtains n strings from HTTP request packets. Those strings will be combined as one string by following the configuration order of method IDs.
	
	Use an example to illustrate how to generate a sticky entry based on HTTP request and response packets:
	
	• Configure method IDs 1, 2, and 3 in the response configuration. If the device obtains strings a, b, and c based on your configuration, the strings can further generate seven strings, namely, a, b, c, ab, ac, bc, and abc.
	
	• Configure method IDs 2, 3, and 4 in the request configuration.
	
	• After receiving HTTP requests, the device generates a sticky entry when the following conditions are met:
	
	  ◦ The device obtains strings a, b, and c based on the request configuration.
	
	  ◦ The combined string abc matches that obtained based on the response configuration.

Item	Description
	• For subsequent HTTP requests matching the sticky entry generated based on the string abc, the device forwards them according to the sticky entry. To configure the request: 1. Click **Create** to create an HTTP-passive sticky method. ◦ **ID**—Enter the method ID. ◦ **Search position**—Select the position to obtain the string from the HTTP request. Options are **Header** and **Content**. ◦ **Header type**—Specify the type of string to obtain from the HTTP request. Options are **Name** and **URL**. This parameter is available only when the **Search position** is set to **Header**. ◦ **Header name**—Enter the HTTP header name, which is case insensitive. This parameter is available only when the **Header type** is set to **Name**. ◦ **Start string**—Specify the regular expression that marks the start of the HTTP header, URL, or HTTP entity. ◦ **Length/End string**—Specify the length and end string of the HTTP header, URL, or HTTP entity. 2. Click **OK**. The HTTP-passive sticky method appears in the request configuration list.
Response configuration	Enable the device to obtain the specified string from HTTP responses for generating HTTP-passive sticky entries. The HTTP-passive sticky method requires both the request and response configuration for generating sticky entries. To configure the response: 3. Click **Create** to create an HTTP-passive sticky method. ◦ **ID**—Enter the method ID. ◦ **Search position**—Select the location to obtain the string from the HTTP response. Options are **Header** and **Content**. ◦ **Header type**—Specify the type of string to obtain from the HTTP response. This parameter is available only when the **Search position** is set to **Header**. ◦ **Header name**—Enter the HTTP header name, which is case insensitive. This parameter is available only when the **Header type** is set to **Name**. ◦ **Start string**—Specify the regular expression that marks the start of

Item	Description
	the HTTP header or HTTP entity. ◦ **Length/End string**—Specify the length and end string of the HTTP header or HTTP entity. **Length** specifies the length of the HTTP header or HTTP entity. The value 0 indicates any length. **End string** specifies the regular expression that marks the end of the HTTP header or HTTP entity. The string cannot contain question marks (?). 4. Click **OK**. The HTTP-passive sticky method appears in the response configuration list.

Table 13 UDP-passive sticky method configuration items

Item	Description
Request configuration	Enable the device to obtain the specified string from UDP requests for matching UDP-passive sticky entries. The UDP-passive sticky method requires both the request and response configuration for generating sticky entries. When the device receives a UDP request, it obtains the specified payload based on the request configuration. If the payload matches the UDP response payload obtained using the response configuration, the device generates a sticky entry based on the payload in the response. For subsequent UDP request packets matching the sticky entry, the device forwards them according to the sticky entry. Select **UDP-Passive sticky method** to configure the following parameters: • **Offset**—Specify the offset value of the UDP payload based on the start of the UDP request packet. • **Start string**—Specify the regular expression that marks the start of the UDP payload. The string cannot contain question marks (?). • **Length/End string**—Specify the length and end string of the UDP payload. **Length** specifies the length of the UDP payload. The value 0 indicates any length. **End string** specifies the regular expression that marks the end of the UDP payload. The string cannot contain question marks (?).
Response configuration	Enable the device to obtain the specified string from UDP responses for generating UDP-passive sticky entries. The UDP-passive sticky method requires both the request and response

Item	Description
	configuration for generating sticky entries. Select **UDP-Passive sticky method** to configure the following parameters: • **Offset**—Specify the offset value of the UDP payload based on the start of the UDP response packet. • **Start string**—Specify the regular expression that marks the start of the UDP payload. The string cannot contain question marks (?). • **Length/End string**—Specify the length and end string of the UDP payload. **Length** specifies the length of the UDP payload. The value 0 indicates any length. **End string** specifies the regular expression that marks the end of the UDP payload. The string cannot contain question marks (?).

Table 14 TCP-payload sticky method configuration items

Item	Description
Offset	Specify the offset value of the TCP payload based on the start of the TCP packet.
Start string	Specify the regular expression that marks the start of the TCP payload. The string cannot contain question marks (?).
Length/End string	Specify the length and end string of the TCP payload. • **Length**—Specify the length of the TCP payload. The value 0 indicates any length. • **End string**—Specify the regular expression that marks the end of the TCP payload. The string cannot contain question marks (?).

4. Click **OK**. The new sticky group appears on the **Sticky Group** page.

Configure an SNAT address pool

After a server farm or a link group references an SNAT address pool, the LB device replaces the source address of packets it receives with an SNAT address before forwarding the packets.

Procedure

1. Select **Policies** > **Load Balancing** > **Common Configuration** > **SNAT Address Pools**.
2. Click **Create** on the **SNAT Address Pool** page.
3. Create an SNAT address pool.

Table 15 SNAT address pool configuration items

Item	Description
SNAT pool name	Enter a name for the SNAT address pool, case insensitive.
VRF	Specify the VPN instance to which the SNAT address pool belongs. When two address pools contain overlapping addresses, specify a VPN instance for each address pool to avoid configuration conflict on the device. For traffic forwarding based on the SNAT address pool, as a best practice, specify the VPN instance of the associated real server as the VPN instance of the SNAT address pool.
Address range list	To add an address range: 1. Click **Add**. ○ **Start IP address**—Enter the start IP address. ○ **End IP address**—Enter the end IP address, which cannot be smaller than the start IP address. 2. Click **OK**. The new address range appears in the

Item	Description
	address range list.
Interfaces for sending gratuitous ARP/ND packets	Specify the interfaces for sending gratuitous ARP packets and ND packets. If the IP address of an interface connected to a server is in the same network segment as the SNAT address pool, you must specify that interface as an interface for sending gratuitous ARP/ND packets.
Description	Enter a description for the SNAT address pool.

4. Click **OK**. The new SNAT address pool appears on the **SNAT Address Pool** page.

Configure proximity

The proximity feature performs link detection to select the optimal link to a destination. If no proximity information for a destination is available, the load balancing module selects a link based on the scheduling algorithm. It then performs proximity detection to generate proximity entries for forwarding subsequent traffic.

To use the proximity feature, configure the proximity probe template and proximity parameters, and then enable the proximity feature in a link group.

Procedure

1. Select **Policies** > **Load Balancing** > **Common Configuration** > **Proximity**.
2. Click **Create** on the **Proximity Parameter** page.
3. Create a proximity parameter.

Table 16 Proximity parameter configuration items

Item	Description
VRF	Specify the VPN instance to which proximity entries belong. You can select an existing VPN instance or create a VPN instance.
Default probe method	Specify the default probe method. You can select an existing probe method or create a probe method.
Mask length	Specify the mask length for IPv4 proximity entries. The value 0 indicates the natural mask.
Aging time	Set the timeout timer for proximity entries.
TTL weight	Set the TTL weight for proximity calculation. A larger value indicates a higher weight.
RTT weight	Set the network delay weight for proximity calculation. A larger value indicates a higher weight.
Cost weight	Set the cost weight for proximity calculation. A larger value indicates a higher cost weight.
Bandwidth weight	Set the bandwidth weights for proximity calculation. • **Inbound**—Set the inbound bandwidth weight for proximity calculation. A larger value indicates a higher bandwidth weight. • **Outbound**—Set the outbound bandwidth weight for proximity calculation. A larger value indicates a higher bandwidth weight.
Max entries	Set the maximum number of proximity entries. The value 0 indicates that the maximum number of proximity entries is not limited.
Packet loss ratio weight	Set the packet loss ratio weight for proximity calculation. This parameter specifies the weight of packet loss ratio in calculating the composite link cost. It applies only when you enable the proximity feature or configure the link quality algorithm. The proximity feature and the link quality algorithm configuration are mutually exclusive.

4. Click **OK**. The new proximity parameter appears on the **Proximity Parameter** page.
5. Click **Create** on the **Proximity Probe Template** page.
6. Create a proximity probe template.

Table 17 Proximity probe template configuration items

Item	Description
Probe template name	Enter a name for the probe template name, case insensitive.
Probe interval	Set the probe interval.
Timeout time	Set the timeout time for probe responses.

7. Click **OK**. The new proximity probe template appears on the **Proximity Probe Template** page.

Configure ISP information

Use the IP addresses assigned by ICANN to configure IP addresses for an ISP. When the destination IP address of packets matches the ISP match rule of an LB class, the LB device selects a link to forward the packets based on the link group configuration.

You can configure ISP information manually, by importing an ISP file, by auto update, or use the combination of these methods.

The system keeps the imported information intact when detecting the following problems:

- The file does not exist.
- The file name is invalid.
- File decryption fails.

If the system quits the import operation because of IP address parsing failure, the system performs the following operations:

- Clears the most recently imported information.
- Saves the information imported this time.

You cannot delete the imported ISP or its IPv4 or IPv6 address. If the manually configured and imported ISP information overlaps, you can delete the manually configured ISP information.

If you import multiple ISP files, the newly imported one overwrites the previously imported one.

Procedure

1. Select **Policies** > **Load Balancing** > **Common Configuration** > **ISP**.
2. Import an ISP file on the ISP page.
   a. Click **Select**, and select the file to be imported.
   b. Click **Import**. The imported file appears in the ISP list.
3. Manually configure ISP information.
   a. Click **Create**.

Table 18 Manual ISP configuration items

Item	Description
ISP name	Enter a name for the ISP, case insensitive.
Description	Enter a description for the ISP.

Item	Description
Whois maintainer object	Configure a whois maintainer object to identify an ISP. Enter a name for the whois maintainer object, and click **Add**. • **Object name**—Enter a name for the whois maintainer object, a string of 1 to 63 characters. A maximum of 10 whois maintainer objects can be configured for one ISP. • **Source**—The way a whois maintainer object is added. It can be **Manually configured**, **Imported from file**, and **Manually configured and Imported from file**.
ISP list	1. Click **Create** to configure an ISP address. ○ **Address type**—Select the address type: IPv4 or IPv6. ○ **IP address**—Enter an IPv4 address and mask length (1-32) or an IPv6 address and prefix length (1-128). 2. Click **OK**. The ISP address appears in the ISP list. ○ **Source**—The way an ISP address is obtained. It can be **Manually configured**, **Imported from file**, and **Auto update**.

b. Click **OK**. The ISP information appears in the ISP list.

4. Configure ISP auto update on the **Auto update** page.

a. Enable ISP auto update and configure ISP auto update parameters.

Table 19 Auto update configuration items

Item	Description
ISP auto update	Enable or disable ISP auto update.
Whois server	Specify the whois server from which the device queries ISP information. You can specify a whois server by specifying a domain name or IP address. • **Domain name**—Specify the domain name of the whois server, a case-insensitive, dot-separated string of 1 to 253 characters. Each dot-separated label in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-),

Item	Description
	underscores (_), and periods (.). • **IPv4 address**—Specify the IPv4 address of the whois server.
ISP update frequency	Specify the interval for ISP auto update. Options include **Per day**, **Per week**, and **Per month**. The specific update time is 4:02:00 a.m.
Last successfully updated	Time of the most recent successful update.
Last updated	Time of the most recent update.
Updated ISPs	Number of ISP addresses in the most recent update.
Update result	Result of the most recent update. Values include **Success**, **Connection error**, **Connection abort**, **DNS error**, and **No update**.

b. Click **Apply** to save and apply the configuration.

Configure a region

A region contains network segments corresponding to different ISPs.

Procedure

1. Select **Policies** > **Load Balancing** > **Common Configuration** > **Regions**.
2. Click **Create** on the **Region** page.
3. Create a region.

Table 20 Region configuration items

Item	Description
Region name	Enter a name for the region, case insensitive.
ISP	Add an ISP. 1. Select an existing ISP or create an ISP. 2. Click **Add**. The added ISP appears in the box below the text box.

4. Click **OK**. The new region appears on the **Region** page.

Advanced configuration

You can configure the aging time for DNS cache entries. The DNS cache entries can be viewed from **Monitor** > **DNS Cache**.

Server load balancing

This help contains the following topics:

Introduction

Server load balancing is a cluster technology that distributes services among multiple servers or firewalls.

Server load balancing is classified into Layer 4 server load balancing and Layer 7 server load balancing.

- **Layer 4 server load balancing**—Identifies network layer and transport layer information, and is implemented based on streams. It distributes packets in the same stream to the same server. Layer 4 server load balancing cannot distribute Layer 7 services based on contents.
- **Layer 7 server load balancing**—Identifies network layer, transport layer, and application layer information, and is implemented based on contents. It analyzes packet contents, distributes packets one by one based on the contents, and distributes connections to the specified server according to the predefined policies. Layer 7 server load balancing applies load balancing services to a large scope.

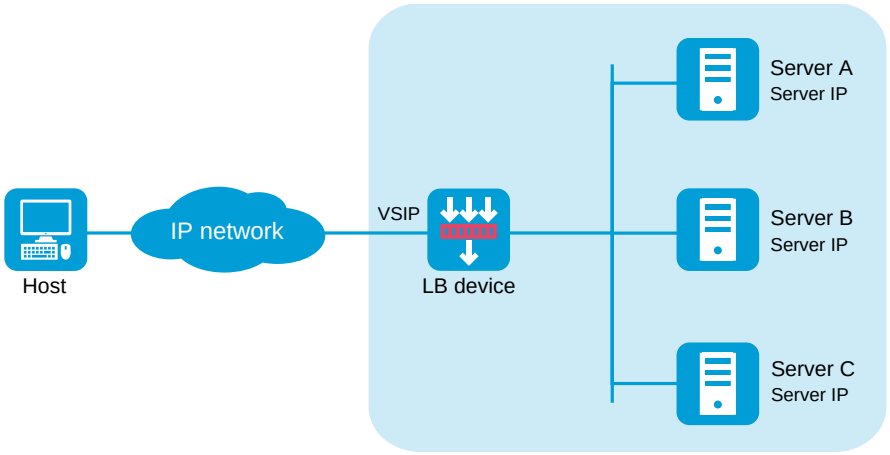
Server load balancing supports IPv4 and IPv6, but Layer 4 server load balancing does not support IPv4-to-IPv6 or IPv6-to-IPv4 translation.

Deployment modes

Server load balancing uses the Network Address Translation (NAT) and indirect deployment modes.

NAT-mode server load balancing

Figure 1 Network diagram

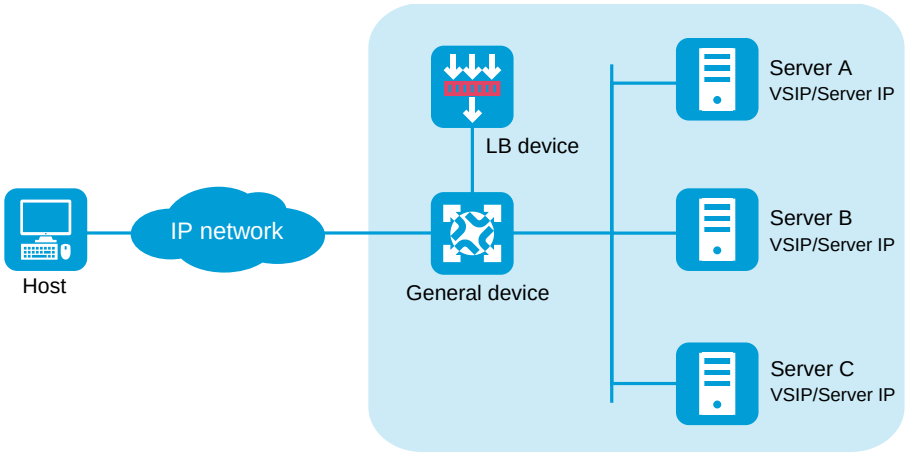


As shown in Figure 1, NAT-mode server load balancing contains the following elements:

- **LB device**—Distributes different service requests to multiple servers.
- **Server**—Responds to and processes different service requests.
- **VSIP**—Virtual service IP address of the cluster, used for users to request services.
- **Server IP**—IP address of a server, used by the LB device to distribute requests.

Indirect-mode server load balancing

Figure 2 Network diagram



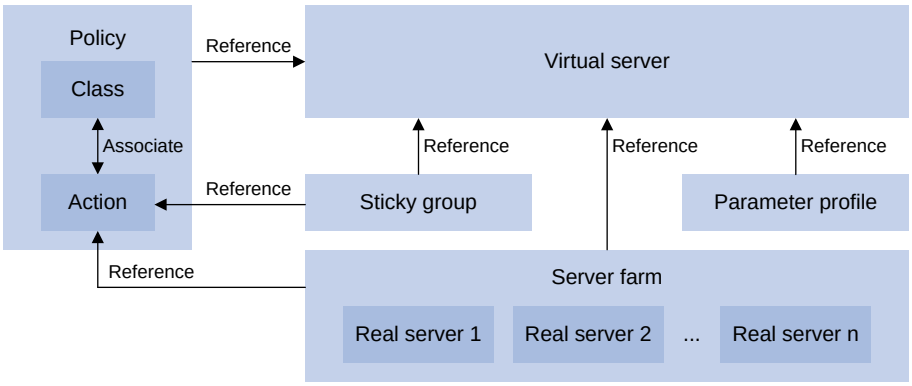
As shown in Figure 2, indirect-mode server load balancing contains the following elements:

- **LB device**—Distributes different service requests to multiple servers.
- **General device**—Forwards data according to general forwarding rules.
- **Server**—Responds to and processes different service requests.
- **VSIP**—Virtual service IP address of the cluster, used for users to request services.
- **Server IP**—IP address of a server, used by the LB device to distribute requests.

Indirect-mode server load balancing requires configuring the VSIP on both the LB device and the servers. Because the VSIP on a server cannot be contained in an ARP request and response, you can configure the VSIP on a loopback interface.

Relationship between the main configuration items

Figure 3 Relationship between the main configuration items

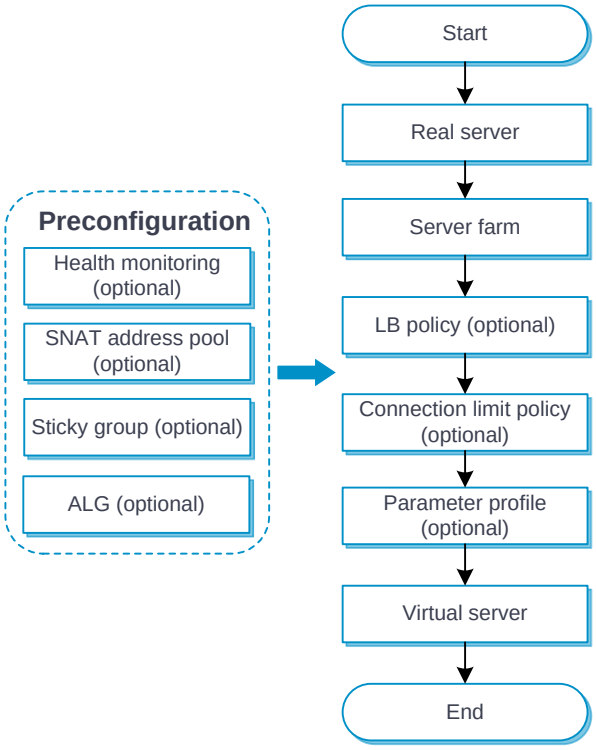


Configure server load balancing

Before configuring server load balancing, install a license correctly. For more information, see the license management help.

Configure server load balancing as shown in Figure 4.

Figure 4 Server load balancing configuration procedure



Configure health monitoring (optional)

A health monitoring probe template can be used by a real server or server farm.

For more information about configuring health monitoring, see the health monitoring help.

For more information about configuring health monitoring, see the help for load balancing common configuration.

Configure an SNAT address pool (optional)

An SNAT address pool can be used by a server farm.

For more information about configuring an SNAT address pool, see the help for load balancing common configuration.

Configure ALG (optional)

For more information about configuring ALG, see the help for load balancing common configuration.

Configure a server farm

You can add real servers that contain similar content to a server farm to facilitate management. A server farm can be used by a virtual server or an action.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Server Farms**.
2. Click **Create**.
3. Create a server farm.

Table 1 Basic configuration items

Item	Description
Server farm name	Enter a name for the server farm, case insensitive.
Scheduling algorithm	Select a scheduling algorithm for the server farm. • **Round robin**—Assigns user requests to real servers based on the weights of real servers. A higher weight indicates more user requests will be assigned.

Item	Description
	• **Random**—Randomly assigns user requests to real servers. • **Weighted least connections**—Always assigns user requests to the real server with the fewest number of weighted active connections (the number of active connections divided by weight). The weight used by this algorithm is configured on the **Create Real Server** page. • **Bandwidth**—Distributes user requests to real servers according to the weights and remaining bandwidth of real servers. • **Maximum bandwidth**—Distributes user requests always to an idle real server that has the largest remaining bandwidth. • **Dynamic feedback**—Assigns new connections to real servers based on load weight values calculated by using the memory, CPU, and disk usage of the real servers. The less the load, the greater the weight value. A real server with a greater weight value is assigned more connections. • **Least time**—Assigns new connections to real servers based on load weight values calculated by using the response time of the real servers. The shorter the response time, the greater the weight value. A real server with a greater weight value is assigned more connections. • **Source IP address hash**—Hashes the source IP address of user requests and distributes user requests to different real servers according to the hash values. • **Source IP address CARP hash**—Hashes the source IP address of user requests and distributes user requests to different real servers according to the CARP hash values. • **Source IP address and port number hash**—Hashes the source IP address and port number of user requests and distributes user requests to different real servers according to the hash values. • **Source IP address and port number CARP hash**—Hashes the source IP address and port number of user requests and distributes user requests to different real servers according to the CARP hash values. • **Destination IP address hash**—Hashes the destination IP address of user requests and distributes user requests to different real servers according to the hash values. • **Destination IP address CARP hash**—Hashes the destination IP address of user requests and distributes user requests to different real servers according to the CARP hash values. • **HTTP hash**—Hashes the content of user requests and distributes user requests to different real servers according to the hash values. This scheduling algorithm takes effect only for an HTTP

Item	Description
	virtual server. • **HTTP CARP hash**—Hashes the content of user requests and distributes user requests to different real servers according to the CARP hash values. This scheduling algorithm takes effect only for an HTTP virtual server. • **Weighted least connections (member)**—Always assigns user requests to the real server with the fewest number of weighted active connections (the number of active connections divided by weight). The weight used by this algorithm is configured on the **Real Server** page. • **Least time (member)**—Always assigns user requests to real servers based on load weight values calculated by using the response time of the real servers. The shorter the response time, the greater the weight value. A real server with a greater weight value is assigned more connections. By default, the source IP address hash algorithm is used.
Offset	Specify the offset value based on the start of the HTTP content. This parameter is supported only when the scheduling algorithm is HTTP hash or HTTP CARP hash.
Start string	Specify the regular expression that marks the start of the HTTP content, a string starting from the offset value. The string cannot contain question marks (?). This parameter is supported only when the scheduling algorithm is HTTP hash or HTTP CARP hash.
Length/End string	• **Length** specifies the length of the HTTP content. • **End string** specifies the regular expression that marks the end of the HTTP content, a string starting from the start string value. The string cannot contain question marks (?). This parameter is supported only when the scheduling algorithm is HTTP hash or HTTP CARP hash.
Priority scheduling	Specify the upper limit and lower limit of real servers in a server farm that can be scheduled. By default, all real servers with the highest priority in a server farm are scheduled. • If the number of real servers with the highest priority is greater than the configured maximum number, the maximum number applies. • If the number of such real servers is less than the minimum number, real servers with lower priority are selected to meet the

Item	Description
	minimum number or until no real servers are available. The real server priority can be configured on the **Real Servers** page.
Real server	You can add a real server to a server farm in one of the following ways: Create a real server and add it to the server farm. 1. Click **Add**, and select **Create real server**. 2. Configure the parameters for the real server (see "Configure a real server"). 3. Click **OK**. The new real server appears in the real server list. Select an existing real server. 4. Click **Add**, and select **Add existing real server**. 5. Select a real server from the list, and configure real server parameters (see "Configure a real server"). 6. Click **OK**. The real server appears in the real server list.
Probe method	Specify a probe template used by the server farm to detect the health and availability of its real servers. You can also configure this parameter for a single real server on the **Real Servers** page. The configuration performed on the **Real Servers** page has higher priority over that performed on the **Server Farms** page. You can select an existing probe template or create a probe template. To create a probe template: 1. Click **Add**. o Template name: Enter a name for the probe template. o Use template's port number for detection: If you select this option, the destination port number specified in the template is used for detection. If you do not select this option, the real server's port number is used for detection. 2. Click **OK**. The new probe template appears on the **Health Monitoring** page.
Description	Enter a description for the server farm.

Table 2 Advanced configuration items

Item	Description
Success criteria	Specify the health monitoring success criteria for the real server. • All probes succeed: Health monitoring succeeds only when all the specified health monitoring methods succeed. • At least n probes succeed: Health monitoring succeeds when a minimum of the specified number of health monitoring methods succeed. When the specified number of health monitoring methods is greater than the number of health monitoring methods on the device, health monitoring succeeds if all health monitoring methods succeed.
SNAT mode	Specify an SNAT mode for the server farm. • SNAT pool: Translates the source IP address into an IP address in the specified SNAT address pool. • Auto mapping: Translates the source IP address into the IP address of the interface connecting to the real servers. • TCP option: Translates the source IP address into the IP address carried in the TCP option field of packets. If SNAT is not configured for a server farm, the server farm uses global SNAT policies for address translation.
SNAT pool name	Select an existing SNAT pool or create an SNAT pool for the server farm. This parameter is supported only when the SNAT mode is SNAT pool.
NAT	Disable NAT for the server farm in indirect-mode NAT configuration, or enable NAT for the server farm in NAT-mode configuration.
RST packet monitoring	Select an existing RST probe template or create an RST probe template for the server farm.
Zero-window packet monitoring	Select an existing zero-window probe template or create a zero-window probe template for the server farm.
HTTP passive probe	Select an existing HTTP passive probe template or create an HTTP passive probe template for the server farm.
Custom monitoring	Select an existing custom probe template or create a custom probe

Item	Description
	template for the server farm.
Auto recovery	Enable or disable auto recovery. This function enables automatic recovery for real servers shut down by intelligent probe templates when the auto recovery timer expires. If health monitoring is not configured, a real server is recovered to the unknown state. If health monitoring is configured and succeeds, a real server is recovered to the available state. If health monitoring fails, a real server is recovered to the health-monitoring-failed state. This function is available only when an HTTP passive, RST, or zero-window probe template is specified for a server farm.
Recovery time	Enter the auto recovery time. The value 0 means that real servers cannot automatically recover. This parameter is available only when auto recovery is enabled.
Fault processing method	Specify the fault processing method for the real server. • **Keep existing connections**—Keeps the connection with the failed real server. Keeping or terminating the connection depends on the timeout mechanism of the protocol. • **Redirect connections**—Redirects the connection to another available real server in the server farm. • **Terminate existing connections**—Terminates the connection with the failed real server by sending RST packets (for TCP packets) or ICMP unreachable packets (for other types of packets).
Slow online	The real servers newly added to a server farm might not be able to immediately process large numbers of services assigned by the LB device. To resolve this issue, enable the slow online feature for the server farm. The feature uses the standby timer and ramp-up timer. When the real servers are brought online, the LB device does not assign any services to the real servers until the standby timer expires. When the standby timer expires, the ramp-up timer starts. During the ramp-up time, the LB device increases the service amount according to the processing capability of the real servers, until the ramp-up timer expires. • Standby time: The value range is 0 to 600 seconds. • Ramp-up time: The value range is 3 to 600 seconds.

Item	Description

Action upon busyness	Specify the action to take when the server farm is busy. A server farm is considered busy when all its real servers are busy. You can configure one of the following actions:
	• **Schedule**—Forcibly assigns client requests to all real servers in the server farm.
	• **Queue and wait**—Stops assigning client requests to a server farm and assigns new client requests to a wait queue.
	  ◦ **Queue length**: New client requests will be dropped when the queue length exceeds the configured length.
	  ◦ **Timeout time**: Client requests already in the queue will be aged out when the configured timeout time expires.
	• **Render scheduling failed**—Stops assigning client requests to a server farm. If the LB policy for the server farm contains the action of matching the next rule, the device compares client requests with the next rule. Otherwise, the device drops the client requests.
	The device determines whether a real server is busy based on the following factors:
	• Maximum number of connections.
	• Maximum number of connections per second.
	• Maximum number of HTTP requests per second.
	• Maximum bandwidth, maximum inbound bandwidth, and maximum outbound bandwidth.
	• SNMP-DCA probe result.

Availability criteria	Set the criteria (lower percentage and upper percentage) to determine whether a server farm is available. This helps implement traffic switchover between the master and backup server farms. • **Lower percentage**—When the number of available real servers to the total number of real servers in the primary server farm is smaller than the lower percentage, traffic is switched to the backup server farm. • **Upper percentage**—When the number of available real servers to the total number of real servers in the primary server farm is greater than the upper percentage, traffic is switched back to the master server farm.
Action when all server farm members are	Specify an action to take when all server farm members are unavailable:

Item	Description
unavailable	• **Drop**. • **Forward**—Forwards requests to the most recently selected server farm member.

4. Click **OK**. The new server farm appears on the **Server Farm** page.

Configure a real server

A real server is an entity on the LB device to process user services. A real server can belong to multiple server farms. A server farm can have multiple real servers.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Real Servers**.
2. Click **Create**.
3. Create a real server.

Table 3 Basic configuration items

Item	Description
Real server name	Enter a name for the real server, case insensitive.
IPv4 address	Specify an IPv4 address for the real server. The IPv4 address cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.
IPv6 address	Specify an IPv6 address for the real server. The IPv6 address cannot be a loopback address, multicast address,

Item	Description
	link-local address, or all-zero address.
Port number	Specify the port number for the real server. If the port number is 0, packets use their respective port numbers.
VPN instance	Specify a VPN instance for the real server.
VPN instance inheritance	Enable or disable VPN instance inheritance. When VPN instance inheritance is enabled, a real server without a VPN instance specified inherits the VPN instance of its virtual server.
Probe logging	Enable or disable logging for health monitoring. This feature logs heath status changes of the real server.
Real server feature	Enable or disable the real server feature.
Description	Enter a description for the real server.

Table 4 Advanced configuration items

Item	Description
Weight	Enter the weight for the real server. For the weighted round robin algorithm and weighted least connections algorithm, a greater value means a higher priority to be selected.
Priority	Enter a priority for the real server in the server farm. A greater value means a higher priority to be selected. If the number of real servers with the highest priority is smaller than the configured minimum number, real servers with lower priority are selected to meet the minimum number. You can configure the maximum number and minimum number on the **Server Farms** page.
Server farm	Select an existing server farm or create a server farm for the real server.

Item	Description

Probe-Probe method	Specify a probe template used by the real server to detect the health and availability. You can also configure this parameter for a server farm on the **Server Farms** page. The configuration performed on the **Real Servers** page has higher priority over that performed on the **Server Farms** page.
	
	You can select an existing probe template or create a probe template
	
	To create a probe template:
	
	3. Click **Add**.
	  ◦ Template name: Enter a name for the probe template.
	  ◦ Use template's port number for detection: If you select this option, the destination port number specified in the template is used for detection. If you do not select this option, the real server's port number is used for detection.
	
	4. Click **OK**. The new probe template appears on the **Health Monitoring** page.

Probe-Success criteria	Specify the health monitoring success criteria for the real server. • All probes succeed: Health monitoring succeeds only when all the specified health monitoring methods succeed. • At least n probes succeed: Health monitoring succeeds when a minimum of the specified number of health monitoring methods succeed. When the specified number of health monitoring methods is greater than the number of health monitoring methods on the device, health monitoring succeeds if all health monitoring methods succeed.
Custom monitoring	Select an existing custom probe template or create a custom probe template for the real server.

Variables	Configure a variable for a server farm member.
	
	To configure a variable:
	
	1. Click **Add**.
	  ◦ Name: Enter a variable name, case-sensitive.
	  ◦ Value: Enter a variable value, case-sensitive.
	
	2. Click **OK**. The new variable appears in the **Variables** list.
	
	This variable is used to rewrite the TCP payload in a general LB action. The specific content in the TCP payload will be replaced with the variable value associated with a server farm member. For

Item	Description
	example, if you configure a variable with name **var1** and value **_1** and configure an action of rewriting **QMGR.S01** as **QMGR.S01%[var1]**, the **QMGR.S01** string in the TCP payload is rewritten as **QMGR.S01_1**.
QoS-Max connections	Specify the maximum number of connections for the real server. 0 means not limited.
QoS-Max connections per second	Specify the maximum number of connections per second for the real server. 0 means not limited.
QoS-HTTP requests per second	Specify the maximum number of HTTP requests per second for the real server. 0 means not limited.
QoS-Total max bandwidth	Specify the maximum bandwidth for the real server. 0 means not limited.
QoS-Max inbound bandwidth	Specify the maximum inbound bandwidth for the real server. 0 means not limited.
QoS-Max outbound bandwidth	Specify the maximum outbound bandwidth for the real server. 0 means not limited.

4. Click **OK**. The new real server appears on the **Real Server** page.

Configure a sticky group (optional)

A sticky group can be used by a virtual server or an action.

For more information about configuring a sticky group, see the help for load balancing common configuration.

Configure an LB policy (optional)

An LB policy associates a class with an action to guide packet forwarding. In an LB policy, you can configure an action for packets matching the specified class, and configure the default action for packets matching no class.

You can specify multiple classes for an LB policy. Packets match the classes in the order the classes are configured. If a class is matched, the specified action is taken. If no class is matched, the default action is taken.

An LB policy can be used by a virtual server.

Configure a class

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Class**.
2. Click **Create**.
3. Create a class.

Table 5 Class configuration items

Item	Description
Class name	Enter a name for the class, case insensitive.
Type	Specify the type for the class. • Generic: Applies to Layer 4 server load balancing. • HTTP: Applies to Layer 7 server load balancing. • RADIUS: Applies to Layer 7 server load balancing. • MySQL: Applies to Layer 7 server load balancing.

Item	Description
Match type	Specify the match type for the class. • Match any: Requires matching any rule of the LB class. • Match all: Requires matching all rules of the LB class.
Match rule	A class classifies packets by comparing packets with specific rules. Matching packets are further processed by actions. You can create a maximum of 65535 rules for a class. 1. Click **Create** to create a match rule. o Rule ID: Specify the rule ID. Rules are matched in ascending order of rule IDs. o Type: Specify the rule type. The rule types include source IPv4 address, source IPv6 address, class, IPv4 ACL, IPv6 ACL, cookie, HTTP header, method, URL, content, user, RADIUS attribute, input interface, HTTP version, ISP, TCP payload, and MySQL. o IPv4 address: Specify an IPv4 address. This parameter is available only when the rule type is source IPv4 address. o Mask length: Specify a mask length. This parameter is available only when the rule type is source IPv4 address. o IPv6 address: Specify an IPv6 address. This parameter is available only when the rule type is source IPv6 address. o Prefix length: Specify a prefix length. This parameter is available only when the rule type is source IPv6 address. o Class: Specify a class. This parameter is available only when the rule type is class. o ACL: Specify an ACL. You can select an existing ACL or create an ACL. This parameter is available only when the rule type is IPv4 ACL or IPv6 ACL. o Cookie name: Specify the cookie name for HTTP packets. The cookie name is a case-sensitive string excluding spaces, horizontal tabs, ASCII characters smaller than or equal to 31, ASCII characters greater than or equal to 127, or the following characters: ( ) < > @ , ; : \ " / [ ] ? = { }. This parameter is available only when the rule type is cookie. o Cookie value: Specify the cookie value regular expression. The string cannot contain question marks (?). This parameter is available only when the rule type is cookie. o Header name: Specify the header name for HTTP packets. The header name is a case-insensitive string excluding

Item	Description
	spaces, horizontal tabs, ASCII characters smaller than or equal to 31, ASCII characters greater than or equal to 127, or the following characters: ( ) < > @ , ; : \ " / [ ] ? = { }. This parameter is available only when the rule type is HTTP header. ◦ Header value: Specify the header value regular expression. The string cannot contain question marks (?). This parameter is available only when the rule type is HTTP header. ◦ Extension type: The extension type can be **Predefined** or **Custom**. This parameter is available only when the rule type is method. ◦ Method: The predefined methods include GET, CONNECT, DELETE, HEAD, OPTIONS, POST, PUT, and TRACE. The custom method is a case-sensitive string excluding spaces, horizontal tabs, ASCII characters smaller than or equal to 31, ASCII characters greater than or equal to 127, or the following characters: ( ) < > @ , ; : \ " / [ ] ? = { }. This parameter is available only when the rule type is method. ◦ URL: Specify the URL regular expression. The string cannot contain question marks (?). This parameter is available only when the rule type is URL. ◦ Content offset: Specify the offset value of the HTTP entity based on the start of the HTTP packet. This parameter is available only when the rule type is content. ◦ Content value: Specify the HTTP entity regular expression. The string cannot contain question marks (?). This parameter is available only when the rule type is content. ◦ User: Select an existing user or user group in an identity domain, or create a user or user group. This parameter is available only when the rule type is user. ◦ Attribute type: Enter an attribute type value. This parameter is available only when the rule type is RADIUS attribute. ◦ Attribute value: Specify the RADIUS attribute regular expression. This parameter is available only when the rule type is RADIUS attribute. ◦ Input interface: Specify an input interface. This parameter is available only when the rule type is input interface. ◦ HTTP version: Specify an HTTP version. This parameter is available only when the rule type is HTTP version. ◦ ISP: Select an existing ISP, or create an ISP. This parameter is available only when the rule type is ISP. ◦ TCP payload: Enter a regular expression used to match TCP

Item	Description
	payloads. This parameter is available only when the rule type is TCP payload. ○ Case insensitivity: Enable case insensitivity for matching. This parameter is available only when the rule type is TCP payload or MySQL. ○ Negate the match rule: If this option is not selected, an LB action is taken when TCP packets match the regular expression. If this option is selected, an LB action is taken when TCP packets do not match the regular expression. This parameter is available only when the rule type is TCP payload or MySQL. ○ Regular expression: Enter a regular expression used to match MySQL statements. This parameter is available only when the rule type is MySQL. 2. Click **OK**.
Description	Enter a description for the class.

4. Click **OK**. The new class appears on the **Class** page.

Configure an action

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Action**.
2. Click **Create**.
3. Create an action.

Table 6 Basic configuration items

Item	Description
Action name	Enter a name for the action, case insensitive.

Item	Description
Type	Specify an action type. • Generic • HTTP • HTTP redirection • RADIUS
Forwarding mode	Specify a forwarding mode: • Load balance • Drop • Forward (supported by generic type and RADIUS type only) • Respond by using a file (supported by HTTP type only)
Uncompressed file	If the URL path in a client request matches the specified URL path, the device responds to the request by using an uncompressed file. 3. Click **Create** to create an uncompressed response file. o URL path: Specifies the URL path used to match HTTP requests, a case-sensitive string. The specified URL path must start with a forward slash (/). o Uncompressed file: Specifies an uncompressed file by its absolute path plus a file name, which is case insensitive, for example, flash:/file.html. Only one uncompressed file can be used for a URL, and one uncompressed file can be used for multiple URLs. 4. Click **OK**. This parameter is available only when the forwarding mode is **Respond by using a file**.
Compressed file	If the URL path in a client request matches the specified working path plus a relative path in the zip file, the device responds to the request by using the file in the zip file. For example, if you configure the working path as **/index** and compressed file as **flash:/za/zb/test.zip**, and a relative path **/css/col.css** exists in **test.zip**, the matching URL is **/index/css/col.css** and the response file is **col.css**. • Working path: Specify a working path plus a relative path in the zip file to match the URL in HTTP requests, a case-sensitive string. The working path must start with a

Item	Description
	forward slash. • Compressed file: Specify a compressed file by its absolute path plus a file name, which is case insensitive. The file must be a zip file, for example, flash:/file.zip. This parameter is available only when the forwarding mode is **Respond by using a file**.
Fallback action	Specify a fallback action. • Match next rule: Matches the next rule upon failure to find an available real server. • Respond by using another file: Responds to client requests with the specified default response file upon failure to find an available real server. ◦ Default response file: Specifies an uncompressed file by its absolute path plus a file name, which is case insensitive, for example, flash:/file.html. • Fin close: Sends FIN packets to close the TCP connection. • Rst close: Sends RST packets to close the TCP connection. This parameter is available only when the forwarding mode is **Load balance**.
Action taken upon failure to find the response file	Specify an action taken upon failure to find the response file. • Match next rule: Matches the next rule upon failure to find a response file. • Respond by using a file: Responds to client requests with the specified default response file upon failure to find a response file. ◦ Default response file: Specifies an uncompressed file by its absolute path plus a file name, which is case insensitive, for example, flash:/file.html. • Fin close: Sends FIN packets to close the TCP connection. • Rst close: Sends RST packets to close the TCP connection. This parameter is available only when the forwarding mode is **Respond by using a file**.
TCP connection close mode	Specify a TCP connection close mode. • By sending FIN: Sends FIN packets to close the TCP

Item	Description
	connection. • By sending RST: Sends RST packets to close the TCP connection. This parameter is available only when the forwarding mode is **Drop**.
ToS	Set the ToS field value of IP packets sent to the server.
Description	Enter a description for the action.
Server farms-Primary server farm	Select an existing server farm or create a server farm as the primary server farm. When the primary server farm is available (contains real servers), packets are forwarded through the primary server farm. When the primary server farm is not available, packets are forwarded through the backup server farm. This parameter is available only when the forwarding mode is **Load balance**.
Server farms-Backup server farm	Select an existing server farm or create a server farm as the backup server farm. This parameter is available only when the forwarding mode is **Load balance**.
Server farms-Sticky group	Select an existing sticky group or create a sticky group. This parameter is available only when the forwarding mode is **Load balance**.
HTTP redirection configuration-Redirection URL	This setting redirects all HTTP request packets matching an action to the specified URL. Specify a redirection URL, a case-sensitive string. You can also specify the question mark (?) or the following character strings as the redirection URL: • %h: Specifies the host name in the client request packet. • %p: Specifies the URL in the client request packet. • %%: Specifies the percentage sign (%). This parameter is available only when the action type is HTTP redirection.

Item	Description
HTTP redirection configuration -Redirection mode	Specify a redirection mode. • Temporary • Permanent This parameter is available only when the action type is HTTP redirection.

Table 7 Advanced configuration items (available only when the action type is HTTP and the forwarding mode is Load balance or Respond by using a file)

Item	Description
TCP payload rewrite	1. Click **Create**. ◦ Direction: Specify the direction, which can be **Both**, **Request**, or **Response**. ◦ Content before rewrite: TCP message body to rewrite, a case-sensitive regular expression string. ◦ Content after rewrite: TCP message body after rewrite. You can also specify the following replacement strings: ◦ **%[***variable***]**—Replaces the specified value with the variable associated with the server farm member. The *variable* is the variable name. ◦ **%[1-9]**—Replaces the specified value with the content in the corresponding parentheses. For example, if you configure the content before rewrite as **(Wel)(co)(me)** and the content after rewrite as **%2**, the string **Welcome** will be replaced with **co** in the second pair of parentheses. 2. Click **OK**. This parameter is supported only in a generic LB action. Only TCP virtual servers operating at Layer 7 support an LB policy containing the TCP payload rewrite configuration.
Insert X-Forwarded-For	Insert the X-Forwarded-For header.

Item	Description
Response content rewrite-Content before rewrite	Specify the HTTP packet content to be rewritten.
Response content rewrite-Content after rewrite	Specify the HTTP packet content after rewrite. • %is: Source IPv4 or IPv6 address. • %ps: Source port number. • %id: Destination IPv4 or IPv6 address. • %pd: Destination port number. • %%: Percentage sign (%). • %[1-9] : Header value enclosed in parenthesis.

Header deletion	1. Click **Create**.
	  ◦ Direction: Specify the direction, which can be **Both**, **Request**, or **Response**.
	  ◦ Header name: Specify the header name, which is case insensitive and can be predefined or customized. It cannot contain spaces, horizontal tabs, ASCII characters less than or equal to 31, ASCII characters greater than or equal to 127, or the following characters: ( ) < > @ , ; : \ " / [ ] ? = { }.
	2. Click **OK**.

Header insertion	1. Click **Create**.
	  ◦ Direction: Specify the direction of HTTP packets, which can be **Both**, **Request**, or **Response**.
	  ◦ Header name: Specify the header name, which is case insensitive and can be predefined or customized. It cannot contain spaces, horizontal tabs, ASCII characters less than or equal to 31, ASCII characters greater than or equal to 127, or the following characters: ( ) < > @ , ; : \ " / [ ] ? = { }.
	  ◦ Header value: Specify the header content to be inserted to the HTTP packet. The string cannot contain question marks (?). You can also specify the following replacement strings:
	  ◦ %is: Source IP address in HTTP requests.
	  ◦ %ps: Source port number in HTTP requests.
	  ◦ %id: Destination IP address in HTTP requests.

Item	Description
	◦ %pd: Destination port number in HTTP requests. ◦ %sps: Source port number in HTTP responses. ◦ %spd: Destination port number in HTTP responses. ◦ %sis: Source IP address in HTTP responses. ◦ %sid: Destination IP address in HTTP responses. ◦ %{x509v}: Certificate version. ◦ %{x509snum}: Certificate serial number. ◦ %{x509sigalgo}: Certificate signature algorithm. ◦ %{x509issuer}: Certificate issuer. ◦ %{x509before}: Certificate effective time. ◦ %{x509after}: Certificate expiration time. ◦ %{x509sub}: Certificate subject. ◦ %{x509spktype}: Public key type for the certificate subject. ◦ %{x509spk}: Public key for the certificate subject. ◦ %{x509spkRSA}: Length of the RSA public key for the certificate subject (available only for an RSA public key). ◦ %{x509hash}: MD5 hash value of the client certificate. ◦ %{dncn}: Issuee. ◦ %{dne}: Email. ◦ %{dno}: Company/Organization. ◦ %{dnou}: Department. ◦ %{dnc}: Country. ◦ %{dns}: State/Province. ◦ %{dnl}: City. ◦ Encoding method: Specify an encoding method for replacement strings, which can be **Not encoded**, **URL**, or **Base64**. URL encoding encodes only spaces and the following special characters in replacement strings ; / ? : @ & = + $ | { } , \ ^ [ ] ` < > # %. Base64 encoding encodes entire replacement strings. 2. Click **OK**.

Item	Description
Header rewrite	1. Click **Create**. ◦ Direction: Specify the direction of HTTP packets, which can be **Both**, **Request**, or **Response**. ◦ Header name: Specify the header name, which is case insensitive and can be predefined or customized. It cannot contain spaces, horizontal tabs, ASCII characters less than or equal to 31, ASCII characters greater than or equal to 127, or the following characters: ( ) < > @ , ; : \ " / [ ] ? = { }. ◦ Header value: Specify the header content after rewrite. The string cannot contain question marks (?). You can also specify the following replacement strings: ◦ %is: Source IP address in HTTP requests. ◦ %ps: Source port number in HTTP requests. ◦ %id: Destination IP address in HTTP requests. ◦ %pd: Destination port number in HTTP requests. ◦ %sps: Source port number in HTTP responses. ◦ %spd: Destination port number in HTTP responses. ◦ %sis: Source IP address in HTTP responses. ◦ %sid: Destination IP address in HTTP responses. ◦ %1-9: Specified string used for replacement. A maximum of nine items are supported. ◦ %{x509v}: Certificate version. ◦ %{x509snum}: Certificate serial number. ◦ %{x509sigalgo}: Certificate signature algorithm. ◦ %{x509issuer}: Certificate issuer. ◦ %{x509before}: Certificate effective time. ◦ %{x509after}: Certificate expiration time. ◦ %{x509sub}: Certificate subject. ◦ %{x509spktype}: Public key type for the certificate subject. ◦ %{x509spk}: Public key for the certificate subject. ◦ %{x509spkRSA}: Length of the RSA public key for the certificate subject (available only for an RSA public key).

Item	Description
	○ %{x509hash}: MD5 hash value of the client certificate. ○ %{dncn}: Issuee. ○ %{dne}: Email. ○ %{dno}: Company/Organization. ○ %{dnou}: Department. ○ %{dnc}: Country. ○ %{dns}: State/Province. ○ %{dnl}: City. ○ Encoding method: Specify an encoding method for replacement strings, which can be **Not encoded**, **URL**, or **Base64**. URL encoding encodes only spaces and the following special characters in replacement strings ; / ? : @ & = + $ | { } , \ ^ [ ] ` < > # %. Base64 encoding encodes entire replacement strings. 2. Click **OK**.
URL rewrite	1. Click **Create**. ○ URL to be rewritten: The URL content cannot contain question marks (?). ○ URL after rewrite: Specify the URL content after rewrite. You can also specify the following replacement strings: ○ %is: Source IP address in HTTP requests. ○ %ps: Source port number in HTTP requests. ○ %id: Destination IP address in HTTP requests. ○ %pd: Destination port number in HTTP requests. ○ %sps: Source port number in HTTP responses. ○ %spd: Destination port number in HTTP responses. ○ %sis: Source IP address in HTTP responses. ○ %sid: Destination IP address in HTTP responses. ○ %1-9: Specified string used for replacement. A maximum of nine items are supported. ○ %{x509v}: Certificate version. ○ %{x509snum}: Certificate serial number.

Item	Description
	◦ %{x509sigalgo}: Certificate signature algorithm. ◦ %{x509issuer}: Certificate issuer. ◦ %{x509before}: Certificate effective time. ◦ %{x509after}: Certificate expiration time. ◦ %{x509sub}: Certificate subject. ◦ %{x509spktype}: Public key type for the certificate subject. ◦ %{x509spk}: Public key for the certificate subject. ◦ %{x509spkRSA}: Length of the RSA public key for the certificate subject (available only for an RSA public key). ◦ %{x509hash}: MD5 hash value of the client certificate. ◦ %{dncn}: Issuee. ◦ %{dne}: Email. ◦ %{dno}: Company/Organization. ◦ %{dnou}: Department. ◦ %{dnc}: Country. ◦ %{dns}: State/Province. ◦ %{dnl}: City. ◦ Encoding method: Specify an encoding method for replacement strings, which can be **Not encoded**, **URL**, or **Base64**. URL encoding encodes only spaces and the following special characters in replacement strings ; / ? : @ & = + $ | { } , \ ^ [ ] ` < > # %. Base64 encoding encodes entire replacement strings. 2. Click **OK**.
SSL security-SSL client policy	Select an existing SSL client policy or create an SSL client policy.
SSL security-SSL redirection URL list	1. Click **Create**. ◦ URL: Specify the Location header URL regular expression. ◦ HTTP port: Specify the HTTP port number to be rewritten. ◦ SSL port: Specify the SSL port number after rewrite. 2. Click **OK**.

4. Click **OK**. The new action appears on the **Action** page.

Configure an LB policy

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Load Balancing Policy**.
2. Click **Create**.
3. Create an LB policy.

Table 8 LB policy configuration items

Item	Description
Name	Enter a name for the LB policy, case insensitive.
Type	Specify the type for the LB policy. • Generic: Applies to Layer 4 server load balancing. • HTTP: Applies to Layer 7 server load balancing. • RADIUS: Applies to Layer 7 server load balancing. • MySQL: Applies to Layer 7 server load balancing.
Default action	Specify a generic action for a generic LB policy, or specify any type of action for an HTTP LB policy. You can select an existing action or create an action.
Rule	Specify an action for packets matching the specified class. 3. Click **Create**. o Class: Select an existing class or create a class. o Action: Select an existing action or create an action. o Insert before: Inserts the target class before a class. 4. Click **OK**.

Item	Description
Description	Enter a description for the LB policy.

4. Click **OK**. The new LB policy appears on the **Load Balancing Policy** page.

Configure a connection limit policy (optional)

Using a connection limit policy can limit the number of connections on the device. It helps prevent a large number of connections from consuming too many device system resources and server resources. In this way, internal network resources (hosts or servers) are protected, and device system resources can be used more appropriately.

A connection limit policy can have multiple rules. Each rule specifies a range of users and the limit to the user connections. A connection limit policy applies only to the user connections matching a rule. When the number of connections for a certain type reaches the upper limit, the device does not accept new connection requests of that type. It accepts new connection requests only when the number of connections drops below the lower limit.

The user ranges in the rules are set by using ACLs.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Connection Limit Policy**.
2. Click **Create**.
3. Create a connection limit policy.

Table 9 Connection limit policy configuration items

Item	Description
Name	Enter a name for the connection limit policy, case insensitive.
Limit rule	Create a rule. 5. Click **Create**. o Rule ID: Specify an ID for the connection limit rule. o Type: Specify a connection limit rule type, which can be IPv4 ACL or IPv6 ACL. o ACL: Specify an ACL. You can select an existing ACL or create an ACL. o Limit by: Select source IP address, destination IP address, or service. Source IP address limits user connections by source IP address. Destination IP address limits user connections by destination IP address. Service limits user connections by service. Services are classified by transport layer protocol and service port number. o Connection limits-Upper limit: Specify the upper limit of connections. When the number of connections in a specified range or for a certain type reaches the upper limit, the device does not accept new connection requests. o Connection limits–Lower limit: Specify the lower limit of connections. The lower limit must be equal to or smaller than the upper limit. The device accepts new connection requests only when the number of connections drops below the lower limit. 6. Click **OK**.
Description	Enter a description for the connection limit policy.

4. Click **OK**. The new connection limit policy appears on the **Connection Limit Policy** page.

Configure a protection policy (optional)

A protection policy can prevent the LB device and internal servers from being attacked. In a protection policy, you can specify protection rules and protection actions. A protection rule defines the URLs to be protected and the protection period. A protection action is taken if the number of times a user accesses a protected URL exceeds the configured protection threshold during the protection period.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Protection Policy**.
2. Click **Create**.
3. Create a protection policy.

Table 10 Protection policy configuration items

Item	Description
Name	Enter a name for the protection policy, case insensitive.
Type	Specify the type for the protection policy. The device supports only the HTTP type.
Protection action	Select protection actions. A protection action is taken if the number of times a user accesses a protected URL exceeds the configured protection threshold. You can specify the following protection actions: • **Warning**—Generates a log message and sends it to the information center. • **Drop**—Drops requests. • **Verify client**—Returns a response carrying a cookie value to the client. If a subsequent request carries the returned cookie value, it passes the verification. If a subsequent request does not carry a

Item	Description
	cookie value or carries a different cookie value, it fails to pass the verification and is dropped. The device supports returning a cookie value by inserting an HTTP header or a JS script.
Protection rule	A protection policy can contain multiple protection rules. Each protection rule defines the URLs to be protected and the protection period. A protection action is taken if the number of times a user accesses a protected URL exceeds the configured protection threshold during the protection period. The device supports using source-IP-based and cookie-based criteria to determine whether requests belong to the same user. If you configure both a cookie-based request threshold and a source-IP-based request threshold, the protection action is taken when either threshold is exceeded. 1. Click **Create** to create a protection rule. ○ Rule ID: Specify the rule ID. ○ Protected URL: Specify a regular expression to match URLs, a case-sensitive string. The regular expression cannot contain question marks (?). ○ Statistics period: Set the protection period. If the number of times that a user accesses a protected URL exceeds the request threshold during the protection period, the protection action is taken. ○ Source-IP-based threshold: Configure a source-IP-based request threshold. ○ Cookie name: Specify an HTTP cookie by its name, a case-sensitive string. The cookie name cannot contain brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). Additionally, the cookie name cannot contain ASCII codes that are less than or equal to 31 and greater than or equal to 127. ○ Cookie-based threshold: Configure a cookie-based protection threshold. 2. Click **OK**.
Description	Enter a description for the protection policy.

4. Click **OK**. The new protection policy appears on the **Protection Policy** page.

Configure a parameter profile (optional)

You can configure advanced parameters through a parameter profile. The virtual server references the parameter profile to analyze, process, and optimize service traffic.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Parameter Profiles**.
2. Click **Create**.
3. Create a parameter profile.

Table 11 Parameter profile configuration items

Item	Description
Parameter profile name	Enter a name for the parameter profile, case insensitive.
Type	Specify the type for the parameter profile. • IP: Applies to Layer 4 server load balancing. For more information about IP parameter configuration, see Table 12. • TCP: Applies to Layer 7 server load balancing. For more information about TCP parameter configuration, see Table 13. • HTTP: Applies to Layer 7 server load balancing. For more information about HTTP parameter configuration, see Table 14. • HTTP-Compression: Applies to Layer 7 server load balancing. For more information about HTTP compression parameter configuration, see Table 15. • HTTP-Statistics: Applies to Layer 7 server load balancing. For more information about HTTP statistics parameter configuration, see Table 16. • OneConnect: Applies to Layer 7 server load balancing. For more information about OneConnect parameter configuration, see Table 17. • TCP-Application: Applies to Layer 7 server load balancing. For

Item	Description
	more information about TCP application parameter configuration, see Table 18. • MySQL: Applies to Layer 7 server load balancing. For more information about MySQL application parameter configuration, see Table 19.
Description	Enter a description for the parameter profile.

Table 12 IP parameter configuration items

Item	Description
ToS sent to client	Set the ToS field value of IP packets sent to the client.

Table 13 TCP parameter configuration items

Item	Description
Option operation list	This feature enables the LB device to insert the client's actual IP address into the specified option in headers of TCP packets sent to the server or remove the specified option. 3. To create an option operation, click **Create**. ◦ Insert: Inserts the client's actual IP address into the specified option in headers of TCP packets sent to the server. ◦ Remove: Removes the specified option from headers of TCP packets sent to the server. ◦ Option number: Number of the option to be operated. ◦ Encoding type: Select the binary or string encoding mode for the TCP option. 4. Click **OK**. The new option operation appears in the **Option operation list**.

Item	Description
Max local window size	Configure the maximum local window size for TCP connections.
Action on MSS-exceeded packets	Specify the action to take on the segments that exceed the MSS in the HTTP requests sent by the client. • Permit: Allows the segments to exceed the MSS. • Drop: Discards the segments that exceed the MSS.
Idle timeout time	Specify the idle timeout time for TCP connections. If no data is transmitted before the idle timeout time expires, the LB device disconnects the TCP connection with the client or server.
TCP MSS	Specify the MSS for the LB device.
TIME-WAIT timeout time	Set the TIME_WAIT state timeout time for TCP connections. A TCP connection is released slowly after it is disconnected, because the TIME_WAIT timer of TCP is long. You can adjust the TIME_WAIT state timeout time. This parameter takes effect only when the TCP parameter profile is used by an HTTP or HTTPS virtual server.
SYN timeout time	Set the SYN packet timeout time for TCP connections. If no SYN-ACK packet is received when the timer expires, the TCP connection is closed. This parameter takes effect only when the TCP parameter profile is used by an HTTP or HTTPS virtual server.
Keepalive timeout time	Set the TCP keepalive packet sending interval for an idle TCP connection. This parameter takes effect only when the TCP parameter profile is used by an HTTP or HTTPS virtual server.
Keepalive retransmission interval	Set the TCP keepalive packet retransmission interval. This parameter takes effect only when the TCP parameter profile is used by an HTTP or HTTPS virtual server.
Keepalive retransmission	Set the TCP keepalive packet retransmission times. This parameter takes effect only when the TCP parameter profile is

Item	Description
times	used by an HTTP or HTTPS virtual server.
FIN-WAIT-1 timeout time	Set the FIN-WAIT-1 state timeout timer for TCP connections. This parameter takes effect only when the TCP parameter profile is used by an HTTP or HTTPS virtual server.
FIN-WAIT-2 timeout time	Set the FIN-WAIT-2 state timeout timer for TCP connections. This parameter takes effect only when the TCP parameter profile is used by an HTTP or HTTPS virtual server.
TCP option number for SNAT	Specify the number of the TCP option used for SNAT. The LB device translates the source IP address of packets into the IP address in the specified TCP option.
Encoding type	Select the binary or string encoding mode for the TCP option.

Table 14 HTTP parameter configuration items

Item	Description
Max header parse length	Set the maximum length of HTTP headers that can be parsed.
Max content parse length	Set the maximum length of the HTTP entities that can be parsed.
Max content length	Set the maximum content length of HTTP requests. If the content length of an HTTP request exceeds the maximum length, the device drops the HTTP request.
Secondary cookie delimiter	Specify the delimiter that separates secondary cookies in URLs, including ! " # ; < > ? [\ ] ^ ` | : @ & $ + * ' ( ) , /.
Secondary cookie start delimiter	Specify the start delimiter for secondary cookies in URLs, including ! " # ; < > ? [\ ] ^ ` |.

Item	Description
Cookie name	Specify the cookie to be encrypted by its name, a case-sensitive string.
Cookie encryption key	Specify a key in plaintext or ciphertext form.
Key	Specifies the key, a case-sensitive string.
Action on max-header-length exceeded packets	Specify the action to take on the HTTP requests when their packet headers exceed the maximum length. • Permit: Allows the HTTP requests to pass. • Drop: Discards the HTTP requests. When the HTTP packet header length exceeds the processing capability of load balancing, the **drop** action applies.
Per-packet load balancing	Enable or disable per-packet load balancing for HTTP requests.
Connection reuse	Enable or disable connection reuse between the LB device and the server. Connection reuse allows the LB device to establish connections to the server that can be reused by clients. Because multiple clients can use the same connection, the number of connections between the clients and the server is reduced.
Case sensitivity	Enable or disable case sensitivity for matching character strings. This setting affects the following content: • HTTP header value, HTTP cookie name and value, and URL for matching classes. • Header value, URL, and key value used for generating sticky entries for the HTTP header sticky method. • Cookie name and value and key value used for generating sticky entries for the cookie get sticky method.
Load balance each request	Enable or disable per-request load balancing for HTTP requests.

Table 15 HTTP compression parameter configuration items

Item	Description
Level	Set the compression level for response packets. A larger value indicates a lower compression speed and a higher compression ratio.
Preferred compression algorithm	Specify the preferred compression algorithm. If the client request supports the configured compression algorithm, the configured compression algorithm applies. If the client request does not support the configured compression algorithm, the compression algorithm contained in the request applies. • gzip: Specifies the GNU zip compression algorithm. • deflate: Specifies the Deflate compression algorithm.
Min content length	Set the minimum length of HTTP response content for compression. The value 0 indicates that the packet content is always compressed, regardless of the content length. If an HTTP response packet contains the Content-Length header, the packet content is compressed only when its length reaches the minimum length of HTTP response content for compression. If the HTTP response packet does not contain the Content-Length header, the configuration does not take effect. The packet content is compressed regardless of its length.
Insert Vary header	Enable or disable insertion of the Vary header into HTTP responses. Enabling this feature inserts the Vary header to HTTP responses and sets the header content to Accept-Encoding before sending them to the client. The setting takes effect regardless of whether the response packets contain the Vary header or whether the packets are compressed.
Compression for HTTP 1.0	Enable or disable compression for responses to HTTP 1.0 requests.
Delete Accept-Encoding header	Enable or disable deletion of the Accept-Encoding header from HTTP requests. Enabling this feature enables the LB device to delete the Accept-Encoding header from the HTTP request before sending it to the server. If the response packet sent by the server matches the specified match rule, the LB device compresses the packet before sending it to the requesting client. If the HTTP request sent by the client does not contain the Accept-Encoding header, the LB device does not compress the response packet regardless of whether this feature is

Item	Description
	enabled.
Memory size	Specify the memory size in KB used for compression. The value can only be 1, 2, 4, 8, 16, 32, or 64.
Window size	Specify the window size in KB used for compression. The value can only be 1, 2, 4, 8, 16, or 32.
Filtering rule for compression	5. Click **Create**. o Rule ID: Specify the rule ID. o Action: Specify permit to compress matching packets, or specify deny to not compress matching packets. o Type: Specify URL to match URLs in packets, or specify content to match content types in the Content-Type header of packets. o URL: Specify a regular expression for matching URLs, a case-sensitive string. The string cannot contain question marks (?). This parameter is available only for the URL type. o Content-Type: Specify a regular expression for matching content types, a case-sensitive string. The string cannot contain question marks (?). This parameter is available only for the content type. 6. Click **OK**.

Table 16 HTTP statistics parameter configuration items

Item	Description
Address object group	If HTTP packets match the specified URL and source IP address object group, they are counted based on the source IP address object group. If HTTP packets match the specified URL but do not match the specified source IP address object group, they are counted based on the source IP address. You can specify a maximum of 1024 source IP address object groups in one HTTP statistics parameter profile.

Item	Description
HTTP statistics node list	7. Click **Create**. ○ Node name: Specify the statistics node name, case insensitive. You can configure a maximum of 256 statistics nodes in one HTTP statistics parameter profile. ○ Description: Enter a description for the statistics node, case sensitive. ○ Statistics rule list: List of URL match rules. You can configure a maximum of 256 URL match rules for one statistics node. ○ ID: Specify the match rule ID. ○ URL: Specify a URL regular expression. The string cannot contain question marks (?). 8. Click **OK**.

Table 17 OneConnect parameter configuration items

Item	Description
Max reuse number	Set the maximum number of times that a TCP connection can be reused. After connection reuse is enabled, a TCP connection is not disconnected until the maximum number of reuse times is reached. After the TCP connection is disconnected, new connection requests trigger establishment of a new TCP connection.
Idle timeout time	Set the idle timeout time for TCP connections between the LB device and servers. The idle timeout time is the amount of time that a TCP connection can stay idle before it is disconnected. After the TCP connection is disconnected, new connection requests trigger establishment of a new TCP connection.
IPv4 mask length	Specify the IPv4 mask length for connection reuse. This setting limits the network segment of clients that can reuse connections between the LB device and servers. If the client that initiates a connection request is in the same network segment as the idle TCP connection, the idle TCP connection is reused. If the client

Item	Description
	does not match this requirement, a new TCP connection is established.
IPv6 prefix length	Specify the IPv6 prefix length for connection reuse. This setting limits the network segment of clients that can reuse connections between the LB device and servers. If the client that initiates a connection request is in the same network segment as the idle TCP connection, the idle TCP connection is reused. If the client does not match this requirement, a new TCP connection is established.

Table 18 TCP application parameter configuration items

Item	Description
TCP buffering period	Specify the buffering period for TCP payload matching.
TCP maximum buffering size	Specify the maximum buffering size. The device stops buffering traffic when the maximum buffering size is reached.
TCP buffering end string	Configure the TCP buffering end string. The device stops buffering traffic when it receives the buffering end string.

Table 19 MySQL parameter configuration items

Item	Description
Connection pool size	Specify the maximum number of TCP connections that can be stored in a connection pool. After MySQL data transfer is completed, the TCP connection is stored in a connection pool instead of being closed. For a new connection request, the device selects an available connection from the

Item	Description
	connection pool before attempting to open a new connection.
Connection reuse	Enable or disable connection reuse. This feature allows the LB device to establish connections to the server that can be reused by multiple clients. This feature helps reduce the connections opened between clients and servers.
Max reuse number	Set the maximum number of times that a TCP connection can be reused. After connection reuse is enabled, a TCP connection is not disconnected until the maximum number of reuse times is reached. After the TCP connection is disconnected, new connection requests trigger establishment of a new TCP connection.
Idle timeout time	Set the idle timeout time for TCP connections between the LB device and servers. The idle timeout time is the amount of time that a TCP connection can stay idle before it is disconnected. After the TCP connection is disconnected, new connection requests trigger establishment of a new TCP connection.
IPv4 mask length	Specify the IPv4 mask length for connection reuse. This setting limits the network segment of clients that can reuse connections between the LB device and servers. If a client that initiates a connection request is in the same network segment as the idle TCP connection, the client reuses the idle TCP connection. If the client does not match this requirement, a new TCP connection is established.
IPv6 prefix length	Specify the IPv6 prefix length for connection reuse. This setting limits the network segment of clients that can reuse connections between the LB device and servers. If a client that initiates a connection request is in the same network segment as the idle TCP connection, the client reuses the idle TCP connection. If the client does not match this requirement, a new TCP connection is established.

4. Click **OK**. The new parameter profile appears on the **Parameter Profile** page.

Configure an intelligent probe template (optional)

You can configure an HTTP passive, RST, zero-window, or custom intelligent probe template to monitor a single server farm member or all members in a server farm.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Probe Templates**.
2. Click **Create**.
3. Create an intelligent probe template.

Table 20 Intelligent probe template configuration items

Item	Description
Probe template name	Enter a name for the probe template, case insensitive.
Type	Specify the type for the intelligent probe template: • RST: Monitors the number of RST packets sent by a real server. For information about configuring an RST probe template, see Table 21. • Zero-window: Monitors the number of zero-window packets sent by a real server. For information about configuring a zero-window probe template, see Table 21. • HTTP passive: Monitors the number of abnormal URLs in HTTP response packets. For information about configuring an HTTP passive probe template, see Table 22. • Custom: Monitors the state of real servers by using a custom script file. For information about configuring a custom probe template, see Table 23.
Description	Enter a description for the intelligent probe template.

Table 21 RST and zero-window probe template configuration items

Item	Description
Monitoring time	Specify the monitoring time. During the monitoring time, the system counts the number of RST packets or zero-window packets sent by each server farm member in a server farm if an RST or zero-window probe template is specified.
Threshold	Specify the maximum number of RST packets or zero-window packets a real server can send before an action is taken.
Action	Specify the action to take when the RST or zero-window packet threshold is reached. • Shut down: Shuts down a real server. • Set to busy: Places a real server in busy state. The system continues to probe the real server at the probe intervals. If the number of RST or zero-window packets sent does not reach the threshold during the probe interval, the real server is placed back in normal state. If the packet number reaches the threshold, the system probes the real server until the maximum probe times is reached. If the result of every probe reaches the threshold, the system automatically shuts down the real server. A real server that is shut down due to packet threshold violation or exceeded probe times will be restored to normal state immediately when the intelligent probe template is deleted.
Probe interval	Specify the interval to probe the real server in busy state.
Probe times	Specify the maximum number of times for probing the real server in busy state. The value 0 means that the number of probe times is not limited.

Table 22 HTTP passive probe template configuration items

Item	Description
Monitoring time	Specify the monitoring time. During the monitoring time, the system monitors the responses of matching HTTP requests if an HTTP passive probe template is specified.

Item	Description
Threshold	Specify the maximum number of abnormal URLs in HTTP response packets. If the number of abnormal URLs exceeds the maximum number, the real server is shut down.
Timeout time	Specify the timeout time for the HTTP passive probe template. The device monitors the responses of HTTP requests with the specified URL. If the response time for an HTTP request exceeds the timeout time, a URL error is recorded.
URLs to check	Configure the URLs to check. The URLs cannot contain question marks (?). If the device receives an HTTP request with any of the specified URLs, the device monitors the responses of the HTTP request. A maximum of 10 URLs can be configured for an HTTP passive probe template.
Response status code	Configure the response status codes to check. If an HTTP response contains any of the specified response status codes, a URL error is recorded. A maximum of 10 response status codes can be configured for an HTTP passive probe template.

Table 23 Custom probe template configuration items

Item	Description
Monitoring time	Specify the monitoring interval. At the monitoring intervals, the system executes the specified script file.
Timeout time	Specify the timeout time for waiting for responses. As a best practice, set timeout time to be smaller than the monitoring interval.
Script parameters	Configure script parameters. When executing a script file, the device transfers the script parameters

Item	Description
	to the script file. Multiple space-separated script parameters are supported.
Script file	Select and import a script file. The device detects the state of real severs according to the detection contents in the script file. The device supports only script files with the **.py** suffix.
Environment variable	Configure an environment variable. You can specify the environment to execute the custom script file by configuring an environment variable.

4. Click **OK**. The new intelligent probe template appears on the **Probe Templates** page.

Configure a global SNAT policy (optional)

A global SNAT policy is used to translate the source IP addresses of packets into the specified IP addresses. You can implement SNAT by configuring a global SNAT policy on the Global SNAT Policy page or by configuring SNAT on the Server Farm page. The SNAT configuration on the Server Farm page has higher priority. A server farm without SNAT configuration uses the global SNAT policy for address translation.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Global SNAT Policies**.
2. Click **Create**.
3. Create a global SNAT policy.

Table 24 Global SNAT policy configuration items

Item	Description
Global SNAT policy name	Enter a name for the global SNAT policy, case insensitive.
SNAT mode	Select an SNAT mode. • SNAT pool: Translates the source IP address into an IP address in the specified SNAT address pool. • Auto mapping: Translates the source IP address into the IP address of the interface connecting to the real servers.
SNAT pool name	Select an existing SNAT pool or create an SNAT pool. This parameter is supported only when the SNAT mode is SNAT pool.
VRF	Specify the VPN instance to which the global SNAT policy belongs.
Priority	Set the priority for the global SNAT policy. You can configure multiple global SNAT policies with different priorities. They are matched in descending order of priority values.
Source IP address object group	Specify a source IP address object group for address translation. The device performs SNAT on only packets with a matching source IP address.
Destination IP address object group	Specify a destination IP address object group for address translation. The device performs SNAT on only packets with a matching destination IP address.
Service object group	Specify a service object group for address translation. The device performs SNAT on only packets with a matching service.
Policy status	Enable or disable the global SNAT policy.
Description	Enter a description for the global SNAT policy.

4. Click **OK**. The new global SNAT policy appears on the **Global SNAT Policy** page.

Configure a virtual server

A virtual server is a virtual service provided by the LB device to determine whether to perform load balancing for packets received on the LB device. Only the packets that match a virtual server are load balanced.

The virtual server types supported by server load balancing include IP, TCP, UDP, SIP-TCP, SIP-UDP, HTTP, Performance (HTTP), HTTPS, HTTP redirection, RADIUS, and MySQL. Do not specify the same VSIP and port number for virtual servers of the UDP and SIP-UDP types; do not specify the same VSIP and port number for virtual servers of the TCP, SIP-TCP, HTTP, Performance (HTTP), HTTPS, HTTP redirection, RADIUS, and MySQL types. For the LB device to correctly process packets, do not configure the Performance (HTTP) virtual server and the TCP client verification feature at the same time. For more information about the TCP client verification feature, see the attack defense help by selecting **Policies** > **Attack Defense** > **Protected IP Addresses**.

Procedure

1. Select **Policies** > **Load Balancing** > **Server Load Balancing** > **Virtual Servers**.
2. Click **Create**.
3. Create a virtual server.

Table 25 Basic configuration items

Item	Description
Virtual server name	Enter a name for the virtual server, case insensitive.

Item	Description
Type	Specify the virtual server type, which can be IP, TCP, UDP, SIP-TCP, SIP-UDP, HTTP, Performance (HTTP), HTTPS, HTTP redirection, RADIUS, or MySQL.
IPv4 address	Configure an IPv4 address/mask length (0-32) for the virtual server.
IPv6 address	Configure an IPv6 address/prefix length (0-128) for the virtual server.
Port number	Configure the port number of the virtual server. 0 indicates any port. For the IP, TCP, UDP, and RADIUS virtual server types, you can enter a comma-separated list of up to 32 port number items. Each item specifies a port number or a range of port numbers, for example, 5,10,20-28.
UDP per-packet load balancing	Enable or disable per-packet load balancing for UDP traffic for a virtual server. When per-packet load balancing for UDP traffic is disabled, the LB device distributes traffic matching the virtual server according to application type. Traffic of the same application type is distributed to one real server. When per-packet load balancing for UDP traffic is enabled, the LB device distributes traffic matching the virtual server on a per-packet basis. This parameter is supported only by virtual servers of the UDP type, SIP-UDP type, and RADIUS type.
SSL server policy	Specify an SSL server policy for a virtual server to encrypt traffic between the LB device (SSL server) and the SSL client. You can select an existing SSL server policy or create an SSL server policy. This parameter is supported only by virtual servers of the TCP and HTTPS types.
Redirection URL	Specify a redirection URL for the virtual server, case sensitive. The redirection feature redirects all request packets matching the virtual server to the URL. You can also specify the question mark (?) or the following character strings as the redirection URL:

Item	Description
	• %h: Specifies the host name in the client request packet. • %p: Specifies the URL in the client request packet. • %%: Specifies the percentage sign (%). This parameter is supported only by virtual servers of the HTTP redirection type.
Redirection mode	Specify a redirection mode for the virtual server. • Temporary • Permanent This parameter is supported only by virtual servers of the HTTP redirection type.
Server farm	Select an existing server farm or create a server farm for the virtual server. This parameter is not supported by virtual servers of the HTTP redirection type.
Sticky group of the server farm	Select an existing sticky group or create a sticky group as the primary sticky group for the server farm. This parameter is not supported by virtual servers of the HTTP redirection type.
VRRP-group-associated interface	Specify the interface to be associated with the VRRP group. If you configure this parameter, you must bind a VRRP group number to the virtual server.
VRRP group number	Specify the number of the VRRP group to be bound to the virtual server. In dual-active mode of the high availability (HA) group, both devices back up each other and process services. If you do not bind a VRRP group number to the virtual server, both devices process services and use the SNAT address pool. If you bind a VRRP group number to the virtual server, only the primary device processes services and uses the SNAT address pool. For more information about the HA group, see its online help. This setting applies only to virtual severs with IPv4 addresses. You can configure this parameter only after you specify a VRRP-group-associated interface.

Item	Description
IPv6 VRRP-group-associated interface	Specify the interface to be associated with the IPv6 VRRP group. If you configure this parameter, you must bind an IPv6 VRRP group number to the virtual server.
IPv6 VRRP group number	Specify the number of the IPv6 VRRP group to be bound to the virtual server. In a dual-active HA network, both devices back up each other and process services. If you do not bind an IPv6 VRRP group number to the virtual server, both devices process services and use the SNAT address pool. If you bind an IPv6 VRRP group number to the virtual server, only the primary device processes services and uses the SNAT address pool. For more information about HA, see its online help. This setting applies only to virtual severs with IPv6 addresses. You can configure this parameter only after you specify an IPv6-VRRP-group-associated interface.
MySQL version	Specify the MySQL database version. The LB device initiates authentication to clients on behalf of the MySQL server and sends database initialization packets of the specified MySQL version to clients.
Read/Write splitting	Enable or disable read/write splitting. This feature allows read commands and write commands to be executed by the read server farm and write server farm, respectively. This feature helps reduce the impact of concurrent read/write requests on database performance. After this feature is enabled, you must configure both a read server farm and a write server farm.
Read server farm	Select an existing server farm or create a server farm as the read server farm for the virtual server. This parameter is available only when read/write splitting is enabled.
Read sticky group	Select an existing sticky group or create a sticky group as the read sticky group for the virtual server. This parameter is available only when read/write splitting is

Item	Description
	enabled.
Write server farm	Select an existing server farm or create a server farm as the write server farm for the virtual server. This parameter is available only when write/write splitting is enabled.
Write sticky group	Select an existing sticky group or create a sticky group as the write sticky group for the virtual server. This parameter is available only when write/write splitting is enabled.
Interfaces for sending gratuitous ARP/ND packets	Specify interfaces for sending gratuitous ARP packets and ND packets. If the IP address of an interface connected to a client is in the same network segment as the virtual server IP address, you must perform the following tasks: • Specify the interface connected to the corresponding client as an interface for sending gratuitous ARP/ND packets. • Enable IP address advertisement.
Operation mode	Operating mode of the virtual server: • Layer 4. • Layer 7. This parameter is supported only by TCP virtual servers.
IP address advertisement	Enable or disable IP address advertisement for the virtual server. After this feature is configured, the device advertises the IP address of the virtual server to OSPF for route calculation. When the service of a data center switches to another data center, the traffic to the virtual server can also be switched to that data center.
Redundancy group traffic distribution	Select an existing redundancy group or create a redundancy group. The traffic matching the virtual server is directed to the specified redundancy group. If the redundancy group does not exist or contains no effective failover groups, this function does not take effect.

Item	Description
	Support for this function depends on the device model.
Session extension information synchronization	Enable or disable session extension information synchronization for the virtual server. This parameter is supported only by virtual servers of the IP, TCP, UDP, SIP-TCP, SIP-UDP, and RADIUS types.
Sticky entry synchronization	Enable or disable sticky entry synchronization for the virtual server. The following configuration changes will cause the device to delete existing sticky entries and generate new ones based on subsequent traffic: • Disable sticky entry synchronization. • Change the sticky entry synchronization type. This parameter is not supported by virtual servers of the HTTP redirection type.
Sticky entry synchronization type	Select the sticky entry synchronization type: • **Intra-group synchronization**—Synchronizes sticky entries to the device in the same failover group. • **Global synchronization**—Synchronizes sticky entries to devices in all failover groups. This function is available only when sticky entry synchronization is enabled. Virtual servers of the HTTP redirection type do not support this function. Support for this function depends on the device model.
Virtual server feature	Enable or disable the virtual server. After you configure a virtual server, you must enable the virtual server for it to work.
Fast log output	Configure the content to be output by using the fast log output feature. Multiple semicolon-separated variables are supported. The device supports the following variables: • **%{is}**—Source IP address in HTTP requests.

Item	Description
	• **%{ps}**—Source port number in HTTP requests. • **%{id}**—Destination IP address in HTTP requests. • **%{pd}**—Destination port number in HTTP requests. • **%{sis}**—Source IP address in HTTP responses. • **%{sps}**—Source port number in HTTP responses. • **%{sid}**—Destination IP address in HTTP responses. • **%{spd}**—Destination port number in HTTP responses. • **%{vsn}**—Virtual server name. • **%{sfn}**—Server farm name. • **%{reqtmstamp}**—HTTP request timestamp. • **%{uri}**—HTTP URI. • **%{ver}**—HTTP version number. • **%{args}**—HTTP access parameters. • **%{method}**—HTTP request method. • **%{xff}**—IP address of XFF (X-Forwarded-For). • **%{ctype}**—Content-Type field in HTTP requests. • **%{clen}**—Content-Length field in HTTP requests. • **%{ref}**—Referer header field in HTTP requests. • **%{ua}**—User-Agent header field in HTTP requests. • **%{host}**—Host header field in HTTP requests. • **%{path}**—Path in HTTP requests. • **%{reqsz}**—HTTP request size in bytes. • **%{reqtm}**—HTTP request duration in milliseconds. The duration is from the time when the device receives an HTTP request to the time when the device receives the HTTP response. • **%{rspclen}**—Content-Type field in HTTP responses. • **%{reqsz}**—HTTP response size in bytes. • **%{rsptm}**—HTTP response duration in milliseconds. The duration is from the time when the device receives an HTTP response to the time when the device finishes sending out

Item	Description
	the HTTP response. • **%{stscode}**—HTTP response status code. • **%{reqbsz}**—Body size of HTTP requests, in bytes. • **%{rspbsz}**—Body size of HTTP responses received by the device from the server, in bytes. • **%{rspsntbsz}**—Body size of HTTP responses sent from the device to the client, in bytes. • **%{cookie**_*cookie-name*__**}**—HTTP cookie name, case-sensitive. The cookie name cannot contain brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), or horizontal tab (HT). Additionally, the cookie name cannot contain ASCII codes that are less than or equal to 31 or greater than or equal to 127. You can specify multiple cookies. This parameter is supported only by HTTP and HTTPS virtual servers.
Description	Enter a description for the virtual server.

User list	Configure the user name and password used to log in to the MySQL server.
	1. Click **Create** to create a user.
	  ◦ Username: Enter a username.
	  ◦ Password: Enter a password.
	2. Click **OK**. The new user appears in the user list.
	The device supports a maximum of 100 login users.

External link domain name rewrite	Enable or disable external link proxy. The external link proxy feature enables an LB device to operate as an external link proxy to request IPv4 resources on behalf of IPv6 clients. This feature helps achieve smooth IPv4-to-IPv6 network transition. When the LB device detects an external link in the HTTP response from the server, it returns a script file for rewriting the external link. The client executes the script file and adds the specified parameters to the domain name of the external link. The parameters include the URI, domain name suffix, and virtual server port number. Upon receiving a DNS request containing the

Item	Description
	modified domain name, the LB device will request the associated IPv4 resource on behalf of the IPv6 client. The format of the domain name after rewrite is *protocol type*://*original domain name*+*URI*+*domain name suffix*+:*virtual server port number*. The protocol type can be HTTP or HTTPS. Suppose the protocol type is HTTP, domain name of the original external link is **www.aaa.com**, URI is **proxy**, domain name suffix is **bbb.com**, and virtual server port number is **8080**. The external link domain name after rewrite is **http://www.aaa.com.proxy.bbb.com:8080**.
URI	Specify the URI for rewriting domain names of external links. The URI is a case-insensitive string that can contain only letters, digits, hyphens (-), and underscores (_). Upon receiving a response from the IPv6 site server, the LB device rewrites the IPv4 external link in the response by adding the specified parameters to the associated domain name. The parameters include the URI, domain name suffix, and virtual server port number. Suppose the domain name of the original external link is **http://www.aaa.com**, URI is **proxy**, domain name suffix is **bbb.com**, and virtual server port number is **8080**. The external link domain name after rewrite is **http://www.aaa.com.proxy.bbb.com:8080**. Upon receiving a DNS request containing this modified domain name, the LB device performs the following operations: 1. Extracts the original domain name. 2. Requests the associated IPv4 resource on behalf of the IPv6 client. 3. Returns the obtained IPv4 resource to the IPv6 client.
Domain name suffix	Specifies the domain name suffix for rewriting domain names of external links. The domain name suffix is a case-insensitive, dot-separated string. Each dot-separated label in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), and dots (.).
SNAT address pool	Specify a SNAT address pool for external link proxy. To request an IPv4 resource as an external link proxy, the LB device will choose an IP address from the specified SNAT pool. The LB device uses this IP address as the client IP address to initiate a request on behalf of the IPv6 client. If you do not specify a SNAT address pool, the LB device uses

Item	Description
	the IP address of the output interface to the server as the client IP address.
SNAT address pool	Specify a SNAT address pool for external link proxy. To request an IPv4 resource as an external link proxy, the LB device will choose an IP address from the specified SNAT pool. The LB device uses this IP address as the client IP address to initiate a request on behalf of the IPv6 client. If you configure a traffic distribution mode, you must specify a SNAT address pool. If you disable traffic distribution, you can choose to specify or not specify a SNAT address pool. If you do not specify a SNAT address pool, the LB device uses the IP address of the output interface to the server as the client IP address.
Allowlists	Add a domain name to the allowlist for external link proxy. 1. Enter a domain name, a case-insensitive, dot-separated string. Each dot-separated label in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), and dots (.). 2. Click **Add**. The domain name appears in the **Allowlists**. The LB device does not rewrite the external links containing any domain names in the allowlist.

Table 26 Advanced configuration items

Item	Description
Scheduling resources-Backup server farm	Specify the backup server farm for the virtual server. When the primary server farm is available (contains real servers), the virtual server forwards packets through the primary server farm. When the primary server farm is not available, the virtual server forwards packets through the backup server farm. You can select an existing server farm or create a server farm.

Item	Description
Scheduling resources-Backup sticky group of the server farm	Specify the backup sticky group for the server farm. If you specify both a primary sticky group and a backup sticky group, the device generates both primary sticky entries and backup sticky entries. If packets do not match primary sticky entries, backup sticky entries are used to match the packets. This parameter is supported only by virtual servers of the HTTP, HTTPS, and RADIUS types.
Scheduling resources-Load balancing policy	Specify an LB policy for the virtual server. By using an LB policy, the virtual server implements load balancing for matching packets based on the packet contents. You can select an existing LB policy or create an LB policy. A virtual server can use the policy template of the specified type. For example, a virtual server of the Performance (HTTP) or HTTP type can use a policy template of the generic type or HTTP type. A virtual server of the IP, TCP, UDP, SIP-TCP, or SIP-UDP type can use a policy template of the generic type only. A virtual server of the RADIUS type can use a policy template of the generic or RADIUS type only.
Scheduling resources-Connection limit policy	Specify a connection limit policy for the virtual server to limit the number of connections on the virtual server. You can select an existing connection limit policy or create a connection limit policy.
Scheduling resources-SSL client policy	Specify an SSL client policy for the virtual server to encrypt traffic between the LB device (SSL client) and the SSL server. You can select an existing SSL client policy or create an SSL client policy. This parameter is supported only by virtual servers of the HTTPS type.

Scheduling resources-SSL server policy with SNI	Configure an SSL server policy with an SNI for the virtual server.
	
	1. Click **Add** to create an SSL server policy with an SNI.
	  ○ Policy name: Enter a policy name, case insensitive.
	  ○ Server name indication (SNI): Enter an SNI, case insensitive.
	
	2. Click **OK**. The new SSL server policy appears in the policy

Item	Description
	list. If you configured both an SSL server policy without an SNI and an SSL server policy with an SNI, the SSL server policy without an SNI takes effect. You cannot configure multiple SSL server policies with the same SNI for a virtual server. This parameter is supported only by virtual servers of the HTTPS type.
Scheduling resources-Cookie sticky group	Specify a cookie sticky group for the virtual server. You can also specify sticky groups to be associated with server farms on the **Create Virtual Server** page or **Create Action** page. The cookie sticky group specified for the virtual server has the highest priority. It is preferentially used to generate sticky entries. Only cookie sticky groups can be specified for this parameter.
Scheduling resources-VPN instance	Specify a VPN instance for the virtual server. You can select an existing VPN instance or create a VPN instance.
Protection policy-HTTP protection policy	Specify an HTTP protection policy for the virtual server to guard against attack traffic matching the protection policy. You can select an existing HTTP protection policy or create an HTTP protection policy.
Parameter profile-IP parameter profile	Specify an IP parameter profile for the virtual server to process matching traffic based on the parameter profile. You can select an existing IP parameter profile or create an IP parameter profile.
Parameter profile-TCP parameter profile (client side)	Specify a TCP parameter profile for the virtual server to process matching traffic based on the parameter profile. A TCP parameter profile (client) used by the virtual server processes and optimizes TCP connections between the device and the client. You can select an existing TCP parameter profile or create a TCP parameter profile. This parameter is supported only by virtual servers of the TCP, Performance (HTTP), HTTP, HTTPS, or MySQL type.

Item	Description
Parameter profile-TCP parameter profile (server side)	Specify a TCP parameter profile for the virtual server to process matching traffic based on the parameter profile. A TCP parameter profile (server) used by the virtual server processes and optimizes TCP connections between the device and the server. You can select an existing TCP parameter profile or create a TCP parameter profile. This parameter is supported only by virtual servers of the TCP, Performance (HTTP), HTTP, HTTPS, or MySQL type.
Parameter profile-TCP-application parameter profile	Specify a TCP-application parameter profile for the virtual server to process matching traffic based on the parameter profile. You can select an existing TCP-application parameter profile or create a TCP-application parameter profile. This parameter is supported only by TCP virtual servers operating at Layer 7.
Parameter profile-HTTP parameter profile	Specify an HTTP parameter profile for the virtual server to process matching traffic based on the parameter profile. You can select an existing HTTP parameter profile or create an HTTP parameter profile. This parameter is supported only by virtual servers of the Performance (HTTP), HTTP, or HTTPS type.
Parameter profile-HTTP statistics parameter profile	Specify an HTTP statistics parameter profile for the virtual server to process matching traffic based on the parameter profile. You can select an existing HTTP statistics parameter profile or create an HTTP statistics parameter profile. This parameter is supported only by virtual servers of the HTTP type.
OneConnect parameter profile	Specify a OneConnect parameter profile for the virtual server to process matching traffic based on the parameter profile. You can select an existing OneConnect parameter profile or create a OneConnect parameter profile. This parameter is supported only by virtual servers of the HTTP or HTTPS type.

Item	Description
MySQL parameter profile	Specify a MySQL parameter profile for the virtual server to process matching traffic based on the parameter profile. You can select an existing MySQL parameter profile or create a MySQL parameter profile. This parameter is supported only by virtual servers of the MySQL type.
QoS-Maximum connections	Specify the maximum number of connections for the virtual server. 0 means not limited.
QoS-Maximum connections per second	Specify the maximum number of connections per second for the virtual server. 0 means not limited.
QoS-Maximum bandwidth	Specify the maximum bandwidth for the virtual server. 0 means not limited.
QoS-Maximum inbound bandwidth	Specify the maximum inbound bandwidth for the virtual server. 0 means not limited.
QoS-Maximum outbound bandwidth	Specify the maximum outbound bandwidth for the virtual server. 0 means not limited.
Content security-Content security function	Enable or disable content security.
Content security-IPS profile	Specify the IPS profile to be used for intrusion protection of traffic matching the virtual server. For more information about IPS profiles, see the IPS online help.
Content security-Anti-virus profile	Specify the antivirus protection configuration file to be used for antivirus protection of traffic matching the virtual server. For more information about anti-virus profiles, see the anti-virus online help.

4. Click **OK**. The new virtual server appears on the **Virtual Server** page.

Outbound link load balancing

This help contains the following topics:

Introduction

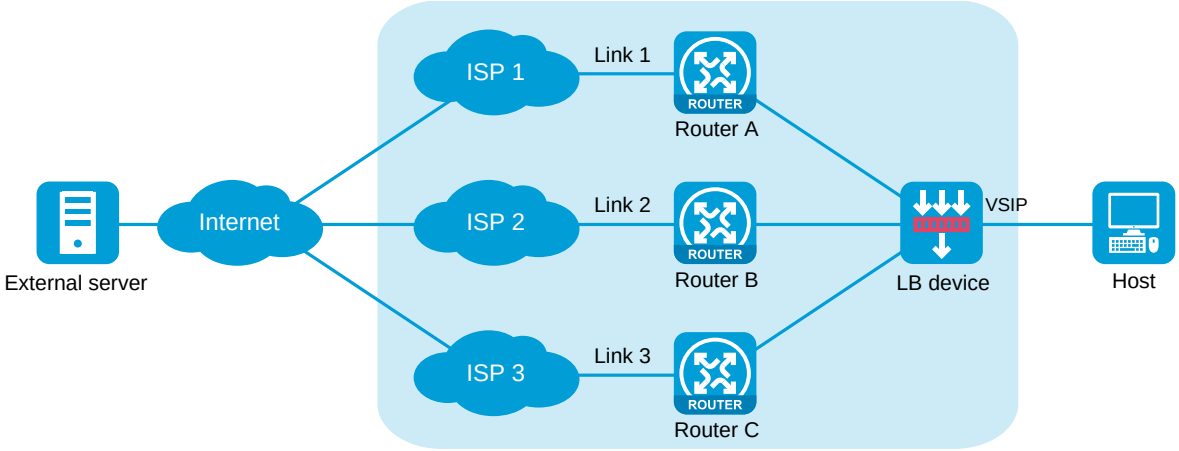
How it works

Outbound link load balancing load balances traffic among the links from the internal network to the external network.

As shown in Figure 1, outbound link load balancing contains the following elements:

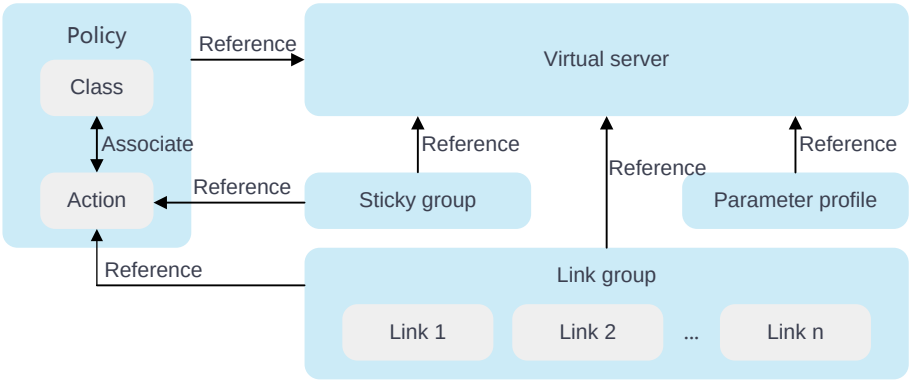
- **LB device**—Distributes outbound traffic among multiple links.
- **Link**—Physical links provided by ISPs.
- **VSIP**—Virtual service IP address of the cluster, which identifies the destination network for packets from the internal network.
- **Server IP**—IP address of a server, used by the LB device to distribute requests.

Figure 1 Network diagram



Relationship among configuration items

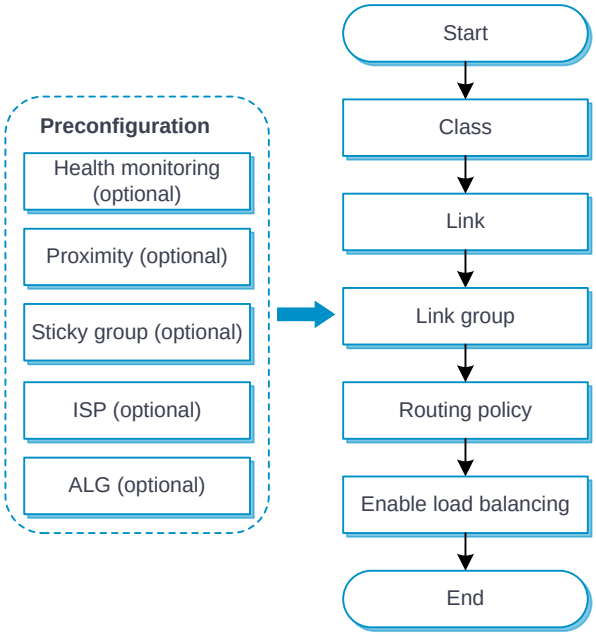
Figure 2 Relationship between the main configuration items



Configure outbound link load balancing

Figure 3 shows the configuration procedure for outbound link load balancing.

Figure 3 Outbound link load balancing configuration procedure



Configure health monitoring (optional)

The health monitoring configuration can be used by a link or link group.

For detailed steps required to configure health monitoring, see the online help for health monitoring.

Configure proximity (optional)

For detailed steps required to configure proximity, see the online help for load balancing common configuration.

Configure a sticky group (optional)

A sticky group can be used by an IPv4 or IPv6 routing policy.

For detailed steps required to configure sticky groups, see the online help for load balancing common configuration.

Configure ISP information

An ISP can be used by a match rule.

For detailed steps required to configure ISPs, see the online help for load balancing common configuration.

Configure ALG

For detailed steps required to configure ALG, see the online help for load balancing common configuration.

Configure a class

An LB class classifies packets by comparing packets against specific rules. Matching packets are further processed by LB actions.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Outbound Link Load Balancing** > **Class**.
2.
3. Click **Create** on the **Class** page.
4. Create a class.

Table 1 Class configuration items

Item	Description
Class	Enter a name for the class, case insensitive.
Match type	Select a match type: • **Match any**—A packet matches a class if it matches any of the rules in the class. • **Match all**—A packet matches a class if it matches all rules in the class.
Match rule	Configure a match rule. A class can contain a maximum of 65535 match rules. 1. Click **Create**, and configure the following parameters on the **Create Match Rule** page: ○ **Rule ID**—Enter a rule ID in the range of 1 to 65535. Rules are matched in ascending order of rule IDs. ○ **Type**—Select a rule type. Options include **Source IPv4 address**, **Source IPv6 address**, **Class**, **IPv4 ACL**, **IPv6 ACL**, **ISP**, **Application group**, **Destination IPv4 address**, **Destination IPv6 address**, **Domain name**, **Input interface**, **User**, and **Input interface**. ○ **IPv4 address**—Specify the IPv4 address to match. This parameter appears only if you have selected **Source IPv4 address** or **Destination IPv4 address** from the **Type** list. ○ **Mask length**—Specify the mask length for the IPv4 address, in the range of 0 to 32. This parameter appears only if you have selected **Source IPv4 address** or **Destination IPv4 address**

Item	Description
	from the **Type** list. ◦ **IPv6 address**—Specify the IPv6 address to match. This parameter appears only if you have selected **Source IPv6 address** or **Destination IPv6 address** from the **Type** list. ◦ **Prefix length**—Specify the prefix length for the IPv6 address, in the range of 0 to 128. This parameter appears only if you have selected **Source IPv6 address** or **Destination IPv6 address** from the **Type** list. ◦ **Class**—Specify the class to match. This parameter appears only if you have selected **Class** from the **Type** list. ◦ **IPv4 ACL**—Specify the IPv4 ACL to match. You can select an existing ACL or create an ACL. This parameter appears only if you have selected **IPv4 ACL** from the **Type** list. ◦ **IPv6 ACL**—Specify the IPv6 ACL to match. You can select an existing ACL or create an ACL. This parameter appears only if you have selected **IPv6 ACL** from the **Type** list. ◦ **ISP**—Specify the ISP to match. You can select an existing ISP or create an ISP. This parameter appears only if you have selected **ISP** from the **Type** list. ◦ **Application group**—Specify the application group to match. You can select an existing application group or create an application group. This parameter appears only if you have selected **Application group** from the **Type** list. ◦ **Domain name**—Specify the destination domain name to match. The LB device stores mappings between domain names and IP addresses in the DNS cache. If the destination IP address of an incoming packet matches an IP address in the DNS cache, the LB device queries the domain name for the IP address. If the queried domain name matches the domain name configured in a match rule, the LB device takes the LB action on the packet. The DNS cache can be viewed from the **Monitor** > **DNS Cache** page. This parameter appears only if you have selected **Domain name** from the **Type** list. ◦ **Input interface**—Specify the input interface to match. This parameter appears only if you have selected **Input interface** from the **Type** list. ◦ **User**—Specify the user or user group to match. This parameter appears only if you have selected **Input interface** from the **Type** list. You can select an existing user or user group or create a user or user group. This parameter appears only if you have selected **User** from the **Type** list. 2. Click **OK**. The new match rule appears in the match rule list.

Item	Description
Description	Enter a description for the class.

5. Click **OK**. The new class appears on the **Class** page.

Configure a link

For detailed steps required to configure links, see the online help for load balancing common configuration.

Configure a link group

You can add links that contain similar functions to a link group to facilitate management. For example, you can create different link groups for different ISPs.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Outbound Link Load Balancing** > **Link Groups**.
2.
3. Click **Create** on the **Link Group** page.
4. Create a link group.

Table 2 Link group configuration items

Item	Description
Link group name	Enter a name for the link group, case insensitive.
Proximity	Enable or disable the proximity feature. Before enabling this function, you must configure proximity parameters from the **Policies** > **Load Balancing** > **Common Configuration** > **Proximity** > **Proximity Parameters** page. The generated proximity entries can be viewed on the **Policies** > **Load Balancing** > **Common Configuration** > **Proximity** > **Proximity Entries** page.
Scheduling algorithm	Select a scheduling algorithm for the link group. • **Weighted round-robin algorithm**—Distributes DNS requests to DNS servers in a round-robin manner according to the weights of DNS servers. A DNS server with a greater weight value is assigned more DNS requests. • **Random algorithm**—Distributes DNS requests to DNS servers randomly. • **Weighted least connection algorithm (least-connection)**—Always assigns user requests to the link with the fewest number of weighted active connections (the number of active connections divided by weight). • **Source IP address hash algorithm (hash address source)**—Hashes the source IP address of user requests and distributes user requests to different links according to the hash values. • **Source IP address and port hash algorithm (hash address source-ip-port)**—Hashes the source IP address and port number of user requests and distributes user requests to different links according to the hash values. • **Destination IP address hash algorithm (hash address destination)**—Hashes the destination IP address of user requests and distributes user requests to different links according to the hash values. • **Bandwidth algorithm (bandwidth)**—Distributes user requests to links according to the weights and remaining bandwidth of links. • **Maximum bandwidth algorithm (max-bandwidth)**—Distributes user requests always to an idle link that has the largest remaining bandwidth. • **Link quality algorithm**—Distributes new connections to links based

Item	Description
	on the link quality. The higher the quality, the more new connections assigned to the link. The link quality is calculated by using the network delay, hop count of routes, and packet loss ratio. By default, the source IP address hash algorithm is used.
Lower percentage	When the percentage of available links in a primary link group is smaller than the lower percentage value, the primary link group becomes unavailable, and the backup link group takes over.
Upper percentage	When the percentage of available links in a primary link group is greater than the upper percentage value, the primary link group becomes available again to process services. The upper percentage value must be greater than or equal to the lower percentage value.
Priority scheduling	Specify the upper limit and lower limit of links in a link group that can be scheduled. By default, all DNS servers with the highest priority in a link group are scheduled. • If the number of links with the highest priority is greater than the configured maximum number, the maximum number applies. • If the number of such links is less than the minimum number, links with lower priority are selected to meet the minimum number or until no links are available. The link priority can be configured on the **Links** page.
Probe method	Specify a probe template for the link group to detect the health and availability of its links. You can also configure this parameter for a single link on the **Links** page. The probe template specified for a single link has higher priority over that specified for a link group. You can select an existing probe template or create a probe template.
Success criteria	Specify the health monitoring success criteria for the link group. • **All probes succeed**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least n probes succeed**—Health monitoring succeeds when a minimum of the specified number of health monitoring methods succeed. When the specified number of health monitoring methods is greater than the number of health monitoring methods on the device, health monitoring succeeds if all health monitoring methods succeed.

Item	Description
Member list	You can add a link to a link group in one of the following ways: Create a link and add it to the link group. 3. Click **Add**, and select **Create link**. 4. Configure the parameters for the link (see "Configure a link"). 5. Click **OK**. The new link appears in the link list. Select an existing link. 6. Click **Add**, and select **Add existing link**. 7. Select a link from the list, and configure link parameters (see "Configure a link"). 8. Click **OK**. The link appears in the member list.
NAT	Enable or disable NAT. In outbound link load balancing, NAT typically needs to be disabled.
NAT	Enable or disable NAT. In link load balancing, NAT typically needs to be disabled.
Fault processing method	Select a fault processing method: • **Keep existing connections**—Does not actively terminate the connection with the failed link. Keeping or terminating the connection depends on the timeout mechanism of the protocol. • **Redirect connections**—Redirects the connection to another available link in the link group. • **Terminate existing connections**—Terminates the connection with the failed link by sending RST packets (for TCP packets) or ICMP unreachable packets (for other types of packets). By default, the fault processing method is **Keep existing connections**.
Description	Enter a description for the link group.

5. Click **OK**. The new link group appears in the **Link Group** page.

Configure a routing policy

A routing policy associates an LB class with an LB action to guide packet forwarding.

You can specify only one class in a routing policy. The device matches packets against routing policies in their configuration order. If a packet matches a class, the device takes the associated action on the packet. If a packet matches no class, the device takes the action associated with the system-defined class named **Default** on the packet.

Common procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Outbound Link Load Balancing** > **IPv4/IPv6 Routing Policy**.
2.
3. On the **IPv4/IPv6 Routing Policy** page, configure the common settings.

Table 3 Common configuration items

Item	Description
LB service	Enable or disable outbound link load balancing.
Link protection	Enable or disable link protection. If the traffic exceeds the bandwidth ratio of a link, the LB device distributes new traffic that does not match any sticky entries to other links.
Session extension information synchronization	Enable or disable session extension information synchronization.
Sticky entry synchronization	Enable or disable sticky entry synchronization.
Sticky entry synchronization	Select the sticky entry synchronization type:

Item	Description
type	• **Intra-group synchronization**—Synchronizes sticky entries to the device in the same failover group. • **Global synchronization**—Synchronizes sticky entries to devices in all failover groups. This function is available only when sticky entry synchronization is enabled.

Procedure for configuring an IPv4/IPv6 routing policy

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **DNS Proxy** > **IPv4/IPv6 Routing Policy**.
2.
3. Click **Create** on the **IPv4/IPv6 Routing Policy** page.
4. Create an IPv4/IPv6 routing policy.

Table 4 IPv4/IPv6 routing policy configuration items

Item	Description
Class	Select an existing class or create a class.
Forwarding action	Select a forwarding action: • Load balance • Discard • Forward
ToS	Enter the ToS field value in IP packets sent to the DNS server. IPv6 routing policies do not support this parameter.

Item	Description
Primary link group	Select an existing link group or create a link group. When the primary link group is available (contains available links), the device forwards packets through the primary link group. When the primary link group is not available, the device forwards packets through the backup link group.
Backup link group	Select an existing link group or create a link group.
Sticky group	Select an existing sticky group or create a sticky group. Only address-port sticky groups are supported.
Fallback action	Specify that the next rule is matched when a failure to find a link occurs.
Busy action	Specify that the next rule is matched when all links are busy.
Insert before	Specify an existing routing policy before which the new policy is inserted.

5. Click **OK**. The new routing policy appears on the **IPv4/IPv6 Routing Policy** page.

Inbound link load balancing

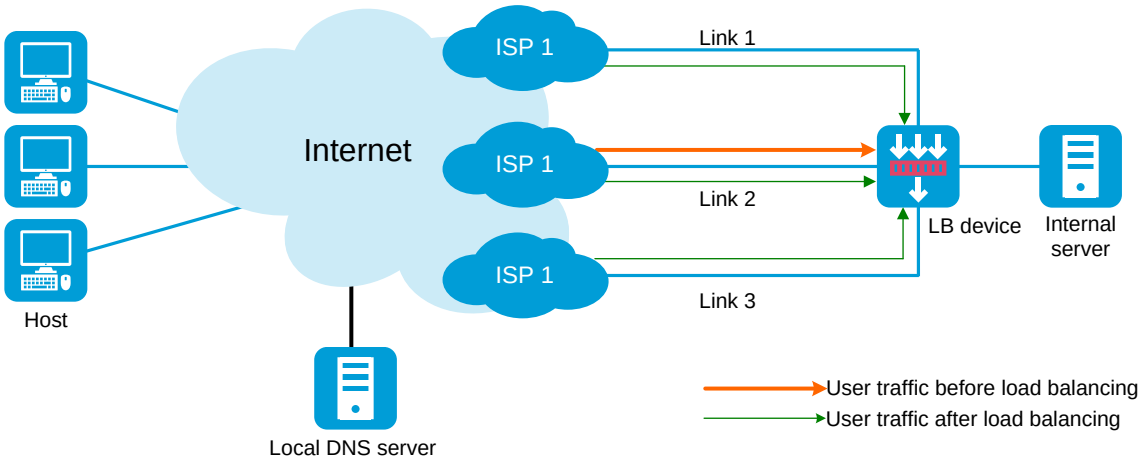
This help contains the following topics:

Introduction

How it works

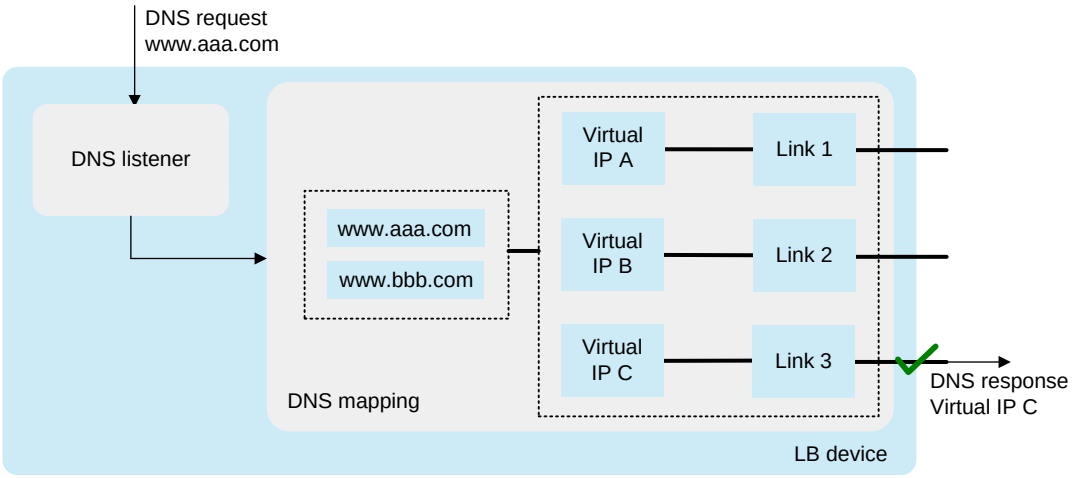
Inbound link load balancing load balances traffic among the links from the external network to the internal network. This feature provides link redundancy and increased link efficiency.

Figure 1 Network diagram



Workflow on the device

Figure 2 Workflow



When the device receives a DNS request with the destination IP address matching the DNS listener IP address, it queries the virtual IP addresses associated with the domain name in DNS mappings. Then, the device selects a virtual IP address for the best link according to the configured scheduling algorithm. The device sends the virtual IP address to the client in the outgoing DNS response. The client uses the virtual IP address as the destination IP address to access the internal server.

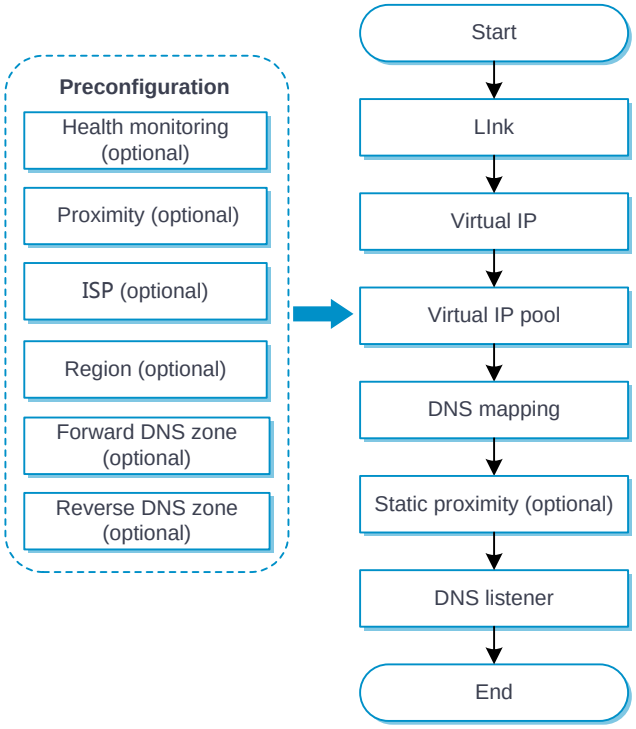
Restrictions and guidelines

To ensure correct operation of inbound link load balancing when server load balancing is also enabled, do not specify the virtual server's IP address as the DNS listener's IP address.

Configure inbound link load balancing

Figure 3 shows the configuration procedure for inbound link load balancing.

Figure 3 Inbound link load balancing configuration procedure



Configure health monitoring (optional)

The health monitoring configuration can be used by a link or link group.

For detailed steps required to configure health monitoring, see the online help for health monitoring.

Configure proximity (optional)

For detailed steps required to configure proximity, see the online help for load balancing common configuration.

Configure ISP information (optional)

For detailed steps required to configure ISP information, see the online help for load balancing common configuration.

Configure a region (optional)

For detailed steps required to configure regions, see the online help for load balancing common configuration.

Configure a forward DNS zone (optional)

During DNS resolution, an LB device looks up the resource records configured in a forward DNS zone for the host name corresponding to the target domain name. DNS resource records are used by an LB device to resolve DNS requests and have the following types:

- **Canonical name (CNAME)**—Maps multiple aliases to one host name (server). For example, an enterprise intranet has a server with host name **host.aaa.com**. The server provides both Web service and mail service. You can configure two aliases (**www.aaa.com** and **mail.aaa.com**) in a CNAME resource record for this server. When a user requests Web

service, the user accesses **www.aaa.com**. When a user requests mail service, the user accesses **mail.aaa.com**. Actually, the user accesses **host.aaa.com** in both cases.

- **Mail exchanger (MX)**—Specifies the mail server for a forward DNS zone.
- **Name server (NS)**—Specifies the authoritative DNS server for a forward DNS zone.
- **Start of authority (SOA)**—Specifies authoritative information about a forward DNS zone, including the primary DNS server and administrator mailbox.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Inbound Link Load Balancing** > **Forward DNS Zone**.
2. Click **Create** on the **Forward DNS Zone** page.
3. Create a forward DNS zone.

Table 1 Forward DNS zone configuration items

Item	Description
Zone name	Specifies a domain name for the forward DNS zone, a case-insensitive string of 1 to 253 characters. Each dot-separated part in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), and dots (.).
TTL	Specify the TTL for all resource records in the forward DNS zone.
Resource record list	1. Click **Create** to add a resource record. ○ **Type**—Select a resource type: MX, NS, or CNAME. ○ **Subname**—Specify a subname for the forward DNS zone, a case-insensitive, dot-separated string of 1 to 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. This parameter appears only if you have

Item	Description
	selected **MX** or **NS** from the **Type** list. ◦ **Mail server host name**—Specify the host name of the mail server, a case-insensitive, dot-separated string that contains a maximum 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. This parameter appears only if you have selected **MX** from the **Type** list. ◦ **Priority**—Specify the preference for the resource record, in the range of 0 to 65535. The smaller the value, the higher the priority. This parameter appears only if you have selected **MX** from the **Type** list. ◦ **Authoritative name server host name**—Specify the host name of the authoritative DNS server, a case-insensitive, dot-separated string that contains a maximum of 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. The smaller the value, the higher the priority. This parameter appears only if you have selected **NS** from the **Type** list. ◦ **Alias**—Specify an alias for a host name, a case-insensitive, dot-separated string that contains a maximum of 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. ◦ **Canonical name**—Specify the host name, a case-insensitive, dot-separated string that contains a maximum 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. This parameter appears only if you have selected **CNAME** from the **Type** list. ◦ **TTL**—Specify the TTL for the current resource record. 2. Click **Create**. The new resource record appears in the resource record list.
SOA configuration-Primary name server host name	Specify the host name for the primary DNS server, a case-insensitive and dot-separated string of up to 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. The host name of the primary DNS server can be a relative domain name (does not end with a dot) or an absolute domain name (ends with a dot). For an absolute domain name, the host name is not

Item	Description
	automatically expanded and cannot exceed 254 characters. For a relative domain name, the current domain name is automatically appended to the host name. The host name plus the appended domain name cannot exceed 254 characters.
SOA configuration-Administrator email address	Specify the email address of the administrator. The email address of the administrator can be a relative domain name (does not end with a dot) or an absolute domain name (ends with a dot). For an absolute domain name, the email address is not automatically expanded and cannot exceed 254 characters. For a relative domain name, the current domain name is automatically appended to the email address. The email address plus the appended domain name cannot exceed 254 characters.
SOA configuration-Serial number	Configure the serial number for a forward DNS zone. The serial number indicates the configuration order of a forward DNS zone. A newly configured forward DNS zone has a greater serial number than an old forward DNS zone. The secondary DNS server periodically queries the serial numbers of forward DNS zones on the primary DNS server and compares them with local serial numbers.
SOA configuration-Refresh interval	Specify the refresh interval. The secondary DNS server obtains SOA resource records from the primary DNS server at the refresh interval. After obtaining SOA resource records, the secondary DNS server compares them with the local SOA resource records.
SOA configuration-Retry interval	Specify the retry interval, which is the amount of time that the secondary DNS server waits after it fails to copy a forward DNS zone.
SOA configuration-Expiration time	Specify the expiration time for SOA resource records. The expiration time for SOA resource records is the amount of time that the secondary DNS server can work after it loses contact with the primary DNS server.
SOA configuration-Minimum TTL	Specify the minimum TTL, which is the amount of time that resource records on the primary DNS server are cached on the secondary DNS server.

4. Click **OK**. The forward DNS zone appears on the **Forward DNS Zone** page.

Configure a reverse DNS zone (optional)

The LB device performs reverse DNS resolution according to the reverse DNS zone configuration. Reverse DNS resolution searches for a domain name according to an IP address. The pointer record (PTR) resource records configured in a reverse DNS zone record mappings between domain names and IP addresses.

Reverse DNS resolution is used to address spam attacks by verifying the validity of the email sender. When a mail server receives an email from an external user, it sends a reverse DNS resolution request to the LB device. The LB device resolves the source IP address of the sender into a domain name according to PTR resource records and sends the domain name to the mail server. The mail server compares the received domain name with the actual domain name of the sender. If the two domain names match, the mail server accepts the email. If not, the mail server considers the email as a spam email and discards it.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Inbound Link Load Balancing** > **Reverse DNS Zone**.
2. Click **Create** on the **Reverse DNS Zone** page.
3. Create a reverse DNS zone.

Table 2 Reverse DNS zone configuration items

Item	Description
Type	Specify a zone type: IPv4 or IPv6.
IPv4 address	Specify an IPv4 address for the reverse DNS zone. This parameter appears only if you have selected **IPv4** from the **Type** list.

Item	Description
IPv6 address	Specify an IPv6 address for the reverse DNS zone. This parameter appears only if you have selected **IPv6** from the **Type** list.
Mask	Specify the mask length for the reverse DNS zone. This parameter appears only if you have selected **IPv4** from the **Type** list.
Prefix	Specify the prefix length for the reverse DNS zone. This parameter appears only if you have selected **IPv6** from the **Type** list.
PTR resource record list	1. Click **Create** to add a PTR resource record. ◦ **IPv4 address**—Specify an IPv4 address. The IPv4 address specified in a PTR resource record must be within the IPv4 address range of the reverse DNS zone. This parameter appears only if you have selected **IPv4** from the **Type** list. ◦ **IPv6 address**—Specify an IPv6 address. The IPv6 address specified in a PTR resource record must be within the IPv6 address range of the reverse DNS zone. This parameter appears only if you have selected **IPv6** from the **Type** list. ◦ **Domain name**—Specify a domain name, a case-insensitive, dot-separated string that contains a maximum of 253 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. ◦ **TTL**—Specify the TTL for the resource record. 2. Click **OK**. The new PTR resource record appears in the PTR resource record list.

4. Click **OK**. The reverse DNS zone appears on the **Reverse DNS Zone** page.

Configure a link

For detailed steps required to configure links, see the online help for load balancing common configuration.

Configure a DNS mapping

By configuring a DNS mapping, you can associate a domain name with virtual IP addresses/virtual servers. The LB device can obtain the virtual IP addresses/virtual servers associated with the domain name in a DNS request and select one virtual IP address/virtual server according to the configured scheduling algorithm.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Inbound Link Load Balancing** > **DNS Mapping**.
2. Click **Create** on the **DNS Mapping** page.
3. Create a DNS mapping.

Table 3 DNS mapping configuration items

Item	Description
DNS mapping name	Enter a name for the DNS mapping, case insensitive.
Domain name list	1. Enter a domain name, a case-insensitive string of 1 to 253 characters. Each dot-separated label in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), dots (.), and wildcards (asterisks and question marks). Dots cannot be used as the start and end characters. When you use wildcards (asterisks and question marks) in a domain name, follow these guidelines: o The wildcards can substitute any characters except for dots (.). o An asterisk (*) can substitute a character string. o A question mark (?) can substitute a single character. 2. Click **Add**. The added domain name appears in the domain name list.

Item	Description

Virtual IP/Virtual server list	1. Click **Create** to add a virtual IP address or virtual server.
	  ○ **Virtual server**—Specify a virtual server. You can select an existing virtual server or create a virtual server.
	  ○ **Virtual IP address**—Configure a virtual IP address. In a scenario where server load balancing is not required, configure only a virtual IP address instead of both a virtual IP address and a virtual server.
	  ○ **Link**—Specify a link to associate with the virtual server or virtual IP address. You can select an existing link or create a link.
	  ○ **Weight**—Specify the weight for the virtual server or virtual IP address. For the weighted round robin and weighted least connections algorithms, a greater value means a higher priority to be referenced.
	2. Click **OK**. The new virtual server or virtual IP address appears in the virtual server/virtual IP list.

Preferred predictor	Specify the preferred predictor for virtual IP addresses/virtual servers. The preferred predictor has the highest priority. If no virtual IP address/virtual server can be selected by using the preferred predictor, the alternative predictor is used to select a virtual IP address/virtual server. If no virtual IP address/virtual server can be selected by using the alternative predictor, the backup predictor is used to select a virtual IP address/virtual server. You can specify one of the following predictors as the preferred predictor: • **Weight round robin**—Assigns DNS requests to virtual IP addresses/virtual servers based on the weights of virtual IP addresses/virtual servers. A higher weight indicates more DNS requests will be assigned. • **Random**—Randomly assigns DNS requests to virtual IP addresses/virtual servers. • **Weighted least connections**—Always assigns DNS requests to the virtual IP addresses/virtual server with the fewest number of weighted active connections (the number of active connections divided by weight). • **Static proximity**—Assigns DNS requests to virtual IP addresses/virtual servers based on static proximity entries. • **Dynamic proximity**—Assigns DNS requests to virtual IP addresses/virtual servers based on dynamic proximity entries. • **Hash source IP address**—Hashes the source IP address of DNS requests and distributes DNS requests to different virtual IP

Item	Description
	addresses/virtual servers according to the hash values. • **Hash source IP address and port number**—Hashes the source IP address and port number of DNS requests and distributes DNS requests to different virtual IP addresses/virtual servers according to the hash values. • **Hash destination IP address**—Hashes the destination IP address of DNS requests and distributes DNS requests to different virtual IP addresses/virtual servers according to the hash values. • **Bandwidth**—Distributes DNS requests to virtual IP addresses/virtual servers according to the weights and remaining bandwidth of them. • **Max bandwidth**—Distributes DNS requests always to an idle virtual IP address/virtual server that has the largest remaining bandwidth. By default, the weighted round robin algorithm is used.
Alternative predictor	Specify the alternative predictor. The supported predictors are the same as those supported by the preferred predictor.
Backup predictor	Specify the backup predictor. The supported predictors are the same as those supported by the preferred predictor.
Link protection	Enable or disable link protection. This feature enables the device to select a virtual IP address based on the bandwidth ratio of the associated link. If the bandwidth ratio of a link is exceeded, the virtual IP address is not selected. You can set the bandwidth ratio of a link on the **Links** page.
TTL	Specify the TTL value in the range of 0 to 4294967295 seconds. This time is the amount of time that DNS records are cached for DNS responses. For the DNS client to get the updated DNS record when the virtual IP configuration changes, set a smaller TTL value, for example, 60 seconds. For stable, fast domain name resolution when the network is stable, set a larger TTL value, for example, 86400 seconds.
DNS mapping	Enable or disable DNS mapping.

4. Click **OK**. The new DNS mapping appears on the **DNS Mapping** page.

Configure static proximity

A static proximity policy associates the region where the local DNS server resides with the IP address range of a virtual IP. When the static proximity algorithm is specified in a DNS mapping, you must configure a static proximity policy.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Inbound Link Load Balancing** > **Static Proximity**.
2. Click **Create** on the **Static Proximity** page.
3. Create a static proximity policy.

Table 4 Static proximity policy configuration items

Item	Description
Region name	Select an existing region or create a region.
Address range	Specify an IPv4 address range in the form of IPv4 address/Mask length or an IPv6 address range in the form of IPv6 address/Prefix length. The mask length is in the range of 0 to 32. If the mask length is 32, the most significant eight bits must be smaller than 224 and cannot be 0 or 127. The prefix length is in the range of 0 to 128.
Priority	Specify a priority value. When a DNS request matches multiple static proximity policies, the static proximity policy with the greatest priority value is selected.

4. Click **OK**. The new static proximity policy appears on the **Static Proximity** page.

Configure a DNS listener

A DNS listener listens DNS requests on the LB device. If the destination address of a DNS request matches the address being listened, inbound link load balancing is performed. The LB device searches for the address-to-domain name mapping, and obtains the virtual IP address corresponding to the domain name. The LB device sends the virtual IP address to the user in a DNS response before the user can establish a connection to the server.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **Inbound Link Load Balancing** > **DNS Listener**.
2. Click **Create** on the **DNS Listener** page.
3. Create a DNS listener.

Table 5 DNS listener configuration items

Item	Description
DNS listener name	Enter a name for the DNS listener, case insensitive.
IPv4 address	Specify an IPv4 for the DNS listener. The IPv4 address cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.
IPv6 address	Specify an IPv6 for the DNS listener. The IPv6 address cannot be a loopback address, multicast address, link-local address, or all-zero address.
Port number	Specify a port number for the DNS listener.
VRF	Select an existing VPN instance or create a VPN instance.

Item	Description
	A created VPN instance can be viewed from **Network** > **VRF**.
DNS listening	Enable or disable DNS listening.
Processing for nonexistent domain	Specify a processing method for DNS mapping search failure. • Do not respond • Respond with a DNS reject • Respond through a DNS proxy

4. Click **OK**. The new DNS listener appears on the **DNS Listener** page.

Transparent DNS proxy

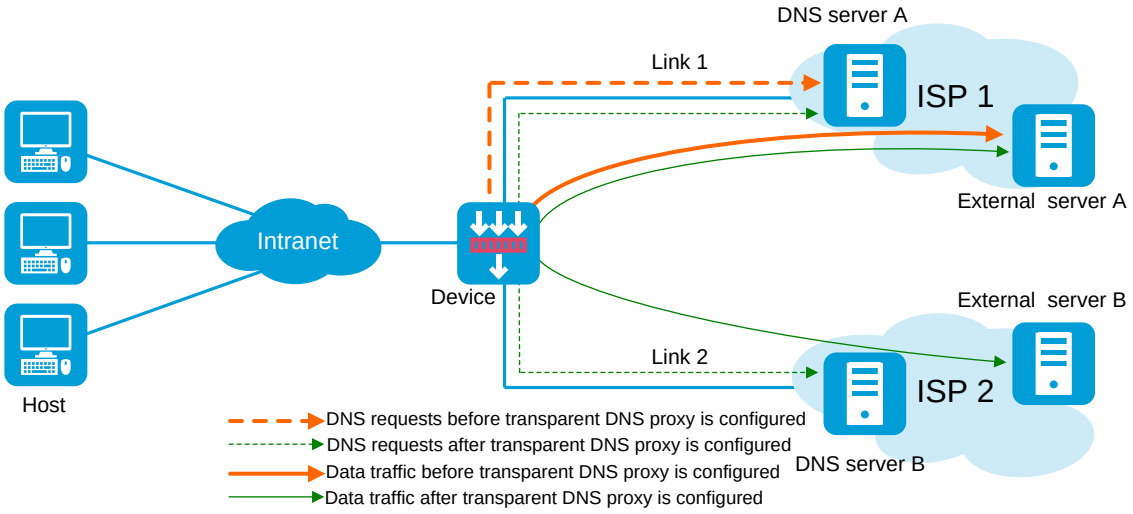
This help contains the following topics:

Introduction

As shown in Figure 1, intranet users of an enterprise can access external servers A and B through link 1 of ISP 1 and link 2 of ISP 2. External servers A and B provide the same services. All DNS requests of intranet users are forwarded to DNS server A, which returns the resolved IP address of external server A to the requesting users. In this way, all traffic of intranet users is forwarded on one link. Link congestion might occur.

The transparent DNS proxy feature can solve this problem by forwarding DNS requests to DNS servers in different ISPs. All traffic from intranet users is evenly distributed on multiple links. This feature can prevent link congestion and ensure service continuity upon a link failure.

Figure 1 Transparent DNS proxy



Transparent DNS proxy workflow

The transparent DNS proxy is implemented by changing the destination IP address of DNS requests.

As shown in Figure 2, if the destination port number of an incoming DNS request is the same as the port number specified for a transparent DNS proxy, the device processes the DNS request as follows:

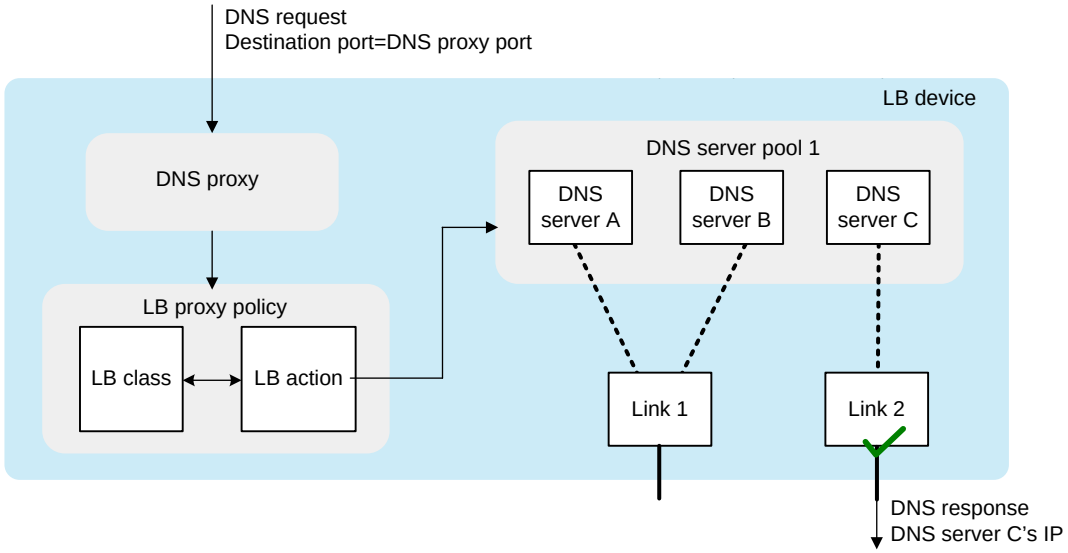
1. Finds the DNS server pool associated with the transparent DNS proxy.
2. Selects a DNS server to service the DNS request according to the scheduling algorithm of the associated DNS server pool.

   The IP address of the selected DNS server is used as the destination IP address of the DNS request.

The DNS server resolves the domain name in the DNS request into the IP address of the external server sends a DNS response.

The intranet user accesses the external server according to the resolved IP address in the DNS response.

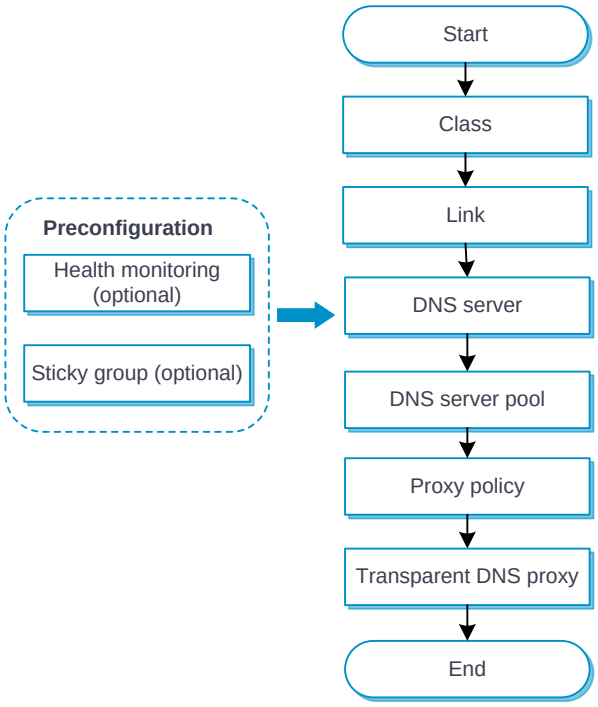
Figure 2 Transparent DNS proxy workflow



Configure transparent DNS proxy

Figure 3 shows the configuration procedure for transparent DNS proxy.

Figure 3 Transparent DNS proxy configuration procedure



Configure health monitoring (optional)

The health monitoring configuration can be used by a DNS server or DNS server pool.

For detailed steps required to configure health monitoring, see the help for load balancing common configuration.

Configure a sticky group (optional)

A sticky group can be used by an IPv4 or IPv6 proxy policy.

For detailed steps required to configure sticky groups, see the help for load balancing common configuration.

Configure a class

A class classifies packets by comparing packets against specific rules. Matching packets are further processed by LB actions.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **DNS Proxy** > **Class**.
2. Click **Create** on the **Class** page.
3. Create a class.

Table 1 Class configuration items

Item	Description
Class name	Enter a name for the class, case insensitive.
Match type	Select a match type: • **Match any**—A packet matches a class if it matches any of the rules in the class. • **Match all**—A packet matches a class if it matches all rules in the class.
Match rule	A class can contain a maximum of 65535 match rules. To configure a match rule: 1. Click **Create**, and configure the following items on the **Create Match Rule** page: ○ **Rule ID**—Enter a rule ID. Rules are matched in ascending order of rule IDs. ○ **Type**—Select a rule type. Options include **Source IPv4 address**, **Source IPv6 address**, **Destination IPv4 address**, **Destination IPv6 address**, **Class**, **IPv4 ACL**, **IPv6 ACL**, **Domain name**, **User**, **and Input interface**. ○ **IPv4 address**—Specify the IPv4 address to match. This parameter appears only if you have selected **Source IPv4 address** or **Destination IPv4 address** from the **Type** list.

Item	Description
	◦ **Mask length**—Specify the mask length for the IPv4 address. This parameter appears only if you have selected **Source IPv4 address** or **Destination IPv4 address** from the **Type** list. ◦ **IPv6 address**—Specify the IPv6 address to match. This parameter appears only if you have selected **Source IPv6 address** or **Destination IPv6 address** from the **Type** list. ◦ **Prefix length**—Specify the prefix length for the IPv6 address. This parameter appears only if you have selected **Source IPv6 address** or **Destination IPv6 address** from the **Type** list. ◦ **Class**—Specify the class to match. This parameter appears only if you have selected **Class** from the **Type** list. ◦ **IPv4 ACL**—Specify the IPv4 ACL to match. You can select an existing ACL or create an ACL. This parameter appears only if you have selected **IPv4 ACL** from the **Type** list. ◦ **IPv6 ACL**—Specify the IPv6 ACL to match. You can select an existing ACL or create an ACL. This parameter appears only if you have selected **IPv6 ACL** from the **Type** list. ◦ **Domain name**—Specify the domain name to match. The domain name is a case-insensitive string of 1 to 253 characters. Each dot-separated part in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), dots (.), and wildcards (asterisks (*) and question marks (?)).The wildcards can substitute any characters except for dots (.). An asterisk (*) can substitute a character string. A question mark (?) can substitute a single character. This parameter appears only if you have selected **Domain name** from the **Type** list. ◦ **User**—Specify the user or user group to match. You can select an existing user or user group or create a user or user group. This parameter appears only if you have selected **User** from the **Type** list. ◦ **Input interface**—Specify the input interface to match. This parameter appears only if you have selected **Input interface** from the **Type** list. 2. Click **OK**. The new match rule appears in the match rule list.

Item	Description
Description	Enter a description for the class.

4. Click **OK**. The new class appears on the **Class** page.

Configure a link

For detailed steps required to configure links, see the help for load balancing common configuration.

Configure a DNS server

Perform this task to configure an entity on the LB device for processing DNS requests. DNS servers configured on the LB device correspond to DNS servers in ISP networks. A DNS server can belong to multiple DNS server pools. A DNS server pool can contain multiple DNS servers.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **DNS Proxy** > **DNS Server**.
2. Click **Create** on the **DNS Server** page.
3. Create a DNS server.

Table 2 DNS server configuration items

Item	Description
DNS server name	Enter a name for the DNS server, case insensitive.
IP address configuration method	Select an IP address configuration method:

Item	Description
	• **Manual**. • **Automatic**—To use this method, an outgoing interface must be specified on the **Create Link** page.
IPv4 address	Enter an IPv4 address for the DNS server. The IPv4 address cannot be a loopback address, multicast address, broadcast address, or 0.X.X.X.
IPv6 address	Enter an IPv6 address for the DNS server. The IPv6 address cannot be a loopback address, multicast address, link-local address, or all-zero address.
Port number	Enter a port number for the DNS server. The value 0 means the port number carried in the packet is used.
Weight	Enter a weight for the DNS server. A DNS server with a greater weight value has a higher priority than a DNS server with a smaller weight value.
Priority	Enter a priority for the DNS server in the DNS server pool. A DNS server with a greater priority value has a higher priority than a DNS server with a smaller priority value. If the number of DNS servers with the highest priority is smaller than the configured minimum number, DNS servers with lower priority are selected to meet the minimum number or until no DNS servers are available. You can configure the maximum number and minimum number on the **DNS Server Pool** page.
Probe method	Specify a probe template used by the DNS server to detect health and availability. You can also configure this parameter for all DNS servers in a DNS server pool on the **DNS Server Pool** page. The configuration performed on the **DNS Server** page has higher priority over that performed on the **DNS Server Pool** page. You can select an existing probe template or create a probe template.
Success criteria	Specify the health monitoring success criteria for the DNS server. • **All probes succeed**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least n probes succeed**—Health monitoring succeeds

Item	Description
	when a minimum of the specified number of health monitoring methods succeed. When the specified number of health monitoring methods is greater than the number of health monitoring methods on the device, health monitoring succeeds if all health monitoring methods succeed.
Link	Specify a link to associate with the DNS server. You can select an existing link or create a link.
Description	Enter a description for the DNS server.

4. Click **OK**. The new DNS server appears on the **DNS Server** page.

Configure a DNS server pool

By configuring a DNS server pool, you can perform centralized management on DNS servers that have similar functions.

Procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **DNS Proxy** > **DNS Server Pool**.
2. Click **Create** on the **DNS Server Pool** page.
3. Create a DNS server pool.

Table 3 DNS server pool configuration items

Item	Description
Pool name	Enter a name for the DNS server pool, case insensitive.
Scheduling algorithm	Select a scheduling algorithm for the DNS server pool. • **Bandwidth algorithm**—Distributes DNS requests to DNS

Item	Description
	servers according to the weights and remaining bandwidths of DNS servers. When the remaining bandwidths of two DNS servers are the same, this algorithm is equivalent to the round-robin algorithm. When the weights of two DNS servers are the same, this algorithm always distributes DNS requests to the DNS server that has larger remaining bandwidth. • **Random algorithm**—Distributes DNS requests to DNS servers randomly. • **Weighted round-robin algorithm**—Distributes DNS requests to DNS servers in a round-robin manner according to the weights of DNS servers. A DNS server with a greater weight value is assigned more DNS requests. • **Maximum bandwidth algorithm**—Distributes DNS requests always to an idle DNS server that has the largest remaining bandwidth. • **Source IP address hash algorithm**—Hashes the source IP address of DNS requests and distributes DNS requests to different DNS servers according to the hash values. • **Source IP address and port hash algorithm**—Hashes the source IP address and port number of DNS requests and distributes DNS requests to different DNS servers according to the hash values. • **Destination IP address hash algorithm**—Hashes the destination IP address of DNS requests and distributes DNS requests to different DNS servers according to the hash values. By default, the bandwidth algorithm is used.
Priority scheduling	Specify the upper limit and lower limit of DNS servers in a DNS server pool that can be scheduled. By default, all DNS servers with the highest priority in a DNS server pool are scheduled. • If the number of DNS servers with the highest priority is greater than the configured maximum number, the maximum number applies. • If the number of such DNS servers is less than the minimum number, DNS servers with lower priority are selected to meet the minimum number or until no DNS servers are available. The DNS server priority can be configured on the **DNS Server** page.
Health monitoring method	Specify a probe template used by the DNS server pool to detect the health and availability of its DNS servers. You can also configure this parameter for a single DNS server on the **DNS Server Pool** page. The configuration performed on the **DNS Server** page has

Item	Description
	higher priority over that performed on the **DNS Server Pool** page. You can select an existing probe template or create a probe template.
Success criteria	Specify the health monitoring success criteria for the DNS server pool. • **All probes succeed**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least n probes succeed**—Health monitoring succeeds when a minimum of the specified number of health monitoring methods succeed. When the specified number of health monitoring methods is greater than the number of health monitoring methods on the device, health monitoring succeeds if all health monitoring methods succeed.
DNS server list	You can add a DNS server to a DNS server pool in one of the following ways: Create a DNS server and add it to the DNS server pool. 3. Click **Add**, and select **Create DNS server**. 4. Configure the parameters for the DNS server (see "Configure a DNS server"). 5. Click **OK**. The new DNS server appears in the DNS server list. Select an existing DNS server. 6. Click **Add**, and select **Select existing DNS server**. 7. Select a DNS server from the list, and configure DNS server parameters (see "Configure a DNS server"). 8. Click **OK**. The DNS server appears in the DNS server list.
Description	Enter a description for the DNS server pool.

4. Click **OK**. The new DNS server pool appears on the **DNS Server Pool** page.

Configure a proxy policy

A proxy policy associates a class and an action. You can specify an action to take on a class of packets in a proxy policy.

You can specify only one class in a proxy policy. The device matches packets against proxy policies in their configuration order. If a packet matches a class, the device takes the associated action on the packet. If a packet matches no class, the device takes the action associated with the system-defined class named **Default** on the packet.

Common procedure

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **DNS Proxy** > **IPv4/IPv6 Proxy Policy**.
2. On the **IPv4/IPv6 Proxy Policy** page, configure the common settings.

Table 4 Common configuration items

Item	Description
Status	Status of the transparent DNS proxy: • Available. • Unavailable. Please check the configuration.
Proxy port	Enter a proxy port number. If the destination port number of an incoming DNS request is the same as the proxy port number, the device performs the transparent DNS proxy on the DNS request.
Transparent DNS proxy	Enable or disable the transparent DNS proxy feature. IPv6 proxy policies do not support this parameter.
Link protection	Enable or disable the link protection feature. This feature enables a transparent DNS proxy to select a DNS server based on the link bandwidth ratio. If the bandwidth ratio of a link is exceeded, the DNS server is not selected.
Session extension	Enable or disable session extension information

Item	Description
information synchronization	synchronization.
Sticky entry synchronization	Enable or disable sticky entry synchronization. The following configuration changes will cause the device to delete existing sticky entries and generate new ones based on subsequent traffic: • Disable sticky entry synchronization. • Change the sticky entry synchronization type.
Sticky entry synchronization type	Select the sticky entry synchronization type: • **Intra-group synchronization**—Synchronizes sticky entries to the device in the same failover group. • **Global synchronization**—Synchronizes sticky entries to devices in all failover groups. This function is available only when sticky entry synchronization is enabled.

Procedure for configuring an IPv4/IPv6 proxy policy

1. Select **Policies** > **Load Balancing** > **Link Load Balancing** > **DNS Proxy** > **IPv4/IPv6 Proxy Policy**.
2. Click **Create** on the **IPv4/IPv6 Proxy Policy** page.
3. Create an IPv4/IPv6 proxy policy.

Table 5 IPv4/IPv6 proxy policy configuration items

Item	Description
Class	Select an existing class or create a class.
Forwarding action	Select a forwarding action. • Load balance

Item	Description
	• Discard • Forward • Skip the transparent DNS proxy
ToS	Enter the ToS field value in IP packets sent to the DNS server.
DNS server pool	Select an existing DNS server pool or create a DNS server pool.
Sticky group	Select an existing sticky group or create a sticky group. Only address-port sticky groups are supported.
Fallback action	Specify that the next rule is matched when a failure to find a DNS server occurs.
Busy action	Specify that the next rule is matched when all DNS servers are busy.
Insert before	Specify an existing proxy policy before which the new policy is inserted.

4. Click **OK**. The new proxy policy appears on the **IPv4/IPv6 Proxy Policy** page.

NetShare control

This help contains the following topics:

Introduction

NetShare control allows you to identify and control network sharing behaviors.

Basic concepts

Max terminals per IP

This item specifies the maximum number of terminals that can share an IP address.

NetShare control determines the action for a packet based on the number of terminals sharing the source IP address of the packet:

- If the number of terminals sharing the IP address exceeds the limit, the action specified in the NetShare policy is taken.
- If the number of terminals sharing the IP address is below the limit, the packet is permitted to pass through.

Freeze and unfreeze

When an IP address is frozen, all packets sourced from the IP address will be dropped.

The device automatically freezes an IP address for the freezing time when the following conditions are met:

- The number of terminals sharing the IP address exceeds the limit of **Max terminals per IP**.
- The **Freeze** action is configured for IP addresses shared by terminals exceeding the limit of **Max terminals per IP**.

You can also manually freeze and unfreeze an IP address on the **NetShare Control** > **NetShare List** page.

NetShare list

The NetShare list lists all IP addresses that are detected to be shared by terminals and their related information, including:

- Position.
- User name.
- VRF.
- Number of terminals sharing the IP address.
- NetShare policy name.
- Whether the IP address is frozen and if yes, the remaining time before expiration of the freezing time.

You can access the NetShare list by selecting **NetShare Control** > **NetShare List** in the navigation pane.

NetShare detection methods

The following methods are available for detecting networking sharing behaviors of terminals:

- **APR-based detection**—The device extracts the application information in packets based on Application Recognition (APR) to detect NetShare behaviors.
- **IPID trail tracking**—The device tracks the values of the IPID fields in packets to detect NetShare behaviors.

  Packets sent by the same host contain incremented IPID values of a unique sequential pattern that starts at a random number. NetShare control tracks the IPID values of packets sourced from the same IP address. If the IPID values in the packets within a time period belong to the same unique sequential pattern, only one terminal is using the IP address. If the IPID values belong to different sequential patterns, the source IP address is shared by multiple terminals.

NetShare control mechanism

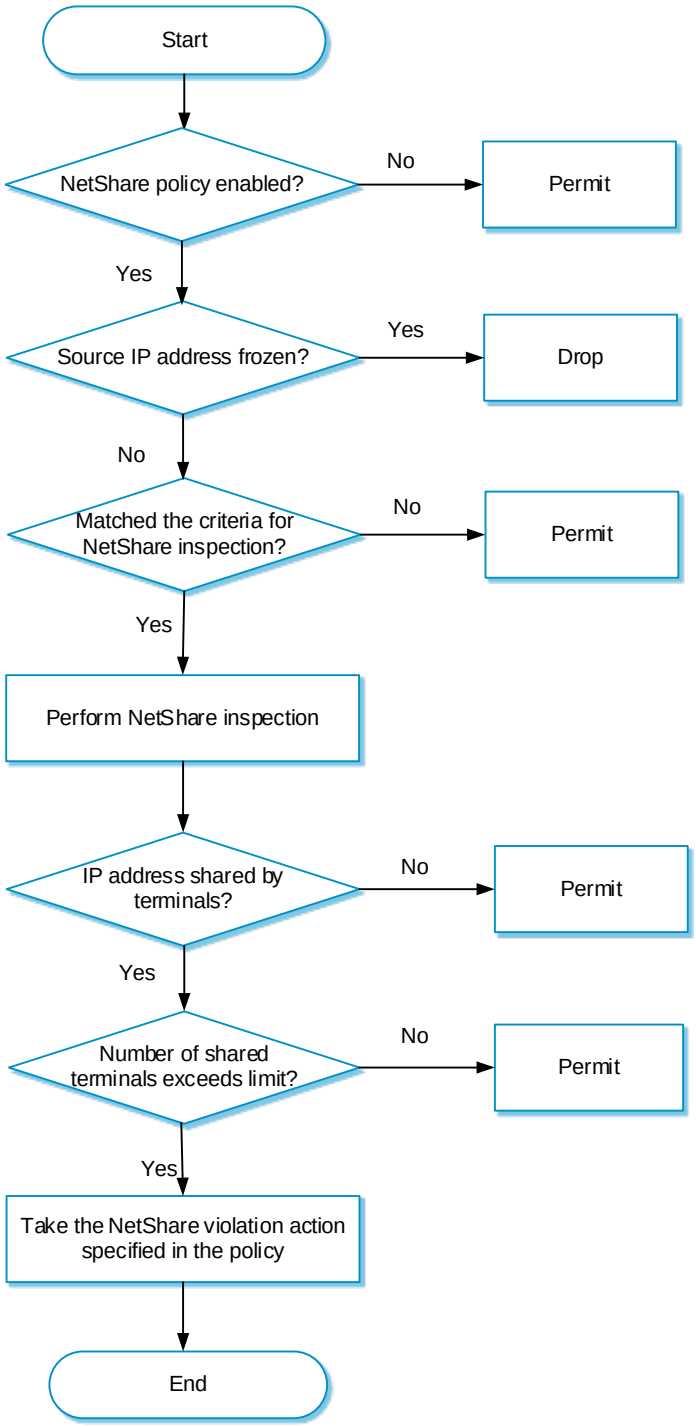
As shown in Figure 1, the NetShare control module processes a packet as follows:

1. Determines if the NetShare policy is enabled.
   - If the policy is disabled, NetShare control permits the packet to pass through.
   - If the policy is enabled, NetShare control proceeds to step 2.
2. Determines if the source IP address of the packet is frozen,

- If yes, NetShare control drops the packet.
- If not, NetShare control proceeds to step 3.

3. Compares the packet with the filters in the NetShare policy to determine if the packet matches the policy.
   - If the packet does not match the policy, NetShare control permits the packet to pass through.
   - If the packet matches the policy, NetShare control proceeds to step 4.
4. Determines if the source IP address of the packet is shared by multiple terminals:
   - If not, NetShare control permits the packet to pass through.
   - If yes, NetShare control further determines whether the number of terminals sharing the IP address exceeds the limit of **Max terminals per IP**:
     - If the limit is exceeded, NetShare control takes the action specified in the NetShare policy.
     - If the limit is not exceeded, NetShare control permits the packet to pass through.

Figure 1 NetShare control mechanism



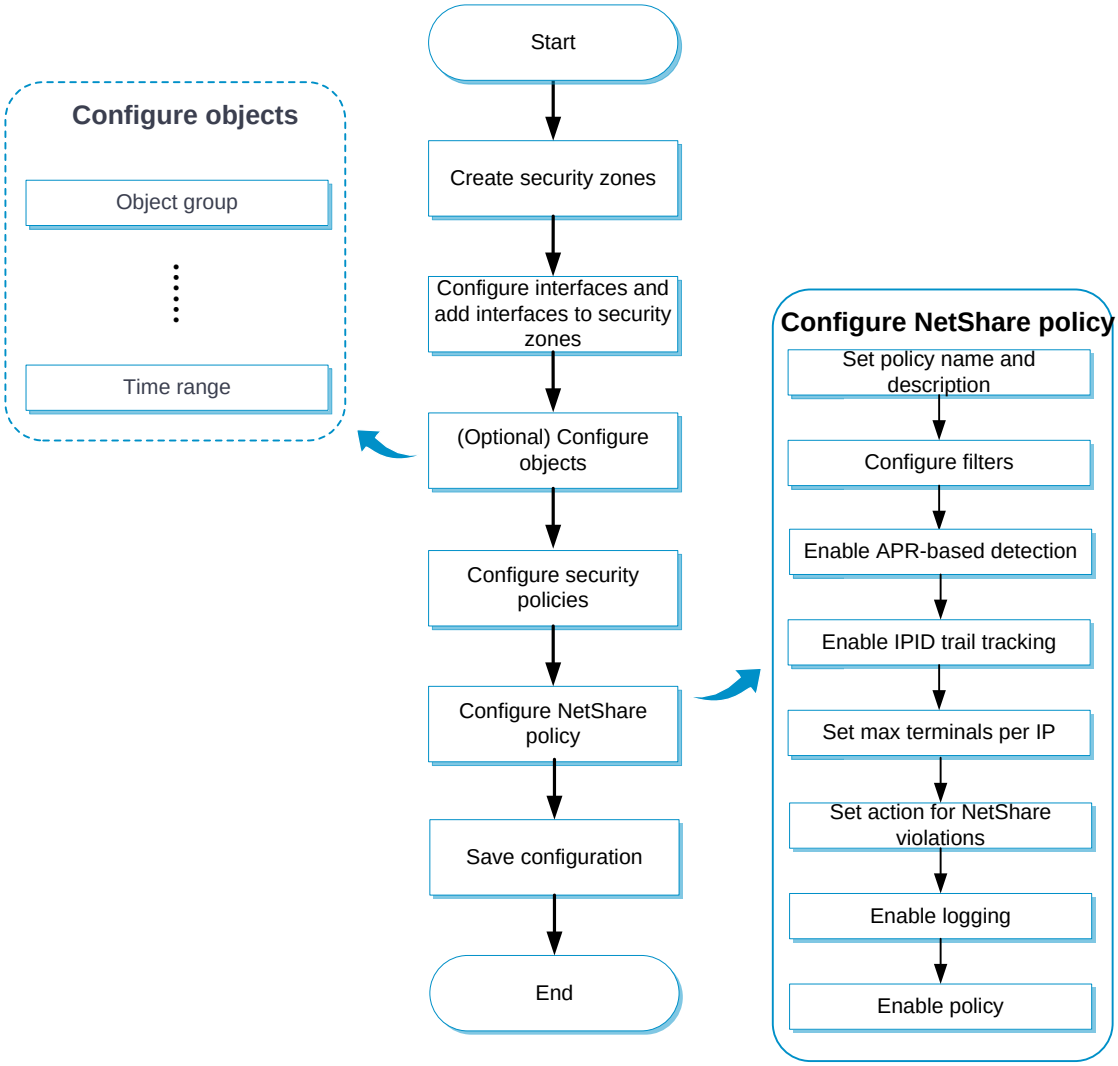
Restrictions and guidelines

- After you create or delete a NetShare policy, the NetShare policy must be activated to take effect. You can click **Submit** to activate the configuration immediately or the configuration will be activated automatically after 40 seconds by default. Clicking **Submit** might temporarily interrupt the DPI service processing, and interrupt other DPI-based services as a result. For example, security policies cannot implement application access control.
- NetShare control applies only to traffic permitted by security policies. For more information about security policies, see security policy help.
- Before using this feature, upgrade the APR signature library to the latest version.
- The device supports only one NetShare control policy, which must be manually created.
- When you use the APR-based detection to detect NetShare behaviors, follow these rules:
  - This detection method only inspects specific applications, such as QQ and WeChat.
  - If an application is encrypted, this detection method cannot inspect it.
- When you use the IPID trail tracking to detect NetShare behaviors, follow these rules:
  - This feature supports detecting the terminals that are running the Windows system, and detecting packets in which values of the IPID fields change regularly. Mobile terminals are not supported.
  - This detection method supports inspecting IPv4 packets.

Configure NetShare control

Configure NetShare control as shown in Figure 2.

Figure 2 NetShare control configuration procedure



Configure a NetShare policy

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **NetShare Control** > **NetShare Policy**.

3. Create a NetShare policy.

Table 1 NetShare policy configuration items

Item	Description
Name	Enter a name for the NetShare policy.
Description	Enter a description for the NetShare policy.
Src security zones	Specify the source security zones to which the policy applies.
Dst security zones	Specify the destination security zones to which the policy applies.
Src IP addresses	Specify the source IP addresses to which the policy applies.
Dst IP addresses	Specify the destination IP addresses to which the policy applies.
User	Specify the users to whom the policy applies.
APR-based detection	Select whether to enable APR-based detection. This feature detects NetShare behaviors based on APR.
IPID trail tracking	Select whether to enable IPID trail tracking. This feature tracks the values of the IPID fields in packets to detect NetShare behaviors.
Max terminals per IP	Enter the maximum number of terminals that can share the same IP address.
Action	Select the action to take when the number of terminals sharing an IP address exceeds the limit. Options are: • **Permit**—Permits the packet to pass through. • **Freeze**—Freezes the IP address so all packets sourced from the IP address will be dropped.
Freezing time	This item is required only when the **Freeze** action is selected. Enter the number of minutes an IP address will be frozen.

Item	Description
Logging	Select whether to enable NetShare control logging. When an IP address is detected to be shared by an excessive number of terminals (exceeding the limit of **Max terminals per IP**), the device generates a log message to record the IP address and the NetShare policy information.
Status	Enable or disable the NetShare policy. The policy takes effect only after you enable it.

4. Click **OK**.

   The new NetShare policy must be activated to take effect. You can click **Submit** to activate the configuration immediately or the configuration will be activated automatically after 40 seconds by default.

Server connection detection

This help contains the following topics:

Introduction

Server connection detection (SCD) enables the device to identify and classify legal and illegal connections initiated by given servers based on user-defined rules. This helps the administrators to monitor internal servers and prevent them from becoming part of a botnet and launching attacks or performing internal network penetration.

Configure SCD

SCD configuration involves the following tasks:

- **Configure SCD learning**—Configure the device to learn connections initiated by given servers. The learning results provide the basis for administrators to create SCD policies to monitor and log illegal connections initiated by the servers.

- **Configure SCD policies**—Create an SCD policy for a server and configure SCD rules to define the legal connections initiated by the server. The device can then log connections initiated by the server that do not match the SCD rules.

Configure SCD learning

Perform this task to enable the device to learn connections initiated by given servers.

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Server Connection Detection**.
3. Click the **SCD Learning** tab.
4. Enter the IP addresses of the servers for server-initiated connection learning and set the learning period.
5. Click **Start**.

   The device starts to learn the connections initiated by the specified servers for the specified learning period and displays the learning results in a list.
6. To set a server-initiated connection as a legal connection, select the connection and click **Create SCD rule**.

   The device automatically creates an SCD policy for the server and creates an SCD rule for the selected server connection in the policy.

Configure an SCD policy

Perform this task to create an SCD policy.

Procedure

1. Click the **Policies** tab.
2. In the navigation pane, select **Server Connection Detection**.
3. Click the **SCD Policy** tab.
4. Click **Create**.
5. Create an SCD policy.

Table 1 SCD policy configuration items

Item	Description
Policy name	Enter a name for the SCD policy.
Server address	Enter a server IP address. The SCD policy will monitor connections initiated by the server.
Enable policy	Select whether to enable the SCD policy.
Logging	Select whether to log connections initiated by the server that do not match any SCD rules.
SCD rules	Each SCD rule defines a set of legal connections initiated by the server. Connections initiated by the server that do not match any SCD rules are considered illegal. To create an SCD rule: 1. Click **Create**. 2. Enter the destination IP address for the connections.

Item	Description
	3. Set the protocols and port numbers for the connections. • A minimum of one protocol must be configured for an SCD rule. 4. Click **OK**.

Application proxy

This help contains the following topics:

Introduction

The device supports TCP proxy and SSL proxy functions. You can configure a proxy policy and set the policy action to **TCP-proxy** or **SSL-decryption**.

- For traffic matching a proxy policy with the action set to **TCP-proxy**, the device acts as the TCP proxy and provides TCP-layer isolation for network traffic.
- For traffic matching a proxy policy with the action set to **SSL-decryption**, the device acts as an SSL proxy to decrypt the SSL traffic and implement deep packet inspection on the traffic.

Filtering criteria in a proxy policy

You can configure the following types of criteria to filter the traffic to which a proxy policy applies:

- Source security zone.
- Destination security zone.
- Source IP address.
- Destinations IP address.
- User.
- Service.

Each filtering criteria type can contain multiple filtering criteria. A packet matches a filtering criteria type if it matches a filtering criterion of the type.

A packet must match all the filtering criteria types in a proxy policy for the policy to apply.

Matching order of proxy policies

The device supports multiple proxy policies.

A packet is matched against the proxy policies in the order they are configured. The match process stops once a matching policy is found.

The more refined the filtering criteria are, the smaller the application range of the proxy policy. Configure the proxy policies in ascending order of their application ranges as a best practice.

Proxy policy actions

The device supports the following actions for traffic matching a proxy policy:

- **TCP-proxy**—The device acts as a TCP proxy and provides TCP-layer isolation for traffic between the TCP client and TCP server.
- **SSL-decryption**—The device acts as an SSL proxy to decrypt the SSL traffic and implement deep packet inspection on the traffic.
- **No-proxy**—The device transmits the traffic transparently.

Whitelist

To disable the proxy function for connections destined for certain servers, add the hostnames of the servers to the whitelist. Connections destined for servers on the whitelist are transmitted transparently.

The device provides a predefined whitelist and allows you to customize the user-defined whitelist.

Predefined whitelist

The predefined whitelist contains the following types of predefined whitelist entries:

- **Chrome-HSTS whitelist entries**—Hostnames of servers that are accessible through only HTTPS by the Google Chrome browser.
- **Non-Chrome-HSTS whitelist entries**.

You can enable or disable entries on the predefined whitelist as needed.

User-defined whitelist

For destination servers of connections that need to be transmitted transparently, manually add their hostnames to the user-defined whitelist.

If the **DNS Name** or **Common Name** value in a server certificate contains a hostname on the SSL hostname whitelist, the device does not proxy the SSL connections destined for the server.

Protection services of the SSL decryption

The SSL decryption supports the following protection services:

- **Internal client protection**—Collaborating with deep packet inspection, the device decrypts the packets and performs deep packet inspection on the decrypted packets. It protects the internal clients from being attacked by external malicious websites. In this scenario, the device requires imported SSL decryption certificates to establish SSL connections with the clients.
- **Internal server protection**—Collaborating with deep packet inspection, the device decrypts the packets and performs deep packet inspection on the packets. It protects the internal servers from being attacked by external malicious websites. In this scenario, the device requires imported internal server certificates to establish SSL connections with the clients.

Select a protection service of the SSL decryption as required and import the corresponding certificates to the device for SSL connection establishment with the clients.

SSL certificates

The SSL certificate types vary by protection service.

SSL decryption certificates

The SSL decryption certificates are required in the scenario of protecting internal clients. When the device acts as an SSL proxy to complete SSL handshakes with the client and server, it must send a certificate to the client to identify itself. The device uses the SSL decryption certificate to issue a new server certificate based on the certificate content of the real server and sends the new certificate to the client.

The device supports a trusted SSL decryption certificate and an untrusted SSL decryption certificate, both of which are CA certificates that must be manually imported to the device. When importing an SSL decryption certificate, you can mark the certificate as **Trusted** or **Untrusted**.

When functioning as a proxy client to complete the SSL handshake with the real SSL server, the device uses the CA certificate of the PKI domain to verify if the server certificate is issued by a trusted CA.

- If the server certificate is issued by a trusted CA, the device uses the trusted SSL decryption certificate to issue a new certificate and sends the certificate to the client. A server certificate issued by the trusted SSL decryption certificate is trusted by the client.
- If the server certificate is issued by an untrusted CA, the device uses the untrusted SSL decryption certificate to issue a new certificate and sends the certificate to the client. A security alarm will be generated on the client and users must clear the alarm to continue the access.

For more information about PKI domains, see PKI domain online help.

Internal server certificates

The internal server certificates are required in the scenario of protecting internal servers. With an internal server certificate imported, the device will decrypt the certificate and generate a CER file and a key file. The CER file is used to identify the server and the key file is used to encrypt and decrypt the packets in the subsequent SSL proxy process. The device will calculate the MD5 value of the CER file and use the MD5 value as the unique identifier of the file.

The SSL proxy process is as follows:

1. The device receives an internal server certificate and calculates the MD5 value of the certificate.
2. The device compares the calculated MD5 value with the MD5 value of the imported internal server certificate:
    - If they are the same, the certificate is trusted and the device will use the certificate to establish an SSL connection with the client.
    - If they are different, the certificate is untrusted.

You can import multiple internal server certificates. If two certificates have the same MD5 value, the new certificate will overwrite the old certificate.

Restrictions and guidelines

The TCP proxy and SSL proxy functions can degrade the forwarding performance of the device. When configuring a proxy policy, redefine the filtering criteria to restrict the application of the policy to only necessary traffic.

For HTTPS websites to be accessed correctly, you must install and trust the SSL decryption certificate in the client's browsers.

Firefox uses its own CA store by default. To use Firefox for SSL connections, import the SSL decryption certificate for Firefox or configure Firefox to use the system CA store if you have imported the certificate for another browser. To configure Firefox to use the system CA store, enter **about:config** in the address bar of Firefox, search for **security.enterprise_roots.enabled**, double-click or right-click the item, and set the boolean value to **true**.

After the SSL proxy function is enabled, the packet capture action of the intrusion prevention system will be invalid.

The SSL decryption action takes effect only on SSL-encrypted protocol traffic, such as HTTPS, SMTPS, and POP3S traffic.

Configure application proxy

Configure a proxy policy

1. Click the **Policies** tab.
2. In the navigation pane, select **Application Proxy** > **Proxy Policy**.
3. Click **Create**.
4. Create a proxy policy.

Table 1 Proxy policy configuration items

Item	Description
Policy name	Enter a name for the proxy policy.
Src security zones	Specify the source security zones to which the policy applies.

Item	Description
Dst security zones	Specify the destination security zones to which the policy applies.
Source addresses	Specify the source IP addresses to which the policy applies.
Destination addresses	Specify the destination IP addresses to which the policy applies.
User	Specify the users to whom the policy applies.
Services	Specify the services to which the policy applies.
Action	Select the action to take on the matching traffic. Options are: • **No-proxy**—Transmits the traffic transparently. • **TCP-proxy**—Implements TCP proxy for the traffic. • **SSL-decryption**—Implements SSL proxy to decrypt the SSL traffic and implement deep packet inspection on the traffic.
Protection service	Select a protection service for the SSL decryption. Options are: • **Internal client protection**. • **Internal server protection**. This field is available after you select SSL decryption as the action on matching traffic.
Enable policy	Select **Yes** to enable the policy, or select **No** to disable the policy.

5. Click **OK**.

Configure the whitelist

Create a user-defined whitelist entry

1. Click the **Policies** tab.
2. In the navigation pane, select **Application Proxy** > **Whitelist**.
3. Click **Create**.
4. Enter the hostname of a server and click **OK**.

Enable or disable predefined whitelist entries

1. Click the **Policies** tab.
2. In the navigation pane, select **Application Proxy** > **Whitelist**.
3. Click **Predefined Whitelist**.
4. To enable a Chrome-HSTS whitelist entry:
    a. Click **Turn on Chrome-HSTS whitelist switch**.
    b. Select the **Enable** option for the Chrome-HSTS whitelist entry you want to enable.
5. To enable a non-Chrome-HSTS whitelist entry, select the **Enable** option for the entry.
6. To disable all Chrome-HSTS whitelist entries, click **Turn off Chrome-HSTS whitelist switch**.
7. Click **Submit** to activate the configuration.

Import SSL decryption certificate

1. Click the **Policies** tab.

2. In the navigation pane, select **Application Proxy** > **SSL Certificates**.
3. On the **SSL Decryption Certificates** tab, click **Import**.
4. Configure the items for importing an SSL decryption certificate.

Table 2 Configuration items for importing an SSL decryption certificate

Item	Description
Certificate file	Click **Select file** to select a certificate file.
Password	Enter the password for the SSL decryption certificate.
Certificate type	Select **Trusted** or **Untrusted**.

5. Click **OK**.

Import internal server certificates

1. Click the **Policies** tab.
2. In the navigation pane, select **Application Proxy** > **SSL Certificates**.
3. Click the **Internal Server Certificates** tab.
4. Click **Import**.
5. Configure the items for importing an internal server certificate.

Table 3 Configuration items for importing an internal server certificate

Item	Description
Certificate file	Click **Select file** to select a certificate file.
Password	Enter the password for the internal server certificate.

6. Click **OK**.

Trusted API proxies

This help contains the following topics:

Introduction

Trusted API proxies are proxies for user traffic to access APIs. The device can direct received user requests to a trusted access controller for authentication and authorization. The trusted access controller returns the associated result to the device to control user access permissions.

Configure a trusted API proxy

1. Click the **Policies** tab.
2. In the navigation pane, select **Zero Trust** > **Trusted API Proxies**.
3. Click **Create**.
4. Configure the trusted API proxy parameters.

Table 1 Basic trusted API proxy configuration items

Item	Description
Name	Enter the name of the trusted API proxy, which is a case-insensitive string.
IPv4 address	Enter the IPv4 address used to provide trusted API proxy services.
Port number	Enter the port number for the trusted API proxy. If the trusted API proxy uses an SSL policy, you must specify a non-default port number for it (a typical example is 443).
Proxy function	Enable or disable the trusted API proxy.
Trusted access controller	Specify a trusted access controller for the trusted API proxy. The device will direct traffic matching the trusted API proxy to the specified trusted access controller for authentication and authorization. Only the users passing the authentication and authorization are allowed to proceed with subsequent procedures. You can select an existing trusted access controller or create a new trusted access controller.
SSL client policy	Specify the SSL client policy used by the trusted API proxy to encrypt traffic exchanged between the device (SSL client) and the SSL server. You can select an existing SSL client policy or create a new SSL client policy.
SSL server policy	Specify the SSL server policy used by the trusted API proxy to encrypt traffic exchanged between the device (SSL server) and the SSL client. You can select an existing SSL server policy or create a new SSL server policy.
Max connections	Set the maximum number of connections allowed by the trusted API proxy. 0 means not limited.
Max connections per second	Set the maximum number of connections allowed by the trusted API proxy per second. 0 means not limited.

Table 2 Advanced trusted API proxy configuration items

Item	Description
LB policy	Specify an LB policy for the trusted API proxy. Based on the LB policy rules, the device performs load balancing for packets matching the trusted API proxy according to their content. You can select an existing LB policy or create a new LB policy. A HTTP-type trusted API proxy can use only an LB policy of the generic or HTTP type.
Connection limit policy	Specify a connection limit policy for the trusted API proxy. The number of connections to the trusted API proxy will be limited by the specified policy. You can select an existing connection limit policy or create a new connection limit policy.
TCP parameter profile (client)	Specify a TCP parameter profile for the trusted API proxy. The device uses the parameter profile settings to process matching traffic. The client-side TCP parameter profile applies only to TCP connections between the device and the client. You can select an existing TCP parameter profile or create a new TCP parameter profile.
TCP parameter profile (server)	Specify a TCP parameter profile for the trusted API proxy. The device uses the parameter profile settings to process matching traffic. The server-side TCP parameter profile applies only to TCP connections between the device and the server. You can select an existing TCP parameter profile or create a new TCP parameter profile.
HTTP protection policy	Specify an HTTP protection policy for the trusted API proxy. The device uses the protection policy settings to protect traffic matching the trusted API proxy. You can select an existing HTTP protection policy or create a new HTTP protection policy.
Content security function	Enable or disable the content security function.
Content security-IPS profile	Specify an IPS profile for content security. The device performs intrusion prevention for traffic matching the trusted API proxy.

Item	Description
	For more information about IPS profiles, see IPS help.
Content security-Anti-virus profile	Specify an anti-virus profile for content security. The device performs anti-virus prevention for traffic matching the trusted API proxy. For more information about anti-virus profiles, see anti-virus help.

5. Click **OK**.

   The trusted API proxy will be displayed on the trusted API proxy page.

Trusted application proxies

This help contains the following topics:

Introduction

Trusted application proxies are proxies for user traffic to access applications. The device can direct received user requests to a trusted access controller for authentication and authorization. The trusted access controller returns the associated result to the device to control user access permissions.

Configure a trusted application proxy

1. Click the **Policies** tab.
2. In the navigation pane, select **Zero Trust** > **Trusted App Proxies**.
3. Click **Create**.
4. Configure the trusted application proxy parameters.

Table 1 Basic trusted application proxy configuration items

Item	Description
Name	Enter the name of the trusted application proxy, which is a case-insensitive string.
IPv4 address	Enter the IPv4 address used to provide trusted application proxy services.
Port number	Enter the port number for the trusted application proxy. If the trusted application proxy uses an SSL policy, you must specify a non-default port number for it (a typical example is 443).
Proxy function	Enable or disable the trusted application proxy.
Trusted access controller	Specify a trusted access controller for the trusted application proxy. The device will direct traffic matching the trusted application proxy to the specified trusted access controller for authentication and authorization. Only the users passing the authentication and authorization are allowed to proceed with subsequent procedures. You can select an existing trusted access controller or create a new trusted access controller.
SSL client policy	Specify the SSL client policy used by the trusted application proxy to encrypt traffic exchanged between the device (SSL client) and the SSL server. You can select an existing SSL client policy or create a new SSL client policy.
SSL server policy	Specify the SSL server policy used by the trusted application proxy to encrypt traffic exchanged between the device (SSL server) and the SSL client. You can select an existing SSL server policy or create a new SSL server policy.
Max connections	Set the maximum number of connections allowed by the trusted application proxy. 0 means not limited.
Max connections per second	Set the maximum number of connections allowed by the trusted application proxy per second. 0 means not limited.

Table 2 Advanced trusted application proxy configuration items

Item	Description
LB policy	Specify an LB policy for the trusted application proxy. Based on the LB policy rules, the device performs load balancing for packets matching the trusted application proxy according to their content. You can select an existing LB policy or create a new LB policy. A HTTP-type trusted application proxy can use only an LB policy of the generic or HTTP type.
Connection limit policy	Specify a connection limit policy for the trusted application proxy. The number of connections to the trusted application proxy will be limited by the specified policy. You can select an existing connection limit policy or create a new connection limit policy.
TCP parameter profile (client)	Specify a TCP parameter profile for the trusted application proxy. The device uses the parameter profile settings to process matching traffic. The client-side TCP parameter profile applies only to TCP connections between the device and the client. You can select an existing TCP parameter profile or create a new TCP parameter profile.
TCP parameter profile (server)	Specify a TCP parameter profile for the trusted application proxy. The device uses the parameter profile settings to process matching traffic. The server-side TCP parameter profile applies only to TCP connections between the device and the server. You can select an existing TCP parameter profile or create a new TCP parameter profile.
HTTP parameter profile	Specify an HTTP parameter profile for the trusted application proxy. The device uses the parameter profile settings to process matching traffic. You can select an existing HTTP parameter profile or create a new HTTP parameter profile.
HTTP protection policy	Specify an HTTP protection policy for the trusted application proxy. The device uses the protection policy settings to protect traffic matching the trusted application proxy. You can select an existing HTTP protection policy or create a new HTTP protection policy.

Item	Description
Content security function	Enable or disable the content security function.
Content security-IPS profile	Specify an IPS profile for content security. The device performs intrusion prevention for traffic matching the trusted application proxy. For more information about IPS profiles, see IPS help.
Content security-Anti-virus profile	Specify an anti-virus profile for content security. The device performs anti-virus prevention for traffic matching the trusted application proxy. For more information about anti-virus profiles, see anti-virus help.

5. Click **OK**.

   The trusted application proxy will be displayed on the trusted application proxy page.

AFT

Introduction

Address Family Translation (AFT) translates an IP address of one address family into an IP address of the other address family.

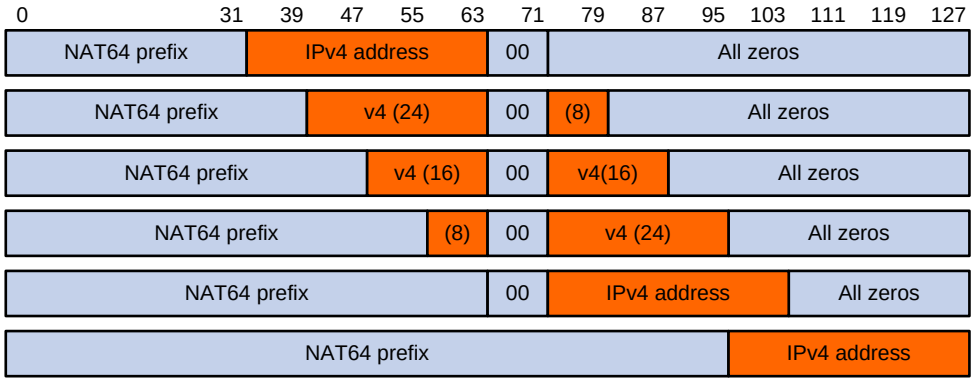
NAT64 prefix

NAT64 prefix is an IPv6 address prefix used to construct an IPv6 address representing an IPv4 node in an IPv6 network. The IPv6 hosts do not use a constructed IPv6 address as their real IP address. The length of a NAT64 prefix can be 32, 40, 48, 56, 64, or 96.

As shown in Figure 1, the construction methods vary depending on the NAT64 prefix length. Bits 64 through 71 in the constructed IPv6 address are reserved bits.

- If the prefix length is 32, 64, or 96 bits, the IPv4 address contained in the IPv6 address will be intact.
- If the prefix length is 40, 48, or 56 bits, the IPv4 address contained in the IPv6 address will be divided into two parts by bits 64 through 71.

Figure 1 IPv6 address construction with NAT64 prefix and IPv4 address



AFT translation methods

When dynamic AFT performs IPv6-to-IPv4 source address translation, the Not Port Address Translation (NO-PAT) and Port Address Translation (PAT) modes are available.

NO-PAT

NO-PAT translates one IPv6 address to one IPv4 address. An IPv4 address assigned to one IPv6 host cannot be used by any other IPv6 host until it is released.

NO-PAT supports all IP packets.

PAT

PAT translates multiple IPv6 addresses to a single IPv4 address by mapping each IPv6 address and port to the IPv4 address and a unique port. PAT supports the following packet types:

- TCP packets.
- UDP packets.

- ICMPv6 echo request and echo reply messages.

PAT supports port blocks for connection limit and user tracing. Port blocks are generated by dividing the port range (1024 to 65535) by the port block size. Port block based PAT maps multiple IPv6 addresses to one IPv4 address and uses a port block for each IPv6 address.

Port block based PAT functions as follows:

1. When an IPv6 host first initiates a connection to the IPv4 network, it creates a mapping from the host's IPv6 address to an IPv4 address and a port block.
2. It translates the IPv6 address to the IPv4 address, and the source ports to ports in the port block for subsequent connections from the IPv6 host until the ports in the port block are exhausted.

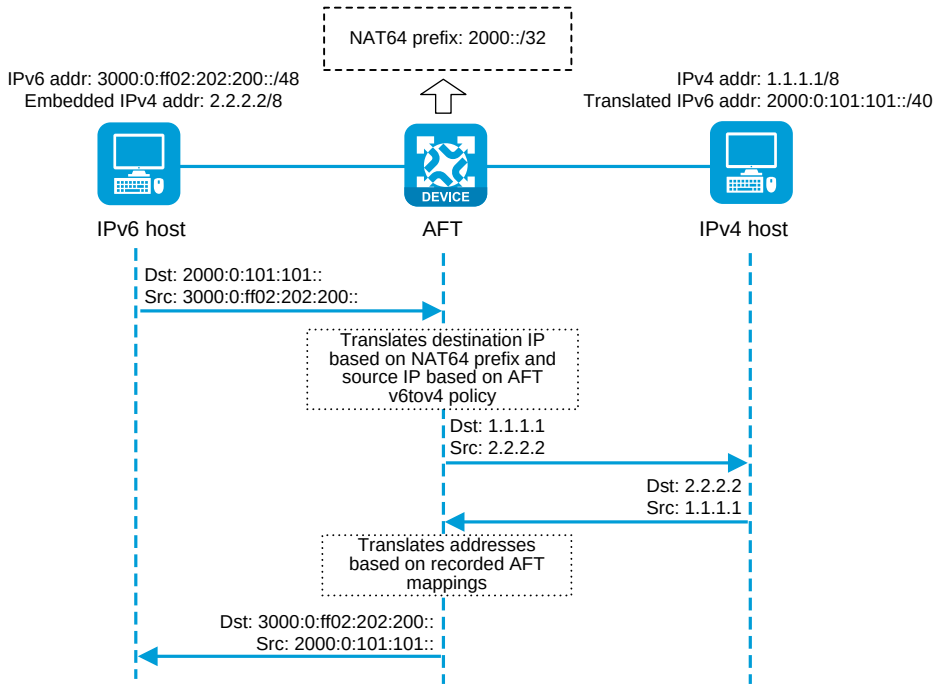
AFT translation process

As shown in Figure 2, when the IPv6 host initiates access to the IPv4 host, AFT operates as follows:

1. Upon receiving a packet from the IPv6 host, AFT compares the packet with IPv6-to-IPv4 destination address translation policies.
    - If a matching policy is found, AFT translates the destination IPv6 address according to the policy.
    - If no matching policy is found, AFT does not process the packet.
2. AFT performs pre-lookup to determine the output interface for the translated packet. PBR is not used for the pre-lookup.
    - If a matching route is found, the process goes to step 3.
    - If no matching route is found, AFT discards the packet.

3. AFT compares the source IPv6 address of the packet with IPv6-to-IPv4 source address translation policies.
    - If a matching policy is found, AFT translates the source IPv6 address according to the policy.
    - If no matching policy is found, AFT discards the packet.
4. AFT forwards the translated packet and records the mappings between IPv6 addresses and IPv4 addresses.
5. AFT translates the IPv4 addresses in the response packet header to IPv6 addresses based on the address mappings before packet forwarding.

Figure 2 AFT process for IPv6-initiated communication



Health monitoring

Introduction

Health monitoring is implemented through Network Quality Analyzer (NQA).

NQA allows you to measure network performance, verify the service levels for IP services and applications, and troubleshoot network problems.

NQA operating mechanism

An NQA operation contains a set of parameters such as the operation type, destination IP address, and port number that define how the operation is performed. You can configure the parameters for an NQA operation in a probe template in health monitoring.

As shown in Figure 1, the NQA source device (NQA client) sends data to the NQA destination device by simulating IP services and applications to measure network performance.

All types of NQA operations require the NQA client, but only the TCP operation requires the NQA server. The NQA operations for services that are already provided by the destination device such as FTP do not need the NQA server. You can configure the NQA server to listen and respond to specific IP addresses and ports to meet various test needs.

Figure 1 Network diagram

Configuration items for probe templates

The following tables describe the configuration items for different probe templates:

- Table 1 Basic configuration items for all probe templates
- Table 2 Basic configuration items for the ICMP template
- Table 3 Basic configuration items for the UDP/TCP template
- Table 4 Basic configuration items for the FTP template
- Table 5 Basic configuration items for the DNS template
- Table 6 Basic configuration items for the HTTP/HTTPS template
- Table 7 Basic configuration items for the RADIUS template
- Table 8 Basic configuration items for the SSL template
- Table 9 Basic configuration items for the TCP half-open template
- Table 10 Basic configuration items for the SNMP-DCA template
- Table 11 Basic configuration items for the RADIUS-ACCOUNT template

Table 1 Basic configuration items for all probe templates

Item	Description
Template name	Enter a name for the template. The template name is case insensitive.
Type	Select an operation type from the list. Options are: • **ICMP**. • **UDP**. • **TCP**. • **FTP**. • **DNS**. • **HTTP**. • **RADIUS**. • **SSL**. • **HTTPS**. • **TCP half-open**. • **SNMP-DCA**. • **RADIUS-ACCOUNT**.
Probe interval	Enter the interval in milliseconds at which the NQA operation repeats. If you set the interval to 0, NQA performs the operation only once and does not generate any statistics.
Probe timeout	Enter the timeout time for waiting for a response, in milliseconds.
Description	Enter a description for the template.

Table 2 Basic configuration items for the ICMP template

Item	Description
Destination IP	Enter the destination IPv4 or IPv6 address for the probe packets.

Item	Description
address	
Data to pad	Enter the case-sensitive payload fill string for probe packets. The payload fill string will be truncated at the end or cyclically repeated to fit the payload size of the probe packet.
Length of data to pad	Enter the payload size for each probe packet, in bytes.
Next hop IP address	Enter the next hop IPv4 or IPv6 address for probe packets. If the next hop address is not configured, the device searches the routing table to determine the next hop address for the probe packets.
Outgoing interface	Enter the outgoing interface for probe packets. For successful operation, the specified outgoing interface must be up.

Table 3 Basic configuration items for the UDP/TCP template

Item	Description
Destination IP address	Enter the destination IPv4 or IPv6 address for the probe packets.
Destination port number	Enter the destination port number for the probe packets.
Data to pad	Enter the case-sensitive payload fill string for probe packets. The payload fill string will be truncated at the end or cyclically repeated to fit the payload size of the probe packet.
Length of data to pad	Enter the payload size for each probe packet, in bytes. This item is not available for the TCP operation.
Next hop IP address	Enter the next hop IPv4 or IPv6 address for probe packets. If the next hop address is not configured, the device looks up the routing table for the next hop address. This item is not available for the UDP operation.

Item	Description
Expected data offset	Enter the offset in bytes after which the first match operation for the expected response data starts. Upon receiving a response packet, the NQA client searches the packet payload for the expected data. • If no offset is configured, the NQA client starts the first match operation from the beginning byte of the payload. If no match is found, it starts another match operation from the second byte of the payload. The process continues until a match is found or the last payload byte is tried. • If an offset is configured, the NQA client starts the first match operation after the specified offset bytes. If no match is found, it continues the match operation as if no offset was configured. In whichever cases, the NQA client marks the NQA operation as successful if a match is found. If no match is found, it marks the NQA operation as failed.
Expected data	Enter the case-sensitive expected response data.

Table 4 Basic configuration items for the FTP template

Item	Description
URL	Enter the URL of the target resource for the FTP operation, a case-sensitive string of 1 to 255 characters. Valid URL formats: • ftp://host/filename. • ftp://*host*:*port*/*filename*. The *host* parameter represents the host name of the server hosting the resource, which must meet the following requirements: • Case sensitive. • Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.), but consecutive dots (.) are not allowed. • Must be a dot-separated series of labels. Each label can contain 1 to 63 characters.

Item	Description
Username	Enter the FTP login username. The username is case sensitive.
Password	Enter the FTP login password in encrypted form.
Operation type	Select the FTP operation type from the list. Options are: • **Download**—Gets a file from the FTP server. • **Upload**—Uploads a file to the FTP server.
Local file name	This item is available only when **Upload** is selected for **Operation type**. Enter the name of the file to be uploaded to the FTP server. The file name is a case-sensitive string of 1 to 200 characters which cannot contain slashes (/).
Mode	Select the data transmission mode for the FTP operation. Options are: • **Active**—In active mode, the FTP server initiates a connection request. • **Passive**—In passive mode, the FTP client initiates a connection request.

Table 5 Basic configuration items for the DNS template

Item	Description
Destination IP address	Enter the IP address of the DNS server as the destination IP address for the probe packets.
Destination port number	Enter the destination port number for the probe packets.
Domain to resolve	Enter the domain name to be resolved. The domain name must meet the following requirements: • 1 to 255 characters in length.

Item	Description
	• Case sensitive. • Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.), but consecutive dots (.) are not allowed. • Must be a dot-separated series of labels. Each label can contain 1 to 63 characters.
Resolving type	Select the domain name resolution type. Options are: • **A**—A type A query resolves a domain name to a mapped IPv4 address. • **AAA**—A type AAAA query resolves a domain name to a mapped IPv6 address.
Expected IPv4 address	This item is available only when **A** is selected for **Resolving type**. Enter the expected IPv4 address. During a DNS operation, the NQA client compares the expected IPv4 address with the IPv4 address resolved by the DNS server. If they are the same, it considers the DNS server legal.
Expected IPv6 address	This item is available only when **AAA** is selected for **Resolving type** Enter the expected IPv6 address. During a DNS operation, the NQA client compares the expected IPv6 address with the IPv6 address resolved by the DNS server. If they are the same, it considers the DNS server legal.
Outgoing interface	Enter the outgoing interface for probe packets.

Table 6 Basic configuration items for the HTTP/HTTPS template

Item	Description
URL	Enter the URL of the target resource, a case-sensitive string of 1 to 255 characters which cannot contain question marks (?). Valid URL formats: • HTTP:

Item	Description
	◦ http://host/resource. ◦ http://*host*:*port*/*resource*. • HTTPS: ◦ https://*host*/*resource*. ◦ https://*host*:*port*/*resource*. The *host* parameter represents the host name of the server hosting the resource, which must meet the following requirements: • Case sensitive. • Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.), but consecutive dots (.) are not allowed. • Must be a dot-separated series of labels. Each label can contain 1 to 63 characters.
Username	Enter the login username. The username is case sensitive.
Password	Enter the login password in encrypted form. The password is case sensitive.
Operation type	Select an operation type from the list. Options are: • **Get**—Gets data from the HTTP or HTTPS server. • **Post**—Transfers data to the HTTP or HTTPS server. • **Raw**—Sends the RAW request to the HTTP or HTTPS server.
Version	Select the version used in the HTTP or HTTPS operation. Options are: • **V1.0**. • **V1.1**.
SSL client policy	This item is available only for the HTTPS template. Select an existing SSL client policy or select **Create SSL client polic**y to create an SSL client policy for the HTTPS template. The created SSL client policy will be displayed on the **Objects** > **SSL** > **SSL Client Policies** page. In the HTTPS operation, the NQA client uses the specified SSL client policy to establish an SSL connection to the server.
Expected status	Enter a comma-separated list of status code items. Each item

Item	Description
code	specifies a status code or a range of status codes in the form of *status-num1-status-num2*. The value ranges for both the *status-num1* and *status-num2* arguments are 0 to 999. The value for the *status-num 2* argument must be equal to or greater than the value for the *status-num 1* argument. Example: 1-4, 6, 8-10.
Expected data offset	Enter the offset in bytes after which the first match operation for the expected response data starts. Upon receiving a response packet, the NQA client searches the packet payload for the expected data. • If no offset is configured, the NQA client starts the first match operation from the beginning byte of the payload. If no match is found, it starts another match operation from the second byte of the payload. The process continues until a match is found or the last payload byte is tried. • If an offset is configured, the NQA client starts the first match operation after the specified offset bytes. If no match is found, it continues the match operation as if no offset was configured. In whichever cases, the NQA client marks the NQA operation as successful if a match is found. If no match is found, it marks the NQA operation as failed.
Expected data	Enter the case-sensitive expected response data.

Table 7 Basic configuration items for the RADIUS template

Item	Description
Destination IP address	Enter the destination IPv4 or IPv6 address for the probe packets.
Destination port number	Enter the destination port number for the probe packets.
Username	Enter the login username for the RADIUS operation. The username is case sensitive.

Item	Description
Password	Enter the login password in encrypted form The password is case sensitive.
Shared key	Enter the shared key in plaintext form. The shared key is case sensitive.

Table 8 Basic configuration items for the SSL template

Item	Description
Destination IP address	Enter the destination IPv4 or IPv6 address for the probe packets.
Destination port number	Enter the destination port number for the probe packets.
SSL client policy	Select an existing SSL client policy or select **Create SSL client polic**y to create an SSL client policy for the SSL template. The created SSL client policy will be displayed on the **Objects** > **SSL** > **SSL Client Policies** page. In the SSL operation, the NQA client uses the specified SSL client policy to establish an SSL connection to the server.

Table 9 Basic configuration items for the TCP half-open template

Item	Description
Destination IP address	Enter the destination IPv4 or IPv6 address for the probe packets.
Next hop IP address	Enter the next hop IPv4 or IPv6 address for probe packets. If the next hop address is not configured, the device searches the routing table to determine the next hop address for the probe

Item	Description
	packets.
Port detection	Enable port detection of the TCP half open template. In the TCP half open operation, port detection probes whether the listening port of the TCP service on the destination device is available. If the NQA client receives the SYN-ACK packet from the destination device within the probe timeout time after sending a SYN packet, the TCP half open operation succeeds. If no SYN-ACK packet is received within the probe timeout time, the TCP half open operation fails.
Destination port number	Enter the destination port number for the probe packets.
Outgoing interface	Enter the outgoing interface for probe packets. For successful operation, the specified outgoing interface must be up.

Table 10 Basic configuration items for the SNMP-DCA template

Item	Description
Destination IP address	Enter the destination IPv4 or IPv6 address for the probe packets.
Destination port number	Enter the destination port number for the probe packets.
SNMP community	Enter the SNMP community name. This item is required if the SNMP agent is configured with a community name. Make sure the specified community name is the same as the community name configured on the SNMP agent.
SNMP version	Select the SNMP version used in the SNMP DCA operation. For the SNMP DCA operation to work correctly, the selected SNMP version must match the version of the SNMP agent to be monitored.

Item	Description
Agent type	Select the type of the SNMP agent. Options are: • Net-SNMP. • Windows. • Customize. The SNMP DCA operation monitors the performance of a device running an SNMP agent. It collects the CPU, memory, and disk usage from the SNMP agent and determines the device performance based on the collected object values and their associated thresholds and weights. Different SNMP agent types use different OIDs for the CPU, memory, and disk usage objects. Make sure the SNMP agent type specified in the SNMP DCA template matches the type of the SNMP agent to be monitored. For Net-SNMP or Windows SNMP agents, the NQA client has built-in OIDs to collect the CPU, memory, and disk usage objects. You can set the thresholds and weights for these objects. You can also add interested SNMP objects in the **OID settings** area. For SNMP agents of the user-defined type, the NQA client does not have predefined SNMP objects to collect. You must configure the interested SNMP objects and their associated thresholds and weights.
CPU usage threshold	This item is available only when the **Net-SNMP** or **Windows** is selected for **Agent type**. Enter the CPU usage threshold. A threshold of 0 means that CPU usage is not used as a metric for measuring the SNMP agent performance.
CPU weight	This item is available only when the **Net-SNMP** or **Windows** is selected for **Agent type**. Enter the weight of the CPU usage object. A weight of 0 means that CPU usage is not used as a metric for measuring the SNMP agent performance.
Memory usage threshold	This item is available only when the **Net-SNMP** or **Windows** is selected for **Agent type**. Enter the memory usage threshold. A threshold of 0 means that memory usage is not used as a metric for

Item	Description
	measuring the SNMP agent performance.
Memory weight	This item is available only when the **Net-SNMP** or **Windows** is selected for **Agent type**. Enter the weight of the memory usage object. A weight of 0 means that memory usage is not used as a metric for measuring the SNMP agent performance.
Disk usage threshold	This item is available only when the **Net-SNMP** or **Windows** is selected for **Agent type**. Enter the disk usage threshold. A threshold of 0 means that disk usage is not used as a metric for measuring the SNMP agent performance.
Disk weight	This item is available only when the **Net-SNMP** or **Windows** is selected for **Agent type**. Enter the weight of the disk usage object. A weight of 0 means that disk usage is not used as a metric for measuring the SNMP agent performance.
OID settings	To configure an SNMP object to monitor: 1. Click **Create** in the **OID settings** area. 2. In the **Create OID** window that opens, configure the following items: o OID—Enter the OID of the SNMP object to monitor. o OID usage threshold—Enter the threshold for the object. A threshold of 0 means that the object is not used as a metric for measuring the performance of the SNMP agent. o OID weight—Enter the weight for the object. A weight of 0 means that the object is not used as a metric for measuring the performance of the SNMP agent. 3. Click **OK**. The OID will be displayed on the OID list. The OID configuration is required if the **Customize** agent type is used. You can add a maximum of eight OIDs.

Table 11 Basic configuration items for the RADIUS-ACCOUNT template

Item	Description
Destination IP address	Enter the destination IPv4 or IPv6 address for the probe packets.
Destination port number	Enter the destination port number for the probe packets.
Username	Enter the login username. The username is case sensitive.
Shared key	Enter the shared key in plaintext form. The shared key is case sensitive.

Table 12 Advanced configuration items for probe templates

Item	Description
VPN instance	Specify the VPN instance to which the operation applies. You can select an existing VPN instance, **Public network**, or you can select **Create VPN instance polic**y to create a VPN instance. The created VPN instance will be displayed on the **Network** > **VPN** page. After you specify the VPN instance, the NQA operation tests the connectivity in the specified VPN instance.
TTL	Enter the maximum number of hops that the probe packets can traverse.
ToS	Enter the ToS value in the IP header of the probe packets.
Source IP address	Enter the source IPv4 or IPv6 address for the probe packets. The source address must be the address of a local interface, and the interface must be up. Otherwise, no probe packets can be sent out. Do not configure this item if the template is intended for use by a NAT address group.

Item	Description

Probe result frequency	Select the probe result sending basis. Options are:
	• **Consecutive probes**—Sends the probe result to the feature that uses the template after the specified number of consecutive failed or successful probes.
	  ◦ Consecutive successful probes—Enter the number of consecutive successful probes that trigger probe result sending.
	  ◦ Consecutive failed probes—Enter the number of consecutive failed probes that trigger probe result sending.
	• **Per probe**—Sends the probe result to the feature that uses the NQA template every time a probe is completed. This option is available only for ICMP and TCP half open templates.

User management

This help contains the following topics:

Introduction

Local users

Users

A local user is a set of user attributes stored in the local user database on the device for network access. A local user is uniquely identified by its username.

To implement local authentication, authorization, and accounting, create local users and configure user attributes on the device.

User groups

User groups simplify local user configuration and management. A user group contains a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized user attributes management for the local users in the group. Local user attributes that are manageable by using user groups are authorization attributes.

Each new created local user belongs to the system defined user group named **system** and has all attributes of the group.

Password control

To enhance password security for users, you can configure the password control feature.

Minimum password length

You can define the minimum length of user passwords. The system rejects any password that is shorter than the configured minimum length. By default, the minimum password length is 10 characters.

Password composition check

A password can be a combination of characters from the following types:

- Uppercase letters A to Z.
- Lowercase letters a to z.
- Digits 0 to 9.
- Special characters. See Table 1.

Table 1 Special characters

Character name	Symbol	Character name	Symbol
Ampersand sign	&	Apostrophe	'
Asterisk	*	At sign	@
Back quote	`	Back slash	\
Blank space	N/A	Caret	^
Colon	:	Comma	,
Dollar sign	$	Dot	.
Equal sign	=	Exclamation point	!
Left angle bracket	<	Left brace	{

Character name	Symbol	Character name	Symbol
Left bracket	[	Left parenthesis	(
Minus sign	-	Percent sign	%
Plus sign	+	Pound sign	#
Quotation marks	"	Right angle bracket	>
Right brace	}	Right bracket	]
Right parenthesis	)	Semi-colon	;
Slash	/	Tilde	~
Underscore	_	Vertical bar	|

Depending on the system's security requirements, you can set the minimum number of character types a password must contain and the minimum number of characters for each type, as shown in Table 2.

Table 2 Password composition check

Password combination level	Minimum number of character types	Minimum number of characters for each type
Level 1	One	One
Level 2	Two	One
Level 3	Three	One
Level 4	Four	One

When a user sets or changes a password, the system examines whether the password meets the combination requirement. If the password does not meet the requirement, the operation fails.

By default, the minimum number of character types is one and the minimum number of characters for each type is one.

Password complexity check

The strength of a password increases as its complexity grows. A less complicated password is more likely to be cracked. For example, a password that contains the username or repeated characters is more likely to be cracked than those do not. To increase system security, configure a password complexity checking policy to make sure the user-configured passwords are complex enough against most password attacks.

You can apply the following password complexity requirements:

- A password cannot contain the username or the username spelled backwards. For example, if the username is **abc**, the password cannot be **abc982** or **2cba**.
- A password cannot contain more than two consecutive identical characters. For example, password **a111** is not allowed.

Password history

This feature allows the system to store passwords that a user has used. When a user changes the password, the system compares the new password with the current password and those stored in the password history records. The new password must be different from the current one and those stored in the history records by a minimum of four characters. If the new password does not meet this requirement, the system displays an error message and rejects the password change operation.

You can set the maximum number of history password records for the system to maintain for each user. When the number of history password records exceeds the setting, the most recent record overwrites the earliest one.

Password updating

This feature allows you to set the minimum interval at which users can change their passwords. A user can only change the password once within the specified interval.

The minimum interval does not apply to the following situations:

- A user is prompted to change the password at the first login.
- The password expiration time expires.

Identity users

The user identification feature can be used with other security features to perform user-based network access control and network privilege management.

The user identification feature has the following benefits:

- Facilitates security policy deployment on a per-user basis.
- Implements network access behaviors auditing on users by providing user-based network attack/access traffic statistics.
- Enables the device to use fixed usernames instead of dynamic IP addresses to implement policy control.

Identity users

Identity users are used to record identification information of network access users from different sources. The identification information includes the username, user group name, and identity

domain name of the users. The user identification module uniformly manages identity users from different sources.

The device supports the following methods to create identity users:

- **Learning from the local user database**—The user identification module learns local user information from the local user database and saves the user information as identity users.
- **Importing from a .csv file**—The network administrator imports user information from a .csv file to the device and the device automatically creates identity users based on the imported information.
- **Importing from third-party servers**—The device initiates user information requests to third-party servers, imports network access user information, and then creates identity users based on the imported information. This method enables the network administrator to manage identity users when user information is on the third-party servers. Supported third-party servers include LDAP servers and IMC RESTful servers.

Identity users will be deleted due to one of the following reasons:

- The network administrator deletes identity users manually.
- The user identification module automatically deletes identity users after the corresponding network access users are deleted from the local user database.

Identity groups

Identity users can be added to different groups for batch configuration and hierarchical user management. The groups are called identity groups. The user identification module uniformly manages identity groups from different sources.

The device supports the following methods to create identity groups:

- **Learning from the local user database**—When a local user group is created, the device instructs the user identification module to create an identity group with the same group name.

- **Importing from a .csv file**—The device imports identity user account information from a .csv file and then automatically creates identity groups based on the imported information.
- **Importing from third-party servers**—The device can import identity user account information from an IMC RESTful server or LDAP servers and then create identity groups based on the group information in the accounts. The device can also directly obtain user group information from LDAP servers and then creates identity groups.

An identity group is activated when it is used by an application module, and all services based on the identity group will take effect. When the application module stops using the identity group, the identity group is inactive.

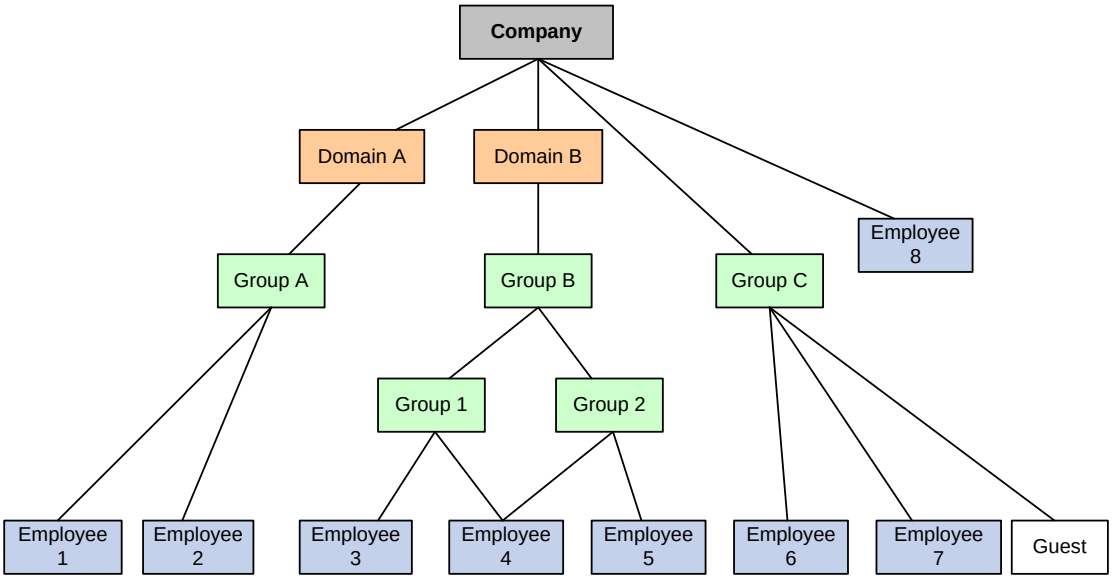
Identity groups will be deleted due to one of the following reasons:

- The network administrator deletes identity groups.
- The user identification module automatically deletes an identity group if the corresponding local user group is deleted from the local user database.

Identity user management

All identity users are organized in a tree structure. An identity user can belong to one or multiple identity groups. An identity group can belong to one or multiple higher-layer identity groups. The tree structure facilitates user location and query. As shown in Figure 1, the device uniquely identifies a managed object by the combination of identity domain and username or the combination of identity domain and identity group.

Figure 1 Identity user management architecture



Identity-based user access control

The following shows the process for identity-based user access control:

1. Identity authentication. A network access user passes identity authentication and comes online.
2. User identification. The device obtains the username and IP address of the online user, and associates the information with the local identity user account and the local identity group. Then, the username-IP mapping for the network access user is created. The administrator can also add static username-IP mappings to permit network access without identity authentication.
3. Identity-based access control. The device identifies the source IP address of the traffic destined for the network, and resolves the IP address to the username and user group based on the mapping. The device performs network access control for the user or user group based on other security feature settings such as blacklist and object policy.

Online users

Online users are online network access users (including portal, PPP, and IPoE users) that are managed by the user identification module. The device records the username, identity domain name, IP address, and MAC address of online users.

Online users include dynamic online users and static online users.

- Dynamic creation.
    - **Online network access users that access the network through the device**—After a user passes local or remote authentication and comes online, the user identification module searches the user's username and domain name in local identity users. If a matching entry is found, the device creates an online user entry for the user.
    - **Online network access users obtained from third-party servers**—After the device obtains information about an online user from a third-party server, the user identification module searches the user's username and domain name in local identity users. If a matching entry is found, the device creates an online user entry for the user. The device can obtain information about all online users of third-party servers (including online users on the other devices) for unified management and monitoring. Supported third-party servers include IMC RESTful server.
- Static configuration.

  The network administrator manually creates online users. Each static identity user contains the mapping between the username and the IP addresses of the user. After a static identity user is created, the user identification module searches the user's username and domain name in local identity users. If a matching entry is found, the device creates a static online user entry for the static identity user. Static online users can access the network without identity authentication but their access to the network is controlled by security features. The network administrator can configure static identity users when only few people need to temporarily access the network.

Application modules can impose security policies on online users. When online user entries are deleted, the user identification module will instruct the application modules to stop processing services for the users.

Online users will be deleted due to one of the following reasons:

- The network administrator deletes online users manually.
- The access modules instruct the user identification module to delete online users after the associated network access users go offline.
- All dynamic online users are deleted after the device restarts up.
- All dynamic online users are deleted after the user identification feature is disabled.
- The third-party servers instruct the device to delete online users after associated users go offline.

User import policies

A user import policy is used to import identity users, online users, or identity groups from a RESTful server or LDAP servers.

The user import policy supports the following import methods:

- **Automatic import**—The device first imports all identity users and online users from the servers specified in the policy and then automatically imports identity users from the servers periodically.
- **Manual import**—The device initiates connection requests to the servers specified in the policy and then imports all identity users and online users from the servers.

Restrictions and guidelines

Restrictions and guidelines for users

A non-password-protected local user passes authentication if the user provides the correct username and passes attribute checks. To enhance security, configure a password for each local user.

For portal users, only the authorization ACL and idle timeout attributes take effect.

For SSL VPN users, only the SSL VPN policy group attribute takes effect.

Deletion of identity users does not delete the corresponding network access users from the local user database.

Restrictions and guidelines for user import policy configuration

When you import users from a .CSV template, make sure the file is a standard .CSV file and do not modify the annotation headers of the template. A violation might cause data loss.

To use the IMC RESTful server, make sure the server is installed with the SSM component and runs on IMC PLAT 7.0 (E0201) or its patch version.

After the device establishes a connection with the RESTful server, the RESTful server sends real-time user login and logout information for the device to update online users.

Restrictions and guidelines for email server configuration

Before you configure the email address of the receiver, you must configure the email server.

Restrictions and guidelines for password control

The password control settings configured on the **User Password Control** page take effect on all local users. To open the **User Password Control** page, access the **User** > **User Management** > **Local Users** > **Users** page and then click the **Password control** button on the menu.

You can configure the minimum password length, password complexity check, and password composition check on both the **User Password Control** page and the **Create User** or **Edit User** page. The settings configured on the **Create User** or **Edit User** page take precedence over the settings configured on the **User Password Control** page.

The **Administrator Password Control** page and the **User Password Control** page share the password control settings. If you change a password control setting on one page, the system automatically synchronizes the new setting to the other page.

After password control is enabled, the password set for a local user must have a minimum of four different characters.

For password control settings configured for a user to take effect, you must enable password control. To enable password control, click **Password control** on the **Users** page to enter the **User Password Control** page and select **Enable password control**.

Configure user management

Configure local users

You can create local users manually or import local users in bulk.

Create a local user

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **User Management** > **Local Users**.
3. Click the **Users** tab and then click **Create**. The **Create User** page opens.
4. Create a local user.

Table 3 Local user configuration items

Item	Description
Username	Enter the name of a network access user. The user accesses the network resources through the device. To implement local authentication, you must configure local users on the device
Set random password	Select to generate a random password for the user.
Receiver email	Enter the email address of the receiver to receive the random password. Before you configure this field, please enter the Email Server page to configure the email server.
Password	Enter the password of the user.
Confirm	Enter the password of the user again,
Validity period	Set the validity period of the user. Expired user accounts cannot be used for authentication. • If both the start time and end time are specified, the end time must be later than the start time. • If only the start time is specified, the user is valid since the specified time. • If only the end time is specified, the user is valid until the specified time.

Item	Description
Authorization user group	Select an authorization user group. Each local user belongs to a user group and has all attributes of the group. The attributes include the password control attributes and authorization attributes.
Identity group	Select an identity group. The user identification module controls the network access of a local user based on the identity group to which the user belongs.
Available services	Select services that the user can use. Local authentication checks the service types of a local user. If none of the service types is available, the user cannot pass authentication.
Max number of concurrent logins	Enter the maximum number of users that can concurrently access the device by using the same username. When the number of logins using a username reaches the limit, no more local users can access the device by using the username.
Description	Enter the descriptive information of the user.

5. (Optional.) Configure authorization attributes.

Table 4 Authorization attribute configuration items

Item	Description
Authorization ACL	Select an authorization ACL. The device restricts authenticated users to access only the network resources permitted by the ACL.
Idle timeout	Enter the idle cut timeout period. The device logs out a user if the user's total traffic in the idle timeout period at the specified direction is less than the specified

Item	Description
	minimum traffic.
Authorization VLAN	Enter a VLAN ID. The device restricts authenticated users to access only the network resources in the VLAN.
SSL VPN policy group	Enter an SSL VPN policy group. The device restricts authenticated users to access only the network resources specified in the SSL VPN policy group.

6. (Optional.) Configure binding attributes.

Table 5 Binding attribute configuration items

Item	Description
Access interface	Select an access interface. If the actual access interface of the user is not the same as the binding interface, the user fails authentication.
IPv4 address	Enter an IPv4 address. If the IP address of the user is not the same as the binding IPv4 address, the user fails authentication.
MAC address	Enter a MAC address. If the MAC address of the user is not the same as the binding MAC address, the user fails authentication.
VLAN	Enter a VLAN ID. If the user belongs to a VLAN different from the binding VLAN, the user fails authentication.

7. (Optional.) Configure password settings.

Table 6 Password setting configuration items

Item	Description
Min password length	Enter the minimum password length. If the password that a user enters is shorter than this value, the system rejects the password setting.
Min character types	Enter the minimum number of character types in a password. If the number of character types in the password that a user enters is less than this value, the system rejects the password setting.
Min number of characters for each type	Enter the minimum number of characters for each type in a password. If the number of characters for each type in the password that a user enters is less than this value, the system rejects the password setting.
No username or reversed username in password	Select this item to reject a password that has the username or the reverse of the username.
No more than two consecutive identical characters in password	Select this item to reject a password that has more than two identical consecutive characters.

8. Click **OK**. The user is displayed on the **Users** page.

Import local users in bulk

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **User Management** > **Local Users**.
3. Click the **Users** tab and then click **Import**. The **Import Users** page opens.
4. Import local users.

Table 7 Configuration items for importing local users

Item	Description
Import file	Specify a .CSV file for the device to import local users. Make sure the .CSV file is a standard .csv file and do not modify the annotation headers of the template. A violation might cause data loss.
Automatically create groups	Select this item to enable the device to automatically create an identity group for a user if the identity group to which the user belongs does not exist on the device. If you do not select this item, the device does not create nonexistent user groups and it assigns the user to the system-defined user group **system**.
Overriding existing user accounts	Select this item to enable the device to override an existing identity user account that has the same name as an identity user account to be imported. If you do not select this item, the device retains the existing identity user account.
Import from line	Enter the number of the line at which the account import begins. If you do not specify the line number, the device imports identity user account information from the first line.

5. Click **OK**. The imported local users are displayed on the **Users** page.

Configure password control

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **User Management** > **Local Users**.
3. Click the **Users** tab and then click **Password Control**. The **User Password Control** page opens.
4. Configure the password control settings.

Table 8 Password control configuration items

Item	Description
Enable password control	Select this item to enable password control.
Enable password length check	Select this item to enable password length check.
Min password length	Enter the minimum password length. If the password that a user enters is shorter than this value, the system rejects the password setting.
Enable password composition check	Select this item to enable password composition check.
Min number of character types	Enter the minimum number of character types in a password. If the number of character types in the password that a user enters is less than this value, the system rejects the password setting.
Min number of characters for each type	Enter the minimum number of characters for each type in a password. If the number of characters for each type in the password that a user enters is less than this value, the system rejects the password setting.
No more than two same consecutive characters in password	Select this item to reject a password that has more than two identical consecutive characters.
No username or reversed username in password	Select this item to reject a password that has the username or the reverse of the username.
Enable password history recording	Select this item to enable password history recording.
Max number of history password records	Enter the maximum number of history password records. When the number of history password records exceeds this value, the most recent record overwrites the earliest one.

Item	Description
Min password update interval	Enter the minimum password update interval. A user can only change the password once within the specified interval.

5. Click **OK**.

Manage online users

To manage online users, perform the following tasks:

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **User Management** > **Online Users**.
3. Manage online users.

Table 9 Configuration items for managing online users

Item	Description
Enable user identification	Click this button to enable the user identification feature.
Username match mode	Select a username match mode. The following modes are available: • **Keep-original**—Uses the username entered by a user to perform username match. • **With-domain**—Uses the username that includes the authentication domain name of a user to perform username match. For example, if the authentication domain is **abc** and the entered username is **test@123**, the device searches username **test@abc** in local user accounts. • **Without-domain**—Uses the username that excludes the

Item	Description
	domain name of a user to perform username match. For example, if the authentication domain is **abc** and the entered username is **test@123**, the device searches username **test** in local user accounts that do not join any identity domains.

Configure a user import policy

Create a user import policy

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **User Management** > **User Import Policies**.
3. Click **Create**. The **Create User Import Policy** page opens.
4. Create a user import policy.

Table 10 User import policy configuration items

Item	Description
Name	Enter the name of a user import policy. The name uniquely identifies a user import policy.
RESTful server	Select a RESTful server. The device imports identity users and online users from the RESTful server.
LDAP schemes	Select LDAP schemes. The device imports identity users from the LDAP servers specified in the LDAP schemes.

Item	Description
Import types	Select the type of information to be imported. This parameter is applicable only to LDAP schemes.
Enable auto import	Select this item to enable automatic user import. After this feature is enabled, the device first imports identity users and online users from the servers specified in the user import policy and then periodically imports identity users from the servers.
Import interval	Enter the automatic import interval. The device automatically imports identity users from the servers specified in the user import policy at the specified interval.

5. Click **OK**. The user import policy is displayed on the **User Import Policy** page.

Manually import users

After you configure the user import policy, you can manually import identity users and online users from the servers specified in the user import policy.

To manually import users, perform the following tasks:

- **Manually import identity users**—The device initiates user information requests to the servers, imports user account information from the servers, and then creates corresponding identity users. If the device fails to import an account, the device skips the account and continues to import the next account.
- **Manually import online users**—The device initiates a real-time online user information request to the server and then imports all online user information. The device can import online identity users only from an IMC RESTful server.

Configure the email server

The device sends a random password in an email notification to a user. Before you configure the email address of the receiver, you must configure the email server.

To configure the email server, perform the following tasks:

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **User Management** > **Email Server**.
3. Configure the email server.

Table 11 Email server configuration items

Item	Description
Email subject	Enter the subject of the email notification.
Email body	Enter the body of the email notification.
Sender address	Set the address of the email sender.
Server address	Enter the URL of the email server, which starts with smtp://.
Username	Enter the username used to log in to the email server.
Password	Enter the password used to log in to the email server.

Authentication

This help contains the following topics:

Introduction

ISP domains

AAA manages users based on the users' ISP domains. Each ISP domain maintains a set of authentication, authorization, and accounting methods to control the AAA behaviors of users in the ISP domain. The administrator can configure authentication, authorization, and accounting methods of an ISP domain based on the user access types and security requirements in the domain.

The device supports the following authentication methods:

- **No authentication**—This method trusts all users and does not perform authentication. For security purposes, do not use this method.
- **Local authentication**—The NAS authenticates users by itself, based on the locally configured user information including the usernames, passwords, and user attributes. Local authentication provides high-speed and low-cost authentication services, but the amount of information that can be stored on the NAS is restricted by the size of the storage space.
- **RADIUS authentication**—RADIUS authentication is a type of remote authentication. The NAS communicates with a remote server through the RADIUS protocol to authenticate users. The server manages user information in a centralized manner. Remote authentication provides high capacity, reliable, and centralized authentication services for multiple NASs. For high availability, you can specify multiple RADIUS servers for user authentication. In addition, you can configure backup methods to be used when the servers are not available.
- **LDAP authentication**—LDAP authentication is a type of remote authentication. The NAS communicates with a remote server through the LDAP protocol to authenticate users. LDAP defines a set of operations to implement its functions. The main operations for authentication

are the bind operation and search operation. In LDAP authentication, the client completes the following tasks:

a. Uses the LDAP server administrator DN to bind with the LDAP server. After the binding is created, the client establishes a connection to the server and obtains the right to search.

b. Constructs search conditions by using the username in the authentication information of a user. The specified root directory of the server is searched and a user DN list is generated.

c. Binds with the LDAP server by using each user DN and password. If a binding is created, the user is considered legal.

- **Single sign-on**—The NAS works with a remote server to authenticate users. The server sends the user identity information to the device configured with user identification after the users pass authentication. Then, the device uses the information to perform identification on the users to complete the authentication.

The device supports the following authorization methods:

- **No authorization**—The NAS performs no authorization exchange. The following default authorization information applies after users pass authentication:
  - Login users obtain the default user role. The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.
  - Non-login users can access the network.
- **Local authorization**—The NAS performs authorization according to the user attributes locally configured for users.
- **RADIUS authorization**—RADIUS authorization is a type of remote authorization. The NAS works with a remote server to authorize users. RADIUS authorization is bound with RADIUS authentication. RADIUS authorization can work only after RADIUS authentication is

successful, and the authorization information is included in the Access-Accept packet. You can configure backup methods to be used when the remote server is not available.

- **LDAP authorization**—LDAP authorization is a type of remote authorization. The NAS works with a remote server to authorize users. In LDAP authorization, the client performs the same tasks as in LDAP authentication except that it obtains both authorization information and the user DN list when it constructs search conditions.

The device supports the following accounting methods:

- **No accounting**—The NAS does not perform accounting for the users.
- **Local accounting**—Local accounting is implemented on the NAS. It counts and controls the number of concurrent users that use the same local user account, but does not provide statistics for charging.
- **RADIUS accounting**—RADIUS accounting is a type of remote accounting. The NAS works with a remote server for accounting. For high availability, you can specify multiple RADIUS servers for user accounting. In addition, you can configure backup methods to be used when the remote server is not available.

On a NAS, each user belongs to one ISP domain. The NAS determines the ISP domain to which a user belongs based on the username entered by the user at login. AAA manages users in the same ISP domain based on the users' access types. The device supports the following user access types:

- **Login**—Login users include Telnet, FTP, and terminal users that log in to the device. Terminal users can access through a console port.
- **LAN access**.
- **Portal**—Portal users must pass portal authentication to access the network.
- **ADVPN.**
- **SSL VPN.**
- PPP.

In a networking scenario with multiple ISPs, the device can connect to users of different ISPs. The device supports multiple ISP domains, including the system-defined ISP domain **system**. On the device, each user belongs to an ISP domain. If a user does not provide an ISP domain name at login, the device considers the user belongs to the default ISP domain. You can specify an ISP domain as the default domain.

The device chooses an authentication domain for each user in the following order:

1. The authentication domain specified for the access module.
2. The ISP domain in the username.
3. The default ISP domain of the device.

RADIUS

Overview

Remote Authentication Dial-In User Service (RADIUS) is a distributed information interaction protocol that uses a client/server model. The protocol can protect networks against unauthorized access and is often used in network environments that require both high security and remote user access.

- **RADIUS client**—The RADIUS client runs on the NASs located throughout the network. It passes user information to RADIUS servers and acts on the responses to, for example, reject or accept user access requests.
- **RADIUS server**—The RADIUS server runs on the computer or workstation at the network center and maintains information related to user authentication and network service access. The RADIUS server operates using the following process:
    a. Receives authentication, authorization, and accounting requests from RADIUS clients.
    b. Performs user authentication, authorization, or accounting.

c. Returns user access control information (for example, rejecting or accepting the user access request) to the clients.

RADIUS uses UDP to transmit packets. The RADIUS client and server exchange information between them with the help of shared keys, which are preconfigured on the client and server.

To provide AAA services to users, you need to configure the RADIUS server parameters on the access device.

Enhanced RADIUS features

- Accounting-on feature

  This feature enables the device to automatically send an accounting-on packet to the RADIUS server after the entire device reboots. Upon receiving the accounting-on packet, the RADIUS server logs out all online users that come online through the device. Without this feature, users cannot log in again after the reboot, because the RADIUS server determines that these users are still online.

  You can configure the interval for which the device waits to resend the accounting-on packet and the maximum number of retries.

- Session-control feature

  The RADIUS server dynamically changes the user authorization information or forcibly disconnect users by using session-control packets. Enable the session-control feature on the device so that the device can receive RADIUS session-control packets on UDP port 1812.

  The RADIUS session-control feature can only work with RADIUS servers running on IMC.

- Online user password change

  This feature enables the device to cooperate with the RADIUS server to allow users to change their passwords online. With this feature enabled, the device sends a RADIUS authentication request to the RADIUS server upon receiving a password change request from an online user. In the authentication request, the device carries the old user password in

RADIUS attribute 2 and the new user password in RADIUS attribute 17. If the device receives a response from the RADIUS server, the online user's password is changed successfully.

LDAP

Overview

The Lightweight Directory Access Protocol (LDAP) provides standard multiplatform directory service. LDAP uses a client/server model, and all directory information is stored in the LDAP server.

LDAP is suitable for storing data that does not often change. The protocol is used to store user information. For example, LDAP server software Active Directory Server is used in Microsoft Windows operating systems. The software stores the user information and user group information for user login authentication and authorization.

LDAP uses directories to maintain the organization information, personnel information, and resource information. The directories are organized in a tree structure and include entries. An entry is a set of attributes with distinguished names (DNs). The attributes are used to store information such as usernames, passwords, emails, computer names, and phone numbers.

LDAP attribute map

The LDAP attribute map feature enables the device to convert LDAP attributes obtained from an LDAP authorization server to device-recognizable AAA attributes based on the mapping entries. Because the device ignores unrecognized LDAP attributes, configure the mapping entries to include important LDAP attributes that should not be ignored.

An LDAP attribute can be mapped only to one AAA attribute. Different LDAP attributes can be mapped to the same AAA attribute. The LDAP attribute map defines a list of LDAP-AAA attribute

mapping entries. To apply the LDAP attribute map, specify the name of the LDAP attribute map in the LDAP scheme used for authorization.

RESTful server

The RESTful server configuration defines the related parameter settings for the device to communicate with the RESTful server. The parameters include the login account and the URIs of the RESTful server. After establishing a connection with the RESTful server, the device can import identity users and online users from the server.

Security management server set

The security management server set configuration defines the related parameters of the device to communicate with third-party servers, including the server IP address, server port, and service port number. After establishing connections with the servers, the device can receive the user login and logout information from the servers to update online users.

Restrictions and guidelines

Restrictions and guidelines: ISP domains

- Accounting for FTP users is not supported.
- If you use RADIUS and other methods for SSL VPN users in an ISP domain, make sure all the methods are in the same order in authentication and authorization.

- For successful RADIUS authorization in an ISP domain, make sure the same RADIUS scheme is used for authentication and authorization.
- If you specify multiple authentication methods for SSL VPN users in an ISP domain, the passwords of the SSL VPN users cannot be modified after they come online on the device.
- If you specify an LDAP scheme for SSL VPN users in an ISP domain, the passwords of the SSL VPN users cannot be modified after they come online on the device.
- If the server or NAS does not authorize a type of attribute to an authenticated user, the device authorizes the attribute in the ISP domain to the user.
- You cannot delete the system-defined ISP domain named **system**.
- By blocking an ISP domain, you disable offline users of the domain from requesting network services. However, the online users are not affected.

Restrictions and guidelines: RADIUS configuration

- Make sure the shared keys configured on the device are the same as the shared keys configured on the RADIUS servers.
- If you remove an actively used accounting server, the device no longer sends users' real-time accounting requests and stop-accounting requests. It does not buffer the stop-accounting requests, either. The accounting results might be inaccurate.
- Make sure the source IP address of RADIUS packets sent by the device matches the IP address of the NAS that is configured on the RADIUS servers.
- For accounting accuracy, make sure the traffic statistics units configured on the device and on the RADIUS accounting servers are the same.
- If two or more ISP domains use the same RADIUS scheme, configure the RADIUS scheme to keep the ISP domain name in usernames for domain identification.

- The device chooses servers based on the following rules:
    - When the primary server is in active state, the device first tries to communicate with the primary server. If the primary server is unreachable, the device searches for an active secondary server in the order the servers are configured.
    - When one or more servers are in active state, the device tries to communicate with these active servers only, even if the servers are unavailable.
    - When all servers are in blocked state, the device only tries to communicate with the primary server.
    - If a server is unreachable, the device changes the server status to blocked and starts a quiet timer for the server. Then, it tries to communicate with the next secondary server in active state that has the highest priority.
    - When the quiet timer of a server expires or you manually set the server to the active state, the status of the server changes back to active. The device does not check the server again during the authentication or accounting process.
    - The search process continues until the device finds an available secondary server or has checked all secondary servers in active state. If no server is reachable, the device determines that the authentication or accounting attempt fails.
- Consider the number of secondary servers when you configure the maximum number of RADIUS packet transmission attempts and the RADIUS server response timeout timer. If the RADIUS scheme includes many secondary servers, the retransmission process might be too long and the client connection in the access module, such as Telnet, can time out.
- Make sure the server quiet timer is set correctly. A timer that is too short might result in frequent authentication or accounting failures. This is because the device will continue to attempt to communicate with an unreachable server that is in active state. A timer that is too long might temporarily block a reachable server that has recovered from a failure. This is because the server will remain in blocked state until the timer expires.

- If you configure the online user password change feature together with Reply-Message attribute parsing rules, the online user password change feature cannot take effect.

Restrictions and guidelines: LDAP configuration

When the device needs to cooperate with an LDAP authorization server, you must configure related LDAP settings on the device at the CLI.

Configure authentication

To manage users of different ISPs, specify authentication, authorization, and accounting methods of different access types for each ISP domain and configure the domain attributes as needed. Domain attributes include the status of an ISP domain and authorization attributes for users in the ISP domain.

- To perform local authentication, configure local users and the related attributes.
- To perform remote authentication, configure the required RADIUS schemes.

Configure an ISP domain

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **Authentication** > **ISP Domains**.
3. Click **Create**.
4. Create an ISP domain.

Table 1 ISP domain configuration items

Item	Description
Domain name	Enter a name for the ISP domain. The ISP domain name is a case-insensitive string of 1 to 255 characters that uniquely identifies an ISP domain. The name must meet the following requirements: • It cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@). • It cannot be **d**, **de**, **def**, **defa**, **defau**, **default**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.
Status	Select a state for the ISP domain. • **Active**—Places the ISP domain in active state to allow the users in the ISP domain to request network services. • **Blocked**—Places the ISP domain in blocked state to prevent users in the ISP domain from requesting network services.
Access types	Select access types for the users in the ISP domain. Select the access type for a user based on the access authentication requirements of the user. For example, select **Login** for administrators.

5. (Optional.) Configure advanced settings.

Table 2 Advanced setting configuration items

Item	Description
Idle timeout	Set the idle timeout period. The device logs out a user if the user's total traffic in the idle timeout period is less than the specified minimum traffic.
Min traffic in an idle	Set the minimum traffic that must be generated in the idle timeout

Item	Description
timeout	period.
IP address pool	Enter the name of an IP address pool. The device assigns an IP address in the IP address pool to each authenticated PPP or portal user.

6. Click **OK**. The new ISP domain is displayed in the **ISP Domains** page.

Configure RADIUS

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **Authentication** > **RADIUS**.
3. Click **Create**.
4. Create a RADIUS scheme.

Table 3 RADIUS scheme configuration items

Item	Description
Authentication servers	Create, edit, or delete authentication servers. The configuration items include the IP address, port number, and shared key.
Accounting servers	Create, edit, or delete accounting servers. The configuration items include the IP address, port number, and shared key.
Advanced settings	Configure the advanced settings for the scheme as needed.

5. Click **OK**. The new RADIUS scheme is displayed in the **RADIUS** page.

Configure LDAP

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **Authentication** > **LDAP** > **LDAP Schemes**.
3. Click **Create**.
4. Create an LDAP scheme.

Table 4 LDAP scheme configuration items

Item	Description
Scheme name	Enter a name for the LDAP scheme. The scheme name uniquely identifies an LDAP scheme.
LDAP attribute map	Select an LDAP attribute map for LDAP authorization. The device converts LDAP attributes obtained from the LDAP authorization server to device-recognizable AAA attributes.
Server name	Enter a name for the LDAP server.
VRF	Select the VRF to which the LDAP server belongs. Do not configure this item if the LDAP server belongs to the public network.
IP address type	Select an IP address type for the LDAP server. Available IP address types include IPv4 and IPv6.
Server IP address	Enter the IP address of the LDAP server.
Port	Enter the service port number of the LDAP server.

Item	Description
Administrator DN	Enter the administrator DN. The administrator DN on the device must be the same as the administrator DN configured on the LDAP server.
Administrator password	Enter the administrator password.
LDAP version	Select an LDAP version. Available LDAP versions include LDAPv2 and LDAPv3. The LDAP version used by the device must be consistent with the version used by the LDAP server.
Server timeout period	Set the LDAP server timeout period. If the device sends a bind or search request to the LDAP server without receiving the server's response within the server timeout period, the authentication or authorization request times out.
Base DN for user search	Enter the base DN for user search. If the LDAP server contains many directory levels, a user DN search starting from the root directory can take a long time. To improve efficiency, you can change the start point by specifying the search base DN.
User search scope	Select a user search scope. • **All-level**—The user search goes through all subdirectories of the base DN. • **Single-level**—The user search goes through only the next lower level of subdirectories under the base DN.
Username attribute	Enter the value of the username attribute. The default value is **cn**.
Username format	Select a format for usernames to be sent to the LDAP server. • **With-domain**—Includes the ISP domain name in the usernames sent to the LDAP server. • **Without-domain**—Excludes the ISP domain name from the usernames sent to the LDAP server.

Item	Description
User object class	Enter a user object class for user search.
User group filter	Enter a user group filter. When the device requests to import user group information from an LDAP server, the LDAP server sends only user groups that match the user group filter to the device.

5. Click **OK**. The new LDAP scheme is displayed in the **LDAP Schemes** page.

Configure a RESTful server

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **Authentication** > **RESTful Server**.
3. Click **Create**.
4. Create a RESTful server.

Table 5 RESTful server configuration items

Item	Description
Name	Enter a name for the RESTful server. The name uniquely identifies a RESTful server.
Username	Enter the username for logging in to the RESTful server.
Password	Enter the password for logging into the RESTful server.
Get-user-account URI	Enter the URI used to request user account information from the RESTful server.

Item	Description
Get-online-user URI	Enter the URI used to request online user information from the RESTful server.
Get-user-group URI	Enter the URI used to request user group information from the RESTful server.
Put-online-user URI	Enter the URI used to upload online user information to the RESTful server. If the device adds an identity user that is not imported from the RESTful server, the device uploads the online user information to the RESTful server.
Put-offline-user URI	Enter the URI used to upload offline user information to the RESTful server. If the device deletes an identity user that is not imported from the RESTful server, the device uploads the offline user information to the RESTful server.
VRF	Select the VRF to which the RESTful server belongs. Do not configure this item if the RESTful server belongs to the public network.
Enable server detection	Select this item to enable RESTful server reachability detection. When this feature is enabled, the device detects the reachability of the RESTful server.

5. Click **OK**. The new RESTful server is displayed in the **RESTful Server** page.

Configure a security management server set

1. Click the **Objects** tab.
2. In the navigation pane, select **User** > **Authentication** > **Sec Mgt Server Set**.
3. Click **Create**.

4. Create a security management server set.

Table 6 Security management server set configuration items

Item	Description
Name	Enter a name for the security management server set. The name uniquely identifies a security management server set.
Server addresses	Enter the IP addresses of the TSM servers.
Listening port	Enter the port for listening to packets from the TSM servers.
Encryption algorithm	Select an encryption algorithm to decrypt packets from the TSM servers.
Shared key	Enter the shared key to decrypt packets from the TSM servers.

5. Click **OK**. The newly created security management server set is displayed on the **Security Management Server Set** page.

Portal

This help contains the following topics:

Introduction

Portal authentication controls user access to networks. Portal authenticates a user by the username and password the user enters on a portal authentication page. Therefore, portal authentication is also known as Web authentication.

Portal authentication flexibly imposes access control on the access layer and vital data entries. It has the following advantages:

- Allows users to perform authentication through webpages without installing client software.
- Provides ISPs with diversified management choices and extended functions. For example, the ISPs can place advertisements, provide community services, and publish information on the authentication page.

- Supports multiple authentication modes. For example, re-DHCP authentication implements a flexible address assignment scheme and saves public IP addresses. Cross-subnet authentication can authenticate users who reside in a different subnet than the access device.

A typical portal system consists of the following components:

- **Authentication client**—An authentication client is a Web browser that runs HTTP/HTTPS or a user host that runs a portal client application.
- **Access device**—An access device refers to a broadband access device such as a switch, a router, or a firewall device.
- **Portal authentication server**—The portal authentication server receives authentication requests from authentication clients and interacts with the access device to authenticate users.
- **Portal Web server**—The portal Web server pushes the Web authentication page to authentication clients and forwards user authentication information (username and password) to the portal authentication server. The portal Web server can be integrated with the portal authentication server or an independent server.
- **AAA server**—The AAA server interacts with the access device to implement authentication, authorization, accounting for portal users.

Portal authentication server

Portal authentication server detection

During portal authentication, if the communication between the access device and portal authentication server is broken, new portal users cannot log in and online portal users cannot log

out normally. To address this problem, the access device needs to be able to detect the reachability changes of the portal server quickly and take corresponding actions to deal with the changes.

The portal authentication server detection feature enables the device to periodically detect portal packets from a portal authentication server to determine the reachability of the server. If the device receives a portal packet within a detection timeout and the portal packet is valid, the device determines that the portal authentication server is reachable. Otherwise, the device determines that the portal authentication server is unreachable. Portal packets include user login packets, user logout packets, and heartbeat packets. You can configure the device to take one or more of the following actions when the server reachability status changes:

- Sending a trap message to the NMS. The trap message contains the name and current state of the portal authentication server.
- Sending a log message, which contains the name, the current state, and the original state of the portal authentication server.

Portal user synchronization

Once the access device loses communication with a portal authentication server, the portal user information on the access device and that on the portal authentication server might be inconsistent after the communication resumes. To address this problem, the device provides the portal user synchronization feature. This feature is implemented by sending and detecting portal synchronization packets, as follows:

1. The portal authentication server sends the online user information to the access device in a synchronization packet at the user heartbeat interval. The user heartbeat interval is set on the portal authentication server.
2. Upon receiving the synchronization packet, the access device compares the users carried in the packet with its own user list and performs the following operations:

- If a user contained in the packet does not exist on the access device, the access device informs the portal authentication server to delete the user. The access device starts the synchronization detection timer immediately when a user logs in.
- If the user does not appear in any synchronization packet within a synchronization detection interval, the access device considers the user does not exist on the portal authentication server and logs the user out.

Portal Web server

Parameters carried in the portal Web server URL

You can configure parameters such as the user IP address, user MAC address, and the originally-requested URL to be added into the portal Web server URL. After you configure the URL parameters, the device sends the portal Web server URL with these parameters to portal users. For example, assume that the URL of a portal Web server is **http://www.test.com/portal**, and you add the user IP address and the original URL **http://www.abc.com/welcome** to the server URL. Then, the access device sends to the user at 1.1.1.1 the URL **http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome**.

Portal Web server detection

A portal authentication process cannot complete if the communication between the access device and the portal Web server is broken. To address this problem, you can enable portal Web server detection on the access device.

With the portal Web server detection feature, the access device simulates a Web access process to initiate a TCP connection to the portal Web server. If the TCP connection can be established

successfully, the access device considers the detection successful, and the portal Web server is reachable. Otherwise, it considers the detection to have failed. Portal authentication status on interfaces of the access device does not affect the portal Web server detection feature.

- Detection parameters
  - **Detection interval**—Interval at which the device detects the server reachability.
  - **Max detection attempts**—If the number of consecutive detection failures reaches this value, the access device considers that the portal Web server is unreachable.
- Actions to take when the server reachability status changes
  - **Log**—Sends a trap message to the NMS. The trap message contains the name and current state of the portal Web server.
  - **Trap**—Sends a log message, which contains the name, the current state, and the original state of the portal Web server.

Local portal Web server

System components

The access device supports the local portal Web server feature to provide the local portal service for portal users. With this feature, the access device also acts as the portal Web server and the portal authentication server. In this case, the portal system consists of only three components: authentication client, access device, and authentication/accounting server.

Client and local portal Web server interaction protocols

HTTP and HTTPS can be used for interaction between an authentication client and a local portal Web server. If HTTP is used, there are potential security problems because HTTP packets are transferred in plain text. If HTTPS is used, secure data transmission is ensured because HTTP packets are secured by SSL.

Portal page customization

The local portal Web server supports custom portal authentication pages. You can customize multiple sets of authentication pages, compress each set of the pages to a .zip file, and upload the compressed files to the storage medium of the device.

For the local portal Web server to push authentication pages to users during portal authentication, you must specify a custom authentication page file as the default authentication page file. If no authentication page file is specified as the default authentication page file, the local portal Web server feature cannot be implemented.

Custom authentication pages

Authentication pages are HTML files. Local portal authentication requires the following authentication pages: logon page, logon success page, logon failure page, online page, system busy page, and logoff success page. You must customize the authentication pages, including the page elements that the authentication pages will use, for example, **back.jpg** for authentication page **Logon.htm**.

Follow the authentication page customization rules when you edit the authentication page files.

File name rules

The names of the main authentication page files are fixed (see Table 1).

Table 1 Main authentication page file names

Main authentication page	File name
Logon page	logon.htm
Logon success page	logonSuccess.htm
Logon failure page	logonFail.htm
Online page Pushed after the user gets online for online notification	online.htm
System busy page Pushed when the system is busy or the user is in the logon process	busy.htm
Logoff success page	logoffSuccess.htm

You can define the names of the files other than the main authentication page files. File names and directory names are case insensitive.

Page request rules

- The local portal Web server supports only Get and Post requests.
- **Get requests**—Used to get the static files in the authentication pages and allow no recursion. For example, if file **Logon.htm** includes contents that perform Get action on file **ca.htm**, file **ca.htm** cannot include any reference to file **Logon.htm**.

- **Post requests**—Used when users submit username and password pairs, log in, and log out.

Post request attribute rules

- Observe the following requirements when editing a form of an authentication page:
    - An authentication page can have multiple forms, but there must be one and only one form whose action is **logon.cgi**. Otherwise, user information cannot be sent to the local portal Web server.
    - The username attribute is fixed as **PtUser**. The password attribute is fixed as **PtPwd**.
    - The value of the **PtButton** attribute is either **Logon** or **Logoff**, which indicates the action that the user requests.
    - A logon Post request must contain **PtUser**, **PtPwd**, and **PtButton** attributes.
    - A logoff Post request must contain the **PtButton** attribute.
- Authentication pages **logon.htm** and **logonFail.htm** must contain the logon Post request.

The following example shows part of the script in page **logon.htm**.

```
<form action=logon.cgi method = post >

<p>User name:<input type="text" name = "PtUser"
style="width:160px;height:22px" maxlength=64>

<p>Password :<input type="password" name = "PtPwd"
style="width:160px;height:22px" maxlength=32>

<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
onclick="form.action=form.action+location.search;" >

</form>
```

- Authentication pages **logonSuccess.htm** and **online.htm** must contain the logoff Post request.

The following example shows part of the script in page **online.htm**.

```
<form action=logon.cgi method = post >

<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">

</form>
```

Page file compression and saving rules

- You must compress the authentication pages and their page elements into a standard zip file. The name of a zip file can contain only letters, numbers, and underscores.
- The authentication pages must be placed in the root directory of the zip file.

Redirecting authenticated users to a specific webpage

To make the device automatically redirect authenticated users to a specific webpage, do the following in logon.htm and logonSuccess.htm:

- In logon.htm, set the target attribute of Form to **_blank**.

See the contents in gray:

```
<form method=post action=logon.cgi target="_blank">
```

- Add the function for page loading pt_init() to logonSuccess.htm.

See the contents in gray:

```
<html>

<head>

<title>LogonSuccessed</title>

<script type="text/javascript" language="javascript"
src="pt_private.js"></script>

</head>
```

```
    <body onload="pt_init();" onbeforeunload="return pt_unload();">
    ... ...
    </body>
</html>
```

Portal-free rule

A portal-free rule allows specified users to access specified external websites (determined by the source and destination information in the rule) without portal authentication.

The matching items for a portal-free rule include the source/destination IP address, TCP/UDP port number, source MAC address, access interface, and VLAN. Packets matching a portal-free rule will not trigger portal authentication, so users sending the packets can directly access the specified external websites.

Interface portal policies

Portal fail-permit

The portal fail-permit feature takes effects when the portal authentication server or portal Web server is unreachable. When the access device detects that the portal authentication server or portal Web server is unreachable, it allows users on the interface to have network access without portal authentication.

BAS-IP or BAS-IPv6 attribute

The device uses the configured BAS-IP or BAS-IPv6 address as the source IP address of the portal notifications sent to the portal authentication server.

If you do not configure the BAS-IP or BAS-IPv6 attribute, the device selects the source IP address for portal packets sent to the portal authentication server as follows:

- The BAS-IP attribute of an IPv4 portal reply packet sent to the portal authentication server is the source IPv4 address of the packet. The BAS-IPv6 attribute of an IPv6 portal reply packet sent to the portal authentication server is the source IPv6 address of the packet.
- The BAS-IP attribute of an IPv4 portal notification packet sent to the portal authentication server is the IPv4 address of the packet's outgoing interface. The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the packet's outgoing interface.

Online user detection

This feature quickly detects abnormal logouts of portal users. ARP or ICMP detection applies to IPv4 portal users, and ND or ICMPv6 detection applies to IPv6 portal users.

ARP and ND detections apply only to direct and re-DHCP portal authentication. ICMP detection applies to all portal authentication modes.

If the device receives no packets from a portal user within the idle time, the device detects the user's online status as follows:

- **ICMP or ICMPv6 detection**—Sends ICMP or ICMPv6 requests to the user at configurable intervals to detect the user status.

- If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
- If the device receives no reply after the maximum number of detection attempts, the device logs out the user.

- **ARP or ND detection**—Sends ARP or ND requests to the user and detects the ARP or ND entry status of the user at configurable intervals.
  - If the ARP or ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ARP or ND entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the ARP or ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

Restrictions and guidelines

Restrictions and guidelines: Portal authentication server detection

- Only the IMC portal authentication server supports sending heartbeat packets. To test server reachability by detecting heartbeat packets, you must enable the server heartbeat feature on the IMC portal authentication server.
- You can configure the device to take one or more actions when the portal authentication server reachability status changes.

Restrictions and guidelines: Portal user synchronization

Portal user synchronization requires a portal authentication server to support the portal user heartbeat function. Only the IMC portal authentication server supports the portal user heartbeat function. To implement the portal user synchronization feature, you also need to configure the user heartbeat function on the portal authentication server. Make sure the user heartbeat interval configured on the portal authentication server is not greater than the synchronization detection timeout configured on the access device.

Restrictions and guidelines: The local portal Web server feature

- The local portal Web server feature implements only some simple portal server functions. It only allows users to log in and log out through the Web interface. It cannot take the place of independent portal Web and authentication servers.
- You can configure only one HTTP-based local portal Web server and one HTTPS-based local portal Web server.
- If an SSL server policy is specified for the HTTPS-based local portal Web server, you cannot specify port 443 as the service port number of the server.

Restrictions and guidelines: Portal-free rules

- If you specify both a VLAN and an interface, the interface must belong to the VLAN. Otherwise, the portal-free rule does not take effect.
- You cannot configure two or more portal-free rules with the same filtering criteria. Otherwise, the system prompts that the rule already exists.

- Regardless of whether portal authentication is enabled or not, you can only add or remove a portal-free rule. You cannot modify it.

Restrictions and guidelines: The BAS-IP or BAS-IPv6 attribute

- If the device runs Portal 2.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP attribute. If the device runs Portal 3.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP or BAS-IPv6 attribute.
- During a re-DHCP portal authentication, the device sends portal notification packets to the portal authentication server. For the authentication to complete, make sure the BAS-IP/BAS-IPv6 attribute is the same as the device IP or IPv6 address specified on the portal authentication server.
- You must configure the BAS-IP or BAS-IPv6 attribute on a portal authentication-enabled interface if the following conditions are met:
    - The portal authentication server is an IMC server.
    - The portal device IP address specified on the portal authentication server is not the IP address of the portal packet output interface.

IPS

This help contains the following topics:

Introduction

The Intrusion prevention system (IPS) feature enables devices to monitor network traffic for malicious activity and to proactively take prevention actions.

IPS functions

IPS provides the following functions:

- **In-depth protection**—IPS inspects the application layer data of packets, performs protocol analysis and reassembly on network traffic flows, and takes actions according to the analysis results.
- **Real-time protection**—IPS monitors network traffic in real-time and can take actions on detected attacks.
- **All-around protection**—IPS can detect and prevent the following types of attacks:
    - Malicious software such as worms, viruses, Trojan, bots, spyware, adware, scanners, and backdoors.
    - Malicious attacks such as common gateway interface (CGI) attacks, cross-site scripting attacks, injection attacks, directory traversal attacks, information leakage attacks, remote file inclusion attacks, buffer overflow attacks, code execution attacks, and DoS attacks.
- **Bidirectional protection**—IPS monitors both incoming and outgoing traffic to prevent attacks arising from the internal and external networks.

IPS profiles

IPS is implemented based on IPS profiles. An IPS profiles contains a set of IPS signatures to match packets and the actions for the matching packets.

IPS signatures

The device compares packets with IPS signatures to detect, classify, and prevent network attacks.

Each IPS signature contains various attributes, including attack category, action, protected target, severity level, and direction. By default, an IPS profile uses all enabled IPS signatures on the device. You can set criteria to filter IPS signatures that an IPS profile uses based on the signature attributes.

The device supports the following types of IPS signatures:

- **Predefined IPS signatures**—Automatically generated by the device based on the local signature library. You cannot add, modify, or delete a predefined IPS signature.
- **User-defined IPS signatures**—For attacks that cannot be detected by predefined signatures, you can create user-defined IPS signatures. You can also modify and delete user-defined signatures.
- **Snort signatures**—Imported from a Snort file. You can import and delete Snort signatures.

Predefined, user-defined, and Snort IPS signatures have default signature actions and enabling status.

To change the action for an IPS signature in an IPS profile, select the IPS signature and customize the settings for the IPS signature. If a signature in the IPS profile is not in effective state, you can change the signature state to effective. The action customized for an IPS signature takes precedence over the default signature action in the IPS profile. For more information about IPS actions, see "IPS actions." You can also add an inactive IPS signature to an IPS profile. For more information about adding an inactive IPS signature, see "Configure an IPS profile."

IPS actions

When the device detects a packet matching an IPS signature, it takes the actions specified for the signature on the packet.

The device supports the following IPS actions:

- **Blacklist**—Drops matching packets and adds the sources of the packets to the IP blacklist. If the IP blacklist feature is enabled, packets from the blacklisted sources will be blocked for the blacklist period. If the IP blacklist feature is not enabled, packets from the blacklisted sources are not blocked.

  For more information about the IP blacklist feature, see attack defense online help.
- **Drop**—Drops matching packets.
- **Permit**—Permits matching packets to pass.
- **Reset**—Closes the TCP or UDP connections for matching packets by sending TCP reset messages or ICMP port unreachable messages.
- **Redirect**—Redirects matching packets to a webpage.
- **Predefined action**—Uses the predefined signature action in the signature library to process the matching packets.
- **Capture**—Captures matching packets.
- **Logging**—Logs matching packets.

IPS mechanism

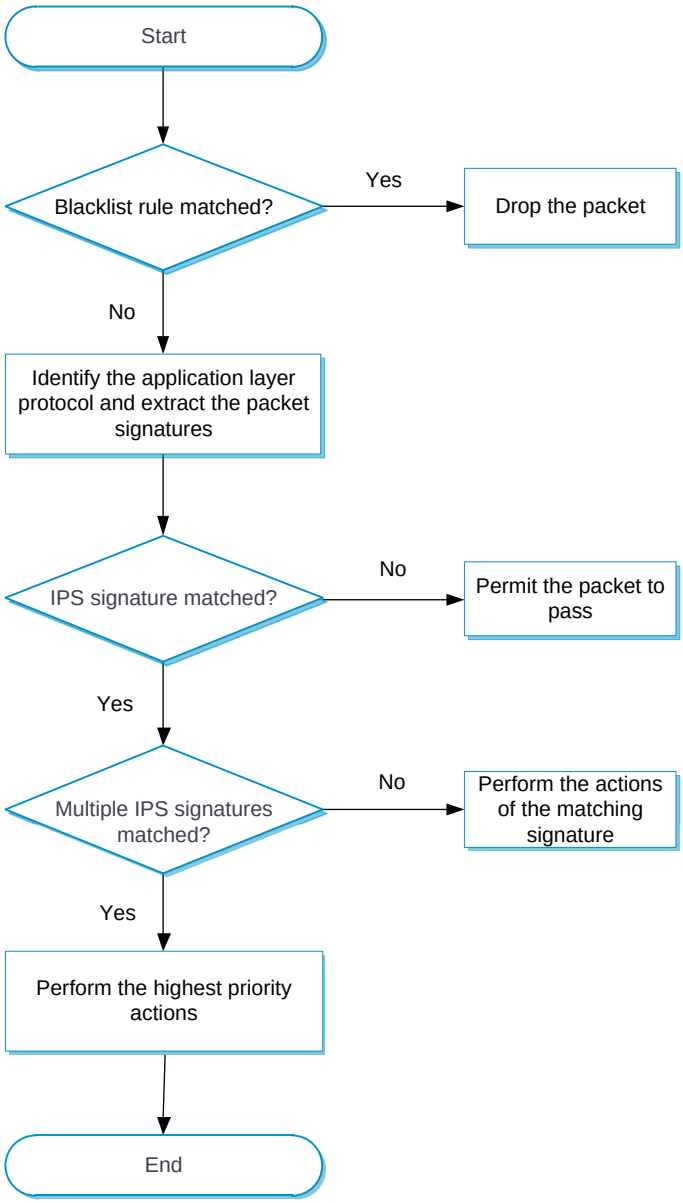
As shown in Figure 1, upon receiving a packet, the device performs the following operations:

1. The device compares the packet with the IP blacklist rules.
   - If a matching rule is found, the device drops the packet.
   - If no matching rule is found, the device goes to step 2.
2. The device compares the packet with the security policies.

   If the packet matches a security policy that is associated with an IPS profile, the device identifies the packet application layer protocol and extracts the packet signatures.

3. The device determines the actions for the packet by comparing the extracted packet signatures with the IPS signatures in the IPS profile:
    - If the packet does not match any IPS signatures, the device permits the packet to pass.
    - If the packet matches only one IPS signature, the device takes the signature actions.
    - If the packet matches multiple IPS signatures, the device uses the following rules to select the actions:
        - If the matching IPS signatures have two or more actions, including **redirect**, **drop, permit**, and **reset**, the device takes the action of the highest priority. The actions in descending order of priority are **reset**, **redirect**, **drop**, and **permit**.
        - The device will execute the **blacklist**, **capture**, and **logging** actions if they are in the matching IPS signatures.

Figure 1 IPS mechanism



Restrictions and guidelines

- After you create, edit, or delete an IPS profile, the configuration must be activated to take effect. You can click **Submit** to activate the configuration immediately or the configuration will be activated automatically 40 seconds later by default. Activating the configuration causes

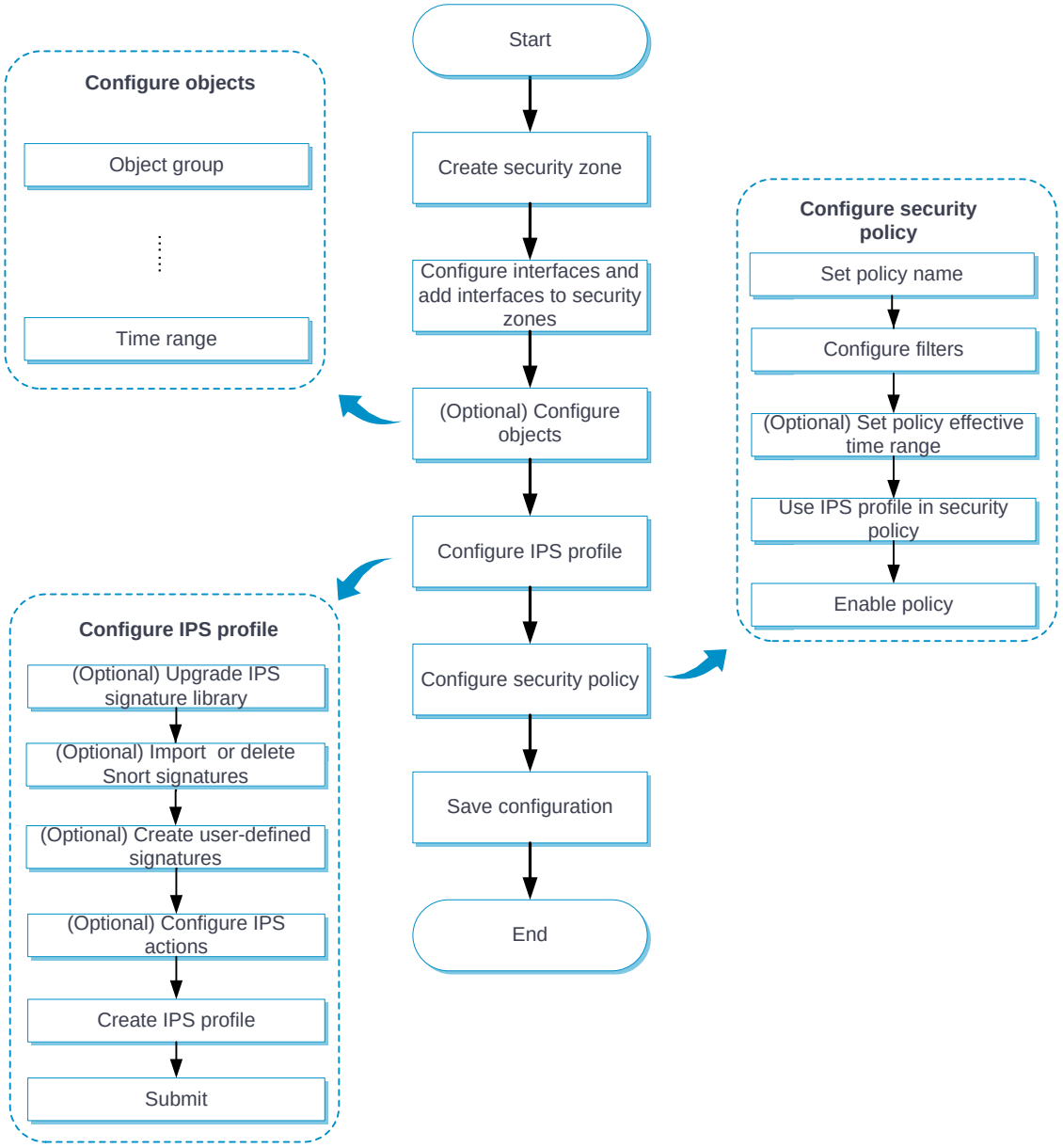
transient DPI service interruption. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.

- The IPS module requires a license to run on the device. If the license expires, you can still use the IPS functions but you can no longer upgrade the IPS signature library on the device. For more information about licenses, see license online help.
- When configuring a whitelist entry, you must enter a threat ID, URL, or IP address, or two or all of them.
- When importing Snort signatures from a Snot file, the Snort file must be encoded in UTF-8 format.

Configure IPS

Configure IPS as shown in Figure 2.

Figure 2 IPS configuration procedure



Configure an IPS profile

The device provides a predefined IPS profile named **default**. The default IPS profile uses all enabled IPS signatures on the device and cannot be modified or deleted.

You can also create IPS profiles on the device. By default, a newly created IPS profile uses all enabled IPS signatures and applies to the packet matching a signature the default signature action. You can filter the IPS signatures used by the IPS profile and change the signature actions.

You can configure global action for an IPS profile or change the action for individual IPS signatures in the profile.

The system selects the actions for packets matching an IPS signature in the following order:

1. Actions configured for the IPS signature as a signature exception in the IPS profile.
2. Global action configured for the IPS profile.
3. Default action of the IPS signature.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APP Security** > **IPS** > **Profiles**.

   The **IPS Profiles** page opens.
3. Click **Create**.

   The **Create IPS Profile** page opens.
4. Configure basic settings for the IPS profile.

Table 1 Basic configuration items for IPS profile

Item	Description
Name	Specify an IPS profile name. As a best practice, do not enter the following special characters for the name of an IPS profile: < > \ / | * ? " : , ; If you export an IPS profile with the name containing these special characters, these special characters in the IPS profile name will be replaced with underscores (_).

Item	Description
Action	Select the global action for the IPS profile. Options are **Predefined action**, **Blacklist**, **Drop**, **Permit**, **Reset**, and **Redirect**. The global action applies to all packets matching the signatures in the IPS profile.

5. Configure the criteria to filter the IPS signatures in the IPS profile.

   If you do not configure any filtering criteria, all IPS signatures in **Enabled** default status are added to the IPS profile.

Table 2 Configuration items for IPS signature filtering

Item	Description
Protected	Select the protected targets for the protected target criterion.
Attack	Select the attack categories for the attack category criterion.
Direction	Select the traffic directions for the direction criterion. Options are: • **To-server**—Client to server direction. • **To-client**—Server to client direction.
Predefined action	Select the predefined actions for the IPS signature action criterion. Options are **Drop**, **Permit**, **Reset**, and **Blacklist**.
Severity level	Select the severity levels for the severity level criterion. Options are **Critical**, **High**, **Medium**, and **Low**.
Predefined status	Select the predefined statuses for the predefined IPS signature status criterion. Options are **Enabled** and **Disabled**.

6. Click **Search**. View the IPS signatures in the **Viewing matching signatures** section.
    - To view the IPS signatures used in the IPS profile, click the **Active Signatures** tab.
    - To view the IPS signatures that are not used by the IPS profile, click the **Inactive Signatures** tab.
7. To change the status or action for an active or inactive IPS signature:
    a. Select the IPS signature on the **Active Signatures** or **Inactive Signatures** tab.
    b. Click **Custom**.
    c. In the dialog box that opens, configure the settings as needed, and then click **OK**.
8. To add an inactive IPS signature to the IPS profile:
    a. Select the IPS signature on the **Inactive Signatures** tab, and click **Custom**.
    b. In the dialog box that opens, select **Enable** for the **Status** field, and then click **OK**.

    The IPS signature will be displayed on the **Active Signatures** tab.
9. To remove an IPS signature from the IPS profile:
    a. Select the IPS signature on the **Active Signatures** tab, and click **Custom**.
    b. In the dialog box that opens, select **Disable** for the **Status** field, and then click **OK**.

    The IPS signature will be displayed on the **Inactive Signatures** tab.
10. Click **Advanced settings**.
11. In the dialog box that opens, configure the advanced settings for the IPS profile.

Table 3 Advanced configuration items for IPS profile

Item	Description
Count policy matches	Enable whether to enable match counting for the IPS profile.

Item	Description
Log settings	Select the method to configure the logging settings. Options are: • **Global**—View or edit the global settings on the **Log Settings** > **Threat Log Settings** > **IPS Logs** page in the **System** tab. • **User-defined**—Continue with logging settings on this page.
Log output	This field is only available after you select **User-defined** for the **Log settings** field. Options are **Output system logs** and **Output through email**. You can select both options at the same time.
Sig. library baseline version	Select a signature library baseline version to enable IPS to use the signatures in the baseline version in addition to the signatures in the current active signature library to match packets. With a signature library baseline version selected, the newly added signatures are in inactive state and cannot be used to match packets. To change the status of those signatures, perform the following tasks: 1. If the current version with newly added signatures is higher than the baseline version, configure the current version number as the baseline version number. 2. If the current version with newly added signatures is lower than the baseline version, select the signatures and click **Custom** to enable the signatures.
Email server	After you select **Output through email** for the **Log output** field, an email server must be configured. You can configure a new email server or select an existing email server. To view or edit the existing email servers, go to the **Log Settings** > **Email Server** page in the **System** tab.
Email output condition	Configure the filtering criteria of the matching IPS signatures for log output via email.
Min. signature severity level	Specify the lowest severity level of the matching IPS signatures for log output via email. The system outputs logs via email only when the severity levels of the matching signatures are not lower than specified severity level.

12. Click **OK**.

The IPS profile is displayed on the **IPS Profiles** page.

13. Use the IPS profile in a security policy. For more information about security policies, see security policy online help.

14. Click **Submit** to activate the configuration immediately or wait 40 seconds for the configuration to be activated automatically.

    After you create an IPS profile, the configuration must be activated to take effect. By default, the configuration will be activated automatically 40 seconds later.

15. To export the IPS signatures used in the IPS profile, click the  icon in the **Export signatures** column for the IPS profile entry in **IPS Profiles** page.

    All IPS signatures in the signature library will be exported to a .csv file, but the IPS signatures used in this IPS profile will be marked **Y** in the **Active** column of the export file.

Import or delete Snort signatures

Import Snort signatures

To add Snort signatures, create an IPS signature file in the Snort format and import the signatures from the file to the device.

Make sure the IPS signature file contains all user-defined signatures that you want to use. All existing Snort signatures on the device will be overwritten by the imported Snort signatures.

For a signature defined by a Snort rule to be imported correctly from the IPS signature file, make sure Snort rule is valid.

To import Snort signatures:

1. Click the **Objects** tab.

2. In the navigation pane, select **APP Security** > **IPS** > **Signatures**.

The **IPS Signatures** page displays all IPS signatures on the device.

3. Click **Import Snort signatures** in the upper-left corner of the page.

   The **Import Snort Signatures** window opens.

4. Select the IPS signature file to import.

5. Click **Import signatures**.

Delete all Snort signatures

1. Click the **Objects** tab.

2. In the navigation pane, select **APP Security** > **IPS** > **Signatures**.

   The **IPS Signatures** page opens.

3. Click **Delete signatures** and then select **Delete all Snort signatures** in the upper-left corner of the page.

4. Click **Yes** in the confirmation dialog box that opens.

Create and delete user-defined IPS signatures

You can create user-defined signatures that do not exist in the current signature library.

A user-defined IPS signature contains basic settings and rules.

A user-defined signature can contain multiple rules. The logical operators between rules are as follows:

- **Logical AND**—A packet matches an IPS signature only when the packet matches all rules in the signature.
- **Logical OR**—A packet matches an IPS signature when the packet matches any rule in the signature.

In a user-defined signature rule, you can configure the match criteria of source IPv4 address, destination IPv4 address, source port, destination port, and request method, the detection items, and the detection trigger conditions.

A user-defined signature can be one of the following types:

- **Keyword**—A keyword type requires configuring one or multiple detection items and only one detection trigger condition. The device continues to compare a packet with detection items only after the packet matches the detection trigger condition. A packet matches a rule only when the packet matches all detection items in the rule.
- **Number**—A number type requires configuring only one detection item. A packet matches a rule only when the packet matches the detection item in the rule.

Create a user-defined IPS signature

1. Click the **Objects** tab.
2. In the navigation pane, select **APP Security** > **IPS** > **Signatures**.

   The **IPS Signatures** page displays all IPS signatures on the device.
3. Click **Create user-defined signature**.
4. On the page that opens, configure basic settings for a user-defined IPS signature.

Table 4 Basic configuration items for an IPS signature

Item	Description
Name	Enter an IPS signature name.
Description	Enter a description for easy identification.
Severity level	Select the severity level of the risk impacts that the matching packets might bring to the network.

Item	Description
	Options are **Critical**, **High**, **Medium**, and **Low**.
Direction	Select the traffic direction for the direction criterion. Options are: • **To-server**—Client to server direction. • **To-client**—Server to client direction. • **To-server, To-client**—Both client-to-server and server-to-client directions.
Action	Select the action for packets matching the IPS signature. Options are **Blacklist**, **Drop**, **Permit**, and **Reset**.
Logging	Select whether to enable logging for matching packets. Options are **Enable** and **Disable**.
Capture	Select whether to enable capture matching packets. Options are **Enable** and **Disable**. The capture action enables the device to capture packets and export the captured packets to the specified URL at the scheduled export time. For more information about configuring the capture action, see security actions online help.

5. In the **Rules** area, select a logical operator before you configure rules for the signature.
6. Click **Create**.
7. On the page that opens, configure basic settings for the rule.

Table 5 Basic configuration items for a rule

Item	Description
ID	Enter a rule ID.
Match pattern type	Select a signature match pattern type. Options are **Keyword** and **Number**.

Item	Description
Application layer protocol	Select an application layer protocol as a filtering criterion.
Transport layer protocol	Select a transport layer protocol as a filtering criterion.
Request method	Select an HTTP request method, such as GET and POST.
Source IPv4 address	Enter a source IPv4 addresses as a filtering criterion.
Source port range	Specify a source port range as filtering criteria.
Destination IPv4 address	Enter a destination IPv4 addresses as a filtering criterion.
Destination port range	Specify a range of destination ports as filtering criteria.

8. In the **Detection trigger conditions** area, click **Create**.

   This area is available only when **Keyword** has been selected as the match pattern type.

9. Create a detection trigger condition.

Table 6 Detection trigger condition configuration items

Item	Description
Protocol field	Select a protocol field to inspect.
Match pattern type	Select the type of the match pattern. Options are **Text** and **Hex**.
Match pattern	Enter the content of the match pattern.
Depth	Specify the number of bytes to be inspected

Item	Description
Offset	Enter an offset in bytes after which the inspection starts. The offset is counted from the beginning of the protocol field.

10. Click **OK**.

    The detection trigger condition is displayed on the **Detection trigger conditions** list.

11. In the **Detection items** area, click **Create**.

12. Create a detection item.

Table 7 Detection item configuration items

Item	Description
ID	Enter a detection item ID.
Protocol field	Select a protocol field.
Operator	Select an operator to define the match operation in the detection item. Options vary by the match pattern type selected in the **Create Rule** page: • If **Keyword** has been selected, the options are **Contain** and **Not contain**. • If **Number** has been selected, the options are **Greater than**, **Equal to**, **Not equal to**, **Less than**, **Greater than or equal to**, and **Less than or equal to**.
Match pattern type	Select the type of the match pattern. Options are **Text**, **Regular expression**, and **Hex**.
Match pattern	Enter the content of the match pattern.
Depth	Specify the number of bytes to be inspected.
Offset	Enter an offset in bytes after which the inspection starts. The offset is

Item	Description
	counted from the beginning of the protocol field.
Relative depth	Specify the number of bytes to be inspected.
Relative offset	Enter an offset after which the inspection starts. The offset is counted from the end of the previous detection item.

13. Click **OK**.

    The detection item is displayed on the **Detection items** list.

14. Click **OK**.

    The rule is displayed on the **Rules** list.

15. Click **OK**.

    The signature is displayed on the **IPS Signatures** page.

16. To have the configuration take effect, click **Submit**.

Delete user-defined IPS signatures

1. Click the **Objects** tab.
2. In the navigation pane, select **APP Security** > **IPS** > **Signatures**.

   The **IPS Signatures** page opens.
3. Select the user-defined signatures that you want to delete.
4. Click **Delete signatures** and then select **Delete user-defined signatures**.
5. Click **Yes** in the confirmation dialog box that opens.

Export all signatures in the signature library

1. Click the **Objects** tab.
2. In the navigation pane, select **APP Security** > **IPS** > **Signatures**.

   The **IPS Signatures** page opens.
3. Click **Export all signatures**.

   All IPS signatures in the signature library will be exported to a .csv file.

Configure IPS whitelist

If false alarms exist in threat logs, you can enable the whitelist feature, and add the detected threat IDs (the IPS signature IDs), URLs, and IP addresses to the whitelist. The device permits packets matching the IPS signatures or URLs on the whitelist to pass through, reducing false alarms.

After the whitelist is enabled, the device will record the hit count for each whitelist entry. You can view the statistics on the **Whitelist** page.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APP Security** > **IPS** > **Whitelist**.

   The **Whitelist** page displays all whitelist entries on the device.
3. Create a whitelist entry.

Table 8 Whitelist entry configuration items

Item	Description
Entry ID	Enter a whitelist entry ID.
Description	Enter a description for the whitelist entry.
Threat ID	Enter a threat ID. You can obtain the threat ID from threat logs.
URL	Enter a URL. You can obtain the URL from threat logs. A URL contains packet header fields and packet first line, for example 111.15.93.166/wnm/get.j. After you create, edit, or delete URLs, you must click **Activate** to have the configuration take effect.
Match type	Select a match type. Options are: • **Exact match**—Deems a match if the detected URL in the packet is exactly the same as the configured URL. • **Substring match**—Deems a match if the detected URL in the packet contains the configured URL.
IP type	Select the type of IP addresses that can be obtained from threat logs. Options are **IPv4** and **IPv6**.
IP address	Enter an IP address. You can obtain the IP address from threat logs.

4. Click **OK**.
5. Click **Enable whitelist**.

Anti-virus

This help contains the following topics:

Introduction

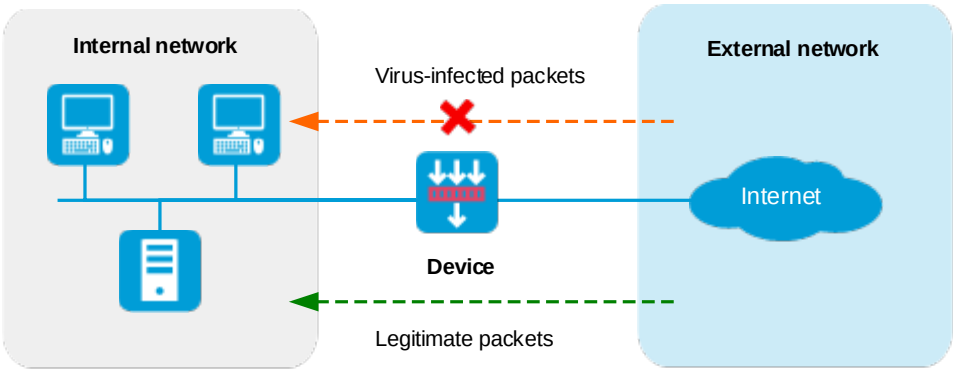
Anti-virus identifies viruses in the application layer of packets based on an up-to-date virus signature library and takes actions to prevent a network from being infected. This feature is typically deployed on a gateway to insulate the internal network from viruses and protect the internal data.

Application scenario

As shown in Figure 1, the device is the gateway of an internal network. Internal users access the external network and download data from the external network. The internal server accepts data uploaded by external users.

In this scenario, you can configure anti-virus on the gateway to protect the internal network. Anti-virus inspects incoming packets, permits legitimate packets to pass, and takes actions, such as alert, block, or redirect, on packets containing viruses.

Figure 1 Anti-virus application scenario



Basic concepts

Virus signature

A virus signature is a character string that uniquely identifies a specific virus. The virus signature library contains the predefined virus signatures.

MD5 rules

An MD5 rule is generated by the system based on the virus signatures in the virus signature library to identify virus-infected files.

Virus exception

Typically, anti-virus takes anti-virus actions on packets matching virus signatures. If a virus proves to be a false alarm, you can set the virus signature as a virus exception. Packets matching the virus exception are permitted to pass.

Application exception

Typically, anti-virus action is protocol specific and applies to all applications carried by the protocol. To take a different action on an application, you can set the application as an exception and specify a different anti-virus action for the application. Application exceptions use application-specific actions and the other applications use protocol-specific actions. For example, the anti-virus action for HTTP is permit. To block the games carried by HTTP, you can set the games as application exceptions and specify the block action for them.

MD5 value exception

If a packet is detected to contain a virus but actually the packet is safe, you can set the MD5 value of the virus as an MD5 value exception. The device will permit subsequent packets matching the MD5 value exception to pass.

You can get the MD5 value of a virus through the threat log.

Anti-virus action

Anti-virus actions apply to the packets that match virus signatures. The actions include the following types:

- **Alarm**—Permits matching packets and generates logs.
- **Block**—Blocks matching packets and generates logs.
- **Redirect**—Redirects matching HTTP connections to a URL and generates logs.
- **Permit**—Permits matching packets.

Virus detection methods

The device supports the following virus detection methods:

- **Virus signature-based detection**—The device matches packets against virus signatures in the virus signature library, and determines that a packet contains viruses if a match is found.
- **MD5 rule-based detection**—The device generates an MD5 hash value for a file to be inspected and compares the value with the system-defined MD5 rules. If a match is found, the file is identified to be virus-infected.

Cloud query

You can enable cloud query in an anti-virus profile. If the file in a packet does not match any local virus signature or MD5 rule, the device will send the MD5 value of the file to the cloud server for cloud query. The device determines the action to apply according to the query result returned from the cloud server.

- If the MD5 value of the file matches an MD5 rule, the file is considered to be virus-infected and the anti-virus action will apply.
- If no matching rule is found for the MD5 value or if the file is verified to be virus-free, the packet will be permitted to pass through.

Anti-virus mechanism

As shown in Figure 2, upon receiving a packet, the anti-virus device performs the following operations:

1. The device compares the packet with the security policies.

If the packet matches a security policy that is associated with an anti-virus policy, the device continues to identify the application layer protocol of the packet.

2. The device identifies whether the anti-virus supports the application layer protocol of the packet.

- If not, the device permits the packet to pass without anti-virus inspection.
- If yes, the device compares the packet with the virus signatures and MD5 rules.

3. If a matching signature or MD5 rule is found, the device performs following operations:

a. Determines if the matching signature is an exception. If yes, the device permits the packet to pass. If not, the device examines whether the application is an exception.

b. If the application is an exception, the device takes the application-specific action (alert, block, or permit). If the application is not an exception, the device takes the protocol-specific action (alert, block, or redirect).

4. If no matching signature or MD5 rule is found, the device performs the following operations:

a. Determines if the MD5 value of the file in the packet is an MD5 value exception.

– If yes, the device permits the packet to pass.

- If not, the device sends the MD5 value of the file in the packet to the cloud server.

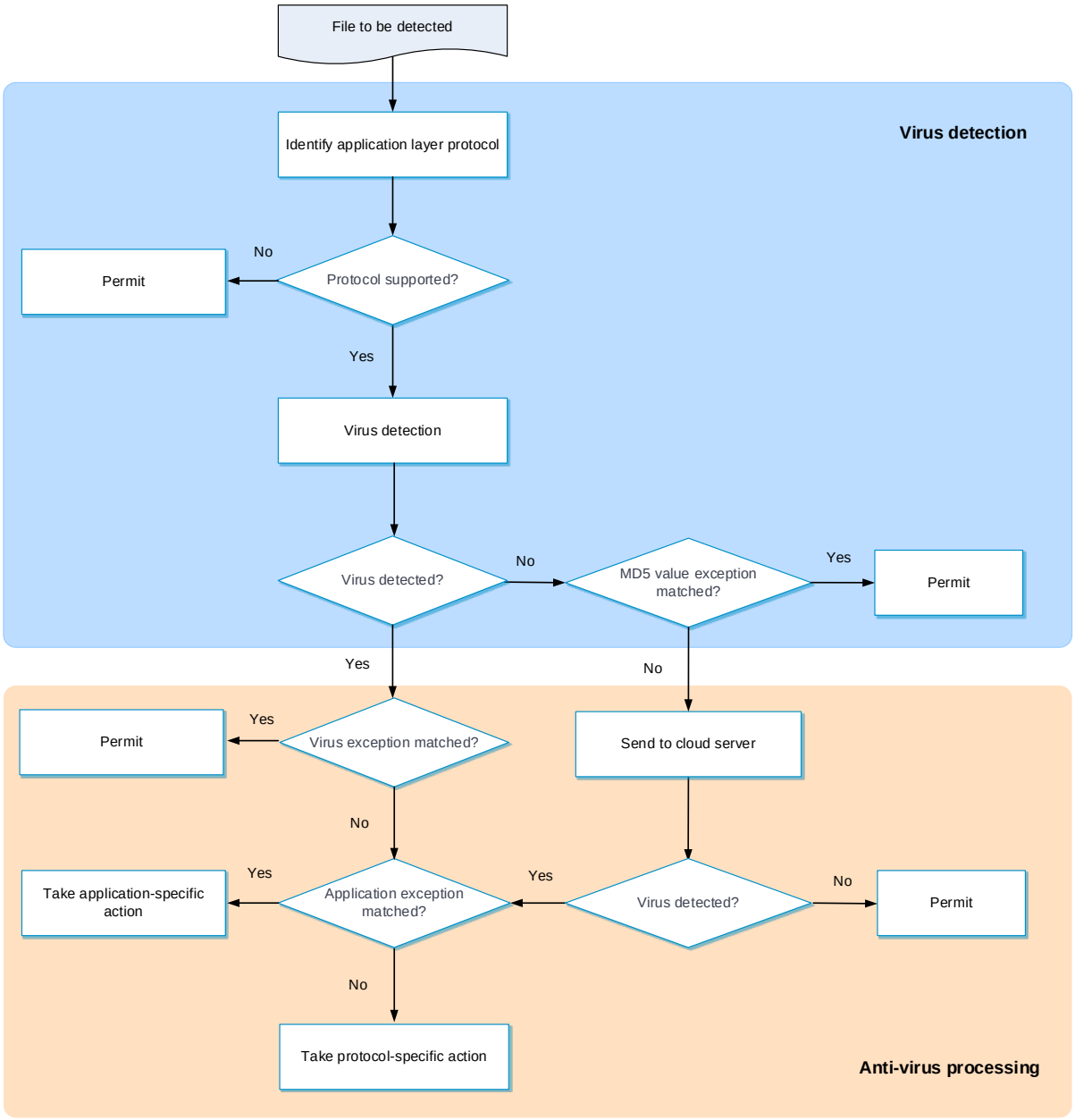
b. If cloud query is disabled in the anti-virus policy, the device permits the packet to pass.

c. If cloud query is enabled in the anti-virus policy but the cloud server does not detect any virus, the device permits the packet to pass.

d. If cloud query is enabled in the anti-virus policy and the cloud server detects the virus, the device determines if the application is an exception.

   - If yes, the device takes the application-specific action (alert, block, or permit).
   - If not, the device takes the protocol-specific action (alert, block, or redirect).

Figure 2 Anti-virus mechanism



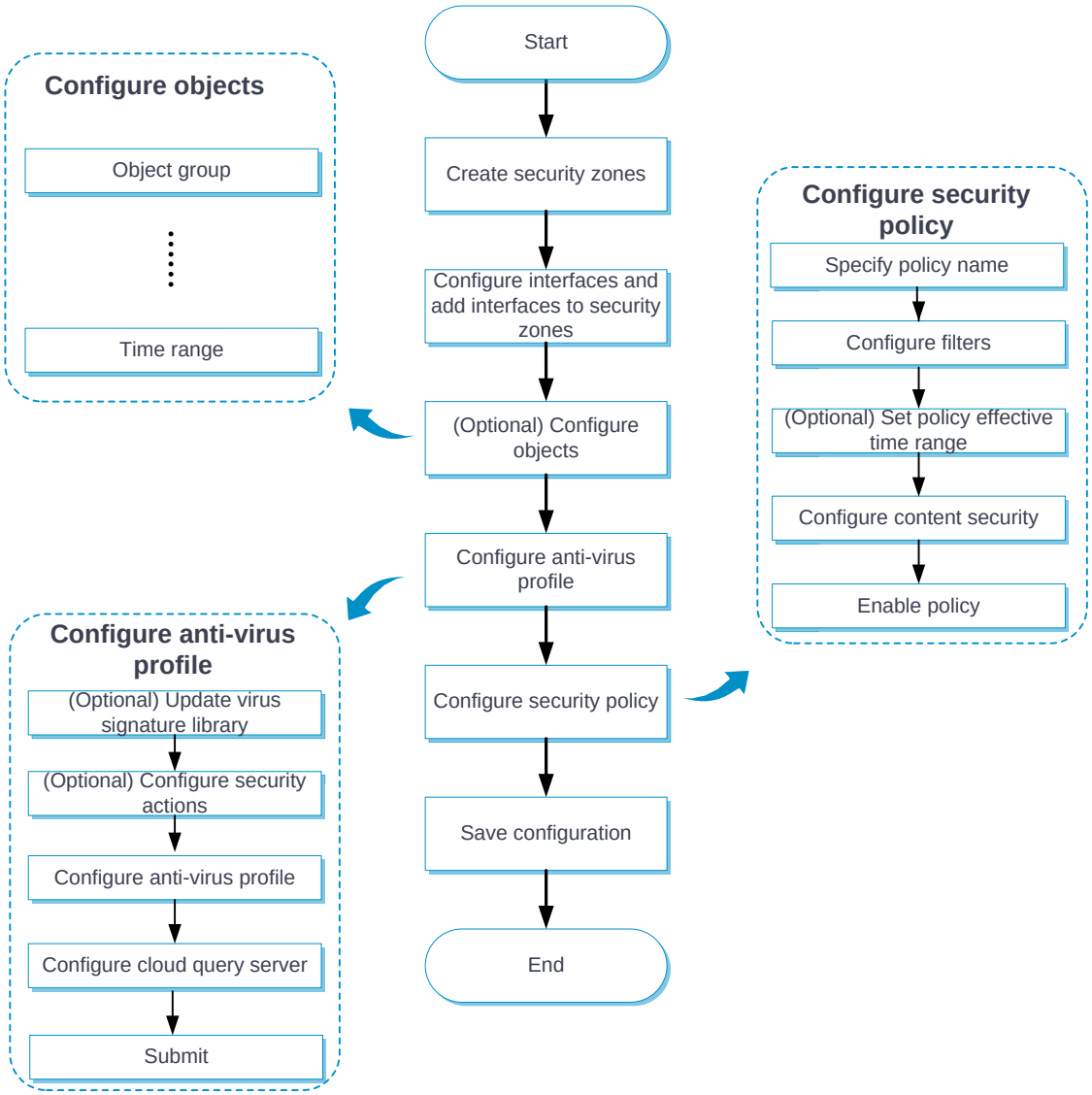
Restrictions and guidelines

- After you create, edit, or delete an anti-virus profile, the configuration must be activated to take effect. You can click **Submit** to activate the configuration immediately or the configuration will be activated automatically 40 seconds later by default. Activating configuration causes transient DPI service interruption. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.
- The anti-virus feature requires a license to run on the device. If the license expires, the anti-virus feature is still available but you can no longer update the virus signature library on the device or use cloud query or sandbox collaboration. For more information about licenses, see the license management online help.
- The cloud query feature is available only for HTTP, IMAP, NFS (read operations only), POP3, and SMTP traffic.
- After you select an alarm template in an anti-virus profile, the **capture** IPS action will no longer take effect on HTTP protocol packets that matching IPS signatures.

Configure anti-virus

Configure anti-virus as shown in Figure 3.

Figure 3 Anti-virus configuration procedure



Configure an anti-virus profile

By default, the device provides a predefined anti-virus profile named **default**, which cannot be modified or deleted.

You can customize anti-virus profiles as needed.

For all protocols that anti-virus supports, the connection requests are always initiated by the client. For anti-virus to work correctly, make sure the security policy that uses the anti-virus profile meets the following requirements:

- The security zone where the client resides is set as the source security zone.
- The security zone where the server resides is set as the destination security zone.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APP Security** > **Anti-Virus** > **Profiles**.
3. Click **Create**.
4. Create an anti-virus profile.

Table 1 Anti-virus profile configuration items

Item	Description
Name	Enter a name for the anti-virus profile.
Description	Enter a description for the anti-virus profile.
Enable cloud query	Select this item to enable cloud query.
Alarm message template	Select an alarm template. This template enables the device to send an alarm message to the client when a virus is detected. This item is supported only when you define the **Block** action on the upload and download HTTP traffic. After creating or applying an alarm message template, you can click **Edit** to import an alarm message. Only TXT or HTML files are supported. After you select an alarm template, the **capture** IPS action will no longer take effect on HTTP protocol packets that matching IPS

Item	Description
	signatures. Support for this item depends on the device model.
Upload	Select this item for a protocol to apply the profile to the upload traffic of the protocol. This item is not available for the POP3 protocol.
Download	Select this item for a protocol to apply the profile to the download traffic of the protocol. This item is not available for the SMTP protocol.
Action	Select the action for matching packets from the **Action** list of a protocol. Supported actions are **Alarm**, **Block**, and **Redirect**. The IMAP protocol supports only the **Alarm** action.
Application exceptions	To set an application as an application exception, select the application, and then click **Add** to add it to the application exception list. On the application exception list, select the action for the application exception from the **Action** list.
Virus exceptions	To set a virus as a virus exception, enter the virus ID, and then click **Add** to add it to the virus exception list.
MD5 value exceptions	To set the MD5 value of a virus as an MD5 value exception, enter the MD5 value, and then click **Add** to add it to the MD5 value exception list.

5. Click **OK**.
6. Use the anti-virus profile in a security policy. For more information about security policies, see the security policy online help.
7. Click **Submit** to activate the configuration immediately or wait 40 seconds for the configuration to be activated automatically.

   After you create an anti-virus profile, the configuration must be activated to take effect. By default, the configuration will be activated automatically 40 seconds later.

Configure the cloud query server

Perform this task to configure the cloud query server for anti-virus.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APP Security** > **Anti-Virus** > **Profiles**.
3. Click **Configure** next to the **Cloud server connectivity** field.
4. Configure the cloud query server.

Table 2 Cloud query server configuration items

Item	Description
Server address	Enter the IP address or hostname of the cloud query server. Only the cloud query server of our company is supported.
Max cached MD5 entries	Specify the maximum number of MD5 entries that can be cached in the hit entry list and non-hit entry list. The non-hit entry list is a list of MD5 values submitted to the cloud server that cannot be determined as viruses. The hit entry list is a list of MD5 values that are determined as viruses.
Min cache time	Specify the minimum cache time for an MD5 entry in minutes. Setting the minimum cache time for MD5 entries ensures that the entries will not be deleted during the specified period of time. However, if the value of configured max cached MD5 entries is less than the value of currently cached entries, the system will delete the oldest cache entries even if their cache periods are equal to or less than the minimum cache time.

Data filtering

This help contains the following topics:

Introduction

Data filtering filters packets based on application layer information. You can use data filtering to effectively prevent leakage of internal information, distribution of illegal information, and unauthorized access to the Internet.

Data filtering supports filtering packets of the following protocols:

- HTTP.
- FTP.

- SMTP.
- IMAP.
- NFS.
- POP3.
- RTMP.
- SMB.

Basic concepts

Keyword

The device provides a list of predefined keywords and allows you to create user-defined keywords in a keyword group.

- **Predefined keyword**—Includes **Phone**, **Bank card**, **Credit card**, and **ID card**. These keywords can be used to identify packets that contain phone numbers, bank card numbers, credit card numbers, and ID card numbers.
- **User-defined keyword**—A text- or regular expression-based string to identify patterns in the application layer data of packets.

Keyword group

A keyword group is a group of up to 32 keywords. A packet matches a keyword group if it matches a keyword in the group. You can enable or disable predefined keywords and create new keywords in a keyword group.

Data filtering rule

A data filtering rule contains a set of packet filtering criteria and the actions for matching packets. The packet filtering criteria include keyword group, direction (**Upload**, **Download**, or **Both**), and applications. The packet processing actions include **Drop**, **Permit**, and **Logging**. A packet must match all the filtering criteria for the actions specified for the rule to apply.

Data filtering mechanism

Upon receiving a packet of a protocol that data filtering supports, the device performs the following operations:

1. Compares the packet with the security policies.

   If the packet matches a security policy that is associated with a data filtering profile, the device extracts the application layer information from the packet.

2. Determines the actions to take on the packet by comparing the extracted application layer information with the data filtering rules in the data filtering policy:
   - If the packet does not match any data filtering rules in the policy, the device permits the packet to pass.
   - If the packet matches only one rule, the device takes the actions specified for the rule.
   - If the packet matches multiple rules, the device determines the actions as follows:
     - If the matching rules have both the permit and drop actions, the device takes the drop action.
     - If the logging action is specified for any of the matching rules, the device logs the packet.

Restrictions and guidelines

Restrictions and guidelines: Profile activation

After you create, edit, or delete a data filtering profile, the configuration must be activated to take effect. You can click **Submit** to activate the configuration immediately or the configuration will be activated automatically 40 seconds later by default. Activating the configuration causes transient DPI service interruption. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.

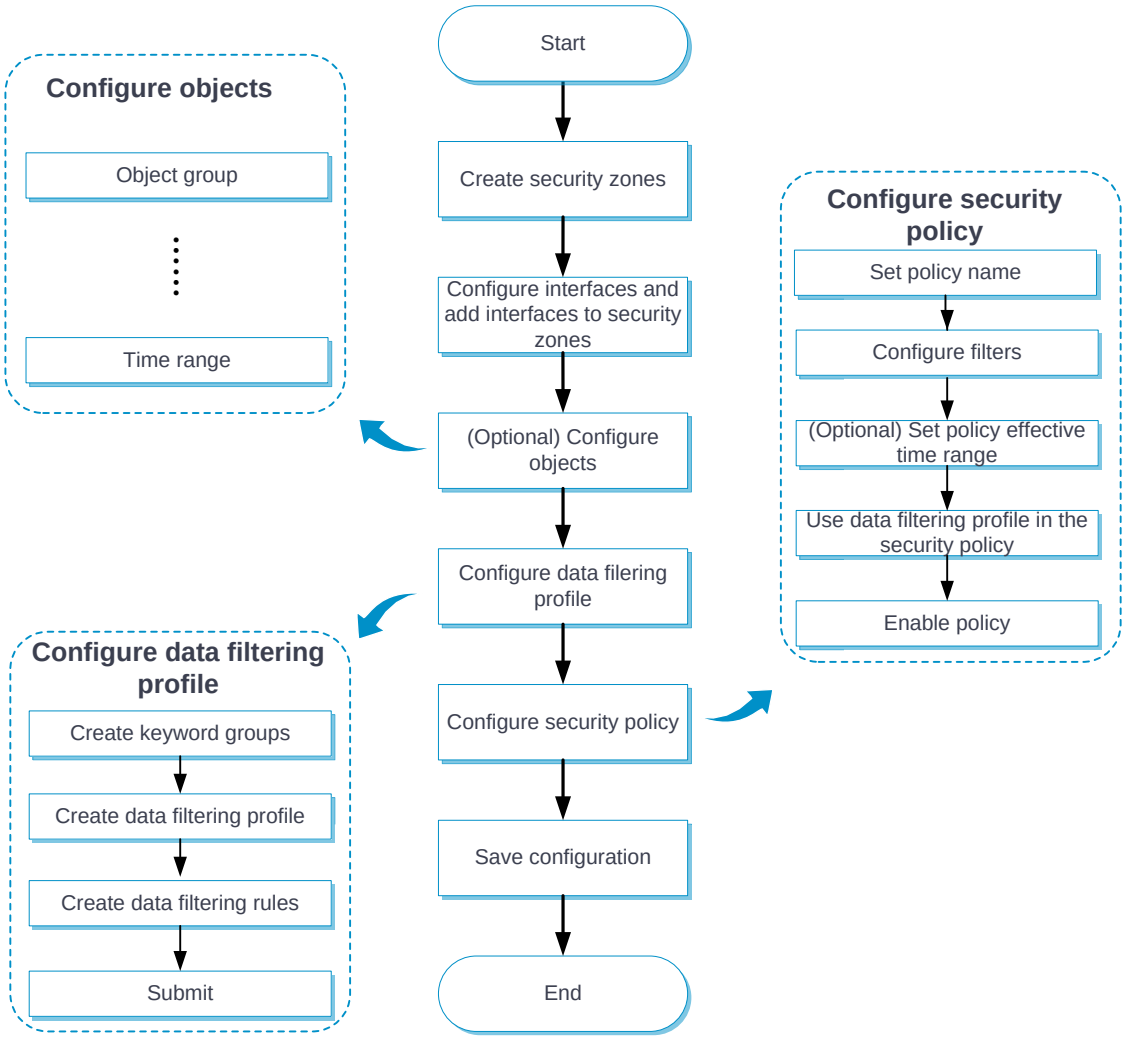
Restrictions and guidelines: Regular expression-based keyword match pattern configuration

- The regular expression pattern can contain a maximum of four branches. For example, **'abc(c|d|e|\x3D)'** is valid, and **'abc(c|onreset|onselect|onchange|style\x3D)'** is invalid.
- Nested braces are not allowed. For example, **'ab((abcs*?))'** is invalid.
- A branch cannot be specified after another branch. For example, **'ab(a|b)(c|d)^\\r\\n]+?'** is invalid.
- A minimum of four non-wildcard characters must exist before an asterisk (*) or question mark (?). For example, **'abc*'** is invalid and **'abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN'** is valid.

Configure data filtering

Configure data filtering as shown in Figure 1.

Figure 1 Data filtering configuration procedure



Configure a keyword group

Perform this task to create a keyword group and configure keywords in the keyword group.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APPSecurity** > **Data Filtering** > **Keyword Groups**.

3. On the page that appears, click **Create**.

4. Create a keyword group.

Table 1 Keyword group configuration items

Item	Description
Name	Enter a name for the keyword group.
Description	Enter a description for the keyword group.

5. In the Predefined **keyword list** area, select **Enable** for a predefined keyword. For example, to identify packets that contain phone numbers, select Enable for Phone.

6. In the User-defined **keyword list** area, click **Create**.

7. Create a keyword.

Table 2 Keyword configuration items

Item	Description
Name	Enter a name for the keyword.
Type	Select the type of the keyword match pattern. Options are: • **Text**—Select this option to configure a text-based match pattern for exact match. • **Regular expression**—Select this option to configure a regular expression-based match pattern for fuzzy match.
Match pattern	Enter the content of the keyword match pattern.

8. Click **OK**.

The keyword is displayed on the user-defined keyword list.

You can add a maximum of 32 more keywords to the keyword group.

9. Click **OK**.

   The keyword group is displayed on the **Keyword Groups** page.

Configure a data filtering profile

Perform this task to create a data filtering profile and configure data filtering rules in the profile.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APPSecurity** > **Data Filtering** > **Profiles**.
3. On the page that appears, click **Create**.
4. Create a data filtering profile.

Table 3 Data filtering profile configuration items

Item	Description
Name	Enter a name for the data filtering profile.
Description	Enter a description for the data filtering profile.

5. In the **Data filtering rules** area, click **Create**.
6. Create a data filtering rule.

Table 4 Data filtering rule configuration items

Item	Description
Name	Enter a name for the data filtering rule.
Keyword group	Select an existing keyword group or create a keyword group.
Applications	Select the application layer protocols of the applications to which the rule applies. Supported application layer protocols are FTP, HTTP, IMAP, NFS, POP3, RTMP, SMB, and SMTP.
Direction	Select the traffic direction to which the rule applies. Options are **Upload**, **Download**, and **Both**.
Action	Select the action for matching packets. Options are **Permit** and **Drop**.
Logging	Select whether to enable logging for matching packets. Options are **Enable** and **Disable**.

7. Click **OK**.

   The data filtering rule is displayed on the data filtering rule list of the data filtering profile.

8. Click **OK**.

   The data filtering profile is displayed on the **Data Filtering Profiles** page.

9. Use the data filtering profile in a security policy. For more information about security policies, see security policy online help.

10. Click **Submit** to activate the configuration immediately or wait 40 seconds for the configuration to be activated automatically.

    After you create a data filtering profile, the configuration must be activated to take effect. By default, the configuration will be activated automatically 40 seconds later.

File filtering

This help contains the following topics:

Introduction

The file filtering feature filters files based on file extensions. You can configure file filtering to perform actions on files based on the file extensions.

File filtering supports filtering packets of the following protocols:

- HTTP.
- FTP.
- SMTP.
- IMAP.
- NFS.
- RTMP.

- SMB.

Basic concepts

File type group

A file type group can contain a maximum of 32 file extensions. A file matches a file type group if it matches a file extension in the group. You can select predefined file extensions and customize file extensions in a file type group.

File filtering rule

A file filtering rule contains a set of file filtering criteria and the actions for matching packets. The file filtering criteria include file type group, direction (**Upload**, **Download**, or **Both**), and applications. The packet processing actions include **Drop**, **Permit**, and **Logging**. A file must match all the filtering criteria for the actions specified for the rule to apply.

Common configuration

The following common configuration items are supported:

- **Action for files with false extension**—Select the action for packets with files carrying false extensions. To perform file filtering inspection based on the real file extension, select **Permit**. To discard such packets directly, select **Drop**.
- **Max decompressed data size**—Specify the maximum size of data that can be decompressed in a file for file filtering inspection. The device can decompress only ZIP files.

File filtering mechanism

Upon receiving a packet of a protocol that file filtering supports, the device performs the following operations:

1. Compares the packet with the security policies.

   If the packet matches a security policy that is associated with a file filtering profile, the device submits the packet to the file filtering module for processing.

2. Extracts and records the file extension in the packet.

3. Identifies the real file extension and compares it with the recorded file extension:

   - If the two file extensions match or if the real file extension cannot be identified, the device proceeds to step 4.
   - If the two file extensions do not match, the device checks the setting of the **Action for files with false extension** item:
     - If the **Drop** action is selected, the device drops the packet directly.
     - If the **Permit** action is selected, the device proceeds to step 4 to perform file filtering inspection based on the real file extension.

4. Determines the actions to take on the packet by comparing the packet attributes (file extension, application layer application, and file transfer direction) with the file filtering rules in the file filtering policy:

   - If the packet does not match any file filtering rules in the policy, the device permits the packet to pass.
   - If the packet matches only one rule, the device takes the actions specified for the rule.
   - If the packet matches multiple rules, the device determines the actions as follows:
     - If the matching rules have both the permit and drop actions, the device takes the drop action.

– The logging action is taken if it is specified for any of the matching rules.

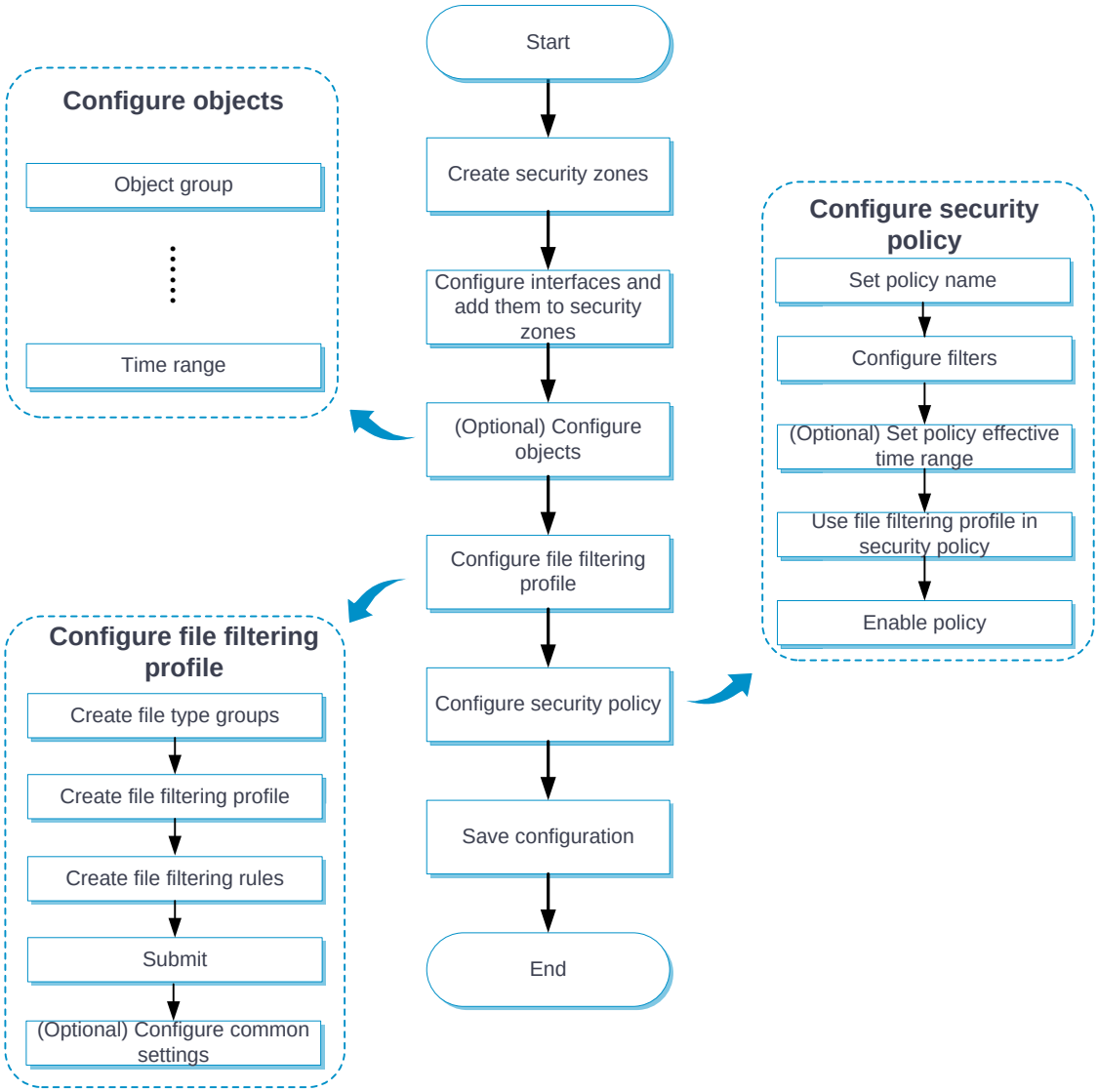
Restrictions and guidelines

After you create, edit, or delete a file filtering profile, the configuration must be activated to take effect. You can click **Submit** to activate the configuration immediately or the configuration will be activated automatically 40 seconds later by default. Activating the configuration causes transient DPI service interruption. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.

Configure file filtering

Configure file filtering as shown in Figure 1.

Figure 1 File filtering configuration procedure



Configure a file type group

Perform this task to create a file type group and configure file extensions in the group.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APPSecurity** > **Data Filtering** > **File Type Groups**.
3. Click **Create**.
4. Create a file type group.

Table 1 File type group configuration items

Item	Description
Name	Enter a name for the file type group.
Description	Enter a description for the file type group.
Predefined file extensions	Select the predefined file extensions for the file type group.
Custom file extensions	Enter the custom file extensions, one per line.

5. Click **OK**.

   The file type group is displayed on the **File Type Groups** page.

Configure a file filtering profile

Perform this task to create a file filtering profile and configure file filtering rules in the profile.

Procedure

1. Click the **Objects** tab.
2. In the navigation pane, select **APPSecurity** > **File Filtering** > **Profiles**.
3. Click **Create**.
4. Create a file filtering profile.

Table 2 File filtering profile configuration items

Items	Description
Name	Enter a name for the file filtering profile.
Description	Enter a description for the file filtering profile.

5. In the **File filtering rules** area, click **Create**.
6. Create a file filtering rule.

Table 3 File filtering rule configuration items

Items	Description
Name	Enter a name for the file filtering profile.
Applications	Select the application layer protocols of the applications to which the rule applies. Supported application layer protocols are FTP, HTTP, IMAP, NFS, POP3, RTMP, SMB, and SMTP.
File type groups	Select the file type group for the file filtering rule. A file matches a file type group if it matches a file extension in the group.

Items	Description
Direction	Select the file transfer direction to which the rule applies. Options are **Upload**, **Download**, and **Both**.
Action	Select the action for matching packets. Options are **Permit** and **Drop**.
Logging	Select whether to enable logging for matching packets. Options are **Enable** and **Disable**.

7. Click **OK**.

   The file filtering rule is displayed on the file filtering rule list of the file filtering profile.

8. Click **OK**.

   The file filtering profile is displayed on the **File Filtering Profiles** page.

9. Use the file filtering profile in a security policy. For more information about security policies, see security policy online help.

10. Click **Submit** to activate the configuration immediately or wait 40 seconds for the configuration to be activated automatically.

    After you create a file filtering profile, the configuration must be activated to take effect. By default, the configuration will be activated automatically 40 seconds later.

APR

This help contains the following topics:

- Introduction
  - PBAR
  - NBAR
  - Application group
- Restrictions and guidelines
- Configure APR
  - Configure an application
  - Configure an application group

Introduction

The application recognition (APR) feature recognizes application protocols of packets for application-based services received on or sent out of ports and collects quantity and transmit rate statistics.

APR uses the following methods to recognize an application protocol:

- Port-based application recognition (PBAR).
- Network-based application recognition (NBAR).

Application protocols in this help are application protocols that can be recognized by APR. Applications are predefined or user-defined.

PBAR

PBAR maps a port to an application protocol and recognizes packets of the application protocol according to the port-protocol mapping.

PBAR supports the following port-protocol mappings:

- **Predefined**—An application protocol uses the port defined by the system.
- **User-defined**—An application protocol uses the port defined by the user.

PBAR offers the following mappings to maintain and apply user-defined port configuration:

- **General port mapping**—Maps a user-defined port to an application protocol. All packets destined for that port are regarded as packets of the application protocol. For example, if port 2121 is mapped to FTP, all packets destined for that port are regarded as FTP packets.
- **Host-port mapping**—Maps a user-defined port to an application protocol for packets to or from some specific hosts. For example, you can establish a host-port mapping so that all packets destined for the network segment 10.110.0.0/16 on port 2121 are regarded as FTP packets. To define the range of the hosts, you can specify the ACL, the host IP address range, or the subnet.

NBAR

NBAR uses predefined or user-defined NBAR rules to match packet contents to recognize the application protocols of matching packets. Predefined NBAR rules are automatically generated from the APR signature library.

In the current software version, only predefined NBAR rules are supported, and they are not configurable.

Application group

You can add application protocols that have similar signatures or restrictions to an application group. APR recognizes packets of the application protocols by matching the packet contents with the signatures or restrictions. If a packet is recognized as the packet of an application protocol in the application group, the packet is considered to be a packet of the application group.

An application group can contain multiple predefined and user-defined applications.

Restrictions and guidelines

- A license is required for APR signature library update. After the license expires, NBAR can still use the existing signature library but cannot update the signature library. For information about licenses, see license management online help.
- Before using the APR feature, update the APR signature library to the latest version.

Configure APR

Configure an application

You can create and modify user-defined applications for PBAR on the **Applications** page.

Port mapping categories

The following port mapping categories are available for PBAR:

- **General port mapping**—Maps a user-defined port to an application protocol. All packets destined for that port are regarded as packets of the application protocol. For example, if port 2121 is mapped to FTP, all packets destined for that port are regarded as FTP packets.
- **ACL-based host-port mapping**—Maps a port to an application protocol for the packets matching the specified ACL.
- **Subnet-based host-port mapping**—Maps a port to an application protocol for the packets sent to the specified subnet. If multiple subnet-based mappings are applied to packets and these subnets overlap, PBAR matches the packets destined for the overlapped segment with the port mapping of the subnet that has the smallest range.
- **IP address-based host-port mapping**—Maps a port to an application protocol for the packets destined for the specified IP addresses.

Create a port mapping

1. Click the **Objects** tab.
2. Select **APPSecurity** > **App Recognition** > **Applications**.
3. Click **Create** to create an application.
4. Enter a name for the application, and select risk types. The device calculates a risk level based on the specified risk types.
5. Click **Create** in the **Port mappings** area.
6. Create a port mapping for the application.

Table 1 Port mapping configuration items

Item	Description
Port number	Enter the number of a port to which the application is mapped.

Item	Description
Protocol	Select a transport layer protocol. Possible values include All, DCCP, SCTP, TCP, UDP, and UDP-Lite. If **All** is selected, packets that meet the following conditions are recognized as the specified application protocol's packets: • Packets are encapsulated by any transport layer protocol. • Packets have the specified port.
Type	Select a match type from the following values: • All, representing general port mapping. • IPv4 address-based host-port mapping. • IPv6 address-based host-port mapping. • IPv4 subnet-based host-port mapping. • IPv6 subnet-based host-port mapping. • IPv4 ACL-based host-port mapping. • IPv6 ACL-based host-port mapping.
Match criteria	• Enter an IP address range if IP address-based host-port mapping was selected earlier. • Enter an IP subnet if subnet-based host-port mapping was selected earlier. • Enter an ACL if ACL-based host-port mapping was selected earlier.
VRF instance	Select a VRF instance.

7. Click **OK**.

   You can create multiple port mappings for an application. PBAR selects a port mapping to recognize the application protocol of a packet in the following order:

   a. IP address-based port mapping.

   b. Subnet-based port mapping.

c. ACL-based host-port mapping.

d. General port mapping.

8. Click **OK** on the **Create Application** page.

   On the **Applications** page, select **Show user-defined applications only** to verify the configuration.

Edit a predefined application

1. Click the **Objects** tab.
2. Select **APPSecurity** > **App Recognition** > **Applications**.
3. Select a predefined application, and click **Edit** on the right side.
4. Follow the step described in "Configure an application" to add port mappings for the application.

   After editing, the newly added port-mappings take effect immediately. A packet that matches a newly added port-mapping can be recognized as the packet of the application.

Configure an application group

You can add applications that have similar characteristics or limitations to an application group.

Procedure

1. Click the **Objects** tab.
2. Select **APPSecurity** > **App Recognition** > **Application Groups**.
3. Click **Create**.
4. Create an application group.

Table 2 Application group configuration items

Item	Description
Group	Enter a name for the application group.
Description	Enter a description for identification and management purposes.
Category	Select categories to filter desired applications.
Risk type	Select risk types to filter desired applications.
Risk level	Select risk levels to filter desired applications.
Filter	Click **Select all** or **Select** to move applications from the **Available Applications** list to the **Selected Applications** list.

5. Click **OK**.

6. Verify the configuration on the **Application Groups** page.

Terminal identification

This help contains the following topics:

Introduction

Identifying IoT terminals, such as cameras and sensors, is fundamental to establish secure Internet of Things (IoT) connections.

When the terminal traffic passes through a device, the device performs the following tasks:

- Analyzes and extracts the terminal information, such as the vendor and model of the terminal.
- Generates a log when terminal information (such as camera vendor) changes.

Terminal

You can predefine terminals in the device characteristics library to identify the terminal characteristics.

To enable terminal identification, select **Objects** > **APPSecurity** > **Terminal Identification** > **Terminals**, and then click **Enable terminal identification logging**.

Terminal group

You can add terminals sharing similar characteristics to a terminal group. The device can provide the same DPI service for packets of the same terminal group.

To add terminals into a terminal group, select **Objects** > **APPSecurity** > **Terminal Identification** > **Terminal Groups**, click **Create**, and then add the available terminals to this terminal group.

Object group for terminal identification

You can configure object groups for accurate terminal address identification. The device supports the following address object groups:

- **Terminal address object group**—A set of terminal IP addresses. If the packet source or destination IP address matches this group, the source or destination IP address is the terminal IP address.
- **Manager address object group**—A set of terminal manager IP addresses. If the packet source or destination IP address matches this group, the destination or source IP address is the terminal IP address.

To configure object groups, select **Objects** > **APP Security** > **Terminal Identification** > **Terminals**, and then click **Configure object groups for terminal identification**. Configure the manager address object group, or the terminal address object group, or both. If you configure both, the manager address object group takes precedence.

Security action

Introduction

The security action module can provide action parameters for DPI service modules such as IPS and antivirus. The following action parameter profiles are available:

- **Block**—Defines the block period for the block source action in DPI service modules. The block source action takes effect only after the blacklist feature is enabled. With the blacklist feature enabled, the device drops a matching packet and adds the packet's source IP address to the IP blacklist. Subsequent packets from the source IP address will be dropped directly during the block period.

  For more information about the blacklist feature, see attack defense online help.

- **Redirect**—Defines the URL to which packets are redirected for the redirect action in DPI service modules.

- **Capture**—Defines parameters for the capture action in DPI service modules, such as maximum number of bytes that can be cached and URL to which cached packets are exported.

  The device caches captured packets locally and exports the cached packets to the designated URL at the daily export time or when the number of cached bytes reaches the limit. After the export, the device clears the local cache and starts to capture new packets. If you do not specify a URL or the specified URL is not reachable, the device still exports the cached captured packets but the export will fail and the local cache will be cleared.

- **Alarm**—Defines the anti-virus alarm message to be displayed on the client. Click **Create** to create an alarm message template, click **Edit** at the right side of the template, and then

import the required alarm message. In one alarm message template, you can define an alarm message by importing a TXT or HTML file. Support for this feature depends on the device model.

Advanced settings

Introduction

Bypass

The bypass feature disables the DPI engine so packets will not be processed by DPI. You can enable bypass when the CPU usage is high to guarantee device performance. By default, the DPI engine is enabled.

Activate

After you edit the policy and rule settings for DPI service modules, you must click Activate to validate the settings. The validation operation can cause temporary service disruptions. As a best practice, perform the operation after all DPI service policy and rule settings are complete.

DPI support for HA

Enable this feature on an HA system in dual-active mode for asymmetric-path traffic of DPI services to be processed correctly. This feature consumes system resources. As a best practice, enable this feature only when asymmetric-path traffic of DPI services exists.

Client IP identification

When a client uses a proxy to access servers, the value in the source IP address field will change. This feature enables the device to obtain the IP address of the originating client by inspecting specific fields of the request packets that have traveled through proxies.

Restrictions and guidelines

- When bypass is enabled, the system does not process received packets by DPI. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.
- Activating configuration causes transient DPI service interruption. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.

Intelligences from the threat management platform

Introduction

The device supports receiving intelligences from the threat management platform, including MD5 reputation. The intelligences supplement the locally loaded reputation and antivirus signature libraries, improving security for internal network users.

Restrictions and guidelines

- To ensure successful receiving of intelligences from the threat management platform, enable NETCONF over SOAP on the device by executing **`netconf soap http enable`** and **`netconf soap https enable`** commands from the CLI of the device.
- To use the threat intelligences correctly, configure anti-virus features first on the device.

Object group

This help contains the following topics:

- Introduction
  - Object groups
  - Time ranges
  - NAT address groups
  - NAT address group probing
  - AFT address group
  - DNS aging
- Restrictions and guidelines

Introduction

Object groups

An object group is a group of objects that can be used by other service modules to identify packets. Object groups are divided into the following types:

- **IPv4 address object group**—A group of IPv4 address objects used to match the IPv4 address in a packet.
- **IPv6 address object group**—A group of IPv6 address objects used to match the IPv6 address in a packet.

- **MAC address object group**—A group of MAC address objects used to match the MAC address in a packet.
- **Service object group**—A group of service objects used to match the protocol type and protocol characteristics (such as TCP/UDP source/destination port and ICMP message type and code) in a packet.

A packet is considered matching an object group if it matches an object in the group.

For simplicity purposes, object groups support object group nesting to allow one object group to use another object group as an object.

Time ranges

You can implement a service based on the time of the day by applying a time range to it. A time-based service takes effect only in time periods specified by the time range. If a time range does not exist, the service based on the time range does not take effect.

The following basic types of time ranges are available:

- **Periodic time range**—Recurs periodically on a day or days of the week.
- **Absolute time range**—Represents only a period of time and does not recur.

A time range is uniquely identified by the time range name. You can create a maximum of 1024 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements.
2. Combining all absolute statements.
3. Taking the intersection of the two statement sets as the active period of the time range.

NAT address groups

A NAT address group contains a group of IP segments or port ranges. It can be used by NAT for dynamic NAT translation.

For the PAT mode, you must specify address group members and a port range. For NAT444 dynamic translation, you must also specify the port block size and configure port block extending.

For the NO-PAT mode, you must specify address group members.

NAT address group probing

NAT address group probing uses an NQA template to detect the reachability of the addresses in the group.

The device periodically sends probe packets to the specified destination address in the NQA template. The source IP addresses in the probe packets are the IP addresses in the NAT address group.

- If the device receives a response packet for a probe, the probed source IP address can be used for address translation.
- If the device does not receive a response packet for a probe, the probed source IP address will be excluded from address translation temporarily. However, in the next NQA operation period, this excluded IP address is also probed. If a response is received in this round, the IP address can be used for address translation.

AFT address group

An AFT address group contains a group of IP segments. It can be used by AFT (NAT64) for dynamic AFT translation.

Support for the AFT address group depends on the device model.

DNS aging

In load-sharing scenarios where a host name corresponds to multiple IP addresses, the IP address converted from a host name might change frequently. By default, the object group module notifies relevant policies (including security policies) every time the converted address changes, which might cause frequent policy acceleration and consume many memory resources.

To resolve this issue, you can enable DNS aging for IP addresses converted from a host name to age out.

With this feature enabled, the object group module maintains an IP address group for each host name. If an address converted from a host name does not exist in the group, the system adds the address to the group and notifies the new IP address range to relevant policies. If a converted address already exists in the group, the system does not notify policies but updates the address aging time instead. After an address ages out, the system notifies the relevant policies of the address deletion. This reduces policy acceleration and memory consumption.

Support for DNS aging depends on the device model.

Restrictions and guidelines

- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.
- Two object groups cannot use each other at the same time.
- You can specify multiple NQA templates for one NAT address group. An IP address in the address group is identified as reachable as long as one probe for this IP address succeeds.
- Make sure the NQA template used for NAT address group probing does not have source IP address configured.

ACL

This help contains the following topics:

- Introduction
  - ACL types
  - Match order
  - Rule numbering
- Restrictions and guidelines

Introduction

An access control list (ACL) is a set of rules for identifying traffic based on criteria such as source IP address, destination IP address, and port number. The rules are also called permit or deny statements. The device processed identified traffic according to the configured policy.

ACL types

Table 1 ACL types

Type	IP version	Match criteria
Basic ACLs	IPv4	Source IPv4 address.
	IPv6	Source IPv6 address.

Type	IP version	Match criteria
Advanced ACLs	IPv4	Source IPv4 address, destination IPv4 address, packet priority, protocol number, and other Layer 3 and Layer 4 header fields.
	IPv6	Source IPv6 address, destination IPv6 address, packet priority, protocol number, and other Layer 3 and Layer 4 header fields.
Layer 2 ACLs	IPv4 and IPv6	Layer 2 header fields, such as source and destination MAC addresses, 802.1p priority, and link layer protocol type.
User-defined ACLs	IPv4 and IPv6	User specified matching patterns in protocol headers.

Match order

The rules in an ACL are sorted in a specific order. When a packet matches a rule, the device stops the match process and performs the action defined in the rule. If an ACL contains overlapping or conflicting rules, the matching result and action to take depend on the rule order.

The following ACL match orders are available:

- **config**—Sorts ACL rules in ascending order of rule ID. A rule with a lower ID is matched before a rule with a higher ID. If you use this method, check the rules and their order carefully.
- **auto**—Sorts ACL rules in depth-first order. Depth-first ordering makes sure any subset of a rule is always matched before the rule. Table 2 lists the sequence of tie breakers that depth-first ordering uses to sort rules for each type of ACL.

Table 2 Sorting ACL rules in depth-first order

ACL type	Sequence of tie breakers
IPv4 basic ACL	1. VPN instance. 2. More 0s in the source IPv4 address wildcard (more 0s means a narrower IPv4 address range). 3. Rule configured earlier.
IPv4 advanced ACL	1. VPN instance. 2. Specific protocol number. 3. More 0s in the source IPv4 address wildcard mask. 4. More 0s in the destination IPv4 address wildcard. 5. Narrower TCP/UDP service port number range. 6. Rule configured earlier.
IPv6 basic ACL	1. VPN instance. 2. Longer prefix for the source IPv6 address (a longer prefix means a narrower IPv6 address range). 3. Rule configured earlier.
IPv6 advanced ACL	1. VPN instance. 2. Specific protocol number. 3. Longer prefix for the source IPv6 address. 4. Longer prefix for the destination IPv6 address. 5. Narrower TCP/UDP service port number range. 6. Rule configured earlier.
Layer 2 ACL	1. More 1s in the source MAC address mask (more 1s means a smaller MAC address). 2. More 1s in the destination MAC address mask. 3. Rule configured earlier.

Rule numbering

If you do not assign an ID to the rule you are creating, the system automatically assigns it a rule ID. The rule numbering step sets the increment by which the system automatically numbers rules. For example, if the ACL rule numbering step is 5 and you do not assign IDs to rules you are creating, they are automatically numbered 0, 5, 10, 15, and so on. The wider the numbering step, the more rules you can insert between two rules.

By introducing a gap between rules rather than contiguously numbering rules, you have the flexibility of inserting rules in an ACL. This feature is important for a config-order ACL, where ACL rules are matched in ascending order of rule ID.

The ID automatically assigned to an ACL rule takes the nearest higher multiple of the numbering step to the current highest rule ID, starting with 0.

For example, if the step is 5, and there are five rules numbered 0, 5, 9, 10, and 12, the newly defined rule is numbered 15. If the ACL does not contain a rule, the first rule is numbered 0.

Whenever the step changes, the rules are renumbered, starting from 0. For example, changing the step from 5 to 2 renumbers rules 5, 10, 13, and 15 as rules 0, 2, 4, and 6.

Restrictions and guidelines

- You can create an ACL on the ACL page or on the page for a feature that uses the ACL. However, you can manage ACLs (for example, modify or delete ACLs) only on the ACL page.
- Deleting or modifying an ACL might affect the feature that uses the ACL.
- If the match order for an ACL is config, you can modify any rules in the ACL. If the match order for an ACL is auto, you cannot modify any rules in the ACL.

SSL

Introduction

Secure Sockets Layer (SSL) is a cryptographic protocol that provides communication security for TCP-based application layer protocols such as HTTP. SSL has been widely used in applications such as e-business and online banking to provide secure data transmission over the Internet.

SSL provides the following security services:

- **Privacy**—SSL uses a symmetric encryption algorithm to encrypt data. It uses the asymmetric key algorithm of RSA to encrypt the key used by the symmetric encryption algorithm.
- **Authentication**—SSL uses certificate-based digital signatures to authenticate the SSL server and client. The SSL server and client obtain digital certificates through PKI.
- **Integrity**—SSL uses the message authentication code (MAC) to verify message integrity.

Restrictions and guidelines

- The SSL protocol versions include SSL 2.0, SSL 3.0, TSL 1.0 (or SSL 3.1), TLS 1.1, TLS 1.2, TLS 1.3, and GM-TLS1.1. As an SSL server, the device can communicate with clients running SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, or GM-TLS1.1. When the server receives an SSL 2.0 Client Hello message from a client, it notifies the client to use a later SSL version for communication.

- An SSL server policy defines a set of SSL parameters used by the SSL server, including the PKI domain and the supported cipher suites. An SSL server policy takes effect only after it is associated with an application such as HTTPS.
- An SSL client policy defines a set of SSL parameters used by the SSL client, including the PKI domain and the preferred cipher suite. The SSL client uses the settings in the client policy to establish a connection to the server. An SSL client policy takes effect only after it is associated with an application, such as DDNS.
- If the configuration in an SSL server or client policy changes, you must re-enable the services that use that SSL server or client policy to apply the new configuration.
- If you modify the SSL protocol version in **Advanced Settings**, you must re-enable the services that use the default SSL policy to apply the new SSL protocol version.

Public key management

This help contains the following topics:

- Introduction
  - Asymmetric key algorithm overview
  - Managing local asymmetric key pairs
  - Managing peer host public key
- Restrictions and guidelines

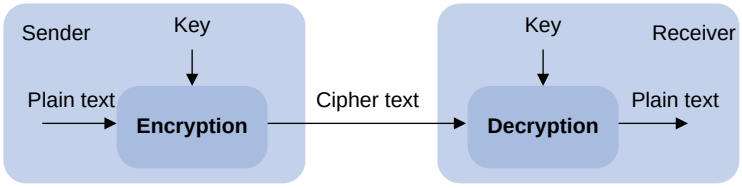
Introduction

The public key management feature is used to manage and advertise keys of asymmetric key algorithms.

Asymmetric key algorithm overview

Asymmetric key algorithms are used by security applications to secure communications between two parties, as shown in Figure 1. Asymmetric key algorithms use two separate keys (one public and one private) for encryption and decryption. Symmetric key algorithms use only one key.

Figure 1 Encryption and decryption



A key owner can distribute the public key in plain text on the network but must keep the private key in privacy. It is mathematically infeasible to calculate the private key even if an attacker knows the algorithm and the public key.

Asymmetric key algorithms include Revest-Shamir-Adleman Algorithm (RSA), Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and SM2.

Security applications (such as SSH, SSL, and PKI) use the asymmetric key algorithms for encryption/decryption and digital signature.

Managing local asymmetric key pairs

Creating a local key pair

On the local device, you can create RSA, DSA, ECDSA, and SM2 key pairs.

Displaying or exporting a host public key

On the device, you can display or export the local host public keys.

- Display a host public key. After the key is displayed on the local device, record the key, for example, copy it to an unformatted file. On the peer device, you must literally enter the key.
- Export a host public key to a file in the specified format. Transfer the file to the peer device. On the peer device, import the key from the file.

When you export a host public key to a file, the specified file name cannot contain semicolons (;) or commas (,).

- Export a host public key to the monitor screen in the specified format, and then save it to a file. Transfer the file to the peer device. On the peer device, import the key from the file.

Destroying a local key pair

To ensure security, destroy the local key pair and generate a new key pair in any of the following situations:

- The local key has leaked. An intrusion event might occur.
- The storage media of the device fails or is replaced, so the device does not have the corresponding private key for decryption/encryption and digital signature.
- The local certificate has expired.

Managing peer host public keys

To encrypt information sent to a peer device or authenticate the digital signature of the peer device, you must configure the peer device's public key on the local device. On the local device, you can import, display, and delete the host public key of the peer device.

You can configure the peer host public key by using the following methods:

- Import the peer host public key from a public key file (recommended).

  You must first obtain the public key file from the peer device through FTP or TFTP. After you import the key, the local device automatically converts the imported public key to a string in the Public Key Cryptography Standards (PKCS) format.

- Manually enter (type or copy) the peer host public key.

You must first display the public key on the peer device and record the key. On the local device, you manually type or copy the key.

Restrictions and guidelines

When you configure a peer host public key, follow these restrictions and guidelines:

- When you manually enter the peer host public key, make sure the entered key is in the correct format. To obtain the peer host public key in the correct format, display the public key on the peer device as described in "Displaying or exporting a host public key." The format of the public key displayed in any other way might be incorrect. If the key is not in the correct format, the system discards the key and displays an error message.
- Always import rather than enter the peer host public key if you are not sure whether the device supports the format of the recorded peer host public key.
- The public key of an SM2 key pair cannot be imported.

PKI

This help contains the following topics:

- Introduction
    - Digital certificate and certificate revocation list
    - PKI architecture
    - PKI applications
    - Certificate management
    - Certificate access control policy
- Restrictions and guidelines

Introduction

Public Key Infrastructure (PKI) is an asymmetric key infrastructure to encrypt and decrypt data for securing network services.

PKI uses digital certificates to distribute and employ public keys, and provides network communication and e-commerce with security services such as user authentication, data confidentiality, and data integrity.

The PKI system of the device provides certificate management for IPsec and SSL.

Digital certificate and certificate revocation list

Digital certificate

A digital certificate is an electronic document signed by a certificate authority (CA). A digital certificate binds a public key with the identity of its owner.

A digital certificate includes the following information:

- Issuer name (name of the CA that issued the certificate).
- Certificate subject (name of the individual or group to which the certificate is issued).
- Identity information of the subject.
- Subject's public key.
- Signature of the CA.
- Validity period.

This help covers the following types of certificates:

- **CA certificate**—Certificate of a CA. Multiple CAs in a PKI system form a CA tree, with the root CA at the top. The root CA generates a self-signed certificate, and each lower level CA holds a CA certificate issued by the CA immediately above it. The chain of these certificates forms a chain of trust.
- **Local certificate**—Digital certificate issued by a CA to a local PKI entity, which contains the entity's public key.

Certificate revocation list

A certificate revocation list (CRL) is a list of serial numbers for certificates that have been revoked. A CRL is created and signed by the CA that originally issued the certificates.

The CA publishes CRLs periodically to revoke certificates. Revoked certificates should not be trusted.

The CA must revoke a certificate when any of the following conditions occurs:

- The certificate subject information is changed.
- The private key is compromised.
- The association between the certificate subject and CA is changed. For example, when an employee terminates employment with an organization.

The device allows you to enable automatic update of CRLs and set the CRL update interval. The device automatically obtains the CRL from the CRL repository at the specified intervals.

PKI architecture

A PKI system consists of certificate subjects, CAs, RAs and a certificate/CRL repository.

Certificate subject

A certificate subject is an end user using PKI certificates. The certificate applicant can be an operator, an organization, a device, or a process running on a computer.

A certificate applicant uses a certificate subject to provide its identity information to a CA. A valid certificate subject must include one or more of following identity categories:

- Certificate subject name, which further includes the common name, country code, state or province name, locality, organization name, and organization unit name. If you configure the certificate subject name, a common name is required.
- FQDN of the certificate applicant. It identifies a PKI entity in the network.
- IP address of the certificate applicant.

CA

A certification authority (CA) issues certificates, defines the certificate validity periods, and revokes certificates by publishing CRLs.

RA

The registration authority (RA) offloads the CA by processing certificate enrollment requests. The RA accepts certificate requests, verifies user identity, and determines whether to ask the CA to issue certificates.

The RA is optional in a PKI system. In cases when there is security concern over exposing the CA to direct network access, it is advisable to delegate some of the tasks to an RA. Then, the CA can concentrate on its primary tasks of signing certificates and CRLs.

Certificate/CRL repository

A certificate/CRL repository is certificate distribution point that stores certificates and CRLs, and distributes the certificates and CRLs to certificate applicants. It also provides the query function. A PKI repository can be a directory server using the LDAP or HTTP protocol, of which LDAP is commonly used.

PKI applications

The PKI technology can meet security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

VPN

A VPN is a private data communication network built on the public communication infrastructure. A VPN can use network layer security protocols (for example, IPsec) in conjunction with PKI-based encryption and digital signature technologies for confidentiality.

Secure emails

PKI can address the email requirements for confidentiality, integrity, authentication, and non-repudiation. A common secure email protocol is Secure/Multipurpose Internet Mail Extensions (S/MIME), which is based on PKI and allows for transfer of encrypted mails with signature.

Web security

PKI can be used in the SSL handshake phase to verify the identities of the communicating parties by digital certificates.

Certificate management

The device manages certificates based on PKI domains and provides the PKI domain-based certificate service for applications such as IPsec and SSL. A PKI domain contains enrollment information for a certificate subject, including the key pairs for certificate request and the certificate usage extensions.

Importing certificates

You can import the CA certificate and local certificates related to a PKI domain from the CA.

Use this method when the CRL repository is not specified, the CA server does not support SCEP, or the CA server generates the key pair for the certificates.

Before you import certificates to a PKI domain, complete the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device.
- To import a local certificate, a CA certificate chain must exist in the PKI domain, or be contained in the certificate to be imported. If the CA certificate chain is not available, import it before you import the local certificate.

When you import a local certificate, follow these restrictions and guidelines:

- If the local certificate contains the CA certificate chain, you can import the CA certificate and the local certificate at the same time.
- If the local certificate does not contain the CA certificate chain, but the CA certificate already exists in a PKI domain, you can directly import the certificate.
- If the certificate file to be imported contains the root certificate, the system will prompt you to confirm the root certificate's fingerprint before the import. Contact the CA administrator to obtain the correct root certificate fingerprint.
- If the local certificate to be imported contains a key pair, the system will prompt for the challenge password used for encrypting the private key. Contact the CA administrator to obtain the challenge password.
- When you import a local certificate file that contains a key pair, the device saves the key pair in the PKI domain as follows.
    - If the PKI domain already contains a key pair that matches key pair in the certificate file, the device prompts whether you want to overwrite the existing key pair.
    - If the PKI domain does not have a key pair, the device creates a key pair according to the key algorithm and the purpose of the key pair in the certificate file. The PKI domain name will be used as the key pair name.
    - If the PKI domain contains a key pair that is different from the key pair in the certificate file, you must specify a different name to save the key pair in the certificate file.

You can import the CA certificate to a PKI domain when either of the following conditions is met:

- The CA certificate to be imported is the root CA certificate or contains the certificate chain with the root certificate.
- The CA certificate contains a certificate chain without the root certificate, but can form a complete certificate chain with an existing CA certificate on the device.

Exporting certificates

You can export the CA certificate and the local certificates in a PKI domain to certificate files. The exported certificate files can then be imported back to the device or other PKI applications.

Requesting certificates

Before you request a local certificate for a certificate subject in a PKI domain, make sure a CA certificate already exists in the PKI domain. The CA certificate will be used to verify the validity of the obtained local certificate.

To request a certificate for a certificate subject in a PKI domain, perform the following tasks:

1. Configure the certificate subject.
2. Use the certificate subject in a PKI domain. In the PKI domain, configure the certificate enrollment settings such as the key pair for certificate request.

   The public key of the key pair is sent along other information in the certificate request to the CA. The CA then signs the request and generates the requested certificate.

   If you specify a nonexistent key pair in the PKI domain, the system automatically generates the key pair according to the key pair settings when generating the certificate request.
3. Generate a certificate request for the certificate subject in the PKI domain.
4. Submit the certificate request to the CA by using an out-of-band method, such as phone or email.

Certificate access control policy

Certificate access control policies allow you to authorize access to a device (for example, an HTTPS server) based on the attributes of an authenticated client's certificate.

A certificate access control policy is a set of permit or deny rules. Each rule contains a set of certificate attribute filters. A certificate attribute filter filters certificates based on an attribute in the certificate issuer name, subject name, or alternative subject name field. A certificate matches a rule if it matches all the certificate attribute filters in the rule.

The device matches a received certificate against the rules on the rule list of the certificate access policy from top to bottom. The match process stops once a matching rule is found.

- If a certificate matches a permit rule, the certificate passes the verification.
- If a certificate matches a deny rule or does not match any rules in the policy, the certificate is regarded invalid.
- If the certificate access control policy specified for a security application (for example, HTTPS) does not exist, all certificates in the application pass the verification.

Restrictions and guidelines

- Whether the identity categories are required or optional depends on the CA policy. Follow the CA policy to configure the certificate subject settings.
- The SCEP add-on on the Windows 2000 CA server has restrictions on the data length of a certificate request. If a request from a PKI entity exceeds the data length limit, the CA server does not respond to the certificate request. In this case, you can use an out-of-band means to submit the request. Other types of CA servers, such as RSA servers and OpenCA servers, do not have such restrictions.

Trusted access controllers

This help contains the following topics:

Introduction

The device can direct received user requests to a trusted access controller for identity authentication, and then verify whether the users passing the authentication are authorized to access the requested resources.

Configure a trusted access controller

1. Click the **Objects** tab.
2. In the navigation pane, select **Trusted Access Controller**.
3. Click **Create**.
4. Configure the trusted access controller parameters.

Table 1 Trusted access controller configuration items

Item	Description
Name	Enter the name of the trusted access controller, which is a case-insensitive string.
Local service URL	Enter the local service URL that is used to collaborate with the trusted access controller. The trusted access controller can use the local service URL to notify the device of user offline and user permission change events. The local service URL must be in the format of **protocol type://server IP address:port number**. • The protocol type can be HTTP or HTTPS. • The server IP address must be an IPv4 address in the current software version. On a device, you cannot configure local service URLs with the same server IP address and port number for different trusted access controllers. You cannot specify the same server IP address and port number for both the local and peer service URLs of a trusted access controller.
Peer service URL	Enter the peer URL that provides external authentication services. The device can use the peer service URL to perform registration and user permission authorization with the trusted access controller. The peer service URL must be in the format of **protocol type://server IP address:port number**. • The protocol type can be HTTP or HTTPS. • The server IP address must be an IPv4 address in the current software version. On a device, you cannot configure peer service URLs with the same server IP address and port number for different trusted access controllers. You cannot specify the same server IP address and port number for both the local and peer service URLs of a trusted access controller.
SSL client policy	Specify the SSL client policy used by the trusted access controller to encrypt traffic exchanged with the device (SSL client). You can select an existing SSL client policy or create a new SSL client policy.
SSL server policy	Specify the SSL server policy used by the trusted access controller to encrypt traffic exchanged with the device (SSL server).

Item	Description
	You can select an existing SSL server policy or create a new SSL server policy.
Authentication service function	Enable or disable the authentication service.

5. Click **OK**.

   The trusted access controller will be displayed on the trusted access controller page.

Scanner

This help contains the following topics:

- Introduction
- Restrictions and guidelines
- Configure the scanner

Introduction

The scanner scans a variety of endpoints (including cameras, PCs, switches, servers, routers, firewalls, APs, printers, and ATMs) on the network and reports endpoint information to the endpoint management server. The endpoint management server manages and monitors the endpoints in a centralized way.

Restrictions and guidelines

- Make sure the route between the device and the endpoint management server is available, so that the scanner can report endpoint information to the endpoint management server.
- When you modify the endpoint management server parameters, you must re-enter the plaintext or ciphertext key.

Configure the scanner

1. Click the **Network** tab.
2. In the navigation pane, select **Scanner**.
3. On the scanner page, select **Enable** for **Scanner**.
4. Configure the endpoint management server parameters as described in Table 1.

Table 1 Endpoint management server configuration items

Item	Description
IPv4 address	Enter the IPv4 address of the endpoint management server.
Port number	Enter the port number of the endpoint management server.
Encryption method	Select an encryption method. Options are **Plaintext key** and **Ciphertext key**.
Plaintext key	Enter the plaintext key string for the communication between the scanner and the endpoint management server. This field is available when you select **Plaintext key** for **Encryption method**.
Ciphertext key	Enter the ciphertext key string for the communication between the scanner and the endpoint management server. This field is available when you select **Ciphertext key** for **Encryption method**.
Log level	Select a log level. Logs of a higher level contain more detailed information and consume more memory resources.
Global parameters	Enable this option to use the global parameter settings of the endpoint management server. If you do not enable this option, the locally configured parameters apply.

5. Click **Apply** to save the configuration.

6. To download the scanning results, click **Obtain log file**.

VRF

Introduction

Virtual Routing and Forwarding (VRF) implements route isolation, data independence, and data security for VPNs.

A VRF has the following components:

- A separate Label Forwarding Information Base (LFIB).
- An IP routing table.
- Interfaces bound to the VRF.
- VRF administration information including a route distinguishers (RD).

An RD is added before a site ID to distinguish the sites that have the same site ID but reside in different VPNs. An RD and a site ID uniquely identify a VPN site.

An RD is a string of 3 to 21 characters in one of the following formats:

- *16-bit AS number*:*32-bit user-defined number*. For example, 101:3.
- *32-bit IP address*:*16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number*:*16-bit user-defined number*, where the minimum value of the AS number is 65536. For example, 65536:1.

VRFs can be bound to the multiple instances of a multicast or routing protocol to implement service isolation. For example, if a device supports multiple OSPF instances, you can bind a VRF to each OSPF process, so that routes learned by an OSPF process are added into the routing table of the bound VRF.

Interface

This help contains the following topics:

- Introduction
  - IPv4 address
  - IPv6 address
  - Link aggregation
  - VLAN termination
- Restrictions and guidelines

Introduction

Your device supports the following types of Ethernet interfaces:

- **Layer 2 Ethernet interface**—Physical Ethernet interface operating at the data link layer (Layer 2) to switch packets.
- **Layer 3 Ethernet interface**—Physical Ethernet interface operating at the network layer (Layer 3) to route packets. You can assign an IP address to a Layer 3 Ethernet interface.
- **Layer-configurable Ethernet interface**—Physical Ethernet interface that can be configured to operate in bridge mode as Layer 2 Ethernet interfaces or in route mode as Layer 3 Ethernet interfaces.
- **Layer 3 Ethernet subinterface**—Logical interface operating at the network layer. You can assign an IP address to a Layer 3 Ethernet subinterface. To enable a Layer 3 Ethernet

interface to transport packets for multiple VLANs, you must create Layer 3 subinterfaces on the Layer 3 Ethernet interface.

- **Layer 2 aggregate interface**—Logical interface that uniquely corresponds to a Layer 2 aggregation group. This type of interface is used for implementing Layer 2 link aggregation.
- **Layer 3 aggregate interface**—Logical interface that uniquely corresponds to a Layer 3 aggregation group. This type of interface can be assigned IP addresses and is used for implementing Layer 3 link aggregation.
- **Layer 3 aggregate subinterface**—Logical interface that can be assigned IP addresses. This type of interface is used to enable a Layer 3 aggregate interface to send and receive VLAN tagged packets.
- **Loopback interface**—Logical interface that can be assigned IP addresses. After a loopback interface is created, the physical layer state of the loopback interface is always up unless the loopback interface is manually shut down.
- **VLAN interface**—Logical interface. Each VLAN corresponds to one VLAN interface. After an IP address is assigned to a VLAN interface, the IP address can be used as the gateway address for network devices in the VLAN, and the VLAN interface can forward packets destined for another IP subnet at Layer 3. For more information about VLAN interfaces, see "VLAN."
- **SSL VPN interface**—Logical interface that can be assigned IP addresses. When a user accesses an SSL VPN gateway through the IP access method, the gateway uses this interface to communicate with the client. For more information about SSL VPN interfaces, see "SSL VPN."
- **Reth interface**—Logical interface that can be assigned IP addresses. A Reth interface uses two member interfaces to ensure link availability. For more information about Reth interfaces, see "Hot backup."

- **Reth subinterface**—Logical interface that can be assigned IP addresses. This type of interface is used to enable a Reth interface to send and receive Layer 2 VLAN-tagged packets. For more information about Reth subinterfaces, see "Hot backup."

IPv4 address

IP address representation and classes

IP addressing uses a 32-bit address to identify each host on an IPv4 network. To make addresses easier to read, they are written in dotted decimal notation, each address being four octets in length. For example, address 00001010000000010000000100000001 in binary is written as 10.1.1.1.

Each IP address breaks down into the following sections:

- **Net ID**—Identifies a network. The first several bits of a net ID, known as the class field or class bits, identify the class of the IP address.
- **Host ID**—Identifies a host on a network.

IP addresses are divided into five classes, as shown in Table 1. The first three classes are most commonly used.

Table 1 IP address classes and ranges

Class	Address range	Remarks
A	0.0.0.0 to 127.255.255.255	The IP address 0.0.0.0 is used by a host at startup for temporary communication. This address is never a valid destination address. Addresses starting with 127 are reserved for loopback test. Packets destined to these addresses are processed locally as input packets rather than sent to the link.
B	128.0.0.0 to	N/A

Class	Address range	Remarks
	191.255.255.255	
C	192.0.0.0 to 223.255.255.255	N/A
D	224.0.0.0 to 239.255.255.255	Multicast addresses.
E	240.0.0.0 to 255.255.255.255	Reserved for future use, except for the broadcast address 255.255.255.255.

Subnetting and masking

Subnetting divides a network into smaller networks called subnets by using some bits of the host ID to create a subnet ID.

Masking identifies the boundary between the host ID and the combination of net ID and subnet ID.

Each subnet mask comprises 32 bits that correspond to the bits in an IP address. In a subnet mask, consecutive ones represent the net ID and subnet ID, and consecutive zeros represent the host ID.

Before being subnetted, Class A, B, and C networks use these default masks (also called natural masks): 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

Subnetting increases the number of addresses that cannot be assigned to hosts. Therefore, using subnets means accommodating fewer hosts.

For example, a Class B network without subnetting can accommodate 1022 more hosts than the same network subnetted into 512 subnets.

- **Without subnetting**—65534 (2^{16} – 2) hosts. (The two deducted addresses are the broadcast address, which has an all-one host ID, and the network address, which has an all-zero host ID.)

- **With subnetting**—Using the first nine bits of the host-id for subnetting provides 512 (2^9) subnets. However, only seven bits remain available for the host ID. This allows 126 ($2^7 – 2$) hosts in each subnet, a total of 64512 (512 × 126) hosts.

IP address assignment

You can manually assign an IP address to an interface or configure the interface to obtain an IP address through DHCP or PPPoE. Support for DHCP and PPPoE depends on the device model.

Interface MTU

When a packet exceeds the MTU of the sending interface, the device processes the packet in one of the following ways:

- If the packet disallows fragmentation, the device discards it.
- If the packet allows fragmentation, the device fragments it and forwards the fragments.

Fragmentation and reassembling consume system resources, so set the MTU based on the network environment to avoid fragmentation.

Last hop holding

When an interface with this feature enabled receives the first packet of the forward traffic, the interface records the traffic characteristics and last hop in the high-speed cache. When the backward traffic reaches the device for forwarding, the device can guide packet forwarding based on the last hop information recorded. This feature ensures that the forward traffic from the peer end to the local end and the backward traffic from the local end to the peer end are transmitted on the same path. Therefore, traffic of the same session can be processed in the same way.

IPv6 address

IPv6, also called IP next generation (IPng), was designed by the IETF as the successor to IPv4. One significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

IPv6 address format

An IPv6 address is represented as a set of 16-bit hexadecimals separated by colons (:). An IPv6 address is divided into eight groups, and each 16-bit group is represented by four hexadecimal numbers, for example, 2001:0000:130F:0000:0000:09C0:876A:130B.

To simplify the representation of IPv6 addresses, you can handle zeros in IPv6 addresses by using the following methods:

- The leading zeros in each group can be removed. For example, the above address can be represented in a shorter format as 2001:0:130F:0:0:9C0:876A:130B.
- If an IPv6 address contains one or more consecutive groups of zeros, they can be replaced by a double colon (::). For example, the above address can be represented in the shortest format as 2001:0:130F::9C0:876A:130B.

An IPv6 address consists of an address prefix and an interface ID, which are equivalent to the network ID and the host ID of an IPv4 address.

An IPv6 address prefix is written in IPv6-address/prefix-length notation. The prefix-length is a decimal number indicating how many leftmost bits of the IPv6 address are in the address prefix.

IPv6 address type

IPv6 addresses include the following types:

- **Unicast address**—An identifier for a single interface, similar to an IPv4 unicast address. A packet sent to a unicast address is delivered to the interface identified by that address.
- **Multicast address**—An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address. Broadcast addresses are replaced by multicast addresses in IPv6.
- **Anycast address**—An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to the nearest interface among the interfaces identified by that address. The nearest interface is chosen according to the routing protocol's measure of distance.

The type of an IPv6 address is designated by the first several bits, called the format prefix.

Table 2 Mappings between address types and format prefixes

Type		Format prefix (binary)	IPv6 prefix ID	Description
Unicast address	Unspecified address	00...0 (128 bits)	::/128	It cannot be assigned to any node. Before acquiring a valid IPv6 address, a node fills this address in the source address field of IPv6 packets. The unspecified address cannot be used as a destination IPv6 address.
	Loopback address	00...1 (128 bits)	::1/128	It has the same function as the loopback address in IPv4. It cannot be assigned to any physical interface. A node uses this address to send an IPv6 packet to itself.
	Link-local address	1111111010	FE80::/10	Used for communication among link-local nodes for neighbor discovery and stateless autoconfiguration. Packets with link-local source or destination addresses are not forwarded to

Type		Format prefix (binary)	IPv6 prefix ID	Description
				other links.
	Global unicast address	Other forms	N/A	Equivalent to public IPv4 addresses, global unicast addresses are provided for Internet service providers. This type of address allows for prefix aggregation to restrict the number of global routing entries.
Multicast address		11111111	FF00::/8	N/A
Anycast address		Anycast addresses use the unicast address space and have the identical structure of unicast addresses.		N/A

IEEE EUI-64 address-based interface identifiers

An interface identifier is 64 bits long and uniquely identifies an interface on a link.

On an IEEE 802 interface (such as a VLAN interface), the interface identifier is derived from the link-layer address (typically a MAC address) of the interface. The MAC address is 48 bits long.

To obtain an EUI-64 address-based interface identifier, follow these steps:

1. Insert the 16-bit binary number 1111111111111110 (hexadecimal value of FFFE) behind the 24th high-order bit of the MAC address.
2. Invert the universal/local (U/L) bit (the seventh high-order bit). This operation makes the interface identifier have the same local or global significance as the MAC address.

On a tunnel interface, the lower 32 bits of the EUI-64 address-based interface identifier are the source IPv4 address of the tunnel interface. The higher 32 bits of the EUI-64 address-based interface identifier of an ISATAP tunnel interface are 0000:5EFE, whereas those of other tunnel interfaces are all zeros.

On an interface of another type (such as a serial interface) the EUI-64 address-based interface identifier is generated randomly by the device.

Configure an IPv6 global unicast address for an interface

Use one of the following methods to configure an IPv6 global unicast address for an interface:

- **EUI-64 IPv6 address**—The IPv6 address prefix of the interface is manually configured, and the interface ID is generated automatically by the interface.
- **Manual configuration**—The IPv6 global unicast address is manually configured.
- **Stateless address autoconfiguration**—The IPv6 global unicast address is generated automatically based on the address prefix information contained in the RA message.
- **Stateful address autoconfiguration**—The IPv6 global unicast address is obtained through DHCPv6.

You can configure multiple IPv6 global unicast addresses on an interface.

Configure an IPv6 link-local address for an interface

Configure IPv6 link-local addresses using one of the following methods:

- **Automatic generation**—The device automatically generates a link-local address for an interface according to the link-local address prefix (FE80::/10) and the link-layer address of the interface.
- **Manual assignment**—Manually configure an IPv6 link-local address for an interface.

An interface can have only one link-local address. As a best practice, use the automatic generation method to avoid link-local address conflicts. If both the automatic generation and manual assignment methods are used, the manual assignment takes precedence.

- If you first use automatic generation and then manual assignment, the manually assigned link-local address overwrites the automatically generated one.

- If you first use manual assignment and then automatic generation, both of the following occur:
    - The link-local address is still the manually assigned one.
    - The automatically generated link-local address does not take effect. If you delete the manually assigned address, the automatically generated link-local address takes effect.

Last hop holding

When an interface with this feature enabled receives the first IP packet of the forward traffic, the interface records the traffic characteristics and last hop in the high-speed cache. When the backward traffic reaches the device for forwarding, the device can guide packet forwarding based on the last hop information recorded. This feature ensures that the forward traffic from the peer end to the local end and the backward traffic from the local end to the peer end are transmitted on the same path. Therefore, traffic of the same session can be processed in the same way.

Link aggregation

Ethernet link aggregation bundles multiple physical Ethernet links into one logical link (called an aggregate link). Link aggregation provides the following benefits:

- Increased bandwidth beyond the limits of a single individual link. In an aggregate link, traffic is distributed across the member ports.
- Improved link reliability. The member ports dynamically back up one another. When a member port fails, its traffic is automatically switched to other member ports.

Aggregation groups

Each link aggregation is represented by a logical aggregate interface. Each aggregate interface has an automatically created aggregation group, which contains member ports to be used for aggregation. The type and number of an aggregation group are the same as its aggregate interface.

An aggregate interface can be one of the following types:

- **Layer 2**—The member ports in a Layer 2 aggregation group can only be Layer 2 Ethernet interfaces.
- **Layer 3**—The member ports in its Layer 3 aggregation group can only be Layer 3 Ethernet interfaces.

The port rate of an aggregate interface equals the total rate of its Selected member ports. Its duplex mode is the same as that of the Selected member ports.

Aggregation states of member ports in an aggregation group

A member port in an aggregation group might be placed in one of the following aggregation states:

- **Selected**—A Selected port can forward traffic.
- **Unselected**—An Unselected port cannot forward traffic.

Operational key

When aggregating ports, the system automatically assigns each port an operational key based on port information, such as port rate and duplex mode. Any change to this information triggers a recalculation of the operational key.

In an aggregation group, all Selected ports have the same operational key.

Attribute configuration

To become a Selected port, a member port must have the same attribute configuration as the aggregate interface. Table 3 describes the attribute configuration.

Table 3 Attribute configuration

Feature	Attribute configuration
Port isolation	Membership of the port in an isolation group. Isolation group number.
VLAN	VLAN attribute settings: • Permitted VLAN IDs. • PVID. VLAN tagging mode.

Link aggregation modes

An aggregation group operates in one of the following modes:

- **Static**—An aggregation group in static mode is called a static aggregation group.
- **Dynamic**—An aggregation group in dynamic mode is called a dynamic aggregation group. Dynamic aggregation implements IEEE 802.3ad Link Aggregation Control Protocol (LACP).

How static link aggregation works

1. Reference port selection process

When setting the aggregation states of the ports in an aggregation group, the system automatically chooses a member port as the reference port. A Selected port must have the same operational key and attribute configurations as the reference port.

All up member ports with the same attribute configuration as the aggregate interface are candidate reference ports. The system chooses a reference port from among the candidate reference ports based on the following tiebreakers in descending order:

a. Highest port priority.

b. Full duplex and high speed.

c. Full duplex and low speed.

d. Half duplex and high speed.

e. Half duplex and low speed.

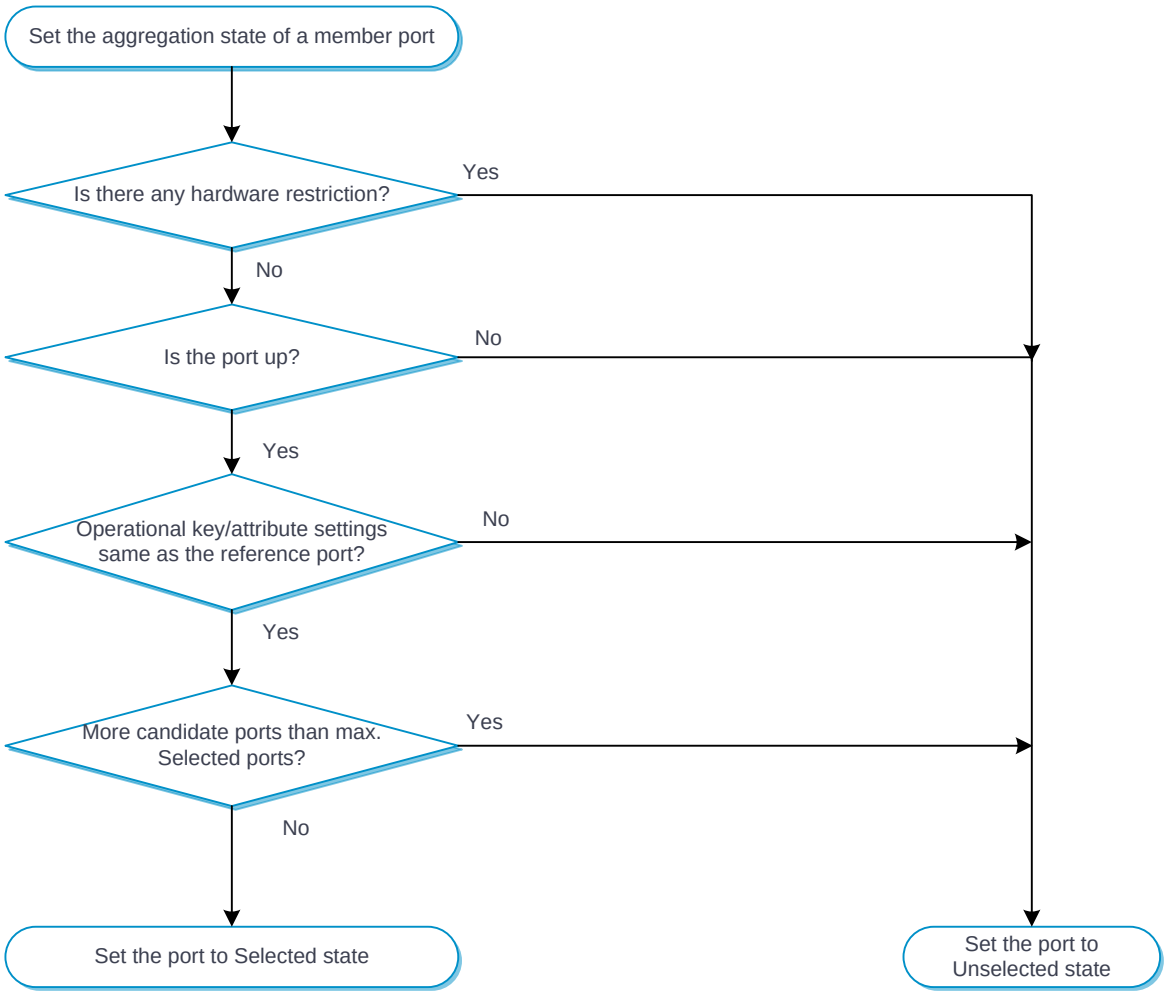
f. Port that used to be Selected.

g. Lowest numbered port.

2. Setting the aggregation state of each member port

After the reference port is chosen, the system sets the aggregation state of each member port in the static aggregation group.

Figure 1 Setting the aggregation state of a member port in a static aggregation group



How dynamic link aggregation works

Dynamic aggregation is an implementation of IEEE 802.3ad Link Aggregation Control Protocol (LACP).

LACP uses LACPDUs to exchange aggregation information between LACP systems. Each member port in a dynamic aggregation group exchanges aggregation information with its peer and compares the received information with information received on the other member ports. Based on the exchanged aggregation information, the two systems reach an agreement on which ports are placed in Selected state.

1. Choosing a reference port

   The system chooses a reference port from the member ports in up state. A Selected port must have the same operational key and attribute configurations as the reference port.

   The local system (the actor) and the peer system (the partner) negotiate a reference port by using the following workflow:

   a. The two systems determine the system with the smaller system ID.

      A system ID contains the LACP system priority and the system MAC address.

      – The two systems compare their LACP priority values.

      The lower the LACP priority, the smaller the system ID. If the LACP priority values are the same, the two systems proceed to the next step.

      – The two systems compare their MAC addresses.

      The lower the MAC address, the smaller the system ID.

   b. The system with the smaller system ID chooses the port with the smallest port ID as the reference port.

      A port ID contains a port priority and a port number. The lower the port priority, the smaller the port ID.

      – The system chooses the port with the lowest priority value as the reference port.

      If the ports have the same priority, the system proceeds to the next step.

      – The system compares their port numbers.

      The smaller the port number, the smaller the port ID.

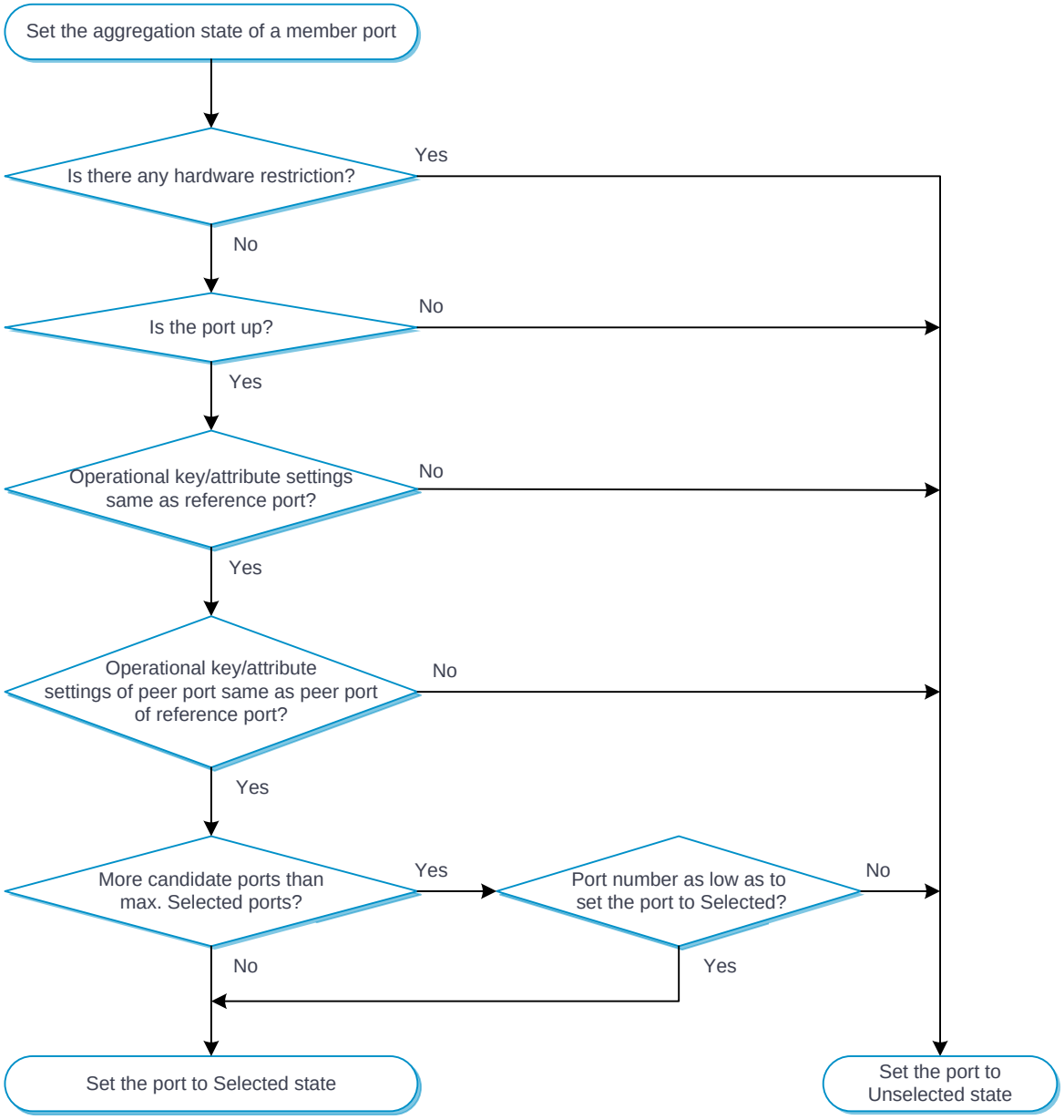
      The port with the smallest port number and the same attribute configurations as the aggregate interface is chosen as the reference port.

2. Setting the aggregation state of each member port

a. After determining the reference port, the system with the smaller system ID sets the state of each member port on its side.

b. The system with the greater system ID detects the aggregation state changes on the peer system. Then, it sets the aggregation state of local member ports to be the same as their peer ports.

Figure 2 Setting the state of a member port in a dynamic aggregation group



A comparison of static link aggregation and dynamic link aggregation

The following are differences between static and dynamic link aggregation modes:

- **Static**—A static aggregation is stable. The peer systems do not negotiate the aggregation states of their member ports. The aggregation state of a member port does not change automatically after the aggregation state of its peer port changes.
- **Dynamic**—The local system and the peer system automatically negotiate and maintain the aggregation states of the member ports.

VLAN termination

About VLAN termination

VLAN termination typically processes packets that include VLAN tags. A VLAN termination-enabled interface performs the following tasks when receiving a VLAN-tagged packet:

- Assigns the packet to an interface according to its VLAN tags.
- Removes the VLAN tags of the packet.
- Delivers the packet to Layer 3 forwarding or other processing pipelines.

Before sending the packet, the VLAN termination-enabled interface determines whether to add new VLAN tags to the packet, based on the VLAN termination type.

VLAN termination types

VLAN termination types	Types of packets to be terminated on the interface	Tags of outgoing packets on the interface
Dot1q termination	The packets must meet both of the following requirements:	Single-tagged

VLAN termination types	Types of packets to be terminated on the interface	Tags of outgoing packets on the interface
	• The packets include one or more layers of VLAN tags. • The outermost VLAN ID matches the configured value.	
Untagged termination	Untagged packets.	Untagged
Default termination	Packets that cannot be processed on any other subinterfaces of the same main interface.	Untagged

VLAN termination mechanism

VLAN interfaces and subinterfaces, such as Layer 3 Ethernet subinterfaces and Layer 3 aggregate subinterfaces, can terminate the following packets:

- Packets whose outermost VLAN IDs match the configured values.
- Packets whose outermost two layers of VLAN IDs match the configured values.

A VLAN interface terminates only the packets whose outermost VLAN ID is the same as the VLAN interface number. For example, VLAN-interface 10 terminates only the packets with the outermost VLAN tag 10.

A main interface does not terminate VLAN-tagged packets (for example, Layer 3 Ethernet interface or Layer 3 aggregate interface). To terminate VLAN-tagged packets, create subinterfaces for the main interface.

Subinterfaces of the same main interface can use different types of VLAN termination. To process received packets, the system selects a subinterface based on the following VLAN termination types in descending order of priority:

- Dot1q termination or support for Dot1q termination by default.

- Untagged termination.
- Default termination.

If none of these VLAN termination types applies, the main interface processes the packets.

If default termination is enabled on a subinterface of an interface, packets are processed by the subinterface instead of the main interface.

When a main interface is bound to a VLAN interface, the main interface processes VLAN-tagged packets according to the VLAN termination configuration of the VLAN interface.

Restrictions and guidelines

- When an interface is shut down, all services that need to pass through the device are interrupted on the network connected to the interface.
- You must set the same aggregation mode at the two ends of an aggregate link.
- For a successful static aggregation, make sure the ports at both ends of each link are in the same aggregation state.
- Deleting a Layer 2 aggregate interface also deletes its Layer 2 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.
- For a link aggregation, attribute configurations are configurable only on the aggregate interface and are automatically synchronized to all member ports. The configuration synchronized from the aggregate interface is retained on the member ports even after the aggregate interface is deleted.
- You cannot assign an interface to a Layer 3 aggregation group if that interface is the member of a Reth interface or is on a redundancy group node.

- Make sure the ports at both ends of a dynamic link aggregation are assigned to the correct aggregation group. The two ends can automatically negotiate the aggregation state of each member port.

Interface pairs

This help contains the following topics:

Introduction

Interface pairs monitor traffic at the data link layer. It is typically used on security devices. Layer 2 traffic arriving at a device is redirected to a security device, filtered, and then forwarded toward the destination.

The following forwarding modes are supported:

- **Reflect-type forwarding**—Forwards a packet through the receiving port of the packet.
- **Blackhole-type forwarding**—Drops the received packets.
- **Forward-type forwarding**—Forwards a packet through a port that is different from the receiving port of the packet.

Forwarding of tunneled packets

By default, tunneled packets are forwarded based on the tunnel headers.

You can configure the device to forward tunneled packets based on the original packet headers.

VLAN ID check

This feature enables the device to check the VLAN ID of each packet that matches a session entry during inline forwarding.

- With VLAN ID check enabled, the device permits a packet only if its VLAN ID is the same as the VLAN ID in the matching session entry.
- With VLAN ID check disabled, the device permits a packet if it matches a session entry.

On a hot backup system, you must disable VLAN ID check if the traffic incoming interfaces on the primary and secondary devices belong to different VLANs. If you enable VLAN ID check, traffic cannot match session entries correctly after a primary/secondary device switchover occurs or when asymmetric-path traffic exists.

Security service bypass

By default, packets are processed by the security service first before being forwarded according to the configured bridge forwarding mode.

The security service bypass feature enables user traffic to bypass security service processing of a security device and be forwarded directly according to the configured bridge forwarding mode.

Security service bypass can be classified into internal bypass and external bypass.

- **Internal bypass**—User traffic is sent to the security device but is not processed by it. The security device directly forwards or drops the traffic according to the configured bridge forwarding mode.
- **External bypass**—User traffic is forwarded by the Power Free Connector (PFC) device directly without passing through the security device.

Internal bypass

User traffic is sent to the security device but is not processed by it. The security device directly forwards or drops the traffic according to the configured bridge forwarding mode.

Internal bypass is available for interface pairs operating in reflect-type, blackhole-type, or forward-type forwarding mode.

External bypass

User traffic is forwarded by the Power Free Connector (PFC) device directly without passing through the security device.

Internal bypass is available only for interface pairs using the forward-type forwarding mode.

External bypass can be further classified in to the following types:

- **Static external bypass**—External bypass takes effect immediately when configured and must be manually disabled.
- **Dynamic external bypass**—External bypass is enabled or disabled automatically based on the status of the links between the security device and the PFC. The security device polls the link status periodically and enables external bypass if one or both links go down. External bypass is disabled automatically if the failed links come up.

Restrictions and guidelines

- Only a Layer 2 or Layer 3 Ethernet interface or a Layer 2 aggregate interface can be added to an interface pair operating in reflect-type, blackhole-type, or forward-type forwarding mode.
- For a forward-type interface pair that is automatically created upon insertion of a hardware bypass subcard, you can enable only internal bypass for the interface pair.
- Support for the external bypass feature depends on the device model.

Interface collaboration

Introduction

The interface collaboration feature assigns different interfaces on a device to a collaboration group and associates the states of these interfaces. All member interfaces in a collaboration group can or cannot transmit packets at the same time.

How it works

The interface collaboration feature works as follows:

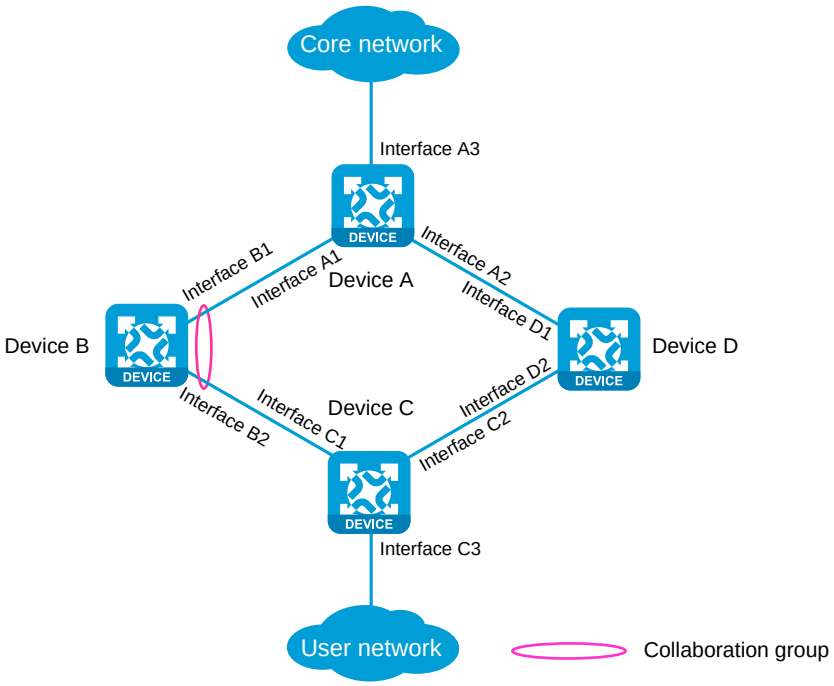
- When any member interface in a collaboration group goes down, the device sets all other member interfaces in the collaboration group to the **Collaboration-down** state. The state of the collaboration group is down, and no member interfaces in the collaboration group can transmit packets.
- When any member interface in **DOWN** or **Collaboration-down** state comes up, the device attempts to bring up all other member interfaces in the collaboration group.
    - If all other member interfaces come up in 10 seconds, the collaboration group comes up. All member interfaces in the collaboration group can transmit packets.
    - If any member interface cannot come up in 10 seconds, the device sets that member interface to **DOWN** state and sets all other member interfaces to the **Collaboration-down** state. The collaboration group remains down, and no member interfaces in the collaboration group can transmit packets.

Typical networking

As shown in Figure 1, LAN users access the Internet through Device B. When interface B1 goes down, the traffic switches over from Device B to Device C. The switchover is slow because interface B2 is still up and route updating is slow.

If the two interfaces belong to one collaboration group, Device B brings down interface B2 when interface B1 goes down to achieve fast traffic switchover. Similarly, the device brings down interface B1 when interface B2 goes down.

Figure 1 Network diagram



Restrictions and guidelines

- Collaboration groups take effect only when Monitor Link is enabled globally.

- An interface can belong to only one collaboration group.
- If the device is connected to the peer device through multiple interfaces, do not assign all these interfaces to the same aggregation group. If you assign all these interfaces to the same aggregation group, all connected peer interfaces go down when one of these interfaces goes down.
- For a collaboration group to work correctly, do not assign its member interfaces to an aggregation group or redundancy group.
- You can assign only one interface of a link to a collaboration group.

Security zones

Introduction

A security zone is a collection of interfaces that have the same security requirements. You can configure security zones to implement security zone-based security management.

Security zone members

A security zone can include the following types of members:

- Layer 2 interface-VLAN combination
- Layer 3 interface:
  - Layer 3 Ethernet interface
  - Layer 3 logical interface, such as a Layer 3 subinterface

Security zone-based packet processing rules

The following table describes how the device handles packets when security zone-based security management is configured:

Packets	Action
Packets between an interface that is in a security zone and an interface that is not in any security	Discard.

Packets	Action
zone	
Packets between two interfaces that are in the same security zone	Discard by default.
Packets between two interfaces that belong to different security zones	Forward or discard, depending on the matching security control policy. If no policy is applied or the policy does not exist or does not take effect, the packets are discarded.
Packets between two interfaces that are not in any security zone	Discard.
Packets originated from or destined for the device itself	Forward or discard, depending on the matching object policy. By default, these packets are discarded.

Restrictions and guidelines

- The device management interface belongs to the **Management** security zone. You can log in to the Web interface of the device from the management interface to manage the device remotely. If you remove the management interface from the **Management** security zone, the Web access is terminated immediately.
- A Layer 3 interface can be added to only one security zone.
- A Layer 2 interface-VLAN combination can be added to only one security zone.
- If a packet does not match any zone pair between specific security zones, the device searches for the any-to-any zone pair.
    - If the zone pair exists, the device processes the packet by using the security policies applied to the zone pair.
    - If the zone pair does not exist, the device discards the packet.

- By default, the device forwards packets between the **Management** and **Local** zones.
- For packets between the **Management** and **Local** security zones, the device uses only security control policies applied to the zone pairs of the two security zones.

VLAN

Introduction

The Virtual Local Area Network (VLAN) technology divides a physical LAN into multiple logical LANs. It has the following benefits:

- **Security**—Hosts in the same VLAN can communicate with one another at Layer 2, but they are isolated from hosts in other VLANs at Layer 2.
- **Broadcast traffic isolation**—Each VLAN is a broadcast domain that limits the transmission of broadcast packets.
- **Flexibility**—A VLAN can be logically divided on a workgroup basis. Hosts in the same workgroup can be assigned to the same VLAN, regardless of their physical locations.

Port-based VLANs

Port-based VLANs group VLAN members by port. A port forwards packets from a VLAN only after it is assigned to the VLAN.

In a VLAN, a port can be added to an untagged port list to be an untagged port or be added to a tagged port list to be a tagged port. The untagged port in the VLAN sends packets untagged and the tagged port in the VLAN sends packets tagged.

You can set the link type of a port to access, trunk, or hybrid. The link types use the following VLAN tag handling methods:

- **Access**—An access port can forward packets only from one VLAN and send these packets untagged. An access port can be added to an untagged port list in only one VLAN.
- **Trunk**—A trunk port can forward packets from multiple VLANs. Except packets from the port VLAN ID (PVID), packets sent out of a trunk port are VLAN-tagged. In the PVID of a trunk port, the port can be added to only an untagged port list. In other VLANs, the port can be added to only an tagged port list.
- **Hybrid**—A hybrid port can forward packets from multiple VLANs. The tagging status of the packets forwarded by a hybrid port depends on the port configuration. In different VLANs, a hybrid port can be added to an untagged port list or a tagged port list upon configuration requirement.

VLAN interfaces

Hosts of different VLANs use VLAN interfaces to communicate at Layer 3. VLAN interfaces are virtual interfaces that do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface and assign an IP address to it. The VLAN interface acts as the gateway of the VLAN to forward packets destined for another IP subnet at Layer 3.

Restrictions and guidelines

As the system default VLAN, VLAN 1 cannot be created or deleted.

MAC

This help contains the following topics:

- Introduction
  - Types of MAC address entries
  - Aging timer for dynamic MAC address entries
  - MAC address learning
  - VLAN ID check
- Restrictions and guidelines

Introduction

An Ethernet device uses a MAC address table to forward frames. A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID. When the device receives a frame, it uses the destination MAC address of the frame to look for a match in the MAC address table.

- The device forwards the frame out of the outgoing interface in the matching entry if a match is found.
- The device floods the frame in the VLAN of the frame if no match is found.

Types of MAC address entries

A MAC address table can contain the following types of entries:

- **Dynamic entries**—A dynamic entry can be manually configured or dynamically learned to forward frames with a specific destination MAC address out of the associated interface. A dynamic entry can age out. A manually configured dynamic entry has the same priority as a dynamically learned one.
- **Static entries**—A static entry is manually added to forward frames with a specific destination MAC address out of the associated interface, and it never ages out. A static entry has higher priority than a dynamically learned one.
- **Blackhole entries**—A blackhole entry is manually configured and never ages out. A blackhole entry is configured for filtering out frames with a specific source or destination MAC address. For example, to block all frames destined for or sourced from a user, you can configure the MAC address of the user as a blackhole MAC address entry.

Aging timer for dynamic MAC address entries

For security and efficient use of table space, the MAC address table uses an aging timer for dynamic entries learned on all interfaces. If a dynamic MAC address entry is not updated before the aging timer expires, the device deletes the entry. This aging mechanism ensures that the MAC address table can promptly update to accommodate latest network topology changes.

A stable network requires a longer aging interval, and an unstable network requires a shorter aging interval.

- An aging interval that is too long might cause the MAC address table to retain outdated entries. As a result, the MAC address table resources might be exhausted, and the MAC address table might fail to update its entries to accommodate the latest network changes.

- An interval that is too short might result in removal of valid entries, which would cause unnecessary floods and possibly affect the device performance.

To reduce floods on a stable network, set a long aging timer or disable the timer to prevent dynamic entries from unnecessarily aging out. Reducing floods improves the network performance. Reducing flooding also improves the security because it reduces the chances for a data frame to reach unintended destinations.

MAC address learning

MAC address learning is enabled by default. To prevent the MAC address table from being saturated when the device is experiencing attacks, disable MAC address learning. For example, you can disable MAC address learning to prevent the device from being attacked by a large amount of frames with different source MAC addresses.

When global MAC address learning is enabled, you can disable MAC address learning on a single interface.

You can also configure the MAC learning limit on an interface to limit the MAC address table size. A large MAC address table will degrade forwarding performance. When the limit is reached, the interface stops learning any MAC addresses. You can also configure whether to forward frames whose source MAC address is not in the MAC address table.

VLAN ID check

This feature enables the device to check the VLAN ID of each packet that matches a session entry during Layer 2 forwarding.

- With VLAN ID check enabled, the device permits a packet only if its VLAN ID is the same as the VLAN ID in the matching session entry.

- With VLAN ID check disabled, the device permits a packet if it matches a session entry.

On a hot backup system, you must disable VLAN ID check if the traffic incoming interfaces on the primary and secondary devices belong to different VLANs. If you enable VLAN ID check, traffic cannot match session entries correctly after a primary/secondary device switchover occurs or when asymmetric-path traffic exists.

Restrictions and guidelines

When you configure MAC address entries, follow these restrictions and guidelines:

- The manually configured static and blackhole MAC address entries cannot survive a reboot if you do not save the configuration.
- The manually configured dynamic MAC address entries are lost upon reboot whether or not you save the configuration.

DNS

This help contains the following topics:

- Introduction
  - DNS
  - DDNS
  - DNS proxy
- Restrictions and guidelines

Introduction

DNS

Domain Name System (DNS) is a distributed database used by TCP/IP applications to translate domain names into IP addresses. IPv4 DNS translates domain names into IPv4 addresses, and IPv6 DNS translates domain names into IPv6 addresses.

The device can function as a DNS client. When the user runs a program on the device using a domain name (for example, Telnet to a device or host), DNS resolves the domain name into its IP address.

Domain name resolution can be static or dynamic:

- Static domain name resolution

Static domain name resolution means manually creating mappings between domain names and IP addresses. For example, you can create a static DNS mapping for a device so that you can Telnet to the device by using the domain name.

- Dynamic domain name resolution

  To use dynamic domain name resolution, you must specify the IP address of the DNS server. Domain name resolution queries are sent to the DNS server.

  You can configure a domain name suffix list so that the resolver can use the list to supply the missing part of an incomplete name. For example, you can configure **com** as the suffix for aabbcc.com. The user only needs to enter **aabbcc** to obtain the IP address of aabbcc.com. The resolver adds the suffix and delimiter before passing the name to the DNS server.

  The name resolver handles the queries based on the domain names that the user enters:

  - If the user enters a domain name without a dot (.) (for example, aabbcc), the resolver considers the domain name to be a host name. It adds a DNS suffix to the host name before performing the query operation. If no match is found for any host name and suffix combination, the resolver uses the user-entered domain name (for example, aabbcc) for the IP address query.
  - If the user enters a domain name with a dot (.) among the letters (for example, www.aabbcc), the resolver directly uses this domain name for the query operation. If the query fails, the resolver adds a DNS suffix for another query operation.
  - If the user enters a domain name with a dot (.) at the end (for example, aabbcc.com.), the resolver considers the domain name an FQDN and returns the successful or failed query result. The dot at the end of the domain name is considered a terminating symbol.

After a user specifies a name, the device checks the static name resolution table for an IP address. If no IP address is available, it contacts the DNS server for dynamic name resolution, which takes more time than static name resolution. To improve efficiency, you can put frequently queried name-to-IP address mappings in the local static name resolution table.

DDNS

DNS provides only the static mappings between domain names and IP addresses. When the IP address of a node changes, your access to the node fails.

Dynamic Domain Name System (DDNS) can dynamically update the mappings between domain names and IP addresses for DNS servers.

To use DDNS, you must first log in to the DDNS server to register an account. The device acts as the DDNS client and sends the DNS server a DDNS update request when the IP address of the device changes. The request contains the latest mapping of the domain name and IP address and user account credentials (username and password). After the DDNS client passes authentication, the DDNS server informs the DNS server to update the domain name and the IP address of the DDNS client.

DDNS is supported by only IPv4 DNS. It is used to update the mappings between domain names and IPv4 addresses.

A DDNS policy contains the DDNS server address, username, password, associated SSL client policy, and update time interval. After creating a DDNS policy, you can apply it to multiple interfaces to simplify DDNS configuration.

DNS proxy

The DNS proxy performs the following functions:

- Forwards the request from the DNS client to the designated DNS server.
- Conveys the reply from the DNS server to the client.

The DNS proxy simplifies network management. When the DNS server address is changed, you can change the configuration only on the DNS proxy instead of on each DNS client.

Restrictions and guidelines

- A DNS server address is required so that DNS queries can be sent to a correct server for resolution. If you specify both an IPv4 address and an IPv6 address, the device performs the following operations:
    - Sends an IPv4 DNS query first to the DNS server IPv4 addresses. If the query fails, the device turns to the DNS server IPv6 addresses.
    - Sends an IPv6 DNS query first to the DNS server IPv6 addresses. If the query fails, the devices turns to the DNS server IPv4 addresses.
- A DNS server address specified earlier has a higher priority. A DNS server address manually specified takes priority over a DNS server address dynamically obtained, for example, through DHCP. The device first sends a DNS query to the DNS server address of the highest priority. If the first query fails, it sends the DNS query to the DNS server address of the second highest priority, and so on.
- A DNS suffix configured earlier has a higher priority. A DNS suffix manually configured takes priority over a DNS suffix dynamically obtained, for example, through DHCP. The device first uses the suffix that has the highest priority. If the query fails, the device uses the suffix that has the second highest priority, and so on.

ARP

Introduction

ARP

ARP resolves IP addresses into MAC addresses on Ethernet networks.

An ARP table stores dynamic ARP entries and static ARP entries.

Dynamic ARP entries

ARP automatically creates and updates dynamic entries. A dynamic ARP entry is removed when its aging timer expires or the output interface goes down. In addition, a dynamic ARP entry can be overwritten by a static ARP entry.

Dynamic ARP entries can be converted into static ARP entries, which cannot be converted into dynamic ARP entries again.

To prevent an interface from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the interface can learn.

Static ARP entries

A static ARP entry is manually configured and maintained. It does not age out and cannot be overwritten by any dynamic ARP entry.

Static ARP entries protect communication between devices because attack packets cannot modify the IP-to-MAC mapping in a static ARP entry.

To communicate with a host by using a fixed IP-to-MAC mapping, configure a short static ARP entry on the device. To communicate with a host by using a fixed IP-to-MAC mapping through an interface in a VLAN, configure a long static ARP entry on the device.

IP-MAC binding entries

The device prevents user spoofing attacks by using an IP-MAC binding table to filter out illegitimate packets with forged source IP addresses or MAC addresses.

IP-MAC binding entries can be created manually or generated in bulk.

- **Manual creation**—You can manually create IP-MAC binding entries one by one. This method is applicable only to networks that do not contain many hosts.
- **Bulk generation**—You can configure the device to generate IPv4-MAC binding entries in bulk based on ARP entries on an interface. This method is applicable only to networks that contain many hosts.

Configure IP-MAC binding entries on the device to improve communication security. Upon receiving a packet, the device compares the source IP address and source MAC address in the packet with the IP-MAC binding entries.

- If the source IP address and source MAC address match the same entry, the device determines that the packet is from a legal user and permits the packet to pass through.
- In the following situations, the device determines that the packet is a forged packet and drops the packet:
    - Only the source IP address or source MAC address matches a binding entry.
    - The source IP address and source MAC address match two different binding entries.
- If the source IP address and the source MAC address match no binding entry, the device processes the packet based on the default action.

ND

Introduction

IP-MAC binding entries

The device prevents user spoofing attacks by using an IP-MAC binding table to filter out illegitimate packets with forged source IPv6 addresses or MAC addresses.

ND

The IPv6 neighbor discovery (ND) process uses ICMP messages for address resolution, neighbor reachability verification, and neighboring device tracking.

Table 1 describes the ICMPv6 messages used by the IPv6 ND protocol.

Table 1 ICMPv6 messages used by ND

ICMPv6 message	Type	Function
Neighbor Solicitation (NS)	135	Acquires the link-layer address of a neighbor on the local link.
		Verifies the reachability of a neighbor.
		Detects duplicate addresses.

ICMPv6 message	Type	Function
Neighbor Advertisement (NA)	136	Responds to an NS message.
		Notifies the neighboring nodes of link layer changes.
Router Solicitation (RS)	133	Requests an address prefix and other configuration information for autoconfiguration after startup.
Router Advertisement (RA)	134	Responds to an RS message.
		Advertises information, such as the Prefix Information options and flag bits.
Redirect	137	Informs the source host of a better next hop on the path to a particular destination when certain conditions are met.

Restrictions and guidelines

Restrictions and guidelines: IP-MAC binding entries

IP-MAC binding entries can be created manually or generated in bulk.

- **Manual creation**—You can manually create IP-MAC binding entries one by one. This method is applicable only to networks that do not contain many hosts.
- **Bulk generation**—You can configure the device to generate IPv6-MAC binding entries in bulk based on ND entries on an interface. This method is applicable to networks that contain many hosts.

Configure IP-MAC binding entries on the device to improve communication security. Upon receiving a packet, the device compares the source IPv6 address and source MAC address in the packet with IP-MAC binding entries.

- If the source IPv6 address and source MAC address match the same IP-MAC binding entry, the device forwards the packet.
- In the following situations, the device determines that the packet is a forged packet and drops the packet:
  - Only the source IP address or source MAC address matches a binding entry.
  - The source IP address and source MAC address match two different binding entries.
- If both the source IPv6 address and the source MAC address match no IP-MAC binding entry, the device permits or drops the packet based on the default action configuration.

Restrictions and guidelines: ND entries

A neighbor entry stores information about a link-local node. The entry can be created dynamically through NS and NA messages, or configured statically.

You can configure a static neighbor entry by using one of the following methods:

- **Method 1**—Associate a neighbor's IPv6 address and link-layer address with the local Layer 3 interface.
- **Method 2**—Associate a neighbor's IPv6 address and link-layer address with a Layer 2 port in a VLAN.

You can use either of the methods to configure a static neighbor entry for a VLAN interface.

- If you use Method 1, the device is required to resolve the Layer 2 port in the related VLAN.
- If you use Method 2, make sure the Layer 2 port belongs to the specified VLAN and the corresponding VLAN interface already exists.

Forwarding advanced settings

Introduction

DF bit processing method

If the size of a packet to be forwarded exceeds the path MTU, the device must fragment it before forwarding it out. If the DF bit of this packet is set, the device does not forward the packet and a communication failure occurs. The device will only send an ICMP error message to the source host of the packet.

This feature allows the device to modify the DF bit setting of IP packets, so that the packets can be fragmented and forwarded.

The feature takes effect only on the IP packets to be forwarded and does not affect the DF bit setting of the locally generated packets.

Packet forwarding modes

Support for the packet distribution policy depends on the device model.

- On a multi-CPU device, packets can be distributed among CPUs based on one of the following policies:

- Flow-based policy—Forwards packets of a flow to one CPU or multiple CPUs. This policy takes the first-in first-out rule. A data flow is defined by using the following criteria:
  - One-tuple—Uses only one of the items for flow identification: source IP address, destination IP address, source port number, or destination port number.
  - Three-tuple—Uses the combination of source IP address, destination IP address, and protocol number for flow identification.
  - Five-tuple—Uses the combination of source IP address, source port number, destination IP address, destination port number, and protocol number for flow identification.

  In enhanced mode, the device uses different CPUs to receive and forward packets of the same flow, improving the flow processing efficiency.
- Packet-based policy—Forwards packets in sequence to different CPUs, even though they are the same flow. This policy does not ensure packet order.

ALG

Introduction

You can enable ALG for the specified application protocol type to analyze and process the application layer packet payload. On the device, you can enable ALG for the following services:

- NAT ALG
  - NAT44 supports ALG for the following protocols:
    - DNS.
    - H323.
    - RTSP.
    - ILS.
    - PPTP.
    - FTP.
    - SIP.
    - SQLNET.
    - MGCP.
    - RSH.
    - ICMP error packets.
    - TFTP.
    - XDMCP.
    - NBT.

        - SCCP.
        - SCTP.
    - NAT64 supports ALG for the following protocols:
        - DNS.
        - FTP.
        - HTTP.
        - ICMP error packets.
    - NAT66 supports ALG for the following protocols:
        - FTP.
        - ICMP error packets.
- LB ALG

  LB LAG supports ALG for the following protocols:
    - DNS.
    - H323.
    - RTSP.
    - ILS.
    - PPTP.
    - FTP.
    - SIP.
    - SQLNET.
    - MGCP.
    - RSH.
    - ICMP error packets.

    - TFTP.
    - XDMCP.
    - NBT.
    - SCCP
- ASPF ALG

  ASPF ALG supports ALG for the FTP protocol,

GRE

This help contains the following topics:

- Introduction
  - GRE encapsulation format
  - GRE tunnel operating principle
  - GRE keepalive mechanism
  - GRE security mechanisms
- Restrictions and guidelines

Introduction

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a protocol (such as IPv4) into a virtual point-to-point tunnel over a network (such as an IPv6 network). Packets are encapsulated at one tunnel end and de-encapsulated at the other tunnel end. The network layer protocol of the packets before encapsulation and after encapsulation can be the same or different.

GRE encapsulation format

A GRE-tunneled packet includes the following parts:

- **Payload packet**—Original packet. The protocol type of the payload packet is called the passenger protocol. The passenger protocol can be any network layer protocol.
- **GRE header**—Header that is added to the payload packet to change the payload packet to a GRE packet. A GRE header includes the number of encapsulations, version, passenger protocol type, checksum, and key. GRE is called the encapsulation protocol.
- **Delivery header**—Header that is added to the GRE packet to deliver it to the tunnel end. The transport protocol (or delivery protocol) is the network layer protocol that transfers GRE packets.

  The device supports GRE tunnels with IPv4 and IPv6 as the transport protocols. When the transport protocol is IPv4, the GRE tunnel mode is GRE over IPv4 (GRE/IPv4). When the transport protocol is IPv6, the GRE tunnel mode is GRE over IPv6 (GRE/IPv6).

GRE tunnel operating principle

An IPv4 or IPv6 protocol packet traverses a transport network through a GRE tunnel as follows:

1. After the source device receives an IPv4 or IPv6 protocol packet from a customer-side interface, it processes the packet as follows:
   a. Looks up the routing table to identify the outgoing interface for the packet.
   b. Submits the packet to the outgoing interface—a GRE tunnel interface.
2. Upon receiving the packet, the tunnel interface encapsulates the packet with GRE and then with the delivery header. In the delivery header, the source address is the tunnel's source address and the destination address is the tunnel's destination address.
3. The source device looks up the routing table according to the destination address in the delivery header. Then, the device forwards the encapsulated packet out of the physical interface of the GRE tunnel.

4. When the packet arrives at the GRE tunnel destination, the destination device checks the destination address. Because the destination is the device itself and the protocol number in the IP header is 47 (the protocol number for GRE), the device submits the packet to GRE for de-encapsulation.
5. GRE first removes the delivery header, and then checks the GRE key, checksum, and packet sequence number. After GRE finishes the checking, it removes the GRE header, and submits the payload to the passenger protocol for forwarding.

GRE keepalive mechanism

This mechanism enables a tunnel interface to send keepalive packets at the specified interval. If the device does not receive any response from the peer within the timeout time, it shuts down the local tunnel interface. The device brings the local tunnel interface up if it receives a keepalive acknowledgment packet from the peer. The timeout time is the result of multiplying the keepalive interval by the keepalive number.

The device always acknowledges the keepalive packets it receives whether or not GRE keepalive is enabled.

GRE security mechanisms

GRE supports the GRE key and GRE checksum security mechanisms.

GRE key

GRE keys ensure packet validity. The sender adds a GRE key into a packet. The receiver compares the GRE key with its own GRE key. If the two keys are the same, the receiver accepts the packet. If the two keys are different, the receiver drops the packet.

GRE checksum

GRE checksums ensure packet integrity. The sender calculates a checksum for the GRE header and payload and sends the packet containing the checksum to the tunnel peer. The receiver calculates a checksum for the received packet and compares it with that carried in the packet. If the checksums are the same, the receiver determines the packet intact and continues to process the packet. If the checksums are different, the receiver discards the packet.

Restrictions and guidelines

When you configure a GRE tunnel, follow the restrictions and guidelines in this section.

Restrictions and guidelines: Address configuration

When the passenger protocol is IPv4, configure an IPv4 address for the tunnel interface at each tunnel end. When the passenger protocol is IPv6, configure an IPv6 address for the tunnel interface at each tunnel end.

You must configure the tunnel source address and destination address at both ends of a tunnel. The tunnel source or destination address at one end must be the tunnel destination or source address at the other end.

The IP address of a tunnel interface and the tunnel destination address configured on the tunnel interface must be in different subnets.

Restrictions and guidelines: Routing configuration

To ensure correct packet forwarding, identify whether the destination network of packets and the IP address of the local tunnel interface are on the same subnet. If they are not, configure a route reaching the destination network through the tunnel interface. You can configure the route by using one of the following methods:

- Configure a static route, using the local tunnel interface as the outgoing interface of the route.
- Enable a dynamic routing protocol on both the tunnel interface and the interface connecting the private network. This allows the dynamic routing protocol to establish a routing entry with the tunnel interface as the outgoing interface.

Restrictions and guidelines: Keepalive configuration

You do not need to enable keepalive on both ends of a GRE tunnel. Enable keepalive on one end of a GRE tunnel as needed.

Restrictions and guidelines: GRE security mechanism configuration

The two ends of a GRE tunnel must have the same key or both have no key.

You can enable or disable GRE checksum at each end of a tunnel. If GRE checksum is enabled at a tunnel end, the tunnel end sends packets carrying the checksum to the peer end. A tunnel end checks the GRE checksum of a received packet if the packet carries a GRE checksum, whether or not the tunnel end is enabled with GRE checksum.

IPsec

This help contains the following topics:

- Introduction
  - Security protocols and encapsulation modes
  - Authentication and encryption
  - IPsec SA
  - IKE negotiation
  - IPsec tunnel establishment
  - IPsec smart link selection
  - Auto-generate security policy
- Restrictions and guidelines

Introduction

IP Security (IPsec) is defined by the IETF to provide interoperable, high-quality, cryptography-based security for IP communications. It is a Layer 3 VPN technology that transmits data in a secure channel established between two endpoints (such as two security gateways). Such a secure channel is usually called an IPsec tunnel.

IPsec is a security framework that has the following protocols and algorithms:

- Authentication Header (AH).
- Encapsulating Security Payload (ESP).

- Internet Key Exchange (IKE).
- Algorithms for authentication and encryption.

AH and ESP are security protocols that provide security services. IKE performs automatic key exchange.

Security protocols and encapsulation modes

Security protocols

IPsec comes with two security protocols, AH and ESP. They define how to encapsulate IP packets and the security services that they can provide.

- AH defines the encapsulation of the AH header in an IP packet. AH can provide data origin authentication, data integrity, and anti-replay services to prevent data tampering, but it cannot prevent eavesdropping. Therefore, it is suitable for transmitting non-confidential data.
- ESP defines the encapsulation of the ESP header and trailer in an IP packet. ESP can provide data encryption, data origin authentication, data integrity, and anti-replay services. Unlike AH, ESP can guarantee data confidentiality because it can encrypt the data before encapsulating the data to IP packets.

Both AH and ESP provide authentication services, but the authentication service provided by AH is stronger. In practice, you can choose either or both security protocols. When both AH and ESP are used, an IP packet is encapsulated first by ESP and then by AH.

Encapsulation modes

IPsec supports the following encapsulation modes:

- Transport mode

The security protocols protect the upper layer data of an IP packet. You can use the transport mode when end-to-end security protection is required (the secured transmission start and end points are the actual start and end points of the data). The transport mode is typically used for protecting host-to-host communications.

- Tunnel mode

  The security protocols protect the entire IP packet. You must use the tunnel mode when the secured transmission start and end points are not the actual start and end points of the data packets (for example, when two gateways provide IPsec but the data start and end points are two hosts behind the gateways). The tunnel mode is typically used for protecting gateway-to-gateway communications

Authentication and encryption

Authentication algorithms

IPsec uses hash algorithms to perform authentication. A hash algorithm produces a fixed-length digest for an arbitrary-length message. IPsec peers respectively calculate message digests for each packet. The receiver compares the local digest with that received from the sender. IPsec supports the following types of authentication algorithms:

- Hash-based Message Authentication Code (HMAC) based authentication algorithms, including HMAC-MD5 and HMAC-SHA.

  HMAC-MD5 is faster but less secure than HMAC-SHA.

- SM3 authentication algorithms.

Encryption algorithms

IPsec uses symmetric encryption algorithms, which encrypt and decrypt data by using the same keys. The following encryption algorithms are available for IPsec on the device:

- **DES**—Encrypts a 64-bit plaintext block with a 56-bit key. DES is the least secure but the fastest algorithm.
- **3DES**—Encrypts plaintext data with three 56-bit DES keys. The key length totals up to 168 bits. It provides moderate security strength and is slower than DES.
- **AES**—Encrypts plaintext data with a 128-bit, 192-bit, or 256-bit key. AES provides the highest security strength and is slower than 3DES.
- **SM**—Encrypts plaintext data with a 128-bit key. SM provides the same level of security strength as AES.

IPsec SA

A security association (SA) is an agreement negotiated between two IPsec peers. An SA includes the following parameters for data protection:

- Security protocols.
- Encapsulation mode.
- Authentication algorithm.
- Encryption algorithm.
- Shared keys and their lifetimes.

An SA is unidirectional. At least two SAs are needed to protect data flows in a bidirectional communication. If two peers want to use both AH and ESP to protect data flows between them, they construct an independent SA for each protocol in each direction.

An SA is uniquely identified by a triplet, which consists of the security parameter index (SPI), destination IP address, and security protocol identifier. An SPI is a 32-bit number. It is transmitted in the AH/ESP header.

An IKE-created SA has a lifetime and will be deleted when its time-based or traffic-based lifetime timer expires. Before the SA lifetime timer expires, IKE negotiates a new SA, which takes over immediately after its creation.

IKE negotiation

IKE negotiates SAs for IPsec and transfers the SAs to IPsec, and IPsec uses the SAs to protect IP packets. IKE negotiates keys and SAs for IPsec in two phases:

1. **Phase 1**—The two peers establish an IKE SA, a secure, authenticated channel for communication.

   Phase 1 negotiation can use the main mode, aggressive mode, or GM main mode. The aggressive mode is faster than the main mode but it does not provide identity information protection. The main mode provides identity information protection but is slower. Choose the appropriate negotiation mode according to your requirements. The GM main mode must be used if the local IKE peer uses the RSA-DE or SM2-DE digital envelop authentication method.

2. **Phase 2**—Using the IKE SA established in phase 1, the two peers negotiate to establish IPsec SAs to protect IP packets.

IPsec tunnel establishment

Two peers establish an IPsec tunnel in between by applying an IPsec policy to an interface. An IPsec policy defines the range of packets to be protected by IPsec and the security parameters used for the protection.

When an IPsec peer identifies the packets to be protected according to the security policy, it sets up an IPsec tunnel and sends the packet to the remote peer through the tunnel. The IPsec tunnel can be set up through IKE negotiation triggered by the packet. The IPsec tunnels are actually the IPsec SAs. The inbound packets are protected by the inbound SA, and the outbound packets are protected by the outbound SA.

- When sending a packet, an interface configured with IPsec policies looks through the IPsec policies in ascending order of policy priorities. If the packet matches a protected flow of an IPsec policy, the interface encapsulates the packet according to the IPsec policy. If no match is found, the interface sends the packet out without IPsec protection.
- When the interface receives an IPsec packet destined for the local device, it searches for the inbound IPsec SA according to the SPI in the IPsec packet header for de-encapsulation. If the de-encapsulated packet matches a protected data flow, the device processes the packet. If the de-encapsulated packet does not match a protected data flow, the device drops the packet.

In an IPsec policy, you can specify whether to protect a data flow by selecting the action (Protect or Do not protect). You can define multiple data flows in an IPsec policy. The device processes a packet according to the action defined in the first matching data flow of the packet.

- Both inbound and outbound packets of an interface need to match the data flows defined in the IPsec policy. The device performs forward matching of the data flows for outbound packets and backward matching of the data flows for inbound packets.

- In outbound direction, packets that match "protect" data flows will be protected by IPsec. Packets that match no data flows or match "unprotect" data flows will not be protected by IPsec.
- In inbound direction, non-IPsec packets that match "protect" data flows will be dropped. IPsec packets destined for the local device will be de-encapsulated.

IPsec smart link selection

To improve network stability and availability, multiple links are typically deployed at the network egress to connect to the destination network. The qualities of these links (in terms of packet loss ratio and delay) are not static but keep changing with time. It is important that the gateway device can dynamically select a link with desired transmission quality to establish the IPsec tunnel to the destination. IPsec smart link selection can meet this requirement.

IPsec smart link selection enables the gateway to monitor the real-time packet loss ratio and delay of the active link over which the IPsec tunnel is established. If the packet loss ratio or delay of the link exceeds the specified threshold, IPsec smart link selection reselects a link for the IPsec tunnel. You can also manually activate a link to establish the IPsec tunnel over that link.

IPsec smart link selection provides the following benefits:

- Avoid the condition that some links are busy and some links are idle when multiple links are deployed at the network egress for load balancing.
- Select proper links for customers when they cannot select links by themselves.
- Avoid forwarding traffic to a failed link between the network egress device and the destination device.

Auto-generate security policy

When you create an IPsec policy, you can select **Auto-generate security policy**. This feature enables the device to automatically generate a security policy that permits IKE negotiation packets.

Restrictions and guidelines

- When you specify the remote host name in an IPsec policy, follow these restrictions and guidelines:
    - If the remote host name is resolved by a DNS server, the local device gets the latest IP address corresponding to the host name by sending a query to the DNS server when the cached DNS entry ages. The DNS entry aging information is obtained from the DNS server.
    - If the remote host name is resolved by a locally configured static DNS entry and the IP address in the entry is changed, you must respecify the remote host name in the IPsec policy to get the new IP address.
- To make sure SAs can be set up and the traffic protected by IPsec can be processed correctly between two IPsec peers, create mirror image ACLs on the IPsec peers. If the ACL rules on IPsec peers do not form mirror images of each other, SAs can be set up only when both of the following requirements are met:
    - The range specified by an ACL rule on one peer is covered by its counterpart ACL rule on the other peer.
    - The peer with the narrower rule initiates SA negotiation.

If a wider ACL rule is used by the SA initiator, the negotiation request might be rejected because the matching traffic is beyond the scope of the responder.

- If you do not configure the local identity in an IPsec policy, the policy uses the global local identity settings configured in the advanced settings.
- Modifications to the following settings in an IPsec policy take effect only on IPsec SAs set up after the modifications:
  - Encapsulation mode.
  - Security protocol.
  - Security algorithms.
  - PFS.
  - IPsec SA lifetimes.
  - IPsec SA idle timeout.

  For the modifications to take effect on existing IPsec SAs, you must reset the IPsec SAs.
- The IPsec peers of an IPsec tunnel must have IPsec policies that use the same security protocols, security algorithms, and encapsulation mode.
- When IKE negotiates IPsec SAs, it uses the IPsec SA lifetime settings configured in the IPsec policy to negotiate the IPsec SA lifetime with the peer. If the IPsec SA lifetime settings are not configured in the IPsec policy, the global IPsec SA lifetime settings are used. IKE uses the local lifetime settings or those proposed by the peer, whichever are smaller.
- If a link used by smart link selection uses the gateway address as the next hop address, you must manually change the link next hop address whenever the gateway address is changed.
- To use quantum encryption, configure the following settings in the **Quantum Encryption** area on the **Advanced Settings** page:
  - Enable quantum encryption.
  - Configure the server address type, server address, and server port.

- Configure the GD-quantum access ID, GD-quantum authentication key, and GD-quantum decryption key.

Contact the administrator of the GD-quantum server to obtain information about the previous quantum key parameters.

ADVPN

This help contains the following topics:

Introduction

Auto Discovery Virtual Private Network (ADVPN) enables enterprise branches that use dynamic public addresses to establish a VPN network. ADVPN uses the VPN Address Management (VAM) protocol to collect, maintain, and distribute dynamic public addresses.

VAM uses the client/server model. All VAM clients (VAMCs) register their public addresses on the VAM server (VAMS). A VAMC obtains the public addresses of other VAMCs from the VAMS to establish ADVPN tunnels.

ADVPN structures

ADVPN uses domains to identify VPNs. VAMCs in a VPN must be assigned to the same ADVPN domain. A VAMC can belong to only one ADVPN domain. A VAMS can serve multiple ADVPN domains and manage their VAMCs.

VAMCs include hubs and spokes.

- **Hub**—A hub is the exchange center of routing information. A hub in a hub-spoke network is also a data forwarding center.
- **Spoke**—A spoke is the gateway of a branch. It does not forward data received from other ADVPN nodes.

ADVPN supports full-mesh, hub-spoke, and hub-group structures.

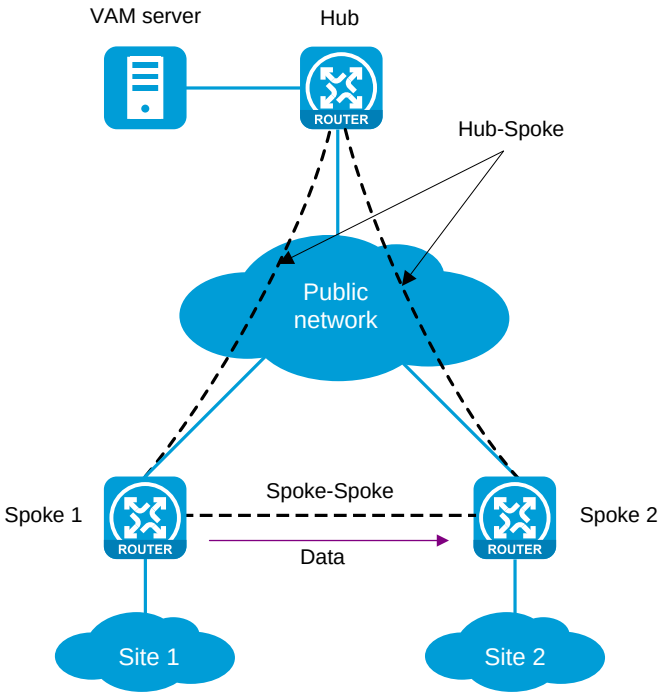
Full-mesh ADVPN

In a full-mesh ADVPN, spokes can directly communicate with each other. The hub acts as the route exchange center.

As shown in Figure 1, the spokes register with the VAMS and obtain hub information in the ADVPN domain. Then, they establish permanent tunnels to the hub.

Any two spokes can establish a dynamic tunnel to directly exchange data. The tunnel is deleted if no data exists during the idle timeout time.

Figure 1 Full-mesh ADVPN

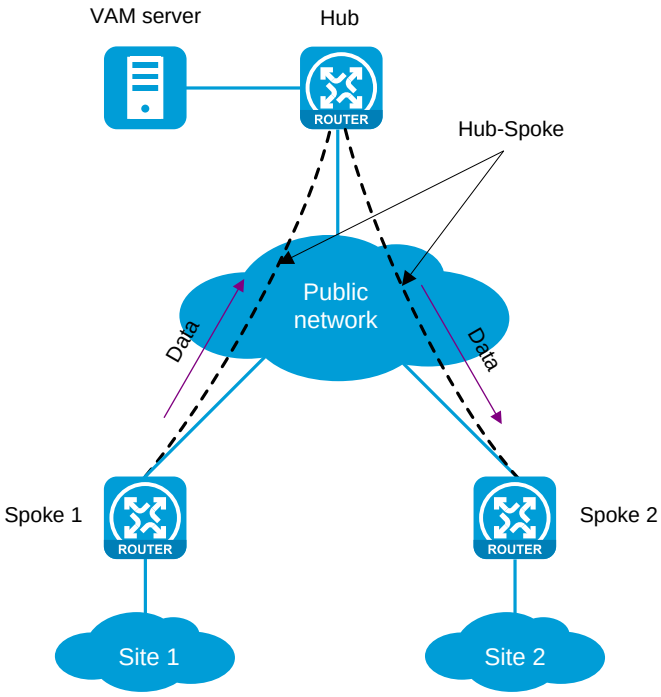


Hub-spoke ADVPN

In a hub-spoke ADVPN, spokes communicate with each other through the hub. The hub acts as both the route exchange center and data forwarding center.

As shown in Figure 2, each spoke establishes a permanent tunnel to the hub. Spokes communicate with each other through the hub.

Figure 2 Hub-spoke ADVPN



Hub-group ADVPN

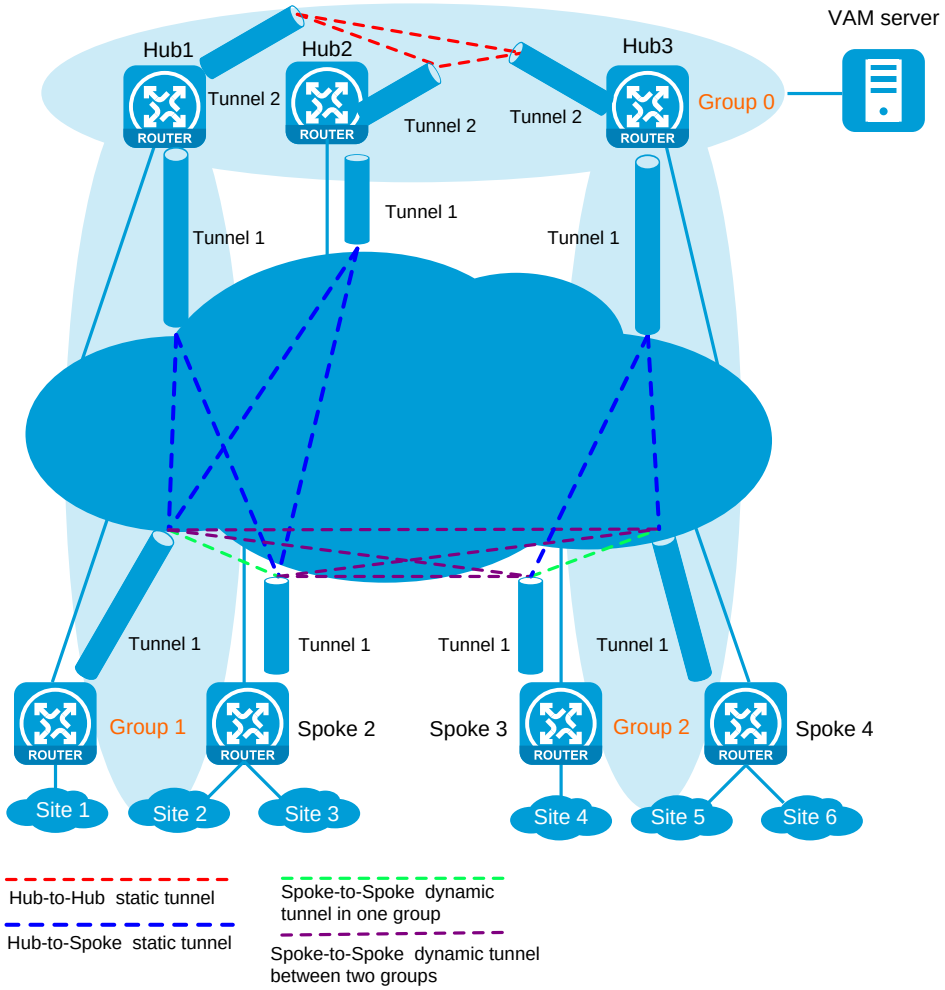
A hub-group ADVPN can accommodate more ADVPN clients. This allows one hub to manage all clients. As shown in Figure 3, a hub-group ADVPN contains multiple hub groups. Each hub group has one or multiple hubs and spokes.

Follow these guidelines to classify hub groups:

- All hubs must belong to the backbone hub group. This hub group forms the full-mesh backbone area. All hubs obtain information about other hubs from the VAMS and establish permanent ADVPN tunnels to each other.
- Spokes must belong to non-backbone hub groups. Each non-backbone hub group includes a minimum of one hub and uses either the full-mesh or hub-spoke structure. Spokes obtain hub information in the ADVPN domain from the VAMS, and establish permanent tunnels to the hub. Spokes can establish tunnels only to the hubs in the hub group.

Tunnel establishment and data forwarding in a hub group depend on the network structure. Inter-group communications between spokes need to pass the hubs of the groups. To reduce the pressure on hubs during inter-group communications, you can allow spokes in different hub groups to establish a dynamic tunnel. The dynamic tunnel is deleted if no data exists during the idle timeout time.

Figure 3 Hub-group ADVPN



ADVPN working mechanisms

The VAMS must have a static public address. VAMCs must have both a public address and a private address. The public address is the address of the interface connected to the public network. It can be manually configured or dynamically assigned. The private address is the address of the ADVPN tunnel interface. It must be manually configured. All the private addresses of VAMCs in an ADVPN domain must belong to the same network segment.

ADVPN includes the following phases:

1. **Connection initialization**—A VAMS and a VAMC perform the following operations to initialize a connection:
    a. The VAMC sends encryption and authentication algorithms to the VAMS in a connection request.
    b. The VAMS compares its algorithms in descending order of priority with the algorithms sent by the VAMC.
    c. The VAMS sends the matching encryption and authentication algorithms to the VAMC.

       If no match is found, the negotiation fails.
    d. The VAMS and the VAMC generate encryption and authentication keys based on the preshared key.

       If authentication and encryption are not needed, they do not generate keys.
    e. The VAMS and the VAMC exchange negotiation acknowledgment packets protected by using the keys.
    f. The VAMS and the VAMC use the keys to protect subsequent packets if they can restore the protected negotiation acknowledgment packets.

       If they cannot restore the packets, the negotiation fails.

2. **Registration**—The VAMC requests to register with the VAMS and the VAMS authenticates the VAMC. The VAMS selects encryption and authentication algorithms for the VAMC based on the information sent by the VAMC. If no match is found, the registration fails.
3. **Tunnel establishment**—In a hub group, each spoke must establish a permanent tunnel to every hub and each hub must establish a permanent tunnel with one another.
4. **Route learning and packet forwarding**—Routes are learned through a routing protocol. The routing protocol determines the network type and the network type determines the packet forwarding method.

ADVPN tunnel NAT traversal

An ADVPN tunnel can traverse a NAT gateway.

- If only the tunnel initiator resides behind a NAT gateway, a spoke-spoke tunnel can be established through the NAT gateway.
- If the tunnel receiver resides behind a NAT gateway, packets must be forwarded by a hub before the receiver originates a tunnel establishment request. If the NAT gateway uses Endpoint-Independent Mapping, a spoke-spoke tunnel can be established through the NAT gateway.
- If both ends reside behind a NAT gateway, no tunnel can be established and packets between them must be forwarded by a hub.

Restrictions and guidelines

General restrictions and guidelines

To ensure network reachability, add ADVPN tunnel interfaces to security zones and configure security policies for the VAMCs to reach one another.

The VAMSs and VAMCs in the same ADVPN domain must have the same preshared key.

All tunnel interfaces in the same ADVPN domain must have the same settings for the keepalive packet sending interval and max retries.

All ADVPN settings are the same on the primary and secondary VAMSs except for the IP address setting.

The ADVPN port configured on a VAMS must be the same as the ADVPN port specified for the VAMS on a VAMC.

To ensure successful registration of a VAMC, make sure the private address of the VAMC is within the private networks of the hub groups on the VAMS.

Restrictions and guidelines: OSPF configuration

To ensure correct communication, make sure the OSPF network type is the same across all VAMSs and VAMCs in the same hub group.

Restrictions and guidelines: GRE key configuration

If a GRE key is configured for one GRE-mode ADVPN tunnel interface on a VAMC, ADVPN tunnel interfaces on the other VAMCs in the same hub group must use the same GRE key.

If multiple GRE-mode ADVPN tunnel interfaces have the same source address or source interface, you must configure different GRE keys for the interfaces.

Configure ADVPN

Before you configure ADVPN, determine the following items:

- ADVPN domain.
- VAMS public address, preshared key, authentication method, encryption algorithms, and authentication algorithms.
- VAMC public address, private address, and private network information.

Configure a VAMS

Support for VAMS Web configuration depends on the device model.

1. Select **Network** > **VPN** > **ADVPN** > **VAMS**.
2. Click **Create**.
3. Configure the items in Table 1 for the VAMS and enable the VAMS.

   You can also enable, disable, or modify an existing VAMS.

Table 1 VAMS configuration items

Item	Description
ADVPN domain	Enter an ADVPN domain for the VAMS. The domain name must be unique.
ADVPN domain ID	Enter an ADVPN domain ID for the VAMS. The domain ID must be unique.
Preshared key	Enter a preshared key. The VAMS uses the preshared key to generate initial encryption and authentication keys during connection initialization with a VAMC. The key is also used to generate encryption and authentication keys for subsequent packets if encryption and authentication are needed.
Authentication method	Select an authentication method for the VAMS to authenticate VAMCs.
ISP domain	Select an ISP domain in which VAMCs are authenticated. For more information, see ISP Domain Online Help. This item is available only when the authentication method is PAP or CHAP.
Hub group	Hub group list. The list also provides interfaces for creating, editing, and deleting hub groups. For more information about configuring hub groups, see Table 2.
Authentication algorithms	Select authentication algorithms used by the VAMS to communicate with VAMCs. An authentication algorithm specified earlier has a higher priority during algorithm negotiation between the VAMS and a VAMC. The VAMS compares its algorithms in descending order of priority with the algorithms sent by the VAMC. If a match is found, the VAMS sends the matching algorithm to the VAMC. If no match is found, the negotiation fails. If you select **None** (no authentication), make sure **None** is placed following all the other algorithms. The algorithms following **None** do not take effect.

Item	Description
Encryption algorithms	Select encryption algorithms used by the VAMS to communicate with VAMCs. The priority and selection mechanisms are the same as those of authentication algorithms.
Keepalive packets: Sending interval	Set the interval at which a VAMC sends keepalive packets to the VAMS. A change to this item does not affect registered VAMCs. The change takes effect only on subsequently registered VAMCs.
Keepalive packets: Max retries	Set the maximum number of attempts that a VAMC resends a keepalive packet to the VAMS. A change to this item does not affect registered VAMCs. The change takes effect only on subsequently registered VAMCs.
VAM packet retry interval	Set the interval at which the VAMS resends a VAM packet.
Enable VAMS	Select this item to enable the VAMS.

Table 2 Hub group configuration items

Item	Description
Group name	Enter a hub group name.
Shortcut rule	Select a rule to control establishing spoke-spoke direct tunnels: • **None**—Spokes are not allowed to establish direct tunnels. • **ACL**—Specifies an ACL to control establishing spoke-spoke direct tunnels. • **All**—No restrictions for establishing spoke-spoke direct tunnels.
Hub	Hub list. The hub list also provides interfaces for creating, editing, and deleting hubs. The **Public address** and **ADVPN port** fields are required for a

Item	Description
	hub if the hub is behind a NAT gateway. The values are the public address and port number translated by NAT.
Spoke	Spoke list. The spoke list also provides interfaces for creating and deleting spokes.

Configure a VAMC

1. Select **Network** > **VPN** > **ADVPN** > **VAMC**.
2. Click **Create**.
3. Configure the items in Table 3 for the VAMC and enable the VAMC.

   You can also enable, disable, or modify an existing VAMC.

Table 3 VAMC configuration items

Item	Description
VAMC name	Enter a VAMC name. The name must be unique in an ADVPN domain.
ADVPN domain	Enter an ADVPN domain name for the VAMC.
Preshared key	Enter a preshared key. The VAMC uses the preshared key to generate initial encryption and authentication keys during connection initialization with a VAMS. The key is also used to generate encryption and authentication keys for subsequent packets if encryption and authentication are needed.
Username	Enter the username and password that the VAMC uses to register

Item	Description
Password	with a VAMS.
Enable VAMC	Select this item to enable the VAMC.
Dumb time	Set the dumb time of the VAMC. The VAMC starts the dumb timer after its connection to a VAMS times out (keepalive times out), and it does not process any packets during the dumb time. When the dumb timer expires, the VAMC sends a new connection request to the VAMS.
VAM packet retry interval	Set the interval at which the VAMC resends a request to a VAMS. After the VAMC sends a request to the VAMS, it resends the request if it does not receive any responses within the retry interval.
VAM packet max retries	Set the maximum number of attempts that the VAMC resends a request to a VAMS.
Primary server address Secondary server address	Select a method to specify the public address of the primary or secondary VAMS. You can enter an IP address or a domain name. The public address is a static IP address.
Primary server port Secondary server port	Enter a port number. The VAMC uses the port to listen to the primary or secondary VAMS.
Tunnel mode	Select an encapsulation mode for ADVPN tunnels.
Tunnel interface ID	Enter an ADVPN tunnel interface ID.
Tunnel private address	Enter the private address of the ADVPN tunnel interface and the network mask.
Tunnel public address	Select a method to specify the tunnel public address. You can enter an IP address or select a source interface. The primary IP address of the selected interface is used.
VRF	Select a VRF for the VAMC.

Item	Description
	The routing table of the VRF is used to forward traffic through the ADVPN tunnel. For more information, see VRF Online Help.
OSPF settings	Select an OSPF instance for the ADVPN tunnel. For more information, see OSPF Online Help.
Network type	Select an OSPF network type, which affects the ADVPN structure. This item is available only after an OSPF instance is selected.
DR priority	Configure the OSPF DR priority of the VAMC. This item is available only after an OSPF instance is selected.
GRE key	Configure the GRE key used in GRE mode. If GRE key is not required, do not configure this item. For more information, see GRE Online Help.
Enable GRE checksum	Select this item to enable GRE checksum to ensure packet integrity in GRE mode. For more information, see GRE Online Help.
Source UDP port	Set the source port number of packets in UDP mode. If you select **ADVPN V0 version compatible**, the source UDP port of this tunnel cannot be the same as the source UDP port of any other ADVPN tunnel.
Register private address list	ADVPN tunnel private network information that the VAMC registers with the VAMS. The VAMC requests the VAMS to resolve the destination address of a packet if the packet is destined for a remote private network. The VAMS sends the node information of the remote VAMC to the current VAMC after it finds that the resolved address is within the register private addresses of that remote VAMC. The list displays existing private networks. It also provides interfaces for creating, editing, and deleting private networks. As a best practice, assign the **Preference** field a value that is higher than other dynamic routing protocols and lower than the static routing. A higher value indicates a lower preference.
ADVPN V0 version compatible	Configure whether the VAMC is compatible with the ADVPN V0 version.

Item	Description
Tunnel dumb time	Set the quiet time. The quiet timer starts after an ADVPN tunnel establishment failure.
Idle timeout time	Set the idle timeout time of the spoke-spoke tunnel. If no data is forwarded along a spoke-spoke tunnel during the idle timeout time, the tunnel will be removed automatically.
ToS of tunneled packets	Set the ToS of ADVPN tunneled packets.
TTL of tunneled packets	Set the TTL of ADVPN tunneled packets.
Set DF bit	Select this item to set the DF bit for tunneled packets.
Enable IPsec	Select this item to enable IPsec.
IPsec profile name	Enter an IPsec profile name.
IKE settings	Configure IKE settings.
AuthN method	Select an IKE authentication method: • Preshared key. • Signature.
Preshared key	Enter a preshared key for the **Preshared key** authentication method.
PKI domain	Select a PKI domain for the certificate in the **Signature** authentication method. For more information, see PKI Online Help.
Cert access policy	Select a certificate access policy for the **Signature** authentication method. For more information, see PKI Online Help.
IKE proposal	Select an IKE proposal used by the IPsec profile. For more information, see IPsec Online Help.
Negotiation mode	Select an IKE negotiation mode.

Item	Description
IPsec configuration	Configure IPsec settings.
Encapsulation mode	Select an IPsec encapsulation mode.
Security protocol	Select an IPsec security protocol.
ESP authentication	Select an ESP authentication algorithm for the ESP or AH-ESP security protocol.
ESP encryption	Select an ESP encryption algorithm for the ESP or AH-ESP security protocol.
AH authentication	Select an AH authentication algorithm for the AH or AH-ESP security protocol.
PFS	Select a group for PFS. The PFS feature is a security feature based on the DH algorithm. After PFS is enabled, an additional DH exchange is performed in IKE phase 2 to make sure IPsec keys have no derivative relations with IKE keys and a broken key brings no threats to other keys.
DPD check	Select this item to enable IKE DPD check.
Check method	Select an IKE DPD check method.
Detect interval	Set the IKE DPD detect interval: • **On demand**—The device performs a DPD detection if it does not receive an IPsec packet from the peer within the specified period. • **Periodic**—The device performs a DPD detection at the specified interval regardless of whether it has received an IPsec packet from the peer.
Retry interval	Set the interval at which the local end resends an IKE PDP packet. If the local end does not receive a response from the peer within the retry interval, it resends the DPD request. If the local end has made two retries without receiving any response from the peer, it deletes the IKE key and the IPsec key corresponding to the IKE key.

L2TP

This help contains the following topics:

- Introduction
  - Typical L2TP network components
  - L2TP tunneling modes
- Troubleshooting L2TP
  - Tunnel setup failure
  - Data transmission failure

Introduction

The Layer 2 Tunneling Protocol (L2TP) is a Virtual Private Dialup Network (VPDN) tunneling protocol. L2TP sets up point-to-point tunnels across a public network (for example, the Internet) and transmits encapsulated PPP frames (L2TP packets) over the tunnels. With L2TP, remote users can access the private networks through L2TP tunnels after connecting to a public network by using PPP.

Typical L2TP network components

A typical L2TP network has the following components:

- Remote system—A remote system is usually a remote user's host or a remote branch's device that needs to access the private network.

- LAC—An L2TP access concentrator (LAC) is both PPP and L2TP capable. It is usually a network access server (NAS) located at a local ISP, which provides access services mainly for PPP users.

  An LAC is an endpoint of an L2TP tunnel and lies between an LNS and a remote system. It encapsulates packets received from a remote system by using L2TP and then sends the encapsulated packets to the LNS. It decapsulates packets received from the LNS and then sends the decapsulated packets to the intended remote system.

- LNS—An L2TP network server (LNS) is both PPP and L2TP capable. It is usually an edge device on an enterprise network.

  An LNS is the other endpoint of an L2TP tunnel. It is the logical termination point of a PPP session tunneled by the LAC. L2TP extends the termination point of a PPP session from a NAS to an LNS by establishing a tunnel.

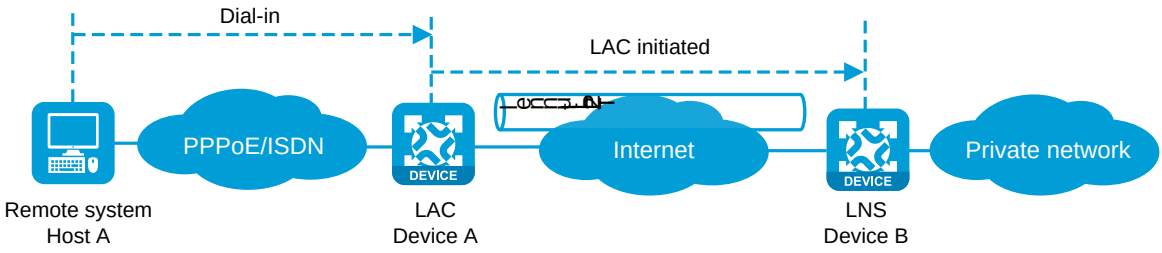
L2TP tunneling modes

L2TP tunneling modes include NAS-initiated, client-initiated, and LAC-auto-initiated.

NAS-initiated tunneling mode

As shown in Figure 1, a remote system dials in to the LAC through a PPPoE/ISDN network. The LAC initiates a tunneling request to the LNS over the Internet.

Figure 1 NAS-initiated tunneling mode



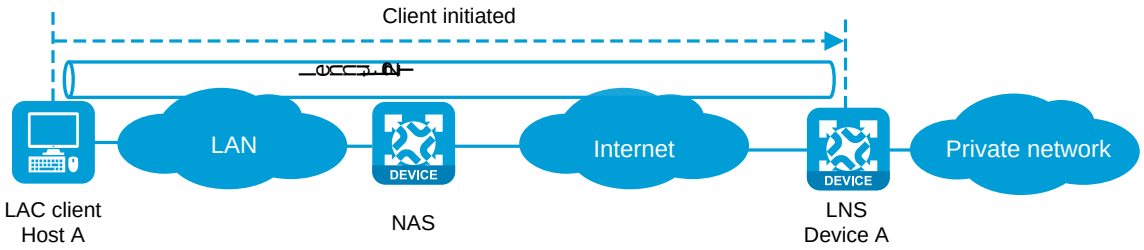
A NAS-initiated tunnel has the following characteristics:

- The remote system only needs to support PPP, and it does not need to support L2TP.
- Authentication and accounting of the remote system can be implemented on the LAC or LNS.

Client-initiated tunneling mode

As shown in Figure 2, a remote system running L2TP (LAC client) has a public IP address to communicate with the LNS through the Internet. The LAC client can directly initiate a tunneling request to the LNS without any dedicated LAC devices.

Figure 2 Client-initiated tunneling mode



A client-initiated tunnel has the following characteristics:

- A client-initiated tunnel has higher security because it is established between a remote system and the LNS.

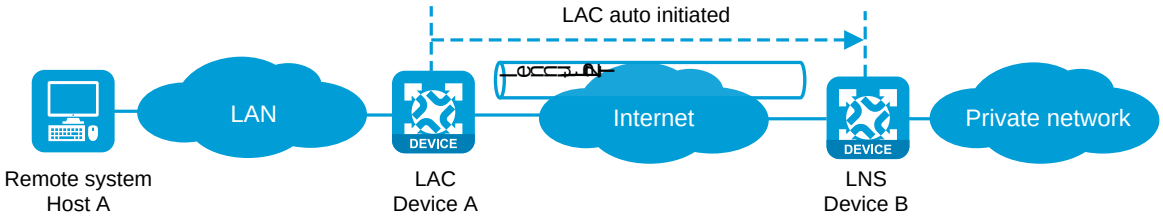
- The remote system must support L2TP and be able to communicate with the LNS. This causes poor expandability.

LAC-auto-initiated tunneling mode

In NAS-initiated mode, a remote system must successfully dial in to the LAC through PPPoE or ISDN.

In LAC-auto-initiated mode, you can configure tunnel settings on the LAC to trigger the LAC to initiate a tunneling request to the LNS. When a remote system accesses the private network, the LAC forwards data through the L2TP tunnel.

Figure 3 LAC-auto-initiated tunneling mode



An LAC-auto-initiated tunnel has the following characteristics:

- The connection between a remote system and the LAC is not confined to a dial-up connection and can be any IP-based connection.
- You do not need to trigger L2TP tunnel establishment by dialup on the remote system.
- An L2TP session is established immediately after an L2TP tunnel is established. Then, the LAC and LNS, acting as the PPPoE client and PPPoE server, respectively, perform PPP negotiation.
- An L2TP tunnel can carry only one L2TP session.
- The LNS assigns a private IP address to the LAC instead of to the remote system.

Troubleshooting L2TP

Tunnel setup failure

Symptom

After you select VPN > L2TP > TunnelInfo, no tunnel information is displayed. Tunnel establishment fails.

Solution

To resolve the problem, verify the following items to avoid tunnel setup failures:

- The address of the LNS is configured correctly on the LAC.
- The same PPP authentication mode is configured for the LAC and the LNS.
- Usernames and passwords are correctly configured on the LAC and the LNS.
- If the L2TP group number is not 1 on the LNS, the same tunnel name is configured for the LAC and the LNS.
- Tunnel authentication succeeds.

  You can enable tunnel authentication on both sides or either side. To ensure a successful tunnel establishment when tunnel authentication is enabled on both sides or either side, set the same non-null key on the LAC and the LNS.

Data transmission failure

Symptom

After you select VPN > L2TP > TunnelInfo, the page shows that tunnels are successfully established. However, data transmission fails. For example, the LAC and LNS cannot ping each other.

Solution

To resolve the problem:

1. Verify that the LAC has a route to the private network behind the LNS, and vice versa. If no route is available, configure a static route or a dynamic routing protocol.
2. Add the Virtual-Template interface on the LNS to a security zone, and permit the traffic from the security zone to security zone Local.
3. Increase the link bandwidth to enhance the link availability.

   Internet backbone congestion and high packet loss ratio might cause data transmission failures. L2TP data transmission is based on UDP, which does not provide the packet error control feature. If the line is unstable, the LAC and LNS might be unable to ping each other.

SSL VPN

This help contains the following topics:

- Configure a shortcut list
- Configure a resource group

- FAQ

Introduction

SSL VPN provides SSL-based secure remote access services through an SSL VPN gateway. Users from anywhere on the Internet can establish a secure connection to an SSL VPN gateway through an SSL-enabled browser to access protected resources behind the gateway.

SSL VPN operating mechanism

To allow remote user access to protected resources behind an SSL VPN gateway, you must configure these resources on the gateway. Remote users can access only the resources authorized to them after they establish an SSL-encrypted connection to the gateway and pass the identity authentication.

SSL VPN operates as follows:

1. The remote user establishes an HTTPS connection to the SSL VPN gateway.

   In this process, the remote user and the SSL VPN gateway perform SSL certificate authentication.

2. The remote user enters the username and password.
3. The SSL VPN gateway authenticates the credentials that the user entered, and authorizes the user to access a range of resources.
4. The user selects a resource to access.

An access request for that resource is sent to the SSL VPN gateway through the SSL connection.

5. The SSL VPN gateway resolves the request and forwards the request to the corresponding internal server.
6. The SSL VPN gateway forwards the server's reply to the user through the SSL connection.

SSL VPN networking modes

SSL VPN supports the following networking modes:

- **Gateway mode**—In gateway mode, the SSL VPN gateway acts as a gateway that connects remote users and the internal servers network. Because the SSL VPN gateway is deployed in line, it can provide full protection to the internal network but it affects data transmission performance.
- **Single-arm mode**—In single-arm mode, the SSL VPN gateway is attached to the network gateway. The gateway forwards user-to-server traffic to the SSL VPN gateway. The SSL VPN gateway processes the traffic and sends the processed traffic back to the gateway. The gateway forwards the traffic to the internal servers. The SSL VPN gateway is not a performance bottleneck in the network because it is not deployed on the key path. However, the SSL VPN gateway cannot provide full protection to the internal network.

SSL VPN access modes

Web access

In Web access mode, remote users use browsers to access Web resources allowed by an SSL VPN gateway through HTTPS. After login, a user can access any resources listed on the webpage. In Web access mode, all operations are performed on webpages.

The resources available for SSL VPN Web access users are Web servers only.

TCP access

In TCP access mode, users access TCP applications on internal servers by accessing the applications' open ports. Supported applications include remote access services (such as Telnet), desktop sharing services, mail services, Notes services, and other TCP services that use fixed ports.

In TCP access mode, a user installs the TCP access client software on the SSL VPN client (the terminal device that the user uses). The client software uses an SSL connection to transmit the application layer data.

IP access

IP access implements secured IP communications between remote users and internal servers.

To access an internal server in IP access mode, a user must install dedicated IP access client software. The client software will install a virtual network interface card (VNIC) on the SSL VPN client.

BYOD access

BYOD access enables secured access to internal resources through mobile clients.

For mobile clients to access internal resources in BYOD access mode:

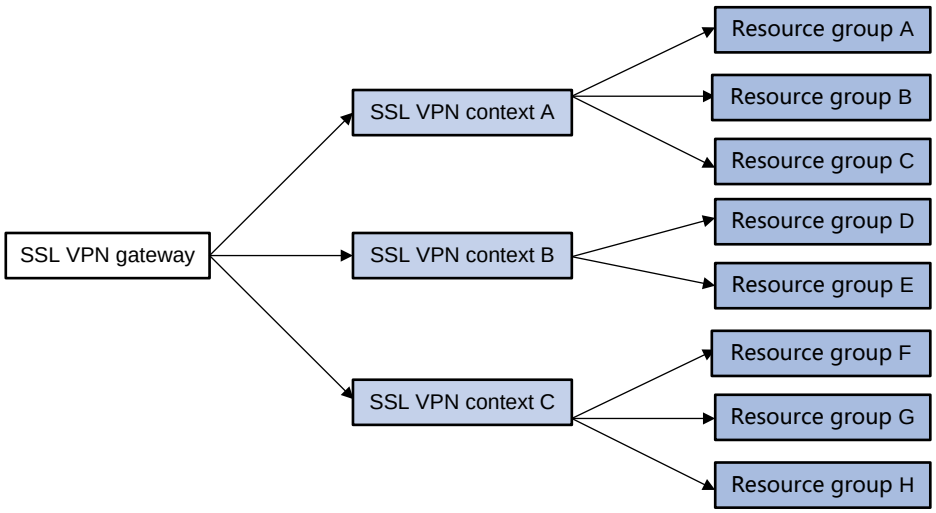
- On the SSL VPN gateway, you must specify an Endpoint Mobile Office (EMO) server for mobile clients. Mobile clients access internal resources through the EMO server.
- On the mobile client, the user must install SSL VPN client software dedicated for mobile clients.

Resource access control

SSL VPN controls user access to resources on a per-user basis.

As shown in Figure 1, an SSL VPN gateway can be associated with multiple SSL VPN contexts. An SSL VPN context contains multiple resource groups. A resource group defines accessible Web resources, TCP resources, and IP resources.

Figure 1 SSL VPN resource access control



An SSL VPN user can access an SSL VPN gateway by using the following methods:

- **Direct access**—If the SSL VPN gateway is associated with only one SSL VPN context, the user can access the SSL VPN context directly by entering the IP address and port number of the SSL VPN gateway.
- **By domain list**—The SSL VPN gateway can be associated with multiple SSL VPN contexts through different domain names. The user will be prompted to select a domain name from the domain list displayed on the SSL VPN gateway login page. The SSL VPN gateway determines the SSL VPN context to which the user belongs based on the selected domain name.
- **By virtual host name**—The SSL VPN gateway can be associated with multiple SSL VPN contexts through different virtual host names. The SSL VPN gateway determines the SSL VPN context to which the user belongs based on the virtual host name entered on the SSL VPN gateway login page.

After determining the SSL VPN context for a user, the SSL VPN gateway uses the authentication and authorization methods of the ISP domain specified for the context to perform authentication and authorization for the user.

- If the SSL VPN gateway authorizes the user to use a resource group, the user can access resources allowed by the resource group.
- If the SSL VPN gateway does not authorize the user to use a resource group, the user can access resources allowed by the default resource group.

The SSL VPN gateway uses AAA to perform user authentication and authorization. SSL VPN supports AAA protocols RADIUS and LDAP. RADIUS is most often used.

Restrictions and guidelines

Disabling an SSL VPN AC interface might interrupt the ongoing IP access service. Please perform this operation with caution.

Restrictions and guidelines: SSL VPN gateway configuration

If the SSL server policy used by an SSL VPN gateway is changed, or the policy settings are changed, you must re-enable the gateway to make the configuration take effect.

Restrictions and guidelines: TCP access configuration

- When configuring the client address for a port forwarding item on the SSL VPN gateway, use an address in network segment 127.0.0.0/8, or use the host name or domain name.
- For a user to access TCP resources through a host, modifications to the **hosts** file on the host might be required. Make sure the user has the administrator privileges on the host.
- The host used for TCP access must have the Java Runtime Environment installed.

Restrictions and guidelines: IP access configuration

When you configure the IP access address pool for IP access clients, follow these restrictions and guidelines:

- The IP access address pool and the IP address of the NIC used on an IP access client host must belong to different network segments.

- To avoid address conflicts, make sure the IP access pool does not contain the IP addresses of interfaces on the SSL VPN gateway device.
- Make sure the IP access address pool and the IP addresses of internal servers hosting accessible IP resources belong to different network segments.

When you bind IP addresses to an SSL VPN user, follow these restrictions and guidelines:

- If an IP access address pool is specified for the SSL VPN resource group authorized to the user, the IP addresses must exist in the address pool.
- If no address pool is specified for the SSL VPN resource group, the IP addresses must exist in the address pool specified for the SSL VPN context of the user.
- You can bind the same IP address to different SSL VPN users only when the SSL VPN contexts of the users are associated with different VPN instances.

Restrictions and guidelines: Domain name configuration

Make sure you specify valid domain names for SSL VPN configuration items such as Web resource URLs or port forwarding entries.

SSL VPN does not check the existence or validity of the specified domain names.

Restrictions and guidelines: Webpage template configuration

- The template files uploaded must be .zip files.
- An uploaded template .zip file must contain both home.html and login html files in the root directory of the .zip file.

Restrictions and guidelines: LDAP authentication configuration

If you configure LDAP authentication for SSL VPN users, you must also configure LDAP authorization. Configure LDAP authorization settings from the CLI on the device.

Restrictions and guidelines: SSO login configuration

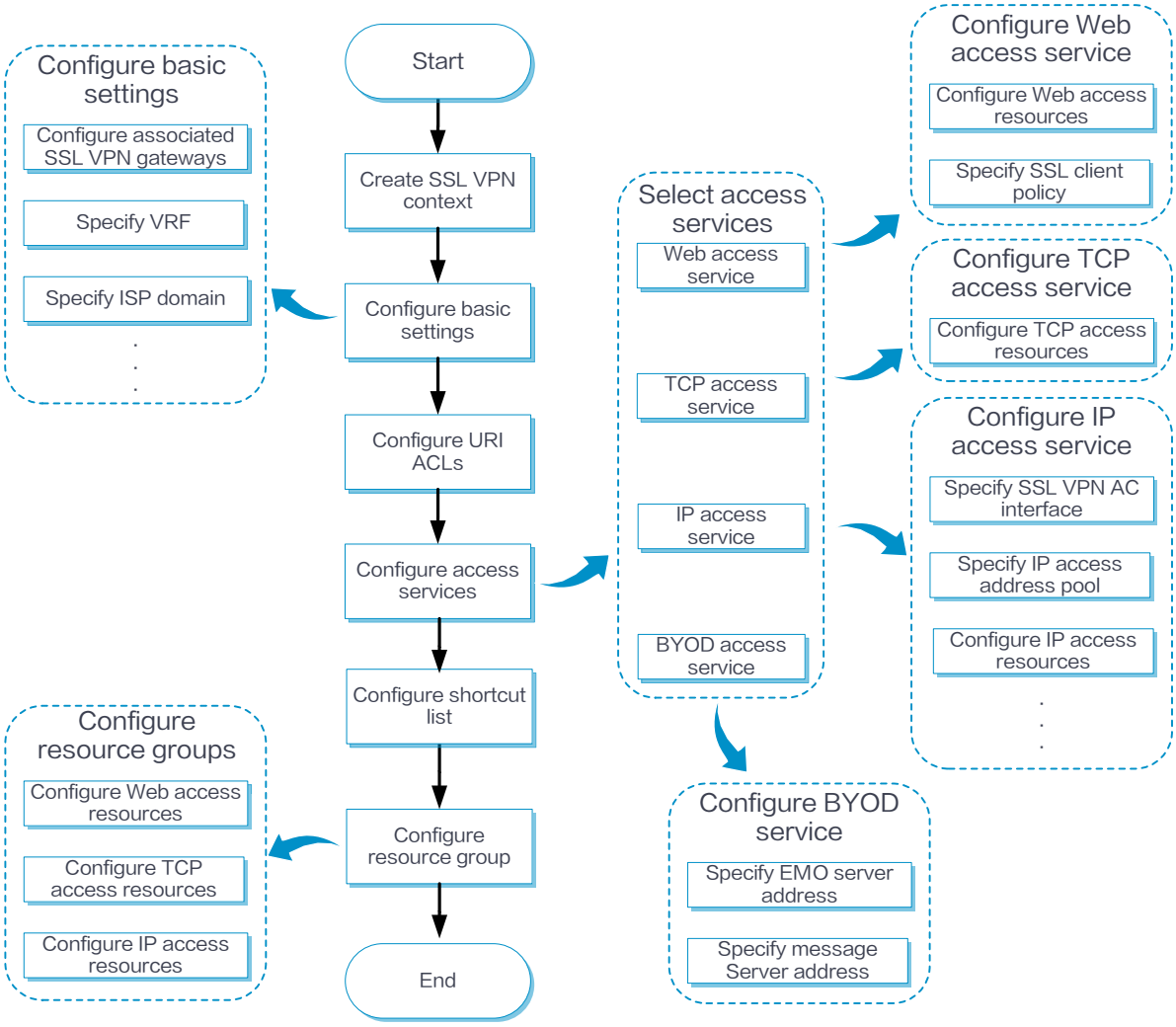
For the auto-build SSO method, the following requirements must be met:

- If a user group name is specified as the SSO login parameter, only remote users are supported.
- SSO login is available only for accessing resources by clicking the URL links on the SSL VPN Web interface. SSO does not work if you access the resources by entering the URLs in a browser address bar or a URL input box.
- SSO login is not available for Web resources that require graphic verification codes.
- SSO login is not available for Web resources that require two-factor authentication or script invocation.

Configure SSL VPN

Configure an SSL VPN context as shown in Figure 2.

Figure 2 SSL VPN configuration procedure



In addition to the preceding configuration procedure, you can also perform the following tasks in SSL VPN:

- Create and edit SSL VPN gateways on the **Network** > **SSL VPN** > **SSL VPN Gateways** page.
- Create and edit IP access address pools on the **Network** > **SSL VPN** > **IP Access Address Pools** page.
- Create and edit SSL VPN AC interfaces on the **Network** > **SSL VPN** > **SSL VPN AC Interfaces** page.

- Edit the webpage template, title, login welcome message, hide-password-box setting, and logo for the SSL VPN Webpage on the **Webpage settings** tab of the **Edit SSL VPN Context** page.
- Edit the following settings on the **Webpage settings** tab of the **Edit SSL VPN Context** page:
    - Chinese and English notices on the SSL VPN gateway login page and resource page.
    - Chinese and English webpage files.
    - Chinese and English password complexity descriptions.
    - Server reply messages rewriting.
- Upload the custom IP access client file on the **Network** > **SSL VPN** > **Global Settings** page. Users can download the client and use it to log in to the SSL VPN gateway. On this page, you can also select a webpage template as the global SSL VPN webpage template.
- Add user-defined SSL VPN webpage templates:

    a. Navigate to the **Network** > **SSL VPN** > **TempManagement** page, and then click **Create**.

    b. On the opened page, upload a user-defined webpage template.

    You can use the uploaded templates on the **Network** > **SSL VPN** > **Global Settings** or **Edit SSL VPN Context** page.
- View the online user information and IP access statistics on the **Network** > **SSL VPN** > **Statistics** page.
- For SSO login, you can export and import the user custom configuration on the **Network** > **SSL VPN** > **Global Settings** page:
    - Click **Export user custom configuration** to export the custom username and password for the current user to perform SSO login.
    - Click **Import user custom configuration** to import the custom username and password for the current user to perform SSO login.

Configure basic settings in an SSL VPN context

Configure the basic settings, including the associated SSL VPN gateways, VRF (VPN instance) to which the SSL VPN context belongs, and the enabling status of the SSL VPN context.

Procedure

1. Click the **Network** tab.
2. In the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

   The **SSL VPN Contexts** page opens.
3. Click **Create**.

   The **Create SSL VPN Context** page opens.
4. On the **Basic settings** tab, configure the basic settings for the SSL VPN context, and then click **Next**.

Table 1 Basic configuration items for an SSL VPN context

Item	Description
Context name	Enter an SSL VPN context name.
Associated gateways	Configure the gateways associated with the SSL VPN context. To add an associated gateway for the SSL VPN context: 1. Click **Create** in the **Associated gateways** field. 2. In the dialog box that opens, select a gateway from the **GateWay** list. If no gateways are available, click **SSL VPN Gateway** to create a gateway. 3. Select an access method. Options include **Exclusive**, **Domain name**, and **Virtual host name**. You must specify a domain name or virtual host name if the SSL VPN gateway is or will be also associated with other SSL VPN contexts. For the context to use the

Item	Description
	gateway exclusively, select the **Exclusive** access method.
VRF	Select the VPN instance to which the SSL VPN context belongs.
Max sessions	Specify the maximum number of SSL VPN sessions for the SSL VPN context. If the limit is reached, new users cannot access the SSL VPN gateway.
Login control	Specify the maximum number of concurrent logins per account. A user cannot log in if the number of logins using the same account reaches the limit. You can enable force logout so when a login is attempted but logins using the account reach the maximum, the user with the longest idle time will be logged out to allow the new login.
Max connt per session	Select whether to enable or disable limiting the number of connections in a session. If the number of connections in a session has reached the limit, new connection requests for the session will be rejected with a 503 Service Unavailable message.
Session idle timeout	Specify the maximum idle time of an SSL VPN session. If the idle time of an SSL VPN session exceeds the specified idle timeout time, the session is terminated.
Idle-cut traffic threshold	Specify the idle-cut traffic threshold in kilobytes. An SSL VPN session will be disconnected if the session traffic observed within the session idle timeout time is below the idle-cut traffic threshold.
Rate limit per session	When the packet transmission rate in a direction of the SSL VPN session exceeds the specified limit, subsequent packets in that direction will be dropped. Uplink traffic refers to the traffic sent from users to the server. Downlink traffic refers to the traffic sent from the server to users.
User login logging	Select this item to enable logging for user login and logout events.
Resource access logging	Select this item to enable logging for resource access. After you enable resource access logging, you can select a logging method. Options include **Log filtering** and **Summary log**. If log filtering is enabled, the device generates only one log for accesses of the same user to the same resource in a minute. When log filtering is disabled, the

Item	Description
	device generates a log for each resource access.
Online password change	Select this item to enable password modification. An SSL VPN user is able to modify the password only when this feature is enabled in both SSL VPN user view and SSL VPN context view.
Enable SSL VPN context	Select this item to enable the SSL VPN context.
Global URL Masking	Select this item to enable URL masking for all Web resources in the SSL VPN context.

Configure authentication settings

The authentication mode for users to log in to an SSL VPN context includes password authentication, certificate authentication, and IMC SMS verification.

Procedure

On the **AuthN Config** tab, configure the authentication settings.

Table 2 Authentication configuration items for an SSL VPN context

Item	Description
ISP domain	Select the ISP domain used for authentication, authorization, and accounting.
Code verification	Select this item to enable code verification. After code verification is enabled, a user must enter a correct verification code to log in to the SSL VPN Web interface.

Item	Description
Certificate auth	Select this item to enable certificate authentication. To use certificate authentication, make sure client authentication is enabled in the SSL server policy. The SSL VPN gateway uses the digital certificate sent by an SSL VPN client to authenticate the client.
Username attribute	Select the certificate attribute to be used as the SSL VPN username. By default, the CN attribute in the Subject field of a certificate is used as the username.
Enable password	Select this item to enable password authentication. After password authentication is enabled, a user can use the username and password to log in to the SSL VPN Web interface.
Certificate and pwdN	Select the authentication mode for users if both certificate and password authentication methods are enabled. To require users to pass both certificate and password authentications, select **Use all methods**. To require users to pass either certificate or password authentication, select **Use any method**.
IMC user pwd modify	Select this item to enable password modification for IMC authentication users. You must specify the IMC server's IP address and port number, and the VRF instance to which the IMC server belongs. For this feature to take effect, make sure the online password change feature is enabled.
IMC SMS verification	Select this item to enable IMC SMS verification. To use this feature, make sure SMS message verification has been configured on the IMC server. After SMS message verification is enabled, an SSL VPN client can dynamically obtain a verification code from the IMC server for SSL VPN gateway login authentication.
Enable WeChat Work authN	Select this item to enable WeChat Work authentication. To use this feature, make sure the following tasks have been completed: • Configuring the company Apps on the WeChat Work management platform. • Configuring the App homepage redirect link and the trusted domain name of the SSL VPN gateway for each App on the WeChat Work management platform. • Completing the domain name ownership verification: download the domain name ownership verification file from the WeChat Work

Item	Description
	management platform, and then upload the file on the **Network** > **SSL VPN** > **Global Settings** page. After the WeChat Work authentication is enabled, the device obtains user information from the third party of WeChat Work and uses the user information for authentication and authorization.
API server address	Enter a WeChat Work API server address. With this address configured, the device interacts with the WeChat Work API server to obtain user information on receiving a message redirected from the WeChat Work server. Then, the device uses the obtained information for user authentication and authorization.
Corp ID	Enter the company ID, which uniquely identifies a company on the WeChat Work.
App secret	Enter an App secret key. Each App has an independent access key. For data security, make sure the App secret key is not leaked.
AuthN request timeout	Enter the timeout time of the authentication request sent from the SSL VPN gateway to the API server. A WeChat Work authentication fails if the SSL VPN gateway does not receive the response from the API server within the timeout time after sending an HTTP request.
User ID field name	Enter a user ID field name. The SSL VPN gateway uses this item to construct the parameter that carries user information in the access requests sent to the internal server.
AuthZ policy group field name	Enter an authorization policy group name. The SSL VPN gateway uses this item to obtain the authorization policy group name from the response of the WeChat Work API server.
WeChat open platform URL	Select a method to configure a WeChat open platform URL. Options include: • **Predefined**—The URL is **https://open.weixin.qq.com** by default, which cannot be edited. • **User-defined**—You can enter a URL as needed. After this item is configured, the client can access the WeChat open platform directly to complete the authentication when the internal server requires client authentication again.

Configure URI ACLs

You can create multiple URI ACLs in an SSL VPN context.

A URI ACL is a set of rules that permit or deny access to resources. You can add multiple rules to a URI ACL. The device matches a packet against the rules in ascending order of the rule ID. The match process stops once a matching rule is found.

A URL ACL can be used for the following purposes:

- Filter resources under the URL specified in a URL item.
- Filter Web, TCP, and IP access requests in an SSL VPN resource group.

Procedure

1. On the **URI ACL** tab, click **Create**.
2. On the **Add URI ACL** page that opens, enter an ACL name.
3. In the **URI ACL Resources** section, click **Create**.
4. On the **Add URI ACL Rule** page that opens, create a URI ACL rule.

Table 3 Configuration items for a rule

Item	Description
Rule ID	Enter a rule ID.
Action	Select the action for the matching packets. Options include **Permit** and **Deny**.

Item	Description
URI pattern	Enter a URI pattern in the format of *protocol*://*host*:*port*/*path*, where protocol and host are required.

5. Click **OK**.

   The rule is displayed on the **Add URI ACL** page.

6. Click **OK**.

   The URI ACL is displayed on the **URI ACL** page.

7. Click **Next**.

Configure access services

You can configure access resources for the following access services: Web access service, TCP access service, and IP access service.

Configure the Web access service

On the Web access service configuration page, perform the following tasks:

1. Select the SSL client policy used by the SSL VPN gateway to access internal HTTPS servers.

   By default, the SSL VPN gateway uses the default SSL client policy to access internal HTTPS servers. The default SSL client policy uses cipher suite **rsa_rc4_128_md5**.

2. Create a URL item for an internal Web resource:

   a. Create a URL item.

   b. Specify the URL of the Web resource for the URL item.

c. Select an existing URI ACL to filter the Web resources under the specified URL.

d. Select a mapping type for the resource URL. Options are **Normal mapping** (the default), **Domain mapping**, and **Port mapping**.

The SSL VPN gateway rewrites the resource URL before sending it to the client. The URL mapping type determines how the gateway rewrites the URL.

The following example describes how URL mapping works when the user accesses internal resource URL **http://www.server.com:8080** behind SSL VPN gateway with name **gw**, domain name **https://www.gateway.com:4430**, and IP address **1.1.1.1**.

- **Normal mapping**—The resource URL returned to the client will be rewritten to **https://www.gateway.com:4430/_proxy2/http/8080/www.server.com**. Normal mapping may cause problems such as missed URL rewriting and rewriting errors, resulting in SSL VPN clients not being able to access the internal resources. Use domain mapping or URL mapping as a best practice.
- **Domain mapping**—The **Domain name** item is displayed after **Domain mapping** is selected. The resource URL returned to the client will be rewritten to **https://*mapped domain name*:4430**, where ***mapped domain name*** is the domain name you entered for the **Domain name** item.
- **Port mapping**—The **Gateway name** and **Virtual host** items are displayed after **Port mapping** is selected. The virtual host name is optional.
  - If you enter **gw2** for the **Gateway name** item and do not enter the virtual host name, the resource URL will be rewritten to **https://2.2.2.2:4430**, where 2.2.2.2 and 4430 are the IP address and port number of SSL VPN gateway **gw2**.
  - If you enter **gw** for the **Gateway name** item and **vhosta** for the **Virtual host** item, the resource URL will be rewritten to **https://vhosta:4430**.

3. Create a URL list and assign URL items to the URL list.

The URL lists can be assigned to resource groups. After the AAA server authorizes a user to use a resource group, the user can access the Web resources provided by the URL list in the resource group.

To configure the Web access service:

4. On the **Access services** tab, select **Web access**, and then click **Next**.
5. In the **Web access resources** section, click **Create** in the **URL Items** area.
6. On the page that opens, configure a URL item, and then click **OK**.

Table 4 Configuration items for a URL item

Item	Description
URL item name	Enter a URL item name.
URL	Enter a URL in the URL item.
URI ACL	Select a URI ACL as a filtering criterion.
Mapping type	Select a mapping type. Options include **Normal mapping**, **Domain mapping**, and **Port mapping**.
Enable URL masking	Select whether to enable the masking for the specified URL. When this feature is enabled, the user will not be able to see the real address of the visited internal server.
Single sign-on	Select whether to enable SSO login. When this feature is enabled, a user can use one set of login credentials to access multiple trusted systems.
SSO mode	Select an SSO login mode. Options include: • **Basic access request**—Requires configuring login parameters. • **Auto-build access request**—Requires configuring the request method, encoding mode, request parameters, and encryption file uploading.

Item	Description
Login parameters	This item is available only after you select **Basic access request** for the **SSO mode** field. Select a method to obtain login parameters. Options include: • **Use SSL VPN login username and password**—Uses SSL VPN login username and password for SSO login. • **Use custom username and password**—Uses a custom username and password for SSO login. The custom username and password are configured on the SSL VPN Web interface.
Request method	This item is available only after you select **Auto-build access request** for the **SSO mode** field. Select a request method. Options include **GET** and **POST**.
Encoding mode	This item is available only after you select **Auto-build access request** for the **SSO mode** field. Select an encoding method. Options include **GB18030** and **UTF-8**.

Request parameters	This item is available only after you select **Auto-build access request** for the **SSO mode** field.
	
	To add a request parameter (attribute name and value), click **Add** in this field, and configure the following items in the dialog box that opens:
	
	• **Parameter name**—Enter a parameter name. The parameter name is the attribute name used for SSO login requests.
	
	• **Type**—Select a parameter type. The parameter value used for SSO login is the actual value abstracted according to the parameter type. Options include:
	
	  ◦ **Login name**—Uses the SSL VPN login username as the value of the SSO request parameter.
	
	  ◦ **Login password**—Uses the SSL VPN login password as the value of the SSO request parameter.
	
	  ◦ **Certificate subject**—Uses the certificate title as the value of the SSO request parameter.
	
	  ◦ **Certificate serial number**—Uses the certificate serial number as the value of the SSO request parameter.
	
	  ◦ **Certificate fingerprint**—Uses the certificate fingerprint as the value of the SSO request parameter.
	
	  ◦ **Phone number**—Uses the mobile phone number as the

Item	Description
	value of the SSO request parameter. ◦ **User group**—Uses the user group name as the value of the SSO request parameter. ◦ **Custom name**—Uses the customized username as the value of the SSO request parameter. ◦ **Custom password**—Uses the customized password as the value of the SSO request parameter. ◦ **Custom**—Specifies an actual parameter value of the SSO request parameter in the **Parameter value** field. • **Encrypt parameter value**—Select whether to enable parameter value encryption.
Set encryption file	This item is available only after you select **Auto-build access request** for the **SSO mode** field. Upload an encryption file for parameter value encryption. The encryption file must be a .js file, and cannot exceed 200 KB. To upload an encryption file, click **Select file** to select a .js file, and then click **Upload**. To cancel the use of the current encryption file, click **Cancel encryption**.
Current encryption file	Display the current encryption file.

7. Click **Create** in the **URL List** area.

8. On the page that opens, configure a URL list, and then click **OK**.

Table 5 Configuration items for a URL list

Item	Description
URL list name	Enter a URL list name.
Heading	Enter a URL list heading.

Item	Description
URL entry list	Select the URL items to add to the URL list.

Configure the TCP access service

On the TCP access service configuration page, perform the following tasks:

1. Create a port forwarding item.

   A port forwarding item maps a TCP service (such as Telnet, SSH, and POP3) provided on an internal server to a local address and port number on the SSL VPN client. Remote users can access the TCP service though the local address and port number.

   For example, you can configure a port forwarding item to allow a client to access HTTP service provided on port 80 of server 192.168.0.213 through IP address 127.0.0.1 and port 80.

   Configure a port forwarding item as follows:

   a. Specify a name for the port forwarding item.

   b. Specify the client host address, client port number, server address, and server port number.

   c. Configure a description for the port forwarding item.

   d. Specify the resource link for the port forwarding item as needed.

      If you configure a resource link for a port forwarding item, the port forwarding item name will be displayed as a link on the SSL VPN Web page. You can click the link to access the resource directly.

2. Create a port forwarding list.

   a. Specify a name for the port forwarding list.

b. Add the port forwarding items to the port forwarding list.

The port forwarding lists can be assigned to resource groups. After the AAA server authorizes a user to use a resource group, the user can access the TCP services provided by the port forwarding list in the resource group.

To configure the TCP access service:

3. On the **Access services** tab, select **TCP access**, and then click **Next**.
4. In the **TCP access resources** section, click **Create** in the **Port Forwarding Item** area.
5. On the page that opens, configure a port forwarding item, and then click **OK**.

Table 6 Configuration items for a port forwarding item

Item	Description
Name	Enter a port forwarding item name.
Client host	Specify the local address or host name of the SSL VPN client to which a TCP service on an internal server is mapped.
Client port	Specify the local port of the SSL VPN client to which a TCP service on an internal server is mapped.
Server address	Specify the IP address or FQDN of the internal server that provides the TCP service.
Server port	Specify the port of the internal server that provides the TCP service.
Description	Enter a description for the port forwarding item.
Resource link	Specify the resource link for the port forwarding item. SSL VPN users can click the resource link on the SSL VPN Web interface to access the resource.

6. Click **Create** in the **Port Forwarding List** area.

7. On the page that opens, configure a port forwarding list, and then click **OK**.

Table 7 Configuration items for a port forwarding list

Item	Description
Port forwarding list	Enter a port forwarding list name.
Port forwarding items	Specify the port forwarding items to add to the port forwarding list.

Configure the IP access service

On the IP access service configuration page, perform the following tasks:

1. Specify an SSL VPN AC interface for IP access.
2. Specify an IP access address pool.

   After a user passes the authentication, the SSL VPN gateway allocates an IP address to the VNIC of the user from the specified address pool.
3. Configure route lists.

   A route list contains the routing entries to be issued to SSL VPN clients.

   You can configure the following types of routing entries in a route list:

   - **Included route**—Client packets matching an included routing entry will be forwarded to the SSL VPN gateway through the VNIC of the client host.
   - **Excluded route**—Client packets matching an excluded routing entry will not be forwarded to the SSL VPN gateway.

The route lists can be assigned to resource groups. After the AAA server authorizes a user to use a resource group, the SSL VPN gateway will issue the routing entries in the route list of the resource group to the user. The user can then access the IP resources provided by the route list in the resource group.

4. To enable automatic startup of the IP access client after Web login, select **Start IP access client**. After a user logs in to the SSL VPN gateway through a Web browser, the IP access client on the user host will automatically connect to the gateway. If the IP access client software is not installed, the user will be prompted to install the software. For the IP access client to connect the SSL VPN gateway correctly, make sure the IP access resources are configured on the SSL VPN gateway.

5. To enable automatic pushing of accessible resources to IP access users, select **Push Web resources**. After a user logs in to the SSL VPN gateway through the IP access client, the SSL VPN gateway automatically pushes accessible SSL VPN resources to the user through the Web page. For successful push of SSL VPN resources through the Web page, make sure SSL VPN resources are configured on the SSL VPN gateway.

6. Configure the rate limits for upstream traffic and downstream traffic. IP access packets will be dropped if the rate limit is exceeded.

7. Create the user-to-IP address bindings.

   Bind IP addresses to an SSL VPN user in one of the following methods:

   - Bind a range of IP addresses to the user.
   - Enable the SSL VPN gateway to automatically bind the specified number of free addresses in the IP access address pool to the user.

   When the user accesses the SSL VPN gateway in IP access mode, the SSL VPN gateway assigns a bound IP address to the user. If an IP address in the specified IP address range has been assigned to another user, the SSL VPN gateway terminates the connection for that user and releases the IP address.

To configure the IP access service:

8. On the **Access services** tab, select **IP access**, and then click **Next**.

9. On the **IP access** page, configure basic settings for the IP access service.

Table 8 Basic configuration items for the IP access service

Item	Description
SSL VPN AC interface	Select an SSL VPN AC interface for IP access.
IP access address pool	Select the address pool from which the SSL VPN gateway assigns an IP address to a client.
Mask length	Specify the mask length for the address pool.
Primary DNS server	Specify the IP address of the internal primary DNS server.
Secondary DNS server	Specify the IP address of the internal secondary DNS server.
Primary WINS server	Specify the IP address of the internal primary WINS server.
Secondary WINS server	Specify the IP address of the internal secondary WINS server.
Keepalive interval	Specify the keepalive interval. A client sends keepalive messages to the SSL VPN gateway to maintain sessions between them.
Start IP access client	Select this item to enable automatic startup of the IP access client after Web login. After a user logs in to the SSL VPN gateway through a Web browser, the IP access client on the user host will automatically start and connect to the gateway.
Push Web resources	Select this item to enable automatic pushing of accessible resources to a user through Web after the user logs in to the SSL VPN gateway through the IP access client.

Item	Description
Rate limit	Specify the rate limits for upstream traffic and downstream traffic. Upstream traffic refers to the traffic sent from the user to the server. Downstream traffic refers to the traffic sent from the server to the user.
Packet drop logging	Select this item to enable logging for IP access packet drop events. The SSL VPN gateway generates logs when packets for SSL VPN IP access users are dropped.
IP connt close logging	Select this item to enable logging for IP access connection close events. The SSL VPN gateway generates logs when the connections established for SSL VPN IP access users are closed.
IP addr asgmt and release logging	Select this item to enable logging for IP address assignment and release events. The SSL VPN gateway generates logs when it assigns or releases an IP address to or from the VNIC of the SSL VPN client.

10. In the **IP access resources** section, click **Create** in the **IP Access Resources** area.
11. On the page that opens, enter a route list name.
12. In the **Route entries** section, click **Create**.
13. On the page that opens, configure a route entry.

Table 9 Configuration items for a route entry

Item	Description
Type	Select a route entry type. Options include: • **Included route**—Add the route entry to the route list as an included route. • **Excluded route**—Add the route entry to the route list as an excluded route. The SSL VPN gateway issues the route list to a login client. The client adds the routes to the local routing table. Traffic that matches the included routes is sent to the SSL VPN gateway. Traffic that matches the excluded

Item	Description
	routes is not sent to the SSL VPN gateway.
Subnet address	Specify the destination address of the route entry. To configure an included route, the destination network of the route entry must be the network where the internal server locates.
Mask length	Specify the subnet mask length.

14. Click **OK**.

    The route entry is displayed on the **Route entries** section.

15. Click **OK**.

    The route list is displayed on the **IP Access Resources** area.

16. In the **URL-to-IP Address Binding** area, click **Create**.

17. On the page that opens, configure a user-to-IP address binding.

Table 10 Configuration items for a user-to-IP address binding

Item	Description
Username	Enter an SSL VPN username.
Auto binding	Select this item to enable automatic user-to-IP address binding. This feature enables the SSL VPN gateway to automatically bind the specified number of free addresses in the IP access address pool to the user.
Number of IP	This item is available only when auto binding is enabled. Specify the number of IP addresses to bind.
Start IP address	Specify the start IP address for the range of IP addresses to bind.

Item	Description
End IP address	Specify the end IP address for the range of IP addresses to bind.

Configure the BYOD access service

1. On the **Access services** tab, select **BYOD access**, and then click **Next**.
2. On the **BYOD access** page, configure the following items:
    - Address and port number of the EMO server.
    - Address and port number of the message server.
3. Click **Next**.

Configure a shortcut list

To provide quick access to frequently accessed internal resources on the SSL VPN Web page, configure shortcuts for these resources and add the shortcuts to a shortcut list.

You can create multiple shortcut lists in an SSL VPN context.

When you configure a resource group, you can assign a shortcut list to the group. The shortcuts on the shortcut list will be displayed on the SSL VPN Web page for the user authorized to use the resource group. The user can click a shortcut to access the associated resource directly.

Procedure

1. On the **Shortcuts** tab, click **Create** in the **Shortcut** area.
2. On the page that opens, configure a shortcut, and then click **OK**.

Table 11 Configuration items for a shortcut

Item	Description
Shortcut name	Enter a name for the shortcut.
Description	Enter a description for the shortcut.
Resource address	Specify the resource address for the shortcut. SSL VPN users can click the link on the SSL VPN Web interface to access the resource. You can configure a resource address in one of the following methods: • Enter a resource link in the format of **url**('*url-value*'). The *url-value* argument specifies the corresponding resource. The complete format for *url-value* is *protocol*://*hostname or address*:*port number*/*resource path*. • Enter an application path in the format of **app**('*app-value*'). The *app-value* argument specifies the corresponding resource. The complete format for *app-value* can be an absolute path or environment variable, for example, c:\windows\system32\notepad++.exe. • Enter an executable JavaScript for a resource to provide access to the resource.

3. In the **Shortcut List** area, click **Create**.
4. On the page that opens, configure a shortcut list, and then click **OK**.

Table 12 Configuration items for a shortcut list

Item	Description
List name	Enter a shortcut list name.
Select shortcuts	Select shortcuts to add them to the shortcut list.

5. Click **Next**.

Configure a resource group

A resource group defines the Web resources, TCP resources, and IP resources that SSL VPN users can access. You can also use ACLs in resource groups to control user access more specifically.

Procedure

1. On the **Resource groups** tab, click **Create** in the **Resource groups** section.
2. On the page that opens, configure basic settings for the resource group.

Table 13 Configuration items for basic resource group settings

Item	Description
Resource group name	Enter a name for the resource group.
Instant access resource after login	Select the resource opened for users immediately after they log in to the SSL VPN gateway. Users do not need to select the resource on the SSL VPN resource page to access the resource.
Shortcut list	Select a shortcut list for the resource group.

3. In the **Web access** section, configure accessible Web resources.
    a. Select the one or more URL lists.
    b. Specify an IPv4 ACL to filter IPv4 Web access requests.
    c. Specify an IPv6 ACL to filter IPv6 Web access requests.
    d. Specify a URI ACL to filter Web access requests.
4. In the **TCP access** section, configure accessible TCP resources.

a. Select a TCP port forwarding list.

b. Specify an IPv4 ACL to filter IPv4 TCP access requests.

c. Specify an IPv6 ACL to filter IPv6 TCP access requests.

d. Specify a URI ACL to filter TCP access requests.

5. In the **IP access** section, configure accessible IP resources.

Table 14 Configuration items for IP access

Item	Description
Force all traffic to SSL VPN	Select this item to force all client packets for which no matching routes can be found in the local routing table to the SSL VPN gateway. The SSL VPN gateway will issue a default route to the SSL VPN client. The default route uses the VNIC as the output interface and has the highest priority among all default routes on the client. Packets for destinations not in the routing table are sent to the SSL VPN gateway through the VNIC. The SSL VPN gateway monitors the SSL VPN client in real time. It does not allow the client to delete the default route or add a default route with a higher priority.
Issue routes to client	Select a route list to issue the routes in the list to the client, or select **Host IPv4 address** and configure a routing entry to issue to the client.
IP access address pool	Specify the address pool from which the SSL VPN gateway assigns IP addresses to IP access users authorized to use the resource group. If no IP access address pool is specified for the authorized resource group, the SSL VPN gateway will assign IP addresses in the address pool specified for the SSL VPN context to IP access users. If no addresses are available in the address pool for a user, the IP access request of the user will be rejected.
IPv4 ACL	Specify an IPv4 ACL to filter IPv4 TCP access requests.
IPv6 ACL	Specify an IPv6 ACL to filter IPv6 TCP access requests.
URI ACL	Specify a URI ACL to filter TCP access requests.

6. Click **OK**.

   The newly created resource group is displayed on the **Resource groups** page.

7. Click **Finish**.

FAQ

After I change resource authorization settings in SSL VPN, the settings do not take effect immediately. Why?

The SSL VPN gateway does not support dynamic authorization. Table 15 describes how and when changed resource authorization settings in SSL VPN will take effect.

Table 15 How and when changed authorization settings take effect

Changed item	How and when the changes take effect
Authorization to a remote server	The changes take effect only on new users. Users already logged in are not affected.
ACL or ACL rules in a resource group	For IP, TCP, and Web access users, the changes take effect immediately.
Accessible Web resources	The changes take effect after the user refreshes the SSL VPN Web page.
Accessible TCP resources	The changes take effect after the user restarts the TCP access client software.
Routing entries, DNS server address, and WINS server address configured for the IP access service	The changes take effect immediately.

Do SSL VPN users need to pass certificate authentication to log in to an SSL VPN gateway?

Whether users need to pass certificate authentication to log in to an SSL VPN gateway depends on the following settings:

- Whether certificate authentication is enabled in the SSL VPN context associated with the SSL VPN gateway.
- Type of certificate authentication method configured in the SSL server policy used by the SSL VPN gateway.

Table 16 describes the possible certificate authentication methods that users might encounter when connecting the SSL VPN gateway.

Table 16 Certificate authentication methods

Authentication method	Description
Certificate authentication disabled	The user will not be asked to select a certificate for authentication when connecting the SSL VPN gateway through the Web browser.
Mandatory certificate authentication enabled	The user will be asked to select a certificate for authentication when connecting the SSL VPN gateway through the Web browser. The connection request will be rejected if the user does not have a certificate.
Optional certificate authentication enabled	The user will be asked to select a certificate for authentication when accessing the SSL VPN gateway through the Web browser. A connection to the SSL VPN gateway will be established in either of the following situations: • The user selects a certificate and passes the identity authentication. • The user chooses not to select a certificate and proceed with the connection request.

If you want users to pass certificate authentication to log in to an SSL VPN gateway, make sure the following requirements are met:

- Certificate authentication is enabled in the SSL VPN context associated with the SSL VPN gateway.
- Mandatory or optional SSL client authentication is enabled in the SSL server policy used by the SSL VPN gateway.

After receiving the client certificate, the SSL VPN gateway will extract the username from the CN field of the certificate, and then sends the username to the AAA server. The user passes the authentication only when extracted username exists on the local AAA server.

Mandatory certificate authentication is supported only for Web users and IP access users. For TCP access users and mobile client users to access the SSL VPN gateway successfully, you need to enable the optional SSL client authentication.

Routing table

Introduction

You can display routing table information, including brief routing table information and route statistics.

Static routing

Introduction

Static routes are manually configured. If a network's topology is simple, you only need to configure static routes for the network to work correctly.

Static routes cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the network administrator must modify the static routes manually.

A default route is used to forward packets that do not match any specific routing entry in the routing table. You can configure a default IPv4 route with destination address 0.0.0.0/0 and configure a default IPv6 route with destination address ::/0.

Policy-based routing

This help contains the following topics:

Introduction

About PBR

Policy-based routing (PBR) uses user-defined policies to route packets. A policy can specify parameters for packets that match specific criteria such as ACLs, packet lengths, service object groups, or application groups. The parameters include the next hop, output interface, default next hop, and default output interface.

Policy

A policy includes match criteria and actions to be taken on the matching packets. A policy can have one or multiple nodes as follows:

- Each node is identified by a node number. A smaller node number has a higher priority.
- A node contains **if-match** and **apply** clauses. An **if-match** clause specifies a match criterion, and an **apply** clause specifies an action.
- A node has a match mode of **permit** or **deny**.

You can specify a policy for local PBR to guide the forwarding of locally generated packets, or apply a policy to an interface to guide the forwarding of packets received on the interface.

A policy compares packets with nodes in priority order. If a packet matches the criteria on a node, it is processed by the action on the node. Otherwise, it goes to the next node for a match. If the packet does not match the criteria on any node, the device performs a routing table lookup

Node

Match criteria

You can set an ACL, service object group, application group, or packet length match criterion to match packets.

To match a node, a packet must match all types of the match criteria for the node.

The supported match criteria vary by device model.

Actions

- Compare packets with the next node upon failure on the current node. This action is taken when the specified actions (setting the VPN instance, next hop, output interface, default next hop, and default output interface) are not configured or become invalid. For example, the specified next hop is unreachable, the specified output interface is down, or the packets cannot be forwarded in the specified VPN instance.

- Set an IP precedence.
- Set the DF bit in the IP header.
- Specify the forwarding tables that can be used for the matching packets.
- Set next hops and default next hops associated with track entries. You can specify that a next hop must be directly connected to take effect.
- Set output interfaces and default output interfaces associated with track entries.

PBR and Track

PBR can work with the Track feature to dynamically adapt the availability status of an action to the link status of a tracked object.

The tracked object can be a next hop, output interface, default next hop, or default output interface. The action is valid only when the track entry status changes to **Positive** or **NotReady**.

OSPF

This help contains the following topics:

Introduction

Open Shortest Path First (OSPF) is a link-state IGP that encapsulates its data directly in IP packets using protocol number 89.

OSPF version 2 and OSPF version 3 are supported. OSPF version 2 is used for IPv4. OSPF version 3 is used for IPv6.

OSPF instances

To enable OSPF, you must first create an OSPF instance, specify the area associated with the instance, and specify network segments and interfaces for the area. An interface attached to a network of an area will run OSPF in the area. OSPF will advertise the direct route of the interface.

OSPF supports multiple instances. You can enable multiple OSPF instances on a device by specifying different names for the OSPF instances. OSPF instance names are locally meaningful. Two devices can exchange packets with each other even if their instance names are different.

OSPF areas

OSPF splits an AS into multiple areas. Each area is identified by an area ID. The boundaries between areas are devices rather than links. A device can belong to different areas, but a network segment (or a link) can only reside in one area. You must specify an area for each OSPF interface. You can configure route summarization on ABRs to reduce the number of LSAs advertised to other areas and minimize the effect of topology changes.

OSPF neighbors

In an OSPF network, two devices can exchange link state information only after they establish a neighbor relationship. Upon receiving a hello packet from an OSPF interface, the device checks parameters in the packet, including router ID, area ID, authentication information, subnet mask, and hello interval. If the parameters match its own, the receiving device considers the sending device an OSPF neighbor.

Configure OSPF

Configure an OSPF instance

1. Click the **Network** tab.
2. In the navigation pane, select **Routing** > **OSPF**.
3. Click the **OSPF Instance** tab.
4. Click **Create**.
5. Configure the OSPF instance parameters.

Table 1 OSPF instance configuration items

Item	Description
Version	Select an OSPF version. Options include **OSPFv2** and **OSPFv3**.
Instance name	Enter a name for the OSPF instance. OSPF instances of the same version cannot have the same name.
VRF	Select a VPN instance for the OSPF instance.
Router ID	Configure a router ID for the device.

6. Click **OK**.

   The OSPF instance will be displayed on the OSPF instance page.

Configure an OSPFv2 area

1. Click the **Network** tab.
2. In the navigation pane, select **Routing** > **OSPF**.
3. Click the **OSPF Instance** tab.
4. Click the number in the **Number of OSPF areas** column of an OSPFv2 instance.
5. Click **Create**.
6. Configure the OSPFv2 area parameters.

Table 2 OSPFv2 area configuration items

Item	Description
Instance name	Name of the OSPFv2 instance to which the OSPFv2 area belongs.
Area ID	Configure an area ID.
Area type	Select an area type.
Subnet	Specify network segments for the area. A network segment can reside in only one area. You can specify network segments one by one or specify all network segments of the device.
Interface	Add interfaces to the area and configure interface parameters.

7. Click **OK**.

   The OSPFv2 area will be displayed on the OSPFv2 area page.
8. Click the **OSPF Instance** tab, and then click the number in the **Number of redistributed routes** column of an OSPFv2 instance.
9. Click **Create**.

10. Configure the OSPFv2 redistributed route parameters.

Table 3 OSPFv2 redistributed route configuration items

Item	Description
Protocol type	Redistribute and advertise routes from the specified routing protocol.
Instance name	Instance ID of the specified routing protocol.

11. Click **OK**.

Configure an OSPFv3 area

1. Click the **Network** tab.
2. In the navigation pane, select **Routing** > **OSPF**.
3. Click the **OSPF Instance** tab.
4. Click the number in the **Number of OSPF areas** column of an OSPFv3 instance.
5. Click **Create**.
6. Configure the OSPFv3 area parameters.

Table 4 OSPFv3 area configuration items

Item	Description
Area type	Select an area type.
Area ID	Configure an area ID.

7. Click **OK**.

   The OSPFv3 area will be displayed on the OSPFv3 area page.

8. Click the **OSPF Instance** tab, and then click the number in the **Number of OSPF interfaces** column of an OSPFv3 instance.

9. Click **Create**.

10. Configure the OSPFv3 interface parameters.

Table 5 OSPFv3 interface configuration items

Item	Description
Area ID	Specify the OSPFv3 area to which the interface belongs.
Interface name	Select an interface.
Interface instance ID	Configure an interface instance ID. Different interface instances of an interface can be added to different OSPFv3 instances.

11. Click **OK**.

    The interface will be displayed on the OSPFv3 interface page.

BGP

Introduction

Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP). It is called internal BGP (IBGP) when it runs within an AS and called external BGP (EBGP) when it runs between ASs. An AS refers to a group of routers that use the same routing policy and work under the same administration.

The current version in use is BGP-4. It is widely used by Internet Service Providers (ISPs).

Basic concepts

BGP speaker and BGP peer

A router running BGP is a BGP speaker. A BGP speaker establishes peer relationships with other BGP speakers to exchange routing information over TCP connections.

BGP peers include the following types:

- **IBGP peers**—Reside in the same AS as the local router.
- **EBGP peers**—Reside in different ASs from the local router.

If you create a BGP peer without selecting an address family for it, the BGP peer remains in idle sta
not attempt to establish peer relationships through Open messages.

MP-BGP

BGP-4 can only advertise IPv4 unicast routing information.

Multiprotocol Extensions for BGP-4 (MP-BGP) can advertise routing information for the following address families:

- IPv6 unicast address family.
- IPv4 multicast address family and IPv6 multicast address family.

  PIM uses static and dynamic unicast routes to perform RPF check before creating multicast routing entries. When the multicast and unicast topologies are different, you can use MP-BGP to advertise the routes for RPF check. MP-BGP stores the routes in the BGP multicast routing table.
- IPv4 MDT address family.

  MP-BGP advertises MDT information including the PE address and default group so that multicast VPN can create a default MDT that uses the PE as the root on the public network. For more information about multicast VPN, see *IP Multicast Configuration Guide*.

Controlling BGP route generation

BGP routes can be generated in the following ways:

1. Inject a local network. Perform this task to inject a network in the local routing table to the BGP routing table, so BGP can advertise the network to BGP peers. The ORIGIN attribute of BGP routes advertised in this way is IGP. You can also use a routing policy to control route advertisement.

The specified network must be available and active in the local IP routing table.

2. Redistribute IGP routes: Perform this task to configure route redistribution from an IGP to BGP.

   By default, BGP does not redistribute default IGP routes. You can configure BGP to redistribute default IGP routes into the BGP routing table.

- The ORIGIN attribute of BGP routes redistributed from IGPs is INCOMPLETE.
- Only active routes can be redistributed.

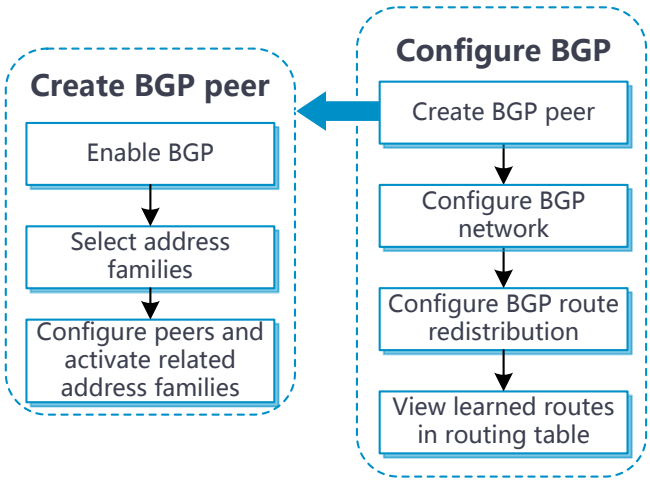
Restrictions and guidelines

- Before you perform operations on the **BGP Network** and **BGP Route Redistribution** tabs, select address families on BGP Address Family tab first. If you do not follow this sequence, the system displays an error message.
- For a device with BGP configuration, if you clear the **Enable BGP** option under **BGP status** and then click **Apply**, the BGP process will be disabled, and the BGP configuration will be lost.

Configure BGP

Configure BGP as shown in Figure 1.

Figure 1 BGP configuration procedure



RIP

Introduction

Routing Information Protocol (RIP) is a distance-vector Interior Gateway Protocol (IGP) suited to small-sized networks. It is still widely used because of easy configuration and maintenance.

Restrictions and guidelines

- The Advertise all networks option is not available when multiple RIP processes exist.
- An interface preferentially uses the interface-specific RIP version. If no interface-specific version is specified, the interface uses the global RIP version.

IPv4 multicast routing

Introduction

Only when IPv4 multicast routing is enabled, other Layer 3 multicast features (such as IGMP and PIM) can take effect.

The following tables are involved in IPv4 multicast routing and forwarding:

- IPv4 multicast routing table of each multicast routing protocol, such as the PIM routing table.
- General IPv4 multicast routing table that summarizes multicast routing information generated by different multicast routing protocols.

IPv6 multicast routing

Introduction

Only when IPv6 multicast routing is enabled, other IPv6 Layer 3 multicast features (such as MLD and IPv6 PIM) can take effect.

The following tables are involved in IPv6 multicast routing and forwarding:

- IPv6 multicast routing table of each multicast routing protocol, such as the IPv6 PIM routing table.
- General IPv6 multicast routing table that summarizes IPv6 multicast routing information generated by different IPv6 multicast routing protocols.

PIM

Introduction

Protocol Independent Multicast (PIM) provides IP multicast forwarding by leveraging unicast static routes or unicast routing tables generated by any unicast routing protocol. PIM uses the underlying unicast routing to generate a multicast routing table without relying on any particular unicast routing protocol.

Based on the implementation mechanism, PIM includes the following categories:

- **Protocol Independent Multicast–Dense Mode (PIM-DM)**—PIM-DM is suitable for small-sized networks with densely distributed multicast members.
- **Protocol Independent Multicast–Sparse Mode (PIM-SM)**—PIM-SM is suitable for large- and medium-sized networks with sparsely and widely distributed multicast group members.
- **Protocol Independent Multicast Source-Specific Multicast (PIM-SSM)**—PIM-SSM can be implemented by leveraging part of the PIM-SM technique. Before you configure PIM-SSM, you must first enable PIM-SM.

If you enable PIM-DM on an interface, the PIM-DM mode is used. If you enabled PIM-SM on an interface, the PIM mode on the interface varies by multicast group for which a multicast packet destines.

- If the multicast group is in the SSM group range, the PIM-SSM mode is used.
- If the multicast group is not in the SSM group range, the PIM-DM mode is used.

IGMP

Introduction

Internet Group Management Protocol (IGMP) establishes and maintains the multicast group memberships between a Layer 3 multicast device and the hosts on the directly connected subnet.

IGMP has the following versions:

- **IGMPv1**—IGMPv1 manages multicast group memberships based on the query and response mechanism.
- **IGMPv2**—Backwards-compatible with IGMPv1, IGMPv2 has introduced a querier election mechanism and a leave-group mechanism.
- **IGMPv3**—Based on and compatible with IGMPv1 and IGMPv2, IGMPv3 enhances the control capabilities of hosts and the query and report capabilities of IGMP routers.
    - IGMPv3 introduced two source filtering modes (Include and Exclude). These modes allow a host to receive or reject multicast data from the specified multicast sources.
    - IGMPv3 introduces IGMP group-and-source queries and IGMP reports carrying group records.
    - After IGMP is enabled on an interface, the interface can establish and maintain multicast group memberships.

MLD

Introduction

Multicast Listener Discovery Protocol (MLD) establishes and maintains the IPv6 multicast group memberships between a Layer 3 multicast device and the hosts on the directly connected subnet.

MLD has the following versions:

- **MLDv1**—Derived from IGMPv2, MLDv1 manages IPv6 multicast group memberships based on the query and response mechanism.
- **MLDv2**—Derived from IGMPv3 and backwards-compatible with MLDv1, MLDv2 provides hosts with enhanced control capabilities and enhances the MLD state.

After MLD is enabled on an interface, the interface can establish and maintain IPv6 multicast group memberships.

DHCP

This help contains the following topics:

- Introduction
- DHCP server
  - DHCP address pool
  - IP address allocation sequence
  - DHCP options
  - IP address conflict detection
- Configure DHCP

Introduction

The Dynamic Host Configuration Protocol (DHCP) provides a framework to assign network configuration information to network devices.

DHCP uses the client-server model. A DHCP network typically contains a DHCP server and multiple DHCP clients. If DHCP clients and the DHCP server are on different subnets, the DHCP clients can obtain configuration parameters from the DHCP server through a DHCP relay agent.

DHCP server

Use a DHCP server to assign IP addresses for the following networks:

- A large-sized network that requires centralized management.
- A network without sufficient IP address space. If the number of hosts is larger than the number of assignable IP addresses, not all hosts can have an IP address at the same time.
- A network with only a few hosts requiring fixed IP addresses.

A DHCP server stores the following information in an address pool: IP addresses, lease duration, network information, domain name suffix, DNS server addresses, WINS server addresses, NetBIOS node types, and DHCP option information. The DHCP server selects an IP address and configuration parameters from the address pool and allocates them to a requesting DHCP client.

Before assigning the IP address to the client, the DHCP server performs IP address conflict detection.

DHCP address pool

The following address assignment mechanisms are available:

- **Static address binding**—Manually bind the MAC address or ID of a client to an IP address in a DHCP address pool. When the client requests an IP address, the DHCP server assigns the IP address in the static binding to the client.
- **Dynamic address allocation**—Specify IP address ranges in a DHCP address pool. Upon receiving a DHCP request, the DHCP server dynamically selects an IP address from the matching IP address range in the address pool.

You can specify the lease duration for statically and dynamically allocated addresses.

The DHCP server observes the following principles to select an address pool for a client:

1. If there is an address pool where an IP address is statically bound to the MAC address or ID of the client, the DHCP server selects this address pool and assigns the statically bound IP address and other configuration parameters to the client.

2. If the above condition is not met, the DHCP server selects an address pool depending on the client location.
    - **Client on the same subnet as the server**—The DHCP server compares the IP address of the receiving interface with subnets of all address pools, and selects the address pool with the longest-matching subnet.
    - **Client on a different subnet than the server**—The DHCP server compares the IP address in the **giaddr** field of the DHCP request with subnets of all address pools, and selects the address pool with the longest-matching primary subnet.

IP address allocation sequence

The DHCP server selects an IP address for a client in the following sequence:

1. IP address statically bound to the client's MAC address or ID.
2. IP address that was ever assigned to the client.
3. IP address designated by the Option 50 field in the DHCP-DISCOVER message sent by the client.

   Option 50 is the Requested IP Address option. The client uses this option to specify the wanted IP address in a DHCP-DISCOVER message. The content of Option 50 is user defined.
4. First assignable IP address found based on the dynamic allocation rule.
5. IP address that was a conflict or passed its lease duration. If no IP address is assignable, the server does not respond.

DHCP options

DHCP uses the options field to carry information for dynamic address allocation and provide additional configuration information for clients.

Use the **DHCP options** feature for the following purposes:

- Add new DHCP options.
- Define vendor-specific option contents. For example, you can pad vendor-specific information into Option 43.
- Configure functions that are not supported on other DHCP Web pages. For example, you can use Option 4 to specify the IP address 1.1.1.1 as the time server address for DHCP clients.
- Extend existing DHCP options to meet user requirements. For example, a maximum of eight DNS server addresses can be configured on the Web page. If you need to configure more DNS servers, you can use the DHCP options for extension.

Table 1 lists common DHCP options.

Table 1 Common DHCP options

Option number	Option name	Recommended option padding type
3	Router Option	IP address
6	Domain Name Server Option	IP address
15	Domain Name	ASCII string
43	Vendor Specific Information	Hexadecimal string
44	NetBIOS over TCP/IP Name Server Option	IP address

Option number	Option name	Recommended option padding type
46	NetBIOS over TCP/IP Node Type Option	Hexadecimal string
66	TFTP server name	ASCII string
67	Bootfile name	ASCII string

IP address conflict detection

Before assigning an IP address, the DHCP server pings that IP address.

- If the server receives a response within the specified period, it selects and pings another IP address.
- If it receives no response, the server continues to ping the IP address until the maximum number of ping packets are sent. If still no response is received, the server assigns the IP address to the requesting client.

Configure DHCP

Configure the DHCP server

To implement the DHCP server function, perform the following tasks:

- Enable DHCP service.
- Configure the interface to operate in DHCP server mode.

- Configure a DHCP address pool. You can select the dynamical allocation method or the static binding for address allocation. You can configure lease duration, domain name suffix, gateway address, and other network parameters for the DHCP address pool.

HTTP/HTTPS

Introduction

The device provides a built-in Web server. You can use a Web browser to log in to the device through HTTP or HTTPS.

- HTTP login

  The device supports HTTP 1.0 and HTTP 1.1.

- HTTPS login

  HTTPS uses SSL to ensure the integrity and security of data exchanged between the client and the server, and is more secure than HTTP.

  To allow HTTPS login, you must enable the HTTPS service. By default, the device uses a self-signed certificate (a certificate that is generated and signed by the device itself) and the default SSL settings.

  For better integrity and security of data exchanged between the client and the server, you can associate an SSL server policy with HTTPS to define the SSL settings.

  The device supports the following HTTPS login types:

  - **Username**—A user must provide a username and password at login.
  - **Certificate**—A user must provide a digital certificate at login.
  - **Username and certificate**—A user must provide a username and password together with a digital certificate at login.

USB key login is a certificate-based HTTPS login method. If a user clicks **Log in using a USB key** on the login page, the user needs to select a digital certificate in the USB key as prompted to log in.

The device can use ACLs to prevent unauthorized HTTP and HTTPS access. If the used ACLs exist and have rules, only users permitted by the ACLs can access the device through HTTP or HTTPS.

SSH

This help contains the following topics:

- Introduction
- Restrictions and guidelines
- Configure SSH

Introduction

Secure Shell (SSH) is a network security protocol. Using encryption and authentication, SSH can implement secure remote access and file transfer over an insecure network.

SSH uses the typical client-server model to establish a channel for secure data transfer based on TCP.

The device supports the following SSH applications:

- **Secure Telnet**—Stelnet provides secure and reliable network terminal access services.
- **Secure File Transfer Protocol**—Based on SSH2, SFTP uses SSH connections to provide secure file transfer.
- **Secure Copy**—Based on SSH2, SCP offers a secure method to copy files.

SSH includes two versions: SSH1.x and SSH2.0 (hereinafter referred to as SSH1 and SSH2), which are not compatible. SSH2 is better than SSH1 in performance and security.

When the device acts as an SSH server, it uses local password authentication to verify the username and password of the SSH client. After the SSH client passes authentication, the SSH client and the SSH server can establish a session and exchange data using this session.

Restrictions and guidelines

- To support SSH clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the SSH server.
- Local DSA, ECDSA, and RSA key pairs for the SSH server use default names. You cannot assign names to the key pairs.
- The key modulus length must be less than 2048 bits when you generate the DSA key pair on the SSH server.
- After the SSH client passes authentication, attributes (for example, user role or FTP directory) assigned to the SSH client are determined by the administrator configuration on the SSH server.
- If the ACL that filters SSH clients' connection requests does not exist or contains no rules, all SSH clients can access the device.
- When acting as an SFTP server, the device does not support SFTP connections initiated by SSH1 clients.

Configure SSH

To enable the SSH server to provide Stelnet, SFTP, or SCP service, perform the following tasks:

- Generate RSA, DSA or ECDSA key pairs.
- Enable Stelnet, SFTP, or SCP service.
- Configure an administrator of the SSH service type.

NTP

Introduction

Network Time Protocol (NTP) is used to synchronize system clocks among distributed time servers and clients on a network.

NTP uses stratums 1 to 15 to define clock accuracy. A lower stratum value represents higher accuracy.

If devices on a network cannot synchronize to an authoritative time source, you can perform the following tasks to achieve NTP synchronization on the network:

1. Select a device that has a relatively accurate clock on the network.
2. Configure the local clock of the device as its reference source.
3. Configure the device as a time server to synchronize other devices on the network.

You can configure a local clock as the reference source from the Web interface.

Restrictions and guidelines

Before configuring a local clock as the reference source, adjust the time on the local clock to ensure that it is accurate.

FTP

Introduction

File Transfer Protocol (FTP) is an application layer protocol for transferring files from one host to another over an IP network. It uses TCP port 20 to transfer data and TCP port 21 to transfer control commands.

FTP uses the client/server model. The device can act as the FTP server.

Telnet

Introduction

The device can act as a Telnet server to allow Telnet login.

The device can use ACLs to prevent unauthorized Telnet access. If the used ACLs exist and have rules, only users permitted by the ACLs can Telnet to the device.

Restrictions and guidelines

To enable Telnet login, you must enable the Telnet server, configure login authentication and common attributes, and assign user roles.

MAC authentication

Introduction

MAC authentication controls network access by authenticating source MAC addresses on an interface. The feature does not require client software, and users do not have to enter a username and password for network access. The device initiates a MAC authentication process when it detects an unknown source MAC address on a MAC authentication-enabled interface.

Restrictions and guidelines

Restrictions and guidelines: Guest VLAN

Before you configure the MAC authentication guest VLAN on an interface, complete the following tasks:

- Create the VLAN to be specified as the MAC authentication guest VLAN.
- Configure the link type of the interface as hybrid, and configure the VLAN as an untagged member on the interface.
- Enable MAC-based VLAN on the interface.

When you configure the MAC authentication guest VLAN on an interface, follow the guidelines in Table 1.

Table 1 Relationships of the MAC authentication guest VLAN with other security features

Feature	Relationship description
Quiet feature of MAC authentication	The MAC authentication guest VLAN feature has higher priority. When a user fails MAC authentication, the user can access the resources in the guest VLAN. The user's MAC address is not marked as a silent MAC address.
Super VLAN	You cannot specify a VLAN as both a super VLAN and a MAC authentication guest VLAN.
Port security intrusion protection	The guest VLAN feature has higher priority than the block MAC action but lower priority than the shutdown action of the port security intrusion protection feature.

Restrictions and guidelines: Critical VLAN

Before you configure the MAC authentication critical VLAN on an interface, complete the following tasks:

- Create the VLAN to be specified as the MAC authentication critical VLAN.
- Configure the link type of the interface as hybrid, and configure the VLAN as an untagged member on the interface.
- Enable MAC-based VLAN on the interface.

When you configure the MAC authentication critical VLAN on an interface, follow the guidelines in Table 2.

Table 2 Relationships of the MAC authentication critical VLAN with other security features

Feature	Relationship description
Quiet feature of MAC authentication	The MAC authentication critical VLAN feature has higher priority. When a user fails MAC authentication because no RADIUS authentication server is reachable, the user can access the resources in the critical VLAN. The user's MAC address is not marked as a silent MAC address.
Super VLAN	You cannot specify a VLAN as both a super VLAN and a MAC authentication critical VLAN.
Port security intrusion protection	The critical VLAN feature has higher priority than the block MAC action but lower priority than the shutdown action of the port security intrusion protection feature.

Configure MAC authentication

1. Click the **Network** tab.
2. In the navigation pane, select **Security Access** > **MAC Access** > **MAC Authentication**.
3. Select **Enable** to enable global MAC authentication.
4. Select **Enable interface-specific MAC authentication** to enable MAC authentication for the target interface.
5. Click **Edit** for the target interface to enter the **Edit MAC Authentication** page.
6. Configure the MAC authentication parameters.

Table 3 MAC authentication configuration items

Item	Description
Authentication delay	Set the MAC authentication delay time. If you do not set a delay time, MAC authentication delay is disabled.
VLAN mode	Select a VLAN mode for the interface, which can be single-VLAN mode or multi-VLAN mode.
Guest VLAN	Specify a guest VLAN to accommodate users that have failed MAC authentication.
Critical VLAN	Specify a critical VLAN to accommodate users that have failed MAC authentication because of server unreachable.
Authentication ISP domain	Specify an authentication ISP domain for users that access the interface.
Max online users	Set the maximum number of concurrent MAC authentication users allowed to access the interface.
Server unreachable for reauthentication	Select whether to log off users or allow users to stay online if no server is reachable for reauthentication of the users.

7. Click **OK**.

MAC address whitelist

Introduction

To allow trustworthy endpoints to access the network without MAC authentication, add them to the MAC address whitelist.

You can add trustworthy endpoints to the MAC address whitelist manually or from the EPS system by using its endpoint scanning feature. On the EPS system, you can configure authentication settings such as passwords for these endpoints as needed.

When a MAC address is added to the MAC address whitelist, the device automatically add a local user account for that MAC address.

Configure the MAC address whitelist

1. Click the **Network** tab.
2. In the navigation pane, select **Security Access** > **MAC Access** > **MAC Address Whitelist**.
3. Click **Create**.
4. Configure MAC address whitelist parameters.

Table 1 MAC address whitelist configuration items

Item	Description
MAC address	MAC address of the whitelist user.

Item	Description
Available services	Services available for the user. By default, LAN access is selected. This item is not user configurable.
Access interface	Select the interface through which the user accesses the device. If you select an interface that is not the user access interface, the user will fail authentication.

5. Click **OK**. The new MAC whitelist user will be displayed in the list on the **MAC Address Whitelist** page.

MAC access silent MAC info

Introduction

The silent MAC list contains information about users whose MAC addresses are marked as silent MAC addresses.

If a user fails MAC authentication, the device marks the MAC address of that user as a silent MAC address and starts a quiet timer (user configurable) for the MAC address. The device will drop all packets from the MAC address within the quiet time. The quiet mechanism avoids repeated authentication during a short time.

MAC access advanced settings

Introduction

User account formats

MAC authentication supports the following user account formats:

- **Shared user account**—You can specify one username and password to be shared by all MAC authentication users on the device. The username and password can be any valid strings, including MAC addresses.
- **MAC-based user account**—The MAC address of each user is used by the device as the username and password for MAC authentication.

Authentication ISP domain

To implement different access policies for users, you can specify authentication ISP domains that have different access policies for MAC authentication users.

Offline detect timer

This timer sets the interval that the device must wait for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer

expires, the device logs off that user and requests the accounting server to stop accounting for the user.

Quiet timer

This timer sets the interval that the device must wait before the device can perform MAC authentication for a user that has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.

Server timeout timer

This timer sets the interval that the device waits for a response from a RADIUS server before the device determines that the RADIUS server is unavailable. If the timer expires during MAC authentication, the user fails MAC authentication.

IP authentication

Introduction

IP authentication automatically generates usernames and passwords based on the user access location information to authenticate users. Users do not need to enter usernames or passwords.

Configure IP authentication

1. Click the **Network** tab.
2. In the navigation pane, select **Security Access** > **IP Access** > **IP Authentication**.
3. Click the **Edit** icon for an interface. The **Edit IP Authentication** page opens.
4. Configure IP authentication parameters for the interface.

Table 1 IP authentication configuration items

Item	Description
IP type	Select an IP protocol type.
IPoE status	Select an IPoE access mode. • **Enable Layer 2 access**—Users are connected to the access device directly or through Layer 2 network devices. The access device must be able to recognize the user MAC addresses. • **Enable Layer 3 access**—User traffic is routed to the access device through a Layer 3 network. Users can be connected to the access device directly or through Layer

Item	Description
	3 forwarding devices. • **Disable**—Disable IPoE.
Unclassified IP access	Specify whether to allow unclassified-IP users to access.
IP whitelist	Specify whether to enable the IP whitelist. If you select to enable the IP whitelist, the IP whitelist takes effect.

5. Click **OK**.

IPv4 whitelist

Introduction

The IPv4 whitelist is used during the IP authentication. When the IPv4 address of a user is on the IPv4 whitelist, the user can directly pass authentication without being authenticated by the authentication server.

Configure the IPv4 whitelist

1. Click the **Network** tab.
2. In the navigation pane, select **Security Access** > **IP Access** > **IPv4 Whitelist**.
3. Click **Create**. The **Create IPv4 Whitelist** page opens.
4. Add an IPv4 whitelist user to the IPv4 whitelist.

Table 1 IPv4 whitelist user configuration items

Item	Description
Interface	Select a device interface through the whitelist user accesses the network.
IPv4 address	Configure the IPv4 address of the whitelist user.
ISP domain	Configure the ISP domain used by the whitelist user. The authentication server must be set to **none** for the ISP domain.

Item	Description
Description	Configure the description of the whitelist user.

5. Click **OK**.

IPv6 whitelist

Introduction

The IPv6 whitelist is used during the IP authentication. When the IPv6 address of a user is on the IPv6 whitelist, the user can directly pass authentication without being authenticated by the authentication server.

Configure the IPv6 whitelist

1. Click the **Network** tab.
2. In the navigation pane, select **Security Access** > **IP Access** > **IPv6 Whitelist**.
3. Click **Create**. The **Create IPv6 Whitelist** page opens.
4. Add an IPv6 whitelist user to the IPv6 whitelist.

Table 1 IPv6 whitelist user configuration items

Item	Description
Interface	Select a device interface through the whitelist user accesses the network.
IPv6 address	Configure the IPv6 address of the whitelist user.
ISP domain	Configure the ISP domain used by the whitelist user. The authentication server must be set to **none** for the ISP domain.

Item	Description
Description	Configure the description of the whitelist user.

5. Click **OK**.

High availability group

This help contains the following topics:

Introduction

The high availability (HA) group is a device-level HA solution. It enables two devices to back up each other dynamically to ensure user service continuity upon failure of one of the devices.

The HA group works with Remote Backup Management to manage multiple VRRP groups on two devices to ensure that they have the same VRRP master and backup. The HA group can

synchronize important configuration and service entries between the master and the backup devices in VRRP groups to ensure service continuity. Two devices must have the same software and hardware environments to join the HA group.

Basic concepts in HA group configuration

Basic concepts in HA group configuration are as follows:

- **Primary and secondary roles**—Control the direction of configuration synchronization between devices. The primary and secondary roles are assigned to the two devices in an HA group, respectively. The primary device synchronizes its configuration to the secondary device, and the configuration on the secondary device is overwritten.
- **VRRP master and backup roles**—Determine which device forwards and processes traffic in a VRRP group. The master and backup roles are assigned to the primary and secondary devices in an HA group, respectively. In a VRRP group, the master forwards traffic of services and backs up service entries to the backup in real time. When the master fails, the backup takes over the master role to ensure service continuity.
- **VRRP active and standby groups**—Associate the HA group with VRRP for the HA group to centrally manage the status of multiple VRRP groups.
- **HA channels**—Transmit status information, important configuration, and service entries between the HA group members.
- **HA group modes**—Include active/standby mode and dual-active mode. In active/standby mode, the primary device processes all services. In dual-active mode, both devices process services to increase the capability of the HA group and load share traffic.
- **HA packets**—Transmitted through TCP over the HA channel between the HA group members.

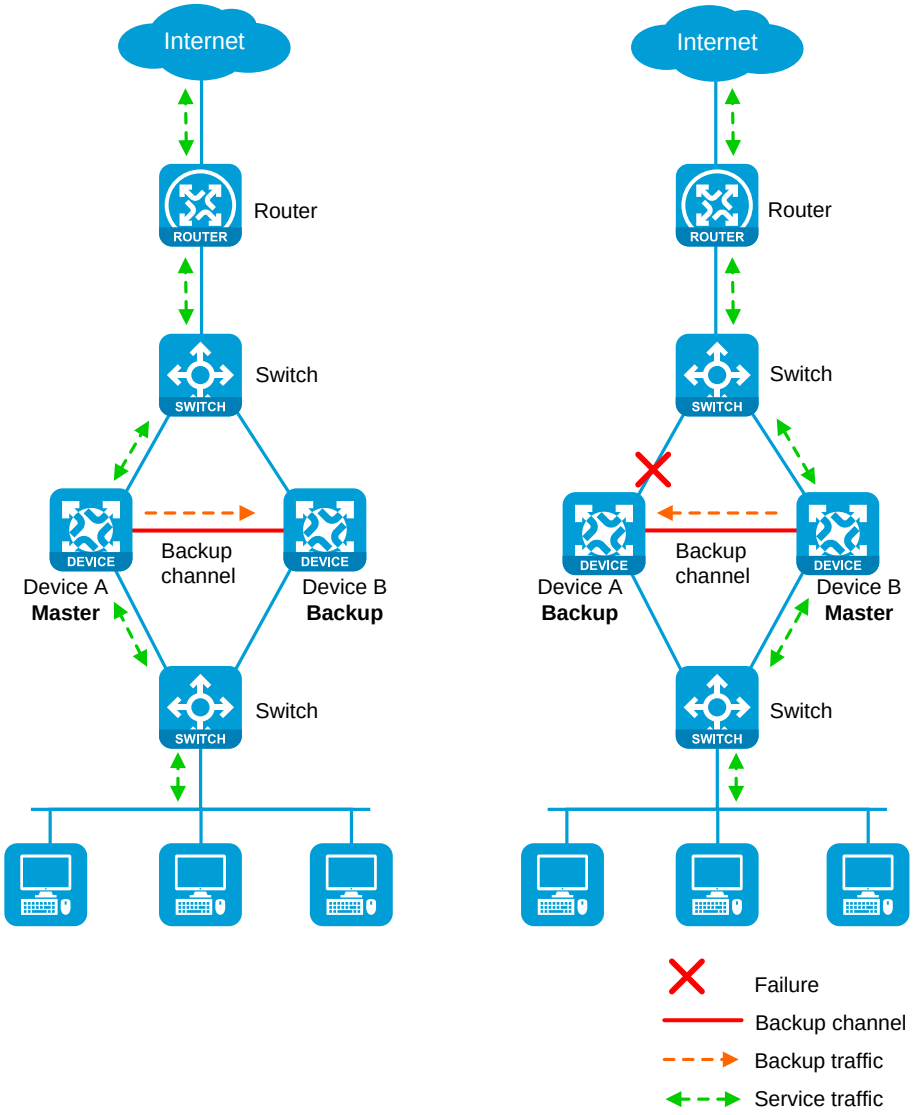
Operating modes of the HA group

The HA group supports the active/standby and dual-active modes.

Active/standby mode

In active/standby mode, one device acts as the master to process services, and the other device stands by as a backup, as shown in Figure 1. When an interface or link on the master fails or when the master fails, the backup takes over the master role to process services.

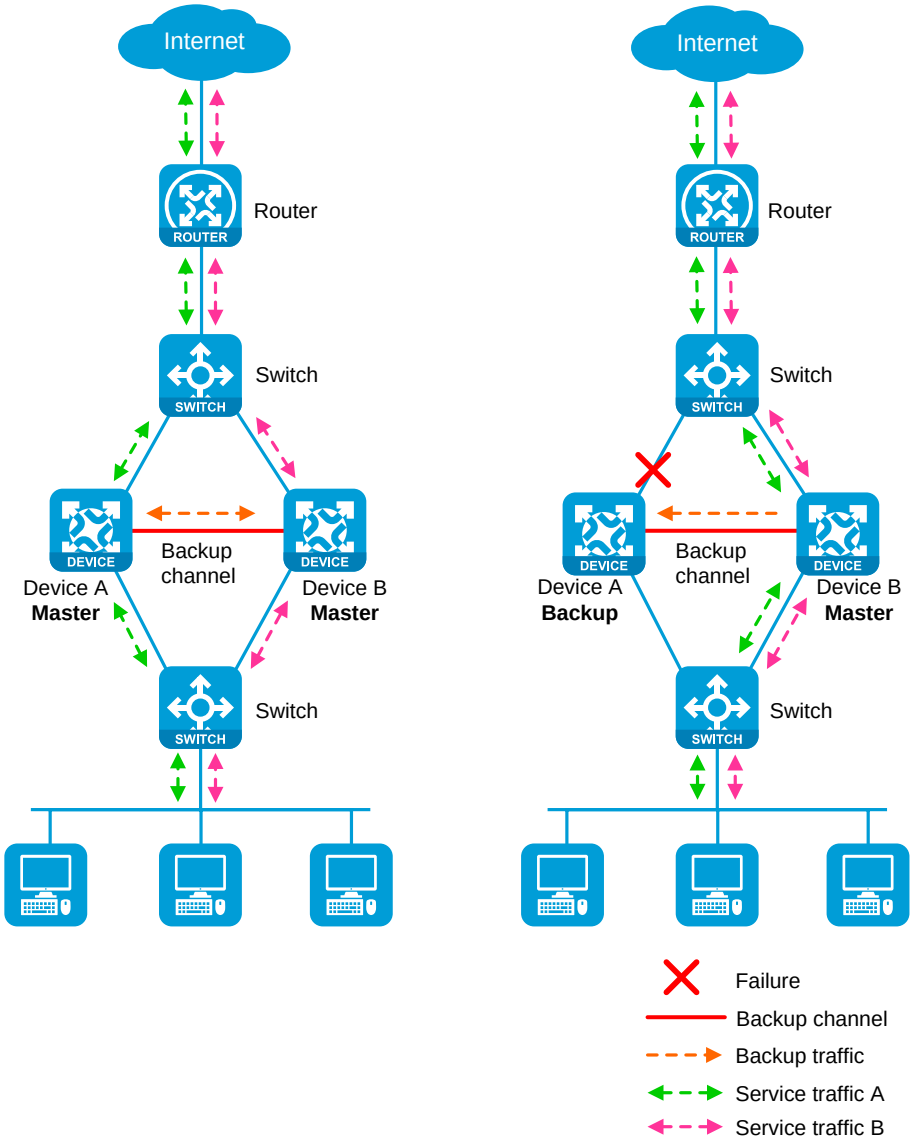
Figure 1 Active/standby mode of the HA group



Dual-active mode

In dual-active mode, both devices process services to increase capability of the HA group, as shown in Figure 2. When one device fails, its traffic is switched to the other device for forwarding.

Figure 2 Dual-active mode of the HA group



HA channels

Overview

The HA group members transmit HA group status, important configuration, and service entries over the following channels:

- **Control channel**—Transmits data by using packets, including HA group status packets, configuration consistency check packets, backup packets for service entries, data packets that require transparent transmission, and configuration synchronization packets.
- **Data channel**—Transmits only backup packets and packets that require transparent transmission. The data channel uses the hardware driver for data transmission and supports only Layer 2 forwarding.

Establishment and keepalive mechanism of the control channel

The control channel uses the keepalive mechanism of TCP for reachability detection. The control channel is established through TCP. In the HA group, the device with the higher IP address acts as the server, and the other device acts as the client to initiate the TCP connection.

Each member device periodically sends HA keepalive packets to the HA peer over the HA control channel. If a device has not received any responses from the peer when the maximum number of HA keepalive attempts is reached, the HA control channel is disconnected.

Service entry backup

Overview

The HA group backs up the service entries generated on the primary device to the secondary device to prevent service interruption when a primary/secondary member switchover occurs.

Security devices like firewalls generate a session entry for each dynamic connection. In the HA group, only the primary device processes traffic and generates session entries. To ensure service continuity, the primary device backs up its session entries to the secondary device in real time. After a primary/secondary member switchover, the new primary device can forward the packets of the existing services based on the session entries without interruption.

Supported services

The HA group can perform hot backup for the following service entries:

- Session entries.
- Session relation entries.
- NAT port blocks.
- AFT port blocks.
- Entries generated by security service modules.

Support for these entries depends on the device model.

Configuration backup

Overview

The HA group backs up important configuration from the primary device to the secondary device to prevent service interruption when a primary/secondary member switchover occurs. The configuration on the secondary device is overwritten. The unidirectional backup mechanism avoids configuration conflicts, especially in dual-active mode. The HA roles can only be manually assigned to devices. As a best practice to ensure correct operation of the HA group, enable configuration backup on the primary device.

Backup type

The HA group supports both automatic backup and manual backup.

Supported services

The HA group can perform configuration backup for the following services:

- Resources: VPN instance, ACL, object group, time range, security zone, session management, APR, AAA.
- DPI: Application layer inspection engine, IPS, URL filter, data filter, file filter, anti-virus, data analysis center.
- Policies: Object policy, security policy, ASPF, attack detection and prevention, connection limit, NAT, AFT, load balancing, bandwidth management, application auditing and management, shared network access management, proxy policy.
- Logs: Fast log output, flow log.
- SSL VPN.
- VLAN.
- Information center.

Support for these services depends on the device model.

Configuration consistency check

The HA group verifies configuration consistency between the HA group members by using configuration consistency check packets. If a device detects configuration inconsistency, it generates a log for you to manually synchronize configuration.

HA group in collaboration with VRRP

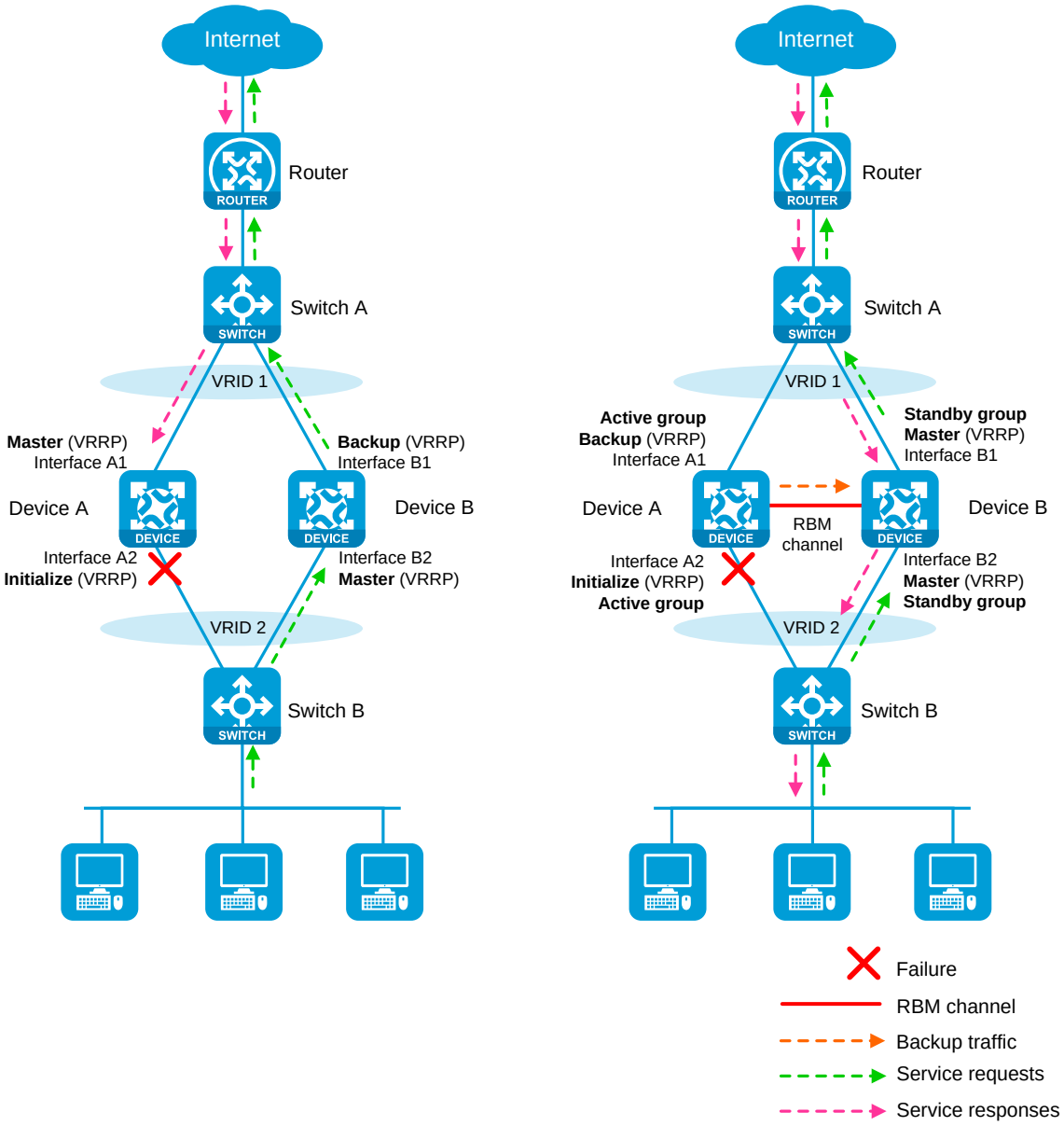
Overview

You can use the HA group and VRRP in combination to control master/backup switchover for device role consistency (master or backup) in multiple VRRP groups. This ensures that both inbound and outbound traffic can be switched to the new master for symmetric forwarding upon device failure.

Figure 3 illustrates VRRP association with the HA group in active/standby mode.

- As shown in the left, VRRP cannot ensure symmetric forwarding upon failure on a device, which causes traffic interruption.
- As shown in the right, after the HA control channel is established, the HA group determines the roles of the devices in all VRRP groups. The master election mechanism of VRRP no longer takes effect. If the HA control channel is disconnected, the master election mechanism of VRRP takes effect again.

Figure 3 HA group in collaboration with VRRP



VRRP active/standby group

The HA group is associated with VRRP by VRRP active and standby groups.

A VRRP active/standby group can be in master or backup state, which determines the state of devices in the associated VRRP groups. For example, if a VRRP active group is in master state, all devices in the associated VRRP groups are masters.

The initial state of a VRRP active/standby group is as follows:

- **Active/Standby mode**—On the primary device, the initial state is master for the VRRP active and standby groups. On the secondary device, the initial state is backup for the VRRP active and standby groups.
- **Dual-active mode**—The state of a VRRP active/standby group is not affected by the HA roles. The initial state is master for the VRRP active group and is backup for the VRRP standby group.

VRRP master election in the HA group environment

After the HA group is associated with VRRP, the HA group determines the roles of the devices in the VRRP groups. As shown in Figure 3, Device A is the master in VRRP group 1 and VRRP group 2, and Device B is the backup in VRRP group 1 and VRRP group 2. When Interface A2 on Device A fails, the following events occur:

1. The HA group receives an interface failure event and sends the status change information of the VRRP active and standby groups to Device B.
2. Device B sets its role to master in the VRRP standby group and then becomes the master in VRRP group 1 and VRRP group 2.
3. Device B sends a response to Device A after the master/backup switchover.
4. Device A sets its role to backup in the VRRP active group and then becomes the backup in VRRP group 1 and VRRP group 2.
5. When Interface A2 recovers, the HA group performs another master/backup switchover following the same procedure. Traffic is switched back to Device A after the switchover.

ARP and MAC learning in VRRP

When the members of a VRRP group receive an ARP request for the group's virtual IP address, the master replies with the group's virtual MAC address. This allows the upstream and downstream Layer 2 devices and hosts to learn the virtual MAC address.

HA group in collaboration with routing protocols

Overview

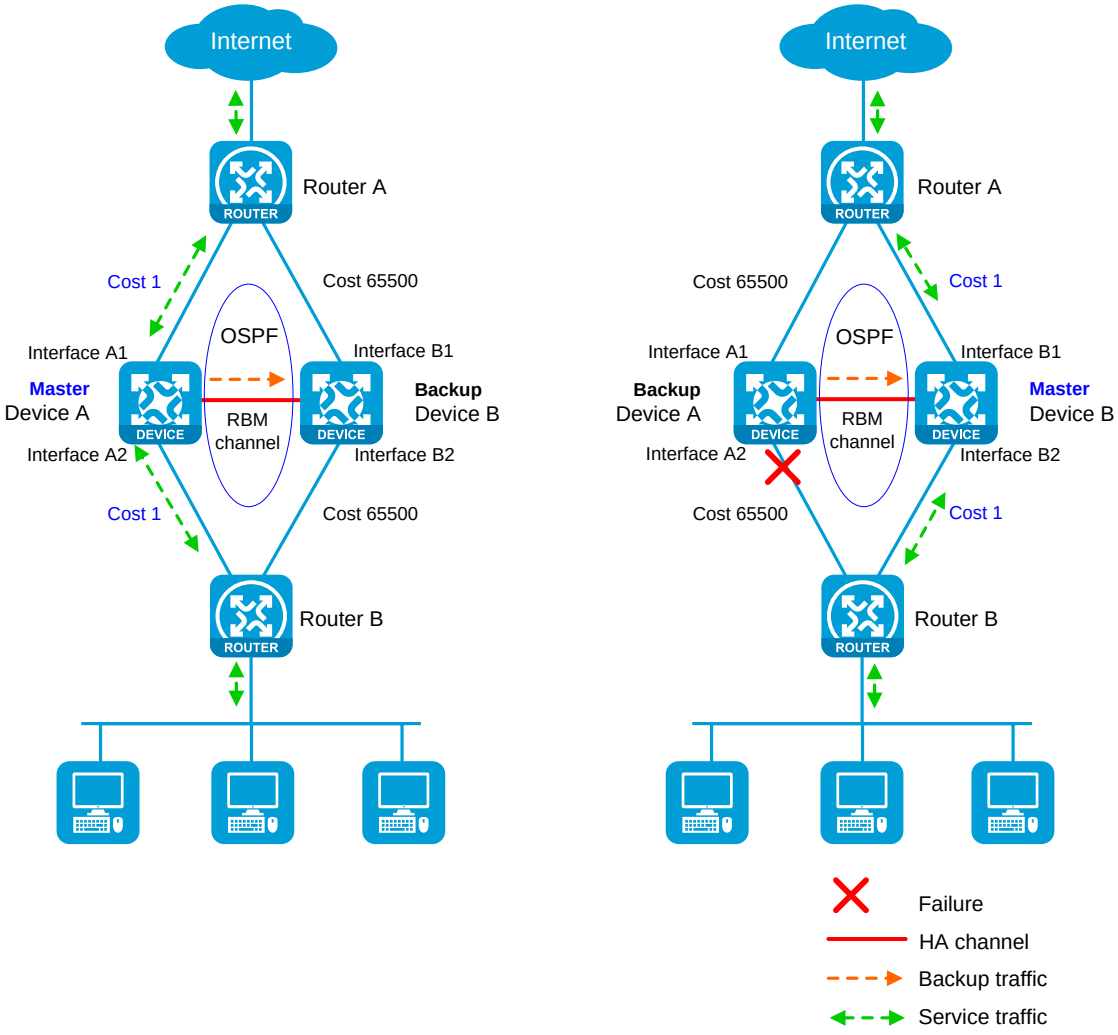
You can use the HA group to enable the routing protocols on the secondary device to advertise modified link cost. The feature ensures that both inbound and outbound traffic can be switched to the new master for symmetric forwarding.

To use the HA group with routing protocols, you must use track entries to monitor the status of uplink and downlink interfaces for the HA group to perform a primary/secondary member switchover when link or interface failure occurs.

The following information uses OSPF on the HA group in active/standby mode to describe how the HA group collaborates with dynamic routing protocols:

- As shown in Figure 4, when both Device A (primary) and Device B (secondary) are operating correctly, Device A advertises the original link cost 1, and Device B advertises the link cost 65500, which has been adjusted by the HA group. As a result, Device A forwards all traffic that traverses the HA group.
- As shown in Figure 4, when downlink Interface A2 of Device A fails, Device A and Device B switch their roles. Then, Device B (primary) advertises the original link cost 1, and Device A (secondary) advertises the adjusted link cost 65500. As a result, Device B forwards all traffic that traverses the HA group.

Figure 4 HA group in collaboration with routing protocols



Mechanism

The HA group adjusts the link costs advertised by dynamic routing protocols by using one of the following methods:

- Replacing the original link cost with the absolute link cost that you configure.
- Adding an increment value to the original link cost.

The link cost changes do not affect the HA roles of devices, and you must configure the same link cost adjustment settings on the primary and secondary member devices.

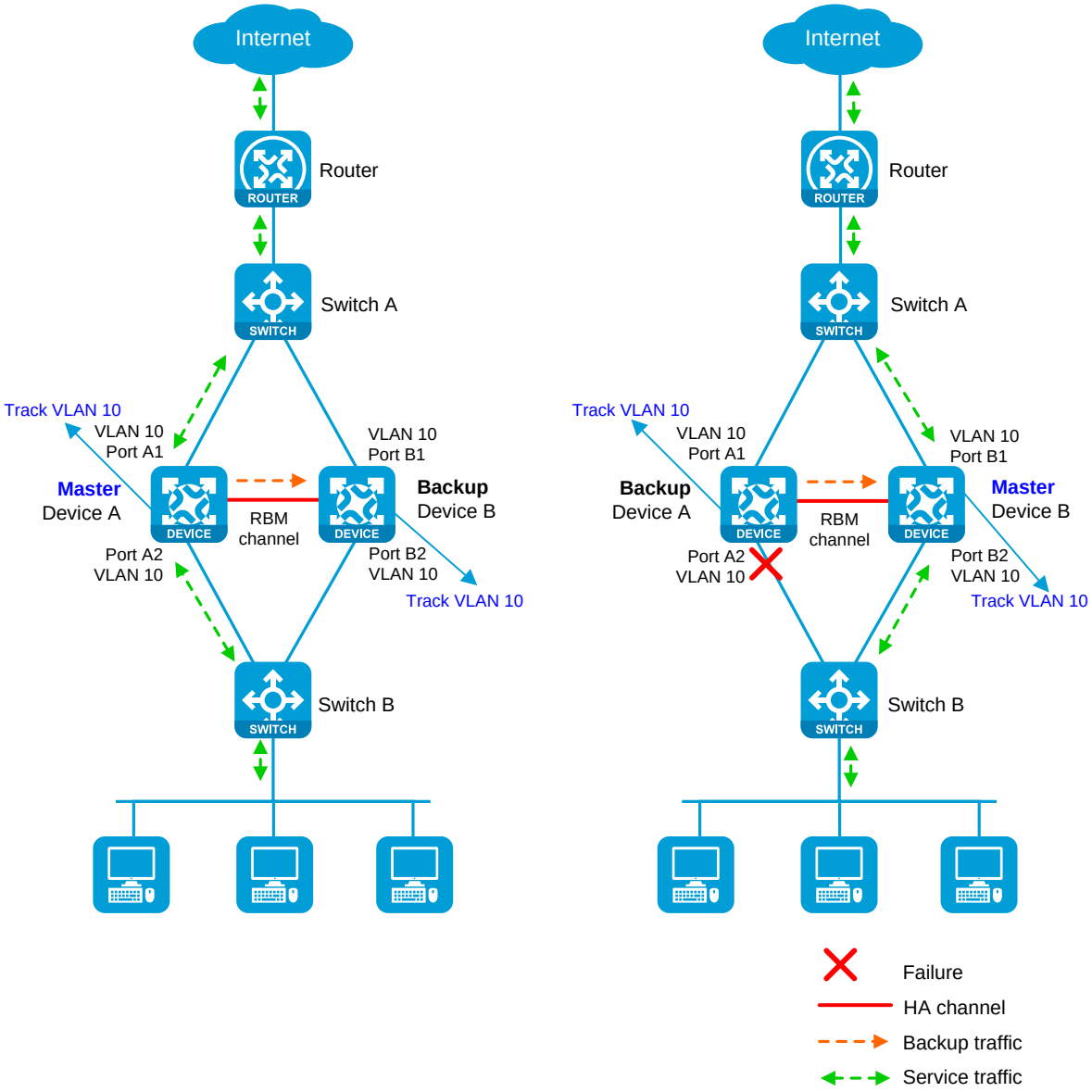
Transparent in-path deployment of the HA group

When you use this networking scheme, you can configure the HA group to monitor interfaces or VLANs to enable collaboration between uplink and downlink interfaces. The monitoring configuration ensures that a group of interfaces have the same status, and uplink and downlink traffic can be switched simultaneously between the member devices.

The following information uses VLAN monitoring as an example to describe how interfaces collaborate:

- As shown in Figure 5, when both Device A (primary) and Device B (secondary) are operating correctly, tracked VLAN 10 is in active state on Device A and in inactive state on Device B. As a result, Device A forwards all traffic that traverses the HA group.
- As shown in Figure 5, when downlink Port A2 of Device A fails, Device A and Device B switch their roles. Then, the HA group places VLAN 10 in inactive state on Device A (secondary) and in active state on Device B (primary). As a result, Device B forwards all traffic that traverses the HA group.

Figure 5 Transparent in-path deployment of the HA group



Restrictions and guidelines

You can use the HA group only with VRRP master/backup mode. VRRP load sharing mode does not support the HA group.

You can configure the HA group to monitor track entries, VLANs, or interfaces, but you cannot configure VLAN monitoring in combination with track entry monitoring or interface monitoring. When you configure the HA group to monitor both track entries and interfaces, make sure the track entries are not associated with the monitored interfaces.

Configure the HA group

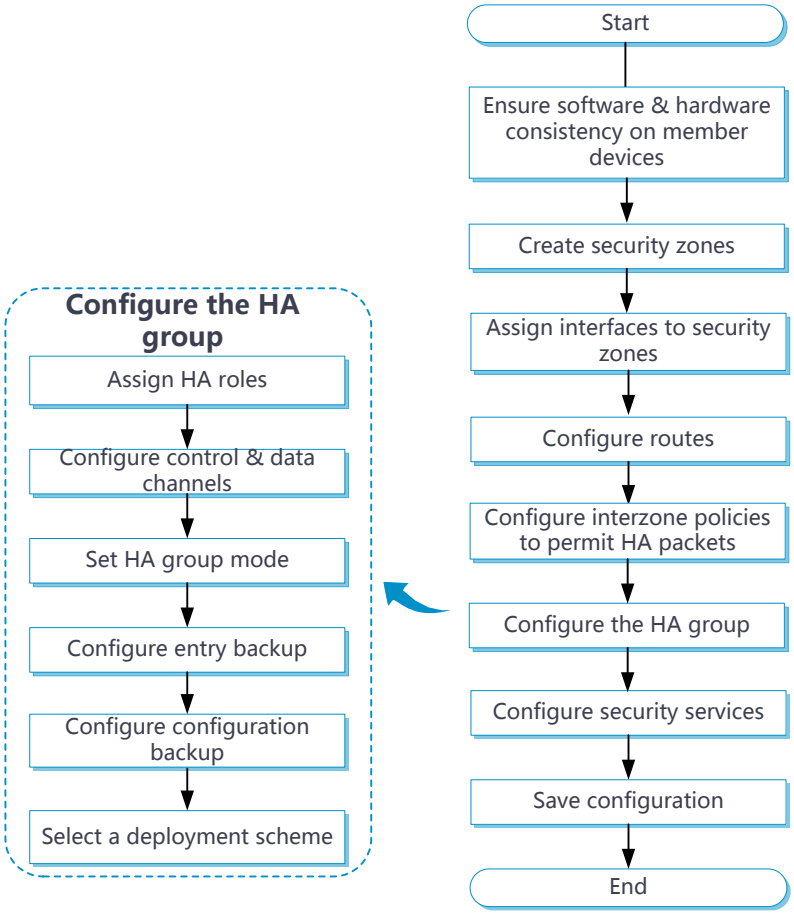
Prerequisites

Before you configure the HA group, verify that the following hardware and software settings are the same on the devices to be assigned to the HA group:

- Device model.
- Software version.
- Interface numbers.
- Interface for setting up the control channel.
- Interface for setting up the data channel.
- Security zone configuration on the interfaces with the same interface number.

HA group configuration flow

Figure 6 HA group configuration flow chart



Configure the HA group

1. Click the **System** tab.
2. In the navigation pane, select **High Availability** > **HA Group**.

   The **HA Group** page opens.
3. Click **Configure**.

   The **Configure HA Group** page opens.

4. Configure the HA group. For more information about the related parameters, see Table 1.

Table 1 HA group parameters

Parameter	Description
HA group	Set the status of the HA group feature.
Operating mode	Set the operating mode of the HA group. • **Active/standby**—The primary device processes services, and the secondary device stands by. • **Dual-active**—Both the primary and secondary devices process services.
Device role	Assign HA roles to the member devices in the HA group.
Local IP	Enter a local IP address to set up the control channel. The server end listens for TCP connection requests at this IP address. You can enter an IPv4 or IPv6 address, but not both.
Peer IP	Enter the peer IP address used for setting up the control channel. You can enter an IPv4 or IPv6 address, but not both.
Peer port	Enter the port number for the control channel. The primary and secondary devices must have the same port number.
Data channel	Select an interface to set up the data channel which transmits backup packets and the packets that require transparent transmission.
Keepalive interval	Set the interval for the device to periodically send keepalive packets to the peer device.
Max keepalive retries	Set the maximum number of keepalive retries. If this limit is reached before the device receives any responses from the peer device, the device disconnects the HA channels to the peer device.
Fallback	Enable this feature for traffic to be switched back to the original primary device upon its recovery.

Parameter	Description
Traffic reversion delay	Set the delay that the primary and secondary devices must wait before a switchback. This delay allows the devices to finish service entry backup to prevent traffic loss.
Back up sessions	Set the status of session backup. If you enable this feature, the primary device backs up service module entries to the secondary device in real time. When the primary device fails, the secondary device can take over without service interruption.
Back up HTTP Back up DNS	Backs up the session entries created for received DNS and HTTP protocol packets. The HA group backs up the sessions created for other application protocols as long as service entry backup is enabled. Enable HTTP and DNS backup if asymmetric-path traffic traverses the HA group. HTTP and DNS backup ensures that a flow and its return traffic are processed correctly on the HA group members. If HA active/standby mode is used or only symmetric-path traffic traverses the HA group, disabling HTTP and DNS backup can improve performance of the HA group members at the expense of delayed data synchronization. When you disable HTTP and DNS backup, make sure you are fully aware of the impact on the network. A device removes a DNS or HTTP connection if packet exchange is inactive. When a switchover interrupts a connection, the DNS or HTTP client re-initiates the connection immediately, which has little impact on user services.
Configuration consistency check	Set the status of the configuration consistency check feature.
Automatic configuration synchronization	Set the status of the automatic configuration synchronization feature. After you enable this feature, the primary device backs up its configuration to the secondary device in bulk. When the configuration on the primary device changes, the primary device backs up the new configuration to the secondary device in real time. If the amount of configuration to be synchronized is large, bulk synchronization might take one to two hours. As a best practice to reduce the bulk synchronization duration, enable this feature when you configure the HA group.

5. Configure Track settings. For more information about the related parameters, see Table 2.

Table 2 Track parameters

Parameter	Description
Track entry association	Select the track entries to be monitored by the HA group. If one of the monitored track entries becomes Negative, the HA group performs a primary/secondary member switchover and switches traffic to the new primary device to ensure service continuity.

6. Click **OK**.

7. Click **Check** or **Synchronize configuration** to check configuration consistency or synchronize configuration on the **HA Group** page.

Table 3 Configuration consistency check and configuration synchronization parameters

Parameter	Description
Check	Perform configuration consistency check manually.
Synchronize configuration	Manually synchronize the configuration of the primary device to the secondary device.

8. Click **Switch states** on the **HA Group** page to switch the HA roles of the devices in the HA group.

Table 4 HA role switchover parameters

Parameter	Description
Switch states	Manually switch the HA roles of the devices in the HA group. You can perform this task when the hardware of the primary device

Parameter	Description
	requires replacement. You can perform this task only on the primary member device when the HA group is operating in active/standby mode. Transient VRRP virtual IP conflicts might occur after you perform this task if VRRP is used with the HA group. The conflicts do not affect services.

Configure VRRP collaboration

Associate the HA group with VRRP on the VRRP page. For more information about the configuration procedure, see VRRP help.

Configure the HA group to collaborate with a routing protocol

1. Click the **System** tab.
2. In the navigation pane, select **High Availability** > **HA Group**.

   The **HA Group** page opens.
3. Click **Configure**.

   The **Configure HA Group** page opens.
4. Configure routing collaboration parameters. For more information about the related parameters, see Table 5.

Table 5 Routing collaboration parameters

Parameter	Description
OSPF	Adjust the link costs advertised by OSPF.

Parameter	Description
IS-IS	Adjust the link costs advertised by IS-IS.
BGP	Adjust the link costs advertised by BGP.
OSPFv3	Adjust the link costs advertised by OSPFv3.
Set absolute cost	Enter an absolute link cost. The HA group will use this value to replace the link costs to be advertised.
Set increment cost	Enter an increment value. The HA group will add this value to the link costs to be advertised.

5. Click **OK**.

Configure transparent in-path deployment

1. Click the **System** tab.
2. In the navigation pane, select **High Availability** > **HA Group**.

   The **HA Group** page opens.
3. Click **Configure**.

   The **Configure HA Group** page opens.
4. Configure monitoring parameters. For more information about the related parameters, see Table 6.

Table 6 Monitoring parameters

Parameter	Description
Interface	Select the interfaces to be monitored by the HA group. You cannot configure the HA group to monitor aggregation

Parameter	Description
	member ports. The HA group monitors the status of the monitored interfaces to ensure interface status consistency. A monitored interface can forward traffic only when all monitored interfaces are up.
VLAN	Select the VLANs to be monitored by the HA group. The HA group monitors the member ports of a monitored VLAN to ensure member port status consistency. A port in a monitored VLAN can forward traffic only when all ports in the VLAN are up. You cannot configure the HA group to monitor VLAN 1. All access ports belong to VLAN 1 by default. If you configure the HA group to monitor VLAN 1, traffic forwarding will be affected on ports in use when an unused port is placed in down state in VLAN 1.

5. Click **OK**.

VRRP

This help contains the following topics:

Introduction

Virtual Router Redundancy Protocol (VRRP) adds a group of network gateways to a VRRP group called a virtual router. The VRRP group has one master and multiple backups, and provides a virtual IP address. The hosts on the subnet use the virtual IP address as their default network gateway to communicate with external networks.

VRRP avoids single points of failure and simplifies the configuration on hosts. When the master in the VRRP group on a multicast or broadcast LAN (for example, an Ethernet network) fails, another device in the VRRP group takes over. The switchover is complete without causing dynamic route recalculation, route re-discovery, gateway reconfiguration on the hosts, or traffic interruption.

VRRP group

VRRP adds a group of network gateways to a VRRP group called a virtual router. The VRRP group has one master and multiple backups.

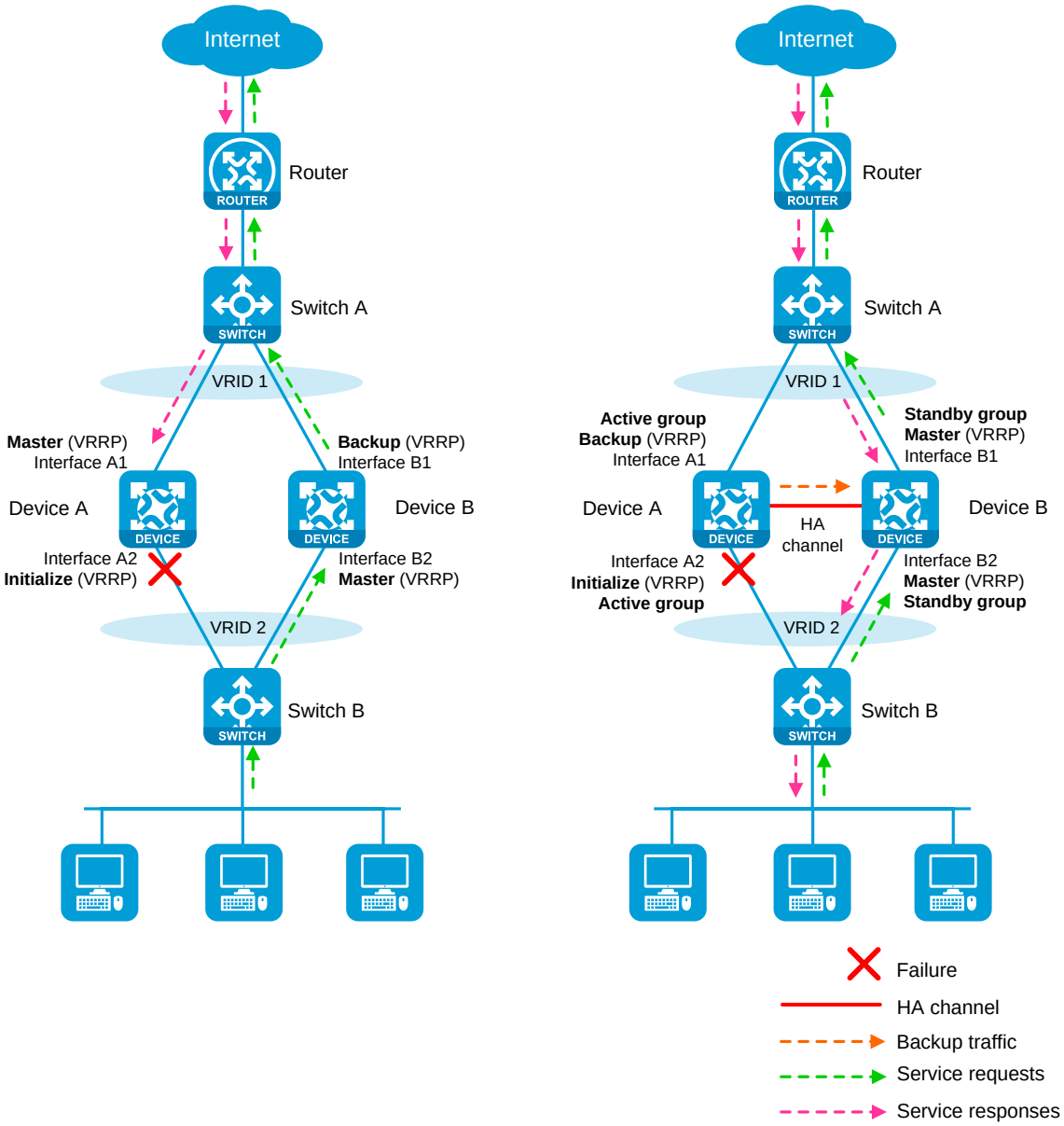
Collaboration with HA group

About collaboration with HA group

Figure 1 shows a typical VRRP network (on the left) and a network configured with VRRP-HA group association (on the right). Upon a link switchover in the typical VRRP network, traffic might be interrupted if the master in uplink and downlink VRRP groups resides on different devices.

To resolve this issue, you can use HA group to control the master/backup state switchover in different VRRP groups.

Figure 1 Network diagram



VRRP active/standby group

A VRRP active/standby group can be in master or backup state, which determines the state of devices in the associated VRRP groups. For example, if a VRRP active group is in master state, all devices in the associated VRRP groups are masters.

The initial state of a VRRP active/standby group is as follows:

- **Active/Standby mode**—On the primary management device, the initial state is master for the VRRP active and standby groups. On the secondary management device, the initial state is backup for the VRRP active and standby groups.
- **Dual-active mode**—The state of a VRRP active/standby group is not affected by the HA roles. The initial state is master for the VRRP active group and is backup for the VRRP standby group.

VRRP master election in the HA group environment

In the network configured with VRRP-HA group association as shown in Figure 1, the master/backup state switchover in the VRRP groups is as follows:

1. Typically, the VRRP active group state is master on Device A (suppose it is the primary device), so Device A is the master in both VRRP group 1 and VRRP group 2. The VRRP standby group state is backup on Device B (suppose it is the secondary device), so Device B is the backup in both VRRP group 1 and VRRP group 2.
2. When Interface A2 (downlink interface on Device A) fails, the HA group receives an interface failure event. The HA group then notifies Device B of the VRRP active/standby group state change event in an update packet, requesting Device B to change the VRRP standby group state to master.
3. Upon receiving the update packet, Device B changes the VRRP standby group state to master. Meantime, Device B changes its state to master in VRRP group 1 and VRRP group 2. After the state change, Device B sends a reply to Device A.
4. Upon receiving the reply, Device A changes the VRRP active group state to backup. Meantime, Device A changes its state to backup in VRRP group 1 and VRRP group 2.

For traffic to switch back when Interface A2 recovers, the devices will perform another master/backup state switchover that is similar to the procedure described above.

Virtual IP address

A VRRP group provides a virtual IP address. The hosts on the subnet use the virtual IP address as their default network gateway to communicate with external networks.

The virtual IP address of the virtual router can be either of the following IP addresses:

- Unused IP address on the subnet where the VRRP group resides.
- IP address of an interface on a device in the VRRP group.

In the latter case, the router is called the IP address owner.

Device priority in a VRRP group

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with higher priority is more likely to become the master.

A VRRP priority can be in the range of 0 to 255, and a greater number represents a higher priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly. A VRRP group can have only one IP address owner.

Preemption

A router in a VRRP group operates in either non-preemptive mode or preemptive mode.

- **Preemptive mode**—A backup starts a new master election and takes over as master when it detects that it has a higher priority than the current master. Preemptive mode ensures that the router with the highest priority in a VRRP group always acts as the master.

- **Non-preemptive mode**—The master router acts as the master as long as it operates correctly, even if a backup router is later assigned a higher priority. Non-preemptive mode helps avoid frequent switchover between the master and backup routers.

You can configure the VRRP preemption delay timer for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

In preemptive mode, a backup does not immediately become the master after it receives an advertisement with priority lower than the local priority. Instead, it waits for a period of time before taking over as the master.

Preemption delay

In preemptive mode, upon receiving an advertisement with priority lower than the local priority, a backup waits for a period of time (preemption delay) before taking over as the master. If the preemption delay is 0, the backup immediately takes over as the master.

VRRP advertisement interval

The master in a VRRP group periodically sends VRRP advertisements to declare its presence.

- As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.
- In VRRPv2, all routers in an IPv4 VRRP group must have the same VRRP advertisement interval.
- In VRRPv3, routers in a VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at specified

intervals, and carries the interval in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a VRRP advertisement before the timer (3 × recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

- A high volume of network traffic might cause a backup to fail to receive VRRP advertisements from the master within the specified time. As a result, an unexpected master switchover occurs. To solve this problem, configure a larger interval.

Authentication method

To avoid attacks from unauthorized users, VRRP members add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication methods:

- **Simple authentication**—The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.
- **MD5 authentication**—The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the packet. The receiver performs the same operation with the authentication key and MD5 algorithm, and compares the result with the content in the authentication header. If the results match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.

On a secure network, you can choose to not authenticate VRRP packets.

VRRP control VLAN

By default, Layer 3 Ethernet subinterfaces on the master with ambiguous VLAN termination configured do not support sending broadcast packets or multicast packets. To allow the master to regularly send VRRP advertisements in multicast to the backups, enable the VLAN termination-enabled subinterfaces to transmit broadcast packets and multicast packets. Then, the master can send VRRP advertisements within all VLANs whose VLAN packets are configured to be terminated by the subinterfaces. If ambiguous VLAN termination is configured on the Layer 3 Ethernet subinterfaces for a large range of VLANs, the VRRP advertisements might overload the subinterfaces. This adversely affects the performance of the routers.

To resolve this problem, you can disable the VLAN termination-enabled subinterfaces from transmitting broadcast packets and multicast packets and configure a VRRP control VLAN. The master sends VRRP advertisements only within the control VLAN.

Specify VRRP control VLANs according to the VLAN termination type.

- For ambiguous Dot1q termination, specify one control VLAN by the outermost layer of VLAN tag.
- For ambiguous QinQ termination, specify two control VLANs by the outermost two layers of VLAN tags.

Restrictions and guidelines

- IPv4 VRRPv3 and IPv6 VRRPv3 do not support VRRP packet authentication.
- You can configure different authentication modes and authentication keys for VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.

Configure VRRP

Configure basic VRRP settings

1. Select **System** > High Availability > VRRP.
2. Click Create.
3. Create a VRRP group.

Table 1 Basic VRRP configuration items

Item	Description
Interface	Specify the interface to where the VRRP group resides.
VRID	Enter a virtual router ID that uniquely identifies a VRRP group. VRRP groups sharing the same VRID on different devices indicate one VRRP group.
IP type	Specify IPv4 or IPv6 VRRP.
Associate with HA Group	Configure this parameter in a VRRP-HA group association scenario to enable collaboration between VRRP groups.
Virtual IP/mask length	Enter the virtual IP addresses of the VRRP group.
Priority	Enter the priority. A higher priority indicates the device is more likely to become the master of the VRRP group.
Preemption mode	Select the preemption mode: preemptive or non-preemptive.
Preemption delay	Enter the preemption delay time. A backup device waits for the specified period of time before it preempts as the master. 0 means the device immediately preempts as the master.

Item	Description
Advertisement interval	Set the VRRP packet advertisement interval. For VRRPv2, the effective value can only be a multiple of 100. For example, if you configure the value as 10 through 100, 101 through 200, or 4001 through 4095, the effective value is 100, 200, or 4100, respectively. For VRRPv3, the configured value takes effect.
Auth mode	Specify the no authentication, simple authentication, or MD5 authentication mode. VRRP validates VRRP packets by adding an authentication key to prevent attacks with forged packets.

Configure advanced VRRP settings

1. Select **System** > High Availability > VRRP Advanced Settings.
2. Click Edit for the target VRRP group.
3. Configure advanced VRRP group settings.

Table 2 Advanced VRRP configuration items

Item	Description
Interface	Specify the interface to which the VRRP group is bound.
Version	Select VRRPv2 or VRRPv3. VRRPv2 supports only IPv4 VRRP. VRRPv3 supports both IPv4 VRRP and IPv6 VRRP. All routers in an IPv4 VRRP group must use the same IPv4 VRRP version.
Control VLAN	Specify the control VLAN for a subinterface configured with ambiguous

Item	Description
	Dot1q termination.
Inner VLAN	Specify the inner VLAN for a subinterface configured with ambiguous QinQ termination.

Track

This help contains the following topics:

Introduction

The Track module works between application modules and detection modules. It shields the differences between various detection modules from application modules.

Collaboration mechanism

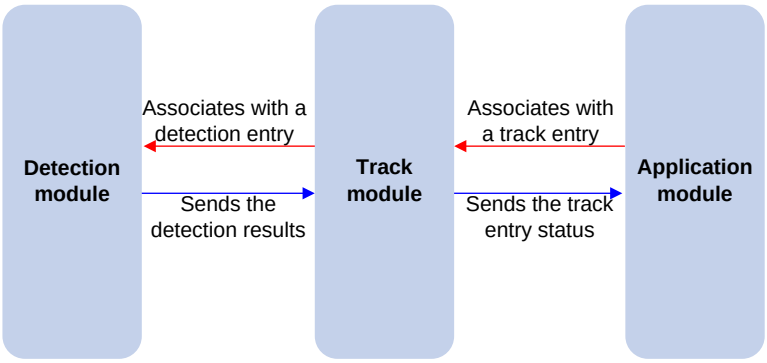
The Track module collaborates with detection modules and application modules.

As shown in Figure 1, collaboration is enabled when you associate the Track module with a detection module and an application module, and it operates as follows:

1. The detection module probes specific objects such as interface status, link status, network reachability, and network performance, and informs the Track module of detection results.
2. The Track module sends the detection results to the application module.

3. When notified of changes for the tracked object, the application modules can react to avoid communication interruption and network performance degradation.

Figure 1 Collaboration through the Track module



Collaboration between the Track module and a detection module

The detection module sends the detection result of the tracked object to the Track module. The Track module changes the status of the track entry as follows:

- If the tracked object operates correctly, the state of the track entry is Positive. For example, the track entry state is Positive in one of the following conditions:
  - The target interface is up.
  - The target network is reachable.
- If the tracked object does not operate correctly, the state of the track entry is Negative. For example, the track entry state is Negative in one of the following conditions:
  - The target interface is down.
  - The target network is unreachable.

If the detection result is invalid, the state of the track entry is NotReady. For example, the track entry state is NotReady if its associated NQA operation does not exist.

Collaboration between the Track module and an application module

The track module reports the track entry status changes to the application module. The application module can then take correct actions to avoid communication interruption and network performance degradation

Configure Track

1. Select **System** > **High Availability** > **Track**.
2. Click **Add**.
3. Create a track entry.

Table 1 Basic Track configuration items

Item	Description
Track entry	Enter the track entry ID that uniquely identifies a track entry.
Detection module	Select a detection module to be associated with Track.
Positive notification delay	Specifies the delay for notifying the application module that the track entry state has changed to Positive. If the Track module immediately notifies the application module of a track entry state change but the route convergence is not complete, a communication failure might occur. In such cases, you can set a notification delay to avoid immediate notification of track entry state changes. The notification delay settings do not take effect if the track entry is not

Item	Description
	associated with an application module.
Negative notification delay	Specifies the delay for notifying the application module that the track entry state has changed to Negative. If the Track module immediately notifies the application module of a track entry state change but the route convergence is not complete, a communication failure might occur. In such cases, you can set a notification delay to avoid immediate notification of track entry state changes. The notification delay settings do not take effect if the track entry is not associated with an application module.

Table 2 Track-BFD association configuration items

Item	Description
BFD packet output interface	Select an interface to send BFD echo packets. Track can be associated with only echo-mode BFD sessions.
Local IP	Enter the local IP address of the BFD session.
Remote IP	Enter the remote IP address of the BFD session.

Table 3 Track-NQA association configuration items

Item	Description
NQA operation administrator	Enter the name of the NQA operation administrator who creates the NQA operation.
Operation tag	Enter the NQA operation tag.
Sequence number	Enter the ID of the reaction entry to be associated with the track entry.

Table 4 Track-interface association configuration items

Item	Description
Monitored interface	Select an interface to be associated with Track.
Monitored interface attribute	Select an interface attribute, which can be physical state, data link layer state, IPv4, or IPv6.

Table 5 Track-route association configuration items

Item	Description
VPN instance	Select the VPN instance for the route to be associated with Track.
IP	Enter the IP address of the route entry, in dotted decimal notation.
Mask length	Enter the mask length of the IP address.

BFD

Introduction

Bidirectional forwarding detection (BFD) provides a general-purpose, standard, medium- and protocol-independent fast failure detection mechanism. It can detect and monitor the connectivity of forwarding paths to detect communication failures quickly so that measures can be taken to ensure service continuity and enhance network availability.

BFD can uniformly and quickly detect the failures of the bidirectional forwarding paths between two devices for upper-layer protocols such as routing protocols. The hello mechanism used by upper-layer protocols needs seconds to detect a link failure, while BFD can provide detection measured in milliseconds.

BFD sessions use echo packets to implement detection. Echo packets are encapsulated into UDP packets with port number 3785.

The local end of the link sends echo packets to establish BFD sessions and monitor link status. The peer end does not establish BFD sessions and only forwards the packets back to the originating end. If the local end does not receive echo packets from the peer end within the detection time, it considers the session to be down.

Configure BFD

1. Select **System** > **High Availability** > **BFD**.
2. Configure BFD.

Table 1 BFD configuration items

Item	Description
Echo packet source IPv4	Specify a source IPv4 address for echo packets. As a best practice, specify an IPv4 address that is not on the same network segment as any local interface's IP address. This behavior prevents the peer from sending a large number of ICMP redirect packets, which will result in link congestion.
Echo packet source IPv6	Specify a source IPv6 address for echo packets. As a best practice, specify an IPv6 address that is not on the same network segment as any local interface's IP address. This behavior prevents the peer from sending a large number of ICMPv6 redirect packets, which will result in link congestion.

NQA

Introduction

NQA

Network quality analyzer (NQA) allows you to measure network performance, verify the service levels for IP services and applications, and troubleshoot network problems.

NQA operating mechanism

As shown in Figure 1, the NQA source device (NQA client) sends data to the NQA destination device by simulating IP services and applications to measure network performance.

All types of NQA operations require the NQA client, but only the TCP operations require the NQA server. The NQA operations for services that are already provided by the destination device such as FTP do not need the NQA server. You can configure the NQA server to listen and respond to specific IP addresses and ports to meet various test needs.

Figure 1 Network diagram

Collaboration with Track

NQA can collaborate with the Track module to notify application modules of state or performance changes so that the application modules can take predefined actions. For more information about Track, see the Track help.

Threshold monitoring

Threshold monitoring enables the NQA client to take a predefined action when the NQA operation performance metrics violate the specified thresholds.

Configure NQA

To configure NQA:

1. Click the **System** tab.
2. In the navigation pane, select **High Availability** > **NQA**.
3. Click **Add**.
4. Configure an NQA operation.

Table 1 NQA operation configuration items

Item	Description
NQA operation administrator	Enter the administrator name of the NQA operation. An nQA operation is identified by an administrator name and operation tag.
Operation tag	Enter an NQA operation tag.
Probe mode	Select a probe mode. NQA supports using packets of different protocols for link detection.
Destination IP	Enter the destination IP address for probe packets.
Destination port	Enter the destination port number for probe packets.
Probe interval	Set the interval at which the NQA operation repeats. If you set the interval to 0, NQA performs the operation only once and does not generate any statistics.
Probe times	Specify the probe times. If an operation is to perform multiple probes, the NQA client starts a new probe in one of the following conditions: • The NQA client receives responses to packets sent in the last probe. • The probe timeout time expires.
Probe timeout	Set the timeout time for waiting for a response.
Save history records	Enable the saving of history records for the NQA operation. If you disable this feature, the device removes existing history records of the NQA operation and does not save history records any more.
Max history records	Set the maximum number of history records that can be saved for an NQA operation. If the number of history records for an NQA operation exceeds the maximum number, earliest history records are removed.
Starting time	Configure the start time of the NQA operation: • **Immediately**—The NQA operation starts immediately after the

Item	Description
	configuration is deployed. • **Scheduled time**—The NQA operation starts at the scheduled time.
Operation duration	Configure the operation duration: • **Permanent**—The device indefinitely repeats the NQA operation. • **Specified duration**—The device repeats the NQA operation during the duration.

Table 2 NQA threshold monitoring configuration items

Item	Description
Reaction entry ID	Enter the ID of the reaction entry.
Monitored element	Select a monitored element. • **probe-duration**—Duration of the probe. • **probe-fail**—Number of probe failures.
Threshold type	Select a threshold type. • **Accumulate**—Checks the total number of threshold violations. • **Consecutive**—Checks the number of consecutive threshold violations after the NQA operation starts.
Probe failures	Set the number of probe failures to determine an operation failure.
Threshold value range	Enter a threshold value range.
Triggered action	Select a triggered action: • **None**—Records the monitoring results locally. • **Trap-only**—Records the monitoring results and sends SNMP trap messages to the NMS. If you select this action, you must

Item	Description
	configure the trap message receiver host on the **System** > **Maintenance** > **SNMP** page. • **Trigger-only**—Records the monitoring results locally and triggers the collaboration with other modules.

Basic log settings

This help contains the following topics:

Introduction

The device generates various types of logs for service modules based on the packets processed by the service modules. These logs help network administrators monitor network performance,

troubleshoot network problems, as well as track, record, analyze, and audit network access behaviors of users.

The device supports outputting logs by using the following methods:

- Syslog.
- Flow log.
- Fast log output.

Syslog

Syslog entries are in ASCII format.

The information center on the device receives syslog messages generated by source modules and outputs the logs to the following destinations:

- Console.
- Monitor terminal.
- Log buffer.
- Log host.
- Log file.

Flow log

About flow log

Flow log records users' access to external networks based on flows. Each flow is identified by a 5-tuple of the source IP address, destination IP address, source port, destination port, and protocol number.

Flow log creates entries based on NAT sessions.

Flow log versions

Flow log has three versions: version 1.0, version 3.0, and version 5.0. Table 1, Table 2, and Table 3 show the fields available in the versions. The fields displayed on your device might differ from those listed in the tables depending the log analysis tool you have used.

Table 1 Flow log 1.0 fields

Field	Description
SrcIP	Source IP address before NAT.
DestIP	Destination IP address before NAT.
SrcPort	Source TCP/UDP port number before NAT.
DestPort	Destination TCP/UDP port number before NAT.
StartTime	Start time of the flow, in seconds.
EndTime	End time of the flow, in seconds. This field is 0 if the **Operator** field is **6** (regular connectivity check record for the active flow).
Protocol	Protocol number.
Operator	Reasons why a flow log entry was generated: • **0**—Reserved. • **1**—Flow was ended normally. • **2**—Flow was aged out because of aging timer expiration. • **3**—Flow was aged out because of configuration change or manual deletion. • **4**—Flow was aged out because of insufficient resources.

Field	Description
	• **5**—Reserved. • **6**—Regular connectivity check record for the active flow. • **7**—Flow was deleted because a new flow was created when the flow table was full. • **8**—Flow was created. • **FE**—Other reasons. • **10-FE-1**—Reserved for future use.
Reserved	Reserved for future use.

Table 2 Flow log 3.0 fields

Field	Description
Protocol	Protocol number.
Operator	Reasons why a flow log was generated: • **0**—Reserved. • **1**—Flow was ended normally. • **2**—Flow was aged out because of aging timer expiration**.** • **3**—Flow was aged out because of configuration change. • **4**—Flow was aged out because of insufficient resources. • **5**—Reserved. • **6**—Regular connectivity check record for the active flow. • **7**—Flow was deleted because a new flow was created when the flow table was full. • **8**—Flow was created. • **FE**—Other reasons. • **10-FE-1**—Reserved for future use.

Field	Description
IPVersion	IP packet version.
TosIPv4	ToS field of the IPv4 packet.
SourceIP	Source IP address before NAT.
SrcNatIP	Source IP address after NAT.
DestIP	Destination IP address before NAT.
DestNatIP	Destination IP address after NAT.
SrcPort	Source TCP/UDP port number before NAT.
SrcNatPort	Source TCP/UDP port number after NAT.
DestPort	Destination TCP/UDP port number before NAT.
DestNatPort	Destination TCP/UDP port number after NAT.
StartTime	Start time of the flow, in seconds.
EndTime	End time of the flow, in seconds. This field is 0 when the **Operator** field is **6** (regular connectivity check record for the active flow).
InTotalPkg	Number of packets received for the session.
InTotalByte	Number of bytes received for the session.
OutTotalPkg	Number of packets sent for the session.
OutTotalByte	Number of bytes sent for the session.
InVPNID	ID of the source VPN instance.
OutVPNID	ID of the destination VPN instance.

Field	Description
Reserved1	Reserved field.
AppID	Application protocol ID.
Reserved3	Reserved field.

Table 3 Flow log 5.0 fields

Field	Description
Protocol	Protocol number.
Operator	• Reasons why a flow log was generated: • **0**—Reserved. • **1**—Flow was ended normally. • **2**—Flow was aged out because of aging timer expiration**.** • **3**—Flow was aged out because of configuration change. • **4**—Flow was aged out because of insufficient resources. • **5**—Reserved. • **6**—Regular connectivity check record for the active flow. • **7**—Flow was deleted because a new flow was created when the flow table was full. • **8**—Flow was created. • **FE**—Other reasons. • **10-FE-1**—Reserved for future use.
IPVersion	IP packet version.
TosIPv4	ToS field of the IPv4 packet.
SourceIP	Source IP address before NAT.

Field	Description
SrcNatIP	Source IP address after NAT.
DestIP	Destination IP address before NAT.
DestNatIP	Destination IP address after NAT.
SrcPort	Source TCP/UDP port number before NAT.
SrcNatPort	Source TCP/UDP port number after NAT.
DestPort	Destination TCP/UDP port number before NAT.
DestNatPort	Destination TCP/UDP port number after NAT.
StartTime	Start time of the flow, in seconds.
EndTime	End time of the flow, in seconds. This field is 0 when the **Operator** field is **6** (regular connectivity check record for the active flow).
InTotalPkg	Number of packets received for the session.
InTotalByte	Number of bytes received for the session.
OutTotalPkg	Number of packets sent for the session.
OutTotalByte	Number of bytes sent for the session.
InVPNID	ID of the source VPN instance.
OutVPNID	ID of the destination VPN instance.
AppID	Application protocol ID.
UserName	Username.
Reserved1	Reserved fields.

Field	Description
Reserved2 Reserved3	

Fast log

The fast log output feature enables fast output of logs to log hosts.

Typically, logs generated by a service module are first sent to the information center, which then outputs the logs to the specified destination (such as to log hosts). When fast log output is configured, logs of service modules are sent directly to log hosts instead of to the information center. Compared to outputting logs to the information center, fast log output saves system resources.

Storage space settings

The device collects log data from service modules for central analysis and reporting.

The collected log data are preferably stored in a hard disk. If a hard disk is not present, the data are stored in a U disk. If a U disk is not present either, the data are stored in the memory. Support for storing the log data in a U disk depends on the device model.

The storage space settings feature allows you to set the storage time limit, storage space limit, and the storage limit-violated action for the traffic service and DPI services.

Before you remove a storage device, complete the following to avoid damaging the storage device or the stored data:

- From the Web interface, click **Unload** to remove the occupation of the service log processes on the file systems of the storage device.
- From the CLI, execute the **`umount`** command in user view to unmount all the file systems on the storage device.

Support for storage space settings depends on the device model.

Storage time limit

The storage time limit specifies the maximum number of days that the log data can be kept.

Processing of expired log data varies by the specified action:

- If the action is **Delete**, the system will delete the expired log data and generate a log message to record the event.
- If the action is **Log-only**, the system will generate a log message, but it does not delete the expired data.

Storage space limit

The storage space limit specifies the percentage of the total storage space the log data of a service can occupy.

Processing of the log data for a service whose storage space limit is exceeded varies by the specified action:

- If the action is **Delete**, the system will delete the oldest log data to save new data. A log message will be generated to record the event.
- If the action is **Log-only**, the system will generate a log message, but it does not delete old log data to save new data.

Action

The action specified for a storage limit of a service determines how the system processes the log data of the service when the storage limit is exceeded.

Supported actions are:

- **Delete**—Deletes data collected on the oldest dates and generates a log message. The data of the current day cannot be deleted.
- **Log-only**—Generates a log message only. When a storage limit is exceeded, old data are not deleted and new data cannot be saved. To view the log data, go to **Monitor** > **Device Logs** > **System Logs**.

Log severity levels

Logs are classified into eight severity levels from 0 through 7 in descending order. If you specify a severity level for log output, logs with a severity level that is higher than or equal to the specified level will be output. For example, if you specify a severity level of 6 (informational), logs that have a severity level from 0 to 6 are output.

Table 4 Log severity levels

Severity value	Level	Description
0	Emergency	The system is unusable. For example, the system authorization has expired.
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power

Severity value	Level	Description
		module fails, or the fan tray fails.
3	Error	Error condition. For example, the link state changes.
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.
5	Notification	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.
6	Informational	Informational message. For example, a command or a ping operation is executed.
7	Debugging	Debugging message.

Security management and audit

The security management feature enables the security management service process on the device. If this feature is disabled, you cannot manage or audit the security services on the device through the security management server.

The security audit log feature enables the device to log security-related configurations and report the log messages to the security audit server. The log messages mainly include the syslog messages generated for operations on the administrator, system, and security-related policies.

Support for the security management and audit features depends on the device model.

Restrictions and guidelines

The device supports the following methods (in descending order of priority) for outputting logs of a module to designated log hosts:

- Fast log output.
- Flow log output.
- Syslog output.

If you configure multiple log output methods for a module, only the method with the highest priority takes effect.

Configure basic log settings

Configure syslog

1. Click the **System** tab.
2. In the navigation pane, select **Log Settings** > **Basic Settings**.
3. Click the **Syslog** tab.
4. Configure the basic syslog settings.

Table 5 Syslog configuration items

Item	Description
Output to log buffer	Select this item to enable system log output to the log buffer. This item enables system log output to log buffers based on the log source modules.

Item	Description
	• Logs generated by modules that have separate log buffers are saved to their respective log buffers. For example, session logs and attack defense logs are saved to the session log buffer and the attack defense log buffer, respectively. • Logs generated by other modules are saved to the general log buffer.
Log buffer size	Enter the maximum number of logs that can be buffered. When the log buffer is full, the system will overwrite the oldest logs with new logs. This item specifies the size of the general log buffer.

5. Click **Apply**.
6. Click **Create**.

   The **Create Log Host** window opens.
7. Create a log host.

Table 6 Log host configuration items

Item	Description
Log host address	Enter the IP address or host name of the log host.
Port number	Enter the port number of the log host.
VRF	Select the VRF (VPN instance) to which the log host belongs. If the log host belongs to the public network, select **Public network**.

8. Click **OK**.

   The new log host is displayed on the log host list of the **Syslog** tab.

Configure flow log

1. Click the **System** tab.
2. In the navigation pane, select **Log Settings** > **Basic Settings**.
3. Click the **Flow Log** tab.
4. Configure the basic flow log settings.

Table 7 Flow log configuration items

Item	Description
Log version	Select a flow log version. Options are **1.0**, **3.0**, and **5.0**. Make sure the specified flow log version is supported on the log hosts specified for flow log export.
Load balancing	Select this item to enable load balancing for flow log entries. By default, load balancing is disabled. The device sends a copy of each flow log entry to all available log hosts. In load balancing mode, flow log entries are distributed among log hosts based on the source IP addresses (before NAT) that are recorded in the entries. The flow log entries generated for the same source IP address are sent to the same log host. If a log host goes down, the flow logs sent to it will be lost.
Source IP for log packets	Specify the source IP address for the flow log packets. By default, the source IP address of flow log packets is the IP address of their outgoing interface. Configure this item when you need to filter flow logs by source IP address on the log host. As a best practice, use a Loopback interface's address as the source IP address for flow log packets. A Loopback interface is always up. The setting avoids export failure on interfaces that might go down.

5. Click **Apply**.

6. Click **Create**.

   The **Create Log Host** window opens.

Table 8 Log host configuration items

Item	Description
Log host address	Enter the IP address or host name of the log host.
Port number	Enter the port number of the log host.
VRF	Select the VPN instance to which the log host belongs. If the log host belongs to the public network, select **Public network**.

7. Click **OK**.

   The new log host is displayed on the log host list of the **Flow Log** tab.

Configure fast log output

1. Click the **System** tab.
2. In the navigation pane, select **Log Settings** > **Basic Settings**.
3. Click the **Fast Log Output** tab.
4. Configure the fast log output settings.

Table 9 Fast log output configuration items

Item	Description
Log timestamp	Select the time zone to use in the log timestamp. Options are:

Item	Description
	• **Greenwich Mean Time (GMT)**—Standard Greenwich Mean Time (GMT). • **Local time**—Standard GMT plus or minus the time zone offset.
Source IP for log packets	Select a source interface for fast log output. The primary IP address of the specified interface is used as the source IP address of fast output logs regardless of the outgoing interface. By default, the source IP address of fast output logs is the primary IP address of the outgoing interface. Configure this item when you need to filter logs by source IP address on the log host. As a best practice, use a Loopback interface's address as the source IP address for fast log output. A Loopback interface is always up. The setting avoids export failure on interfaces that might go down.

5. Click **Apply**.
6. Click **Create**.

   The **Create Log Host** window opens.

Table 10 Log host configuration items

Item	Description
Log host address	Enter the IP address or host name of the log host.
Port number	Enter the port number of the log host.
VRF	Select the VPN instance to which the log host belongs. If the log host belongs to the public network, select **Public network**.
Session logs	Select this item to enable fast output of session logs to the log host.

Item	Description
NAT logs	Select this item to enable fast output of NAT logs to the log host.
Log format	This item is available only when the NAT logs item is selected. Select a log output format. Options are **China Unicom**, **China Telecom**, and **CMCC**.
NAT session logs	This item is available only when the NAT logs item is selected. Select this item to enable fast output of NAT session logs to the log host.
NAT444 user logs	This item is available only when the NAT logs item is selected. Select this item to enable fast output of NAT444 user logs to the log host.
AFT logs	Select this item to enable fast output of AFT port block logs to the log host.
Application audit logs	Select this item to enable fast output of application audit logs to the log host.
URL filtering logs	Select this item to enable fast output of URL filtering logs to the log host.
Attack defense logs	Select this item to enable output of attack defense logs to the log host.
Netshare logs	Select this item to enable fast output of netshare control logs to the log host.
Security policy logs	Select this item to enable fast output of security policy configuration logs to the log host.
Heartbeat logs	Select this item to enable fast output of heartbeat logs to the log host.
IPS logs	Select this item to enable fast output of IPS logs to the log host.
Bandwidth management logs	Select this item to enable fast output of bandwidth management logs to the log host.
Sandbox logs	Select this item to enable fast output of sandbox logs to the log host.

Item	Description
LB logs	Select this item to enable fast output of load balancing logs to the log host. LB logs include inbound link LB logs logs.
Terminal identification logging	Select this item to enable fast output of terminal identification logs to the log host.
Anti-virus logs	Select this item to enable fast output of anti-virus logs to the log host.
External authentication logs	Select this item to enable fast output of external authentication logs to the log host.
Notification logs	Select this item to enable fast output of policy notification logs to the log host.

7. Click **OK**.

   The new log host is displayed on the log host list of the **Fast Log Output** tab.

Configure storage space settings

1. Click the **System** tab.
2. In the navigation pane, select **Log Settings** > **Basic Settings**.
3. Click the **Storage Space Settings** tab.
4. Click the **Edit** icon for a service, and then configure the storage space settings for the service.

Table 11 Storage space configuration items

Item	Description
Service	Name of the service for which you can configure storage space limit settings.
Max storage days	Specify the maximum number of days that the log data can be kept. This item is available only when a hard disk or U disk is present.
Max storage space	Specify the percentage of the total storage space the log data of the service can occupy. This item is available only when a hard disk or U disk is present.
Action	Specify the action to take when the storage time limit or storage space limit of the service is exceeded. This item is available only when a hard disk or U disk is present.
Enable	Enable logging for the service.

5. Click **OK**.

Configure security management and audit

1. Click the **System** tab.
2. In the navigation pane, select **Log Settings** > **Basic Settings**.
3. Click the **Security Management&Audit** tab.

Table 12 Security management and audit configuration items

Item	Description
Security management	After this feature is enabled, the device opens the security management service process.
Send security audit logs	After this feature is enabled, the device records security audit related log messages and reports the log messages to the security audit server.
Security audit server IP	Specify the IPv4 address of the security audit server.
Security audit server port	Specify the port number on which the security audit server receives security audit log messages.

4. Click **Apply**.
5. To export the device's security management service configuration file to the local device, click **Export**.

Email server

This help contains the following topics:

- Introduction
- Configure the email server

Introduction

If you want to output logs through email, you must configure an email server. Then, logs can be sent to email recipients.

Configure the email server

1. Click the **System** tab.
2. In the navigation pane, select **Log Settings** > **Email Server**.
3. Click **Create**.
4. Configure the email server settings.

Table 1 Email server configuration items

Item	Description
Email server name	Enter the name of the email server.

Item	Description
Email server address	Enter the IP address or host name of the email server.
Sender address	Enter the email sender address.
Recipient addresses	• Enter a colon-separated list of email recipient addresses.
DNS server address	Enter the IP address of the DNS server.
Identity authentication	Select **Enable** to enable email client authentication. Enable this function if identity authentication is required by the email server.
Secure user info transmission	Select this item to enable secure transmission of user authentication credentials.
Username	Enter the username for logging in to the email server.
Password	Enter the password for logging in to the email server.
Email sending interval	Enter an interval for sending emails. The device caches the emails to be sent and sends them only when the interval expires.
Max. emails per interval	Specify the maximum number of emails to be sent per interval. If the maximum number is reached within the sending interval and more emails are generated to send, the device compares the severity levels of the new emails and the existing emails. If the severity level of a new email is higher than that of an existing cached email, the new one overwrites the most recent email with the lowest severity level. The severity level of an email is the severity level of the matching IPS signature of the log. When multiple service modules are operating concurrently, this setting takes effect separately on each service module.

5. Click **OK**.

Session log settings

Introduction

Session logs provide information about user access, IP address translation, and network traffic for security auditing. They can be output in flow log or fast log output format.

The device supports time-based or traffic-based logging:

- **Time-based logging**—The device outputs session logs regularly.
- **Traffic-based logging**—The device outputs a session log when the traffic amount of a session reaches a threshold.

If you set both time-based and traffic-based logging, the device outputs a session log when whichever is reached. After outputting a session log, the device resets the traffic counter and restarts the interval for the session.

Session logs can be generated only when session logging is enabled on interfaces.

Configure session log settings

Procedure

1. Click the **System** tab.
2. Select **Log Settings** > **Session Log Settings**.
3. Configure session logging.

Table 1 Session logging configuration items

Item	Description
Log type	Select a log type. By default, flow log is used.
Session creation logging	This feature enables the device to output a session log when a session entry is created.
Session deletion logging	This feature enables the device to output a session log when a session entry is removed.
Traffic-based logging	Set either the byte-based threshold or the packet-based threshold. The device outputs a session log when the traffic amount of a session reaches the set threshold.
Time-based logging	Set the time-based threshold for the device to output session logs.

4. Click **Apply**.

5. Click **Add interface** to enable session logging on the specified interface.

Table 2 Configuration items for enabling session logging on an interface

Item	Description
IP version	Select an IP version, IPv4 or IPv6.
Port	Select a port. You can also enable session logging on the specified directions of the port.
ACL	Select an ACL to filter IPv4 or IPv6 sessions that can trigger session logging on the interface. If no ACL is specified, the device outputs session logs for all IPv4 or IPv6 sessions on the interface.

6. Click **OK**.

7. Verify the configuration on the **Session Logging** page.

NAT log settings

Introduction

NAT session log settings

NAT session logging records NAT session information, including translation information and access information. NAT session logs can be output in flow logs or fast logs. By default, NAT session logs are output in flow logs.

The device generates NAT session logs for the following events:

- NAT session establishment.
- NAT session removal. This event occurs when you add a configuration with a higher priority, remove a configuration, change ACLs, when a NAT session ages out, or when you manually delete a NAT session.
- Active NAT session logging.

NAT444 log settings

NAT444 logs are used for user tracing. The NAT444 gateway generates a user log whenever it assigns or withdraws a port block. The log includes the private IP address, public IP address, and port block. You can use the public IP address and port numbers to locate the user's private IP address from the user logs. NAT444 logs can be output only in fast logs.

A NAT444 gateway generates NAT444 logs when one of the following events occurs:

- A port block is assigned.

  For the NAT444 static port block mapping, the NAT444 gateway generates a user log when it translates the first connection from a private IP address.

  For the NAT444 dynamic port block mapping, the NAT444 gateway generates a user log when it assigns or extends a port block for a private IP address.

- A port block is withdrawn.

  For the NAT444 static port block mapping, the NAT444 gateway generates a user log when all connections from a private IP address are disconnected.

  For the NAT444 dynamic port block mapping, the NAT444 gateway generates a user log when all the following conditions are met:

  - All connections from a private IP address are disconnected.
  - The port blocks (including the extended ones) assigned to the private IP address are withdrawn.
  - The corresponding mapping entry is deleted.

NAT resources exhaustion log settings

After you enable NAT resource exhaustion logging, the device outputs logs when the NAT resources run out. In NO-PAT, the NAT resources refer to the public IP addresses. In EIM PAT, the NAT resources refer to public IP addresses and ports. In NAT444, the NAT resources refer to public IP addresses, port blocks, or ports in port blocks. To enable the device to generate logs about NAT444 resource exhaustion events, enable fast log output in conjunction with this feature.

AFT log settings

Introduction

AFT session log settings

For security auditing, you can configure AFT logging to record AFT session information. AFT sessions refer to the sessions whose source and destination addresses have been translated by AFT.

AFT session logs can be output only in flow logs. AFT can log the creation and deletion events of AFT sessions.

Port block log settings

If a port block size is specified for a dynamic translation policy in PAT mode, AFT generates a port block log when an AFT session is created or deleted.

Port block logs can be output in system logs or fast logs. By default, port block logs are output in system logs.

Sandbox log settings

Introduction

The sandbox logs record the sandbox inspection results. The sandbox logs support only fast log output.

Threat log settings

This help contains the following topics:

- Introduction
  - IPS log settings
  - Anti-virus log settings
- Restrictions and guidelines

Introduction

Threat logs record detected network attack behaviors. Threat logs can be classified into IPS logs and anti-virus logs.

IPS log settings

IPS logs can be output as system logs to the information center, as fast logs to designated log hosts, or be output to designated email recipients through email.

IPS logs can be output as fast logs in either of the following formats:

- Standard.
- SGCC.

  Only IPS alarm logs and signature update logs can be output in SGCC format. You can set the daily log output time for signature update logs in SGCC format.

  Support for the SGCC format depends on the device model.

Anti-virus log settings

Anti-virus logs can be output as system logs to the information center, as fast logs to designated log hosts, or be output to designated email recipients via email.

Restrictions and guidelines

IPS logs can be output in Chinese. If you select Chinese for outputting IPS logs, the attack name, attack category, and attack subcategory fields of an IPS log message are displayed in Chinese.

Application audit log settings

Introduction

Application audit logs record the Internet access behaviors of users. Application audit logs can be output as system logs or fast logs. By default, application audit logs are output as fast logs.

NetShare log settings

This help contains the following topics:

Introduction

NetShare logs record network sharing behaviors. NetShare log output supports system log output and fast log output. By default, NetShare logs are output as system logs.

URL filtering log settings

This help contains the following topics:

Introduction

URL filtering logs record the website access behaviors of users.

URL filtering logs can be output as system logs or fast logs. By default, URL filtering logs are output as system logs.

When you select the Fast log output option, the Non-standard format option is displayed, which allows you to specify a carrier-customized format (Unicom) for fast log output. By default, fast logs are output in the standard format.

Attack defense log settings

Introduction

Attack defense logs can be output in system logs or fast logs. By default, attack defense logs are output in system logs.

Log aggregation for single-packet attack events

When you enable logging for single-packet attacks, the device generates logs when it detects single-packet attacks. The log generation and output require more system resources if single-packet attacks frequently occur. You can enable **Log aggregation for single-packet attacks** to save system resources. This feature aggregates multiple logs generated during a period of time and sends one log. Logs that are aggregated must have the following attributes in common:

- Attacks are detected on the same interface or security zone or are destined for the device.
- Attack type.
- Attack defense action.
- Source and destination IP addresses.
- VRF to which the victim IP address belongs.

Blacklist logging

With logging enabled for the blacklist feature, the system outputs logs in the following situations:

- A blacklist entry is manually added.
- A blacklist entry is dynamically added by the scanning attack detection feature.
- A blacklist entry is manually deleted.
- A blacklist entry ages out.

A blacklist log records the following information:

- Source IP address of the blacklist entry.
- Remote IP address of the DS-Lite tunnel.
- VRF name.
- Reason for adding or deleting the blacklist entry.
- Aging time for the blacklist entry.

Log buffer and log file

The device provides separate log buffers and log files for the blacklist module and the attack defense module. To enable outputting logs of service modules to their log buffers and log files, select the **Output to log buffer** option on the basic settings page for the syslog.

Logs are saved in the log file buffer before they are saved to the log file. After the system saves logs to the log file, the log file buffer is cleared.

When the maximum capacity of the log file is reached, the system replaces the oldest logs with new logs.

Bandwidth alarm logs

Introduction

This feature monitors the total incoming traffic on the device. The device examines the total incoming traffic rate every 5 seconds and uses the average traffic rate during the 5 seconds to compare with the threshold. A log message is generated if the total incoming traffic rate on the device has reached or exceeded the threshold for the specified duration. After that, a log message is generated if the average traffic rate during a 5-second period reaches or exceeds the threshold. A log message is also generated when the average traffic rate falls below the threshold for the first time. Bandwidth alarm logs can only be output as system logs.

Configuration log settings

Introduction

This feature logs operations that administrators perform on the device.

The device can create a dedicated configuration log buffer and a separate log file to store configuration log messages. For the device to do so, click the **System** tab, select Log Settings > Basic Settings, and then select the **Output to log buffer** option on the Syslog page.

The device saves configuration log messages to the log file buffer before writing the messages to the log file in bulk. After writing the log messages in the log file buffer to the log file, the device clears the log file buffer.

The size of a log file is limited. After the limit is reached, the device replaces the oldest log messages with new log messages.

Security policy log

Introduction

This feature enables the system to fast output settings of enabled security policies as logs in SGCC format every day at the specified time.

Terminal identification logging

Introduction

The device generates a terminal identification log when terminal information (such as camera vendor) changes.

Terminal identification logs support fast log output to log hosts.

Heartbeat log settings

Introduction

After heartbeat logging is enabled, the device sends heartbeat log messages to the log server periodically. If the log server cannot receive the heartbeat log messages in a specific period of time, it determines that the device is down.

IP access logs

Introduction

With this feature enabled, the device will send to the log host the login and logout logs of users using IP authentication.

MAC access log

Introduction

After the MAC access log feature is enabled, the device will send to the log host the logs generated for the login and logoff events of MAC authentication users.

Load balancing logging

Introduction

After you enable LB scheduled logging, the device can generate logs about forwarded traffic.

After you enable fast log output for LB, the device outputs the specified LB-related content to the log host by using the fast log output feature. The device supports fast log output for server load balancing, inbound link load balancing, outbound link load balancing, and transparent DNS proxies.

You can configure the content to be output for server load balancing on the virtual server page.

Bandwidth management logs

Introduction

This feature logs the packets that match a traffic policy and sends the logs to log hosts by using the fast log output feature.

Context rate limit logging

Introduction

The context rate limit logging feature generates and sends a log message when an incoming broadcast or multicast packet is dropped because of rate limiting on contexts. In the current software version, the feature supports generating and sending only system log messages.

Zero trust logs

Introduction

After you enable external authentication fast log output, the device will send log information in fast logs to the log host. The device supports outputting authentication logs and notification logs. Authentication logs contain authentication results of trusted access controllers. Notification logs contain user offline and permission change information.

Report settings

This help contains the following topics:

Introduction

Report export

Both scheduled export and manual export are supported. You can export reports periodically or export only one report as required:

- **Scheduled export**—The device exports reports to the address specified by the user according to the specified export schedule. You can configure the statistical objects in the reports by using the report template.

- **Manual export**—The device exports a report immediately according to the configured measured objects and time range.

Report subscription

After you add a subscriber for a report, the report will be sent to the subscriber through email.

For the subscribers to receive the report, you must configure the email server.

The device sends the daily report during the least busy hours (1 a.m. to 5 a.m.). The monthly report of the previous month is sent on the first day of each month.

The report subscription feature supports the following types of reports:

- **Summary report**—Displays summarized service statistics collected over a time range.
- **Comparison report**—Provides comparison of service statistics collected over two time ranges that contain the same number of days.
- **Intelligent report**—Provides intelligent analysis of users' work efficiency, data leakage, and turnover risks based on their network access behaviors.
- **Comprehensive report**—Illustrates the overall device operational and network security status based on analysis of critical service statistics.

Email server

To configure the device to send reports to the specified email address or enable the report subscription feature, you must configure the email server.

Configure report settings

Export reports

Export reports periodically

1. Click the **System** tab.
2. In the navigation pane, select **Report Settings** > **Report Export**.
3. Click the **Report Templates** tab.
4. Click **Create**.

Table 1 Report template configuration items

Item	Description
Template name	Enter a report template name.
Language	Select a report language. Options are **Chinese** and **English**.
Statistical object	Select objects to be counted in the report. The following options are available: • **Link**. • **Routing policy**. • **Virtual server**. • **Real server**. • **Server farm**. • **Server farm member**.

Item	Description
Link statistics Link Link measured items	Select links and select items to be measured for the links. Options are: • **Application**. • **Packet loss rate**. • **Network delay**. • **Connections**. • **Concurrent connections**. • **Abnormal traffic**. • **Status**.
Routing policy statistics Routing policy	Select routing policies. If you select a routing policy, the system will count the number of matches with different classes in the routing policy.
Virtual server statistics Virtual server Statistics items	Select virtual servers and select items to be counted in the report for the virtual servers. The following items are available: • **Status**. • **HTTP status code**. • **Traffic compression ratio**.
Real server statistics Real server Statistics items	Select real servers and select items to be counted in the report for the real servers. Supported items are **Status** and **HTTP delay**.
Server farm statistics Server farm	Select server farms. If you select a server farm, the system will count status statistics for the server farm.
Server farm member statistics Server farm	Select members from a server farm and select items to be counted in the report for the server farm members. Supported items are **Status** and **HTTP delay**.

Item	Description
Server farm member Statistics items	

5. Click **OK**.

   The report template is displayed on the **Report Templates** page.

6. Click the **Auto Export** tab.

7. Click **Create**.

Table 2 Report export task configuration items

Item	Description
Export destination	Select a report export destination. Options are **Local** and **Email**.
Export schedule	Select a report export schedule. Options are **Hourly**, **Daily**, **Weekly**, **Monthly**, **Quarterly**, and **Yearly**.
Report template	Select a report template used for a periodic report type.

Export a report manually

1. Click the **System** tab.

2. In the navigation pane, select **Report Settings** > **Report Export**.

3. Click the **Manual Export** tab.

Table 3 Manual export configuration items

Item	Description
Statistical object	Select objects to be counted in the report. The following options are available: • **Link**. • **Routing policy**. • **Virtual server**. • **Real server**. • **Server farm**. • **Server farm member**.
Link statistics Link Link measured items	Select links and select items to be measured for the links. Options are: • **Application**. • **Packet loss rate**. • **Network delay**. • **Connections**. • **Concurrent connections**. • **Abnormal traffic**. • **Status**.
Routing policy statistics Routing policy	Select routing policies. If you select a routing policy, the system will count the number of matches with different classes in the routing policy.
Virtual server statistics Virtual server Statistics items	Select virtual servers and select items to be counted in the report for the virtual servers. The following items are available: • **Status**. • **HTTP status code**. • **Traffic compression ratio**.

Item	Description
Real server statistics Real server Statistics items	Select real servers and select items to be counted in the report for the real servers. Supported items are **Status** and **HTTP delay**.
Server farm statistics Server farm	Select server farms. If you select a server farm, the system will count status statistics for the server farm.
Server farm member statistics Server farm Server farm member Statistics items	Select members from a server farm and select items to be counted in the report for the server farm members. Supported items are **Status** and **HTTP delay**.
Time range	Specify a time range for the report.

4. Click **Export now**.

   The device exports the reports according to the configured parameters.

Configure report subscription

1. Click the **System** tab.
2. In the navigation pane, select **Report Settings** > **Report Subscription**.
3. Click **Add** for a report.
4. Enter the email address of the report subscriber and select a language for the reports.

Configure the email server

1. Click the **System** tab.
2. In the navigation pane, select **Report Settings** > **Email Server**.
3. Configure the email server.

Table 4 Email server configuration items

Item	Description
Email server address	Enter the IP address or host name of the email server.
Sender address	Enter the email sender address.
DNS server IP	Enter the IP address of the DNS server.
Identity authentication	Select **Enable** to enable email client authentication. Enable email client authentication as required by the email server.
Secure user credential transmission	Select **Enable** to enable secure transmission of user authentication credentials.
Username	Enter the username for connecting to the email server.
Password	Enter the password for connecting to the email server.

4. Click **Apply**.

Session settings

This help contains the following topics:

Introduction

Session management is a common module, providing basic services for service modules to implement session-based services.

Session management defines packet exchanges at transport layer as sessions. It updates session states and ages out sessions according to data flows from the initiators or responders. Session management allows multiple features to process the same service packet.

Session management operation

Session management tracks the session status by inspecting the transport layer protocol information. It performs unified status maintenance and management of all connections based on session tables and relation tables.

When a connection request passes through the device from a client to a server, the device creates a session entry. The entry can contain the request and response information, such as:

- Source IP address and port number.
- Destination IP address and port number.
- Transport layer protocol.
- Application layer protocol.
- Protocol state of the session.

A multichannel protocol requires that the client and the server negotiate a new connection based on an existing connection to implement an application. Session management enables the device to create a relation entry for each connection during the negotiation phase. The entry is used to associate the connection with the application. Relation entries will be removed after the associated connections are established.

If the destination IP address of a packet is a multicast IP address, the packet will be forwarded out of multiple ports. When a multicast connection request is received on an inbound interface, the device performs the following operations:

- Creates a multicast session entry on the inbound interface.
- Creates a corresponding multicast session entry for each outbound interface.

Unless otherwise stated, "session entry" in this document refers to both unicast and multicast session entries.

In actual applications, session management must work with other service modules. It only tracks connection status. It does not block potential attack packets.

Session management functions

Session management enables the device to provide the following functions:

- Creates sessions for protocol packets, updates session states, and sets aging time for sessions in different protocol states.
- Supports port mapping for application layer protocols (see APR online help), enabling application layer protocols to use customized ports.
- Sets aging time for sessions based on application layer protocols.
- Supports ICMP/ICMPv6 error packet mapping, enabling the device to search for original sessions according to the payloads in the ICMP/ICMPv6 error packets.
- Supports session management for the control channels and dynamic data channels of application layer protocols, for example, FTP.

Session types

When receiving the first packet of a data flow, the device processes the packet and creates a session entry based on the processing result. For subsequent packets of the data flow, the device performs fast forwarding based on the session entry.

Sessions are classified into the following types according to the action taken on the packets that match a session entry:

- **Permit session**—The device permits all packets of a permit session. The device generates a permit session entry for a data flow if it permits the first packet of the data flow.

  A permit session can only track connection status. It cannot deny potential attack packets. To deny specific packets, you must use permit sessions together with security features.
- **Deny session**—The device drops all packets of a deny session. The device generates a deny session entry for a data flow if it drops the first packet of the data flow.

  For the device to generate deny sessions for dropped packets, you must enable the deny session feature.

Unless otherwise stated, the sessions in this document refer to permit sessions.

Restrictions and guidelines

- The aging time for sessions of different applications are valid for stable session TCP sessions in ESTABLISHED state or UDP sessions in READY state.
- For a session in a stable state, the priority order of the associated aging time is as follows:
  - Aging time for sessions of application layer protocols.
  - Aging time for sessions in different protocol states.
- The device generates deny sessions only for the packets dropped by the ASPF or connection limit module.
- The deny session feature supports only software-based fast packet drop. It does not support hardware-based fast packet drop.
- Session hot backup does not support deny sessions.

Signature upgrade

This help contains the following topics:

Introduction

A DPI signature library is a collection of common signatures that DPI uses for service identification. The company's official website releases up-to-date signatures in the form of DPI signature library files. You can manually download the files or configure the device to automatically download the files to update the DPI signature libraries. You can also roll back the signature library for a DPI service module.

DPI signature libraries include the IPS signature library, URL filtering signature library, APR signature library, and virus signature library.

Signature library upgrade

The following methods are available for updating the signature library for a DPI service module:

- Automatic update.

  The device automatically downloads the most up-to-date signature file to update its local signature library periodically.

- Manual update.

  Use this method when the device cannot obtain the signature file automatically.

  You must manually download the most up-to-date signature file, and then use the file to update the signature library on the device.

Signature library roll back

If filtering false alarms or filtering exceptions occur on a DPI service module frequently, you can roll back its signature library to the previous version or to the factory default version.

Restrictions and guidelines

- Signature library upgrade and rollback can cause temporary outage for DPI services. Services based on the DPI services might also be interrupted. For example, security policies cannot control access to applications.
- To upgrade the signature library for a DPI service module such as APR, and IPS, anti-virus, the correct license is required. If the license for a DPI service module expires, you can still

use the existing signature library, but you can no longer upgrade the signature library. For more information about licenses, see license online help.

- Do not perform signature library update or rollback when the device's free memory is below the normal state threshold. The signature library update or rollback operation performed under such conditions is likely to fail and the DPI service will be affected.
- Update only one signature library at a time.
- Only the default context supports the signature library update. A user context supports only viewing the signature library version.

Configure signature library upgrade and rollback

You can upgrade the signature library for a DPI service module to the latest version or roll back the signature library to the previous or the factory default version.

You can also configure a proxy server through which the device can access the company's official website for automatic or immediate online signature library update.

Configure automatic signature library update

Perform this task to configure automatic signature library update for a DPI service module.

For automatic signature library update to work correctly, make sure the device can access the company's official website to obtain the latest signature file.

Procedure

1. Click the **System** tab.

2. In the navigation pane, select **Upgrade Center** > **Signature Upgrade**.
3. Click the box in the **Auto update** column for a signature library.

   In this example, click the box in the **Auto update** column for the IPS signature library.

   The **Configure Scheduled Update For IPS Signature Library** window opens.
4. Set the scheduled update time.

   The automatic signature library update starts actually at a random time between the following time points:

   - One hour before the scheduled update time.
   - One hour after the scheduled update time.
5. Click **OK**.

Perform a manual signature library update

Perform this task to manually update the signature libraries for DPI service modules by using locally stored signature files.

Use this method if the device cannot access the signature database services on the company's official website.

Store the update file on the master device for successful signature library update.

Procedure

1. Click the **System** tab.
2. In the navigation pane, select **Upgrade Center** > **Signature Upgrade**.
3. Click **Manual update** in the **Actions** column for a signature library. In this example, click **Manual update** for the IPS signature library.

The **Update IPS Signature Library** window opens.

4. Click **Select** to select the local update file.
5. Click **OK**.

Configure a proxy server

The device must access the company's official website for online or automatic signature library update. If direct connectivity is not available, the device can access the company's official website through the specified proxy server.

Procedure

1. Click the **System** tab.
2. In the navigation pane, select **Upgrade Center** > **Signature Upgrade**.
3. Click **Configure proxy server**.

   The **Configure Proxy Server** window opens.
4. Configure the proxy server settings, including the server address, port number, login username, and login password.
5. Click **OK**.

Roll back a signature library

If a signature library update causes exceptions or a high false alarm rate, you can roll back the signature library.

Before rolling back the signature library, the device backs up the current signature library as the previous version. For example, the previous library version is V1 and the current library version is V2. If you perform a rollback to the previous version, library version V1 becomes the current version and library version V2 becomes the previous version. If you perform a rollback to the previous version again, the library rolls back to library version V2.

Procedure

1. Click the **System** tab.
2. In the navigation pane, select **Upgrade Center** > **Signature Upgrade**.
3. Click **Roll back** in the **Actions** column for a signature library. In this example, click **Roll back** for the IPS signature library.

   The **Roll Back IPS Signature Library** window opens.
4. Select **Roll back to previous version** or **Roll back to factory default**.
5. Click **OK**.

Test the signature library server connectivity

Before configuring automatic signature library update, or updating the signature library by using the proxy server, click **Test signature library server connectivity**. If the device fails to connect to the signature library server, resolve the issue according to the prompt on the page.

Software upgrade

This help contains the following topics:

Introduction

The device runs a Boot ROM image and network OS images to provide functions and services.

Images for interface modules and switching fabric modules are integrated in the image package for MPUs. When you upgrade MPUs, the system automatically upgrades interface modules and switching fabric modules.

Service modules have separate image files. The image files are released together with the image files for MPUs. You must upgrade service modules manually.

Boot ROM image

At startup, the device first runs the Boot ROM image to perform hardware initialization and bootstrap the system.

The Boot ROM image is stored in the Boot ROM of the device. It contains a basic segment and an extended segment.

- The basic segment is the minimum code that bootstraps the system.
- The extended segment enables hardware initialization and provides system management menus. When the device cannot start up correctly, you can use the menus to load software images and a configuration file or manage files.

Typically, the Boot ROM image is integrated in the Boot image to avoid software compatibility errors.

Network OS images

Network OS image types

- **Boot image**—A .bin file that contains the Linux operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
- **System image**—A .bin file that contains the network OS kernel and standard features, including device management, interface management, configuration management, and routing.
- **Feature image**—A .bin file that contains advanced or customized software features.
- **Patch image**—A .bin file that is released for fixing bugs without rebooting the device. A patch image does not add or remove features.

A Boot ROM image, boot image, and system image are required for the device to operate. You can purchase and install feature images as needed.

Software release forms

Software images are released in one of the following forms:

- Separate .bin files. You must verify compatibility between software images.
- As a whole in one .ipe package file. The images in an .ipe package file are compatible. When you use an .ipe package file to upgrade software, the system automatically decompresses the .ipe file, loads the .bin images, and sets them as startup software images.

Restrictions and guidelines

- The device will reboot and services will be interrupted during a software upgrade. As a best practice, perform a planned software upgrade.
- Read the release notes to identify whether the upgrade images require a license. If licenses are required, register and activate licenses for each license-based image.
- Before installing feature or patch images, verify that the images are compatible with the images running on the device.
- To uninstall feature images from an IRF fabric, uninstall the images from the global standby MPUs before uninstalling the images from the global active MPU.
- After deleting feature or patch image files that the device is using, you cannot uninstall the files.
- On an IRF fabric, do not perform a switchover while you are managing image files.
- If the device has both MPUs and service modules, you can import image files only to the MPUs.

Manage image files

You can import, delete, install, and uninstall image files on the device, and specify startup image files. The specified startup image files take effect after a device reboot.

Procedure

1. Select **System** > **Upgrade Center** > **Software Upgrade**.
2. Click **Manage file**.

Table 1 Manage image files

Item	Description
Import	Transfer .bin or .ipe image files to the device. When you transfer an .ipe file to the device, the device automatically decompresses the .ipe file and saves the .bin files.
Delete	Delete unused image files.
Operation	You can perform the following task: • Specify startup image files. • Install feature or patch image files. • Uninstall feature or patch image files.
Set as next startup files	Specify the startup image files to be loaded at the next startup, including a boot image file and a system image file of the same version. The startup image files take effect after a device reboot.
Install feature/patch files	Install or upgrade feature and patch image files without causing system outage. The device can install multiple feature image files at the same time. To install a new patch image file, you must uninstall the old patch image file first.
Uninstall	Uninstall feature and patch image files. Uninstalled image files are not active and do not provide services, but they are still stored on the

Item	Description
feature/patch files	device.

Upgrade software immediately

Use an .ipe file to upgrade the software

1. Select **System** > **Upgrade Center** > **Software Upgrade**.
2. Click **Upgrade immediately**, and then select **ipe** for the startup file type.
3. Click **Select** to select the upgrade file. Use the default settings for other parameters.
4. Click **OK**.

Use .bin files to upgrade the software

1. Select **System** > **Upgrade Center** > **Software Upgrade**.
2. Click **Upgrade immediately**, and then select **bin** for the startup file type.
3. Click **Select** to select the upgrade boot file and system file. Use the default settings for other parameters.
4. (Optional.) If the size of the .bin files exceeds the free storage space, select the **Delete all startup files** option.
5. Click **OK**.

License management

This help contains the following topics:

Introduction

To use a license-based feature, you must purchase a formal license or obtain a trial license and install the license for the feature.

License validity period

The following types of validity period are available:

- **Permanent**—A permanent license is always valid and never expires.

- **Date restricted**—A license valid for an absolute date range, for example, 2015-05-01 to 2015-05-30.

Trial and formal licenses

Licenses include trial licenses and formal licenses. Trial licenses typically have time limits and they cannot be transferred. Purchase and install a formal license for a license-based feature before its trial license expires, so that the feature is still usable.

Restrictions and guidelines

General restrictions and guidelines

- Make sure no one else is performing license management tasks on the device you are working with.
- Expired formal licenses cannot be uninstalled. Expired licenses remain in the license storage area unless you compress the license storage area. The exhaustion of the license storage area will cause installation failures of new licenses.
- Before registering licenses, view the available number and installed number on the **Compress License Storage** page. Make sure the number of registered licenses and installed licenses are no more than the available number.
- Compressing the license storage area changes DID and deletes expired licenses and uninstalled license information. Before you compress the license storage area, back up Uninstall keys, and make sure all activation files generated based on the old DID have been installed. These activation files cannot be installed after the compression.

- When installing a license, the system also searches the storage media for a matching feature package. When it finds a matching package, it stops searching and installs the package.
- When uninstalling a license, the system checks whether the feature package for the license is running. If it is running, the system uninstalls the package automatically.
- If you cannot obtain or re-register the activation file due to issues such as operating system and browser errors of the HTTP client, contact the technical support.

Restrictions and guidelines: File safety

- Save and back up the obtained activation file in case of loss.
- Do not open the DID file or activation file to avoid file corruption.
- Do not modify the name of the DID file or activation file to avoid licensing error.
- Do not delete activation files in the **In use** or **Usable** state on the device. If you delete an activation file that is usable or in use, the related feature will not function correctly. If a file is missing or corrupted, copy the backup file to the license folder to recover the license. If the state of the recovered license is **In use**, but not all licensed features can function, reboot the device.

Configure license management

Install licenses

You must purchase a license key for the hardware of each location. To license the hardware, use the license key, SN, and DID of the hardware to register an activation file, and install the activation file on the specified location. A hardware is licensed even if it is installed on another device.

Procedure

1. Go to **System** > **License Config**.
2. Identify features to be licensed.
3. Purchase a license key.
4. Obtain the SN and DID.
5. Use the product category, license key, SN, and DID to register an activation file.
6. Click **Install** to install the activation file.

Compress the license storage area

Before registering an activation file, make sure the license storage area has sufficient space for installing the new activation file. If the license storage space is not sufficient, compress the license storage area. The compression deletes expired licenses and uninstalled license information.

IRF

This help contains the following topics:

- Introduction
  - IRF network model
  - Basic concepts
  - Master election
  - IRF bridge MAC persistence
  - IRF software auto-update
- Restrictions and guidelines
- Configure IRF

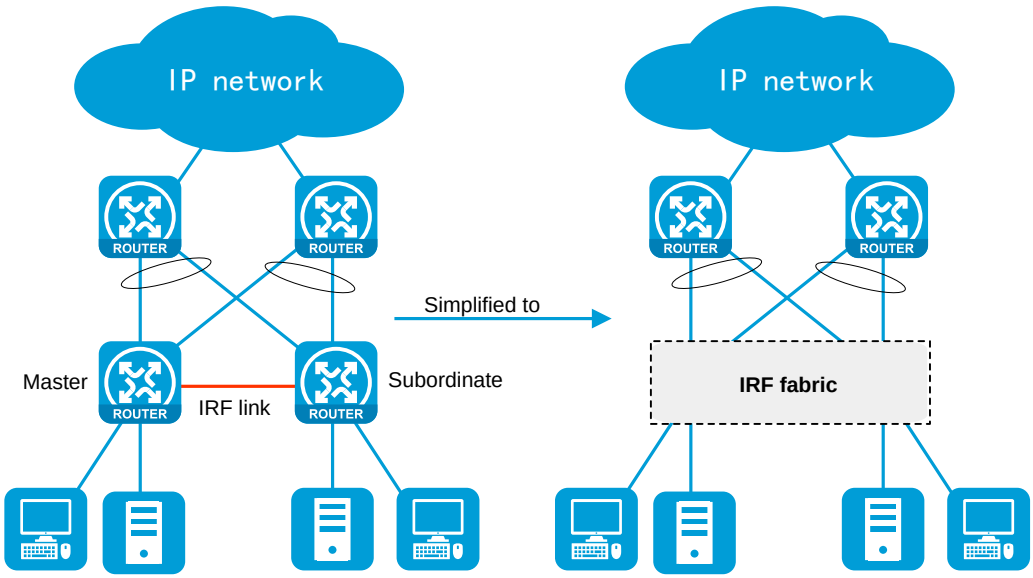
Introduction

The Intelligent Resilient Framework (IRF) technology virtualizes multiple physical devices at the same layer into one virtual fabric to provide data center class availability and scalability. IRF virtualization technology offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

IRF network model

Figure 1 shows an IRF fabric that has two devices, which appear as a single node to the upper-layer and lower-layer devices.

Figure 1 IRF application scenario



Basic concepts

IRF member roles

IRF uses two member roles: master and standby (also called subordinate).

When devices form an IRF fabric, they elect a master to manage and control the IRF fabric, and all the other devices back up the master. When the master device fails, the other devices automatically elect a new master.

IRF domain ID

One IRF fabric forms one IRF domain. IRF uses IRF domain IDs to uniquely identify IRF fabrics and prevent IRF fabrics from interfering with one another.

IRF member ID

An IRF fabric uses member IDs to uniquely identify and manage its members. This member ID information is included as the first part of interface numbers and file paths to uniquely identify interfaces and files in an IRF fabric. Two devices cannot form an IRF fabric if they use the same member ID. A device cannot join an IRF fabric if its member ID has been used in the fabric.

Member priority

Member priority determines the possibility of a member device to be elected the master. A member with higher priority is more likely to be elected the master.

IRF port

An IRF port is a logical interface that connects IRF member devices. Every IRF-capable device has two IRF ports.

The IRF ports are named IRF-port *n*/1 and IRF-port *n*/2, where *n* is the member ID of the device. The two IRF ports are also referred to as IRF-port 1 and IRF-port 2 for simplicity.

To use an IRF port, you must bind a minimum of one physical interface to it. The physical interfaces assigned to an IRF port automatically form an aggregate IRF link. An IRF port goes down when all its IRF physical interfaces are down.

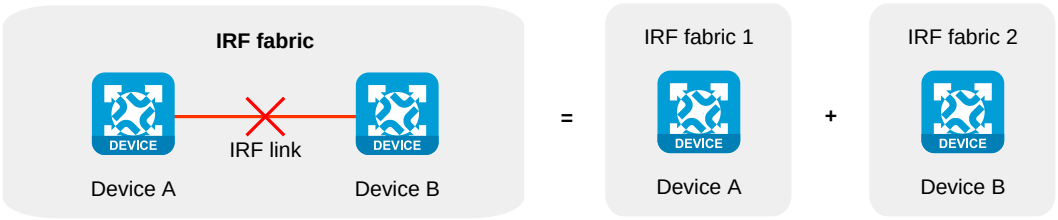
IRF physical interface

IRF physical interfaces connect IRF member devices and must be bound to an IRF port. They forward traffic between member devices, including IRF protocol packets and data packets that must travel across IRF member devices.

IRF split

IRF split occurs when an IRF fabric breaks up into two IRF fabrics because of IRF link failures, as shown in Figure 2. The split IRF fabrics operate with the same IP address. IRF split causes routing and forwarding problems on the network.

Figure 2 IRF split



IRF merge

IRF merge occurs when two split IRF fabrics reunite or when two independent IRF fabrics are united, as shown in Figure 3.

Figure 3 IRF merge

Master election

Master election occurs each time the IRF fabric topology changes in the following situations:

- The IRF fabric is established.
- The master device fails or leaves.
- The IRF fabric splits.
- Independent IRF fabrics merge.

Master election does not occur when split IRF fabrics merge.

Master election selects a master in descending order:

1. Current master, even if a new member has higher priority.

   When an IRF fabric is being formed, all members consider themselves as the master. This rule is skipped.

2. Member with higher priority.
3. Member with the longest system uptime.

Two members are considered to start up at the same time if the difference between their startup times is equal to or less than 10 minutes. For these members, the next tiebreaker applies.

4. Member with the lowest CPU MAC address.

For the setup of a new IRF fabric, the subordinate devices must reboot to complete the setup after the master election.

For an IRF merge, devices must reboot if they are in the IRF fabric that fails the master election.

IRF bridge MAC persistence

By default, an IRF fabric uses the bridge MAC address of the master device as its bridge MAC address. Layer 2 protocols, such as LACP, use this bridge MAC address to identify the IRF fabric. On a switched LAN, the bridge MAC address must be unique.

To avoid duplicate bridge MAC addresses, an IRF fabric can change its bridge MAC address automatically after its bridge MAC owner leaves. However, the change causes temporary traffic disruption.

Depending on the network condition, enable the IRF fabric to retain or change its bridge MAC address after the address owner leaves. Available options include:

- **6 minutes**—Bridge MAC address of the IRF fabric remains unchanged for 6 minutes after the address owner leaves. If the owner does not return before the timer expires, the IRF fabric uses the bridge MAC address of the current master as its bridge MAC address. This option avoids unnecessary bridge MAC address changes caused by device reboot, transient link failure, or purposeful link disconnection.
- **Always**—Bridge MAC address of the IRF fabric does not change after the address owner leaves.

- **Not retain**—Bridge MAC address of the current master replaces the original one as soon as the owner of the original bridge MAC leaves.

IRF software auto-update

The software auto-update feature automatically synchronizes the current software images of the master to devices that are attempting to join the IRF fabric.

To join an IRF fabric, a device must use the same software images as the master in the fabric.

When you add a device to the IRF fabric, software auto-update compares the startup software images of the device with the current software images of the IRF master. If the two sets of images are different, the device automatically performs the following operations:

1. Downloads the current software images of the master.
2. Sets the downloaded images as its main startup software images.
3. Reboots with the new software images to rejoin the IRF fabric.

You must manually update the new device with the software images running on the IRF fabric if software auto-update is disabled.

To ensure a successful software auto-update in a multi-user environment, prevent anyone from r
member devices during the auto-update process. To inform administrators of the auto-update sta
configure **Log Settings** to output the status messages to configuration terminals.

Restrictions and guidelines

The following information only provides basic IRF configuration restrictions and guidelines. For more information, see IRF configuration in the configuration guides for the device.

Hardware compatibility with IRF

A firewall can form an IRF fabric only with the firewalls in the same series.

Software requirements for IRF

All IRF member devices must run the same software image version. Make sure the software auto-update feature is enabled on all member devices.

IRF fabric size

A firewall IRF fabric can contain a maximum of two member devices.

Member ID configuration restrictions

If you change the member ID for a member device, the new member ID takes effect at reboot. After the device reboots, the settings on all member ID-related physical resources (including common physical network ports) are removed, regardless of whether you have saved the configuration.

In an IRF fabric, changing IRF member IDs might cause undesirable configuration changes and data loss. Before you do that, back up the configuration, and make sure you fully understand the impact on your network.

Bridge MAC address restrictions for IRF members

When IRF fabrics merge or an IRF fabric is set up, IRF ignores the IRF bridge MAC address and checks the bridge MAC address of each member device. IRF setup or merge fails if any two member devices have the same bridge MAC address.

Candidate IRF physical interfaces

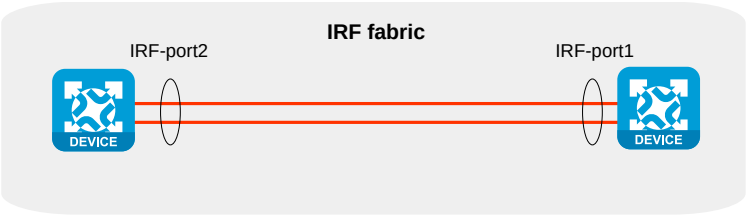
Candidate IRF physical interfaces vary by device model. For more information, see IRF configuration in the configuration guides for the device.

IRF port connection

When you connect two neighboring IRF members, follow these restrictions and guidelines:

- You must connect the physical interfaces of IRF-port 1 on one member to the physical interfaces of IRF-port 2 on the other, as shown in Figure 4.
- An IRF fabric can only use daisy-chain topology. No intermediate devices are allowed between neighboring IRF member devices.
- Make sure the two ends of an aggregate IRF link have the same number of IRF physical interfaces and the IRF physical interfaces are the same type.

Figure 4 Connecting IRF physical interfaces



IRF physical interface configuration restrictions and guidelines

Binding a physical interface in up state to an IRF port causes service interruption on that physical interface.

To temporarily shut down all IRF physical interfaces on the master device, you must make sure the master device has a higher priority than the subordinate device.

You must always shut down the peer interface of a physical interface before you bind the physical interface to an IRF port or removing the binding.

IRF domain ID restrictions

An IRF fabric has only one IRF domain ID. The domain ID takes effect on all IRF member devices. Make sure each IRF fabric in the network has a unique domain ID.

License installation requirements for license-based features

For a license-based feature to run correctly on an IRF fabric, make sure the licenses installed for the feature on all member devices are the same.

Configure IRF

For a successful IRF setup, follow this IRF fabric setup procedure:

1. Plan the IRF fabric setup. Determine the master, member ID assignment, and IRF connection scheme.
2. Perform the following tasks on each member device:
   a. Configure basic IRF settings, including a unique member ID and priority.
   b. Bind physical interfaces to the IRF ports.
   c. Save the configuration to the startup configuration file.
   d. Connect the IRF physical interfaces. Make sure the connections are consistent with the IRF port bindings.
   e. Reboot the device.

      The member ID assignment takes effect at reboot. The member devices perform a master election to form an IRF fabric that contains one master and one subordinate.
3. Log in to the IRF fabric. You can log in to the Web interface of the IRF fabric at the IP address of the management port on the master device.
4. Perform the following tasks:
   a. View the IRF fabric topology to verify its correctness.
   b. (Optional.) Modify the member ID, priority, or IRF port binding configuration.

Changing member IDs in an IRF fabric can void member ID-related configuration and cause unex problems. Make sure you understand the impact on your live network before you change membe

Changing IRF port bindings might cause IRF split. Make sure you understand the impact on your network before you change IRF port bindings.

   c. Configure advanced IRF settings on the IRF fabric.

d. Save the configuration to the startup configuration file.

On the IRF fabric, you can configure software features as you do on a standalone device.

IRF advanced settings

This help contains the following topics:

Introduction

IRF advanced settings are IRF high availability (HA) settings. IRF HA enables two IRF member devices to back up each other dynamically to ensure forwarding service continuity upon failure on one of the devices. For more information about IRF, see IRF help.

Mechanisms

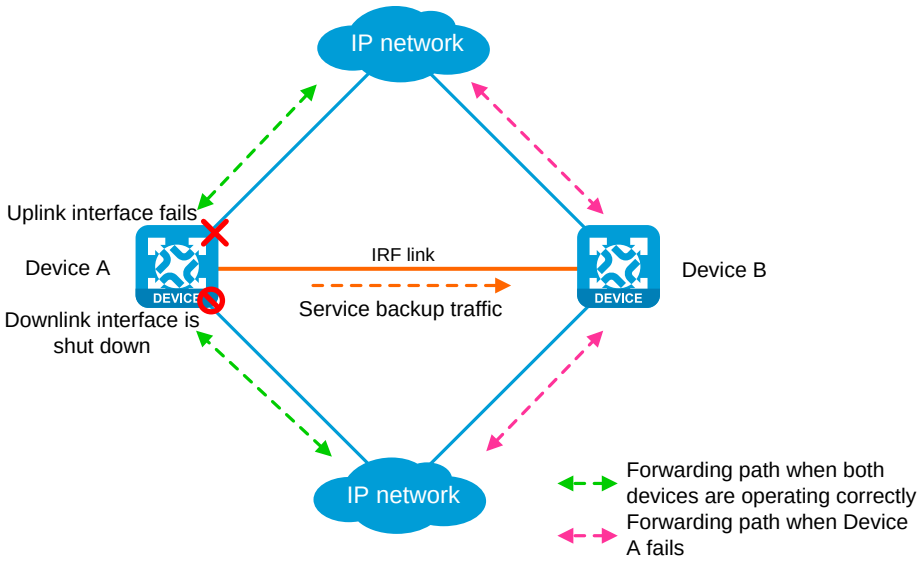
IRF HA provides the following services:

- **Service backup**—Backs up the data and entries of services between the two devices. This minimizes the forwarding interruption time when traffic is switched from one device to the other.
- **Traffic migration**—Switches traffic from one device to the other by using a redundancy group. A redundancy group allows traffic to enter and leave the HA system through the same device. The redundancy group works with Track to detect uplink and downlink failures. When detecting a failure, the redundancy group switches all its members from the failed device to the other device.

IRF HA works as follows, as shown in Figure 1:

1. When both devices are working correctly, Device A forwards traffic, and service data and entries are backed up from Device A to Device B.
2. Track detects that the uplink interface of Device A fails.
3. The redundancy group shuts down the downlink interface of Device A.
4. Traffic is switched to Device B for forwarding. Because Device B already has service data and entries, traffic migration almost has no impact on the services.

Figure 1 IRF HA workflow



Operating modes

IRF HA supports the following modes:

- **Active/standby mode**—Only one device processes services.
- **Dual-active mode**—Both devices process services.

Redundancy groups

Redundancy group nodes

A redundancy group contains two nodes. A redundancy group node can act as the primary or secondary node. Only the primary node can forward traffic. When both nodes are working correctly, only interfaces and CPUs on the primary node are processing traffic (such as forwarding packets

and creating session entries). The secondary node acts as a backup and does not process traffic as long as the primary node is working correctly.

Redundancy group nodes are associated with physical devices in a cluster by member IDs. The primary node can be the master device or standby device in a cluster. Typically, the primary node is the master device.

Member interfaces

You can assign physical interfaces to a redundancy group by binding them to their respective redundancy group nodes.

For symmetric traffic switchover, you must bind a minimum of one downlink interface and a minimum of one uplink interface with each node of the redundancy group.

The state of the member physical interfaces changes with the state of the redundancy group nodes. Only the member interfaces on the primary node can forward traffic.

As shown in Figure 2, Port 1 and Port 2 are on Node 1, and Port 3 and Port 4 are on Node 2. When Node 1 is in primary state, Port 1 and Port 2 are up to forward traffic, while Port 3 and Port 4 are shut down by the Reth module.

When Port 1 goes down, the Reth module places Node 1 in secondary state and shuts down Port 2. Node 2 changes to the primary state, and Port 3 and Port 4 come up to forward traffic, as shown in Figure 3.

Figure 2 States of the member interfaces when both nodes are operating correctly

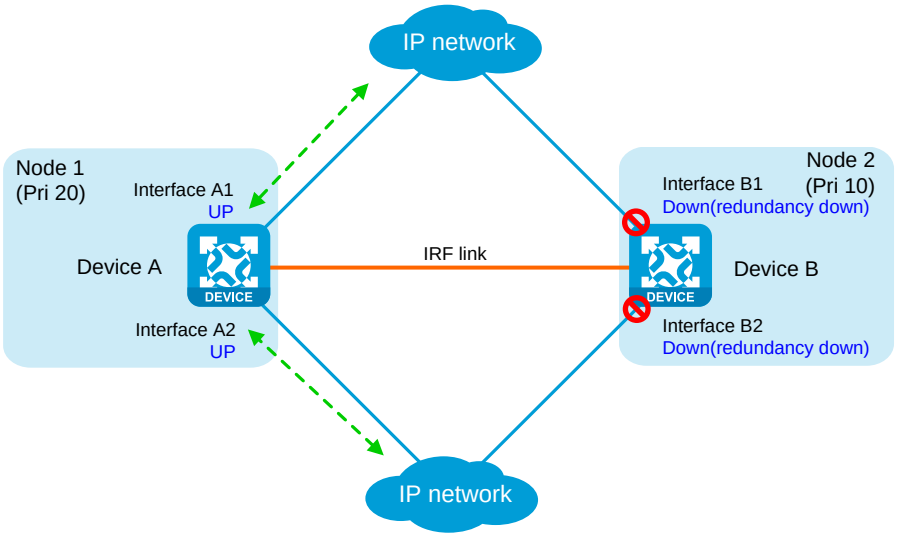
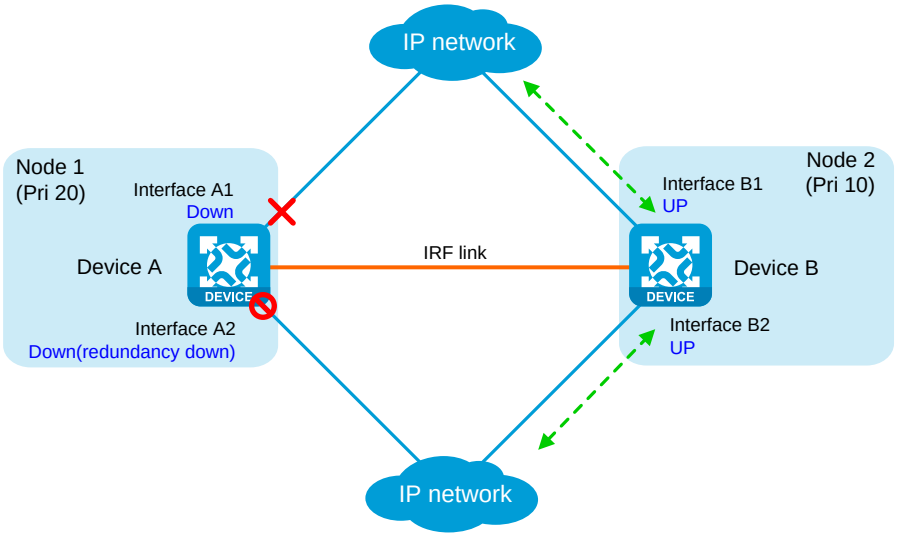


Figure 3 States of the member interfaces after a switchover



Reth interfaces

To use Reth interfaces for symmetric forwarding, you must assign two Reth interfaces to a redundancy group: one for uplink traffic and the other for downlink traffic. The Reth interfaces must meet the following requirements:

- The Reth interface for uplink traffic contains one uplink port on each redundancy group node.
- The Reth interface for downlink traffic contains one downlink port on each redundancy group node.
- The high-priority member of each Reth interface belongs to the high-priority node.

The state of each Reth interface's members depends on the state of the redundancy group nodes.

- When the high-priority node is in primary state, the high-priority member is active.
- When the low-priority node is in primary state, the low-priority member is active.

As shown in Figure 4, redundancy group 1 contains Reth 1 for uplink traffic and Reth 2 for downlink traffic. Reth 1 contains Port 1 (on Node 1) and Port 3 (on Node 2). Reth 2 contains Port 2 (on Node 1) and Port 4 (on Node 2).

When Node 1 is in primary state, Port 1 in Reth 1 and Port 2 in Reth 2 are active to forward uplink and downlink traffic, respectively.

When Port 1 fails, the Reth module places Node 1 in secondary state and shuts down Port 2, as shown in Figure 5. Node 2 changes to the primary state, and Port 3 and Port 4 become active to forward uplink and downlink traffic.

Figure 4 States of each Reth interface's members when both nodes are operating correctly

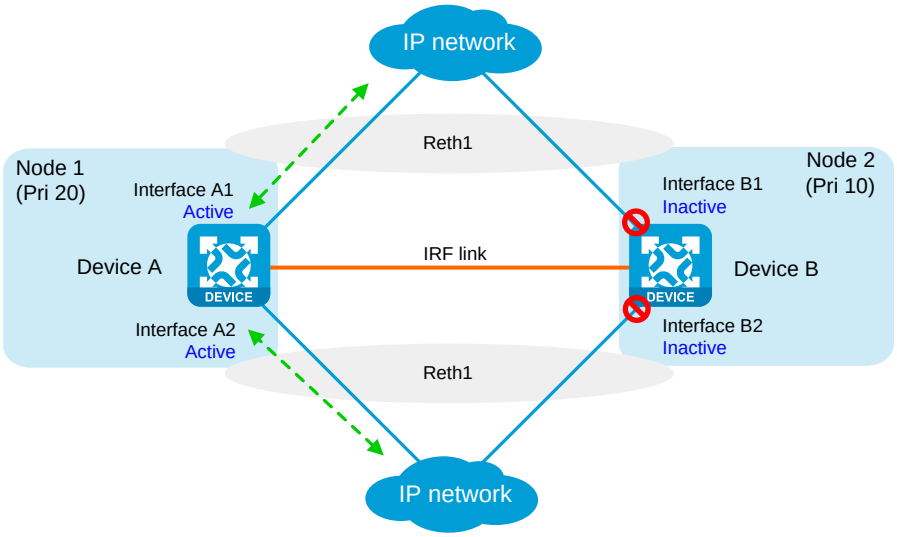
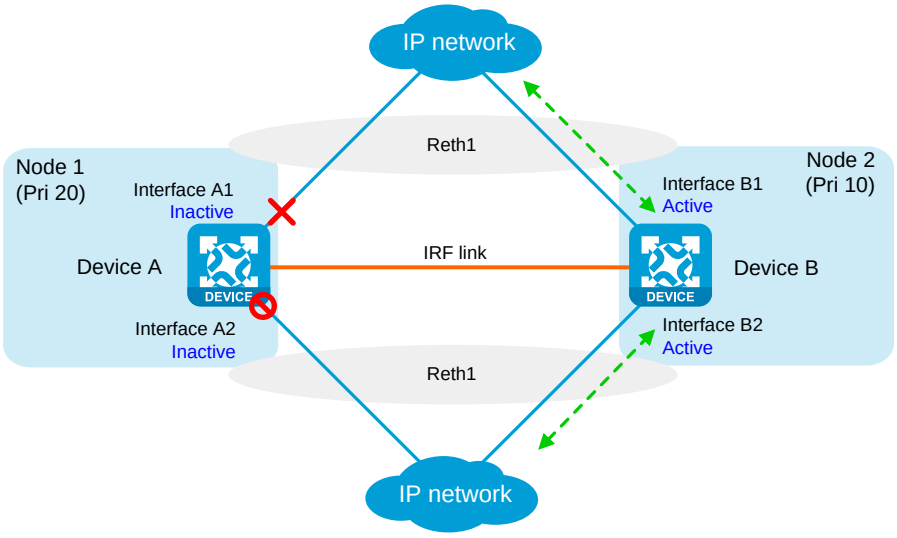


Figure 5 States of each Reth interface's members after a switchover



Failover and fallback

In a redundancy group, one node is in primary state, and the other node is in secondary state. Only the primary node forwards traffic. When the primary node fails, the redundancy group switches over to the secondary node. This mechanism ensures path symmetry for traffic.

A redundancy group performs a switchover as follows:

1. When both redundancy group nodes are operating correctly, the redundancy group forwards traffic through the primary node and backs up services and data to the secondary node.
2. When the upstream interface on the primary node fails, the redundancy group shuts down the downstream interface on the primary node and switches traffic over to the secondary node.

When the primary node recovers, the redundancy group switches traffic back to the primary node.

Redundancy group switchovers include automatic switchovers and manual switchovers.

- **Automatic switchover**—A redundancy group cooperates with the Track module to monitor link and interface status for automatic switchovers.
- **Manual switchover**—You issue a manual switchover request.

When a switchover is triggered, traffic is not migrated immediately. Whether traffic is migrated depends on the status of the primary node and the preemption delay timer.

Preemption delay timer

The preemption delay timer specifies the delay for a switchover back to the high-priority node. The preemption delay timer starts when the switchover is triggered. The redundancy group performs the switchover only after the timer expires. The delay allows the system to process events (such as

interface state changes) required for the switchover. If the high-priority node is not ready when this timer expires, the switchover is not performed.

Restrictions and guidelines

- Do not assign management interfaces to a redundancy group or Reth interface. If you do so, remote management connections are interrupted if the redundancy group or Reth interface is deleted.
- If sessions are created in hash-based mode and transparent UDP packet transmission is enabled, UDP packets are distributed across cards based on hash results.
- In dual-active mode, devices support only the flow-based policy for flow classification.
- In dual-active mode, devices do not support AFT.

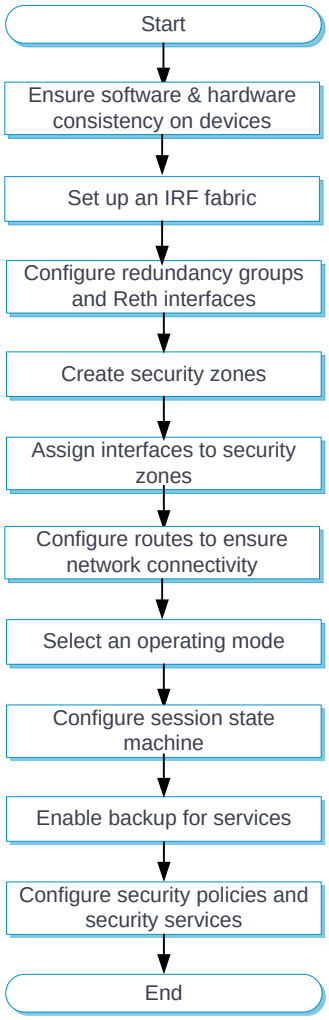
Configure IRF HA

Prerequisites

Set up an IRF fabric by using two devices before you configure IRF HA on them.

IRF HA configuration flow

Figure 6 IRF HA configuration flow chart



Configure HA on the IRF fabric

1. Click the **System** tab.
2. In the navigation pane, select **Virtualization Advanced Settings** > **IRF Advanced Settings**.

   The **IRF Advanced Settings** page opens.

3. Configure IRF HA. For more information about related-parameters, see Table 1.

Table 1 IRF HA parameters

Parameter	Description
Operating mode	Set the operating mode of IRF HA. • **Active/standby**—The primary device processes services, and the secondary device stands by. • **Dual-active**—Both the primary and secondary devices process services.
Session state machine mode	Set the session state machine mode. • **Strict**—Strict mode. Use this mode if all traffic paths are symmetric. • **Loose**—Loose mode. Use this mode if asymmetric-path traffic exists in an HA system operating in active/standby mode to avoid traffic loss. • **Compact**—Compact mode. Use this mode if asymmetric-path traffic exists in an HA system operating in dual-active mode for disconnected sessions to age out timely.
Session creation mode	Set the session creation mode. To balance the service load on the devices, you can use one of the following session creation modes: • **Hash-based session creation**—A session is created on the device to which its first packet is relayed according to the hash result. The device where a session is created might not be the device that receives the traffic. This mode applies if traffic is unevenly distributed among the devices. • **Local-based session creation**—A session is created on the device where the first packet of the session arrives. This mode applies if traffic is evenly distributed among the devices. This parameter is available only in dual-active mode.
Transparent transmission for UDP packets	Set the status of transparent transmission for UDP packets. This feature allows a device to relay UDP packets that do not match any sessions to the other device in the HA system. If the UDP packets also do not match any sessions on the other device, a new session is created locally. This parameter is available only in dual-active mode.

Enable backup for services

Enable backup for services on an IRF HA system for smooth service migration.

1. Click the **System** tab.
2. In the navigation pane, select **Virtualization Advanced Settings** > **IRF Advanced Settings**.

   The **IRF Advanced Settings** page opens.
3. Enable backup for services. For more information about related-parameters, see Table 2.

Table 2 Service backup parameters

Parameter	Description
Back up NAT444 port blocks	Backs up NAT444 port blocks dynamically.
Back up sessions	Backs up sessions and dynamic entries of session-based services. You must select this feature for IRF HA.
Back up DNS Back up HTTP	Backs up DNS and HTTP. A device removes a DNS or HTTP connection if packet exchange is inactive. When a switchover interrupts a connection, the DNS or HTTP client re-initiates the connection immediately, which has little impact on user services. Typically, you do not need to enable DNS or HTTP backup.
Back up IPsec SAs	Backs up the lowest sequence number of the IPsec anti-replay window in the inbound direction and the anti-replay sequence numbers of outgoing IPsec packets on interfaces. This feature ensures continuity of IPsec traffic and the anti-replay service after a switchover.
Back up last hops	Backs up the last hop information on interfaces enabled with last hot holding. This feature ensures continuity of the last hop holding service after a switchover.

Parameter	Description
	Last hop holding implements symmetric routing. It tracks the last hop MAC address for a connection's first outgoing IP packet, and sends the return packets to the hop that transmitted the request.

Configure redundancy groups and Reth interfaces

1. Click the **System** tab.
2. In the navigation pane, select **Virtualization Advanced Settings** > **IRF Advanced Settings**.

   The **IRF Advanced Settings** page opens.
3. Click **Redundancy groups**.
4. Click **Create**, configure the redundancy group name, and click **OK**.
5. Configure the redundancy group and Reth interfaces. For more information about the related parameters, see Table 3 and Table 4.

Table 3 Redundancy group parameters

Parameter	Description
Member Devices	Specify a maximum of two member devices for the redundancy group. One member device is the primary device, and the other is the secondary device. Typically, the primary device is the IRF master.
Member ID	Set the IRF member ID of each device.
Member interfaces	Specify the member interfaces of the redundancy group. Configure member interfaces when the upstream and downstream devices of the HA system run a dynamic routing protocol. In this scenario, you must configure the uplink and downlink physical Ethernet interfaces of the member devices as member interfaces of the redundancy group.

Parameter	Description
Reth interfaces	Configure Reth interfaces. Use Reth interfaces when the upstream and downstream devices of the HA system do not run a dynamic routing protocol. For more information, see Table 5. You must configure a minimum of two Reth interfaces, one containing uplink interfaces and the other containing downlink interfaces.
Track	Associate track entries with the redundancy group to trigger redundancy group member switchover.

Table 4 Advanced settings for a redundancy group

Parameter	Description
Hold-down timer	Set the hold-down timer. This timer specifies the minimum interval between two switchovers to prevent frequent switchovers.
Preemption delay timer	Set the preemption delay timer. This timer specifies the delay before a switchback.
Manual switchover	Manually perform a switchover or switchback.

6. Click **Create** in the **Reth interfaces** area.
7. Configure the Reth interface. For more information about the related parameters, see Table 5.

Table 5 Reth interface parameters

Parameter	Description
Primary member interface	Select an uplink or downlink interface on the primary member device.
Secondary member	Select an uplink or downlink interface on the secondary member

Parameter	Description
interface	device.
Fast failback	Set the status of the fast failback feature. Fast failback reduces the failback time when traffic is switched from the secondary member interface back to the primary member interface. This feature sets the physical link state of the primary member interface to up when that interface is in inactive state. Only the data link layer state of that interface is set to down.

You can configure multiple Reth interfaces in a redundancy group. Typically, you must configure at least two Reth interfaces. One Reth interface contains the uplink interfaces on the member devices, and the other contains the downlink interfaces on the member devices.

Contexts

This help contains the following topics:

Introduction

A physical firewall or an IRF fabric can be virtualized into multiple logical firewalls called contexts. Each context is assigned separate hardware and software resources, and operates independently of other contexts. From the user's perspective, a context is a standalone firewall.

Default context and non-default contexts

A device supporting contexts is considered to be a context. This context is called the default context. The default context always uses the name **Admin** and the ID 1. You cannot delete it or change its name or ID.

When you log in to the physical firewall, you are logged in to the default context. On the default context, you can perform the following tasks:

- Manage the entire physical firewall.
- Create and delete non-default contexts.
- Assign non-default contexts resources, including CPU resources, disk space, memory space, interfaces, and VLANs.

You cannot create contexts on a non-default context.

A non-default context can use only resources assigned to it. Resources that are not assigned to non-default contexts belong to the default context.

Unless otherwise stated, the term "context" on webpages refers to a non-default context.

Assigning resources to a context

You can assign a context CPU resources, disk space, memory space, interfaces, and VLANs.

Assigning VLANs to a context

When you create a context, you can specify whether the context share VLAN resources with other contexts.

- **Shared mode**—Share VLAN resources with other contexts. The VLANs can be created and managed only on the default context. Non-default contexts can use only VLANs assigned from the default context. A VLAN can be used by multiple contexts. After receiving a packet, the physical device forwards the packet to the context that matches the incoming interface and VLAN tag of the packet. This mode applies scenarios where multiple contexts share the same VLANs.
- **Exclusive mode**—Do not share VLAN resources with other contexts. Administrators of the context must log in to the context and create VLANs for the context. This mode applies scenarios where contexts require their independent VLANs.

Assigning interfaces to a context

By default, all interfaces belong to the default context. A non-default context cannot use any interfaces. To enable a non-default context to communicate, you must assign it interfaces.

You can assign interfaces to contexts in exclusive or shared mode:

- **Exclusive mode**—An interface assigned to a context in this mode belongs to the context exclusively. After logging in to the context, you can see the interface and use all commands supported on the interface.
- **Shared mode**—When you assign an interface to multiple contexts in shared mode, the system creates a virtual interface for each context. The virtual interfaces use the same name as the physical interface but have different MAC addresses and IP addresses. They forward and receive packets through the physical interface. The shared mode improves interface usage.

  You can see the physical interface and perform all commands supported on the interface from the default context. The administrator of a context can only see the context's virtual interface and use the shutdown, description, and network- and security-related commands.

Specifying a CPU weight for a context

When the CPU resources cannot meet the processing requirements from contexts, the system allocates CPU resources as follows:

1. Identifies the CPU weights of all contexts.
2. Calculates the percentage of each context's CPU weight among the CPU weights of all contexts.
3. Allocates CPU resources to contexts based on their CPU weight percentages.

For example, three contexts share the same CPU. You can assign a weight of 2 to the key context and a weight of 1 to each of the other two contexts. When the system is running out of CPU resources, the key context can use approximately two times of the CPU resources that each of the other two contexts can use.

Assigning disk and memory resources to a context

To prevent one context from occupying too many disk or memory resources, specify a disk space percentage and a memory space percentage for the context.

Before you specify a disk or memory space percentage for a context, start the context and view t
of disk or memory space that the context is using. Make sure the disk or memory space you assi
context is sufficient for the context to start and operate correctly.

Setting the maximum number of concurrent unicast sessions

A large number of sessions occupy too much memory. This degrades context performance and affects other contexts. When the maximum number is reached, no additional sessions can be established. To solve this issue, set the maximum number of concurrent unicast sessions for a context.

This feature does not affect local traffic, such as FTP traffic and Telnet traffic.

If the maximum number you set is smaller than the number of existing concurrent unicast sessions, this setting still takes effect. The context does not delete extra existing concurrent unicast sessions and allows new unicast sessions to be created only when the number of concurrent unicast sessions drops below the maximum number.

Setting the upper limit of the session establishment rate

This feature limits the number of sessions that can be established per second for a context. If a context establishes sessions too frequently, other contexts will not be able to establish sessions because of inadequate CPU processing capacity. When the upper limit is reached for a context, no additional sessions can be established.

This feature does not affect local traffic, such as FTP traffic and Telnet traffic.

Setting the maximum number of security policy rules

This feature limits the number of security policy rules that can be configured for a context. Security policy rules occupy memory space. Configuring too many security policy rules might affect operation of other features. When the upper limit is reached for a context, no additional security policy rules can be configured.

If the maximum number you set is smaller than the number of existing security policy rules, this setting still takes effect. The context does not delete extra existing security policy rules and allows new security policy rules to be created only when the number of security policy rules drops below the maximum number.

Setting the maximum number of SSL VPN users

This feature limits the number of SSL VPN users that can log in to a context. When the maximum number is reached, the context will reject the login requests of new SSL VPN users.

If the maximum number you set is smaller than the number of SSL VPN users that already have logged in to a context, this setting still takes effect. The context does not log out the currently logged-in users and allows new users to log in only when the number of the logged-in users drops below the maximum number.

Setting a throughput threshold

This feature limits the throughput for a context to prevent it from occupying too many shared resources on the device. This feature drops service packets preferentially to ensure forwarding of protocol packets.

Collecting information

On the default context, you can collect log messages, diagnostic information, and configuration information about multiple or all contexts.

Rate limiting

Rate limiting takes effect only on active contexts that share interfaces with other contexts.

Rate limiting controls the numbers of incoming broadcast packets and multicast packets in a second on contexts. This feature prevents a context from using too many resources and degrading the service processing capabilities of other contexts.

This feature uses the following limits:

- **Total broadcast rate limit**—Limit on the total number of incoming broadcast packets in a second on the device.

- **Total multicast rate limit**—Limit on the total number of incoming multicast packets in a second on the device.
- **Per-context broadcast rate limit**—Limit on the number of incoming broadcast packets in a second on a context.
- **Per-context multicast rate limit**—Limit on the number of incoming multicast packets in a second on a context.

When both a per-context limit and the corresponding total limit are reached, the device drops subsequent packets of the type that arrive at the context.

Setting a total limit to 0 disables the corresponding rate limiting feature.

If an effective per-context limit is smaller than 1000, the value is the default limit. A default limit is the corresponding total limit divided by the number of active contexts that share interfaces with other contexts.

If an effective per-context limit is equal to or greater than 1000, the value might be the default limit or the configured limit.

Restrictions and guidelines

Restrictions and guidelines: Stopping a context

Stop a context with caution. Stopping a context stops all services on the context and logs out all users on the context.

Restrictions and guidelines: VLAN assignment

- VLANs to be shared must already exist. Before assigning VLANs to contexts, you must create the VLANs on the default context.
- The following VLANs cannot be shared among contexts:
  - VLAN 1.
  - Default VLANs of ports.
  - VLANs for which VLAN interfaces have been created.

Restrictions and guidelines: Interface assignment

- Physical interfaces can be assigned to a context in shared or exclusive mode. Logical interfaces such as subinterfaces and aggregate interfaces can be assigned to a context only in shared mode.
- After assigning a subinterface to a context, you cannot assign its primary interface to any contexts. After assigning a primary interface to a context, you cannot assign its subinterfaces to any contexts.
- After assigning an interface to one context in shared mode, you cannot assign the interface to other contexts in exclusive mode before reclaiming the interface from the context.
- When the device operates in IRF mode, do not assign IRF physical interfaces to a non-default context.
- Member interfaces of an aggregate interface cannot be assigned to a context.
- A member interface of a Reth interface cannot be assigned to a context. If a member interface of a Reth interface is a subinterface, the corresponding primary interface cannot be assigned to a context either.

Restrictions and guidelines: Information collection

- On the default context, you cannot collect log messages for a non-default context that is never started.
- On the default context, you cannot collect configuration information for a non-default context that is not started.

Configure a context

1. Display assignment and configuration information about interfaces.
2. Create a context.
3. Assign resources to the context:
    - Assign VLANs and interfaces to the context.
    - Assign CPU, disk, and memory resources to the context
    - Set the maximum number of concurrent unicast sessions.
    - Set the upper limit of the session establishment rate.
    - Set the maximum number of security policy rules.
    - Set the maximum number of SSL VPN login users.
    - Set the throughput threshold.
4. Monitor resource usage on the context.

Administrators

Introduction

An administrator configures and manages the device from the following aspects:

- **User account management**—Manages user account information and attributes (for example, username and password).
- **Role-based access control**—Manages user access permissions by user role.
- **Password control**—Manages user passwords and controls user login status based on predefined policies.

The service type of an administrator can be HTTP, HTTPS, SSH, Telnet, FTP, PAD, or terminal. A terminal user can access the device through the console port.

User account management

A user account on the device manages attributes for users that log in to the device with the same username. The attributes include the username, password, role, services, and password control parameters.

Role-based access control

The device implements access permission control for users by assigning roles to the users. A role contains a set of features that are accessible or inaccessible to users.

Access permission control

On the Web interface, you can configure a role to have access permissions to specific Web pages and deny a role from accessing specific Web pages. These Web pages are called Web menus.

The Web menus are controlled based on the following options:

- **Read-only**—If you select this option, the role that you configure has access permissions to the Web menus that display configuration and maintenance information of the specified item.
- **Read and write**—If you select this option, the role that you configure has access permissions to the following Web menus of the specified item:
  - Web menus that display configuration and maintenance information.
  - Web menus that configure the item.
- **No permissions**—If you select this option, the role that you configure does not have any access permission to the specified item.

Predefined roles

The system provides predefined roles. The access permissions of these roles differ, as shown in Table 1. If the predefined roles cannot meet users' requirements, administrators can configure roles for the users as required.

Table 1 Predefined roles and permissions matrix

Role name	Permissions
network-admin	This role has the rights to access all features in the system.
security-admin	This role has the rights to configure security service features and monitor processing status of security services.
audit-admin	This role only has the rights to audit device operations.

Role name	Permissions
system-admin	This role has the rights to configure system features and monitor device running status.
context-admin	This role has the rights to access all features in a context.
vsys-admin	This role has the rights to access all features in a vSystem. Support for this role depends on the device model.

Role assignment

Assign access permissions to a user by assigning a role to the user. The user can use the collection of items accessible to the role assigned to the user.

Depending on the authentication method, role assignment has the following methods:

- **Local AAA authorization**—If a user passes local authorization, the device assigns the role specified in the local user account to the user.
- **Remote AAA authorization**—If a user passes remote authorization, the remote AAA server assigns the role specified on the server to the user.

If a user is not assigned any role, it cannot log in to the device.

You can assign only one role to a user.

Password control

Password control provides the following features:

- Manage login and super password setup, expirations, and updates for local users.
- Control user login status based on predefined policies.

Password control settings include global settings and user-specific settings.

- The settings on the **Administrator Password Control** page are global password control settings, which apply to all administrator users.
- The password control settings configured on the **Create Administrator** or **Edit Administrator** page are user-specific settings, which apply only to the user.

Unless otherwise stated, user-specific password control settings have higher priority than global password control settings.

Minimum password length

You can define the minimum length of user passwords. The system rejects a password if it is shorter than the configured minimum length.

Password complexity check

The strength of a password increases as its complexity grows. A less complicated password is more likely to be cracked. For example, a password that contains the username or repeated characters is more likely to be cracked than those do not. To increase system security, configure a password complexity policy to make sure the user-configured passwords are complex enough against most password attacks.

You can apply the following password complexity requirements:

- A password cannot contain the username or the username spelled backwards. For example, if the username is **abc**, the password cannot be **abc982** or **2cba**. To have this requirement take effect on a user, you must enable it both on the global and user-specific password control configuration pages.
- A password cannot contain more than two consecutive identical characters. For example, password **a111** is not allowed. To have this requirement take effect on a user, you must

enable it either on the user-specific password control configuration page or on the global password control configuration page.

Password composition check

To have the user-specific settings for this feature take effect, you must also enable this feature on the global password control configuration page.

A password can be a combination of characters from the following types:

- Uppercase letters A to Z.
- Lowercase letters a to z.
- Digits 0 to 9.
- Special characters. See Table 2.

Table 2 Special characters

Character name	Symbol	Character name	Symbol
Ampersand sign	&	Apostrophe	'
Asterisk	*	At sign	@
Back quote	`	Back slash	\
Blank space	N/A	Caret	^
Colon	:	Comma	,
Dollar sign	$	Dot	.
Equal sign	=	Exclamation point	!
Left angle bracket	<	Left brace	{

Character name	Symbol	Character name	Symbol
Left bracket	[	Left parenthesis	(
Minus sign	-	Percent sign	%
Plus sign	+	Pound sign	#
Quotation marks	"	Right angle bracket	>
Right brace	}	Right bracket	]
Right parenthesis	)	Semi-colon	;
Slash	/	Tilde	~
Underscore	_	Vertical bar	|

Depending on the system's security requirements, you can set the minimum number of character types a password must contain and the minimum number of characters for each type, as shown in Table 3.

Table 3 Password composition policy

Password combination level	Minimum number of character types	Minimum number of characters for each type
Level 1	One	One
Level 2	Two	One
Level 3	Three	One
Level 4	Four	One

When a user sets or changes a password, the system examines whether the password meets the combination requirement. If the password does not meet the requirement, the operation fails.

Password updating

This feature allows you to set the minimum interval at which users can change their passwords. A user can only change the password once within the specified interval.

The minimum interval does not apply to the following situations:

- A user is prompted to change the password at the first login.
- The password expiration time expires.

Password expiration

To have the user-specific settings for this feature take effect, you must also enable this feature on the global password control configuration page.

Password expiration imposes a lifecycle on a user password. After the password expires, the user needs to change the password.

The system displays an error message for a login attempt with an expired password. The user is asked to provide a new password. The new password must be valid, and the user must enter exactly the same password when confirming it.

Telnet users, SSH users, and console users can change their own passwords. FTP users must have their passwords changed by the administrator.

Password expiration notification

When a user logs in, the system determines whether the password will expire in a time equal to or less than the specified notification period. If so, the system notifies the user when the password will expire and provides a choice for the user to change the password.

- If the user sets a new valid password, the system records the new password and the setup time.
- If the user does not or fails to change the password, the system allows the user to log in by using the current password until the password expires.

Telnet users, SSH users, and console users can change their own passwords. FTP users must have their passwords changed by the administrator.

Login with an expired password

You can allow a user to log in a certain number of times within a period of time after the password expires. For example, if you set the maximum number of logins with an expired password to 3 and the time period to 15 days, a user can log in three times within 15 days after the password expires.

Password history

This feature allows the system to store passwords that a user has used. When a user changes the password, the system compares the new password with the current password and those stored in the password history records. The new password must be different from the current one and those stored in the history records by a minimum of four different characters. If the new password does not meet this requirement, the system displays an error message and rejects the password change operation.

You can set the maximum number of history password records for the system to maintain for each user. When the number of history password records exceeds the setting, the most recent record overwrites the earliest one.

Current login passwords are not stored in the password history for administrators. Administrators have their passwords saved in cipher text, which cannot be recovered to plaintext passwords.

Login attempt limit

Limiting the number of consecutive login failures can effectively prevent password guessing. To have the user-specific settings for this feature take effect, you must also enable this feature on the global password control configuration page.

Login attempt limit takes effect on FTP and VTY users. It does not take effect on the following types of users:

- Nonexistent users (users not configured on the device).
- Users logging in to the device through console ports.

If a user fails to log in, the system adds the user account and the user's IP address to the password control blacklist. When the user fails to log in after making the maximum number of consecutive attempts, login attempt limit limits the user and user account in any of the following ways:

- **Lock permanently**—Disables the user account until the account is manually removed from the password control blacklist.
- **Not lock**—Allows the user to continue using the user account. The user's IP address and user account are removed from the password control blacklist when the user uses this account to successfully log in to the device.
- **Lock temporarily**—Disables the user account for a period of time.

  The user can use the account to log in when either of the following conditions exist:

  - The locking timer expires.
  - The account is manually removed from the password control blacklist before the locking timer expires.

This account is locked only for this user. Other users can still use this account, and the blacklisted use other user accounts.

Maximum account idle time

You can set the maximum account idle time for user accounts. When an account is idle for this period of time since the last successful login, the account becomes invalid.

Password strength management

When an administrator user logs in with a weak password, the device prompts the user to change the password regardless of whether password control is enabled.

- If mandatory weak password change is enabled, the user must change its weak password to a complicated enough password in order to log in to the device.
- If mandatory weak password change is disabled, the user can ignore the password change prompt and continue to log in to the device.

The device determines a password is weak if that password has the following characteristics:

- Shorter than the minimum password length. For more information, see "Minimum password length."
- Incompliant with the password composition policy. For more information, see "Password composition check."
- Contain the username or the username spelled backwards. For more information, see "Password complexity check."
- Contain three or more identical consecutive characters when password control is enabled. For more information, see "Password complexity check."

Restrictions and guidelines

Restrictions and guidelines: Role-based access control

Any access permission modification for a role takes effect only on users that are logged in with the role after the modification.

Restrictions and guidelines: Password control

- When a user fails the maximum number of consecutive attempts, the system prevents the user from using the user account to log in through the user's IP address.
- For password control settings to take effect, you must enable password control. To enable password control, click **Password control** on the **Administrators** page to enter the **Administrator Password Control** page and select **Enable password control**.
- The **Administrator Password Control** page and the **User Password Control** page share the password control settings. If you change a password control setting on one page, the system automatically synchronizes the new setting to the other page.
- When the password control feature is enabled, a new password must contain a minimum of four different characters.
- The following settings can be configured on both the **Administrator Password Control** page and in the **Advanced settings** area on the **Create Administrator** or **Edit Administrator** page:
    - Password expiration time.
    - Minimum password length.
    - Password complexity policy.

- Password composition policy.
- Maximum login attempts.

The password control settings on the **Administrator Password Control** page take effect on all administrators. However, the settings on the **Create Administrator** or **Edit Administrator** page have a higher priority than those on the **Administrator Password Control** page.

Restrictions and guidelines: Password strength management

To enable mandatory weak password change, you must enable a minimum of one password strength check criterion.

The mandatory weak password change feature takes effect only on users that log in to the device after the feature is enabled. The feature does not affect users that have logged in to the device.

Restrictions and guidelines: FTP users

FTP users do not support accounting. These users are not restricted by the value in the **Max concurrent logins** field.

An FTP user cannot log in to the device with an expired password. FTP users must have their passwords changed by the administrator.

Date and time

This help contains the following topics:

- Introduction
  - Date and time obtaining methods
  - NTP/SNTP
  - NTP/SNTP clock source
  - NTP and SNTP clock source authentication
- Restrictions and guidelines

Introduction

Date and time obtaining methods

Correct system time is essential to network management and communication. Configure the system time correctly before you run the device on the network.

The device can use one of the following methods to obtain the system time:

- **Manual configuration**—Uses the locally set system time, whether or not the time zone or daylight saving time has been configured. Then, the device uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

- **Automatic synchronization**—Periodically obtains the UTC time by using a time protocol, and uses the UTC time, time zone, and daylight saving time to calculate the system time. The system time calculated by using the UTC time from a time source is more precise.

If you configure or change the time zone or daylight saving time after the device obtains the system time, the device recalculates the system time.

Make sure each network device uses the time zone of the place where the device resides.

Set the daylight saving time for devices that reside in a region that uses daylight saving time. Typically, the system time is one hour ahead of the standard time during the daylight saving time. If the system time page is open when the daylight saving time starts, refresh the page to display the adjusted time.

NTP/SNTP

NTP is used to synchronize system clocks among distributed time servers and clients on a network.

SNTP is a simplified, client-only version of NTP. It uses the same packet format and packet exchange procedure as NTP, but provides faster synchronization at the price of time accuracy.

Support for this feature depends on the device model.

NTP/SNTP clock source association modes

NTP supports the client/server mode and symmetric active/passive mode (peer mode). As shown in Table 1, the device can operate only as a client in client/server mode or a symmetric active peer in peer mode.

SNTP supports only the client/server mode. An SNTP-enabled device can receive time from NTP servers, but cannot provide time services to other devices.

Table 1 NTP association modes

Mode	Working process	Principle	Application scenario
Client/server	On the client, specify the IP address of the NTP server. A client sends a clock synchronization message to the NTP servers. Upon receiving the message, the servers automatically operate in server mode and send a reply. If the client can be synchronized to multiple time servers, it selects an optimal clock and synchronizes its local clock to the optimal reference source after receiving the replies from the servers.	A client can synchronize to a server, but a server cannot synchronize to a client.	This mode is intended for configurations where devices of a higher stratum synchronize to devices with a lower stratum.
Symmetric active/passive	On the symmetric active peer, specify the IP address of the symmetric passive peer. A symmetric active peer periodically sends clock synchronization messages to a symmetric passive peer. The symmetric passive peer automatically operates in symmetric passive mode and sends a reply. If the symmetric active peer can be synchronized to multiple time servers, it selects an optimal clock and synchronizes its local clock to the optimal reference source after receiving the replies from the servers.	A symmetric active peer and a symmetric passive peer can be synchronized to each other. If both of them are synchronized, the peer with a higher stratum is synchronized to the peer with a lower stratum.	This mode is most often used between servers with the same stratum to operate as a backup for one another. If a server fails to communicate with all the servers of a lower stratum, the server can still synchronize to the servers of the same stratum.

Support for this feature depends on the device model.

NTP and SNTP clock source authentication

Use this feature to authenticate NTP messages for security purposes. If an NTP message passes authentication, the device resolves the message to obtain time synchronization information. If not, the device discards the message. This function makes sure the device does not synchronize to an unauthorized time server.

Support for this feature depends on the device model.

Restrictions and guidelines

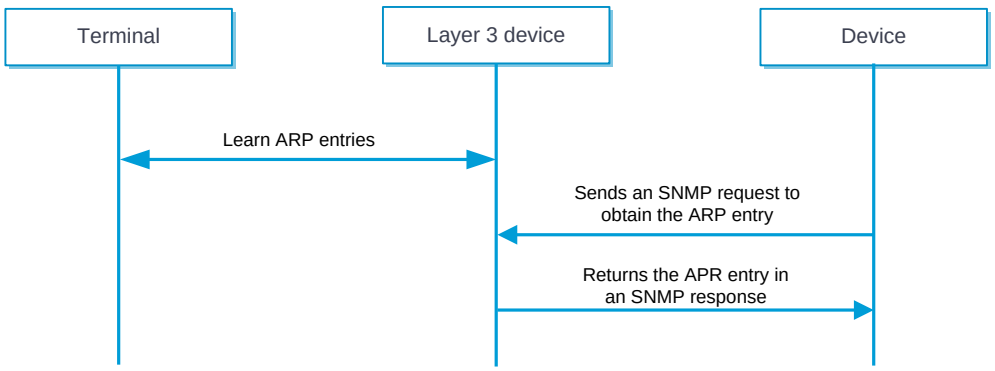
- To ensure a successful NTP authentication in client/server mode, enable NTP authentication and configure the same authentication key ID and key on the server and client.
- To ensure a successful NTP authentication in symmetric active/passive mode, enable NTP authentication and configure the same authentication key ID and key on the active peer and passive peer.

MAC address learning through a Layer 3 device

Introduction

This feature enables the device to learn the MAC address of a terminal (a PC for example) when a Layer 3 device (typically a gateway) exists between the device and the terminal for network traffic control.

Figure 1 MAC address learning through a Layer 3 device workflow



As shown in Figure 1, MAC address learning through a Layer 3 device proceeds as follows:

2. The Layer 3 device learns the IP-MAC binding of the terminal, and then generates an ARP entry.
3. The device sends SNMP requests to the Layer 3 device at the specified intervals to request the ARP entry.
4. The Layer 3 device sends a response that contains the ARP entry.
5. Upon receiving the response, the device saves the ARP entry in the memory. Then it can learn the MAC address of the terminal.

Restrictions and guidelines

- Make sure the Layer 3 device supports SNMPv2c or SNMPv3, has SNMP agent enabled, and has a community name configured.
- Only MAC addresses mapped from IPv4 addresses can be learned.
- Make sure no NAT devices exist between the device and the Layer 3 device.
- This feature is not applicable to a VRF network.

Configure MAC address learning through a Layer 3 device

Procedure

1. Select **System** > **Maintenance** > **MAC Learning Through L3 Device** > **L3 Device Access Setting**.
2. Click **Enable** to enable MAC address learning through a Layer 3 device.
3. (Optional.) Set the polling interval and idle timeout

Table 1 Configuration items for MAC address learning through a Layer 3 device

Item	Description
Polling interval	Interval for sending SNMP requests, in seconds
Idle timeout	Idle timeout for SNMP responses, in seconds

4. Click **Apply**.

5. Add a Layer 3 device:

   a. Click **Add**.

   b. Configure the following settings:

Item	Description
SNMP version	SNMP version. Options include v2c and v3.
IP address	IP address of the target Layer 3 device, typically the gateway of the terminal network. Only IPv4 addresses are supported.
Community name (SNMPv2c)	Devices in a community use a community name for authentication. The device can communicate with the Layer 3 device only if it has the same community name as the SNMP agent on the Layer 3 device.
Username (SNMPv3)	Authentication can be performed only if the device and the SNMP agent on the Layer 3 device have the same username.
Authentication algorithm	For a successful authentication, make sure these settings are the same as those on the SNMP agent of the Layer 3 device.
Authentication password	
Encryption algorithm	
Encryption password	

6. Click **OK**.

SNMP

Introduction

Simple Network Management Protocol (SNMP) is used for a management station to access and operate the devices on a network, regardless of their vendors, physical characteristics, and interconnect technologies.

SNMP enables network administrators to read and set the variables on managed devices for state monitoring, troubleshooting, statistics collection, and other management purposes.

SNMP framework

The SNMP framework contains the following elements:

- **SNMP manager**—Works on an NMS to monitor and manage the SNMP-capable devices in the network.
- **SNMP agent**—Works on a managed device to receive and handle requests from the NMS, and sends notifications to the NMS when events, such as an interface state change, occur.
- **Management Information Base (MIB)**—Specifies the variables (for example, interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set.

SNMP versions

The device supports SNMPv1, SNMPv2c, and SNMPv3. For an NMS and an SNMP agent to establish an SNMP connection, they must use the same SNMP version.

- **SNMPv1**—Uses community names for authentication. To access an SNMP agent, an NMS must use the same community name as set on the SNMP agent. If the community name used by the NMS differs from the community name set on the agent, the NMS cannot establish an SNMP session to access the agent or receive traps from the agent.
- **SNMPv2c**—Uses community names for authentication. SNMPv2c is compatible with SNMPv1, but supports more operation types, data types, and error codes.
- **SNMPv3**—Uses a user-based security model (USM) to secure SNMP communication. You can configure authentication and privacy mechanisms to authenticate and encrypt SNMP packets for integrity, authenticity, and confidentiality.

Configuration management

Introduction

A configuration file contains a set of software feature settings for the device. You can save software feature settings to a configuration file so the configuration can survive a reboot. You can also back up configuration files to a server for future use. For example, import a configuration file to multiple devices that share the same configuration.

Configuration types

Factory defaults

Factory defaults are basic settings that came with the device. The device starts up with the factory defaults if no startup configuration files are available.

Startup configuration

The device uses the startup configuration to configure software features during startup. After the device starts up, you can specify the configuration file to be loaded at the next startup. If no startup configuration files are available, the device starts up with the factory defaults.

Running configuration

The running configuration takes effect while the device is operating. It includes unchanged startup settings and new settings. The running configuration is stored in memory and is cleared at a device reboot or power-off. To use the running configuration after a power cycling or reboot, save it to a configuration file.

Configuration backup

Use this feature to back up the running configuration on the device to a local configuration file or to a configuration file on an FTP or TFTP server. The device supports immediate backup and periodic backup.

You can use the backup configuration files for configuration rollback.

Configuration rollback

Use this feature to replace the running configuration with the configuration in a configuration file. The configuration file can be saved on the local device or on an FTP or TFTP server. If you use a configuration file on an FTP or TFTP server for configuration rollback, you must specify the rollback time.

Restrictions and guidelines

Restoring the factory defaults removes all configurations you have made from the device.

If server-based backup or rollback is used, make sure the device can reach the remote FTP or TFTP server.

Manage the running configuration

Back up the running configuration

1. Click the **System** tab.
2. In the navigation pane, select **Maintenance** > **Configuration Management**.
3. Click **Back up current configuration**.
4. Configure the configuration backup parameters.

Table 1 Configuration backup configuration items

Item	Description
Backup type	Select a location to save the backup configuration files: • **Back up to local**. • **Back up to server**.
Auto backup interval	Enter the interval for periodic configuration backup. If you do not configure this parameter, the device does not periodically back up the running configuration.
Max backup files	Enter the maximum number of backup configuration files that can be saved on the device. After the maximum number is reached, the system deletes the oldest backup file for the new backup file.
Local backup path	Enter the directory where the backup configuration files will be saved on the device.

Item	Description
	The directory must already exist on the device.
Prefix name	Enter a file name prefix for backup configuration files. Backup configuration files are named in the format of *prefix_serial number***.cfg**.
Immediate backup	To back up the running configuration immediately, select this item.
Server type	Select the file transfer protocol. Options include FTP and TFTP.
Address	Enter the IPv4 or IPv6 address of the file server.
VRF	Select the name of the VPN instance to which the file server belongs.
Username	Enter the username for logging in to the file server.
Password	Enter the password for logging in to the file server.
Port	Enter the port number of the file server.
Backup path	Enter the path where the backup configuration files will be saved on the server.

5. Click **OK**.

Roll back the configuration

1. Click the **System** tab.
2. In the navigation pane, select **Maintenance** > **Configuration Management**.
3. Click **Configure rollback**.
4. Select the rollback file location:

- To use a configuration file saved on the local storage device, select **Local device**.
- To use a configuration file saved on a remote file server, select **Server**.

5. Roll back the configuration or schedule a rollback:
   - **If you are using a local configuration file for rollback, specify a** local directory in the **Location** field, click **Access to the file** to show configuration files in the directory, identify the configuration file you are using, and then click its **Roll Back** link to roll back the configuration.
   - **If you are using a configuration file on a remote server for rollback, config**ure the parameters as shown in Table 2 to schedule a rollback, and then click **OK**.

Table 2 Configuration items for server-based rollback

Item	Description
Server type	Select the server type. Options include FTP and TFTP.
Address	Enter the IPv4 or IPv6 address of the server.
VRF	Select the name of the VPN instance to which the server belongs.
Username	Enter the username for logging in to the FTP or TFTP server.
Password	Enter the password for logging in to the FTP or TFTP server.
Port	Enter the port number of the FTP or TFTP server.
Rollback file path	Enter the path where the rollback configuration file is saved.
Default rollback file	Enter the name of the default rollback configuration file. If you do not specify a rollback configuration file, the default rollback configuration file will be used.
Rollback file	Enter the name of the rollback configuration file.

Item	Description
Rollback date	Set the date on which the configuration rollback will be performed.
Rollback time	Set the time when the configuration rollback will be performed. Setting a rollback time is required.
Cancel scheduled rollback	Select this option to cancel the rollback schedule.

Reboot

Introduction

The reboot feature enables you to remotely reboot the device.

Restrictions and guidelines

Rebooting the device might cause service interruption. Before performing this task, make sure you understand its impact on the live network.

As a best practice, save the running configuration before rebooting the device.

About

This help provides information about the device, including the device name, sequence number, model, description, location, contact, software version, vendor, production serial number, and legal statements.

Ping

Introduction

Use the ping utility to determine if a destination is reachable. You can specify the IP address or host name of the destination when you perform a ping operation. The ping page will display statistics about the ping operation. You can measure the network performance by analyzing these statistics.

Tracert

Introduction

Tracert (also called Traceroute) enables retrieval of the IP addresses of Layer 3 devices in the path to a destination. In the event of network failure, use tracert to test network connectivity and identify failed nodes. You can specify the IP address or host name of the destination when you perform a tracert operation.

Packet capture

This help contains the following topics:

- Introduction
- Restrictions and guidelines
- Perform packet capture
    - Start packet capture
    - Configure packet capture settings

Introduction

The packet capture feature captures incoming and outgoing packets, generates packet capture records, and saves the records to a .cap file. The file can reside on the device or a remote file server. You can use a packet analyzer such as Wireshark to view the file for traffic analysis.

Restrictions and guidelines

- Only one packet capture process can run on the device.
- You can configure packet capture parameters only when packet capture is not started.
- Start packet capture only when necessary. Packet capture affects device performance.

- If packet capture saves .cap files on the device, back up the .cap files on the device as required after you finish packet capture. Starting packet capture again deletes the existing .cap files.
- Packet capture is not supported on shared interfaces of a non-default context.

Perform packet capture

Start packet capture

1. Select **System** > **Diagnosis Center** > **Packet Capture**.
2. Click **Start packet capture**.
3. Configure filters as shown in Table 1.

Table 1 Configuration items for setting filters

Item	Description
Interface	Capture packets received or sent by an interface.
ACL	Capture packets permitted by an advanced ACL.

4. Click **Start**.

   On the **Packet Capture** page, the **Packet Capture Status** field displays **Started**.
5. To stop packet capture, click **Stop packet capture**.

   The **Packet Capture Status** field displays **Stopped**. The bottom pane displays information about generated .cap files.

Configure packet capture settings

1. Select **System** > **Diagnosis Center** > **Packet Capture**.
2. Click **Set packet capture parameters**.
3. Configure packet capture parameters as shown in Table 2:

Table 2 Packet capture configuration items

Item	Description
Maximum bytes per packet	Specify the maximum number of bytes for a capture record. If a packet is longer than the value of this item, the system truncates the packet.
Maximum packets per file	Specify the maximum number of packet capture records for a .cap file. The system first saves packet capture records to memory. After the maximum number of packet capture records for a file is reached, the system saves the records to a file and clears the records in memory. A greater value for this item requires more memory space. If the available memory space is limited, decrease the value.
Save files on the device	Save the .cap files on the device. If you select this option, you can set the **Maximum storage space** item to specify the maximum storage space for .cap files. After the maximum storage space is reached, the system stops capturing packets.
Save files to a remote server	Save the .cap files to an FTP or TFTP server. To save .cap files to an FTP server, you must configure the username and password for accessing the FTP server.

4. Click **OK**.

Webpage Diagnosis

This help contains the following topics:

- Introduction
- Restrictions and guidelines
- Perform a webpage diagnosis

Introduction

This feature outputs easy-to-read diagnosis results to help you quickly troubleshoot webpage access failures of internal users. With this feature, you do not need to manually ping servers or display log messages.

Restrictions and guidelines

- This feature supports only IPv4.
- This feature supports only HTTP webpages.
- Before starting a webpage diagnosis, you must configure security policies to ensure connectivity between the following security zones:
    - Security zone where the user resides.
    - Security zone where the Web server resides.
    - Security zone **Local**.

Perform a webpage diagnosis

1. Select **System** > **Diagnosis Center** > **Webpage Diagnosis**.
2. Configure webpage diagnosis parameters.

Table 1 Webpage diagnosis configuration items

Item	Description
User IP	IP address of the user.
User VRF	VPN instance to which the user belongs.
Webpage URL	URL that the user accessed, for example, http://www.example.com.
Webpage VRF	VPN instance to which the webpage belongs.

3. Click **Diagnose**.
4. View the webpage diagnosis result to analyze the failure and resolve the issue.
5. (Optional.) Click **Export** to export the webpage diagnosis result to a .xml file.

Diagnostic Info

Introduction

Diagnostic information is helpful in device routine maintenance and troubleshooting. You can collect diagnostic information for individual features or use this function to collect diagnostic information for all features by clicking a single button.

Packet trace

This help contains the following topics:

Introduction

The packet trace feature traces packets processed by security services, and provides detailed information about the packets to help you troubleshoot network failures. Examples of security services include attack protection, uRPF, session management, and connection limit services.

Application scenarios

Packet trace applies to scenarios where a large number of security services are deployed and it is difficult to locate network failures rapidly and accurately.

Packet trace modes

To meet troubleshooting requirements in various situations, the packet trace feature provides the following packet trace modes:

- **Tracing real traffic**—Traces real traffic on the device in a live network. Use this mode for troubleshooting in a live network.
- **Tracing imported packets**—Imports captured packets from a .cap or .pcap file and analyzes the packets. Use this mode if packets required for troubleshooting have been captured. Using this mode, you can help troubleshoot failures on other networks.
- **Tracing constructed packets**—Uses settings configured by the administrator to construct a packet and verify packet processing results for configured security services. When you complete device configuration, use this mode to create a packet to verify the expected packet processing result.

Restrictions and guidelines

- The system generates .cap files only if you select Capture diagnose packets before clicking Diagnose.
- You cannot export the same .cap files repeatedly. Once being exported, .cap files are deleted from the device.
- Importing captured packets from a .cap or .pcap file imports only packets of the first 10 data flows, 10 packets each data flow. The packet trace feature traces only imported packets that are complete. It does not trace packets that are incomplete.

Configure packet trace

Before enabling packet trace, configure the following items to identify the packets to be traced:

- **IP type**—Specifies the IPv4 or IPv6 packet type. To trace IPv4 packets, select **IPv4**. To trace IPv6 packets, select **IPv6**.
- **Incoming interface**—Specifies the incoming interface of the packets.
- **Protocol**—Specifies the protocol used by the packets.
- **Source address**—Specifies the source address of the packets.
- **Source port**—Specifies the source port of the packets.
- **Destination address**—Specifies the destination address of the packets.
- **Destination port**—Specifies the destination port of the packets.
- **Source MAC**—Specifies the source MAC of the packets.
- **Destination MAC**—Specifies the destination MAC of the packets.
- **VLAN ID**—Specifies the VLAN ID of the packets.
- **Diagnosis time**—Specifies the packet trace duration. When the specified time expires, packet trace stops. This setting is supported only in real traffic mode.
- Capture diagnose packets—Indicates whether to capture traced packets and save the packets to .cap files. To capture and save the packets, select this option. To export the .cap files, click Export, select Captured diagnostic packets, and click OK.

The packet trace output shows the packet processing procedures of security service modules. If a service module processes packets correctly, the system displays . If a service module drops packets, the system displays and the packet loss causes.

Load balancing test

Introduction

The administrator can test the load balancing result by specifying the protocol, source IPv4/IPv6 address, source port number, destination IPv4/IPv6 address, and destination port number.

Performing a load balancing test

Procedure

1. Select **System** > **Diagnosis Center** > **Load Balancing Test**.
2. Configure test parameters.

Table 1 Test parameter configuration items

Item	Description
Slot number	Specify the slot number to be tested.
IP type	IP address type: • IPv4 • IPv6
VPN instance	Specify the VPN instance to be tested.
Destination	Specify the destination IPv4/IPv6 address to be tested. Typically,

Item	Description
IPv4/IPv6 address	specify the IP address of the virtual server.
Source IPv4/IPv6 address	Specify the source IPv4/IPv6 address to be tested.
Protocol layer	Specify the layer of the information that can be identified by load balancing. • Layer 4: Identifies network layer and transport layer information. • Layer 7: Identifies network layer, transport layer, and application layer information.
Layer 4 protocol	Select a way to identify a protocol: • Protocol name • Protocol number
Protocol name	Specify the protocol to be tested: • ICMP • TCP • UDP
Protocol number	Enter the number of the protocol to be tested.
Layer 7 protocol	Specify a way to identify an HTTP packet: • Import HTTP packet • Construct HTTP packet
Import HTTP packet	Import the HTTP packet to be tested. The file containing the HTTP packet content must be suffixed with .txt, and cannot be larger than 5000 bytes.
HTTP request method	Specify an HTTP request method: • GET • POST
URL	Specify a URL for the HTTP packet, case sensitive. A URL can contain

Item	Description
	letters, digits, hyphens (-), underscores (_), and periods (.). The URL cannot contain consecutive periods and question marks (?).
HTTP packet header	Specify a space-separated list of up to 10 HTTP packet headers. A header cannot contain question marks (?).
HTTP packet content	Specify the content of the HTTP packet body. The HTTP packet content cannot contain question marks (?).
Destination port number	Enter the destination port number to be tested. Support for this parameter depends on the protocol.
Source port number	Enter the source port number to be tested. Support for this parameter depends on the protocol.

3. Click **Start testing**. For more information about the test result, see Table 2.

Table 2 Test result

Field	Description
Slot number	Slot number of the device. The displayed value for this field depends on your configuration.
Matched virtual server name	Name of the matching virtual server. The displayed value for this field depends on your configuration.
No virtual server is matched	N/A
Matched class name	Name of the matching class. The displayed value for this field depends on your configuration.
Default action is matched	N/A
Matched server farm name	Name of the matching default server farm. The displayed value for this field depends on your configuration.

Field	Description
Matched link group name	Name of the matching default link group. The displayed value for this field depends on your configuration.
Forwarding mode	Forwarding mode: • Load balancing is not performed because the destination address is the address of the local device. • Load balancing is not supported because an HTTP virtual server is matched. • Forwards packets. • Forwards packets to the real server. • Forwards packets to the link. • Drops packets. • Redirects packets.
Selected real server name	Name of the matching real server. The displayed value for this field depends on your configuration.
Selected link name	Name of the matching link. The displayed value for this field depends on your configuration.
Scheduling algorithm used to select a real server	Scheduling algorithm used to select the real server: • Predictor • Sticky method
Scheduling algorithm used to select a link	Scheduling algorithm used to select the link: • Predictor • Sticky method • Proximity
Packet drop reason	Packet drop reason: • Number of connections or bandwidth for the virtual server exceeded the limit. • No class is matched and no available server farm is configured.

Field	Description
	• No class is matched and no available link group is configured. • No available real server in the server farm. • No available link in the link group. • Action is drop. • A sticky entry was matched but the number of connections or bandwidth for the real server exceeded the limit. • A sticky entry was matched but the number of connections or bandwidth for the link exceeded the limit. • A class was matched but no available server farm exists in the action of the class. • A class was matched but no available link group exists in the action of the class. • The HTTP packet is invalid. • The HTTP request line is invalid. • The HTTP header is invalid. • The chunk HTTP content is invalid.

IPsec diagnosis

Introduction

IPsec diagnosis can detect the status of IPsec connections. If the diagnosed IPsec connection is faulty, you can use the diagnosis results to check for misconfigurations and find possible causes.

The following diagnosis modes are supported:

- **Data flow**—The system obtains the IPsec policy according to the specified data flow to initiate diagnosis of IPsec with the peer.
- **Interface**—The system obtains the IPsec policy according to the specified interface to initiate diagnosis of IPsec with the peer.
- **IP address**—The system starts diagnosis of IPsec with the peer (specified by its IP address) after the peer initiates the IPsec connection.

Table 1 IPsec diagnosis items

Item	Description
IPsec peer reachability	Determines whether a route to the peer IP address exists in the routing table.
Interface state	Determines the physical layer status and IP protocol layer status of the interface. The system determines the interface to check according to the diagnosis mode: • In data flow and IP address modes, the outgoing interface found through routing table lookup is checked.

Item	Description
	• In interface mode, the interface specified by the user is checked.
If IPsec policy applied on interface	Determines whether an IPsec policy is applied to the interface.
If ACL rule in IPsec policy matches specified flow	This item is available only for IPsec diagnosis in data flow mode. Check the IPsec policy configuration if this item displays **No**.
If ACL rule can match flow on the interface	This item is available only for IPsec diagnosis in interface mode. This item shows whether the ACL used in the IPsec policy contains permit rules to identify traffic that needs IPsec protection. The permit rules are required for IPsec to operate correctly.

IPsec policy configuration check	Checks if the IPsec policy configuration is complete.
	• In data flow or interface mode, the following settings are checked:
	  ◦ ACL used to identify the traffic to be protected.
	  ◦ Security parameters for IPsec SA negotiation.
	  ◦ Local and remote IP addresses of the IPsec tunnel.
	  ◦ SA parameters.
	• In IP address mode, the following settings are checked:
	  ◦ Security parameters for IPsec SA negotiation.
	  ◦ SA parameters.

IKE negotiation result	If the IKE negotiation is operating correctly, this item displays **IKE negotiation succeeded** or **IKE SA already exists**. Any other information indicates that the IKE negotiation is faulty. Follow the instructions to find the cause. For example, verify that the local end and peer end have correct and matching IKE profiles.
IPsec negotiation result	If the IPsec negotiation is operating correctly, this item displays **IPsec negotiation succeeded** or **IPsec tunnel already exists**. Any other information indicates that the IPsec negotiation is faulty. Follow the instructions to find the cause. For example, verify that the local end and peer end have correct and matching

Item	Description
	IPsec policy settings.

Restrictions and guidelines

- In data flow mode, specify the source and destination IP addresses of the data flow before IPsec encapsulation in the **Source IP address** and **Destination IP address** fields.
- In data flow and interface modes, IPsec diagnosis works only if the device can find an IPsec policy to initiate an IPsec connection. IPsec policies configured by using IPsec policy templates cannot initiate IPsec connections, so they are ignored during IPsec diagnosis in data flow or interface mode.
- An IPsec diagnosis in data flow or interface mode can last up to 20 minutes. After the timer expires, the diagnosis stops and the completed diagnosis items are displayed.
- An IPsec diagnosis in IP address mode starts when it detects an IPsec connection initiated by the peer and stops when it finishes diagnosis for the IPsec connection.
- Only one IPsec diagnosis can run at the same time.
- IPsec diagnosis is available only on the IPv4 network.
- The device supports IPsec policy-based IPsec diagnosis but does not support IPsec profile-based IPsec diagnosis.
- The VRF is the VPN instance of the interface where the IPsec policy is applied.

Fast Internet Access

Introduction

Perform this task to fast configure the device to access the Internet.

Access mode

Access modes include the routing mode and the transparent mode.

Routing mode

This mode uses the routing function of the device gateway. In this mode, three Internet access methods are supported. Select a method according to the information provided by the service provider.

1. Configure the WAN interface.

The WAN interface supports the following access methods, as shown in Table 1.

Table 1 Access methods

Item	Description
Specified IP address	Select this method when you get a fixed IP address from the service provider.
DHCP	Select this method if you want to automatically obtain IP addresses from the service provider (or DHCP server).

Item	Description
PPPoE	Select this method if you obtain an Internet access account from the service provider.

- When you select **Specified IP address** for the Internet access method, Table 2 describes the WAN interface configuration items.

Table 2 WAN interface configuration items when Specified IP address is selected

Item	Description
Interface	Select the WAN interface.
IP address/subnet mask	IP address and subnet mask of the WAN interface. This parameter is provided by the service provider. The IP address is in dotted decimal notation, for example, 10.1.1.1. The subnet mask is in the range of 1 to 31.
Default gateway	IP address of the default gateway of the WAN interface. Packets that users in the internal network send to access the Internet are sent to the default gateway through the WAN interface. Then, the default gateway forwards the packets. This parameter is provided by the service provider and is in dotted decimal notation, for example, 10.1.1.254.
Primary DNS server	IP address of the primary DNS server. For more information about DNS, see DNS Help. This parameter is provided by the service provider.
Secondary DNS server	IP address of the secondary DNS server. When the primary DNS server fails, the device uses the secondary DNS server for name resolution. This parameter is provided by the service provider.

- When you select **DHCP** for the Internet access method, Table 3 describes the WAN interface configuration items.

Table 3 WAN interface configuration items when DHCP is selected

Item	Description
Interface	Select the WAN interface.

- When you select **PPPoE** for the Internet access method, Table 4 describes the WAN interface configuration items.

Table 4 WAN interface configuration items when PPPoE is selected

Item	Description
Interface	Select the WAN interface.
Username	Username of the Internet access account, which is provided by the service provider.
Password	Password of the Internet access account, which is provided by the service provider.
Online mode	• **Permanently online**—The PPPoE session permanently exists after it is established. • **Auto offline after idle timeout**—The device automatically disconnects the PPPoE session if no traffic passes within the specified period. As a best practice, select this mode for time-based accounting users.
Automatically obtain IP address	The Internet access interface automatically obtains an IP address from the service provider.
Use specified IP address	Manually configure an IP address for the Internet access interface.
IP address/subnet mask	This parameter is provided by the service provider. The IP address is in dotted decimal notation, for example, 10.1.1.1. The subnet mask is in the range of 1 to 31.

2. Configure the LAN interface.

Table 5 describes the LAN interface configuration items.

Table 5 LAN interface configuration items

Item	Description
Interface	Select the interface for connecting to the LAN.
IP address/subnet mask	Specify the IP address and subnet mask for the LAN interface. The IP address is in dotted decimal notation, for example, 172.16.1.1. The subnet mask is in the range of 1 to 31.
DHCP	With DHCP enabled, users in the LAN can automatically obtain IP addresses. For more information about DHCP, see DHCP Help.
Address pool name	DHCP address pool name
Address range for allocation	Address range allocated to DHCP clients.

3. Configure the DMZ interface.

Table 6 describes the DMZ interface configuration items.

Table 6 DMZ interface configuration items

Parameter	Description
Interface	Select the interface for connecting to the DMZ zone. Typically, the DMZ zone is used for placing the devices providing external services, for example, the servers.
IP address/subnet mask	Specify the IP address and subnet mask for the DMZ interface. The IP address is in dotted decimal

Parameter	Description
	notation, for example, 172.16.1.1. The subnet mask is in the range of 1 to 31.

4. Configure security.

The IPS feature protects the enterprises' information systems and networks against attacks.

The IPS feature needs a license. To use this feature, purchase and correctly install the license.

Support for this feature depends on the device model.

5. Configure WAN acceleration.

This feature ensures the transmission of enterprises' critical data when the bandwidth is limited.

Support for this feature depends on the device model.

6. Configure flow control.

This feature limits the expected bandwidth of each WAN interface and the maximum bandwidth and guaranteed bandwidth of each application.

Set the expected bandwidth for WAN interfaces according to the bandwidth allocated by the service provider.

Support for this feature depends on the device model.

7. Configure the cloud manager server connection.

The cloud manager server is a platform for managing security devices. It supports fast deployment of security device configurations, differentiated deployment of security capabilities, modification of device configurations, and visualization of device status.

Configure the domain name of the cloud manager server for the device to connect to the cloud manager server.

Support for this feature depends on the device model.

Transparent mode

This mode does not change the current network structure. The interfaces configured as WAN interface, LAN interface, and DMZ interface become Layer 2 interfaces. Table 7 describes the transparent mode configuration items.

Table 7 Transparent mode configuration items

Parameter	Description
WAN interface	Select a WAN interface.
LAN interface	Select the interface for connecting to the LAN.
DMZ interface	Select the interface for connecting to the DMZ zone.
Security configuration	Configure IPS. Support for this feature depends on the device model.
WAN acceleration	Configure WAN acceleration. Support for this feature depends on the device model.
Flow control	Configure flow control. Support for this feature depends on the device model.
Cloud manager server connection	Enable the cloud manager server connection, and enter the domain name and port number of the server to connect the device to the server. Support for this feature depends on the device model.

Troubleshooting security policies, NAT, and SSL VPN

This help contains the following troubleshooting information:

- Troubleshooting security policies
- Troubleshooting NAT
- Troubleshooting SSL VPN

Troubleshooting security policies

This section contains the troubleshooting methods for the following issues:

- Network connectivity issues
    - Device ping failure from a directly connected PC
    - Connectivity failure between two PCs connected through the device
    - Connectivity failure between PCs connected through the device in the same security zone

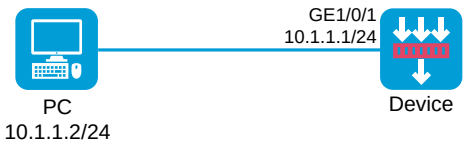
Network connectivity issues

Device ping failure from a directly connected PC

Symptom

The PC is connected to a service interface of the device through a network cable and is in the same subnet as the device. However, you cannot successfully ping the device from the PC.

Figure 1 Network diagram



Analysis

For a directly connected PC to access the device, you must add the connection interface on the device to a security zone and allow packets between the zone and the local zone to pass.

Solution

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Network** > **Security Zones** page.
3. Click the **Edit** icon for the target security zone.
4. Add the interface that connects the device to the PC as a member interface.

5. Click **OK**.
6. Access the **Policies** > **Security Policies** > **Security Policies** page.
7. Click **Create** and then click **Create a policy**.
8. Configure policy parameters as needed:
    - **Source zone**—Select the zone to which the interface belongs as the source zone. In this example, the source zone is Trust.
    - **Name**—Specify the policy name. In this example, the name is **trust-local**.
    - **Destination zone**—Select Local as the destination zone.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of the PC as the source IP. In this example, the address is 10.1.1.2.
    - **Destination IPv4 address**—Specify the IP address of the device as the destination IP. In this example, the address is 10.1.1.1.
9. For the device to access the PC, create a security policy to permit packets from the device to the PC.
    - **Name**—Specify the policy name. In this example, the name is **local-trust**.
    - **Source zone**—Select Local as the source zone.
    - **Destination zone**—Select the zone to which the interface belongs as the destination zone. In this example, the destination zone is Trust.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of the device as the source IP. In this example, the address is 10.1.1.1.
    - **Destination IPv4 address**—Specify the IP address of the PC as the destination IP. In this example, the address is 10.1.1.2.

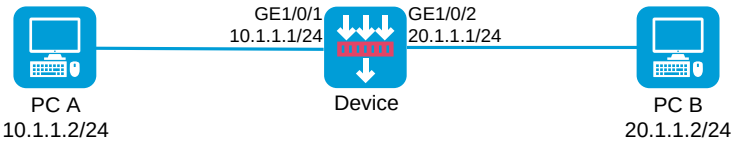
10. Click **OK**.

Connectivity failure between two PCs connected through the device

Symptom

Two PCs are connected through the device, and IP and route settings are configured correctly. However, the two PCs cannot reach each other.

Figure 2 Network diagram



Analysis

For traffic to be permitted on the device, you must add the input and output interfaces of the traffic to security zones and configure security policies to permit packets between the security zones.

Solution

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Network** > **Security Zones** page.
3. Click the **Edit** icon for the target security zone.
4. Add the interface that connects the device to a PC as a member interface.

5. Click **OK**.
6. Repeat the previous steps to add the device's interface for the other PC to another security zone.
7. Access the **Policies** > **Security Policies** page.
8. Click **Create**, and then click **Create a policy**. Create a security policy to permit packets from PC A to PC B.
9. Configure policy parameters as needed. As a best practice, specify exact match criteria.
    - **Name**—Specify the policy name. In this example, the name is **trust-untrust**.
    - **Source zone**—Select the zone to which the interface connecting PC A belongs as the source zone. In this example, the source zone is Trust.
    - **Destination zone**—Select the zone to which the interface connecting PC B belongs as the destination zone. In this example, the destination zone is Untrust.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC A as the source IP. In this example, the address is 10.1.1.2.
    - **Destination IPv4 address**—Specify the IP address of PC B as the destination IP. In this example, the address is 20.1.1.1.
10. Repeat the previous steps to create a security policy and permit packets from PC B to PC A.
    - **Name**—Specify the policy name. In this example, the name is **untrust-trust**.
    - **Source zone**—Select the zone to which the interface connecting PC B belongs as the source zone. In this example, the source zone is Untrust.
    - **Destination zone**—Select the zone to which the interface connecting PC A belongs as the destination zone. In this example, the destination zone is Trust.
    - **Action**—Select **Permit** as the action.

- **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 20.1.1.2.
- **Destination IPv4 address**—Specify the IP address of PC A as the destination IP. In this example, the address is 10.1.1.1.

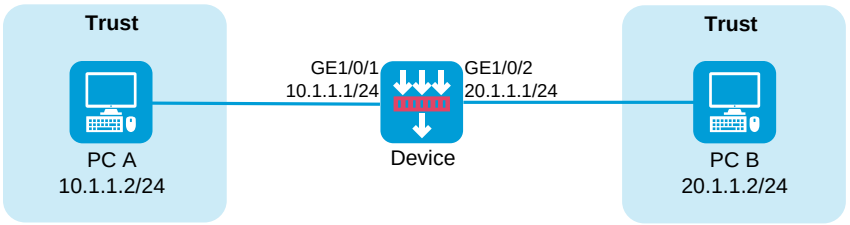
11. Click **OK**.

Connectivity failure between PCs connected through the device in the same security zone

Symptom

Two PCs are connected through the device, and IP and route settings are configured correctly. The PCs are in the same security zone but cannot reach each other.

Figure 3 Network diagram



Analysis

By default, the device drops packets whose source security zone and destination security zone are the same. For such packets to be transmitted, you must configure security policies to permit traffic from and to the same security zone.

Solution

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed.
    - **Name**—Specify the policy name. In this example, the name is **trust-trust**.
    - **Source zone**—Select the zone to which the PCs belong as the source zone. In this example, the source zone is Trust.
    - **Destination zone**—Select the same zone as the destination zone.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP addresses of PC A and PC B as the source IPs. In this example, the addresses are 10.1.1.2 and 20.1.1.2 for PC A and PC B, respectively.
    - **Destination IPv4 address**—Specify the IP addresses of PC B and PC A as the destination IPs. In this example, the addresses are 20.1.1.2 and 10.1.1.2 for PC B and PC A, respectively.
5. Click **OK**.

Troubleshooting NAT

This section contains the troubleshooting methods for the following issues:

- Policy-based NAT

- Failure of internal users to access the external network
- Source address translation failure
- Destination address translation failure
- Destination address translation failure (source address translation together with destination address translation)
- IPsec configuration failure (IPsec with NAT)
- Failure of internal users to access the device configured with policy-based NAT
- Failure of external users to access the device configured with source address translation
- Failure of external users to access the device configured with destination address translation

- Interface NAT
  - Failure of internal users to access the external network
  - Source address translation failure
  - Destination address translation failure
  - Destination address translation failure (source address translation together with destination address translation)
  - IPsec configuration failure (IPsec with NAT)
  - Failure of external users to access the device configured with source address translation
  - Failure of external users to access the device configured with destination address translation

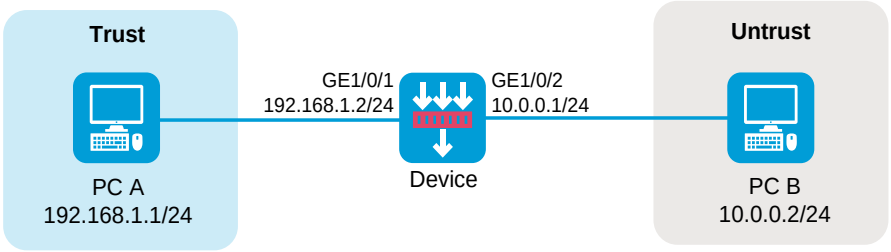
Policy-based NAT

Failure of internal users to access the external network

Symptom

PC A in the internal network cannot access PC B in the external network through the device.

Figure 4 Network diagram



Analysis

- No security policies are configured to permit packets from PC A to PC B.
- No policy-based NAT rules are configured to translate the source IP address of packets.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.

4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy1**.
    - **Source zone**—Select the zone to which the interface connected to PC A belongs as the source zone. In this example, the source zone is Trust.
    - **Destination zone**—Select the zone to which the interface connected to PC B belongs as the destination zone. In this example, the destination zone is Untrust.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC A as the source IP. In this example, the address is 192.168.1.1.
    - **Destination IPv4 address**—Specify the IP address of PC B as the destination IP. In this example, the address is 10.0.0.2.
5. Click **OK**.

Solution (policy-based NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Policy-based NAT** page.
3. Click **Create**.
4. Configure policy parameters as needed:
    - **Rule name**—Specify the rule name. In this example, the name is policy1.
    - **Rule type**—Specify the rule type. In this example, the type is NAT44.
    - **Src zone**—Select the zone to which the interface connected to PC A belongs as the source zone. In this example, the source zone is Trust.

- **Dst zone**—Select the zone to which the interface connected to PC B belongs as the destination zone. In this example, the destination zone is Untrust.
- **Source IP**—Specify the IP address of PC A as the source IP. In this example, the address is 192.168.1.1.
- **Destination IP**—Specify the IP address of PC B as the destination IP. In this example, the address is 10.0.0.2.
- **Translation method**—Select **Dynamic IP** as the translation method for source address translation.
- **Address**—Select a NAT address type for source address translation. In this example, the address type is NAT address group.
- **Source address after NAT**—Select a public NAT address group for source address translation.

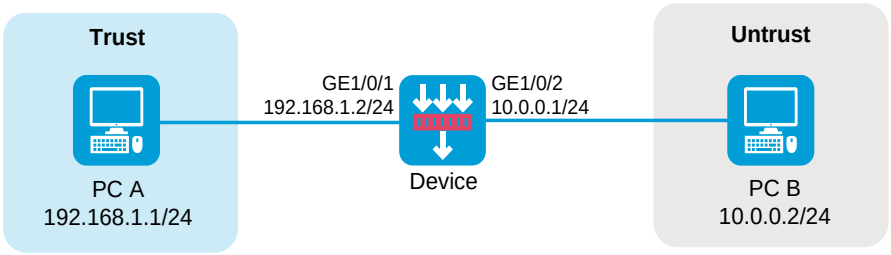
5. Click **OK**.

Source address translation failure

Symptom

The gateway device is configured with source address translation. PC A in the internal network cannot access PC B in the external network.

Figure 5 Network diagram



Analysis

- No security policies are configured to permit packets from PC A to PC B.
- The source address after NAT and the address of the interface connected to the external network are on different subnets, so return packets cannot access the device.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
   - **Name**—Specify the policy name. In this example, the name is **secpolicy2**.
   - **Source zone**—Select the zone to which the interface connected to PC A belongs as the source zone. In this example, the source zone is Trust.
   - **Destination zone**—Select the zone to which the interface connected to PC B belongs as the destination zone. In this example, the destination zone is Untrust.
   - **Action**—Select **Permit** as the action.

- **Source IPv4 address**—Specify the IP address of PC A as the source IP. In this example, the address is 192.168.1.1.
- **Destination IPv4 address**—Specify the IP address of PC B as the destination IP. In this example, the address is 10.0.0.2.

5. Click **OK**.

Solution (policy-based NAT issue)

To resolve the issue:

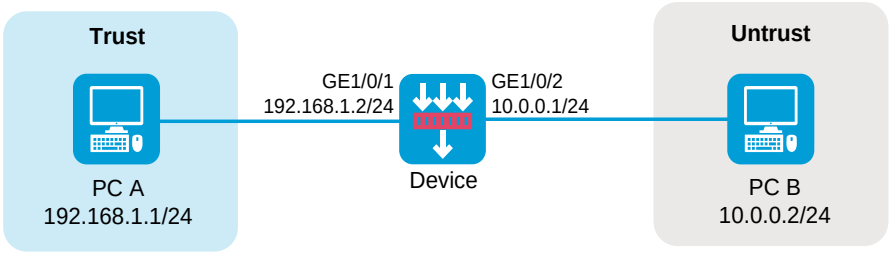
1. Log in to the Web interface of the device.
2. Access the **Policies** > **Policy-based NAT** page.
3. Click the **Edit** icon for the corresponding source address translation rules.
4. In the **Modify NAT policy** dialog box that opens, check if addresses of the following parameters are within the 10.0.0.1/24 network:
   - Source IP addresses after NAT.
   - Network addresses for address translation.
   - Address objects in the address group for address translation.
   - Addresses in the NAT address group for address translation.
5. If any, modify the configuration to ensure that return packets can be transmitted to interface GE1/0/2, the interface connected to the external network.
6. Click **OK**.

Destination address translation failure

Symptom

The gateway device is configured with destination address translation. PC B in the external network cannot access PC A in the internal network.

Figure 6 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to PC A.
- The service that PC B uses to access PC A does not match the destination address translation configuration, so the destination address of packets cannot be translated.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.

4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy3**.
    - **Source zone**—Select the zone to which the interface connected to PC B belongs as the source zone. In this example, the source zone is Untrust.
    - **Destination zone**—Select the zone to which the interface connected to PC A belongs as the destination zone. In this example, the destination zone is Trust.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
    - **Destination IPv4 address**—Specify the IP address of PC A as the destination IP. In this example, the address is 192.168.1.1.
5. Click **OK**.

Solution (policy-based NAT issue)

To resolve the issue:

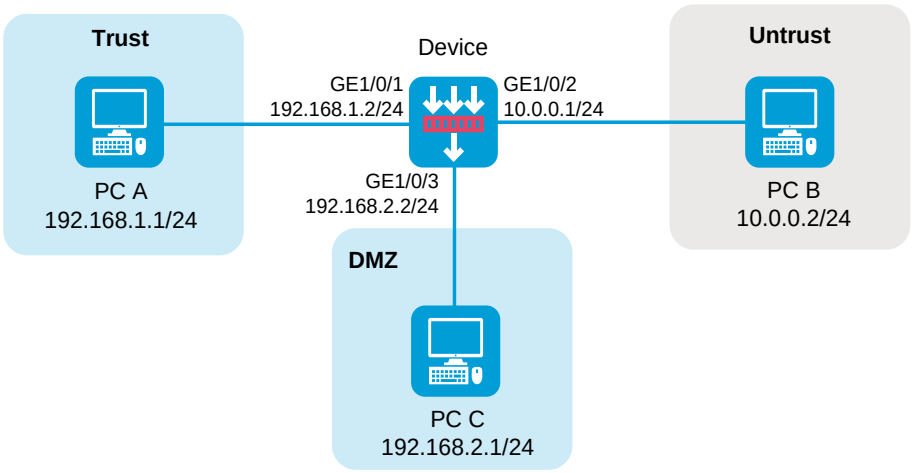
1. Log in to the Web interface of the device.
2. Access the **Policies** > **Policy-based NAT** page.
3. Click the **Edit** icon for the corresponding destination address translation rules.
4. Verify that the rules have correct service configuration.
5. Click **OK**.

Destination address translation failure (source address translation together with destination address translation)

Symptom

The gateway device is configured with source address translation and destination address translation (NAT Server feature). PC B in the external network cannot access PC C by using public address 10.0.0.100 and destination port 80.

Figure 7 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to PC C.
- A source address translation rule uses the same IP address and port number as the destination address translation rule, and packets from the device to PC C match the source address translation rule.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy4**.
    - **Source zone**—Select the zone to which the interface connected to PC B belongs as the source zone. In this example, the source zone is Untrust.
    - **Destination zone**—Select the zone to which the interface connected to PC C belongs as the destination zone. In this example, the destination zone is DMZ.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
    - **Destination IPv4 address**—Specify the IP address of PC C as the destination IP. In this example, the address is 192.168.2.1.
5. Click **OK**.

Solution (policy-based NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Policy-based NAT** page.
3. If a rule displays **Dynamic IP** in the **Translation method** column, click the **Edit** icon.

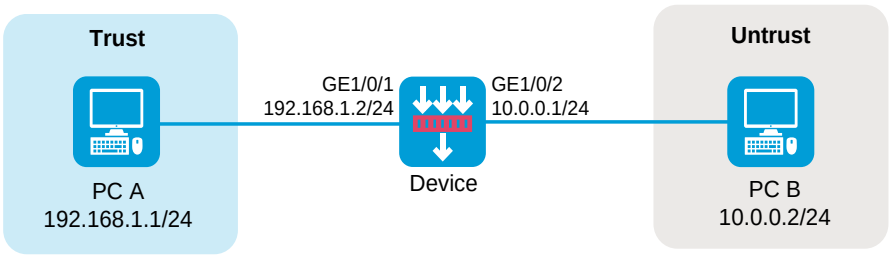
4. In the dialog box that opens, remove port number 80 from the port range in the NAT address group.
5. Click **OK**.

IPsec configuration failure (IPsec with NAT)

Symptom

The gateway device is configured with both IPsec and source address translation. When PC A sends a packet to PC B, the device cannot perform IPsec protection for the packet after source address translation.

Figure 8 Network diagram



Analysis

To protect NATed packets with IPsec, make sure the source and destination IP addresses of the traffic to be protected are the addresses after NAT.

Solution

To resolve the issue:

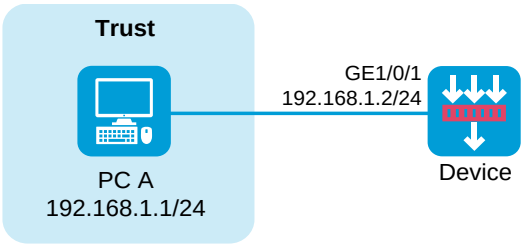
1. Log in to the Web interface of the device.
2. Access the **Network** > **VPN** > **IPsec** > **IPsec Policies** page.
3. Click the **Edit** icon for the corresponding IPsec policies.
4. In the **Data flow filter rule** area, change the source and destination addresses of the protected flow to the addresses after NAT.
5. Click **OK**.

Failure of internal users to access the device configured with policy-based NAT

Symptom

PC A in the internal network cannot access the device.

Figure 9 Network diagram



Analysis

- No security policies are configured to permit packets from PC A to the device.
- The destination addresses of packets from PC A to the device are translated.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy5**.
    - **Source zone**—Select the zone to which the interface connecting PC A belongs as the source zone. In this example, the source zone is Trust.
    - **Destination zone**—Select Local as the destination zone.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC A as the source IP. In this example, the address is 192.168.1.1.
    - **Destination IPv4 address**—Specify the IP address of the interface connected to the internal network as the destination IP. In this example, the address is 192.168.1.2.
5. Click **OK**.

Solution (policy-based NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Policy-based NAT** page.
3. If a rule displays **Any** in the **Source security zone** column, click the **Edit** icon.

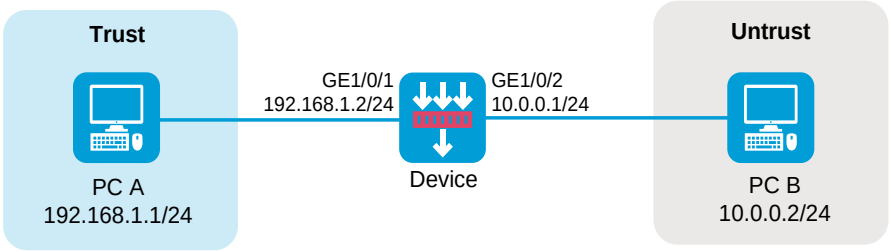
4. In the dialog box that opens, modify the following packet match parameters for the destination address translation:
   - **Dst zone**—Specify a destination security zone. The value for the parameter cannot be Local.
   - **Source IP**—Specify a source IPv4 address. The value for the parameter cannot be 192.168.1.1.
   - **Destination IP**—Specify a destination IPv4 address. The value for the parameter cannot be 192.168.1.2.
5. Click **OK**.

Failure of external users to access the device configured with source address translation

Symptom

The gateway device is configured with source address translation. PC B in the external network cannot access the device.

Figure 10 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to the device.
- The destination address of the traffic from PC B to the device is translated into the address of PC A because it matches the source address translation rule.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy6**.
    - **Source zone**—Select the zone to which the interface connected to PC B belongs as the source zone. In this example, the source zone is Untrust.
    - **Destination zone**—Select Local as the destination zone.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
    - **Destination IPv4 address**—Specify the IP address of the interface connected to the external network as the destination IP. In this example, the address is 10.0.0.1.
5. Click **OK**.

Solution (policy-based NAT issue)

To resolve the issue:

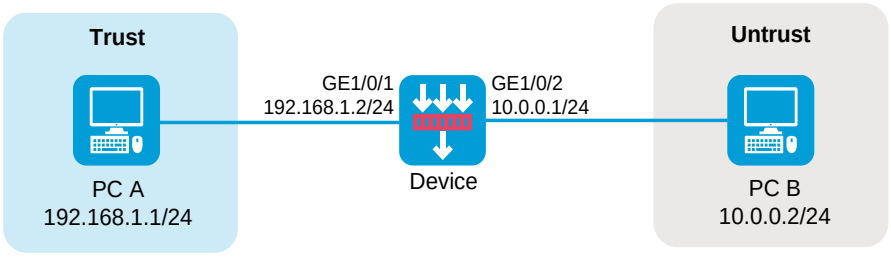
1. Log in to the Web interface of the device.
2. Access the **Policies** > **Policy-based NAT** page.
3. If a rule displays **Dynamic IP** in the **Translation method** column, click the **Edit** icon to edit the rule.
4. If the address object group or NAT address group for source address translation contains the address of the interface connected to the external network, remove the address from the groups.
5. Click **OK**.

Failure of external users to access the device configured with destination address translation

Symptom

The gateway device is configured with destination address translation. PC B in the external network cannot access the device.

Figure 11 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to the device.
- Traffic from PC B to the device uses the same service as that of the destination address translation rule, and the destination address of the traffic is translated.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy7**.
    - **Source zone**—Select the zone to which the interface connected to PC B belongs as the source zone. In this example, the source zone is Untrust.
    - **Destination zone**—Select Local as the destination zone.
    - **Action**—Select **Permit** as the action.

- **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
- **Destination IPv4 address**—Specify the IP address of the interface connected to the external network on Device as the destination IP. In this example, the address is 10.0.0.1.

5. Click **OK**.

Solution (policy-based NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Log in to the Web interface of the device.
3. Access the **Policies** > **Policy-based NAT** page.
4. Click the **Edit** icon for the corresponding destination address translation rules.
5. If the destination address match condition contains the address of the interface connected to the external network on the device, check the service match condition.
6. If the condition contains the service that PC B uses to access the device, perform the following based on the actual situation:
   - Modify the service that PC B uses to access the device.
   - Remove the service from the service match condition to make sure that the NAT module does not perform destination address translation on traffic containing the service.
7. Click **OK**.

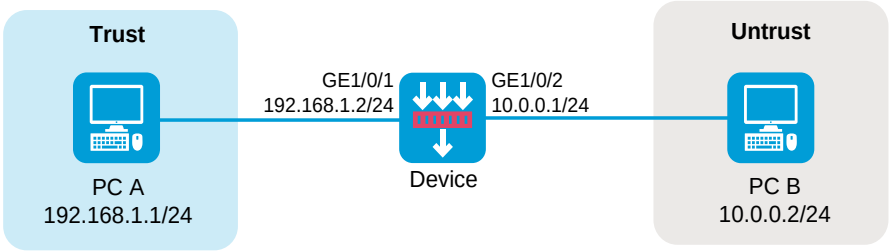
Interface NAT

Failure of internal users to access the external network

Symptom

PC A in the internal network cannot access PC B in the external network through the device.

Figure 12 Network diagram



Analysis

- No security policies are configured to permit packets from PC A to PC B.
- No interface NAT rules are configured to translate the source IP address of packets.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.

4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy1**.
    - **Source zone**—Select the zone to which the interface connecting PC A belongs as the source zone. In this example, the source zone is Trust.
    - **Destination zone**—Select the zone to which the interface connecting PC B belongs as the destination zone. In this example, the destination zone is Untrust.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC A as the source IP. In this example, the address is 192.168.1.1.
    - **Destination IPv4 address**—Specify the IP address of PC B as the destination IP. In this example, the address is 10.0.0.2.
5. Click **OK**.

Solution (interface NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Interface NAT** > **IPv4** > **Dynamic NAT** page.
3. Click the **Out Dynamic NAT (ACL-Based)** tab.
4. Click **Create**.
5. Configure policy parameters as needed:
    - **Interface**—Specify an interface. In this example, the interface is GE1/0/2.
    - **ACL**—Specify an ACL to define the source IP addresses of outgoing packets to be translated by the NAT module.

- **Source address after NAT**—Specify a NAT address group. In this example, IP addresses are public addresses used for source address translation.
- **Translation mode**—Select **PAT** as the translation mode.

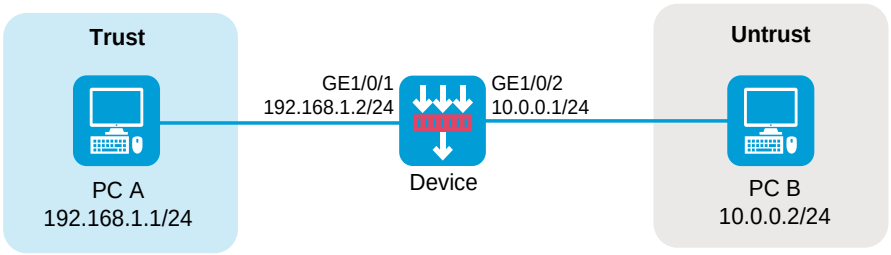
6. Click **OK**.

Source address translation failure

Symptom

The gateway device is configured with source address translation. PC A in the internal network cannot access PC B in the external network.

Figure 13 Network diagram



Analysis

- No security policies are configured to permit packets from PC A to PC B.
- The source address after NAT and the address of the interface connected to the external network are on different subnets, so return packets cannot access the device.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy2**.
    - **Source zone**—Select the zone to which the interface connected to PC A belongs as the source zone. In this example, the source zone is Trust.
    - **Destination zone**—Select the zone to which the interface connected to PC B belongs as the destination zone. In this example, the destination zone is Untrust.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC A as the source IP. In this example, the address is 192.168.1.1.
    - **Destination IPv4 address**—Specify the IP address of PC B as the destination IP. In this example, the address is 10.0.0.2.
5. Click **OK**.

Solution (interface NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Interface NAT** > **IPv4** > **Dynamic NAT** page
3. Click the **Edit** icon for the corresponding source address translation rules.

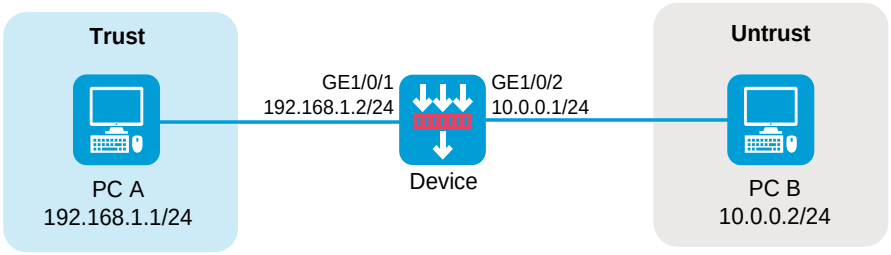
4. In the dialog box that opens, check if addresses of the following parameters are within the 10.0.0.1/24 network:
    - Source addresses after NAT.
    - Network addresses for address translation.
    - Address objects in the address object group for address translation.
    - Addresses in the NAT address group for address translation.
5. If any, modify related configurations to verify that return packets can be transmitted to interface GE 1/0/2 on the device.
6. Click **OK**.

Destination address translation failure

Symptom

The gateway device is configured with destination address translation. PC B in the external network cannot access PC A in the internal network.

Figure 14 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to PC A.
- The destination port of traffic from PC B to PC A does not match the destination address translation rule, so the destination address of the traffic cannot be translated.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy3**.
    - **Source zone**—Select the zone to which the interface connected to PC B belongs as the source zone. In this example, the source zone is Untrust.
    - **Destination zone**—Select the zone to which the interface connected to PC A belongs as the destination zone. In this example, the destination zone is Trust.
    - **Action**—Select **Permit** as the action.
    - **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
    - **Destination IPv4 address**—Specify the IP address of PC A as the destination IP. In this example, the address is 192.168.1.1.
5. Click **OK**.

Solution (interface NAT issue)

To resolve the issue:

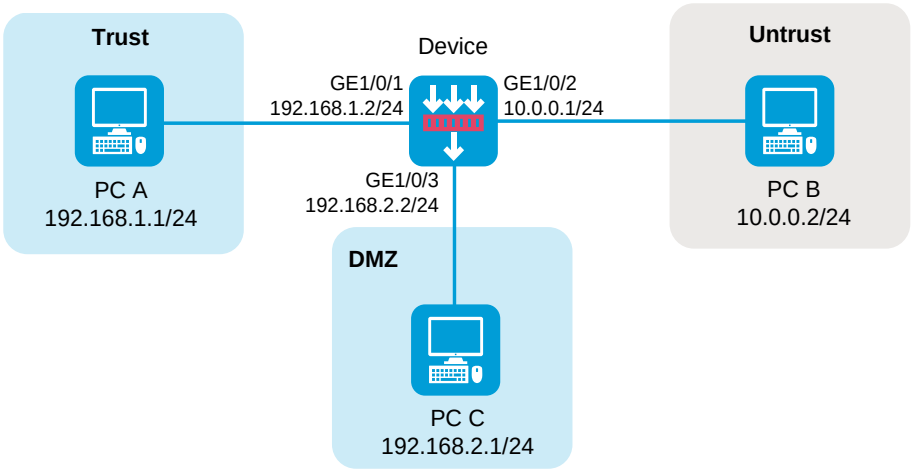
1. Log in to the Web interface of the device.
2. Access the **Policies** > **Interface NAT** > **IPv4** > **NAT Servers** > **Policy Configuration** page.
3. Check whether the public port of the NAT Server is in actual use.
4. If not, change the public port match condition to make sure that the public port is in actual use for the NAT Server rule.
5. Click **OK**.

Destination address translation failure (source address translation together with destination address translation)

Symptom

The gateway device is configured with source address translation and destination address translation (NAT Server feature). PC B in the external network cannot access PC C by using public address 10.0.0.100 and destination port 80.

Figure 15 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to PC C.
- A source address translation rule uses the same IP address and port number as the destination address translation rule, and packets from the device to PC C match the source address translation rule.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
    - **Name**—Specify the policy name. In this example, the name is **secpolicy4**.

- **Source zone**—Select the zone to which the interface connected to PC B belongs as the source zone. In this example, the source zone is Untrust.
- **Destination zone**—Select the zone to which the interface connected to PC C belongs as the destination zone. In this example, the destination zone is DMZ.
- **Action**—Select **Permit** as the action.
- **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
- **Destination IPv4 address**—Specify the IP address of PC C as the destination IP. In this example, the address is 192.168.2.1.

5. Click **OK**.

Solution (interface NAT issue)

To resolve the issue:

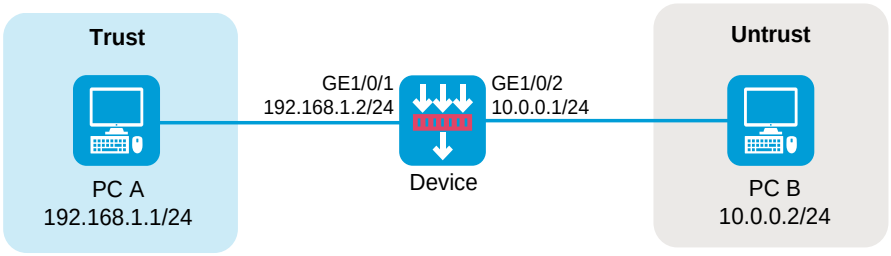
1. Log in to the Web interface of the device.
2. Access the **Policies** > **Interface NAT** > **IPv4** > **Dynamic NAT** page.
3. Click the **Out Dynamic NAT (Object Group-Based)** tab to view rule details.
4. If the action is **PAT**, click the **Edit** icon to remove port number 80 from the port range in the NAT address group.
5. Click **OK**.
6. Click the **Out Dynamic NAT (ACL-Based)** tab to view rule details.
7. If the translation mode is **PAT**, click the **Edit** icon to remove port number 80 from the port range in the NAT address group.
8. Click **OK**.

IPsec configuration failure (IPsec with NAT)

Symptom

The device is configured with both IPsec and source address translation. When PC A sends a packet to PC B, the device cannot perform IPsec protection for the packet after source address translation.

Figure 16 Network diagram



Analysis

To protect NATed packets with IPsec, make sure the source and destination IP addresses of the traffic to be protected are the addresses after NAT.

Solution

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Network** > **VPN** > **IPsec** > **IPsec Policies** page.
3. Click the **Edit** icon for the corresponding IPsec policies.

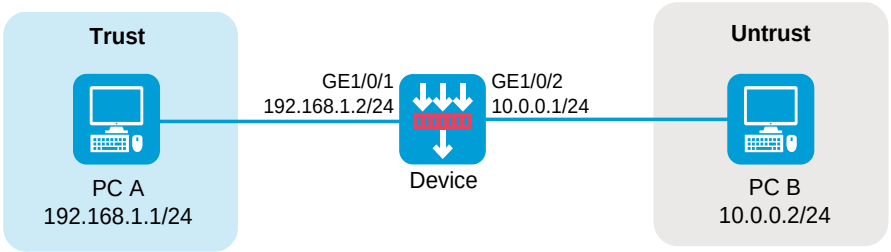
4. In the **Data flow filter rule** area, change the source and destination addresses of the protected flow to the addresses after NAT.
5. Click **OK**.

Failure of external users to access the device configured with source address translation

Symptom

The gateway device is configured with source address translation. PC B in the external network cannot access the device.

Figure 17 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to the device.
- The destination address of the traffic from PC B to the device is translated into the address of PC A because it matches the source address translation rule.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
   - **Name**—Specify the policy name. In this example, the name is **secpolicy5**.
   - **Source zone**—Select the zone to which the interface connecting PC B belongs as the source zone. In this example, the source zone is Untrust.
   - **Destination zone**—Select Local as the destination zone.
   - **Action**—Select **Permit** as the action.
   - **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
   - **Destination IPv4 address**—Specify the IP address of the interface connected to the external network as the destination IP. In this example, the address is 10.0.0.1.
5. Click **OK**.

Solution (interface NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Interface NAT** > **IPv4** > **NAT** > **Dynamic NAT** page.
3. Click the **Out Dynamic NAT (Object Group-Based)** tab to check if the **Action** column is **NO-PAT**.

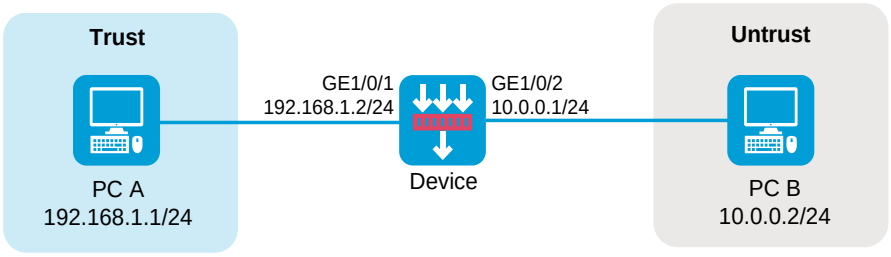
4. If the action is **NO-PAT**, click the **Edit** icon to remove IP address 10.0.0.1, if any, from the NAT address group for packet matching.
5. Click **OK**.
6. Click the **Out Dynamic NAT (ACL-Based)** tab to check if the **Translation method** column is **NO-PAT**.
7. If the translation mode is **NO-PAT**, click the **Edit** icon to open the **NAT Dynamic NAT Rule** dialog box:
    - If IP addresses for address translation belong to an address group, verify that the NAT address group does not contain 10.0.0.1.
    - If the translation mode is **Easy IP**, the specified interface for address translation cannot be GE 1/0/2.
8. Click **OK**.

Failure of external users to access the device configured with destination address translation

Symptom

The gateway device is configured with destination address translation. PC B in the external network cannot access the device.

Figure 18 Network diagram



Analysis

- No security policies are configured to permit packets from PC B to the device.
- Traffic from PC B to the device uses the same service as that of the destination address translation rule, and the destination address of the traffic is translated.

Solution (security policy issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Security Policies** > **Security Policies** page.
3. Click **Create**, and then click **Create a policy**.
4. Configure policy parameters as needed:
   - **Name**—Specify the policy name. In this example, the name is **secpolicy6**.
   - **Source zone**—Select the zone to which the interface connecting PC B belongs as the source zone. In this example, the source zone is Untrust.
   - **Destination zone**—Select Local as the destination zone.
   - **Action**—Select **Permit** as the action.

- **Source IPv4 address**—Specify the IP address of PC B as the source IP. In this example, the address is 10.0.0.2.
- **Destination IPv4 address**—Specify the IP address of the interface connected to the external network on the device as the destination IP. In this example, the address is 10.0.0.1.

5. Click **OK**.

Solution (interface NAT issue)

To resolve the issue:

1. Log in to the Web interface of the device.
2. Access the **Policies** > **Interface NAT** > **IPv4** > **NAT Servers** > **Policy Configuration** page.
3. Check if IP address 10.0.0.1 is used by a NAT Server rule.
4. If IP address 10.0.0.1 is displayed in the **Public IP address** column, click the **Edit** icon for the rule.
5. In the **Edit NAT Server Rule** dialog box that opens, check if the public port is the port for PC B to access the device.
6. If the port is the port for the PC B to access the device, select one of the following solutions:
   - Modify the protocol or destination port for the traffic from PC B to the device.
   - Modify the ACL-based packet match rule to prevent the traffic to be processed by destination address translation.
7. Click **OK**.

Troubleshooting SSL VPN

This section contains the troubleshooting methods for the following issues:

- Browser access issues
  - Failure to access the SSL VPN Web interface from a browser
  - Failure to log in to the SSL VPN gateway from a browser
  - Failure to access internal resources from a browser
- iNode client access issues
  - Failure to obtain SSL VPN gateway information from an iNode client
  - Failure to log in to the SSL VPN gateway from an iNode client
  - Failure to access internal resources from an iNode client
  - Failure to terminate idle SSL VPN sessions of iNode client users
- Others
  - User filtering, monitoring, and IP binding settings not take effect
  - Failure to relog in to the SSL VPN gateway

Browser access issues

Failure to access the SSL VPN Web interface from a browser

Symptom

A user cannot access the SSL VPN Web interface by entering the address of the SSL VPN gateway in a browser.

Solution

To resolve the issue:

1. Verify that the address of the SSL VPN gateway is reachable.
   - If ping is allowed, ping the SSL VPN gateway address from a PC.
   - If ping is not allowed, capture packets to verify the connectivity.
2. View SSL VPN gateway information to verify the following:
   - Verify that the SSL VPN gateway is up. If the **Operation state** field displays **Up**, the SSL VPN gateway is up. If the SSL VPN gateway is not up, enable the SSL VPN gateway from the Web interface or execute the **`service enable`** command in SSL VPN gateway view from the CLI.
   - Verify that the SSL-related configuration is correct. By default, the device uses its self-signed certificate. To use the CA-signed certificate, apply an SSL server policy to the SSL VPN gateway. To cancel the use of the CA-signed certificate, cancel the application of the SSL server policy for the SSL VPN gateway.
   - Verify that the SSL server policy being used by the SSL VPN gateway is the desired one.

     If the used SSL server policy's configuration is edited or another SSL server policy is configured for the SSL VPN gateway, re-enable the SSL VPN gateway to make the new configuration take effect.

     To re-enable the SSL VPN gateway, execute the **`undo service enable`** command and then the **`service enable`** command.

   The following is an example of the SSL VPN gateway information:

```
[Device] display sslvpn gateway

Gateway name: gw

  Operation state: Up
```

```
  IP: 1.1.1.2  Port: 2000

  SSL server policy configured: sslnew

  SSL server policy in use: ssl

  Front VPN instance: Not configured
```

3. View SSL VPN context information to verify the following:

   - Verify that the SSL VPN context is up. If the **Operation state** field displays **Up**, the SSL VPN context is up. If the SSL VPN context is not up, enable the SSL VPN context from the Web interface or execute the **`service enable`** command in SSL VPN context view from the CLI.
   - Verify that the SSL VPN context is associated with an SSL VPN gateway. The **Associated SSL VPN gateway** field displays the name of the SSL VPN gateway if the SSL VPN context is associated with an SSL VPN gateway. If the SSL VPN context is not associated with an SSL VPN gateway, associate one from the Web interface, or execute the **`gateway`** command in SSL VPN context view from the CLI.

   The following is an example of the SSL VPN context information:

```
[Device] display sslvpn context

Context name: ctx

  Operation state: Up

  Associated SSL VPN gateway: gw

  SSL client policy configured: sslnew

  SSL client policy in use: ssl
```

4. Verify that the SSL VPN gateway listening address and ports are correctly configured on all service modules, and the listening ports on each service module is enabled.

   The following is an example of TCP proxy information:

```
<Device> dis tcp-proxy slot 1
```

```
Local Addr:port       Foreign Addr:port     State           Service
type
1.1.1.2:2000          0.0.0.0:0                 LISTEN       SSLVPN
```

Failure to log in to the SSL VPN gateway from a browser

Symptom

A user can open the SSL VPN Web interface from a browser but cannot log in to the SSL VPN gateway.

Solution

To resolve the issue:

1. Verify that the address of the SSL VPN gateway is reachable.
   - If ping is allowed, ping the SSL VPN gateway address from a PC.
   - If ping is not allowed, capture packets to verify the connectivity.
2. View SSL VPN gateway information to verify the following:
   - Verify that the SSL VPN gateway is up. If the **Operation state** field displays **Up**, the SSL VPN gateway is up. If the SSL VPN gateway is not up, enable the SSL VPN gateway from the Web interface or execute the **`service enable`** command in SSL VPN gateway view from the CLI.
   - Verify that the SSL-related configuration is correct. By default, the device uses its self-signed certificate. To use the CA-signed certificate, apply an SSL server policy to the SSL VPN gateway. To cancel the use of the CA-signed certificate, cancel the application of the SSL server policy for the SSL VPN gateway.

- Verify that the SSL server policy being used by the SSL VPN gateway is the desired one.

  If the used SSL server policy's configuration is edited or another SSL server policy is configured for the SSL VPN gateway, re-enable the SSL VPN gateway to make the new configuration take effect.

  To re-enable the SSL VPN gateway, execute the **undo service enable** command and then the **service enable** command.

The following is an example of the SSL VPN gateway information:

```
[Device] display sslvpn gateway

Gateway name: gw

  Operation state: Up

  IP: 1.1.1.2  Port: 2000

  SSL server policy configured: sslnew

  SSL server policy in use: ssl

  Front VPN instance: Not configured
```

3. View SSL VPN context information to verify the following:

   - Verify that the SSL VPN context is up. If the **Operation state** field displays **Up**, the SSL VPN context is up. If the SSL VPN context is not up, enable the SSL VPN context from the Web interface or execute the **service enable** command in SSL VPN context view from the CLI.
   - Verify that the SSL VPN context is associated with an SSL VPN gateway. The **Associated SSL VPN gateway** field displays the name of the SSL VPN gateway if the SSL VPN context is associated with an SSL VPN gateway. If the SSL VPN context is not associated with an SSL VPN gateway, associate one from the Web interface, or execute the **gateway** command in SSL VPN context view from the CLI.

The following is an example of the SSL VPN context information:

```
[Device] display sslvpn context

Context name: ctx

  Operation state: Up

  Associated SSL VPN gateway: gw

  SSL client policy configured: sslnew

  SSL client policy in use: ssl
```

4. Verify that the SSL VPN gateway listening address and ports are correctly configured on all service modules, and the listening ports on each service module is enabled.

   The following is an example of TCP proxy information:

```
<Device> dis tcp-proxy slot 1

Local Addr:port       Foreign Addr:port     State           Service
type

1.1.1.2:2000          0.0.0.0:0                 LISTEN      SSLVPN
```

5. Verify that the SSL VPN user is configured correctly.
   - **For a local user**—Verify that the local user is a network access user, the service type for the user is SSL VPN, the user is authorized to access a resource group, and the resource group is well configured.
   - **For a remote user**—Verify that the user's user group on the remote authentication server is configured in the SSL VPN context as a resource group. The user group and the resource group must use the same name.
6. If certificate authentication is enabled on the server and client, make sure certificates are installed correctly on the server and client.

Failure to access internal resources from a browser

Symptom

A user cannot access internal resources after logging in to the SSL VPN gateway successfully from a browser.

Solution

To resolve the issue:

1. Verify that the access resources are configured in one of the following methods:
   - Configure a resource list. For example:

     # Create a URL item named **urlitem** and specify the resource URL in the URL item.

     ```
     [Device-sslvpn-context-ctxweb1] url-item urlitem
     [Device-sslvpn-context-ctxweb1-url-item-urlitem] url
     http://20.2.2.2
     [Device-sslvpn-context-ctxweb1-url-item-urlitem] quit
     ```

     # Create a URL list named **urllist** in SSL VPN context **ctxweb1**.

     ```
     [Device-sslvpn-context-ctxweb1] url-list urllist
     ```

     # Configure the heading as **web** for the URL list.

     ```
     [Device-sslvpn-context-ctxweb1-url-list-urllist] heading web
     ```

     # Assign URL item **urlitem** to URL list **urllist**.

     ```
     [Device-sslvpn-context-ctxweb1-url-list-urllist] resources
     url-item urlitem
     [Device-sslvpn-context-ctxweb1-url-list-urllist] quit
     ```

Create an SSL VPN policy group named **resourcegrp1** for SSL VPN context **ctxweb1**, and then add URL list **urllist** to the policy group for Web access.

```
[Device-sslvpn-context-ctxweb1] policy-group resourcegrp1
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] resources url-list urllist
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] quit
```

- Configure an ACL or a URI ACL to permit access to the internal servers, and then specify the ACL for SSL VPN Web access. For example:

```
[Device-sslvpn-context-ctxweb1] policy-group resourcegrp1
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] filter web-access acl 3000
```

2. Verify that the SSL VPN gateway can ping the internal resources successfully. Add routes to reach the peer devices if needed.
3. View SSL VPN gateway information to verify the following:
   - Verify that the SSL VPN gateway is up. If the **Operation state** field displays **Up**, the SSL VPN gateway is up. If the SSL VPN gateway is not up, enable the SSL VPN gateway from the Web interface or execute the **`service enable`** command in SSL VPN gateway view from the CLI.
   - Verify that the SSL-related configuration is correct. By default, the device uses its self-signed certificate. To use the CA-signed certificate, apply an SSL server policy to the SSL VPN gateway. To cancel the use of the CA-signed certificate, cancel the application of the SSL server policy for the SSL VPN gateway.
   - Verify that the SSL server policy being used by the SSL VPN gateway is the desired one.

If the used SSL server policy's configuration is edited or another SSL server policy is configured for the SSL VPN gateway, re-enable the SSL VPN gateway to make the new configuration take effect.

To re-enable the SSL VPN gateway, execute the **undo service enable** command and then the **service enable** command.

The following is an example of the SSL VPN gateway information:

```
[Device] display sslvpn gateway

Gateway name: gw

  Operation state: Up

  IP: 1.1.1.2  Port: 2000

  SSL server policy configured: sslnew

  SSL server policy in use: ssl

  Front VPN instance: Not configured
```

4. View SSL VPN context information to verify the following:
   - Verify that the SSL VPN context is up. If the **Operation state** field displays **Up**, the SSL VPN context is up. If the SSL VPN context is not up, enable the SSL VPN context from the Web interface or execute the **service enable** command in SSL VPN context view from the CLI.
   - Verify that the SSL VPN context is associated with an SSL VPN gateway. The **Associated SSL VPN gateway** field displays the name of the SSL VPN gateway if the SSL VPN context is associated with an SSL VPN gateway. If the SSL VPN context is not associated with an SSL VPN gateway, associate one from the Web interface, or execute the **gateway** command in SSL VPN context view from the CLI.

   The following is an example of the SSL VPN context information:

   ```
   [Device] display sslvpn context
   ```

```
Context name: ctx

  Operation state: Up

  Associated SSL VPN gateway: gw

  SSL client policy configured: sslnew

  SSL client policy in use: ssl
```

5. Verify that both the uplinks and downlinks operate correctly. An uplink or downlink error might occur in one of the following situations:
   - The routes to the internal resources are not configured on the SSL VPN gateway. You can check the routing table on the device for route configuration.
   - The internal servers do not have routes to reach the SSL VPN gateway.
   - An address conflict occurs.
   - An improper policy-based routing (PBR) is configured.
   - Improper SSL VPN load balancing is configured.
   - The device operates in dual-active mode.

     To resolve this issue, change the dual-active mode to the active/standby mode, and the uplink and downlink interfaces to redundant interfaces.

iNode client access issues

Failure to obtain SSL VPN gateway information from an iNode client

Symptom

A user cannot access the SSL VPN Web interface by entering the address of the SSL VPN gateway in a browser. Or, an iNode client fails to obtain the SSL VPN gateway information after the gateway address is entered.

Solution

To resolve the issue:

1. Verify that the address of the SSL VPN gateway is reachable.
   - If ping is allowed, ping the SSL VPN gateway address from a PC.
   - If ping is not allowed, capture packets to verify the connectivity.
2. View SSL VPN gateway information to verify the following:
   - Verify that the SSL VPN gateway is up. If the **Operation state** field displays **Up**, the SSL VPN gateway is up. If the SSL VPN gateway is not up, enable the SSL VPN gateway from the Web interface or execute the **`service enable`** command in SSL VPN gateway view from the CLI.
   - Verify that the SSL-related configuration is correct. By default, the device uses its self-signed certificate. To use the CA-signed certificate, apply an SSL server policy to the SSL VPN gateway. To cancel the use of the CA-signed certificate, cancel the application of the SSL server policy for the SSL VPN gateway.

- Verify that the SSL server policy being used by the SSL VPN gateway is the desired one.

  If the used SSL server policy's configuration is edited or another SSL server policy is configured for the SSL VPN gateway, re-enable the SSL VPN gateway to make the new configuration take effect.

  To re-enable the SSL VPN gateway, execute the **undo service enable** command and then the **service enable** command.

The following is an example of the SSL VPN gateway information:

```
[Device] display sslvpn gateway

Gateway name: gw

  Operation state: Up

  IP: 1.1.1.2  Port: 2000

  SSL server policy configured: sslnew

  SSL server policy in use: ssl

  Front VPN instance: Not configured
```

3. View SSL VPN context information to verify the following:

   - Verify that the SSL VPN context is up. If the **Operation state** field displays **Up**, the SSL VPN context is up. If the SSL VPN context is not up, enable the SSL VPN context from the Web interface or execute the **service enable** command in SSL VPN context view from the CLI.
   - Verify that the SSL VPN context is associated with an SSL VPN gateway. The **Associated SSL VPN gateway** field displays the name of the SSL VPN gateway if the SSL VPN context is associated with an SSL VPN gateway. If the SSL VPN context is not associated with an SSL VPN gateway, associate one from the Web interface, or execute the **gateway** command in SSL VPN context view from the CLI.

The following is an example of the SSL VPN context information:

```
[Device] display sslvpn context

Context name: ctx

  Operation state: Up

  Associated SSL VPN gateway: gw

  SSL client policy configured: sslnew

  SSL client policy in use: ssl
```

4. Verify that the SSL VPN gateway listening address and ports are correctly configured on all service modules, and the listening ports on each service module is enabled.

   The following is an example of TCP proxy information:

```
<Device> dis tcp-proxy slot 1

Local Addr:port       Foreign Addr:port     State           Service
type

1.1.1.2:2000          0.0.0.0:0                 LISTEN       SSLVPN
```

Failure to log in to the SSL VPN gateway from an iNode client

Symptom

An iNode client obtains the SSL VPN gateway information successfully, but SSL VPN login fails.

Solution

To resolve the issue:

1. Verify that the address of the SSL VPN gateway is reachable.

- If ping is allowed, ping the SSL VPN gateway address from a PC.
- If ping is not allowed, capture packets to verify the connectivity.

2. View SSL VPN gateway information to verify the following:
   - Verify that the SSL VPN gateway is up. If the **Operation state** field displays **Up**, the SSL VPN gateway is up. If the SSL VPN gateway is not up, enable the SSL VPN gateway from the Web interface or execute the **`service enable`** command in SSL VPN gateway view from the CLI.
   - Verify that the SSL-related configuration is correct. By default, the device uses its self-signed certificate. To use the CA-signed certificate, apply an SSL server policy to the SSL VPN gateway. To cancel the use of the CA-signed certificate, cancel the application of the SSL server policy for the SSL VPN gateway.
   - Verify that the SSL server policy being used by the SSL VPN gateway is the desired one.

     If the used SSL server policy's configuration is edited or another SSL server policy is configured for the SSL VPN gateway, re-enable the SSL VPN gateway to make the new configuration take effect.

     To re-enable the SSL VPN gateway, execute the **`undo service enable`** command and then the **`service enable`** command.

The following is an example of the SSL VPN gateway information:

```
[Device] display sslvpn gateway

Gateway name: gw

  Operation state: Up

  IP: 1.1.1.2  Port: 2000

  SSL server policy configured: sslnew

  SSL server policy in use: ssl
```

```
  Front VPN instance: Not configured
```

3. View SSL VPN context information to verify the following:

   - Verify that the SSL VPN context is up. If the **Operation state** field displays **Up**, the SSL VPN context is up. If the SSL VPN context is not up, enable the SSL VPN context from the Web interface or execute the **`service enable`** command in SSL VPN context view from the CLI.
   - Verify that the SSL VPN context is associated with an SSL VPN gateway. The **Associated SSL VPN gateway** field displays the name of the SSL VPN gateway if the SSL VPN context is associated with an SSL VPN gateway. If the SSL VPN context is not associated with an SSL VPN gateway, associate one from the Web interface, or execute the **`gateway`** command in SSL VPN context view from the CLI.

   The following is an example of the SSL VPN context information:

```
[Device] display sslvpn context

Context name: ctx

  Operation state: Up

  Associated SSL VPN gateway: gw

  SSL client policy configured: sslnew

  SSL client policy in use: ssl
```

4. Verify that the SSL VPN gateway listening address and ports are correctly configured on all service modules, and the listening ports on each service module is enabled.

   The following is an example of TCP proxy information:

```
<Device> dis tcp-proxy slot 1

Local Addr:port       Foreign Addr:port     State           Service
type

1.1.1.2:2000          0.0.0.0:0                 LISTEN      SSLVPN
```

5. Verify that an SSL VPN AC interface is created, an IP address is configured for the interface, and the interface is specified in the SSL VPN context for the user.

   The following is an example of SSL VPN AC interface configuration:

```
[Device] interface SSLVPN-AC 1
[Device-SSLVPN-AC1] ip address 1.1.1.1 24
[Device-SSLVPN-AC1] quit
[Device] sslvpn context ctx
[Device-sslvpn-context-ctx] ip-tunnel interface SSLVPN-AC 1
[Device-sslvpn-context-ctx] quit
[Device] display interface SSLVPN-AC 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface                Link   Protocol    Primary IP     Description
SSLVPN-AC1           UP    UP            1.1.1.1
```

6. Verify that an address pool is configured, and is specified for the SSL VPN context or the authorization resource group for the user. The address pool cannot contain the address of the SSL VPN gateway.

   The following is an example of address pool configuration and application:

```
[Device] sslvpn ip address-pool name 1.1.1.1 1.1.1.10
[Device] sslvpn context ctx
[Device-sslvpn-context-ctx] ip-tunnel address-pool name mask 24
```

7. Verify that SSL VPN users are configured correctly.
8. Verify that the SSL VPN user is configured correctly.

- **For a local user**—Verify that the local user is a network access user, the service type for the user is SSL VPN, the user is authorized to access a resource group, and the resource group is well configured.
- **For a remote user**—Verify that the user's user group on the remote authentication server is configured in the SSL VPN context as a resource group. The user group and the resource group must use the same name.

9. If certificate authentication is enabled on the server and client, make sure certificates are installed correctly on the server and client.
10. Verify that the iNode client is of the latest version.

Failure to access internal resources from an iNode client

Symptom

A user cannot access internal resources after logging in to the SSL VPN gateway successfully from an iNode client.

Solution

To resolve the issue:

1. Verify that an SSL VPN AC interface is added to a security zone and is permitted by security policies.
2. Verify that the IP address of the VNIC assigned to the iNode client is added to a security zone and is permitted by security policies.
3. Configure an ACL or a URI ACL to permit access to the internal servers, and then specify the ACL for SSL VPN Web access. For example:

```
[Device-sslvpn-context-ctxip1] policy-group resourcegrp1
[Device-sslvpn-context-ctxip1-policy-group-resourcegrp1] filter
web-access acl 3000
```

4. Verify that the SSL VPN gateway can ping the internal resources successfully. Add routes to reach the peer devices if needed.
5. Verify that the iNode client is of the latest version.
6. Verify that both the uplinks and downlinks operate correctly. An uplink or downlink error might occur in one of the following situations:
   - The routes to the internal resources are not configured on the SSL VPN gateway. You can check the routing table on the device for route configuration.
   - The internal servers do not have routes to reach the SSL VPN gateway.
   - The device operates in dual-active mode.
   - To resolve this issue, change the dual-active mode to the active/standby mode, and the uplink and downlink interfaces to redundant interfaces.
   - An address conflict occurs.
   - An improper policy-based routing (PBR) is configured.
   - Improper SSL VPN load balancing is configured.

Failure to terminate idle SSL VPN sessions of iNode client users

Symptom

The SSL VPN sessions of iNode client users do not age out even if they are idle for a long time, consuming license resources.

Solution

An iNode client periodically sends keepalive messages so the SSL VPN sessions of the iNode client users do not age out. You can configure the idle-cut feature to force users who do not access internal resources to go offline.

The idle-cut feature sets the idle-cut traffic threshold for SSL VPN sessions. SSL VPN sessions that generate traffic less than the specified threshold within the idle timeout time are terminated. The following example sets the idle-cut traffic threshold to 1000 Kilobytes:

```
<Device> system-view

[Device] sslvpn context ctx1

[Device-sslvpn-context-ctx1] idle-cut traffic-threshold 1000
```

Others

User filtering, monitoring, and IP binding settings not take effect

Symptom

The ACL filtering, monitoring, and IP binding configuration in local user view for an SSL VPN user does not take effect.

Solution

To resolve the issue, configure these settings in SSL VPN context view instead of in local user view. This is because that some SSL VPN user management settings can only be configured in SSL VPN context view.

Failure to relog in to the SSL VPN gateway

Symptom

A user fails to relog in to the SSL VPN gateway after previous successful logins.

Solution

To resolve the issue:

1. Check whether a limit is set to the number of concurrent logins for each account. In this example, the maximum number is set to 1.

   ```
   [Device] sslvpn context ctx

   [Device-sslvpn-context-ctx] max-onlines 1
   ```

2. You can remove the configuration of the **max-onlines** command if no such limit is needed. If the limit is set and you do not want to remove it, you can enable the force logout feature. When a login is attempted but logins using the account reach the maximum, this feature logs out the user with the longest idle time to allow the new login.

   To configure the force logout feature, execute the following commands:

   ```
   [Device] sslvpn context ctx

   [Device-sslvpn-context-ctx] force-logout max-onlines enable
   ```

Web login configuration examples

Contents

Introduction

The following information provides Web login configuration examples.

The device supports both HTTP and HTTPS. You can use either of them to log in to the Web interface of the device.

When the device was shipped, HTTPS was enabled and the following settings were configured:

- Username **admin**.
- Password **admin**.
- User role **network-admin**.
- Management interface IP address **192.168.0.1/24**.

You can use the settings to log in to the Web interface of the device.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the Web login feature.

Restrictions and guidelines

When you configure Web login, follow these restrictions and guidelines:

- As a best practice, use one of the following Web browsers: Chrome 40 or later, Firefox 19 or later, or Internet Explorer 9 or later.
- Configure the Web browser to accept cookies from Web sites and use active scripts or JavaScript. For information about how to configure the Web browser, see the Web browser user guide.
- To use Internet Explorer, you must also enable the following features:
    - Execute scripts for ActiveX controls that are marked as secure scripts
    - Run ActiveX controls and plug-ins.
- After a device software version change, clear the browser cache to make sure the Web interface displays the correct information.

Example: Configuring Web login

Network configuration

As shown in Figure 1, connect the host to the device. Configure the device to allow the host to log in to the Web interface of the device through a non-management interface.

Figure 1 Network diagram

Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Using the factory-default settings to log in

1. Use an Ethernet cable to connect the host to management interface GE 1/0/0 on the device.
2. Assign IP address 192.168.0.2/24 to the host.

   This IP address belongs to the same subnet as management interface GE 1/0/0. The host and the device can reach each other.

3. Launch the Web browser and enter **https://192.168.0.1** in the address bar.

   The Web interface login page opens.

4. Enter the username **admin** and password **admin**, select a language, and click **Login**.

   In the dialog box that opens, change the default password for the factory-default account immediately.

Configuring Web login through a non-management interface

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/2.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask length of the interface. In this example, enter 192.168.200.1/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

2. Create a security policy:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy named **trust-to-local** to permit the specified traffic from the **Trust** to **Local** security zones:

   - Enter policy name **trust-to-local**.
   - Select source zone **Trust**.
   - Select destination zone **Local**.
   - Select type **IPv4**.
   - Select action **Permit**.

- Select source IPv4 address **192.168.200.0/24**.
- Use the default settings for other parameters.

Click **OK**.

3. Configure a Web login user:

   # On the top navigation bar, click **System**.

   # From the navigation pane, select **Administrators** > **Administrators**.

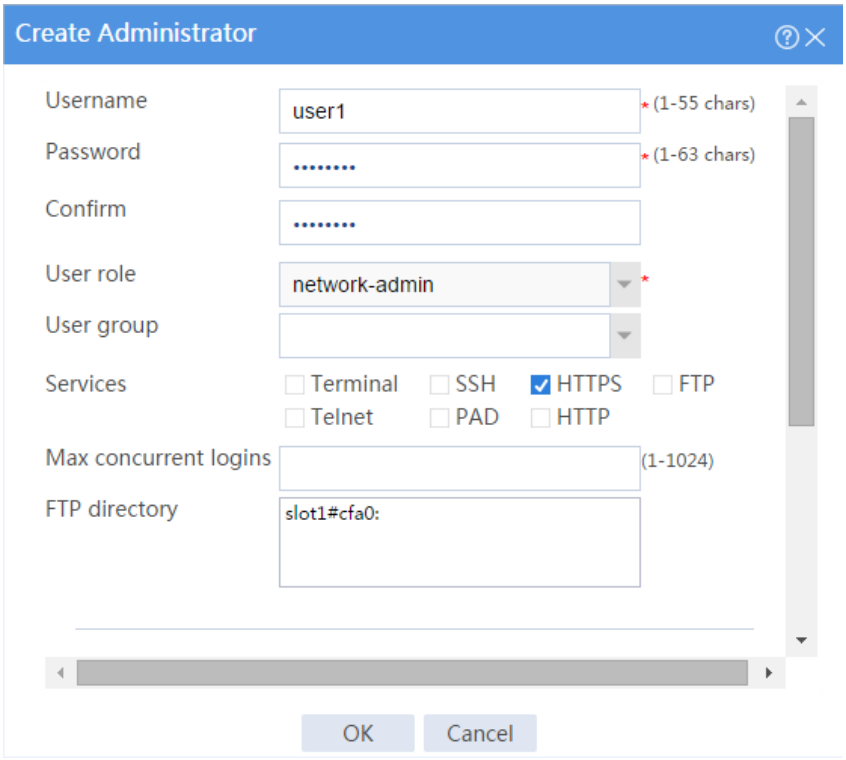
   # Click **Create**.

   # In the dialog box that opens, configure a Web login user:

   - Enter username **user1**.
   - Enter a password and confirm the password.
   - Select user role **network-admin**.
   - Select service **HTTPS**.
   - Use the default settings for other parameters.

   # Click **OK**.

Figure 2 Configuring a Web login user



Verifying the configuration

1. Launch the Web browser and enter **https://192.168.200.1** in the address bar.

   The Web interface login page opens.

2. Enter username **user1** and the password, select a language, and click **Login**.

   The Web interface of the device opens.

Internet access through a static IP address configuration examples

Contents

Introduction

The following information provides the configuration examples of using a static IP address to access the Internet.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of IP features.

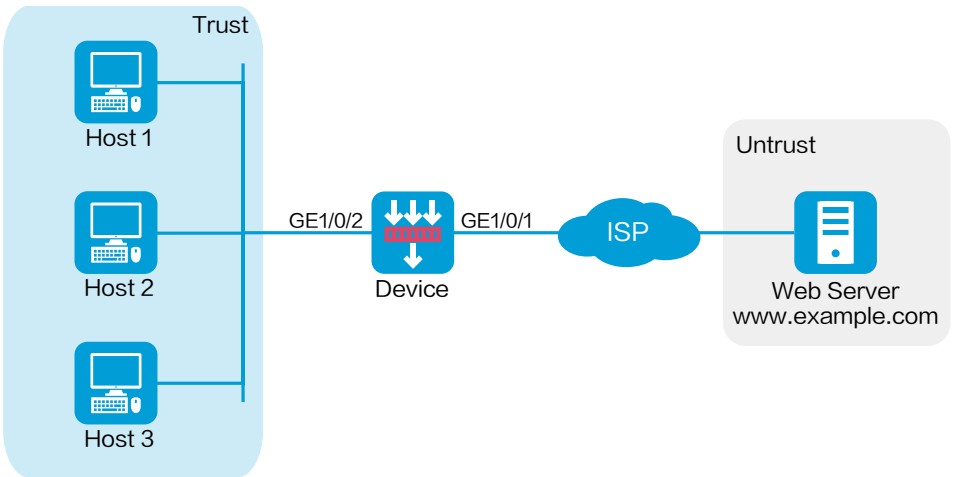
Example: Configuring Internet access through a static IP address

Network configuration

As shown in Figure 1, a device is deployed as the egress device that connects the internal network to the ISP. Perform the following tasks to allow the internal users to access the Internet:

- Configure the DHCP server on the device to assign private IP addresses and the DNS server address to the hosts.
- Allow the internal users to access the Web server on the Internet. The website of the Web server is www.example.com.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

When you configure the DHCP server on the device, perform the following tasks:

- Allow traffic from security zones **Trust** (to which the DHCP server belongs) to **Local** to ensure that the DHCP clients can obtain IP addresses.
- Enable DNS proxy on the device to convey DNS requests between the DNS server and the DNS clients.

Procedures

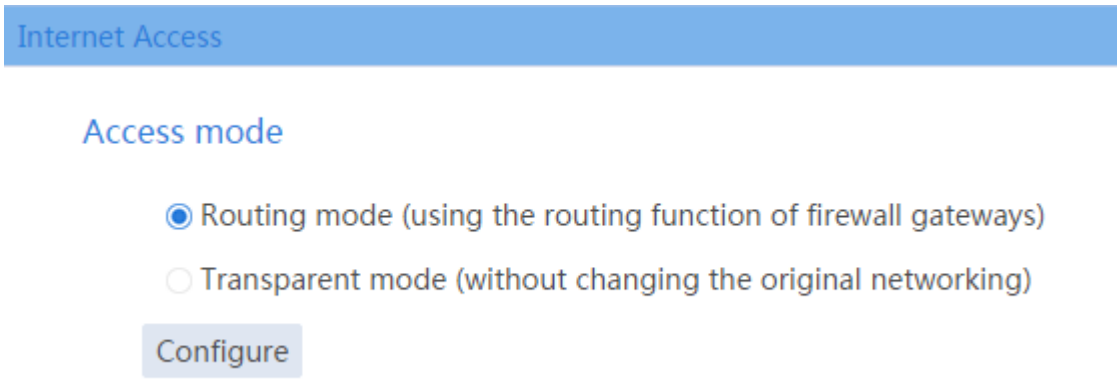
Configuring the device

1. Configure a static IP address.

On the top navigation bar, click **System**.

From the navigation pane, select **Configuration Wizard** > **Internet Access**.

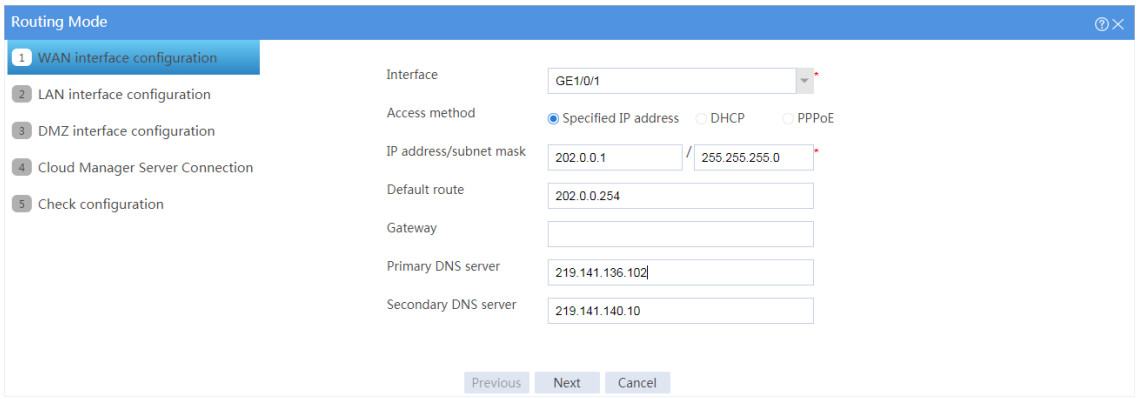
Figure 2 Internet access configuration page



Select the routing mode and click **Configure**.

Configure the WAN interface as shown in Figure 3.

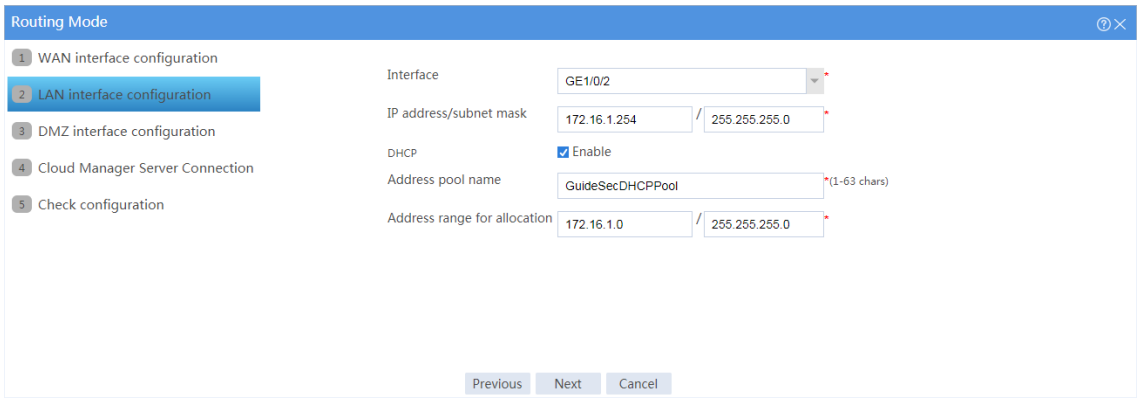
Figure 3 WAN interface configuration



Click **Next**.

Configure the LAN interface as shown in Figure 4.

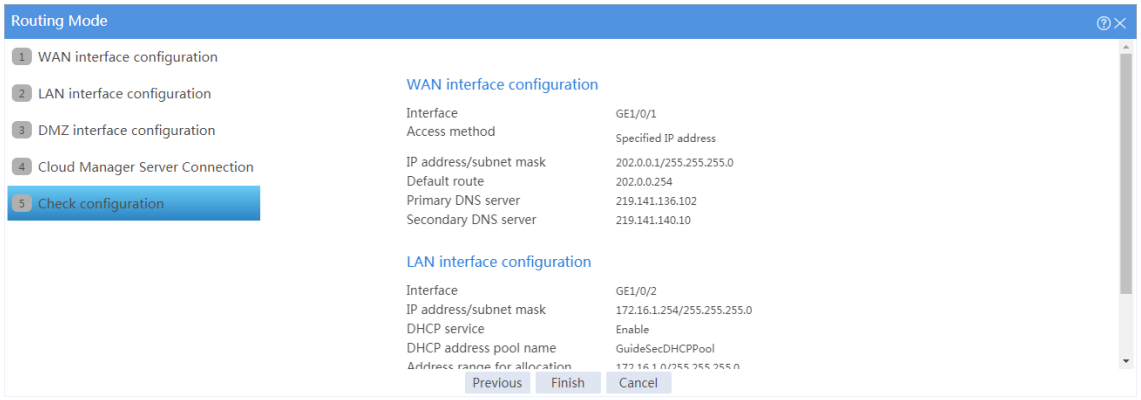
Figure 4 LAN interface configuration



Click **Next**. Skip the configuration for the DMZ interface and security cloud.

Click **Next**. The following page opens.

Figure 5 Verify the configuration



Verify the configuration and click **Finish**.

2. Configure a security policy.

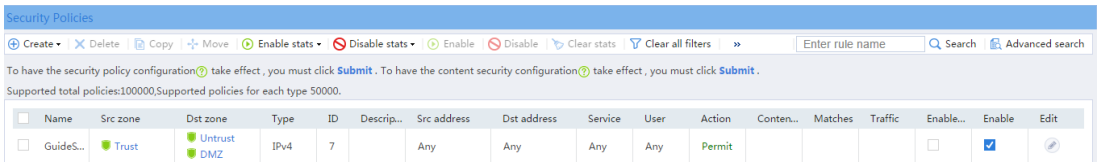
After you configure the Internet access through a static IP address, the system automatically creates a security policy named **GuideSecPolicy**.

To view the security policy:

a. On the top navigation bar, click **Policies**.

b. From the navigation pane, select **Security Policies** > **Security Policies**.

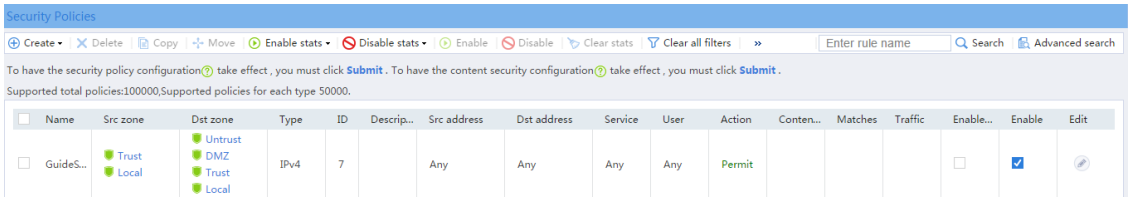
Figure 6 Security policy configuration page



Click the **Edit** icon for this security policy.

In the dialog box that opens, add security zone **Local** to the source zones, and add security zones **Trust** and **Local** to the destination zones.

Figure 7 Editing the security policy



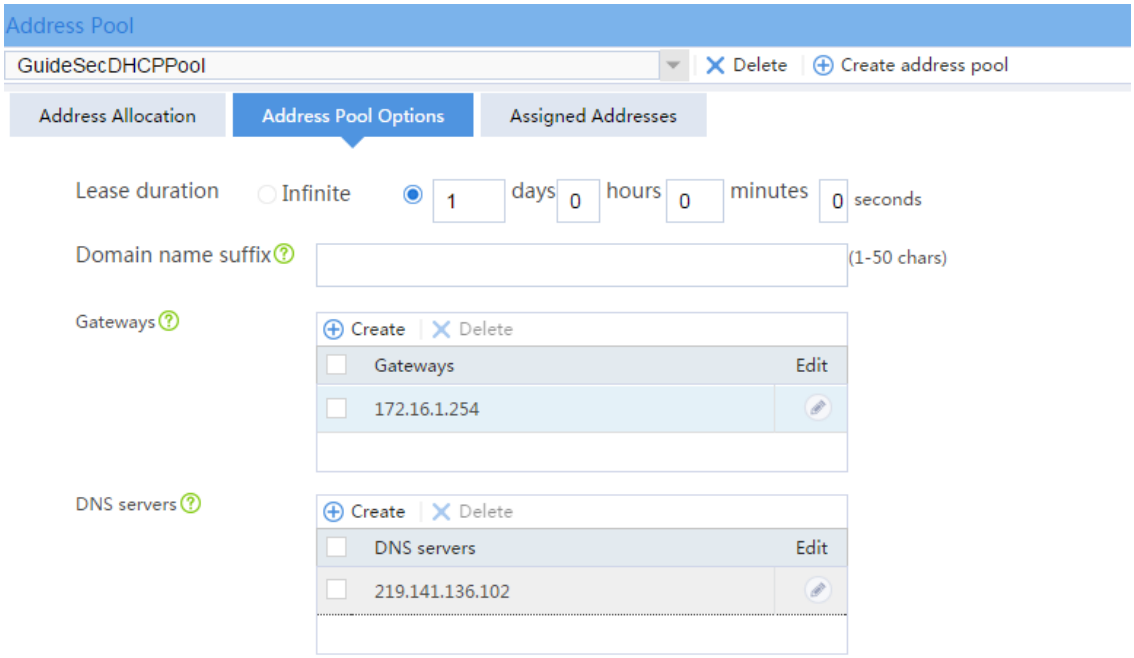
3. Configure DHCP.

On the top navigation bar, click **Network**.

From the navigation pane, select **DHCP** > **DHCP Address Pools**.

Click the **Address Pool Options** tab, and configure the settings as shown in Figure 8.

Figure 8 Address pool option configuration



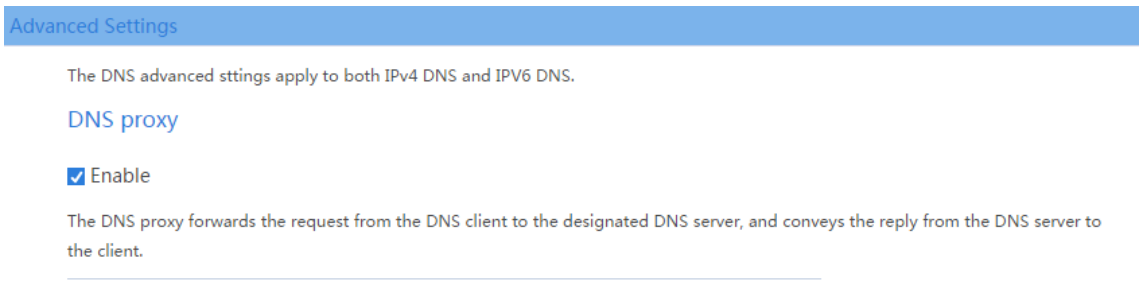
4. Configure DNS proxy.

On the top navigation bar, click **Network**.

From the navigation pane, select **DNS** > **Advanced Settings**.

Enable the DNS proxy.

Figure 9 DNS proxy configuration page



Configuring the host

Configure the host to obtain an IP address through DHCP.

Verifying the configuration

1. Display the IP address that the host obtains.

```
C:\>ipconfig /all

Ethernet adapter Ethernet 1:

   Connection-specific DNS SUffix.:

   Description.....................: Intel(R) 82579LM Gigabit Network
Connection

   Physical Address................: E8-39-35-5C-92-B8

   DHCP Enabled ...................: Yes

   Autoconfiguration Enabled......: Yes

   Link-local IPv6 Address........:
fe80::b8dd:d091:201a:6db2%13(Preferred)

   IPv4 Address....................: 172.16.1.3(Preferred)

   Subnet Mask.....................: 255.255.255.0

   Lease Obtained..................: Monday, October 8, 2018 2:44:36 AM

   Lease Expires...................: Tuesday, October 9, 2018 2:44:36 AM

   Default Gateway.................: 172.16.1.254

   DHCP Server.....................: 172.16.1.254

   DHCPv6 IAID.....................: 384317749
```

```
   DHCPv6 Client DUID.............:
00-01-00-01-1F-B4-A3-F5-B8-A3-86-6F-0F-02

   DNS Server.....................: 219.141.136.102

   NetBIOS over Tcpip.............: Enabled
```

2. Verify that you can ping a domain name on the public network from the host.

```
C:\>ping www.example.com


Pinging www.example.com [192.168.100.201] with 32 bytes of data:

Reply from 192.168.100.201: bytes=32 time<1ms TTL=253

Reply from 192.168.100.201: bytes=32 time<1ms TTL=253

Reply from 192.168.100.201: bytes=32 time<1ms TTL=253

Reply from 192.168.100.201: bytes=32 time<1ms TTL=253


Ping statistics for 192.168.100.201:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Internet access through PPPoE configuration examples

Contents

Introduction

The following information provides Internet access through PPPoE examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

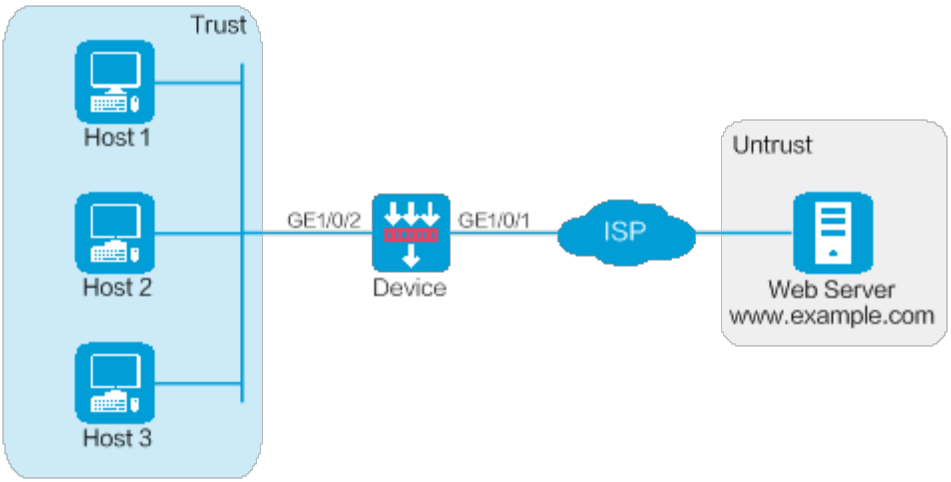
The following information is provided based on the assumption that you have basic knowledge of PPPoE.

Example: Accessing the Internet through PPPoE

Network configuration

As shown in Figure 1, Device is deployed at the egress of the enterprise network. The enterprise applies for a PPPoE account with the username as **pppoeuser1** and password as **123456** from the ISP. Configure PPPoE for users in the enterprise network to access the Web server with the address www.example.com in the Internet.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

When the device acts as a DHCP server, for the DHCP clients to obtain IP addresses, you must permit the traffic from the security zone where the DHCP-enabled interfaces reside to the local security zone. In this example, you must permit the traffic from security zone **Trust** to security zone **Local**.

Procedures

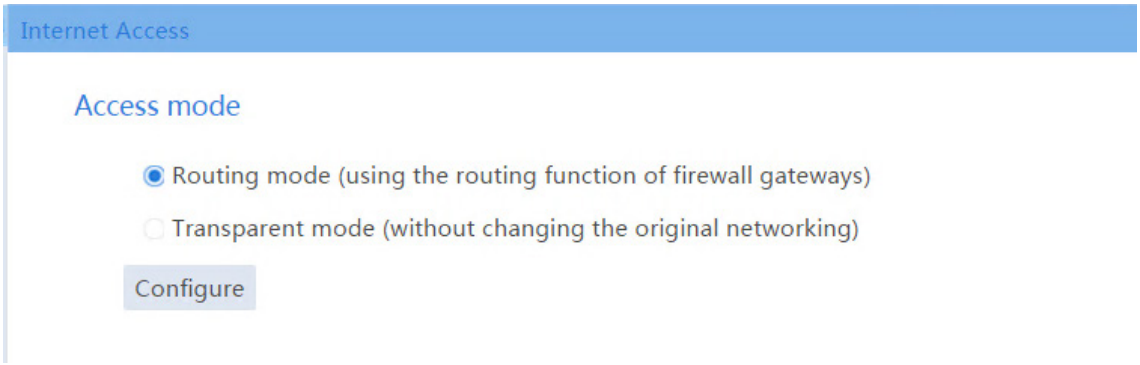
Configuring Device

1. Configure PPPoE.

On the top navigation bar, click **System**.

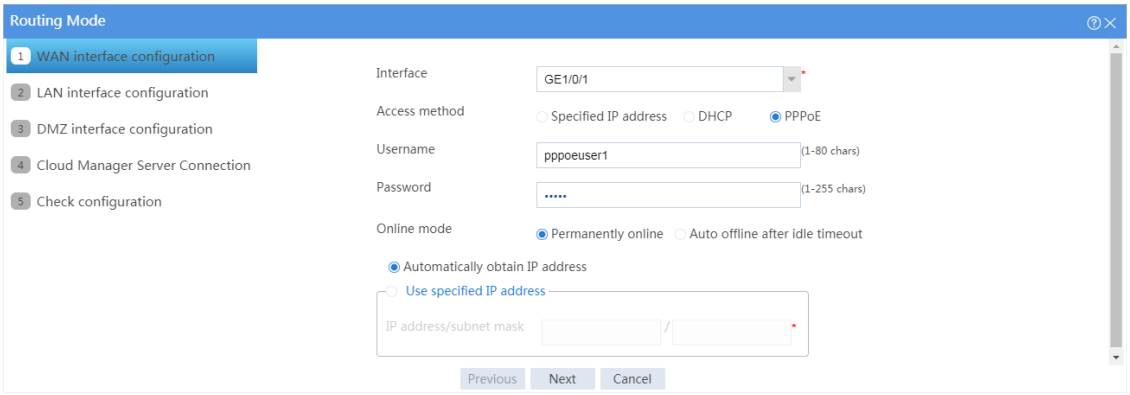
From the navigation pane, select **Configuration Wizard** > **Internet Access**. The page as shown in Figure 2 opens.

Figure 2 Internet Access



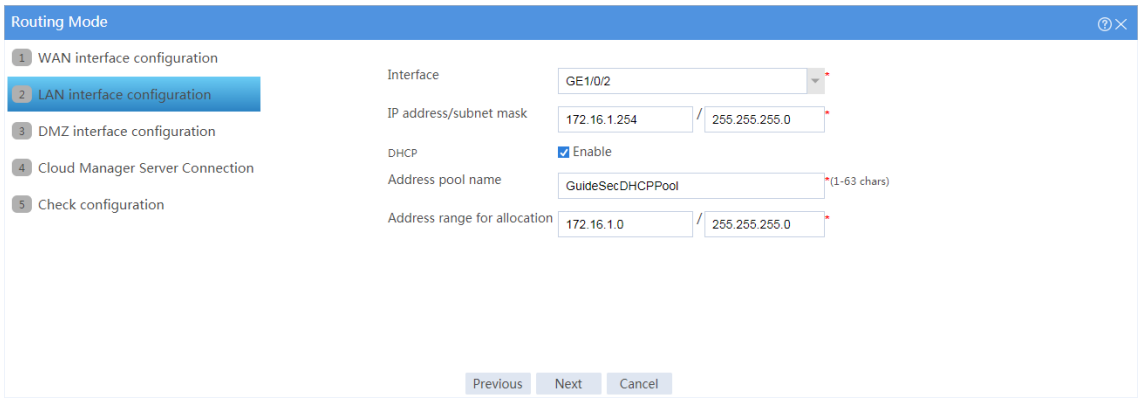
Select **Routing mode**, and click **Configure**. Configure the WAN interface parameters as shown in Figure 3.

Figure 3 WAN interface configuration



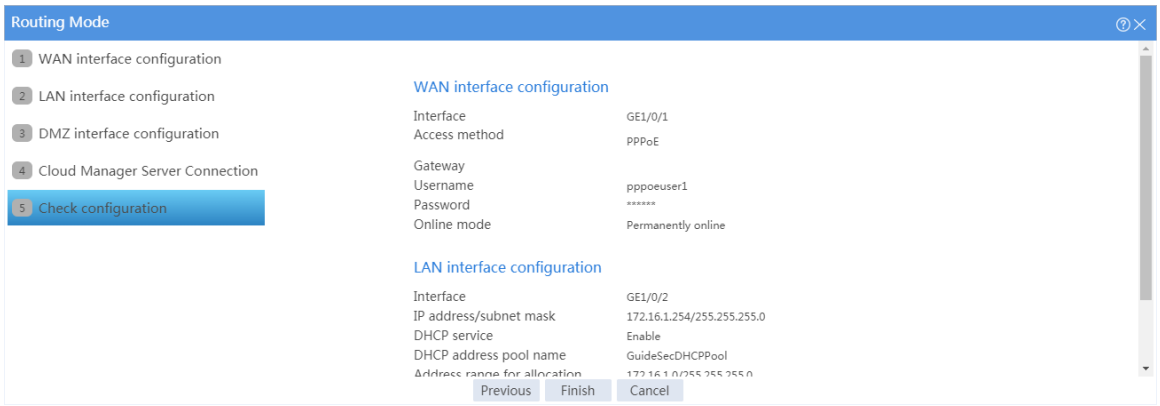
Click **Next**. Configure the LAN interface parameters as shown in Figure 4.

Figure 4 LAN interface configuration



Click **Next**. Do not make any DMZ interface or WAN cloud manager server connection configuration on the page that opens, and click **Next** to check the configuration.

Figure 5 Check configuration



Verify that the configurations are correct, and click **Finish**.

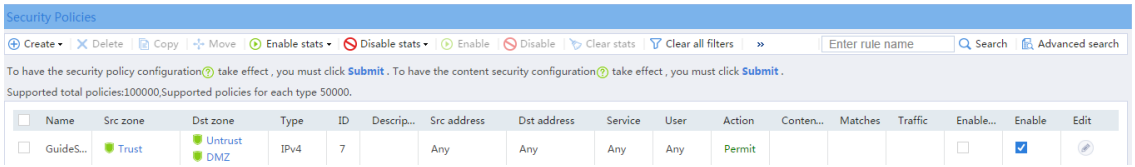
2. Configure a security policy.

After PPPoE is configured, the system automatically creates a security policy named **GuideSecPolicy**.

On the top navigation bar, click **Policies**.

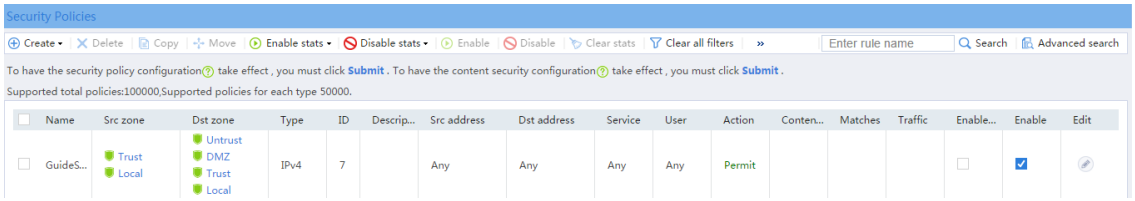
From the navigation pane, select **Security Policies** > **Security Policies**. The **Security Policies** page as shown in Figure 6 opens.

Figure 6 Security policy configuration page



Select the security policy **GuideSecPolicy**, and click the icon in the **Edit** column. Add the source zone **Local**, and add the destination zones **Trust** and **Local**, as shown in Figure 7.

Figure 7 Adding a security policy



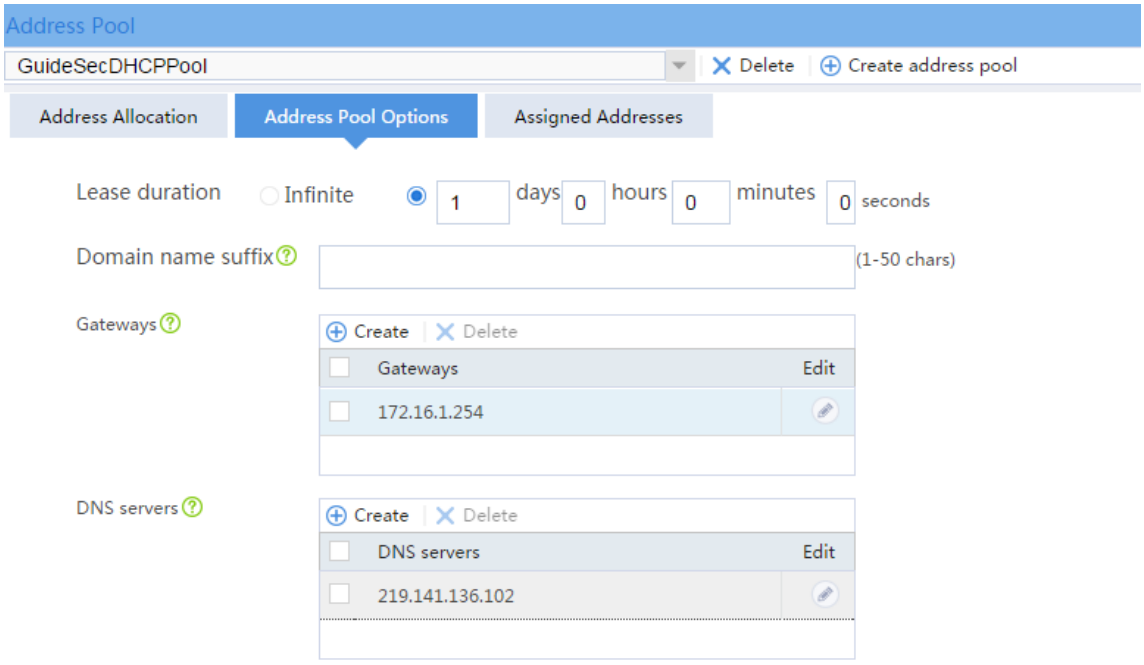
3. Configure DHCP.

On the top navigation bar, click **Network**.

From the navigation pane, select **DHCP** > **DHCP Address Pools**.

Click the **Address Pool Options** tab. Configure parameters as shown in Figure 8.

Figure 8 Address pool options

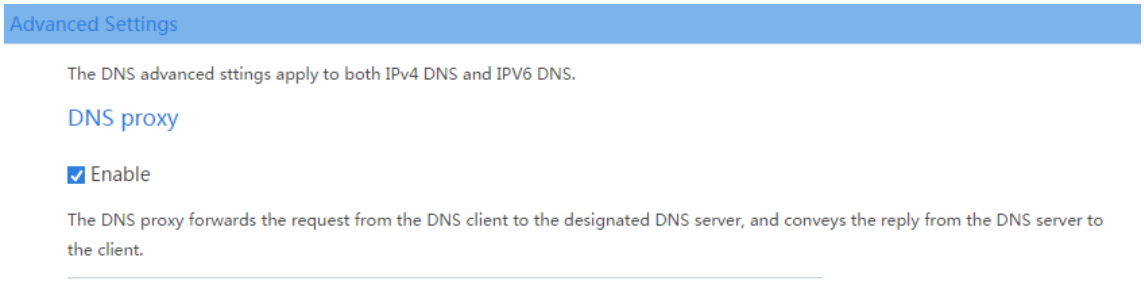


4. Configure DNS proxy.

On the top navigation bar, click **Network**.

From the navigation pane, select **DNS** > **Advanced Settings**. On the page as shown in Figure 9, enable DNS proxy.

Figure 9 DNS proxy



Configuring the hosts

Configure the hosts to automatically obtain IP addresses.

Verifying the configuration

1. View the address information that a host obtains.

```
C:\>ipconfig /all

Ethernet adapter Local Area Connection:


   Connection-specific DNS Suffix.....:

   Description.....................: Intel(R) 82579LM Gigabit
Network Connection

   Physical Address.................: E8-39-35-5C-92-B8

   DHCP Enabled ..............: Yes

   Autoconfiguration Enabled..............: Yes

   Link-local IPv6 address.....:
fe80::b8dd:d091:201a:6db2%13(Preferred)

   IPv4 Address..................: 172.16.1.3(Preferred)

   Subnet Mask.....................: 255.255.255.0

   Lease Obtained..............: May 25, 2017 14:01:30

   Lease Expires..............: May 26, 2017 14:01:30

   Default Gateway.....................: 172.16.1.254

   DHCP Server..................: 172.16.1.254
```

```
   DHCPv6 IAID.................: 384317749

   DHCPv6 Client DUID...........:
00-01-00-01-1F-B4-A3-F5-B8-A3-86-6F-0F-02


   DNS Servers.................: 172.16.1.254

   NetBIOS over Tcpip..........: Enabled
```

2. Verify that a host can ping the server address www.example.com.

```
C:\>ping www.example.com


Ping www.example.com [192.168.100.201]: 32 data bytes

32 bytes from 192.168.100.201: time<1ms TTL=253

32 bytes from 192.168.100.201: time<1ms TTL=253

32 bytes from 192.168.100.201: time<1ms TTL=253

32 bytes from 192.168.100.201: time<1ms TTL=253


--- Ping statistics for 192.168.100.201 ---

4 packets transmitted, 4 packets received, 0.0% packet loss

round-trip min/avg/max = 0/0/0 ms
```

Signature library update configuration examples

Contents

Introduction

The following information provides signature library update configuration examples.

The following methods are available for updating the signature library on the device:

- **Automatic scheduled update**—The device automatically downloads the most up-to-date signature file to update its local signature library periodically.
- **Manual update**—Use this method when the device cannot obtain the signature file automatically. You must manually download the most up-to-date signature file, and then use the file to update the signature library on the device.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the signature library upgrade feature.

General restrictions and guidelines

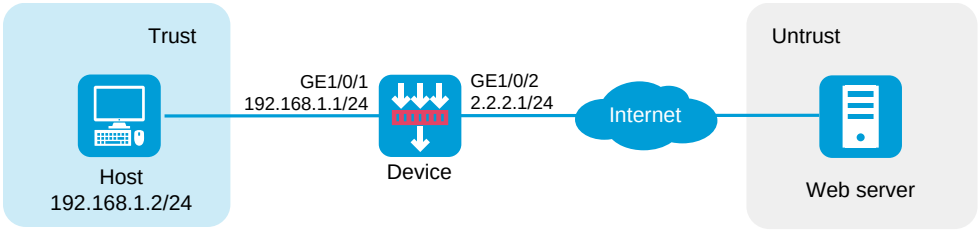
The signature library for each security service requires a license to run on the device. After the license expires, the related service can use the existing signature library on the device, but the library cannot be updated.

Example: Configuring scheduled automatic update of the signature library

Network configuration

As shown in Figure 1, the internal users in the **Trust** security zone can access the Internet resources in the **Untrust** security zone. Configure the device to update the IPS signature library at 3:00:00 every Saturday.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

Before configuring this feature, make sure:

- The device can access the update server directly or through a proxy server.
- The IPS license is in running status.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Trust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 192.168.1.1/24.
   - Use the default settings for other parameters.
   - Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 2.2.2.1./24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

   This example configures static routes.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure an IPv4 static route:

- Enter destination address **0.0.0.0**.
- Enter mask length 0.
- Enter next-hop address **2.2.2.2**.
- Use the default settings for other parameters.
- Click **OK**.

3. Configure a DNS server:

This example uses DNS server IP address 10.72.66.36.

On the top navigation bar, click **Network**.

From the navigation pane, select **DNS** > **DNS Clients**.

Enter DNS server IP address 10.72.66.36, and click **Add**.

4. Configure a security policy named **Local-to-Untrust**:

- Enter policy name **Local-to-Untrust**.
- Select source security zone **Local**.
- Select destination security zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Use the default settings for other parameters.
- Click **OK**.

5. Configure the device to update the IPS signature library automatically at a scheduled time.

On the top navigation bar, click **System**.

From the navigation pane, select **Upgrade Center** > **Signature Upgrade**.

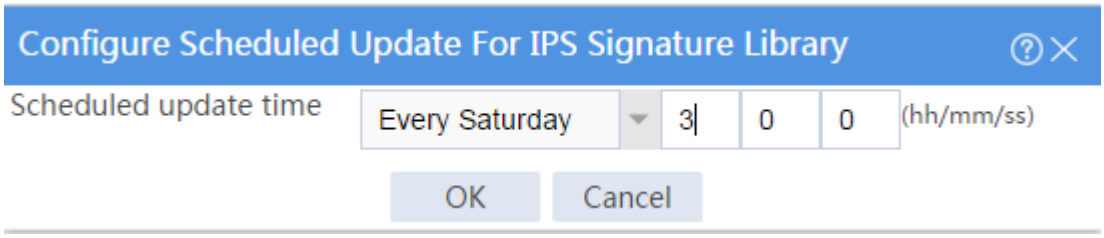
Select the check box for **Auto update** for the IPS signature library.

In the dialog box that opens, set the scheduled update time to 03:00:00 every Saturday.

A scheduled automatic library update will occur at a random time between the following time points:

- An hour before the specified start time.
- An hour after the specified start time.

Figure 2 IPS signature library scheduled update configuration



Click **OK**.

Verifying the configuration

After the scheduled update time, access the signature library update list and verify that the IPS signature library has been updated.

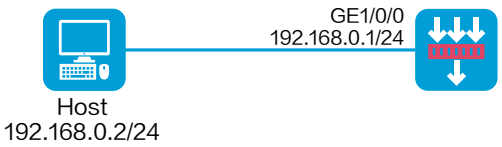
Figure 3 Viewing the signature library version

Example: Using a local signature file to update the device signature library

Network configuration

As shown in Figure 4, the up-to-date IPS signature file V7-IPS-1.0.128.dat is saved locally. Use the manual update method to load the file to the update the device IPS signature library.

Figure 4 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

The device is preconfigured with a management port (for example, GE1/0/0) that has an IP address of 192.168.0.1/24. The IP address of the host must be I the same subnet as the

management port. You can log in to the Web interface of the device to configure the device by entering https://192.168.0.1 in the browser.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Trust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.
   - Use the default settings for other parameters.
   - Click **OK**.

2. Configure a security policy named **Trust-Local**, ensuring that the internal users can use a PC to access the Internet:

   - Enter policy name **Trust-Local**.
   - Select source security zones **Trust** and **Local**.
   - Select destination security zones **Trust** and **Local**.
   - Select type **IPv4**.
   - Select action **Permit**.
   - Use the default settings for other parameters.
   - Click **OK**.

3. Import the local IPS signature file.

   # On the top navigation bar, click **System**.

   # From the navigation pane, select **Upgrade Center** > **Signature Upgrade**.

   # Click the **Manual update** link for the IPS signature library.

   # In the dialog box that opens, select the locally saved signature file V7-IPS-1.0.128.dat.

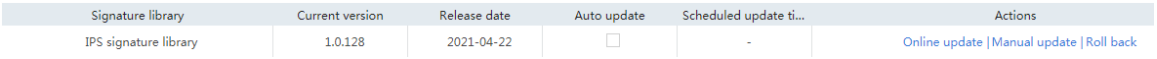
Figure 5 Selecting the locally saved signature file

   # Click **OK**.

Verifying the configuration

On the signature library update list, verify that the IPS signature library has been updated.

Figure 6 Signature library update list



Software upgrade examples

Contents

Introduction

The following information provides Web-based software upgrade examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the software upgrade feature.

Restrictions and guidelines

To upgrade device software, follow these restrictions and guidelines:

- To reduce impact on users, upgrade software when user traffic is low.
- Before upgrading software, back up the current software images.
- Make sure the connection between the configuration terminal and the device is not closed during the upgrade.
- When the device was shipped, HTTPS was enabled and the following settings were configured:
    - Username **admin**.
    - Password **admin**.
    - User role **network-admin**.
    - Management interface IP address **192.168.0.1/24**.

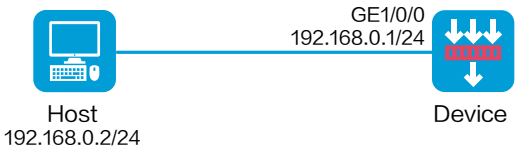
    By default, you can connect a configuration terminal to the management interface and use the settings to log in to the Web interface of the device to manage the device.

Example: Upgrading software

Network configuration

As shown in Figure 1, use the host to log in to the device and upgrade device software.

Figure 1 Network diagram



Software versions used

This example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring the host

1. Use an Ethernet cable to connect the host to management interface GE 1/0/0 on the device.
2. Assign IP address 192.168.0.2/24 to the host.

   This IP address belongs to the same subnet as management interface GE 1/0/0. The host and the device can reach each other.

3. Launch the Web browser and enter **https://192.168.0.1** in the address bar.

   The Web interface login page opens.

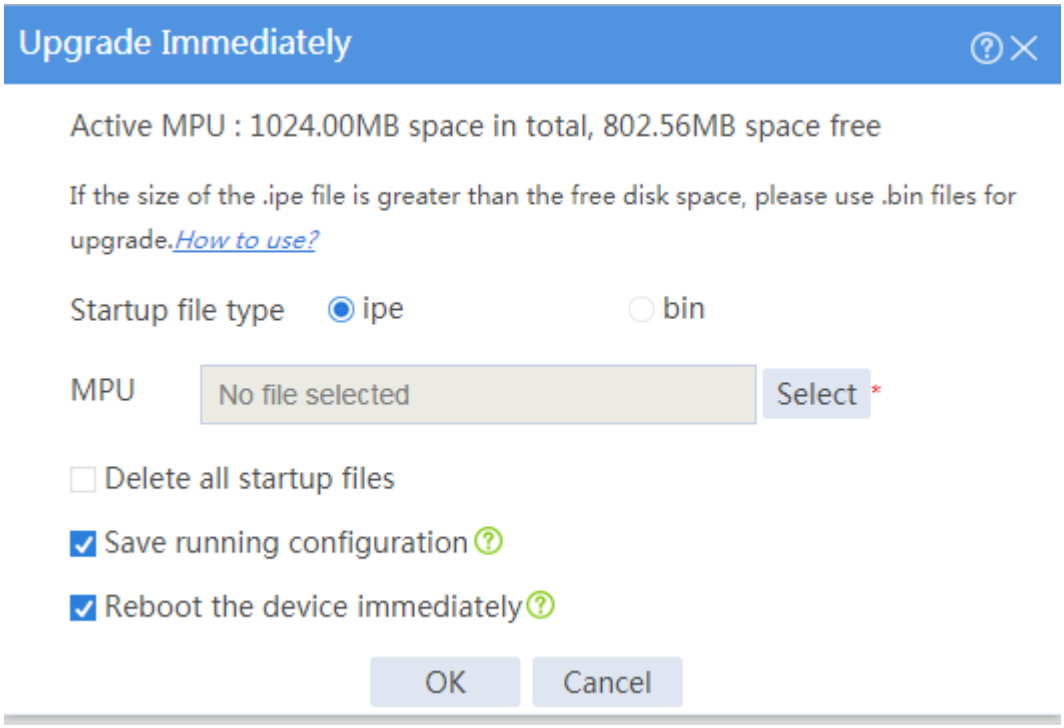
4. Enter the username **admin** and password **admin**, select a language, and click **Login**.

> IMPORTANT:
> For device security, change the password for the factory-default account immediately.

Upgrading software

1. On the top navigation bar, click **System**.
2. From the navigation pane, select Upgrade Center > Software Upgrade.
3. Click **Upgrade immediately**.
4. Click **Select** and select the .ipe upgrade file.
5. Verify that the **Reboot the device immediately** option is selected.
6. Click **OK**.

Figure 2 Upgrading software



Verifying the configuration

On the top navigation bar, click **System**.

From the navigation pane, select **Maintenance** > **About** > **Version Info**.

View the version information.

Routing deployment configuration examples

Contents

Introduction

Routing deployment enables the device to operate at Layer 3 (both the uplink and downlink service interfaces of the device operate at Layer 3) in the network, implementing security inspection and control for network traffic.

Routing deployment requires changing the existing network address plan, and enables the device to support various routing and security features.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

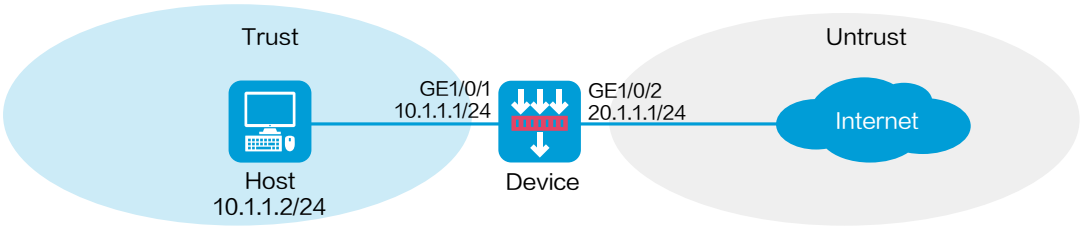
The following information is provided based on the assumption that you have basic knowledge of interface configuration and security policies.

Example: Configuring routing deployment

Network configuration

As shown in Figure 1, an enterprise deploys a device as a security protection device at the network border. The device can connect the internal network and the Internet, perform security inspection and control for network traffic, and support routing and various security features.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the IP address and security zone settings as shown in Figure 2.

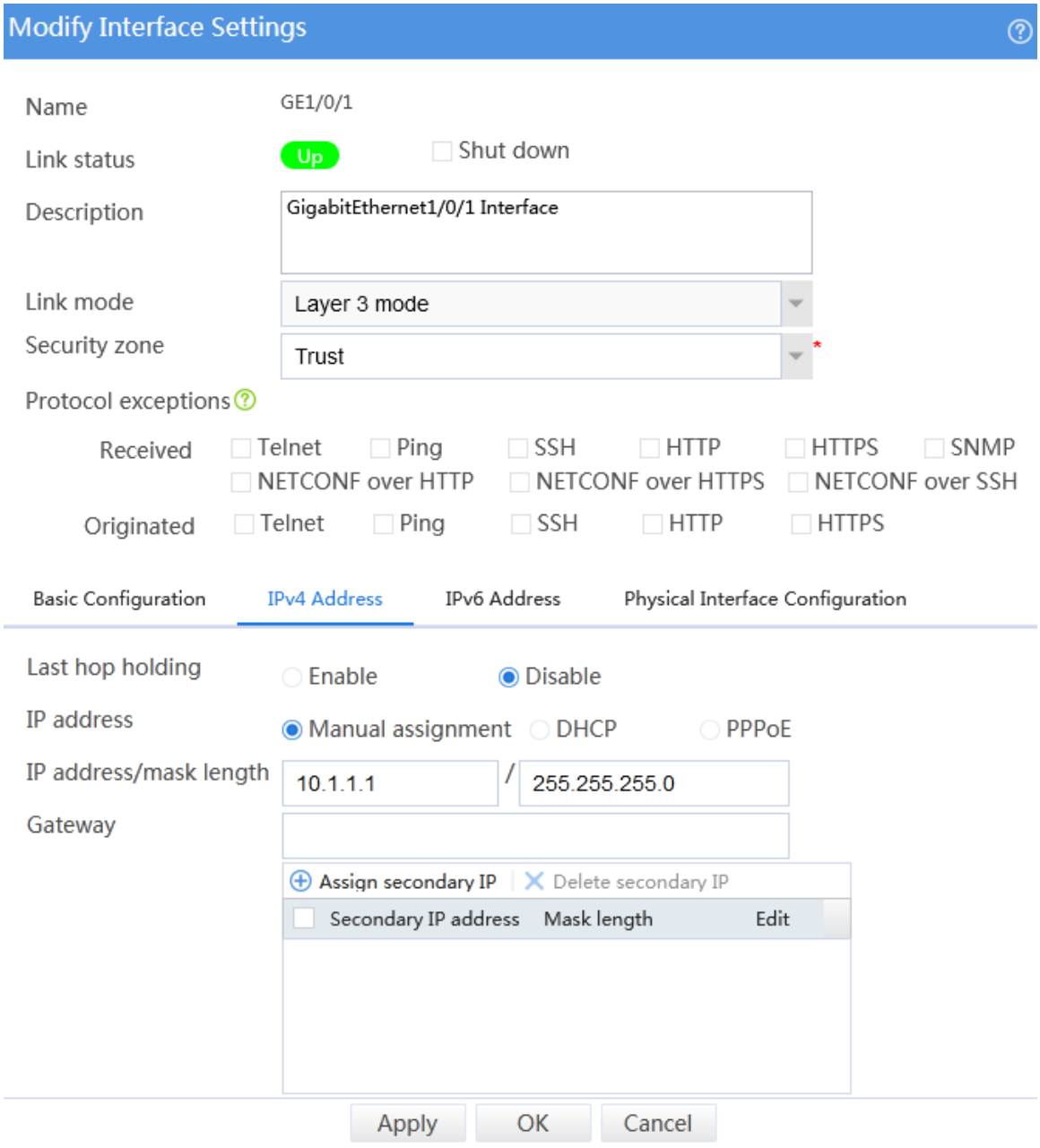
a. Select the **Trust** security zone.

b. Enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.

c. Use default settings for other parameters.

d. Click **OK**.

Figure 2 Configuring interface information



Configure the IP address and security zone settings for GE 1/0/2 in the same way you configure GE 1/0/1.

2. Configure a static route:

You can configure a dynamic routing protocol based on network requirements. This example uses a static route as an example. Assume the next hop IP address that the device connects to the external network is 20.1.1.2.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure the following parameters:

a. Enter the destination IP address 0.0.0.0.

b. Specify the mask length as 0.

c. Specify the next hop IP address as 20.1.1.2.

d. Use default settings for other parameters.

Click **OK**.

3. Create a security policy to enable the host to access the external network.

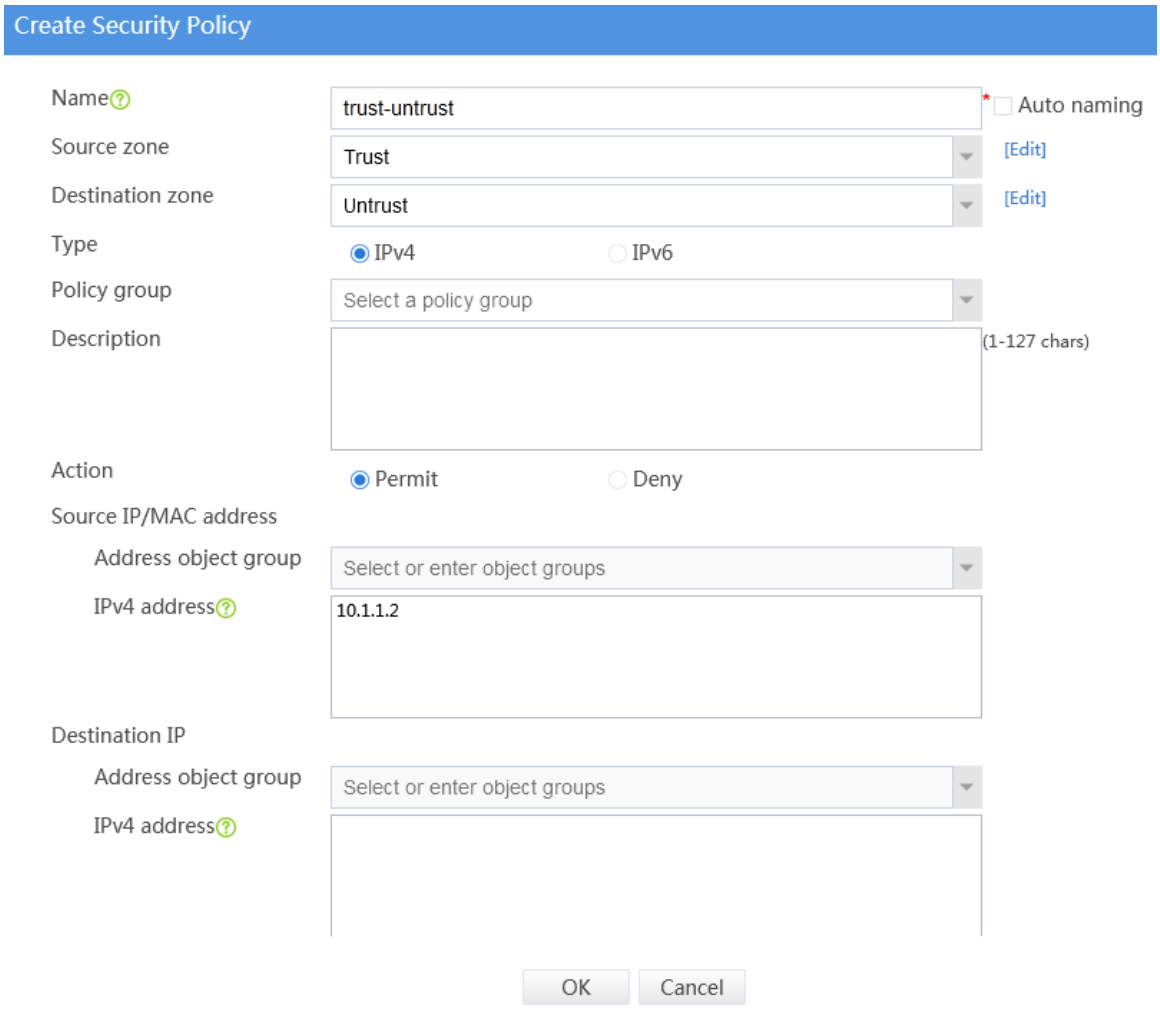
On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure the security policy as shown in Figure 3.

Figure 3 Creating a security policy



Use default settings for other parameters, and then click **OK**.

Configuring the host

Configure the IPv4 address of the default gateway as 10.1.1.1 for the host.

Verifying the configuration

Verify that only the host with IP address 10.1.1.2 in the internal network can access the external network. Other hosts cannot access the external network.

Transparent deployment configuration examples

Contents

Introduction

Transparent deployment enables the device to operate at Layer 2 (both the uplink and downlink service interfaces of the device operate at Layer 2) in the network, implementing security inspection and control for network traffic.

Transparent deployment can implement fast device deployment and security service onboarding without changing the existing network address plan.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

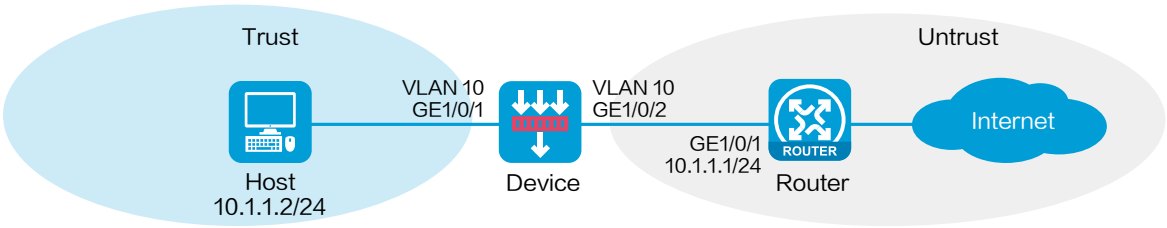
The following information is provided based on the assumption that you have basic knowledge of interface configuration, VLAN, and security policies.

Example: Configuring transparent deployment

Network configuration

As shown in Figure 1, an enterprise deploys a device as a security protection device at the network border. The device can connect the internal network and the Internet and perform security inspection and control for network traffic without requiring changing the existing network configuration.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring the router

Configure the IPv4 address of GigabitEthernet 1/0/1 as 10.1.1.1/24.

Configure a route, setting the next hop IPv4 address for traffic destined to the Internet as the IPv4 address of the peer end of the output interface.

Configuring the device

1. Create VLAN 10.

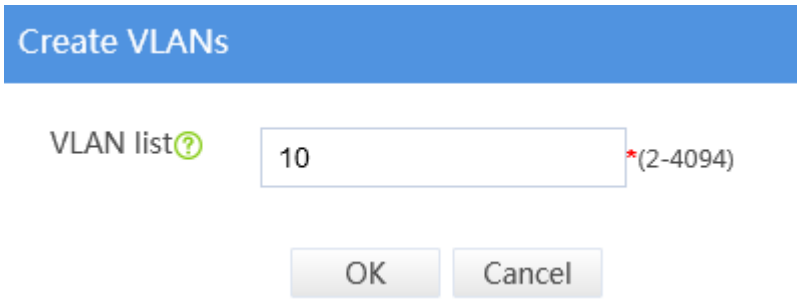
On the top navigation bar, click **Network**.

From the navigation pane, select **Link** > **VLANs**.

Click **Create**.

In the dialog box that opens, enter 10 for the **VLAN list** field, as shown in Figure 2.

Figure 2 Creating a VLAN



Click **OK**.

2. Specify the link mode, security zone, and VLAN settings for interfaces.

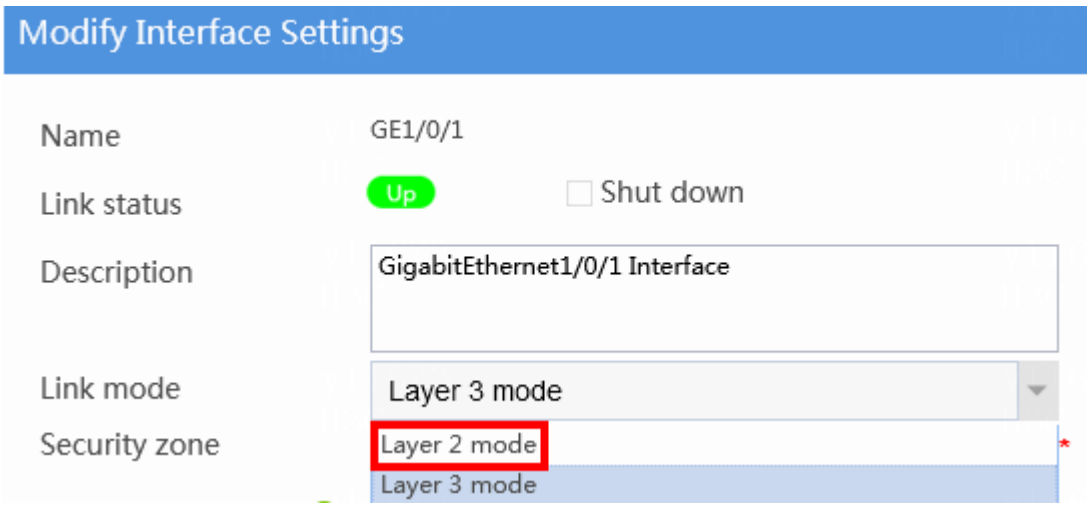
On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

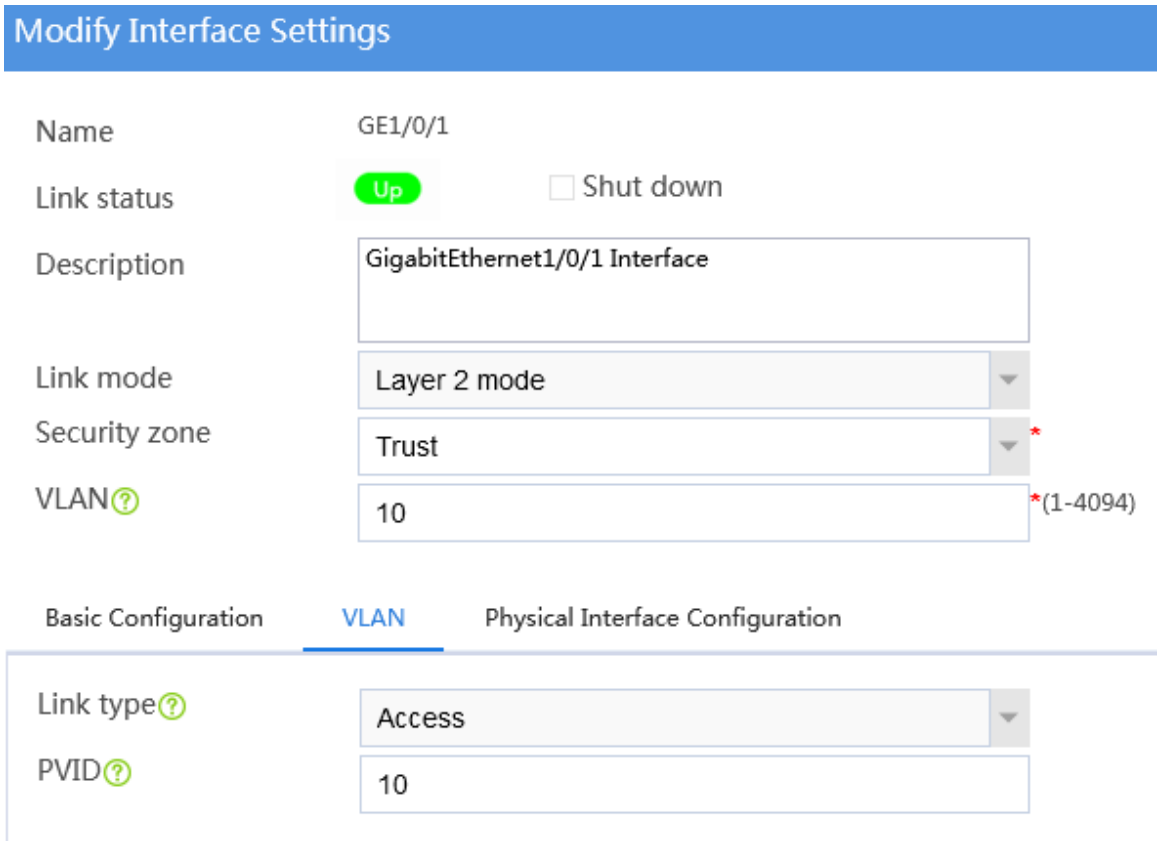
In the dialog box that opens, set the link mode for the interface to Layer 2 mode, as shown in Figure 3.

Figure 3 Setting the Layer 2 link mode



Add GE 1/0/1 to the security zone **Trust** and VLAN 10, as shown in Figure 4.

Figure 4 Specifying the security zone and VLAN for the interface



Use default settings for other parameters, and click **OK**.

Specify the link mode (**Layer 2 mode**), security zone (**Untrust**), and VLAN (VLAN 10) settings for GE 1/0/2 in the same way GE 1/0/1 is configured. (Details not shown.)

3. Create a security policy to enable the host to access the external network.

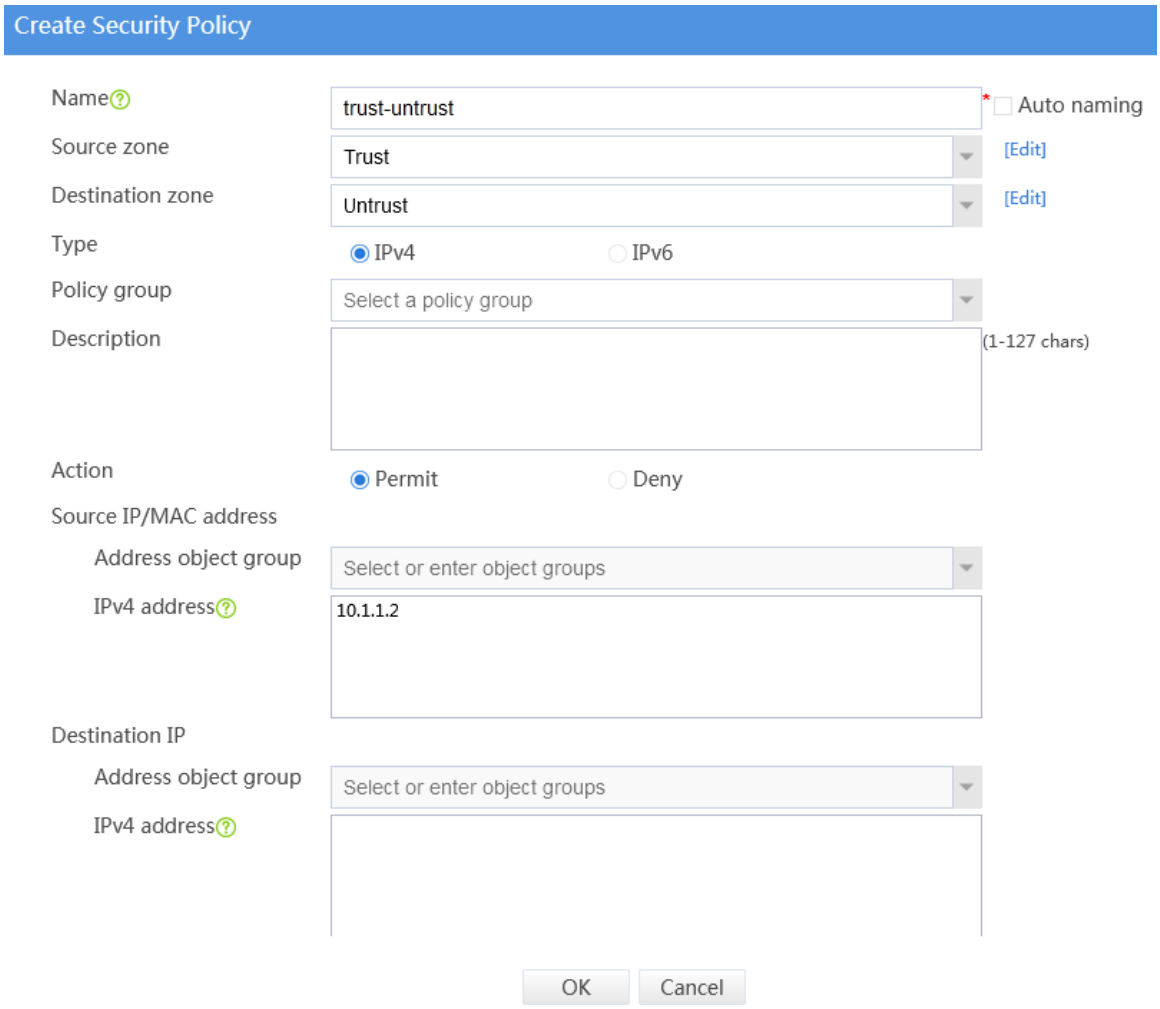
On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure the security policy as shown in Figure 5.

Figure 5 Creating a security policy



Use default settings for other parameters, and then click **OK**.

Configuring the host

Configure the IPv4 address of the default gateway as 10.1.1.1 for the host.

Verifying the configuration

Verify that only the host with IP address 10.1.1.2 in the internal network can access the external network. Other hosts cannot access the external network.

Static routing configuration examples

Contents

Introduction

The following information provides static routing configuration examples.

Static routes are manually configured. If a network's topology is simple, you only need to configure static routes for the network to work correctly.

Static routes cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the network administrator must modify the static routes manually.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the static routing feature.

Restrictions and guidelines

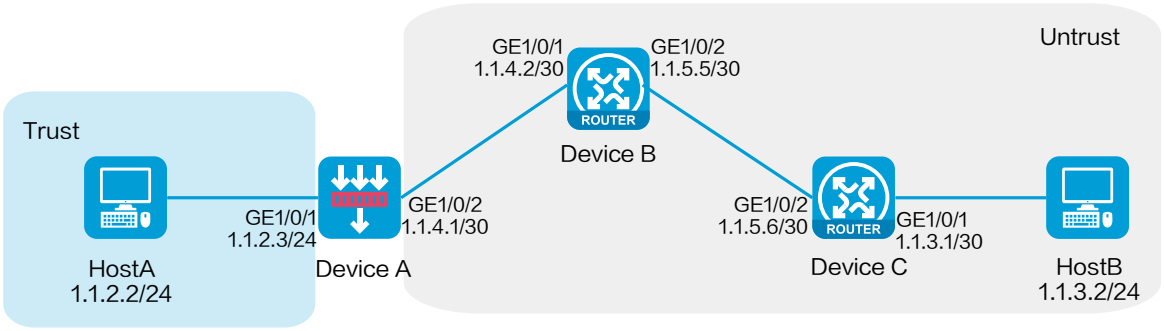
When you configure a static route, make sure the network of its next hop is reachable. In addition, make sure the next hop device has a minimum of one route to reach the local device.

Example: Configuring static routes

Network configuration

As shown in Figure 1, configure static routes on Device A, Device B, and Device C for interconnections between Host A and Host B.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/2.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 1.1.4.1/30.

c. Click **OK**.

Add GE 1/0/1 to the **Trust** security zone and set its IP address to 1.1.2.3/24 in the same way you configure GE 1/0/2.

2. Configure security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure security policy **test-a**:

- Enter security policy name **test-a**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Set the type to IPv4.
- Set the action to **Permit**.
- Set the source IPv4 address to 1.1.2.2/24.
- Set the destination IPv4 address to 1.1.3.2/24.

Click **OK**.

Click **Create** to create another security policy.

In the dialog box that opens, configure security policy **test-b**:

- Enter security policy name **test-b**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Set the type to IPv4.
- Set the action to **Permit**.

- Set the source IPv4 address to 1.1.3.2/24.
- Set the destination IPv4 address to 1.1.2.2/24.

Click **OK**.

3. Configure a static route:

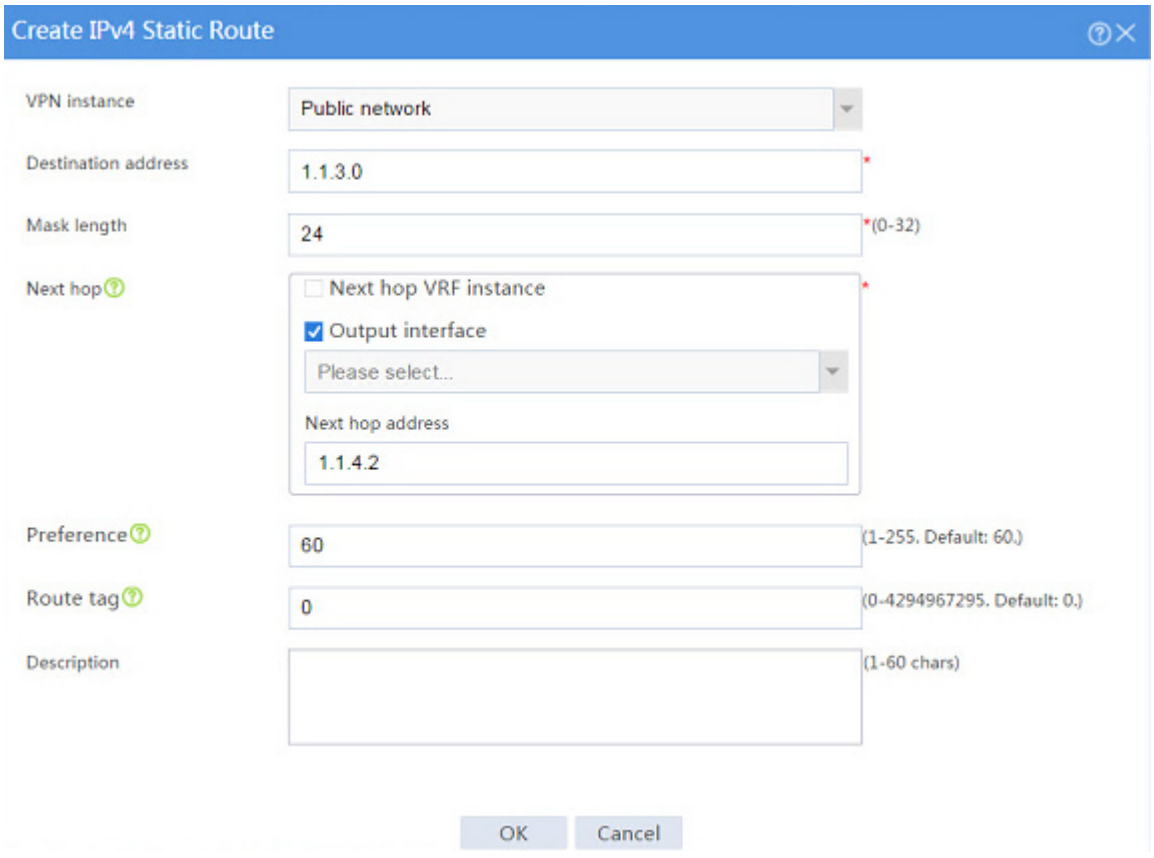
On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv4 static route, as shown in Figure 2.

Figure 2 Creating an IPv4 static route



Click **OK**.

Configuring Device B

Configure two static routes to reach networks 1.1.2.0/24 (Device A) and 1.1.3.0/24 (Device C), respectively. The configuration method is the same as that you configure the static route on Device A. (Details not shown.)

Configuring Device C

Configure two static routes to reach networks 1.1.2.0/24 (Device A) and 1.1.4.0/30 (Device B), respectively. The configuration method is the same as that you configure the static route on Device A. (Details not shown.)

Verifying the configuration

Verify that Host A can ping Host B.

```
C:\Users\abc>ping 1.1.3.2


Pinging 1.1.3.2 with 32 bytes of data:

Reply from 1.1.3.2: bytes=32 time=1ms TTL=255

Reply from 1.1.3.2: bytes=32 time=1ms TTL=255

Reply from 1.1.3.2: bytes=32 time=1ms TTL=255

Reply from 1.1.3.2: bytes=32 time=1ms TTL=255


Ping statistics for 1.1.3.2:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:

    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

The output shows that Host B can be pinged from Host A.

RIP configuration examples

Contents

Introduction

The following information provides RIP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the RIP feature.

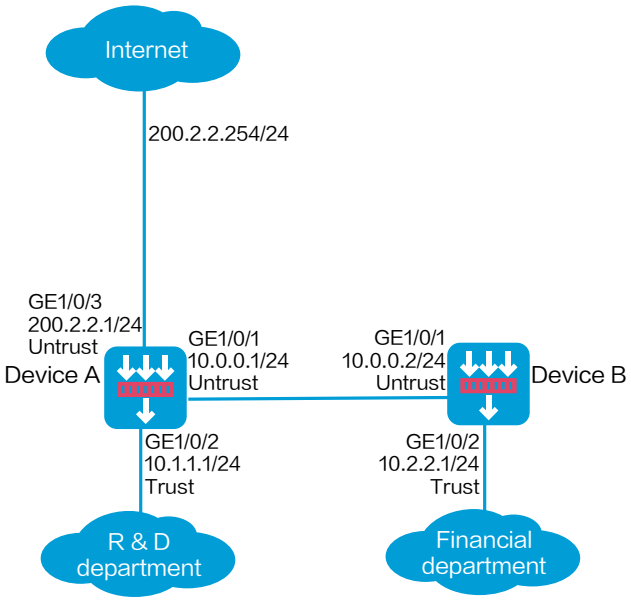
Example: Configuring RIP

Network configuration

As shown in Figure 1, an enterprise deploys Device A and Device B for the R&D and financial departments, respectively. Device A also acts as the gateway to the Internet.

Configure RIP for the departments to learn routes from each other. Configure a default route on Device A, with the next hop pointing to the gateway address 200.2.2.254, and redistribute the default route to RIP.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

RIP updates routing table information through multicast. You must configure a security policy to permit the traffic between the local security zone and the security zone that contains the RIP interface. For more information, see the configuration procedure.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.0.0.1/24.

c. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 10.1.1.1/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Untrust** security zone and set its IP address to 200.2.2.1/24 in the same way you configure GE 1/0/1.

2. Create security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure security policy **rip-a**:

a. Enter policy name **rip-a**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select type **IPv4**.

e. Select action **Permit**.

f. Enter source IPv4 address 10.1.1.0/24.

g. Click **OK**.

Configure security policy **rip-b**:

a. Enter policy name **rip-b**.

b. Select source zone **Local**.

c. Select destination zone **Untrust**.

d. Select type **IPv4**.

e. Select action **Permit**.

f. Click **OK**.

Configure security policy **rip-c**:

a. Enter policy name **rip-c**.

b. Select source zone **Untrust**.

c. Select destination zone **Local**.

d. Select type **IPv4**.

e. Select service object group **rip**.

f. Select action **Permit**.

g. Click **OK**.

Configure security policy **rip-d**:

a. Enter policy name **rip-d**.

b. Select source zone **Untrust**.

c. Select destination zone **Untrust**.

d. Select type **IPv4**.

e. Enter source IPv4 address 10.2.2.0/24.

f. Select action **Permit**.

g. Click **OK**.

3. Configure a default route to the ISP.

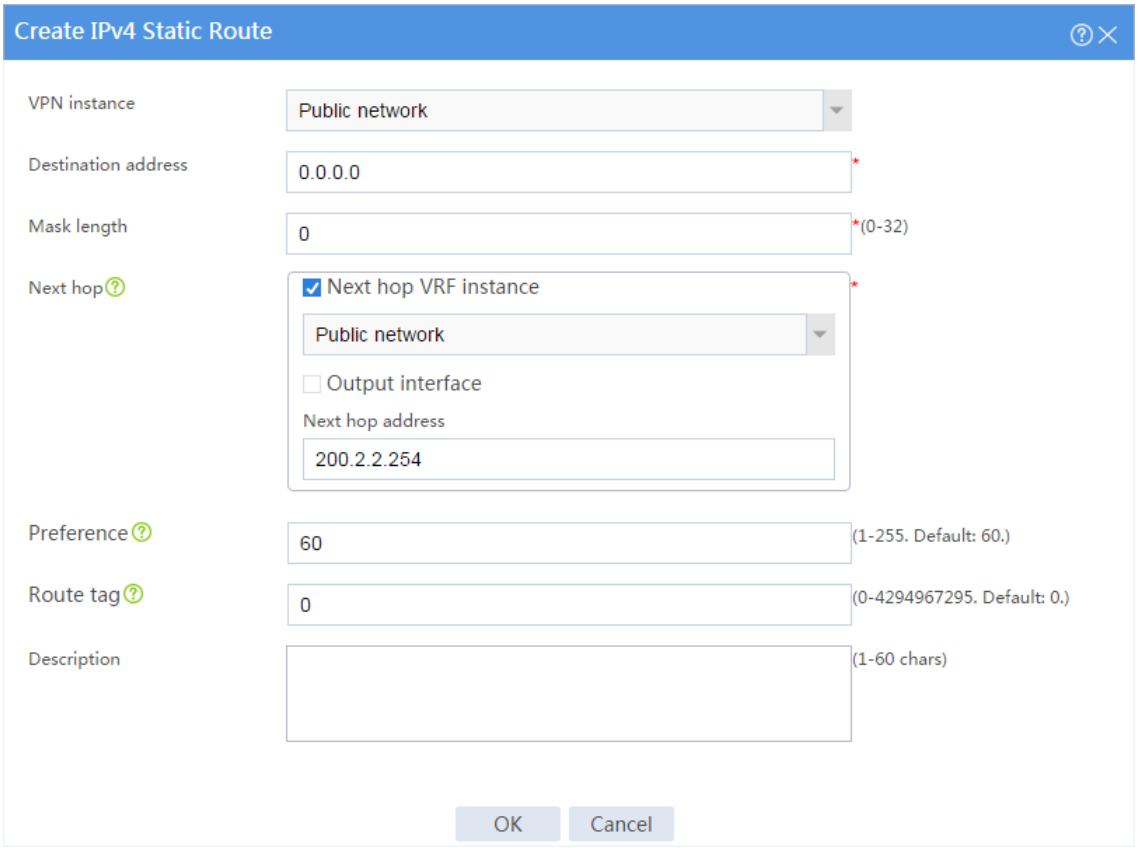
On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

Click **Create**.

In the dialog box that opens, configure a static route as shown in Figure 2.

Figure 2 Creating a static route



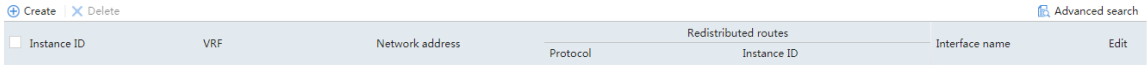
Click **OK**.

4. Configure RIP.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **RIP**. The RIP configuration page opens, as shown in Figure 3.

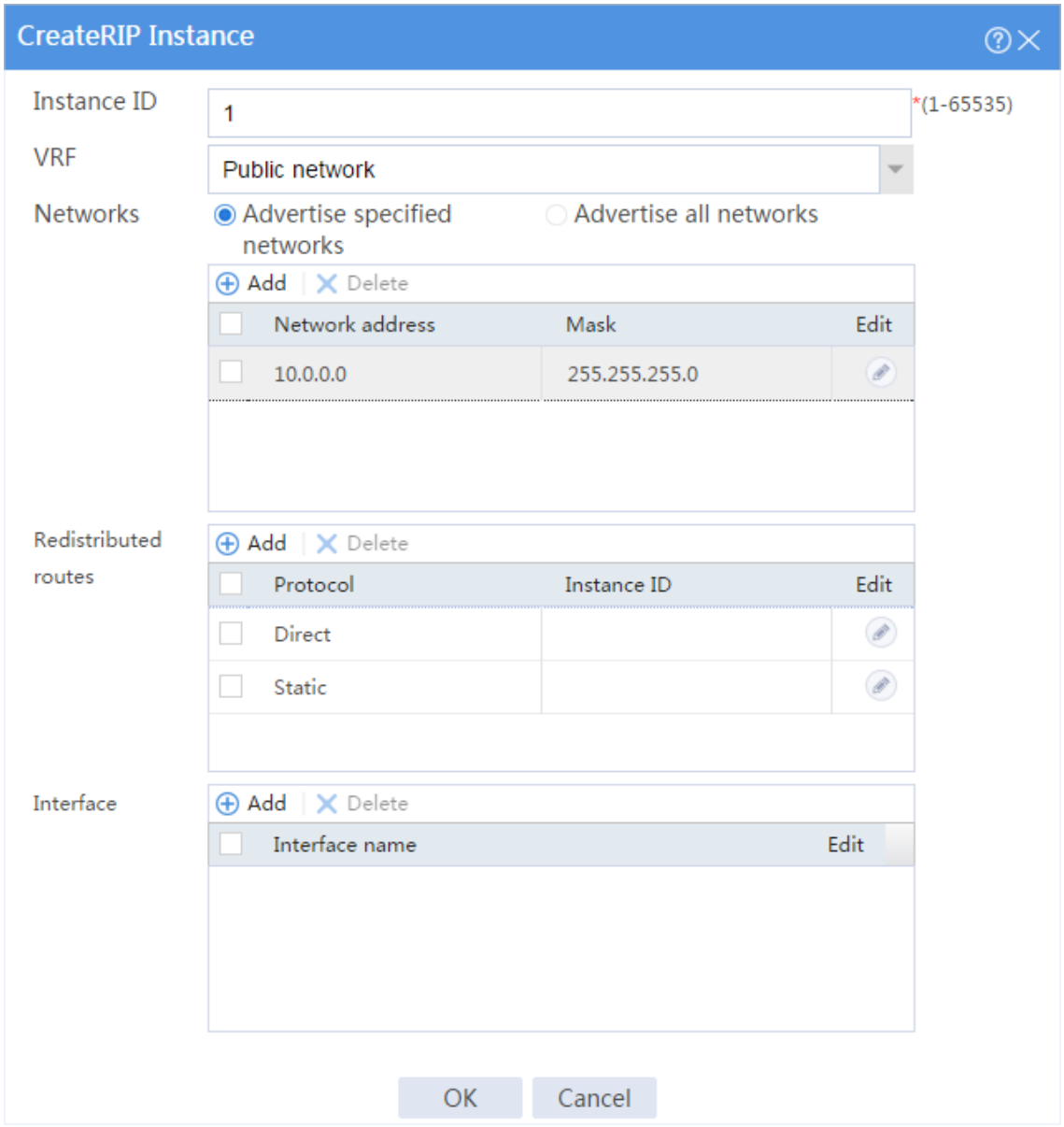
Figure 3 RIP configuration page



Click **Create**.

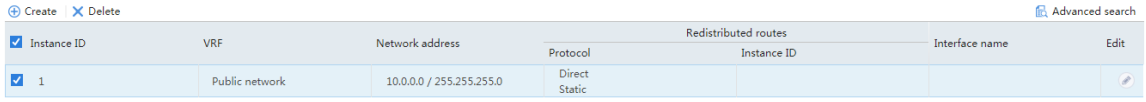
In the dialog box that opens, configure the RIP instance as shown in Figure 4. Add the configured static route and the direct network of the R&D department as redistributed routes.

Figure 4 Creating a RIP instance



Click **OK**. The RIP instance is created, as shown in Figure 5.

Figure 5 RIP instance



Configuring Device B

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.0.0.2/24.

c. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 10.2.2.1/24 in the same way you configure GE 1/0/1.

2. Create security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure security policy **rip-a**:

a. Enter policy name **rip-a**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select type **IPv4**.

e. Select action **Permit**.

f. Enter source IPv4 address 10.2.2.0/24.

g. Click **OK**.

Configure security policy **rip-b**:

a. Enter policy name **rip-b**.

b. Select source zone **Local**.

c. Select destination zone **Untrust**.

d. Select type **IPv4**.

e. Select service object group **rip**.

f. Select action **Permit**.

g. Click **OK**.

Configure security policy **rip-c**:

a. Enter policy name **rip-c**.

b. Select source zone **Untrust**.

c. Select destination zone **Local**.

d. Select type **IPv4**.

e. Select action **Permit**.

f. Select service object group **rip**.

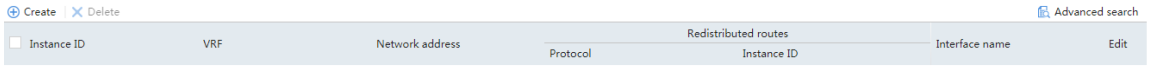
g. Click **OK**.

3. Configure RIP.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **RIP**. The RIP configuration page opens, as shown in Figure 6.

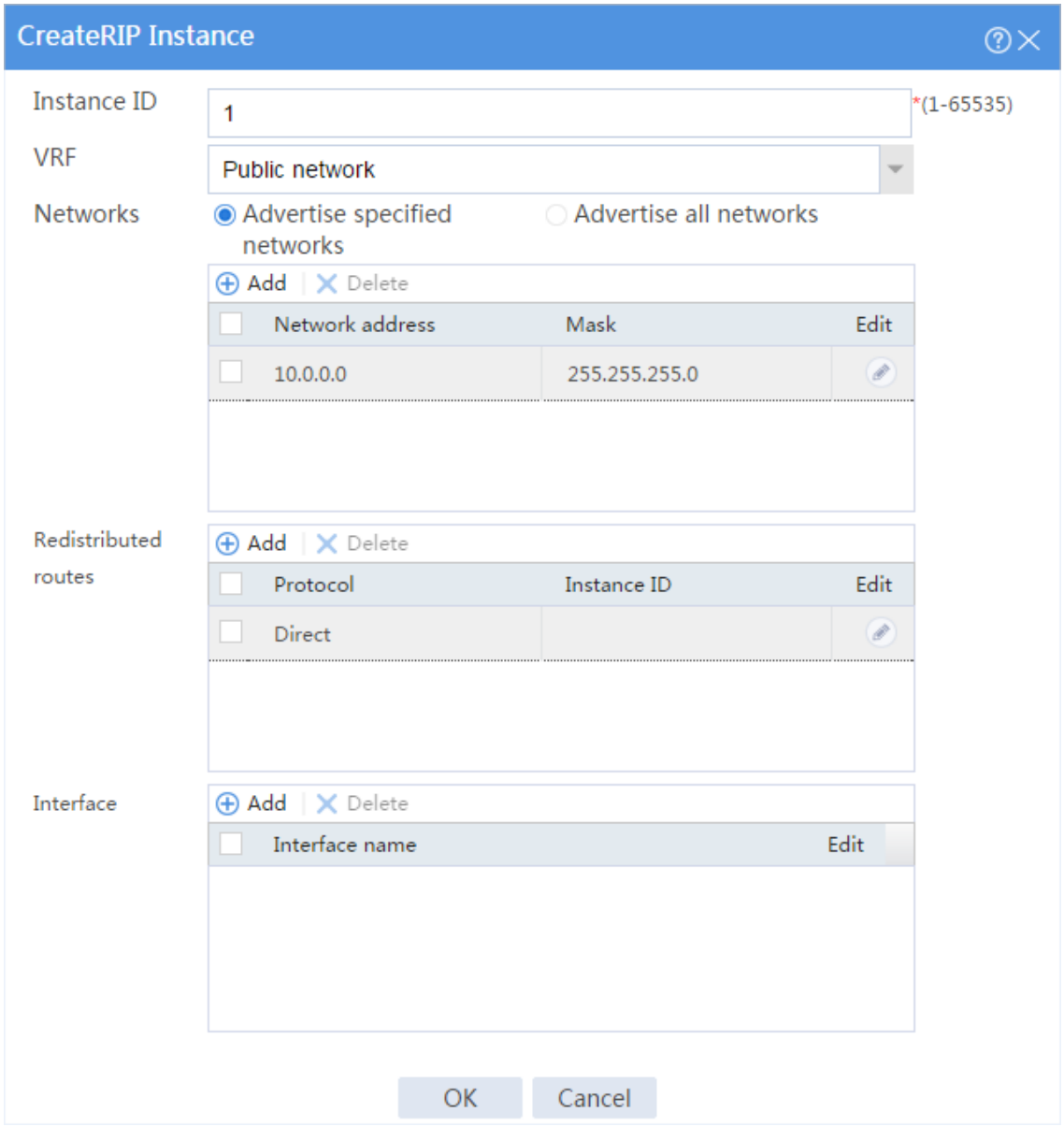
Figure 6 RIP configuration page



Click **Create**.

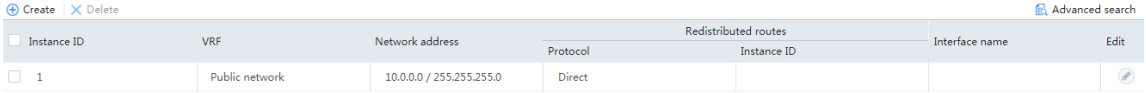
In the dialog box that opens, configure the RIP instance as shown in Figure 7. Add the direct network of the financial department as a redistributed route.

Figure 7 Creating a RIP instance



Click **OK**. The RIP instance is created, as shown in Figure 8.

Figure 8 RIP instance



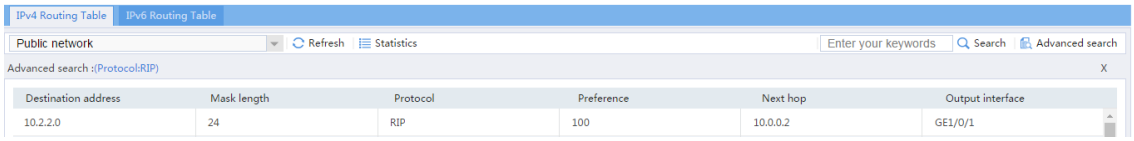
Verifying the configuration

1. Display the RIP routing table of Device A.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Routing Table**. The routing table is displayed, as shown in Figure 9.

   Figure 9 Displaying the RIP routing table of Device A

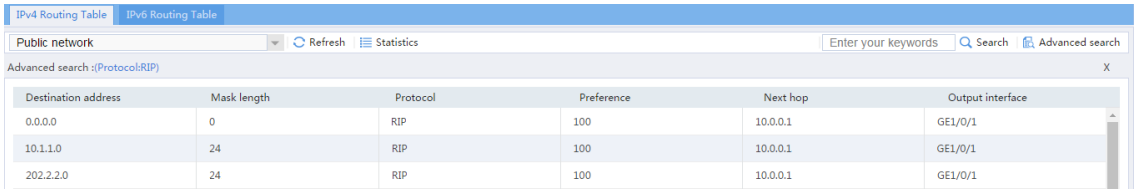


2. Display the RIP routing table of Device B.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Routing Table**. The routing table is displayed, as shown in Figure 10.

   Figure 10 Displaying the RIP routing table of Device B



3. Ping the gateway address 200.2.2.254 of the ISP on Device A.

   ```
   <Device A> ping -a 10.1.1.1 200.2.2.254
   ```

```
Ping 200.2.2.254 (200.2.2.254) from 10.1.1.1: 56 data bytes, press
CTRL_C to break

56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.423 ms

56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.222 ms

56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.173 ms

56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.170 ms

56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.167 ms


--- Ping statistics for 200.2.2.254 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 0.167/0.231/0.423/0.098 ms
```

The output shows that the gateway can be pinged.

4. Ping the gateway address 200.2.2.254 of the ISP on Device B.

```
<Device B> ping -a 10.0.0.2 200.2.2.254

Ping 200.2.2.254 (200.2.2.254) from 10.0.0.2: 56 data bytes, press
CTRL_C to break

56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.437 ms

56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.209 ms

56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.194 ms

56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.174 ms

56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.179 ms


--- Ping statistics for 200.2.2.254 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 0.174/0.239/0.437/0.100 ms
```

The output shows that the gateway can be pinged.

OSPF configuration examples

Contents

Introduction

The following information provides OSPF configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network

The following information is provided based on the assumption that you have basic knowledge of OSPF.

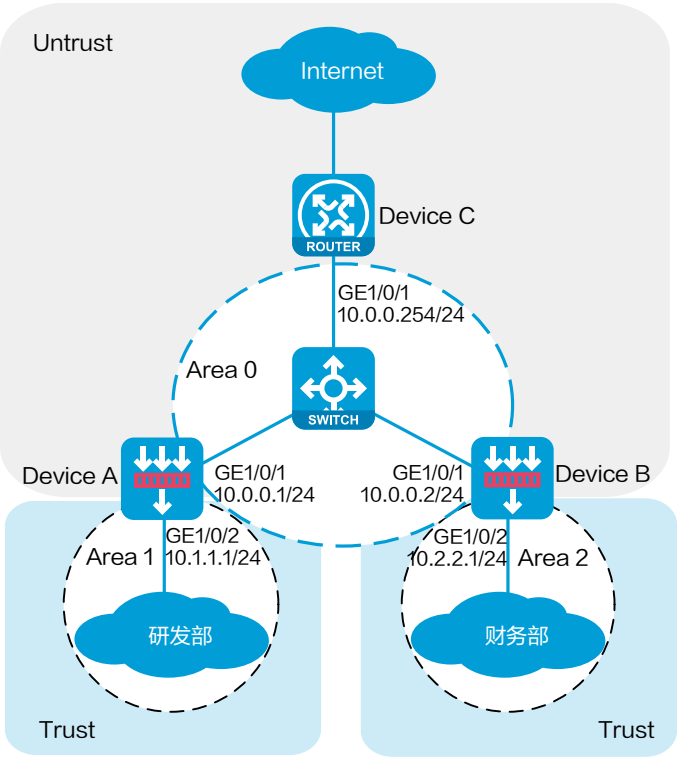
Example: Configuring OSPF

Network configuration

As shown in Figure 1, Device A and Device B are connected to R&D and finance departments, respectively. Device C is a router that acts as the gateway to the Internet.

Configure OSPF on the devices to enable the R&D and finance departments to learn routing information from each other. Configure a default route with the next hop being the gateway address 200.2.2.254 on Device C, and redistribute the default route to OSPF.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

OSPF uses multicast addresses 224.0.0.5 and 224.0.0.6 to establish neighbor relationships. You must configure a security policy to permit the traffic between the local security zone and the security zones that contain the OSPF interfaces. For more information, see the configuration procedure.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.0.0.1/24.

c. Retain the default configuration for the rest of parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 10.1.1.1/24 in the same way you configure GE 1/0/1.

2. Create security policies.

On the top navigation bar, click the **Policies** tab.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

Create security policy **ospf-a**:

- Enter policy name **ospf-a**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter 10.1.1.0/24 as the source address.
- Retain the default configuration for the rest of parameters.

Click **OK**.

Create security policy **ospf-b**:

- Enter policy name **ospf-b**.
- Select source zone **Local**.
- Select destination zone **Unrust**.
- Select type **IPv4**.
- Select service object group **ospf**.
- Select action **Permit**.
- Retain the default configuration for the rest of parameters.

Click **OK**.

Create security policy **ospf-c**:

- Enter policy name **ospf-c**.
- Select source zone **Unrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select service object group **ospf**.
- Select action **Permit**.

- Retain the default configuration for the rest of parameters.

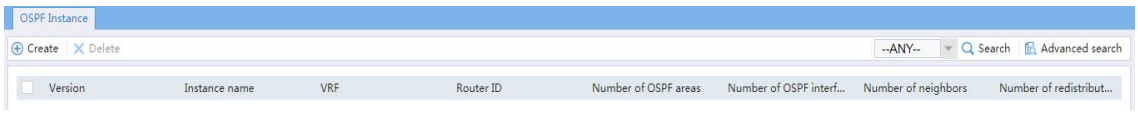
Click **OK**.

3. Configure OSPF.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

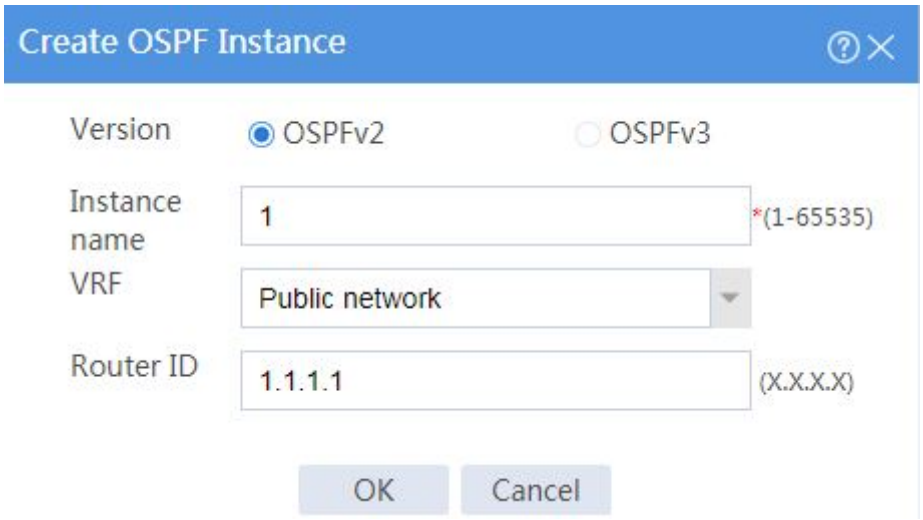
Figure 2 Configuring OSPF



Click **Create**.

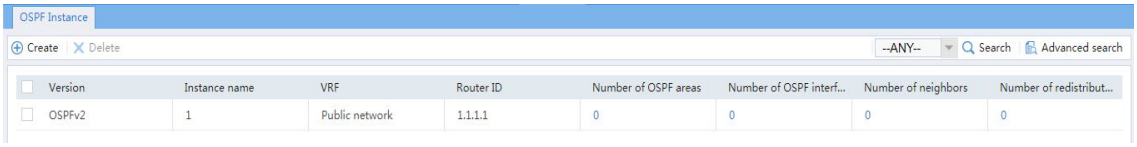
In the dialog box that opens, configure an OSPF instance.

Figure 3 Creating an OSPF instance



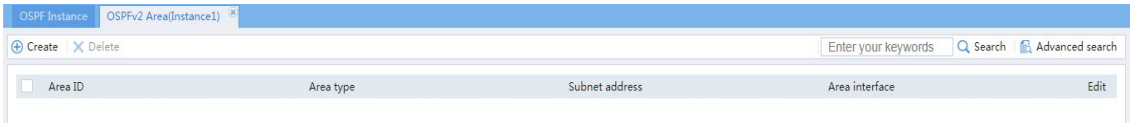
Click **OK**.

Figure 4 OSPF instance



Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

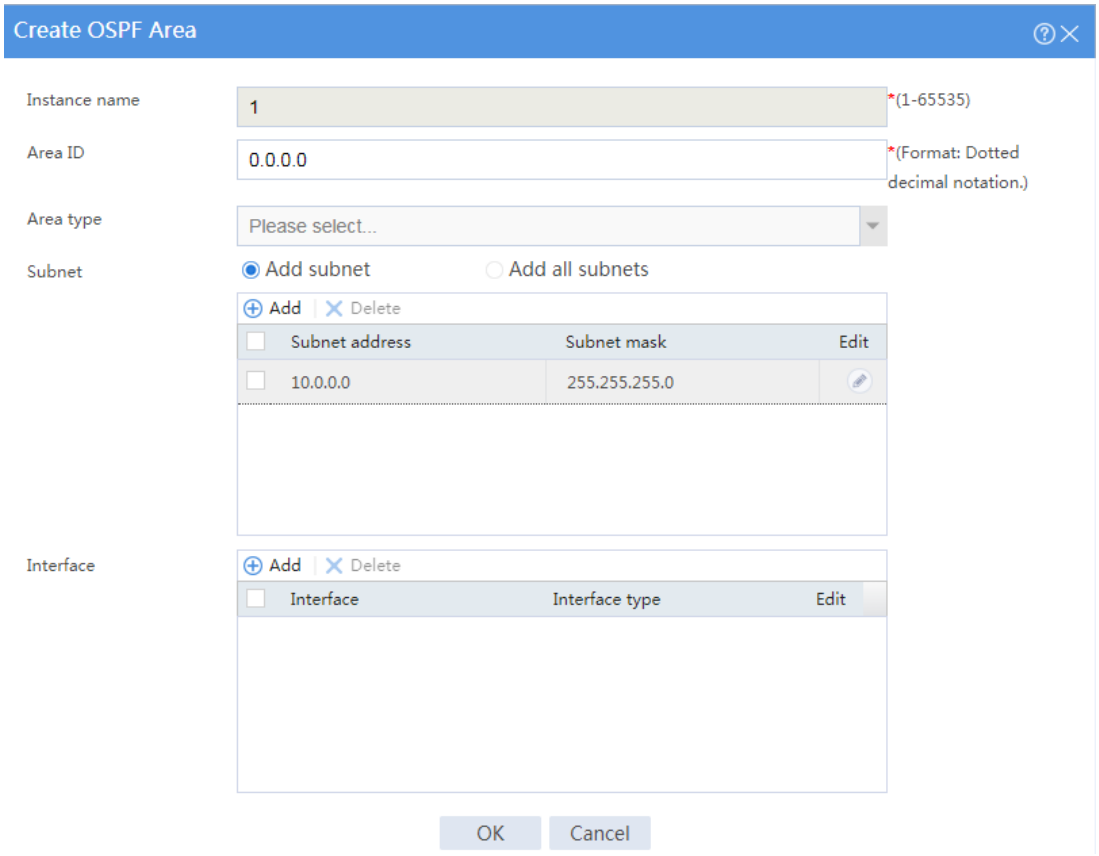
Figure 5 OSPF areas



On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure Area 0.

Figure 6 Creating Area 0

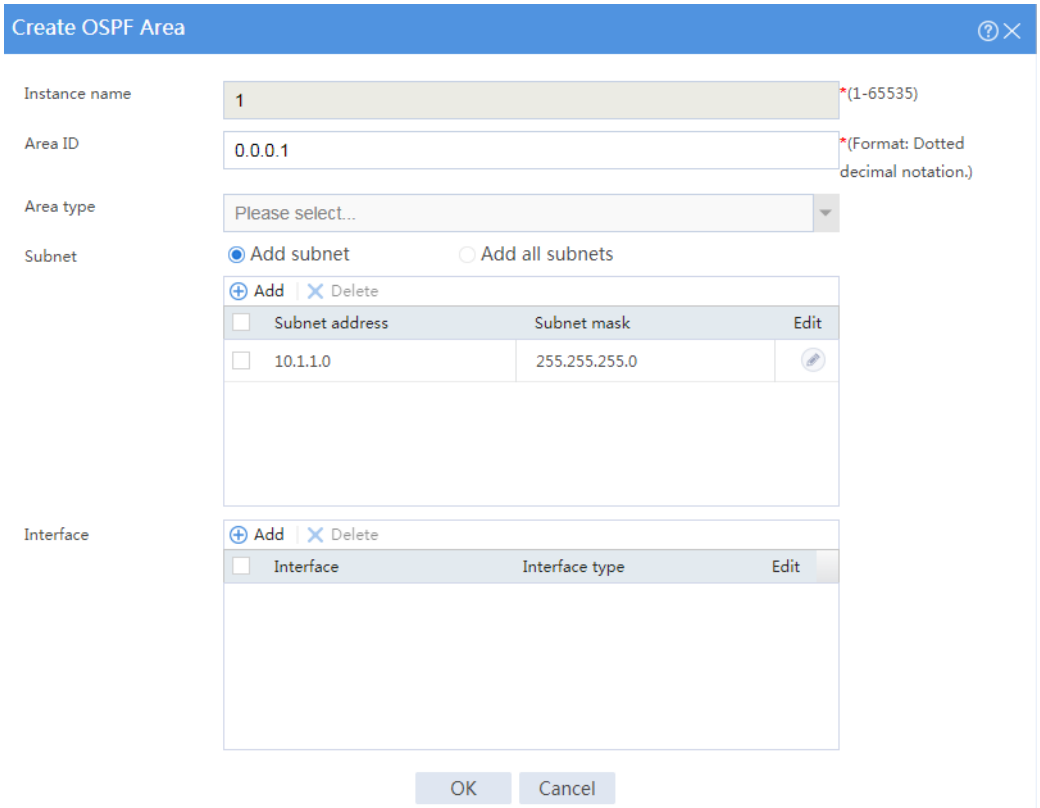


Click **OK**.

On the OSPF area configuration page, click **Create**.

In the dialog box that opens, configure Area 1.

Figure 7 Creating Area 1



Configuring Device B

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.0.0.2/24.

c. Retain the default configuration for the rest of parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 10.2.2.1/24 in the same way you configure GE 1/0/1.

2. Create security policies.

   # On the top navigation bar, click the **Policies** tab.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Select **Create** > **Create a policy**.

   # Create security policy **ospf-a**:

   - Enter policy name **ospf-a**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select action **Permit**.
   - Select type **IPv4**.
   - Enter 10.2.2.0/24 as the source address.
   - Retain the default configuration for the rest of parameters.

   # Click **OK**.

   # Create security policy **ospf-b**:

   - Enter policy name **ospf-b**.
   - Select source zone **Local**.
   - Select destination zone **Untrust**.
   - Select type **IPv4**.
   - Select action **Permit**.
   - Select service object group **ospf**.
   - Retain the default configuration for the rest of parameters.

   # Click **OK**.

   # Create security policy **ospf-c**:

   - Enter policy name **ospf-b**.
   - Select source zone **Untrust**.
   - Select destination zone **Local**.
   - Select type **IPv4**.
   - Select action **Permit**.

- Select service object group **ospf**.
- Retain the default configuration for the rest of parameters.

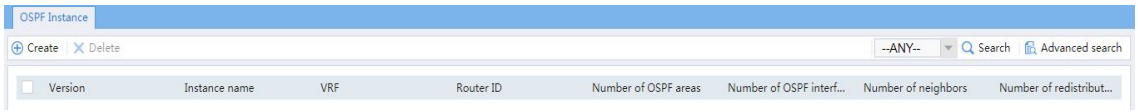
Click **OK**.

3. Configure OSPF.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

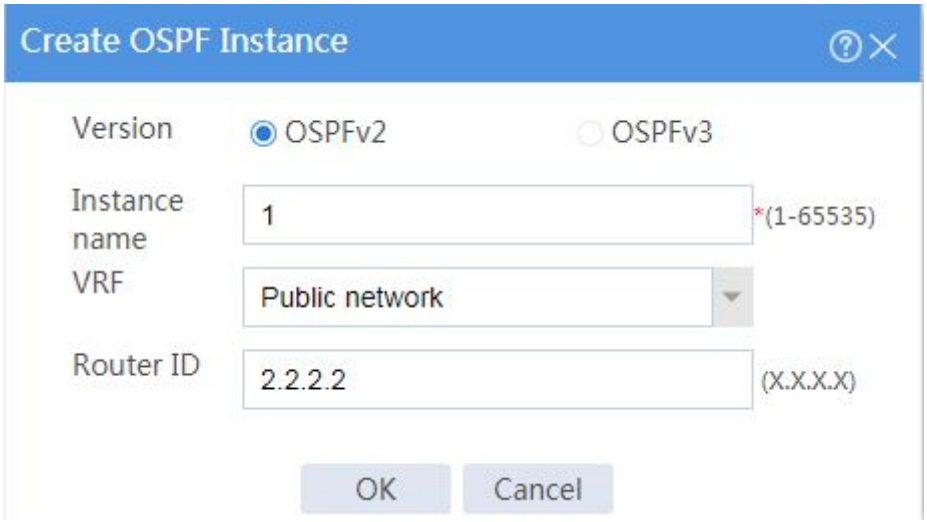
Figure 8 Configuring OSPF



Click **Create**.

In the dialog box that opens, configure an OSPF instance.

Figure 9 Creating an OSPF instance

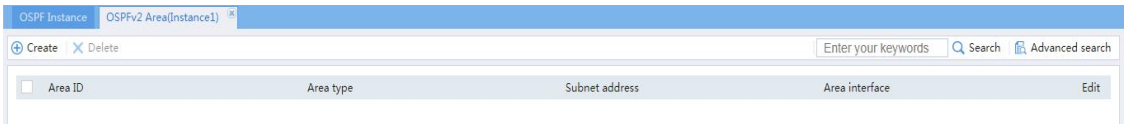


Click **OK**.

Figure 10 OSPF instance

Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

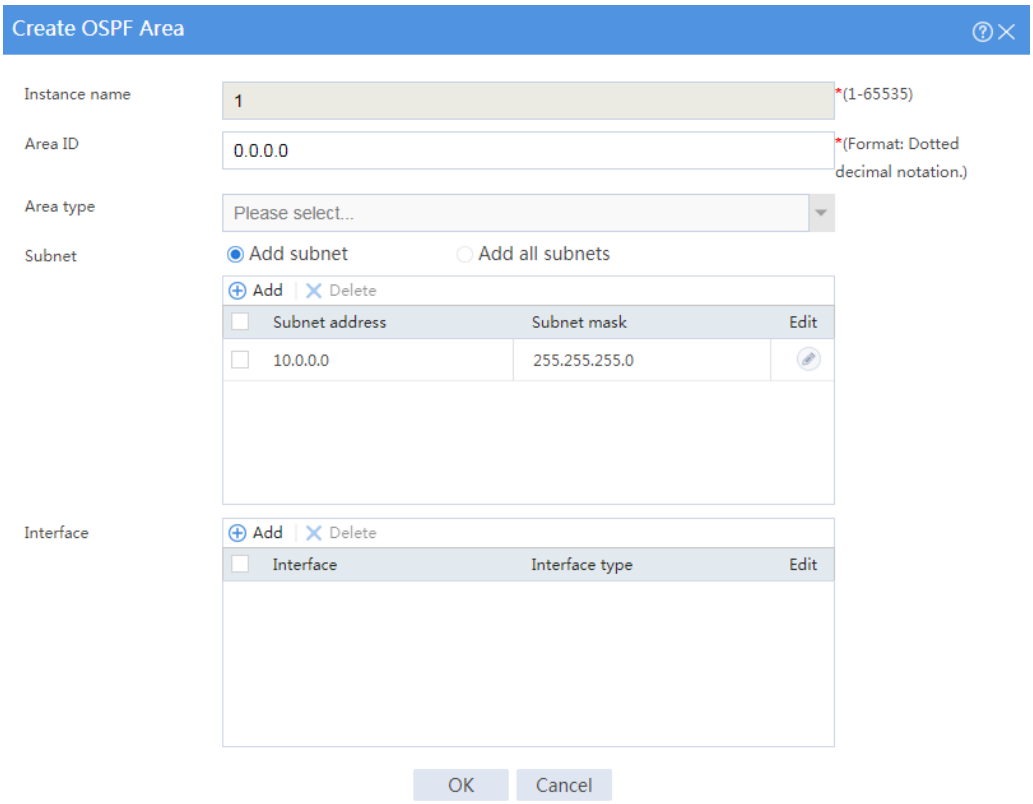
Figure 11 OSPF areas



On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure Area 0.

Figure 12 Creating Area 0

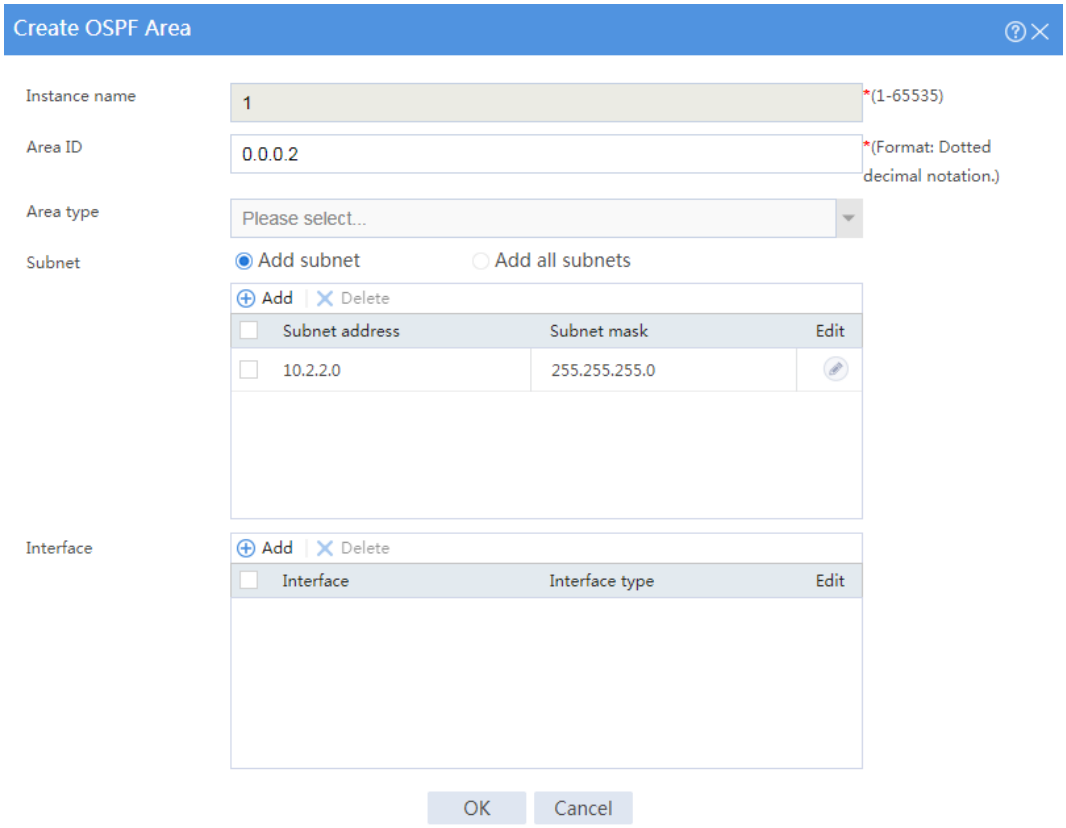


Click **OK**.

On the OSPF area configuration page, click **Create**.

In the dialog box that opens, configure Area 2.

Figure 13 Creating Area 2



Click **OK**.

Configuring Device C

1. Assign IP addresses to interfaces. (Details not shown.)
2. Configure OSPF.

   # Enable OSPF process 1, and specify the router ID as 3.3.3.3.

   ```
   <Device C> system-view
   [Device C] ospf 1 router-id 3.3.3.3
   ```

   # Create Area 0 and enter Area 0 view.

```
[Device C-ospf-1] area 0.0.0.0
```

Advertise network 10.0.0.0/24.

```
[Device C-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
[Device C-ospf-1-area-0.0.0.0] quit
```

Redistribute the default route into the OSPF routing table.

```
<Sysname> system-view
[Device C-ospf-1] default-route-advertise always
[Device C-ospf-1] quit
```

Configure the default route to the ISP.

```
[Device C] ip route-static 0.0.0.0 0 200.2.2.254
```

Verifying the configuration

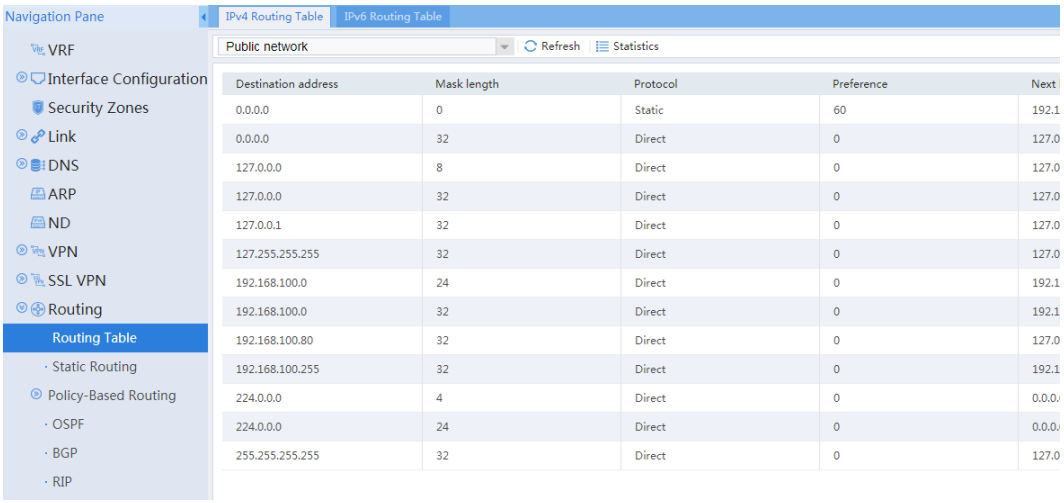
1. View information about the OSPF routing table of Device A.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Routing Table**.

   # On the **IPv4 Routing Table** tab, view the OSPF routing table information.

Figure 14 OSPF routing table of Device A



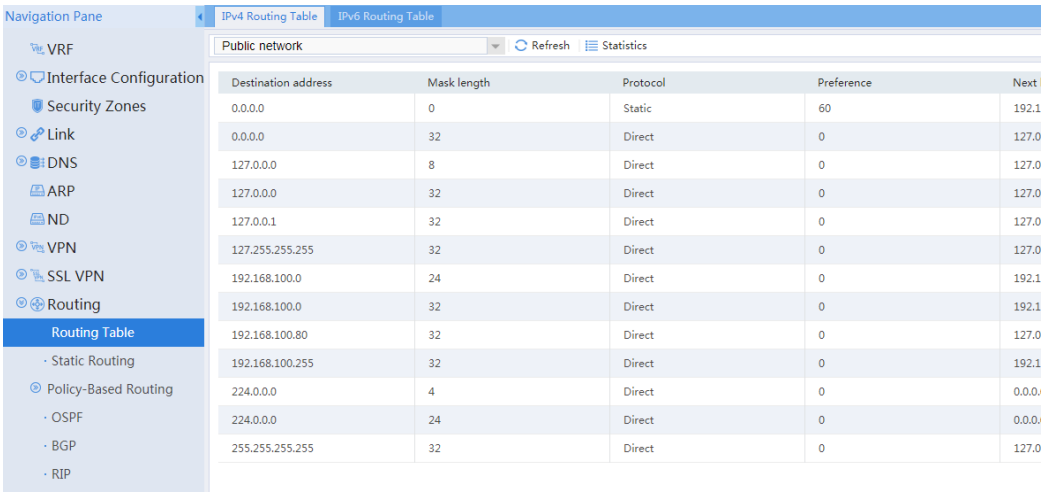
2. View information about the OSPF routing table of Device B.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Routing Table**.

   # On the **IPv4 Routing Table** tab, view the OSPF routing table information.

Figure 15 OSPF routing table of Device B



3. Verify that Device A can ping the ISP.

```
<Device A> ping -a 10.1.1.1 200.2.2.254

Ping 200.2.2.254 (200.2.2.254) from 10.1.1.1: 56 data bytes, press
CTRL_C to break

56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.423 ms

56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.222 ms

56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.173 ms

56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.170 ms

56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.167 ms


--- Ping statistics for 200.2.2.254 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 0.167/0.231/0.423/0.098 ms
```

The output shows that the ISP can be pinged.

4. Verify that Device B can ping the ISP.

```
<Device B> ping -a 10.0.0.2 200.2.2.254
Ping 200.2.2.254 (200.2.2.254) from 10.0.0.2: 56 data bytes, press
CTRL_C to break
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.437 ms
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.209 ms
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.194 ms
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.174 ms
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.179 ms

--- Ping statistics for 200.2.2.254 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.174/0.239/0.437/0.100 ms
```

The output shows that the ISP can be pinged.

BGP configuration examples

Contents

Introduction

The following information provides BGP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of BGP.

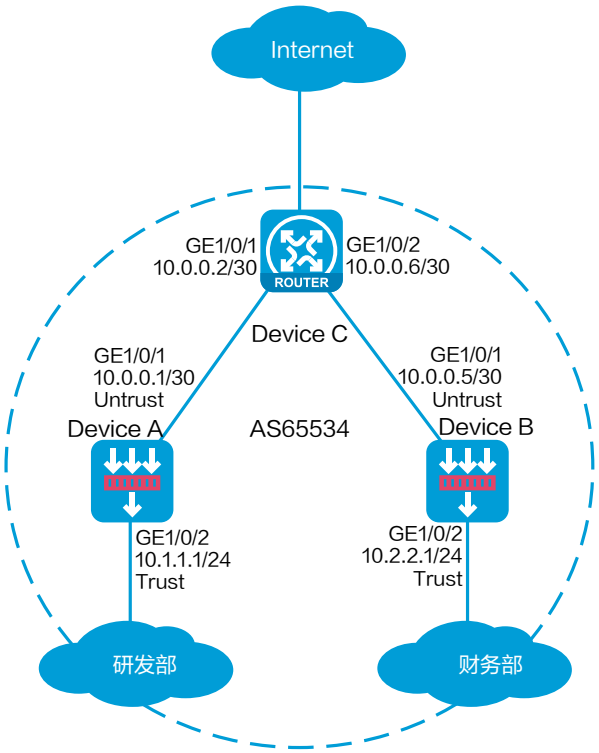
Example: Configuring BGP

Network configuration

As shown in Figure 1, Device A and Device B are connected to R&D and finance departments, respectively. Device C is a router that acts as the gateway to the Internet.

Configure BGP on the devices to enable the R&D and finance departments to learn routing information from each other. Configure a default route with the next hop being gateway address 200.2.2.254 on Device C, and redistribute the default route to BGP.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

BGP uses TCP (port number 179) to establish peer relationships. You must configure a security policy to permit the traffic between the local security zone and the security zones that contain the BGP interfaces. For more information, see the configuration procedure.

By default, BGP does not redistribute default IGP routes. To redistribute default IGP routes into the BGP routing table, you must use the **`default-route imported`** command together with the **`import-route`** command.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.0.0.1/30.

c. Retain the default configuration for the rest of parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 10.1.1.1/24 in the same way you configure GE 1/0/1.

2. Create security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

Create security policy **bgp-a**:

- Enter policy name **bgp-a**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter 10.1.1.0/24 as the source address.
- Retain the default configuration for the rest of parameters.

Click **OK**.

Create security policy **bgp-b**:

- Enter policy name **bgp-b**.
- Select source zone **Local**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select service object group **bgp**.
- Select action **Permit**.
- Retain the default configuration for the rest of parameters.

Click **OK**.

Create security policy **bgp-c**:

- Enter policy name **bgp-c**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.

- Select service object group **bgp**.
- Select action **Permit**.
- Retain the default configuration for the rest of parameters.

Click **OK**.

3. Configure an underlying routing protocol. In this example, configure RIP.

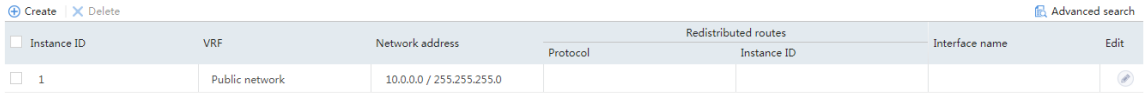
On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **RIP**.

Click **Create**.

In the dialog box that opens, configure a RIP instance.

Figure 2 RIP instance



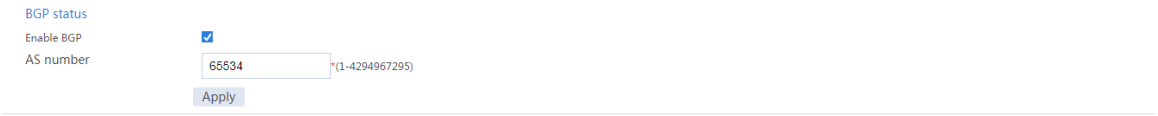
4. Configure BGP.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **BGP**.

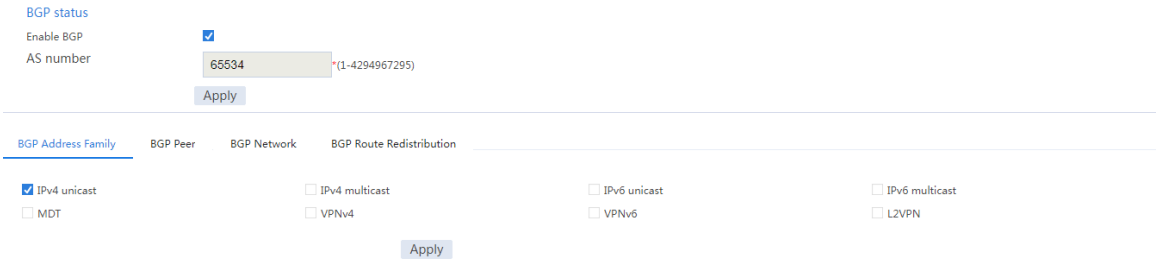
Select **Enable BGP**, enter AS number **65534**, and then click **Apply**.

Figure 3 Configuring BGP



On the **BGP Address Family** tab, select an address family, and then click **Apply**.

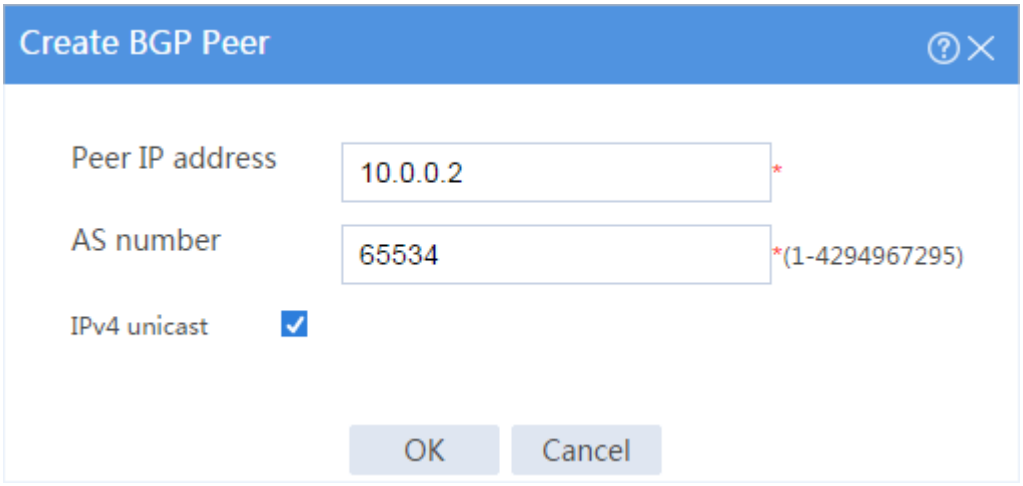
Figure 4 Selecting a BGP address family



On the **BGP Peer** tab, click **Create**.

In the dialog box that opens, specify a BGP peer, and then click **OK**.

Figure 5 Specifying a BGP peer



Repeat the above two steps to specify another BGP peer.

Figure 6 Specifying another BGP peer

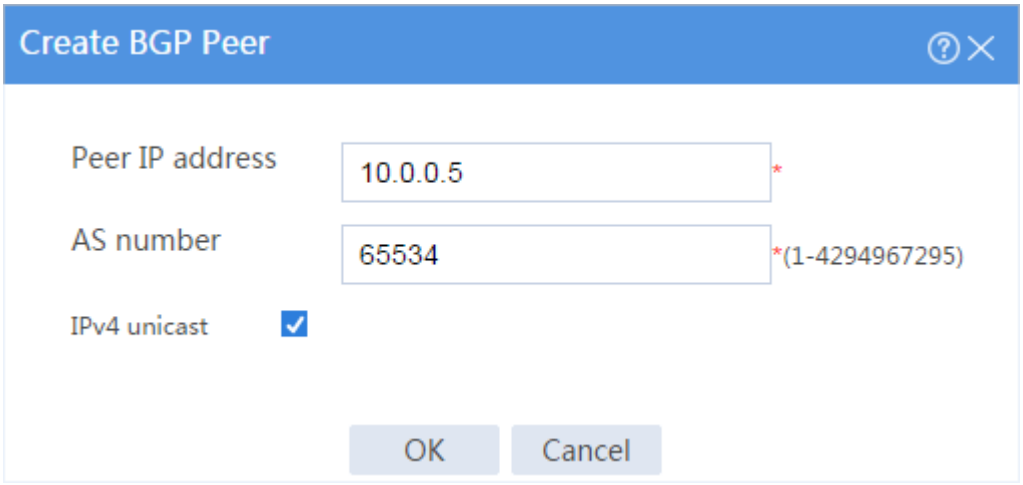
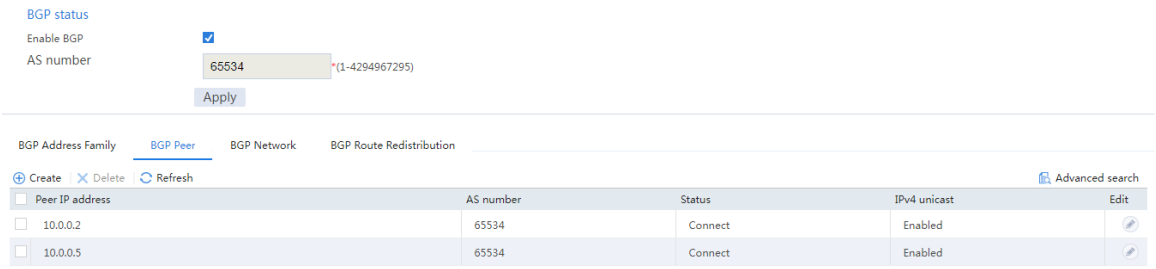


Figure 7 BGP peers



On the **BGP Network** tab, click **Create**.

In the dialog box that opens, specify the network to be advertised for the specified address family, and then click **OK**.

Figure 8 BGP network advertisement

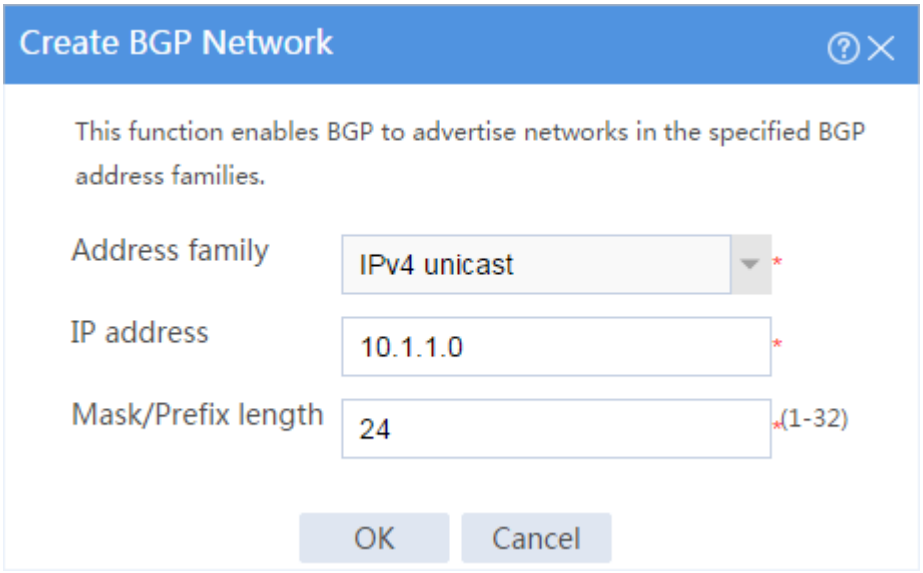
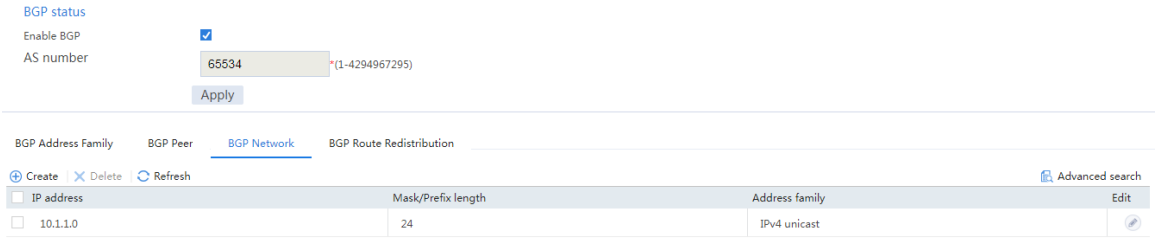


Figure 9 BGP network advertisement



Configuring Device B

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.0.0.5/30.

c. Retain the default configuration for the rest of parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 10.2.2.1/24 in the same way you configure GE 1/0/1.

2. Create security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

Create security policy **bgp-a**:

- Enter policy name **bgp-a**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter 10.2.2.0/24 as the source address.
- Retain the default configuration for the rest of parameters.

Click **OK**.

Create security policy **bgp-b**:

- Enter policy name **bgp-a**.
- Select source zone **Local**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select service object group **bgp**.
- Select action **Permit**.
- Retain the default configuration for the rest of parameters.

Click **OK**.

Create security policy **bgp-c**:

- Enter policy name **bgp-c**.
- Select source zone **Untrust**.

- Select destination zone **Local**.
- Select type **IPv4**.
- Select service object group **bgp**.
- Select action **Permit**.
- Retain the default configuration for the rest of parameters.

Click **OK**.

3. Configure an underlying routing protocol. In this example, configure RIP.

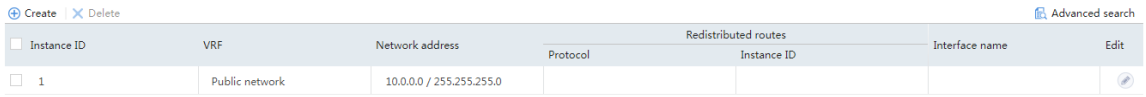
On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **RIP**.

Click **Create**.

In the dialog box that opens, configure a RIP instance.

Figure 10 RIP instance



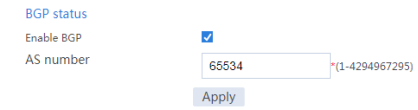
4. Configure BGP.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **BGP**.

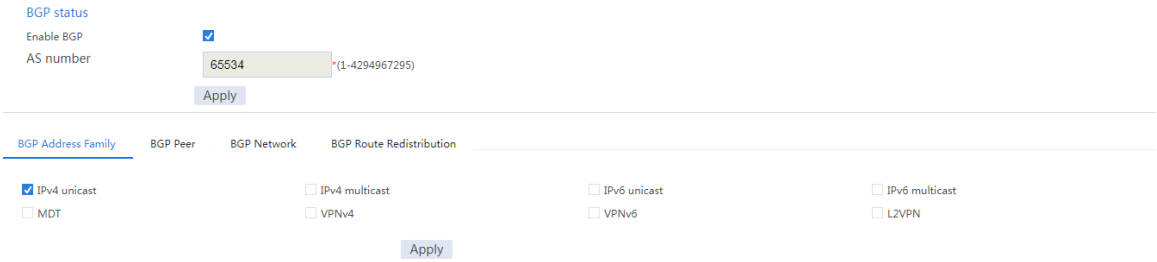
Select **Enable BGP**, enter AS number **65534**, and then click **Apply**.

Figure 11 Configuring BGP



On the **BGP Address Family** tab, select an address family, and then click **Apply**.

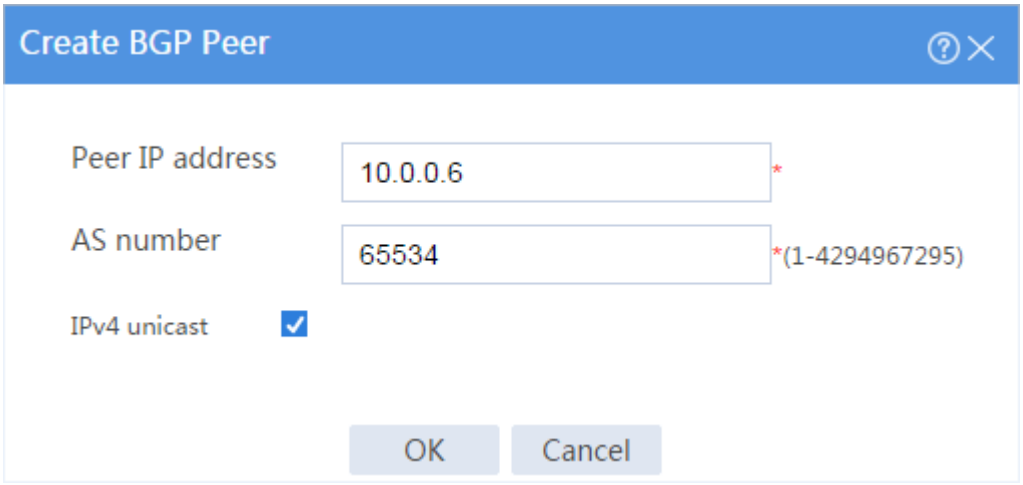
Figure 12 Selecting a BGP address family



On the **BGP Peer** tab, click **Create**.

In the dialog box that opens, specify a BGP peer, and then click **OK**.

Figure 13 Specifying a BGP peer



Repeat the above two steps to specify another BGP peer.

Figure 14 Specifying another BGP peer

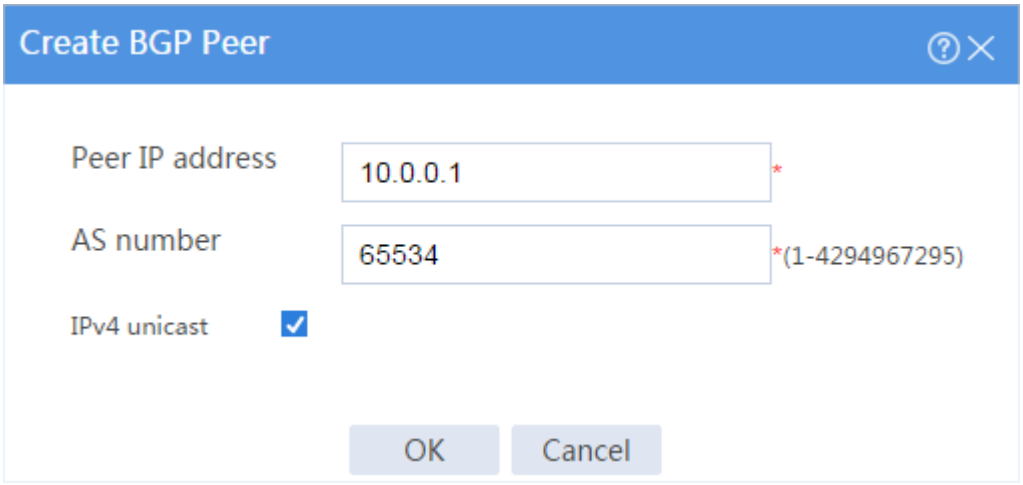
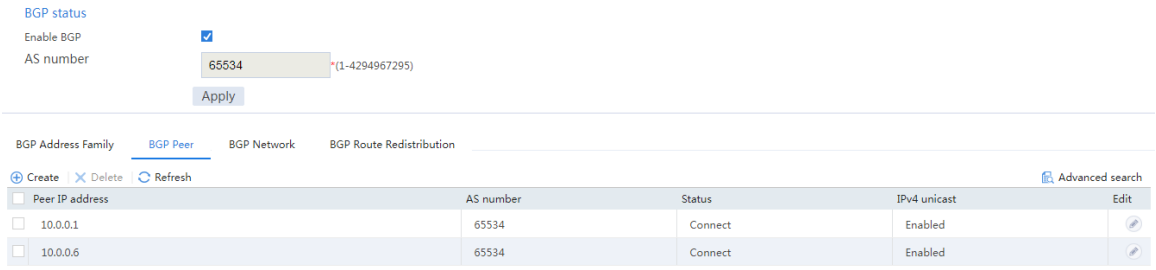


Figure 15 BGP peers



On the **BGP Network** tab, click **Create**.

In the dialog box that opens, specify the network to be advertised for the specified address family, and then click **OK**.

Figure 16 BGP network advertisement

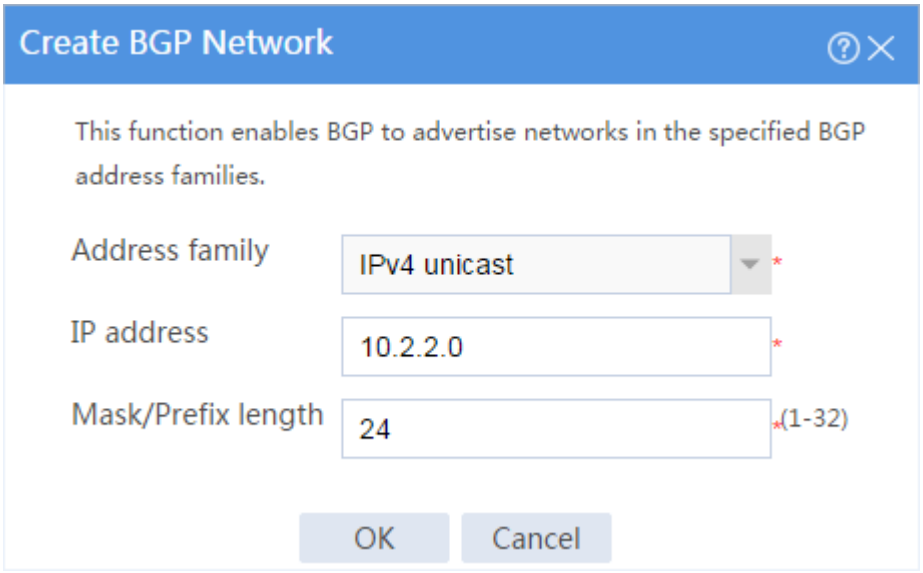
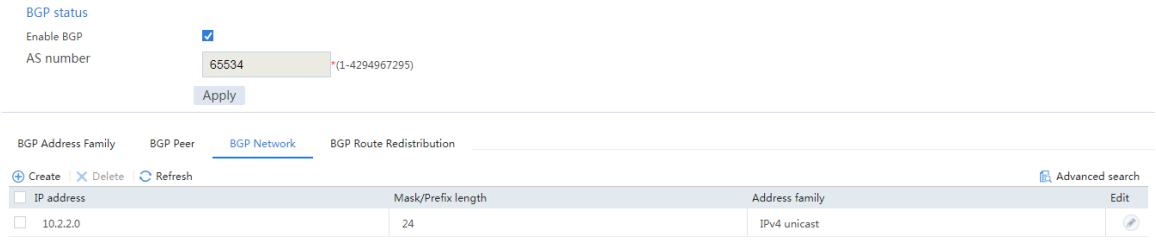


Figure 17 BGP network advertisement



Configuring Device C

1. Assign IP addresses to interfaces. (Details not shown.)
2. Configure an underlying routing protocol. In this example, configure RIP.

```
<Device C> system-view
[Device C]rip
[Device C-rip-1]network 10.0.0.0 0.0.0.255
```

3. Configure BGP.

   # Enable BGP.

```
<Device C> system-view
```

```
[Device C] bgp 65534
```

Specify BGP peers.

```
[Device C-bgp-default]peer 10.0.0.1 as 65534
[Device C-bgp-default]peer 10.0.0.5 as 65534
```

Enable BGP peers.

```
[Device C-bgp-default]address-family ipv4 unicast
[Device C-bgp-default-ipv4]peer 10.0.0.1 enable
[Device C-bgp-default-ipv4]peer 10.0.0.5 enable
[Device C-bgp-default-ipv4]quit
[Device C-bgp-default]quit
```

Configure the default route to the ISP.

```
[Device C] ip route-static 0.0.0.0 0 200.2.2.254
```

Redistribute the default route to the BGP routing table.

```
[Device C]bgp 65534
[Device C-bgp-default]address-family ipv4 unicast
[Device C-bgp-default-ipv4]import-route static
[Device C-bgp-default-ipv4]default-route imported
```

Verifying the configuration

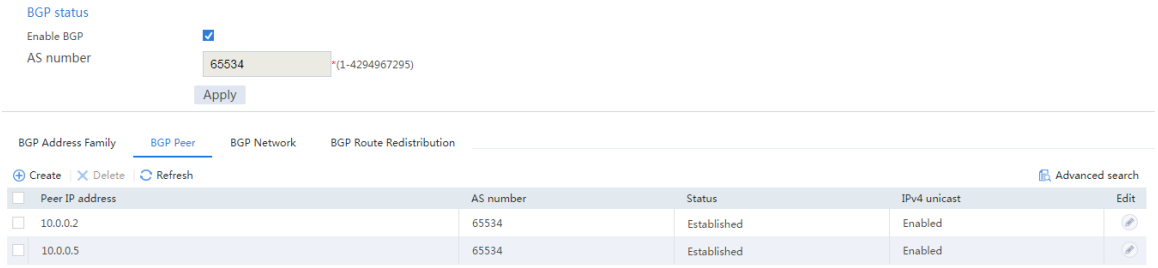
1. View information about BGP peers of Device A.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **BGP**.

   # On the **BGP Peer** tab, verify that the BGP peers are in **Established** state.

Figure 18 BGP routing table of Device A



You can see that the BGP peers are in **Established** state.

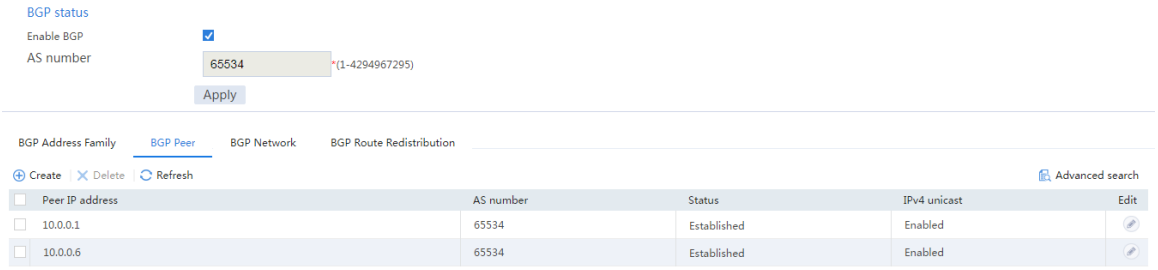
2. View information about BGP peers of Device B.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **BGP**.

   # On the **BGP Peer** tab, verify that the BGP peers are in **Established** state.

Figure 19 BGP routing table of Device B



You can see that the BGP peers are in **Established** state.

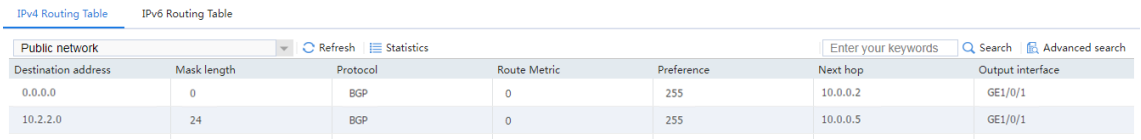
3. View information about the BGP routing table of Device A.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Routing Table**.

   # On the **IPv4 Routing Table** tab, view the BGP routing table information.

Figure 20 BGP routing table of Device A



You can see the redistributed BGP route and default route.

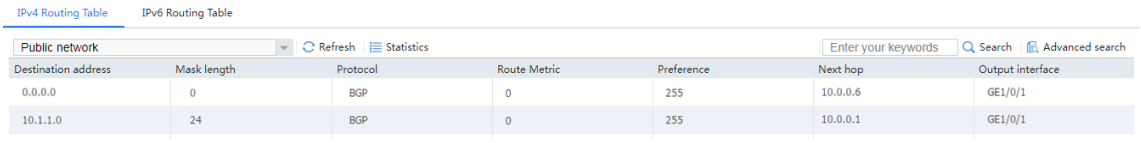
4. View information about the BGP routing table of Device B.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Routing Table**.

   # On the **IPv4 Routing Table** tab, view the BGP routing table information.

Figure 21 BGP routing table of Device B



You can see the redistributed BGP route and default route.

5. Verify that Device A can ping the ISP.

```
<Device A> ping -a 10.1.1.1 200.2.2.254
Ping 200.2.2.254 (200.2.2.254) from 10.1.1.1: 56 data bytes, press
CTRL_C to break
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.423 ms
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.222 ms
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.173 ms
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.170 ms
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.167 ms

--- Ping statistics for 200.2.2.254 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.167/0.231/0.423/0.098 ms
```

The output shows that the ISP can be pinged.

6. Verify that Device B can ping the ISP.

```
<Device B> ping -a 10.0.0.5 200.2.2.254
Ping 200.2.2.254 (200.2.2.254) from 10.0.0.5: 56 data bytes, press
CTRL_C to break
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.437 ms
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.209 ms
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.194 ms
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.174 ms
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.179 ms

--- Ping statistics for 200.2.2.254 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.174/0.239/0.437/0.100 ms
```

The output shows that the ISP can be pinged.

Policy-based routing configuration examples

Contents

Introduction

This document provides policy-based routing configuration examples.

Policy-based routing (PBR) uses user-defined policies to route packets. A policy can specify parameters for packets that match specific criteria such as ACLs. The parameters include the next hop and output interface. PBR has higher forwarding priority than static routing and dynamic routing (for example, BGP) that forward packets according to routing table lookup.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of PBR.

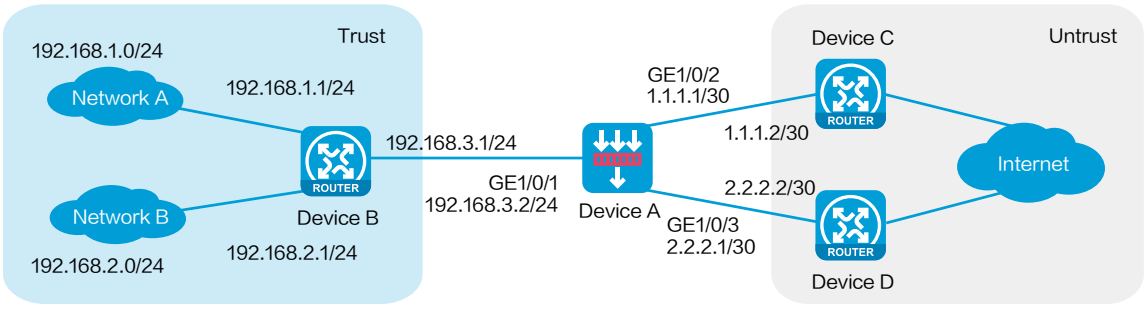
Example: Configuring policy-based routing

Network configuration

As shown in Figure 1, an enterprise deploys a security gateway Device A that is connected to internal networks A (192.168.1.0/24) and B (192.168.2.0/24) and ISP links A and B. ISP link A is connected to access device C with access point IP address 1.1.1.2/30. ISP link B is connected to access device D with access point IP address 2.2.2.2/30. Configure PBR to meet the following requirements:

- Users in network A access the external network through ISP link A, and users in network B access the external network through ISP link B.
- When one of the ISP links fails, user traffic from the internal network can be forwarded through the other ISP link.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the IP address and security zone settings:

   a. Select the **Trust** security zone.

   b. Enter the IP address and mask of the interface. In this example, enter 192.168.3.2/24.

   c. Use default settings for other parameters.

Configure the IP address and security zone settings for GE 1/0/2:

a. Select the **Untrust** security zone.

b. Enter the IP address and mask of the interface. In this example, enter 1.1.1.1/30.

c. Use default settings for other parameters.

Configure the IP address and security zone settings for GE 1/0/3:

a. Select the **Untrust** security zone.

b. Enter the IP address and mask of the interface. In this example, enter 2.2.2.1/30.

c. Use default settings for other parameters.

Click **OK**.

2. Configure static routes:

You can configure a dynamic routing protocol based on network requirements. This example uses static routes as an example.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure the following parameters for the static route to access network A:

a. Enter the destination IP address 192.168.1.0.

b. Specify the mask length as 24.

c. Specify the next hop IP address as 192.168.3.1.

d. Use default settings for other parameters.

Click **OK**.

Configure the following parameters for the static route to access network B:

a. Enter the destination IP address 192.168.2.0.

b. Specify the mask length as 24.

c. Specify the next hop IP address as 192.168.3.1.

d. Use default settings for other parameters.

Click **OK**.

3. Create a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure security policy **secpolicy**:

a. Enter the name **secpolicy**.

b. Specify the source zone as **Trust**.

c. Specify the destination zone as **Untrust**.

d. Select the IPv4 type.

e. Specify the action as **Permit**.

f. Specify source IPv4 addresses 192.168.1.0/24 and 192.168.2.0/24.

g. Use default settings for other parameters.

Click **OK**.

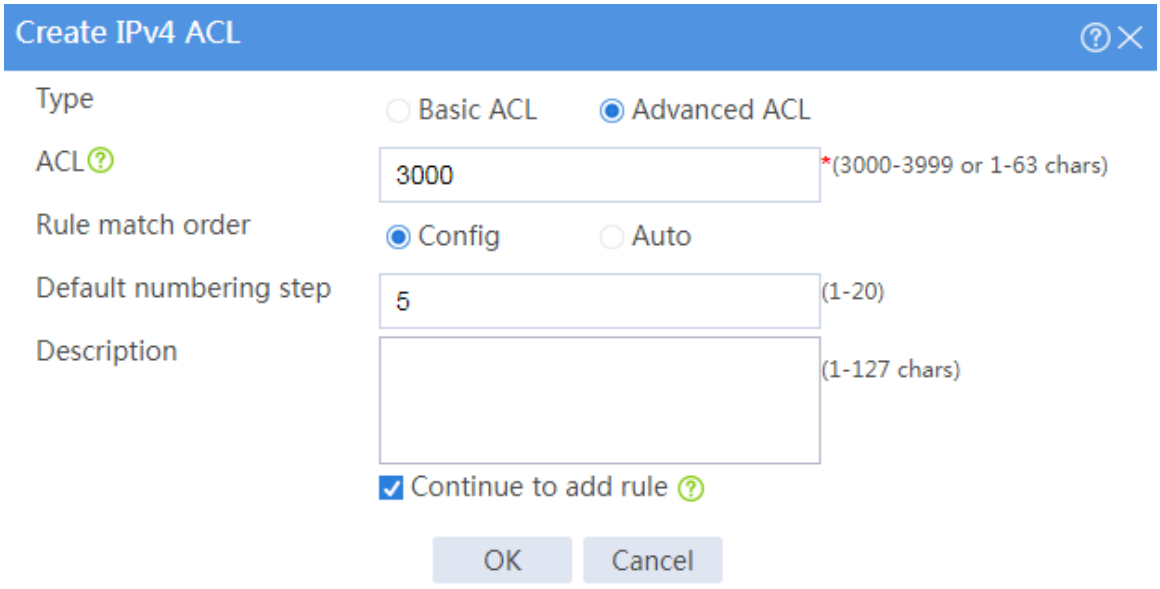
4. Create ACLs.

On the top navigation bar, click **Objects**.

From the navigation pane, select **ACL** > **IPv4**.

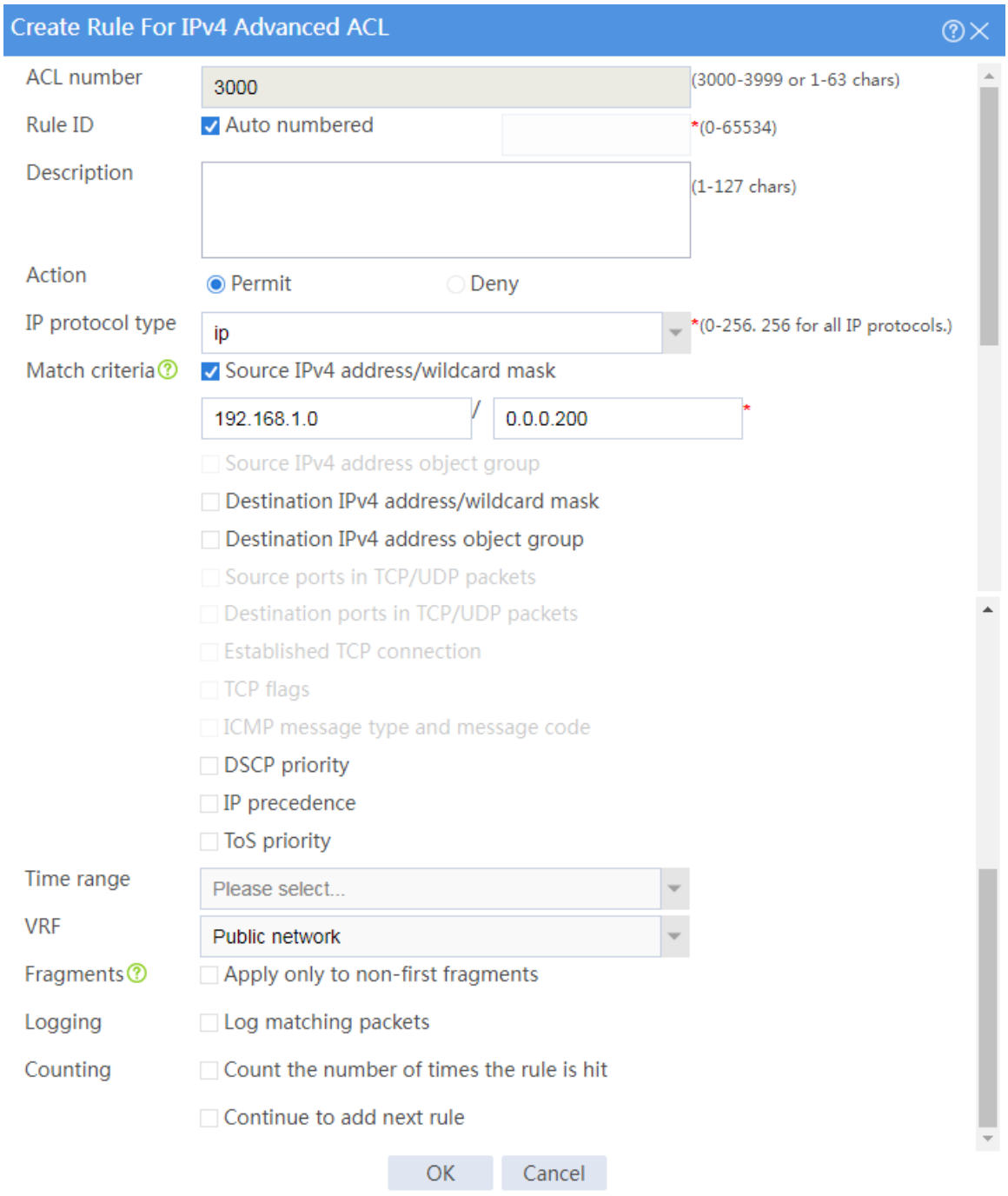
Select **Create** to create an ACL to match user traffic from network A to the external network, as shown in Figure 2.

Figure 2 Creating ACL 3000



Click **OK**, and then add ACL rules, as shown in Figure 3.

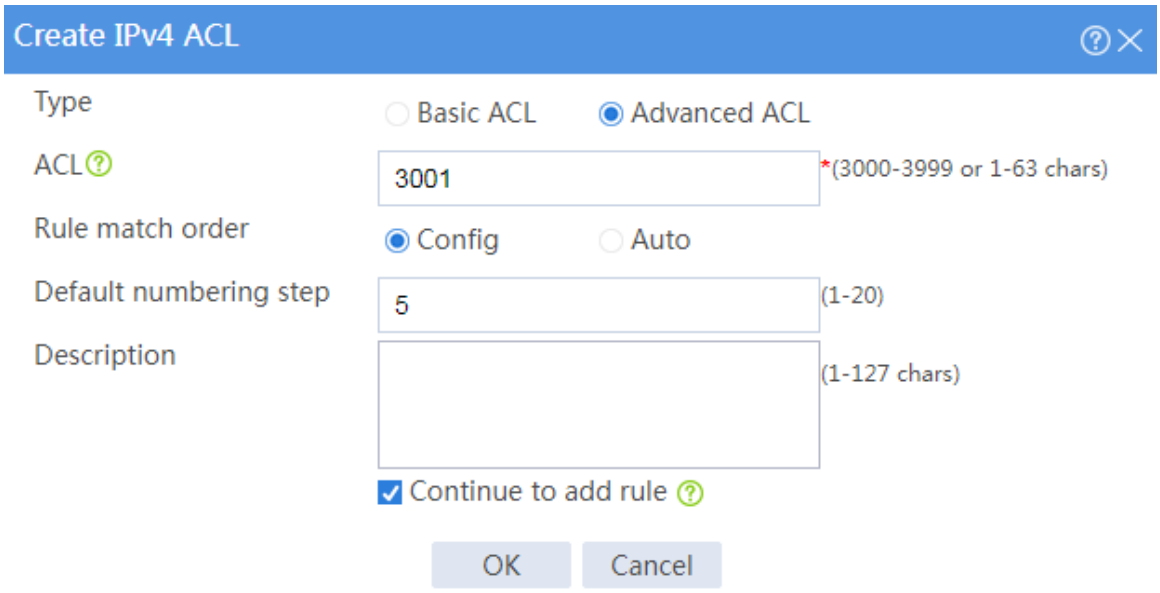
Figure 3 Adding rules to ACL 3000



Click **OK.**

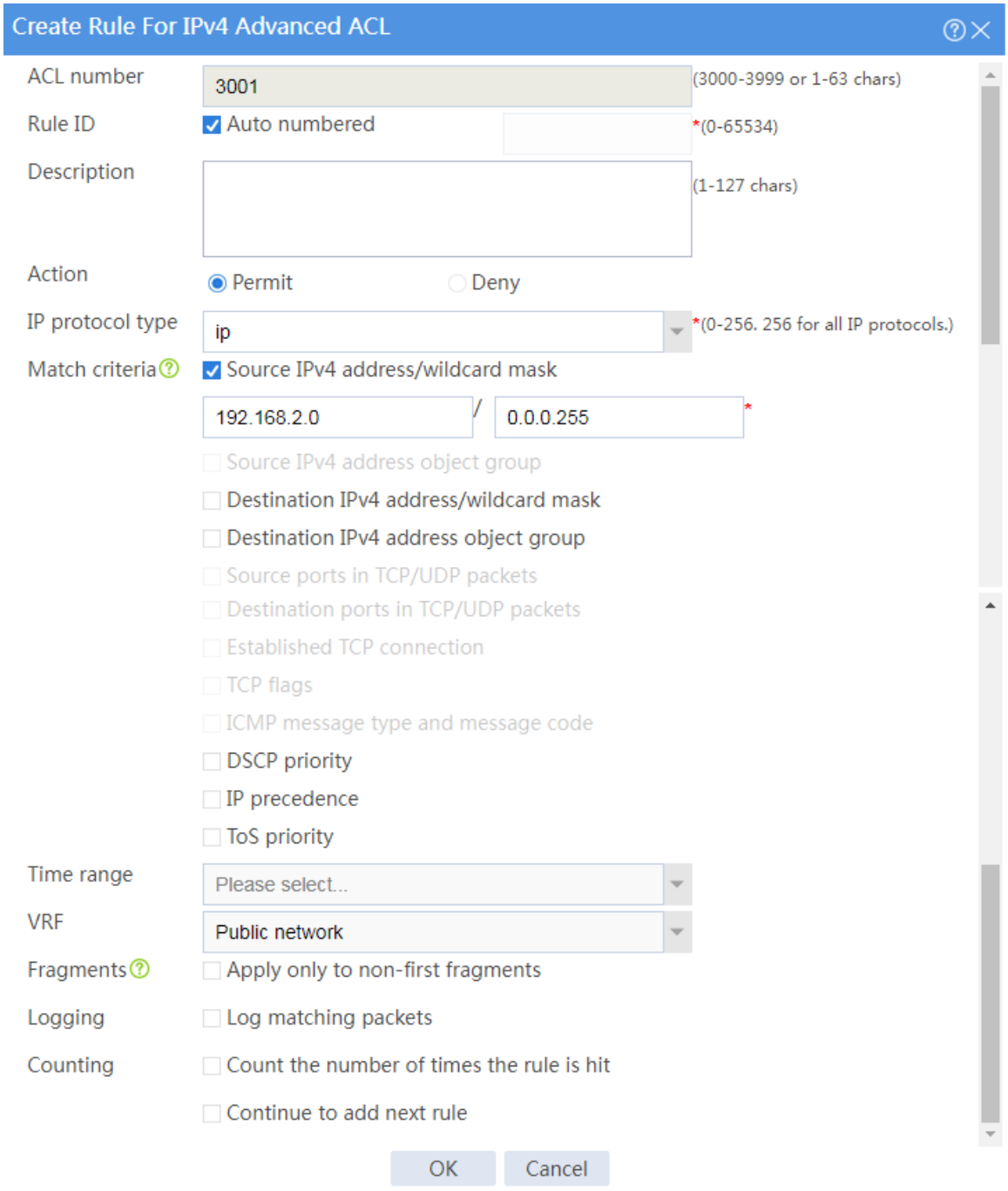
Click **Create** to create an ACL to match user traffic from network B to the external network, as shown in Figure 4.

Figure 4 Adding rules to ACL 3001



Click **OK**, and then add ACL rules, as shown in Figure 5.

Figure 5 Adding rules to ACL 3001



Click **OK.**

5. Configure PBR:

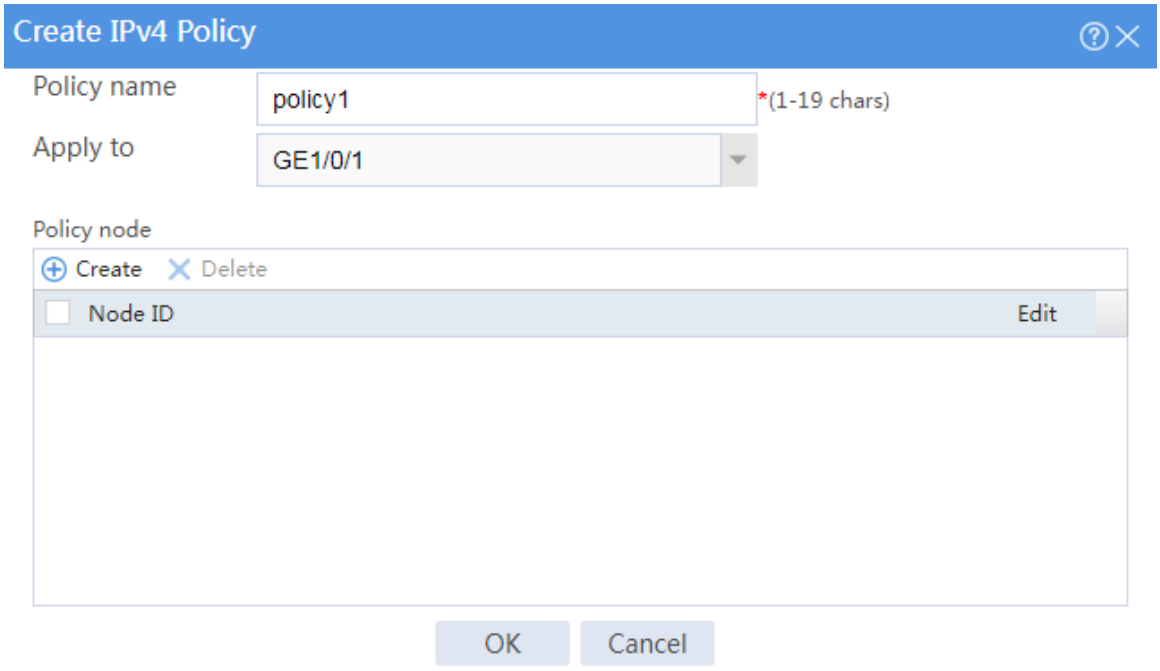
On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **PBR** > **IPv4 PBR**.

Click **Create**.

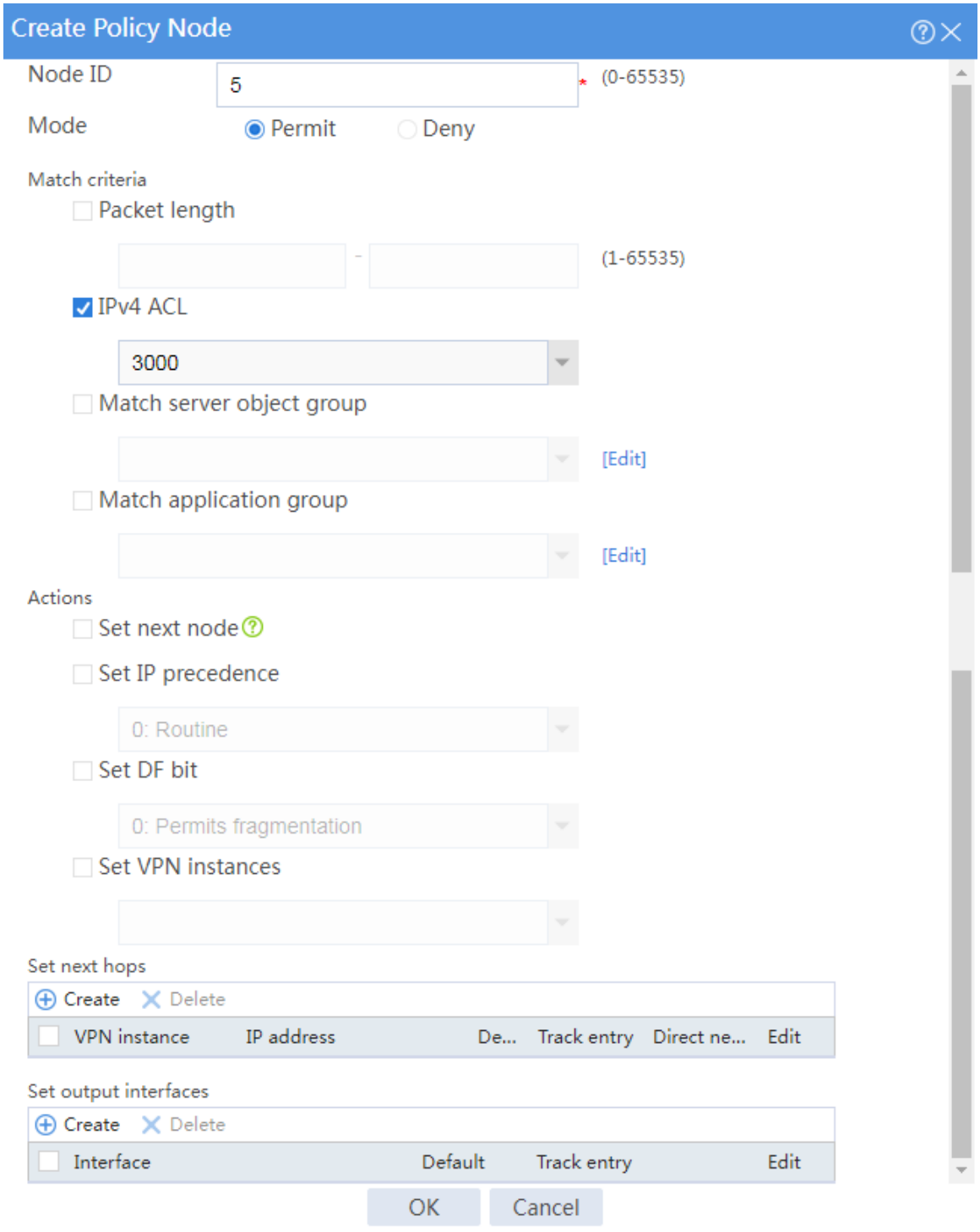
In the dialog box that opens, configure the following parameters for the IPv4 PBR policy, as shown in Figure 6.

Figure 6 Creating an IPv4 PBR policy



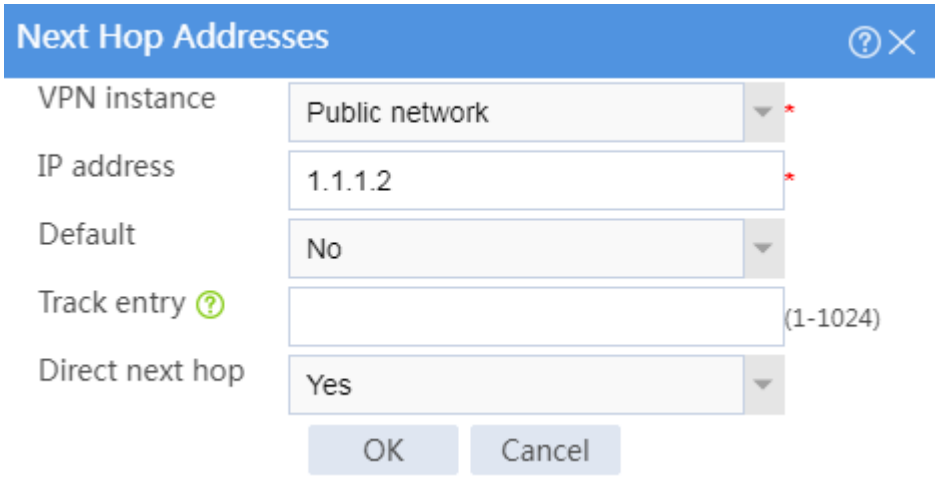
Click **Create** to create policy node 5 to forward user traffic from network A to the external network, as shown in Figure 7.

Figure 7 Creating policy node 5



Click **Create** in the **Set next hops** area, and configure the next hop settings as shown in Figure 8.

Figure 8 Setting the next hop

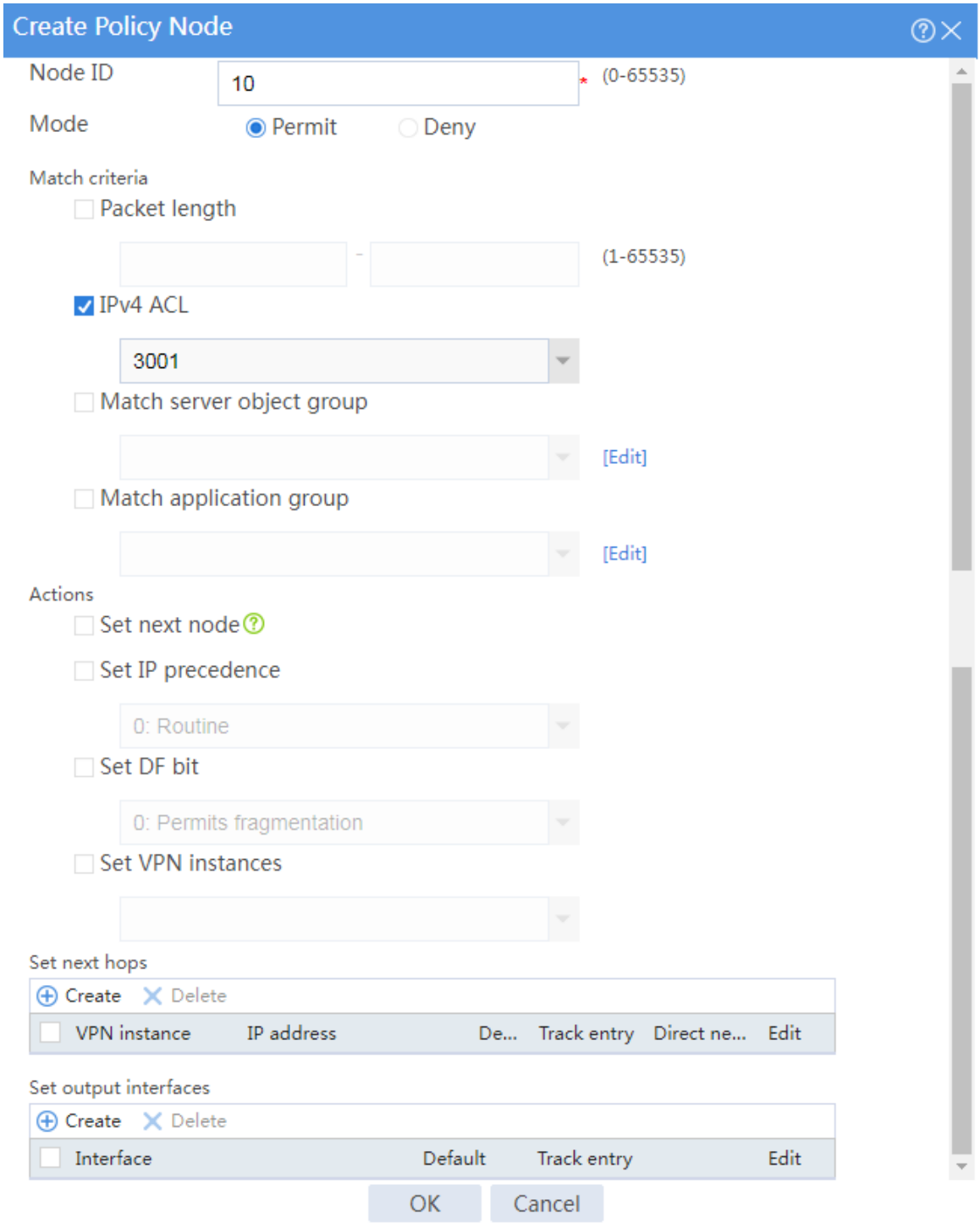


Click **OK** to complete the next hop configuration.

Click **OK** to complete the policy node configuration.

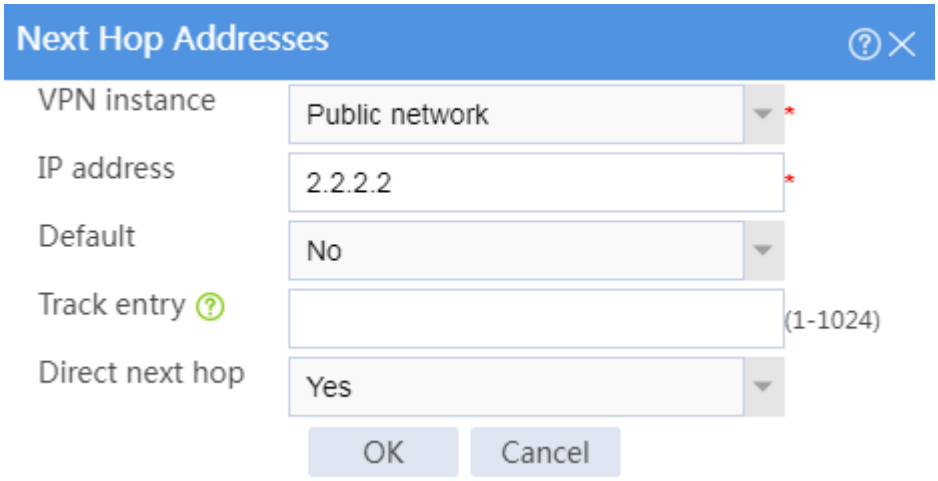
Click **Create** to create policy node 10 to forward user traffic from network B to the external network, as shown in Figure 9.

Figure 9 Creating policy node 10



Click **Create** in the **Set next hops** area, and configure the next hop settings as shown in Figure 10.

Figure 10 Setting the next hop



Click **OK** to complete the next hop configuration.

Click **OK** to complete the policy node configuration.

Click **OK** to complete the IPv4 PBR policy configuration.

Configuring Device B

Configure a static route to ensure that packets from the internal network to the external network can be forwarded to GE 1/0/1 on Device A. (Details not shown.)

Verifying the configuration

1. Use the **tracert** command to identify the path from a host in internal network A to external network IP address 3.3.3.3. Hop 3 is the access point IP address 1.1.1.2 of ISP link A.

```
C:\Users\abc>tracert 3.3.3.3

The path to 3.3.3.3 has a maximum of 30 hops.

1    1 ms      1 ms      1 ms      192.168.1.1
```

```
2    2 ms      2 ms      2 ms      192.168.3.2

3    4 ms      7 ms      6 ms      1.1.1.2

4    5 ms      5 ms      4 ms      3.3.3.3
```

Traceroute completed.

2. Use the **tracert** command to identify the path from a host in internal network B to external network IP address 3.3.3.3. Hop 3 is the access point IP address 2.2.2.2 of ISP link B.

```
C:\Users\xyz>tracert 3.3.3.3
```

The path to 3.3.3.3 has a maximum of 30 hops.

```
1    1 ms      1 ms      1 ms      192.168.2.1

2    2 ms      2 ms      2 ms      192.168.3.2

3    5 ms      6 ms      5 ms      2.2.2.2

4    6 ms      4 ms      5 ms      3.3.3.3
```

Traceroute completed.

Security policy configuration examples

Contents

Introduction

The following information provides security policy configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the security policy feature.

Restrictions and guidelines

Packet filtering, if configured, is performed only on packets that do not match any security policy rule. As a best practice, make sure security policies have stricter filtering criteria than packet filtering, so the unmatched packets can still be filtered by packet filtering.

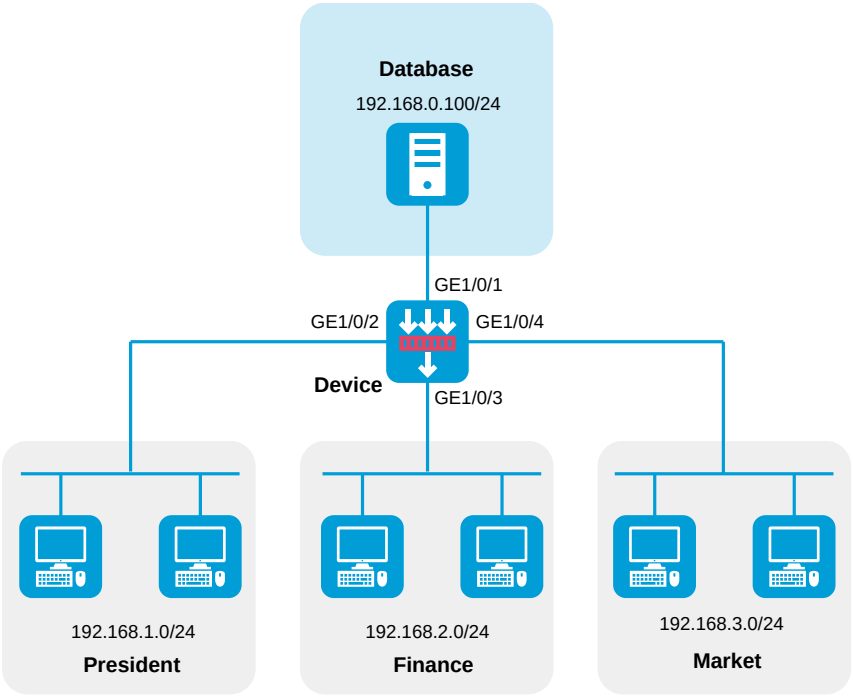
Example: Configuring basic security policies

Network configuration

As shown in Figure 1, configure security policy to achieve the following goals:

- The president office can access the financial database server through HTTP at any time.
- The financial office can access the financial database server through HTTP from 8:00 to 18:00 on weekdays.
- The marketing office cannot access the financial database server through HTTP at any time.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Create a security zone.

On the top navigation bar, click **Network**.

From the navigation pane, select **Security Zones**.

Perform the following tasks:

- Create a security zone named **database**, and add GigabitEthernet 1/0/1 to the zone.
- Create a security zone named **president**, and add GigabitEthernet 1/0/2 to the zone.
- Create a security zone named **finance**, and add GigabitEthernet 1/0/3 to the zone.
- Create a security zone named **market**, and add GigabitEthernet 1/0/4 to the zone.

2. Assign IP addresses to interfaces.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 192.168.0.1/24.

b. Click **OK**.

Set the IP addresses of GE 1/0/2, GE 1/0/3, and GE 1/0/4 to 192.168.1.1/24, 192.168.2.1/24, and 192.168.3.1/24, respectively, in the same way you configure GE 1/0/1.

3. Create a time range.

On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **Time Ranges**.

Click **Create**.

In the dialog box that appears, enter name **work** and then click **Create** for **Periodic time range**.

In the dialog box that appears, configure the time range:

- Set the start time to **08:00**.
- Set the end time to **18:00**.

- Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, and **Friday**.

Click **OK**.

4. Create a security policy from security zone **president** to security zone **database** to allow the president office to access the database through HTTP at any time.

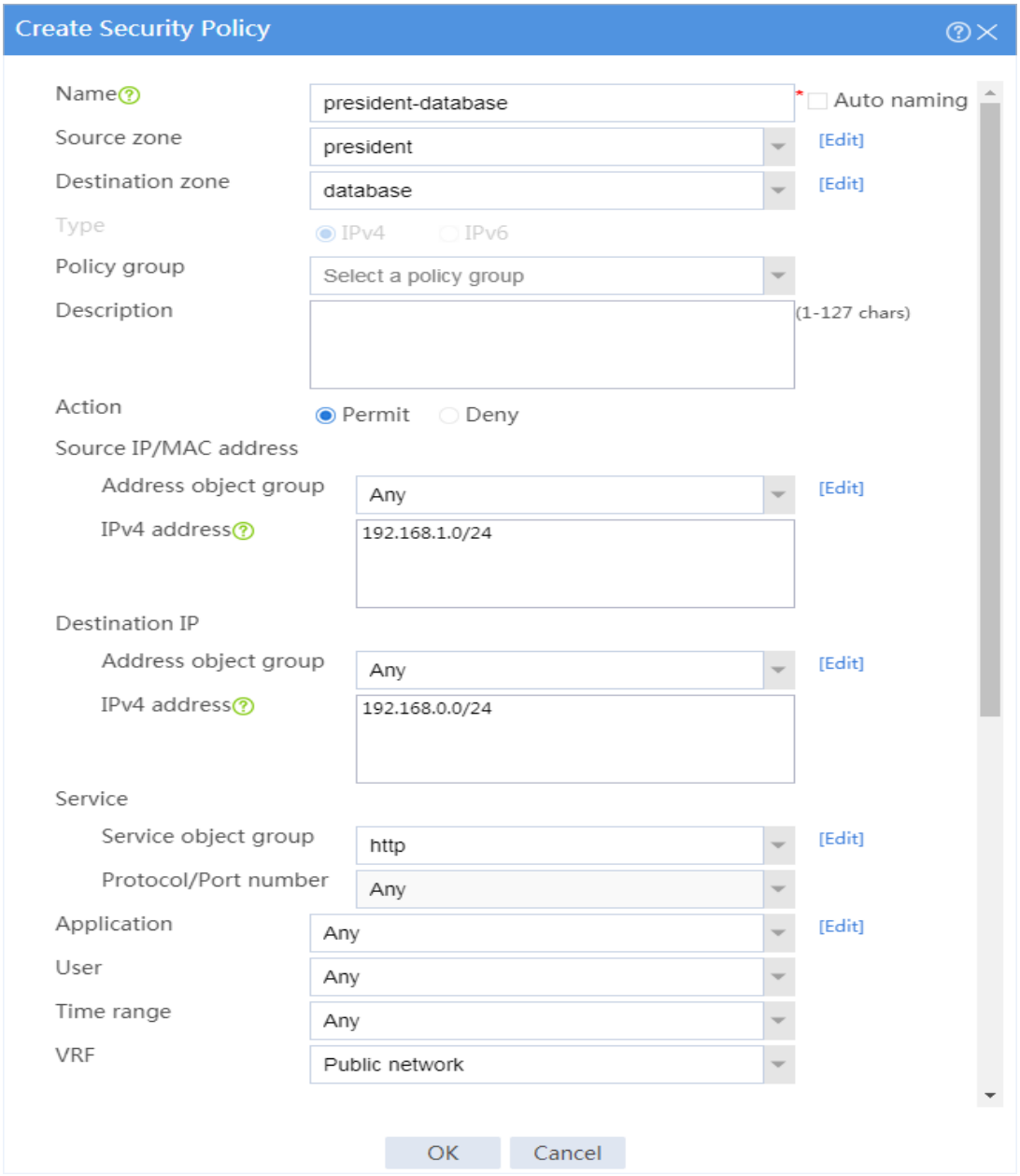
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, create a security policy as shown in Figure 2:

Figure 2 Create a security policy for the president office



Click **OK**.

5. Create a security policy from security zone **finance** to security zone **database** to allow the financial office to access the database through HTTP from 8:00 to 18:00 on weekdays.

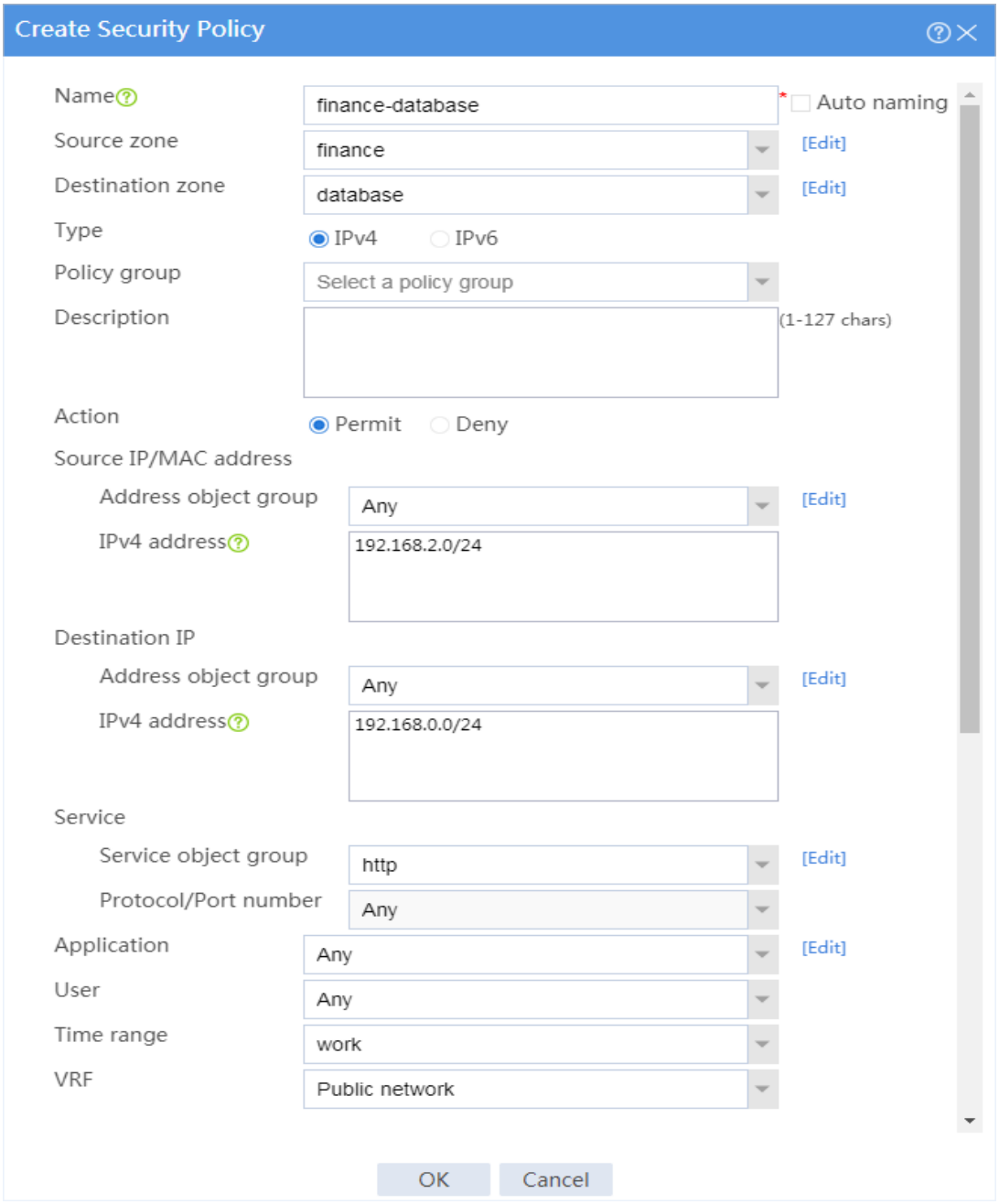
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, create a security policy as shown in Figure 3:

Figure 3 Create a security policy for the financial office



Click **OK**.

6. Create a security policy from security zone **market** to security zone **database** to forbid the marketing office from accessing the database through HTTP at any time.

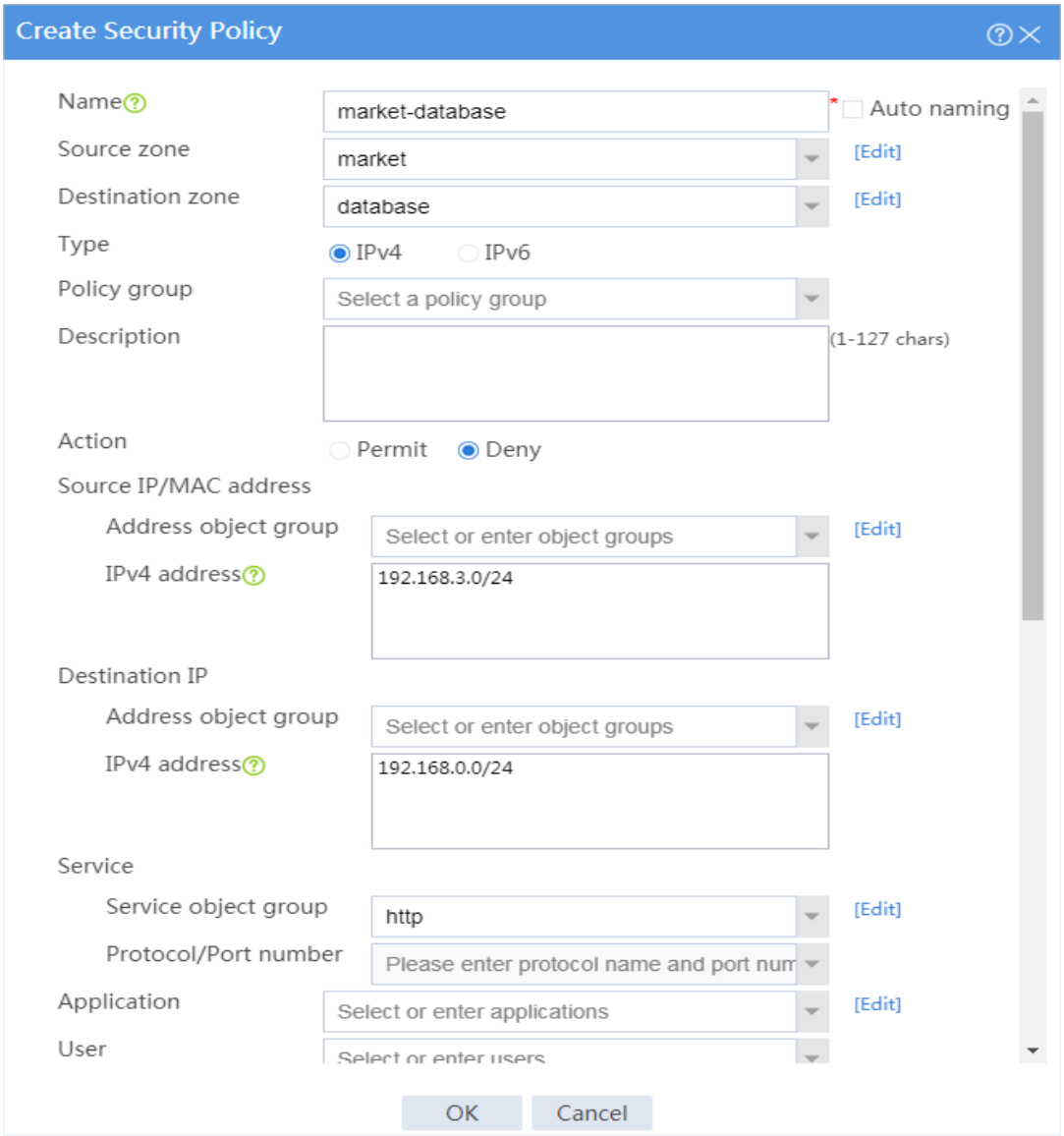
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, create a security policy as shown in Figure 4:

Figure 4 Create a security policy for the marketing office



Click **OK**.

7. For the security policies to take effect immediately, activate security policy matching acceleration.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Activate** (the first **Submit** in this example).

Verifying the configuration

Use a PC in each office to access the Web service of the financial database server through the browser.

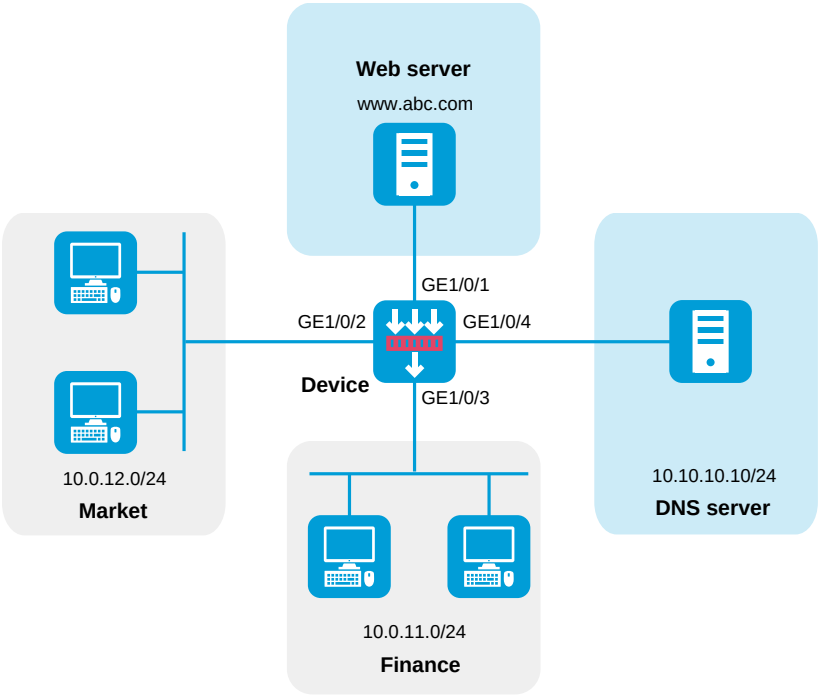
Example: Configuring domain name-based security policies

Network configuration

As shown in Figure 5, a Web server with domain name www.abc.com is deployed for financial management, and the domain name has been registered on the DNS server in the internal network. Configure a security policy to achieve the following goals:

- The financial office can access the financial server through HTTP.
- The marketing office cannot access the financial server through HTTP at any time.

Figure 5 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Create a security zone.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Security Zones**.

   # Perform the following tasks:

- Create a security zone named **web**, and add GigabitEthernet 1/0/1 to the zone.
- Create a security zone named **market**, and add GigabitEthernet 1/0/2 to the zone.
- Create a security zone named **finance**, and add GigabitEthernet 1/0/3 to the zone.
- Create a security zone named **dns**, and add GigabitEthernet 1/0/4 to the zone.

2. Assign IP addresses to interfaces.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.0.0.1/24.

b. Click **OK**.

Set the IP addresses of GE 1/0/2, GE 1/0/3, and GE 1/0/4 to 10.0.12.1/24, 10.0.11.1/24, and 10.0.10.1/24, respectively, in the same way you configure GE 1/0/1.

3. Create an IPv4 address object.

On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **IPv4 Address Object Groups**.

Create an IPv4 address object group named **web** and specify the host name as **www.abc.com**.

4. Configure DNS settings.

On the top navigation bar, click **Network**.

From the navigation pane, select **DNS** > **DNS Client**.

On the page that opens, enter domain server address **10.10.10.10**, and then click the plus icon to add a DNS server.

5. Create a security policy from security zone **local** to security zone **dns** to allow the device to access the DNS server for host name translation.

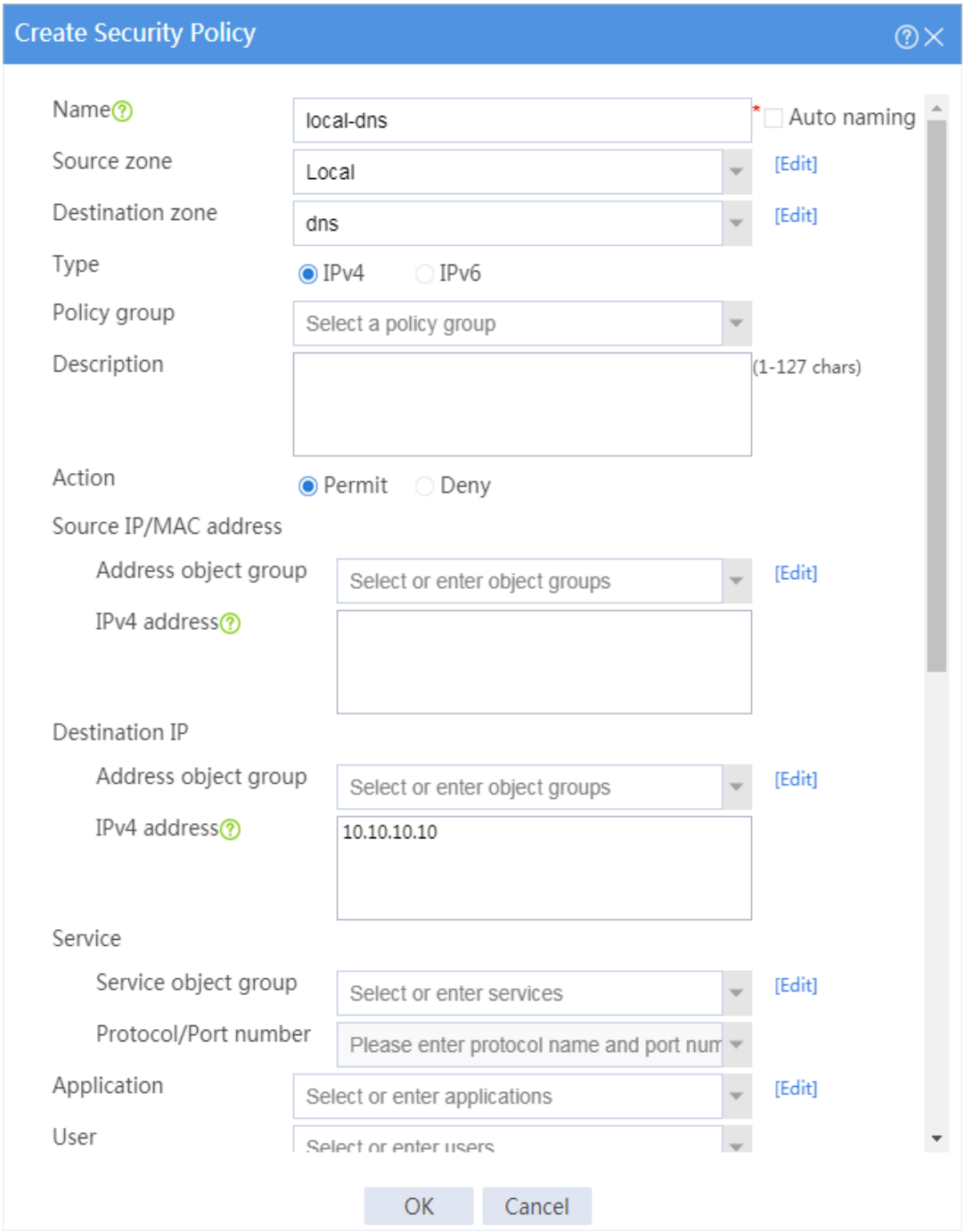
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, create a security policy as shown in Figure 6:

Figure 6 Create a security policy for the device to access the DNS server



Click **OK**.

6. Create a security policy from security zones **market** and **finance** to security zone **dns** to allow hosts in the internal network to access the DNS server for host name translation.

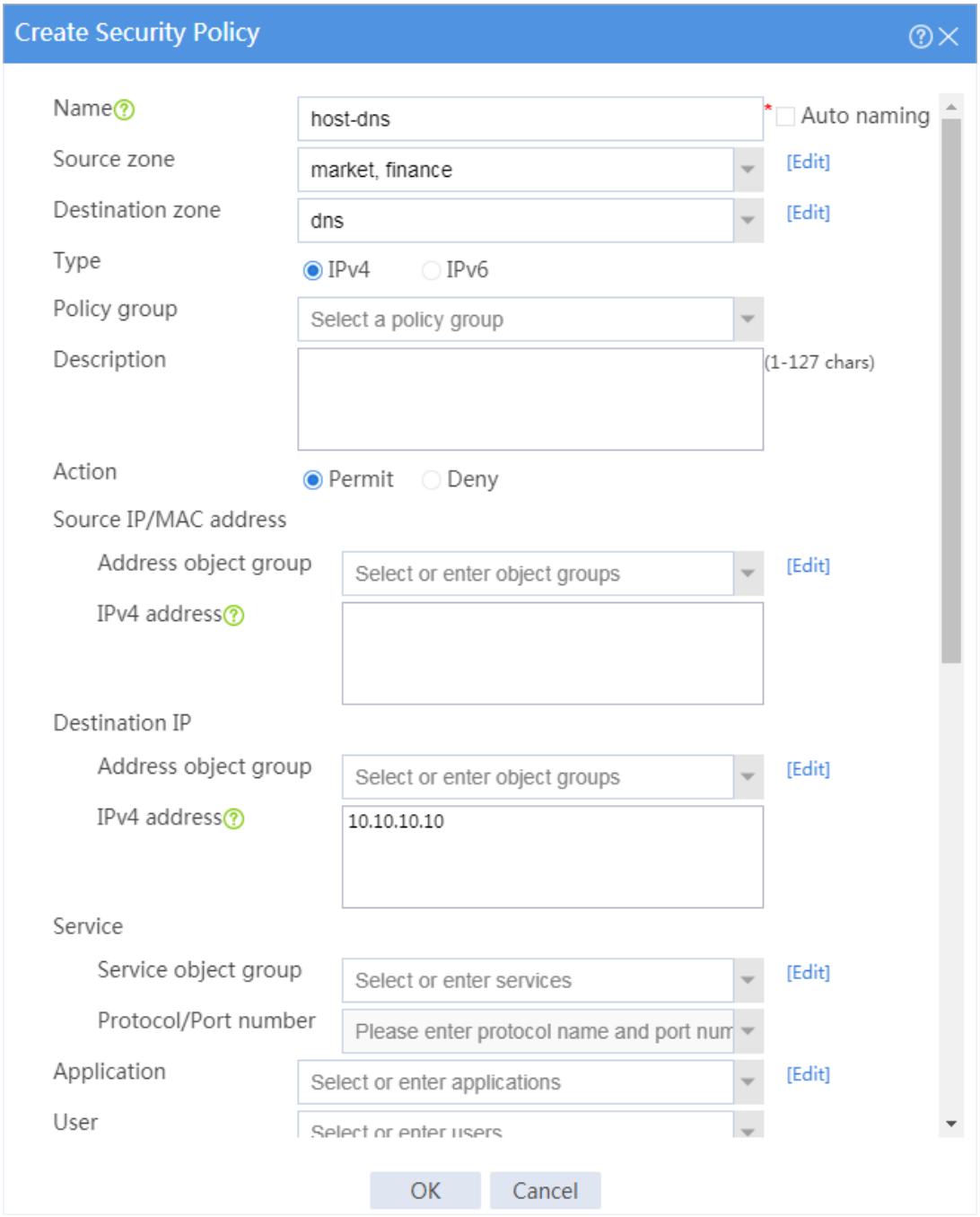
On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, create a security policy as shown in Figure 7:

Figure 7 Create a security policy for the internal network



Click **OK**.

7. Create a security policy from security zone **finance** to security zone **web** for the financial office to access the financial Web server through HTTP.

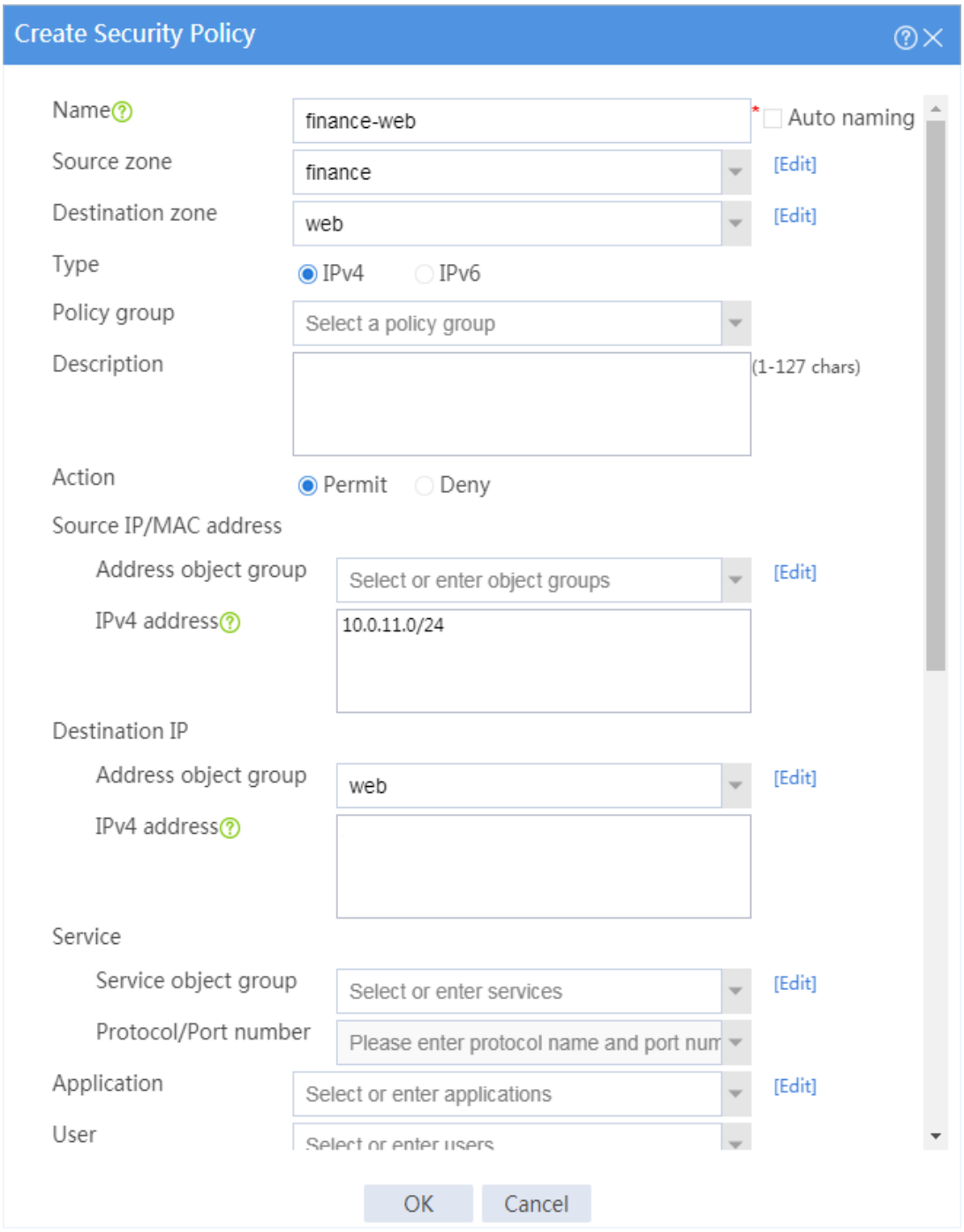
On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, create a security policy as shown in Figure 8:

Figure 8 Create a security policy for the financial office



Click **OK**.

8. Create a security policy from security zone **market** to security zone **web** to forbid the marketing office from accessing the financial Web server through HTTP at any time.

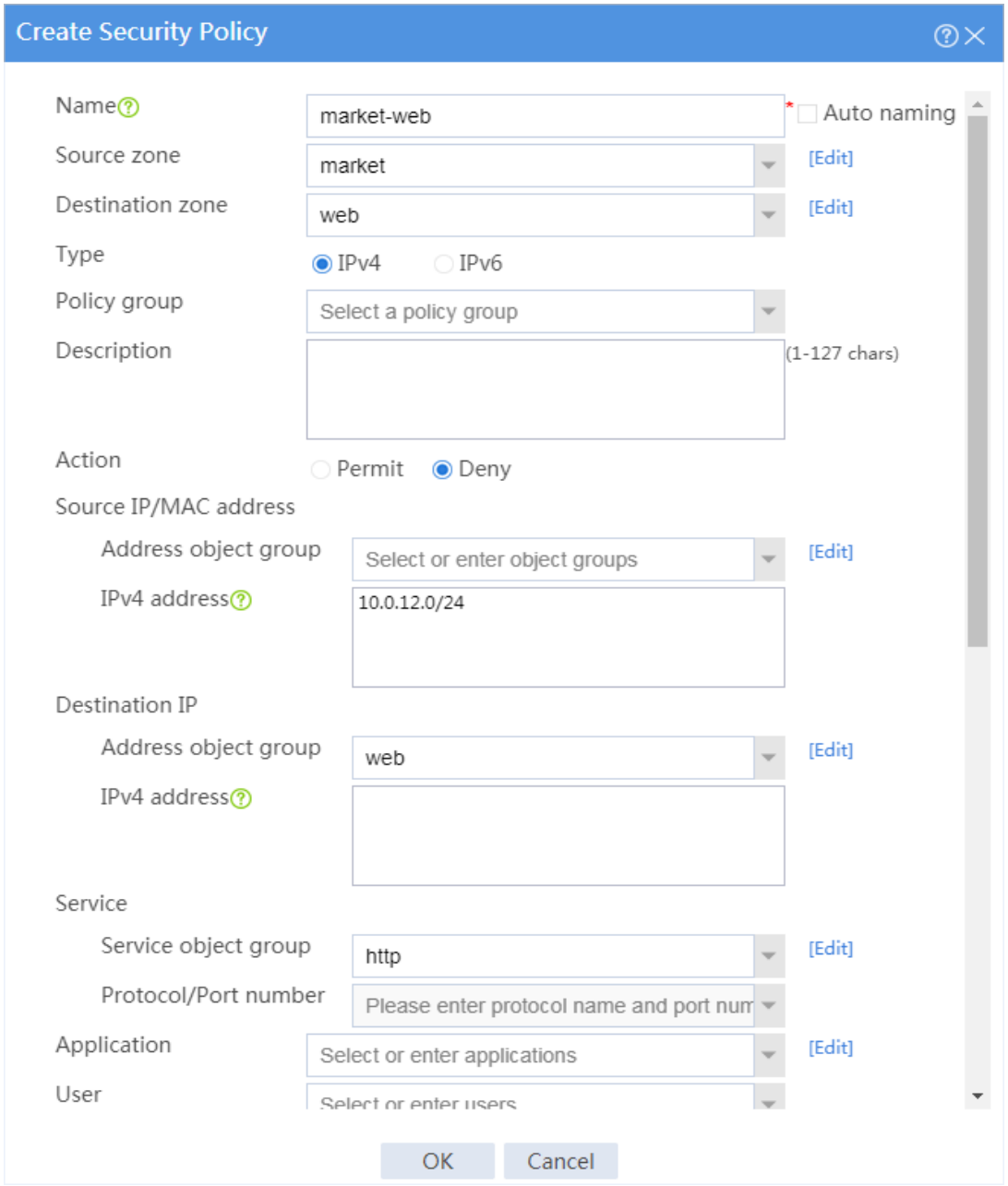
On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, create a security policy as shown in Figure 9:

Figure 9 Create a security policy for the marketing office



Click **OK**.

9. For the security policies to take effect immediately, activate security policy matching acceleration.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Activate** (the first **Submit** in this example).

Verifying the configuration

Use a PC in each office to access the Web service of the financial server through the browser.

Example: Configuring security policies and DPI

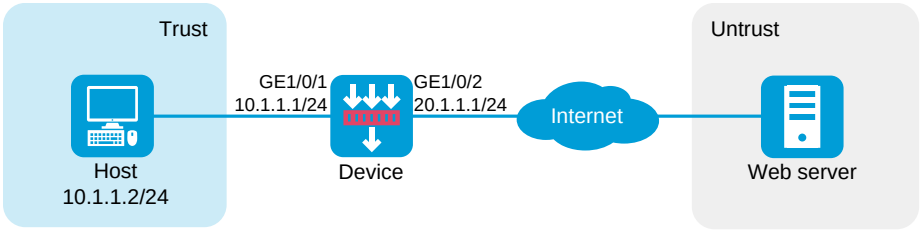
Network configuration

As shown in Figure 10, the host in the internal network accesses the Internet through the device.

Configure a security policy and DPI on the device with the following settings:

- Perform anti-virus detection on data packets from the internal network and drop packets with viruses.
- Specify virus with ID 90321 as a virus exception.
- Specify RenMinWang as an application exception. Enable the system to permit packets with viruses to RenMinWang and generate alarms.

Figure 10 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1/24 in the same way you configure GE 1/0/1.

2. Create an anti-virus profile.

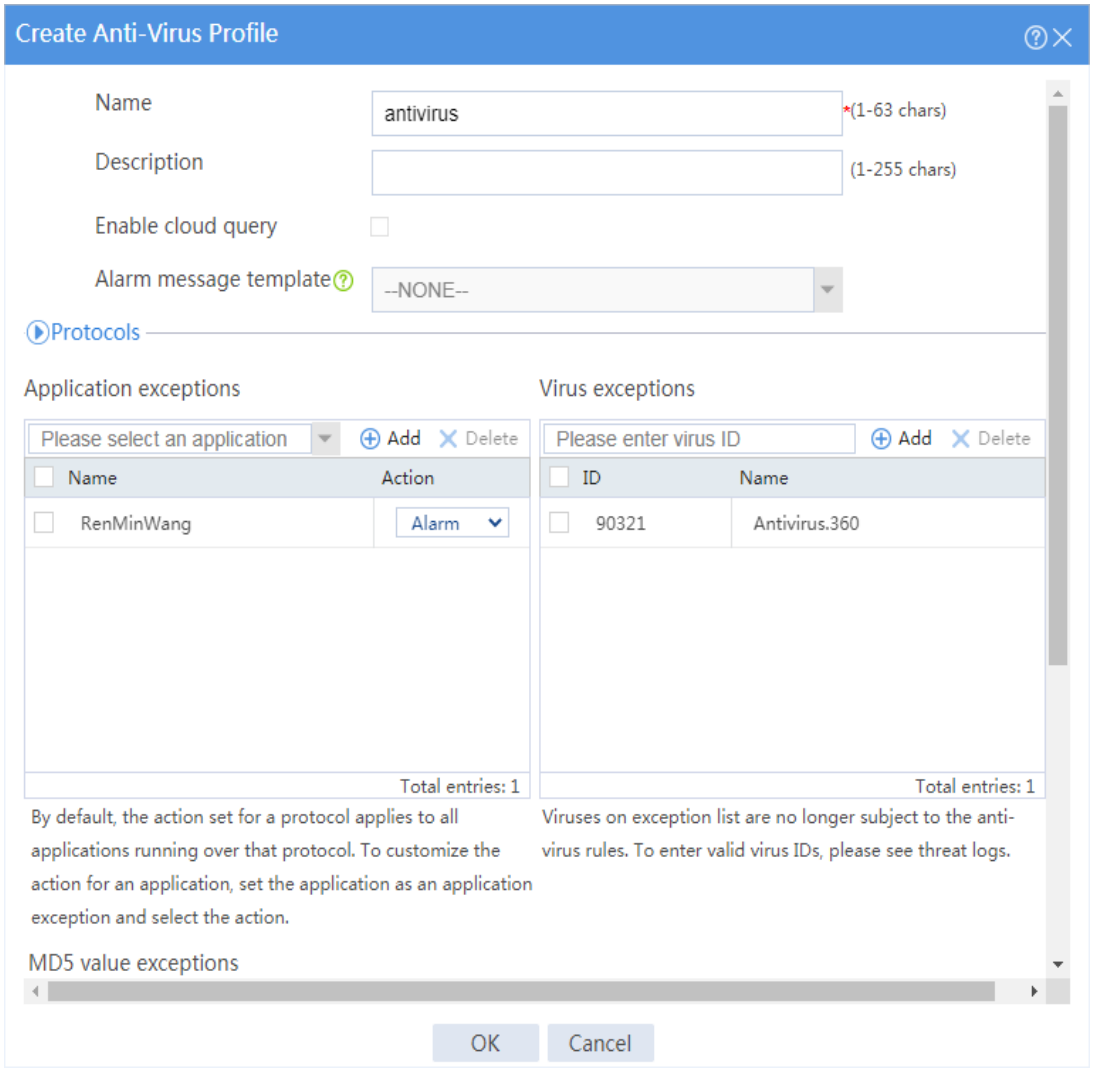
On the top navigation bar, click **Objects**.

From the navigation pane, select **APPSecurity** > **Anti-Virus** > **Profile**.

Click **Create**.

In the dialog box that opens, create an anti-virus profile as shown in Figure 11.

Figure 11 Create an anti-virus profile



Click **OK**.

3. Create a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that appears, create a security policy as shown in Figure 12 and Figure 13.

Figure 12 Create basic security policy settings

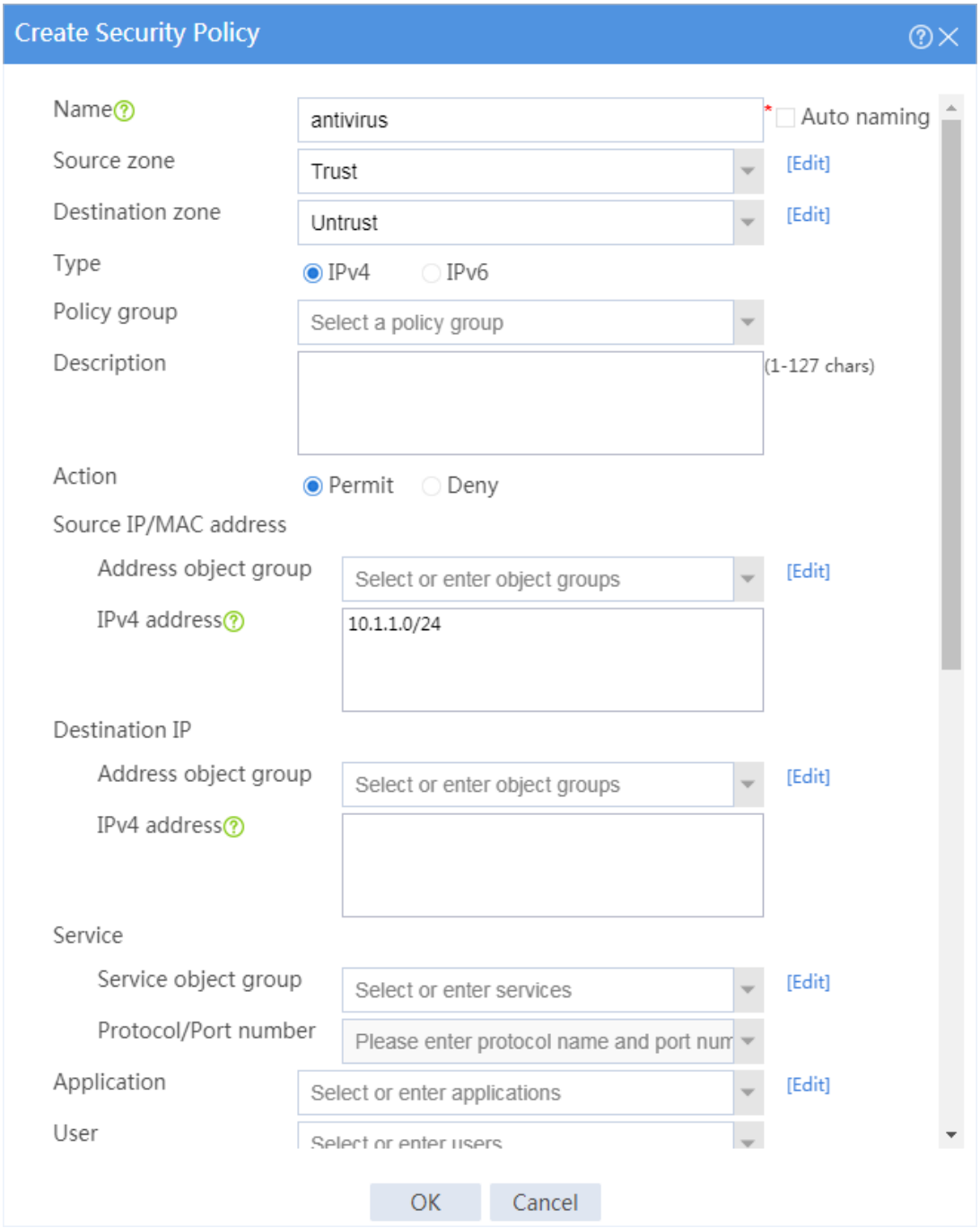
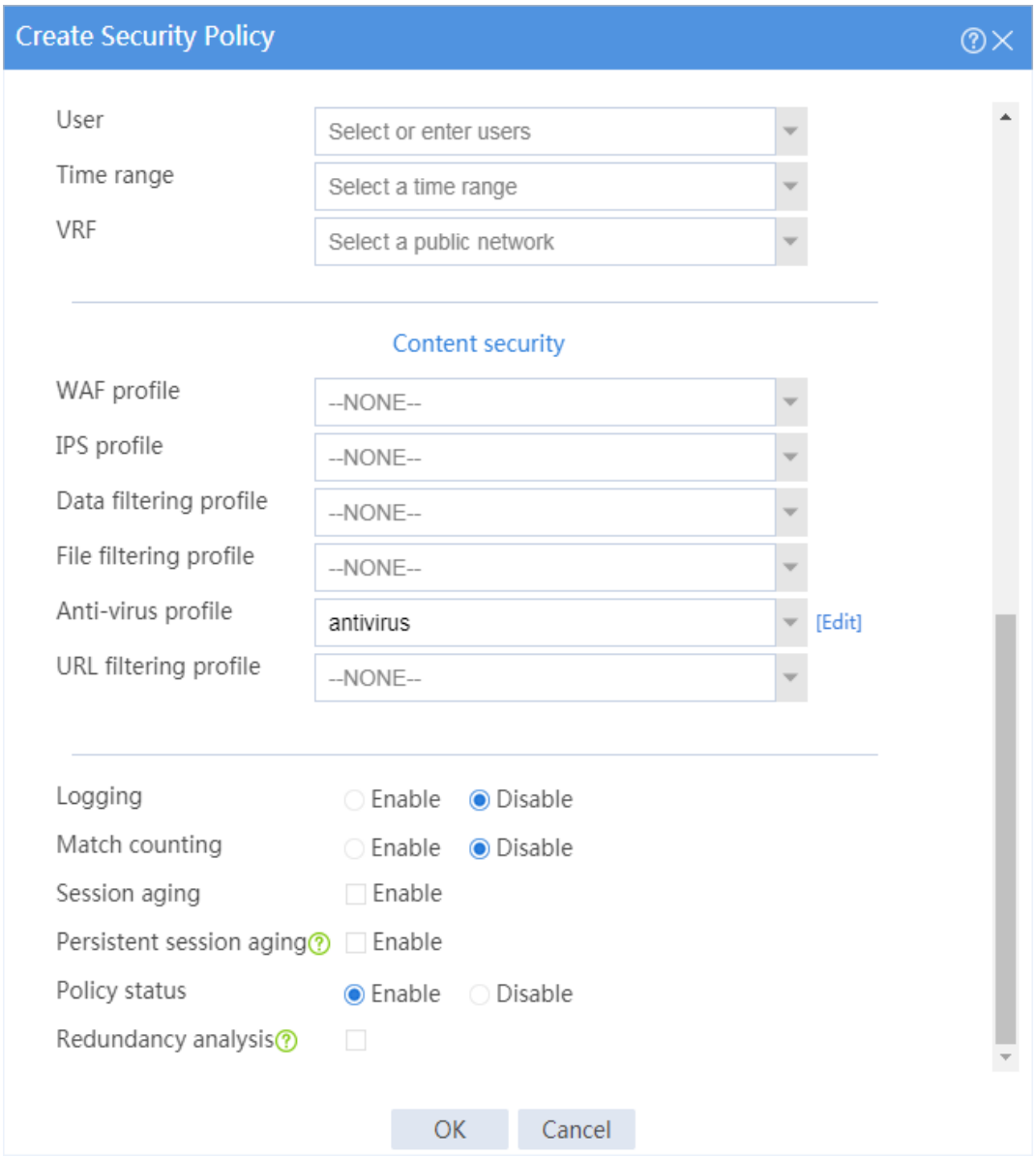


Figure 13 Configure content security settings



Click **OK**.

4. For the security policy to take effect immediately, activate security policy matching acceleration.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Activate** (the first **Submit** in this example).

5. Submit content security settings for the settings to take effect.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Submit** (the second **Submit** in this example).

Verifying the configuration

Verify that virus attacks on internal users can be prohibited effectively.

APR-based security policy configuration examples

Contents

Introduction

The following information provides APR-based security policy configuration examples.

A security policy defines a set of rules for forwarding control and Deep Packet Inspection (DPI). It matches packets against the rules and takes the action stated in the rules on the matched packets.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the APR and security policy features.

Restrictions and guidelines

Packet filtering, if configured, is performed only on packets that do not match any security policy rule. As a best practice, make sure security policies have stricter filtering criteria than packet filtering, so the unmatched packets can still be filtered by packet filtering.

For security purposes, configure APR-based, strict security policies.

Example: Configuring APR-based, strict security policies

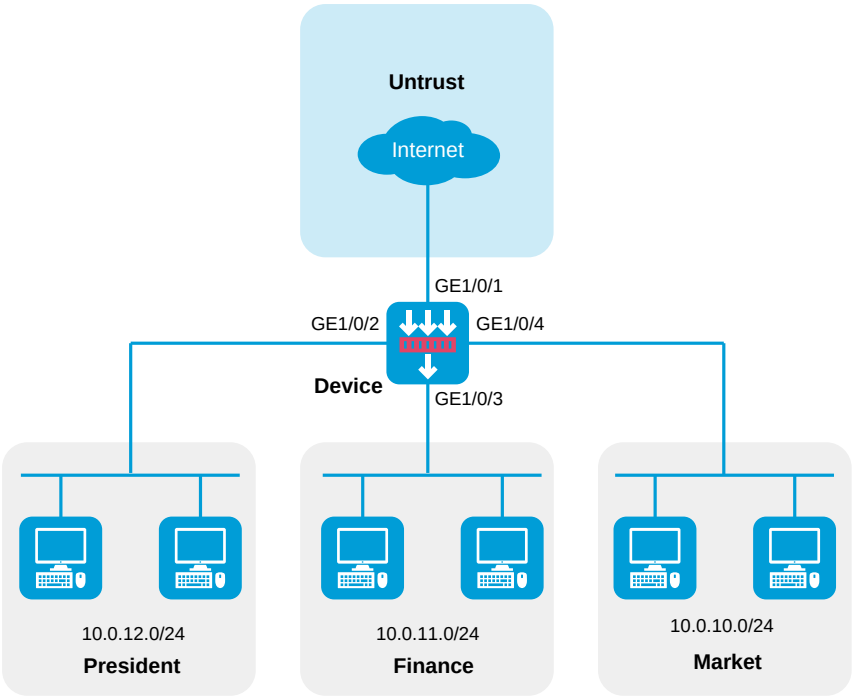
Network configuration

As shown in Figure 1, configure security policies to achieve the following goals:

- The president office can access all network resources at any time.

- The financial office can access only its own resources.
- The marketing office can access some resources on the Internet from 8:00 to 18:00 on workdays.
    - Cannot access gaming, streaming media, P2P, or network community resources, but can access YouKu.
    - Can only access WeChat and cannot access any other IM applications.
    - Can access MSN, DingTalk, and security forum resources.
    - Can access any resources except the listed resources that cannot be accessed.
- The financial office cannot be accessed by anyone, and the financial office and the marketing office cannot access each other.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

When you configure a security policy, follow these restrictions and guidelines:

- Update the APR signature library to the latest version.
- For the applications in a security policy to be identified, you must allow the dependent protocols of the applications to pass through.

Analysis

- Configure security policy **president_permit** to allow the employees in the president office to freely access any network resources.
- Configure security policy **finance_permit** to allow the employees in the financial office to communicate with one another.
- Configure security policy **market_permit1** to allow the employees in the marketing office to use WeChat, MSN, DingTalk, YouKu, and security forum resources. By default, a security policy does not allow use of IM applications.
- Configure security policy **market_deny1** to deny network community and streaming media applications for the marketing office from 8:00 to 18:00 on workdays. This security policy prevents employees in the marketing office from playing games, watching video, and accessing network community sites from 8:00 to 18:00 on workdays. To permit WeChat,

MSN, DingTalk, YouKu, and security forum applications, you must configure security policy **market_permit1** before **market_deny1**.

- Configure security policy **market_permit2** to allow the employees in the marketing office to use some OA, email, and protocol applications that are not easy to identify. To deny such an application, remove it from the application group or configure another security policy to deny it.
- Configure security policy **market_permit3** to allow common protocols for APR to identify applications correctly. Common protocols include TCP, UDP, DNS, HTTP, HTTPS, SMTP, IMAP, and POP3. The security policy **market_permit2** might permit these protocols. As a best practice for APR to identify applications correctly when security policy **market_permit2** changes, configure security policy **market_permit3** to allow these protocols.
- Configure the security policies in the following order:
    a. **president_permit**
    b. **finance_permit**
    c. **market_permit1**
    d. **market_deny1**
    e. **market_permit2**
    f. **market_permit3**

Procedure

1. Configure security zones.

    # On the top navigation bar, click **Network**.

    # From the navigation pane, click **Security Zones**.

Click the **Edit** icon for security zone **Untrust**.

In the dialog box that opens, add GE 1/0/1 to the security zone.

Create a security zone named **president**, and add GE 1/0/2 to the security zone.

Create a security zone named **finance**, and add GE 1/0/3 to the security zone.

Create a security zone named **market**, and add GE 1/0/4 to the security zone.

2. Assign IP addresses to interfaces.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.2.2.1/24.

b. Click **OK**.

Configure the IP addresses of GE 1/0/2, GE 1/0/3, and GE 1/0/4 as 10.0.12.1/24, 10.0.11.1/24, and 10.0.10.1/24, respectively, in the same way you configure GE 1/0/1.

3. Configure a time range.

On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **Time Ranges**.

Click **Create**.

In the dialog box that opens, configure the time range:

a. Enter a time range name. In this example, enter **work**.

b. Create a periodic time range from 8:00 to 18:00 on workdays, and click **OK**.

c. Click **OK**.

4. Configure application groups.

   # On the top navigation bar, click **Objects**.

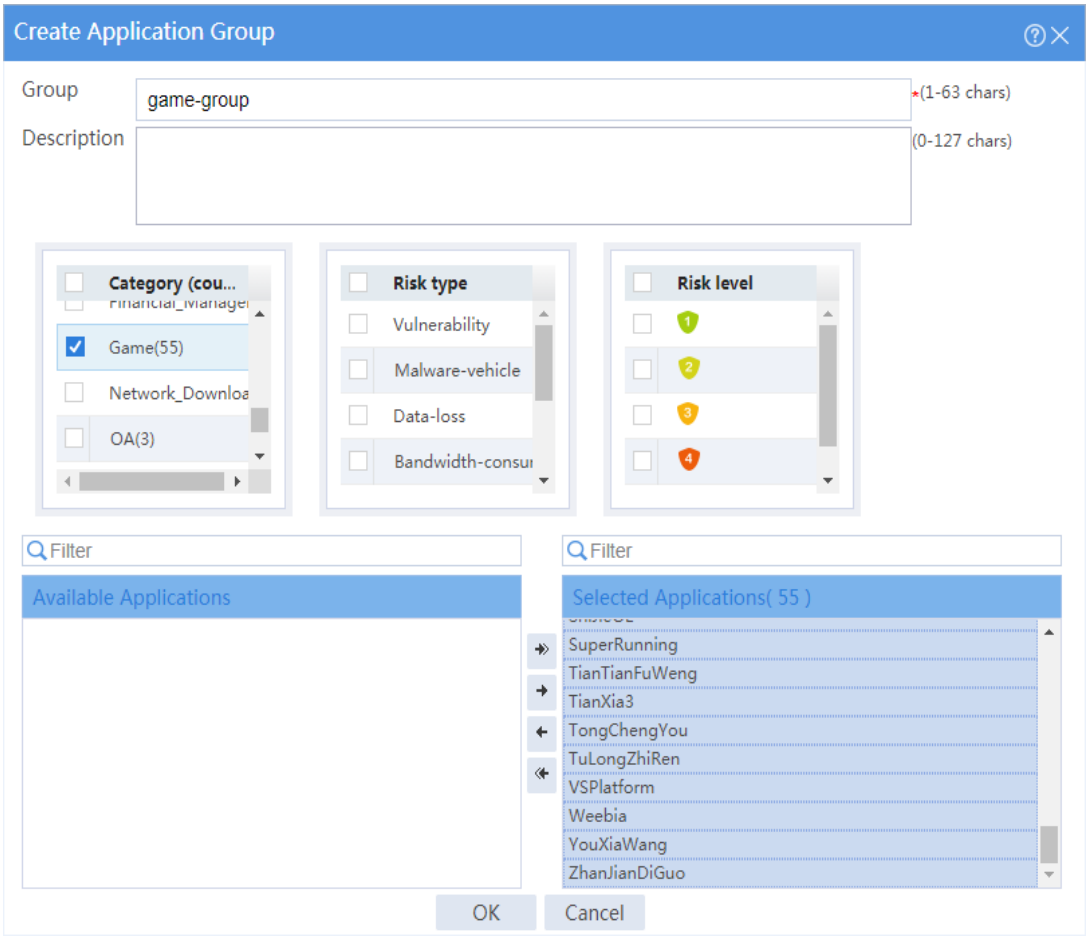
   # From the navigation pane, select **APPSecurity** > **APP Recognition** > **Application Groups**.

   # Click **Create**.

   # In the dialog box that opens, configure an application group named **game-group**:

   - Enter group name **game-group**.
   - Add all applications in the **Game** category to the **Selected Applications** pane.
   - Click **OK**.

Figure 2 Creating an application group



Create an application group named **p2p-group**, and add all applications in the **P2P** category to the application group.

Create an application group named **streaming-media-group**, and add all applications in the **Streaming_Media** category to the application group.

Create an application group named **network-community-group**, and add all applications in the **Network-Community** category to the application group.

Create an application group named **permit-others**, and add some applications in the **E-Mail**, **OA**, and **Protocol** categories that are not easy to identify to the application group.

Create an application group named **protocol-permit**, and add common protocols (such as TCP, UDP, DNS, HTTP, HTTPS, SMTP, IMAP, and POP3) to the application group.

5. Configure a security policy named **president_permit**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

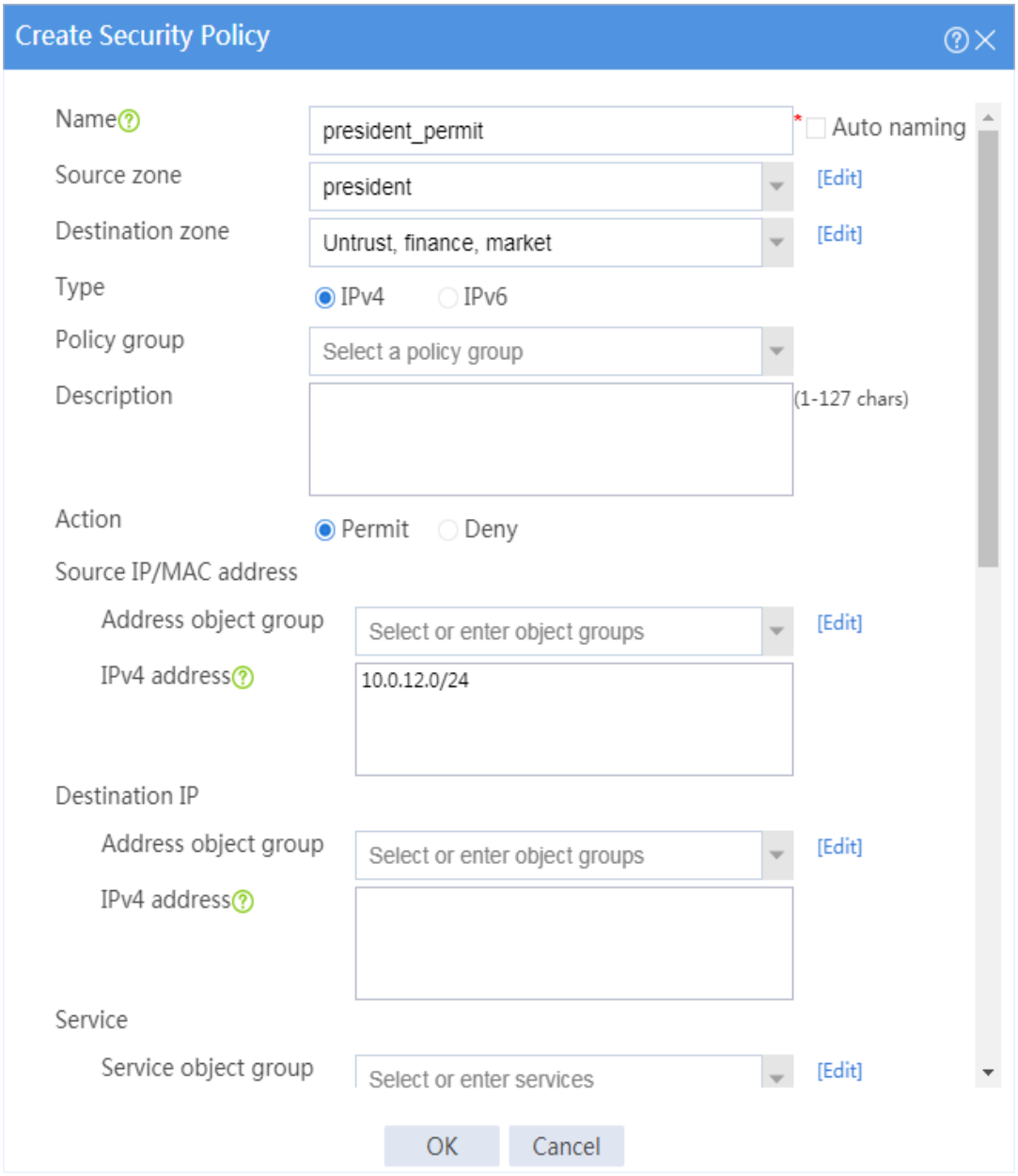
   # Click **Create**.

   # In the dialog box that appears, configure the security policy:

   - Enter policy name **president_permit**.
   - Select source zone **president**.
   - Select destination zones **Untrust**, **finance**, and **market**.
   - Select policy type **IPv4**.
   - Select action **Permit**.
   - Select source IP address **president**.

   # Click **OK**.

Figure 3 Creating security policy president_permit



6. Configure a security policy named **finance_permit**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

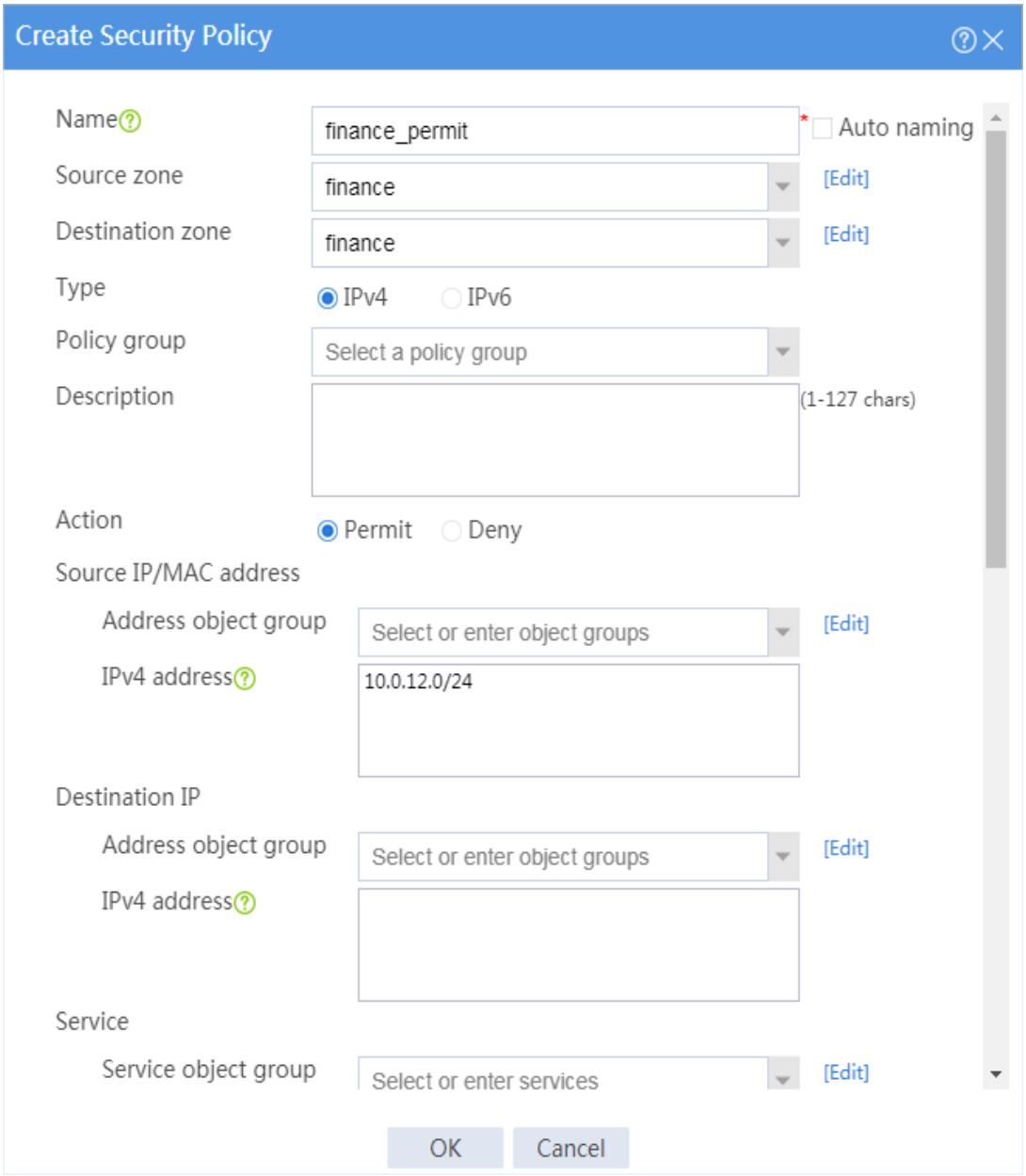
   # Click **Create**.

   # In the dialog box that appears, configure the security policy:

- Enter policy name **finance_permit**.
- Select source zone **finance**.
- Select destination zone **finance**.
- Select policy type **IPv4**.
- Select action **Permit**.

Click **OK**.

Figure 4 Creating security policy finance_permit



7. Configure a security policy named **market_permit1**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

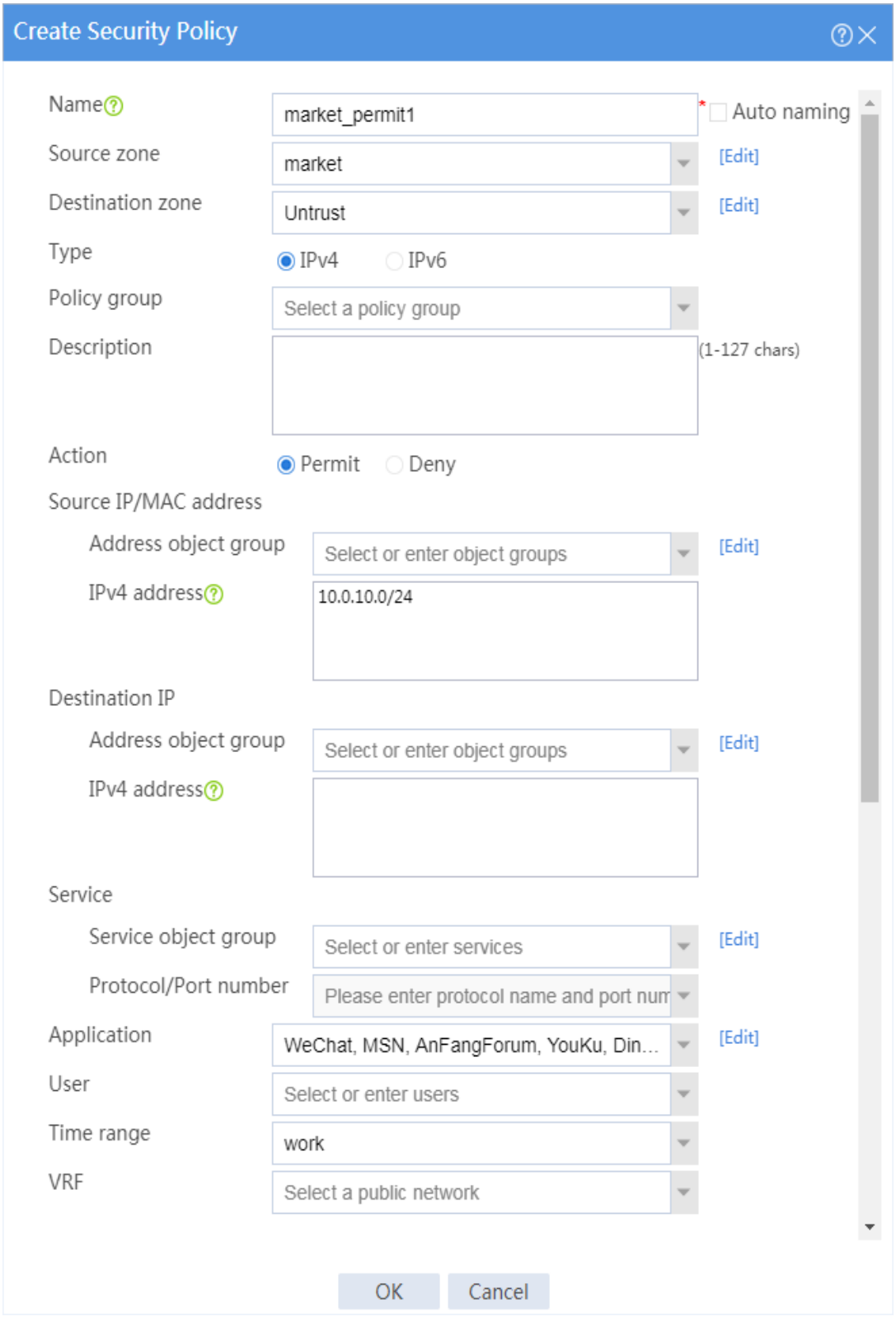
   # Click **Create**.

   # In the dialog box that appears, configure the security policy:

- Enter policy name **market_permit1**.
- Select source zone **market**.
- Select destination zone **Untrust**.
- Select policy type **IPv4**.
- Select action **Permit**.
- Select source IP address **market**.
- Select applications **WeChat**, **MSN**, **AnFang Forum** (security forum), and **YouKu**.
- Select time range **work**.

Click **OK**.

Figure 5 Creating security policy market_permit1



8. Configure a security policy named **market_deny1**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

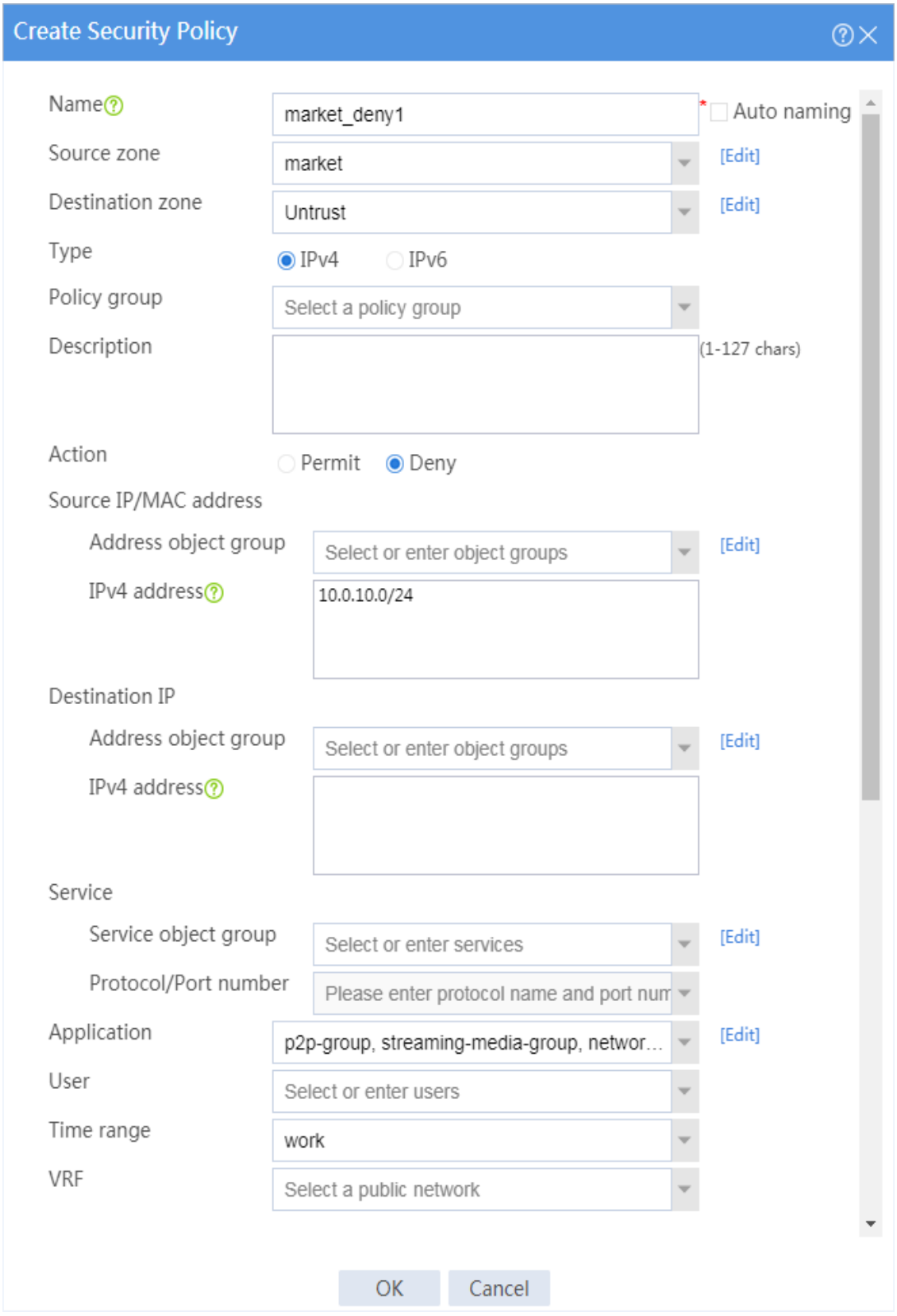
   # Click **Create**.

   # In the dialog box that appears, configure the security policy:

   - Enter policy name **market_deny1**.
   - Select source zone **market**.
   - Select destination zone **Untrust**.
   - Select policy type **IPv4**.
   - Select action **Permit**.
   - Select source IP address **market**.
   - Select application groups **p2p-group**, **streaming-media-group**, **network-community-group**, and **game-group**.
   - Select time range **work**.

   # Click **OK**.

Figure 6 Creating security policy market_deny1



9. Configure a security policy named **market_permit2**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

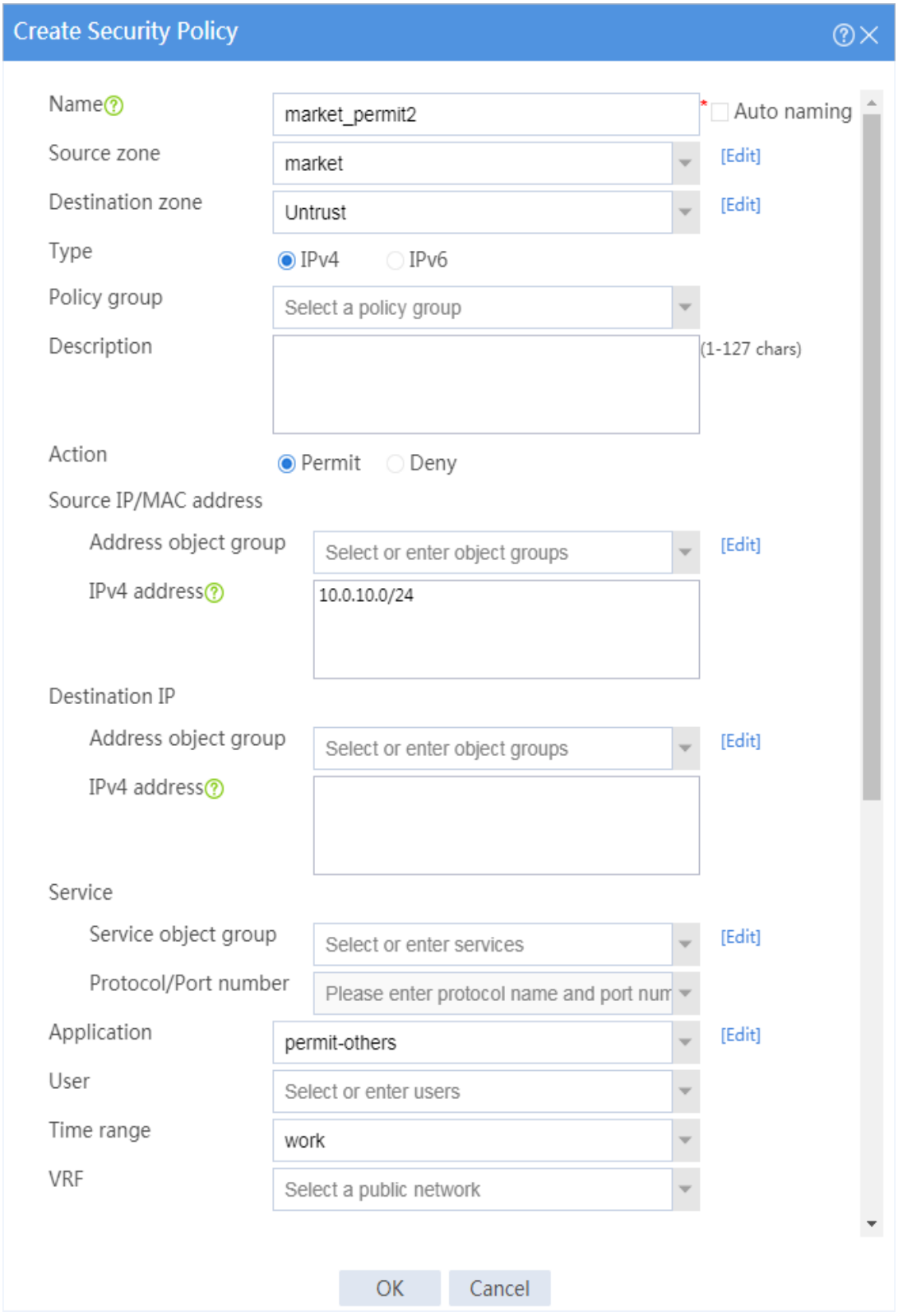
Click **Create**.

In the dialog box that appears, configure the security policy:

- Enter policy name **market_permit2**.
- Select source zone **market**.
- Select destination zone **Untrust**.
- Select policy type **IPv4**.
- Select action **Permit**.
- Select source IP address **market**.
- Select application group **permit-others**.
- Select time range **work**.

Click **OK**.

Figure 7 Creating security policy market_permit2



10. Configure a security policy named **market_permit3**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

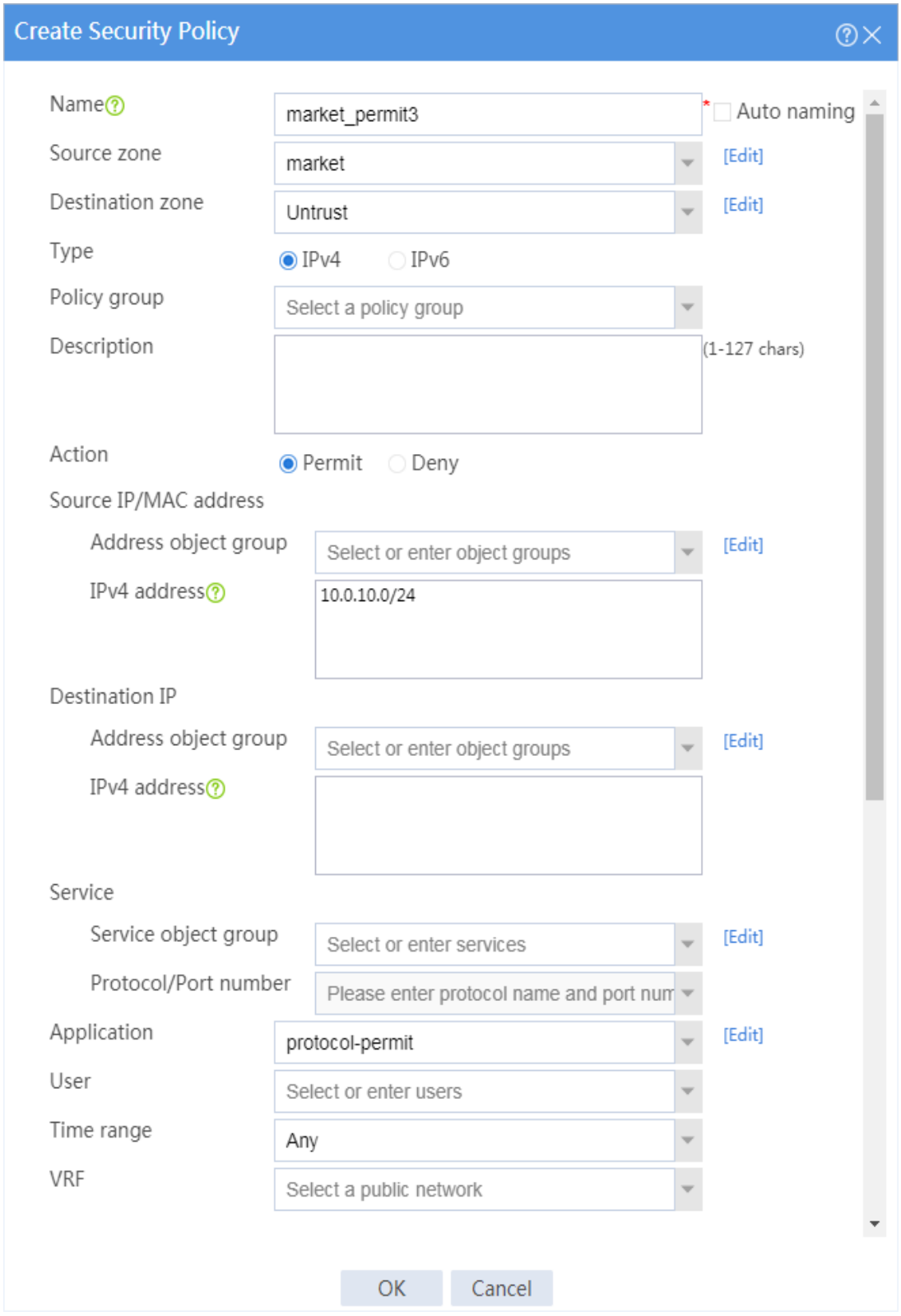
Click **Create**.

In the dialog box that appears, configure the security policy:

- Enter policy name **market_permit3**.
- Select source zone **market**.
- Select destination zone **Untrust**.
- Select policy type **IPv4**.
- Select action **Permit**.
- Select source IP address **market**.
- Select application group **protocol-permit**.

Click **OK**.

Figure 8 Creating security policy market_permit3



Verifying the configuration

Verify that the employees in the president office can freely access any network resources.

Verify that the employees in the financial office can communicate with one another.

Verify that the marketing office can access some resources on the Internet from 8:00 to 18:00 on workdays.

- Cannot access gaming, streaming media, P2P, or network community resources, but can access YouKu.
- Can only access WeChat and cannot access any other IM applications.
- Can access MSN, DingTalk, and security forum resources.
- Can access any resources except the listed resources that cannot be accessed.

Verify that the financial office cannot be accessed by anyone, and the financial office and the marketing office cannot access each other.

Verify that security polices can be hit correctly by selecting **Monitor** > **Security Logs** > **Security Policy Logs**. The following are examples of security policy hitting:

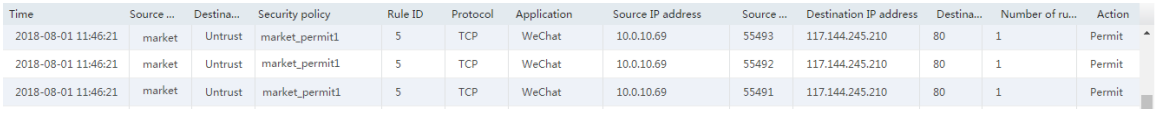
Figure 9 Denying Xunleikankan

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:16:42	market	Untrust	market_deny1	1	TCP	XunLeiKanKan	10.0.10.69	49558	183.251.28.253	80	1	Deny

Figure 10 Permitting YouKu

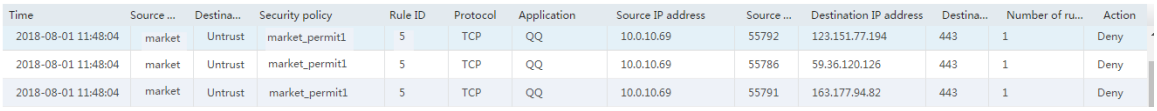
Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 14:24:59	market	Untrust	market_permit1	3	TCP	YouKu	10.0.10.69	50013	106.11.208.145	443	1	Permit

Figure 11 Permitting WeChat



Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:46:21	market	Untrust	market_permit1	5	TCP	WeChat	10.0.10.69	55493	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	market	Untrust	market_permit1	5	TCP	WeChat	10.0.10.69	55492	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	market	Untrust	market_permit1	5	TCP	WeChat	10.0.10.69	55491	117.144.245.210	80	1	Permit

Figure 12 Denying QQ



Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:48:04	market	Untrust	market_permit1	5	TCP	QQ	10.0.10.69	55792	123.151.77.194	443	1	Deny
2018-08-01 11:48:04	market	Untrust	market_permit1	5	TCP	QQ	10.0.10.69	55786	59.36.120.126	443	1	Deny
2018-08-01 11:48:04	market	Untrust	market_permit1	5	TCP	QQ	10.0.10.69	55791	163.177.94.82	443	1	Deny

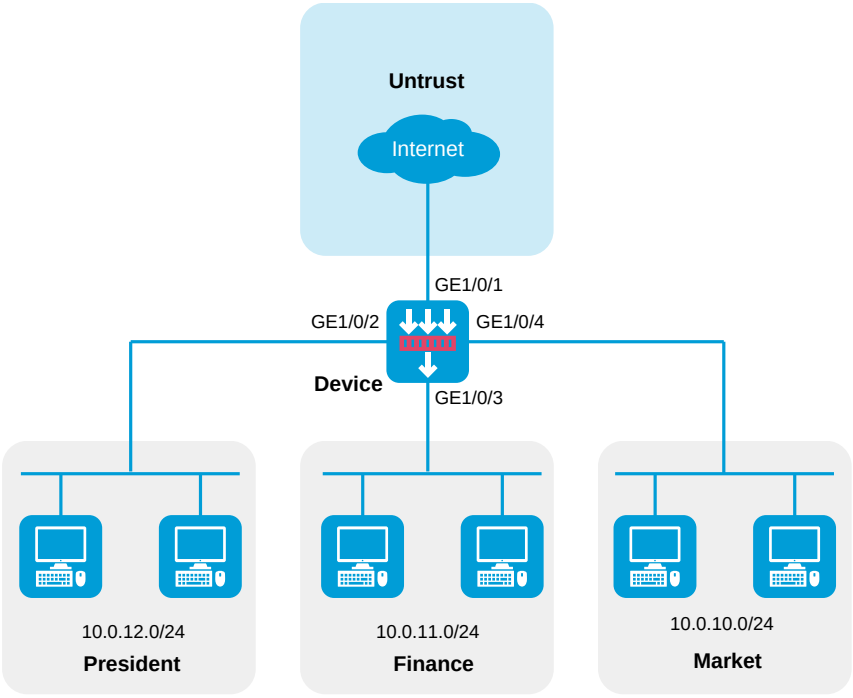
Example: Configuring APR-based, loose security policies

Network configuration

As shown in Figure 13, configure security policies to achieve the following goals:

- The president office can access all network resources at any time.
- The financial office can access only its own resources.
- The marketing office can access all network resources except video and game applications from 8:00 to 18:00 on workdays and can play games and watch video during non-working hours.

Figure 13 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

When you configure a security policy, follow these restrictions and guidelines:

- Update the APR signature library to the latest version.
- For the applications in a security policy to be identified, you must allow the dependent protocols of the applications to pass through.

Analysis

- Configure security policy **finance_permit** to allow the employees in the financial office to communicate with one another.
- Configure security policy **market_deny1** to deny game and streaming video applications for the marketing office from 8:00 to 18:00 on workdays. This security policy prevents employees in the marketing office from playing games and watching video from 8:00 to 18:00 on workdays.
- Configure security policy **president_market_permit** to allow packets from the president office and the marketing office to pass through. This security policy can meet the following requirements:
    - The president office can access all network resources at any time.
    - The marketing office can access all network resources except video and game applications from 8:00 to 18:00 on workdays and can play games and watch video during non-working hours.
- Configure the security policies in the following order:
    a. **finance_permit**
    b. **market_deny1**
    c. **president_market_permit**

Procedure

1. Configure security zones.

On the top navigation bar, click **Network**.

From the navigation pane, click **Security Zones**.

Click the **Edit** icon for security zone **Untrust**.

In the dialog box that opens, add GE 1/0/1 to the security zone.

Create a security zone named **president**, and add GE 1/0/2 to the security zone.

Create a security zone named **finance**, and add GE 1/0/3 to the security zone.

Create a security zone named **market**, and add GE 1/0/4 to the security zone.

2. Assign IP addresses to interfaces.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.2.2.1/24.

b. Click **OK**.

Configure the IP addresses of GE 1/0/2, GE 1/0/3, and GE 1/0/4 as 10.0.12.1/24, 10.0.11.1/24, and 10.0.10.1/24, respectively, in the same way you configure GE 1/0/1.

3. Configure a time range.

On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **Time Ranges**.

Click **Create**.

In the dialog box that opens, configure the time range:

a. Enter a time range name. In this example, enter **work**.

b. Create a periodic time range from 8:00 to 18:00 on workdays, and click **OK**.

c. Click **OK**.

4. Configure application groups.

On the top navigation bar, click **Objects**.

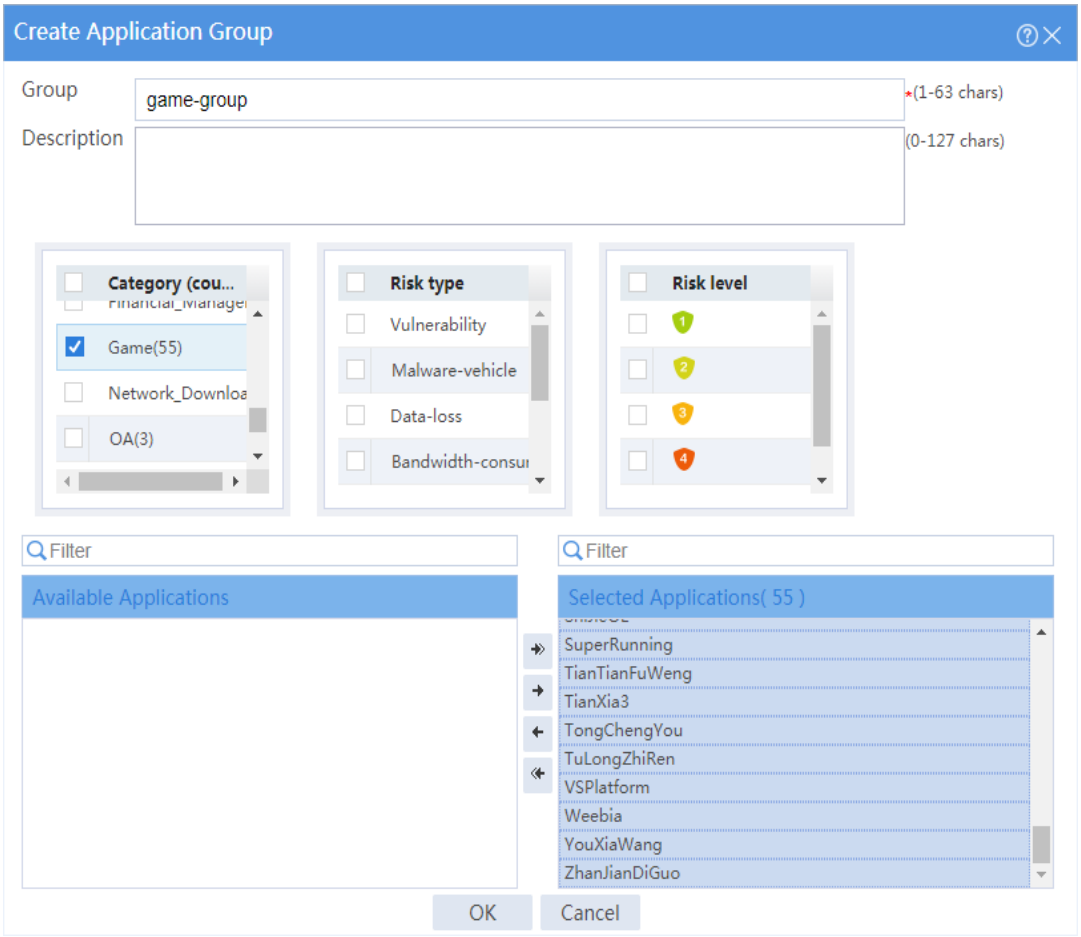
From the navigation pane, select **APPSecurity** > **APP Recognition** > **Application Groups**.

Click **Create**.

In the dialog box that opens, configure an application group named **game-group**:

- Enter group name **game-group**.
- Add all applications in the **Game** category to the **Selected Applications** pane.
- Click **OK**.

Figure 14 Creating application group game-group



Create an application group named **p2p-group**, and add all applications in the **P2P** category to the application group.

Create an application group named **streaming-media-group**, and add all applications in the **Streaming_Media** category to the application group.

Create an application group named **network-community-group**, and add all applications in the **Network-Community** category to the application group.

5. Configure a security policy named **finance_permit**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

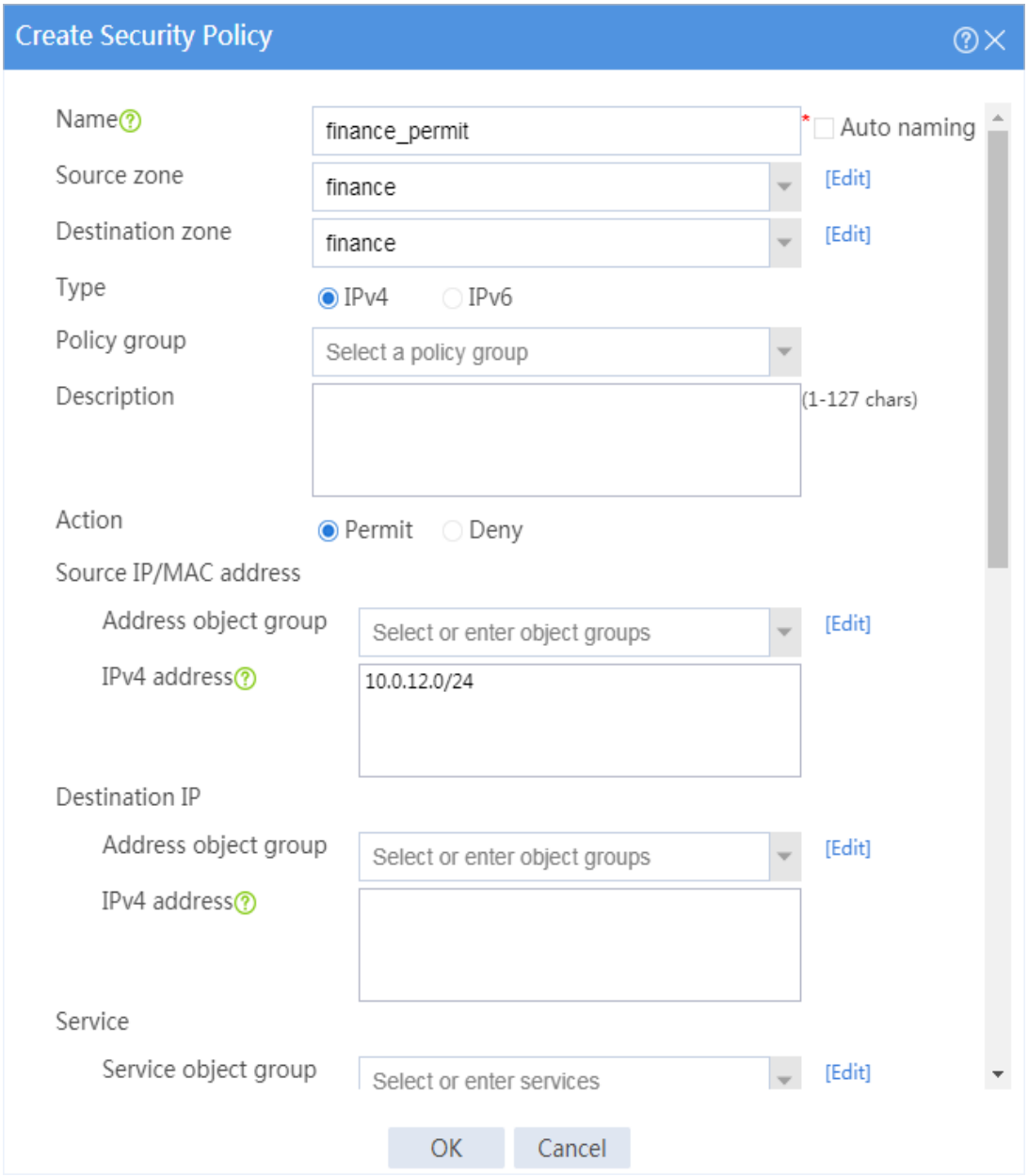
Click **Create**.

In the dialog box that appears, configure the security policy:

- Enter policy name **finance_permit**.
- Select source zone **finance**.
- Select destination zone **finance**.
- Select policy type **IPv4**.
- Select action **Permit**.

Click **OK**.

Figure 15 Creating security policy finance_permit



6. Configure a security policy named **market_deny1**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

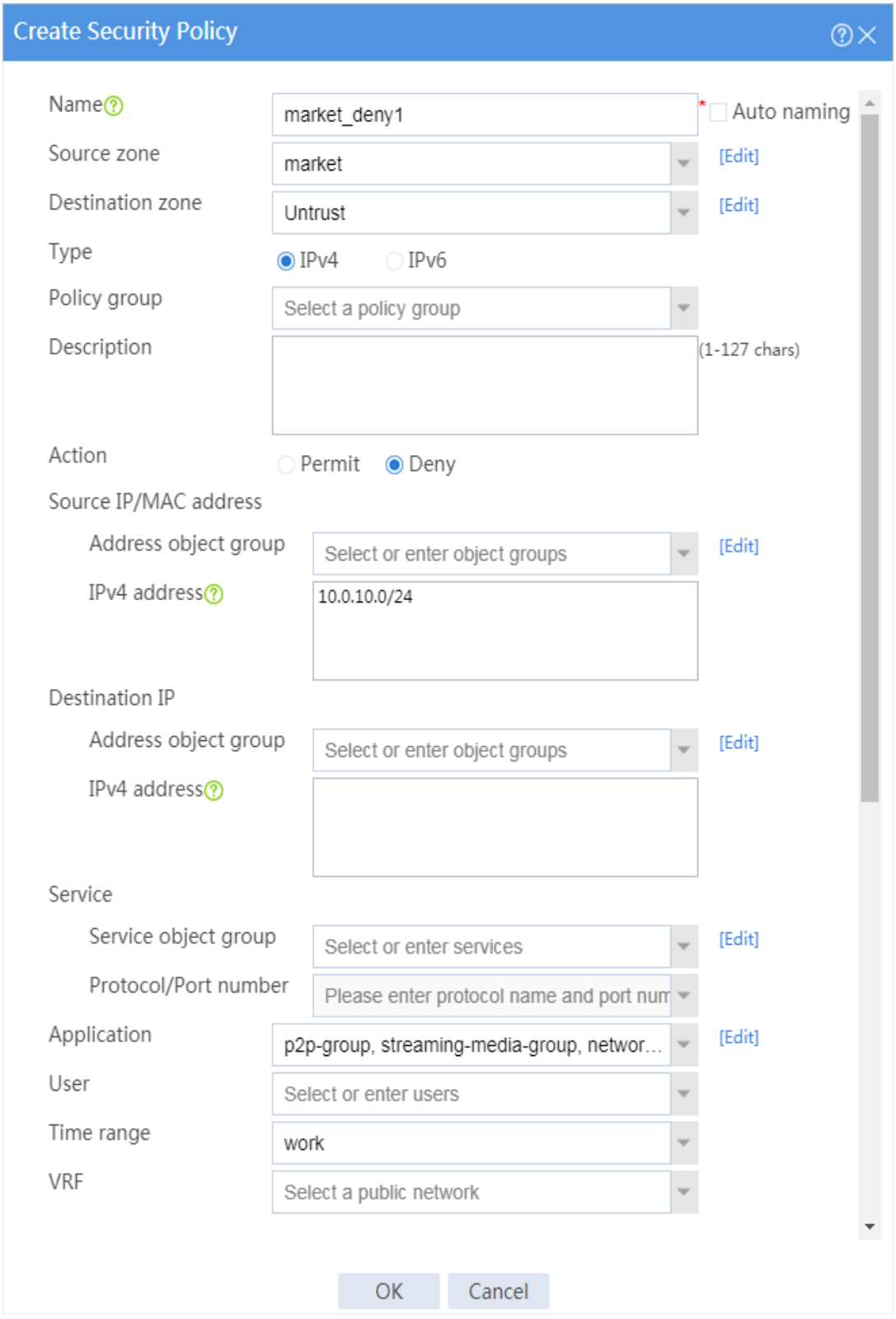
   # Click **Create**.

   # In the dialog box that appears, configure the security policy:

- Enter policy name **market_deny1**.
- Select source zone **market**.
- Select destination zone **Untrust**.
- Select policy type **IPv4**.
- Select action **Deny**.
- Select source IP address **market**.
- Select application groups **p2p-group**, **streaming-media-group**, **network-community-group**, and **game-group**.
- Select time range **work**.

Click **OK**.

Figure 16 Creating security policy market_deny1



7. Configure a security policy named **president_market_permit**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

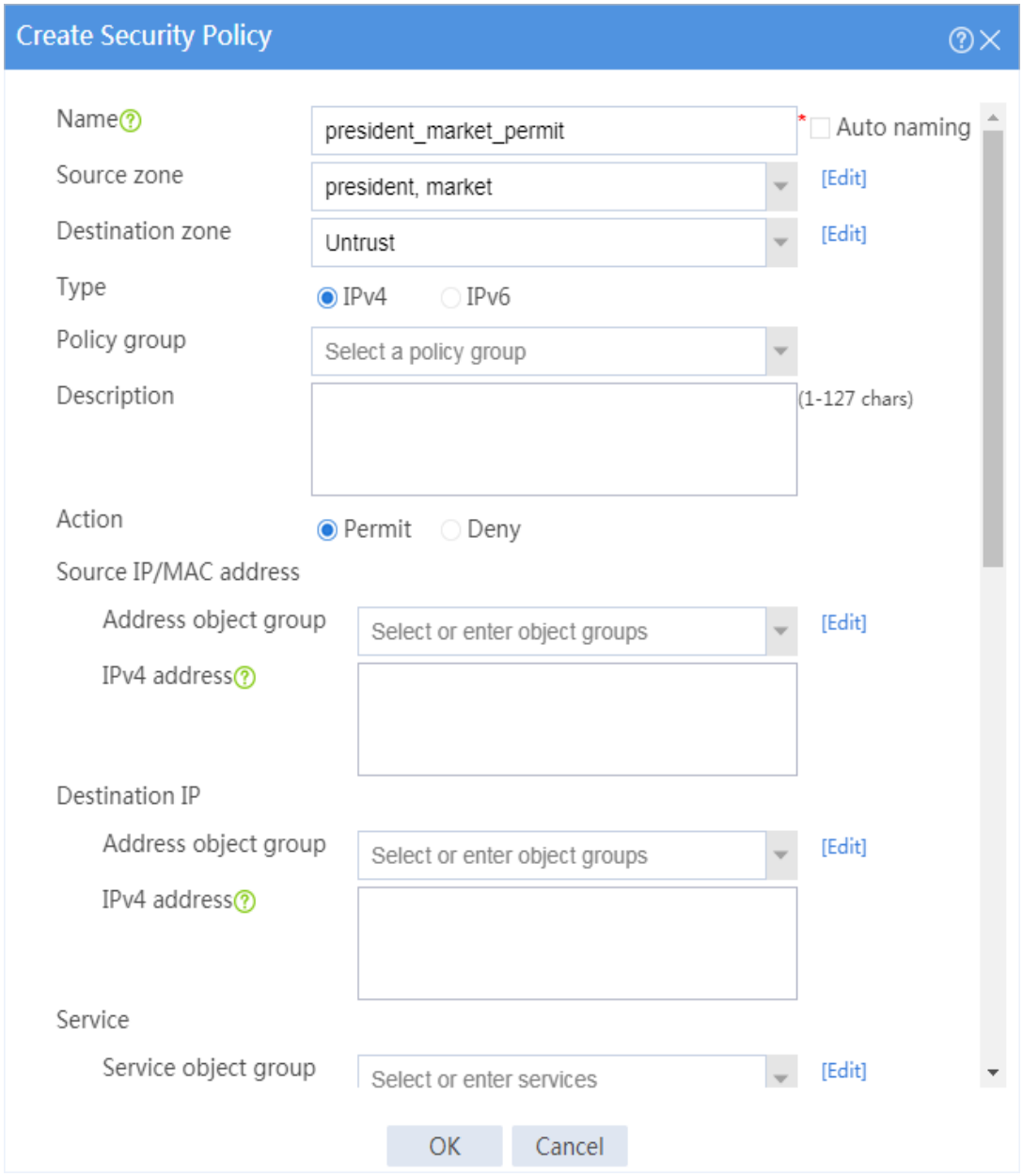
   # Click **Create**.

   # In the dialog box that appears, configure the security policy:

   - Enter policy name **president_market_permit**.
   - Select policy type **IPv4**.
   - Select action **Permit**.

   # Click **OK**.

Figure 17 Creating security policy president_market_permit



Verifying the configuration

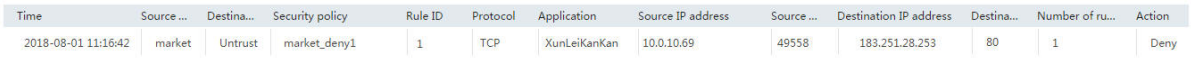
Verify that the employees in the president office can freely access any network resources.

Verify that the employees in the financial office can communicate with one another.

Verify that the marketing office can access all network resources except video and game applications from 8:00 to 18:00 on workdays and can play games and watch video during non-working hours.

Verify that security polices can be hit correctly by selecting **Monitor** > **Security Logs** > **Security Policy Logs**. The following are examples of security policy hitting:

Figure 18 Denying Xunleikankan



Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:16:42	market	Untrust	market_deny1	1	TCP	XunLeiKanKan	10.0.10.69	49558	183.251.28.253	80	1	Deny

Figure 19 Permitting WeChat

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:46:21	Any	Any	president_market_permit	2	TCP	WeChat	10.0.10.69	55493	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	Any	Any	president_market_permit	2	TCP	WeChat	10.0.10.69	55492	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	Any	Any	president_market_permit	2	TCP	WeChat	10.0.10.69	55491	117.144.245.210	80	1	Permit

Object group configuration examples

Contents

Introduction

The following information provides examples for configuring IPv4 address, IPv6 address, MAC address, and service object groups and time ranges.

- **IPv4 address object group**—A group of IPv4 address objects used to match the IPv4 address in a packet.
- **IPv6 address object group**—A group of IPv6 address objects used to match the IPv6 address in a packet.

- **MAC address object group**—A group of MAC address objects used to match the MAC address in a packet.
- **Service object group**—A group of service objects used to match the protocol type and protocol characteristics (such as TCP/UDP source/destination port and ICMP message type and code) in a packet.
- **Time range**—You can implement a service based on the time of the day by applying a time range to it. A time-based service takes effect only in time periods specified by the time range. If a time range does not exist, the service based on the time range does not take effect.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the object group feature.

Restrictions and guidelines

When you configure object groups, follow these restrictions and guidelines:

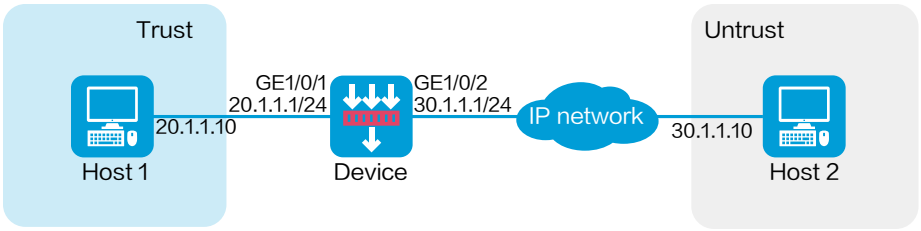
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.
- Two object groups cannot use each other at the same time.

Example: Configuring an IPv4 address object group

Network configuration

As shown in Figure 1, configure an IPv4 address object group on the device to allow Host 1 to communicate with Host 2.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 20.1.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 30.1.1.1./24 in the same way you configure GE 1/0/1.

2. Create an IPv4 address object group.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Object Groups** > **IPv4 Address Object Groups**.

   # Click **Create**.

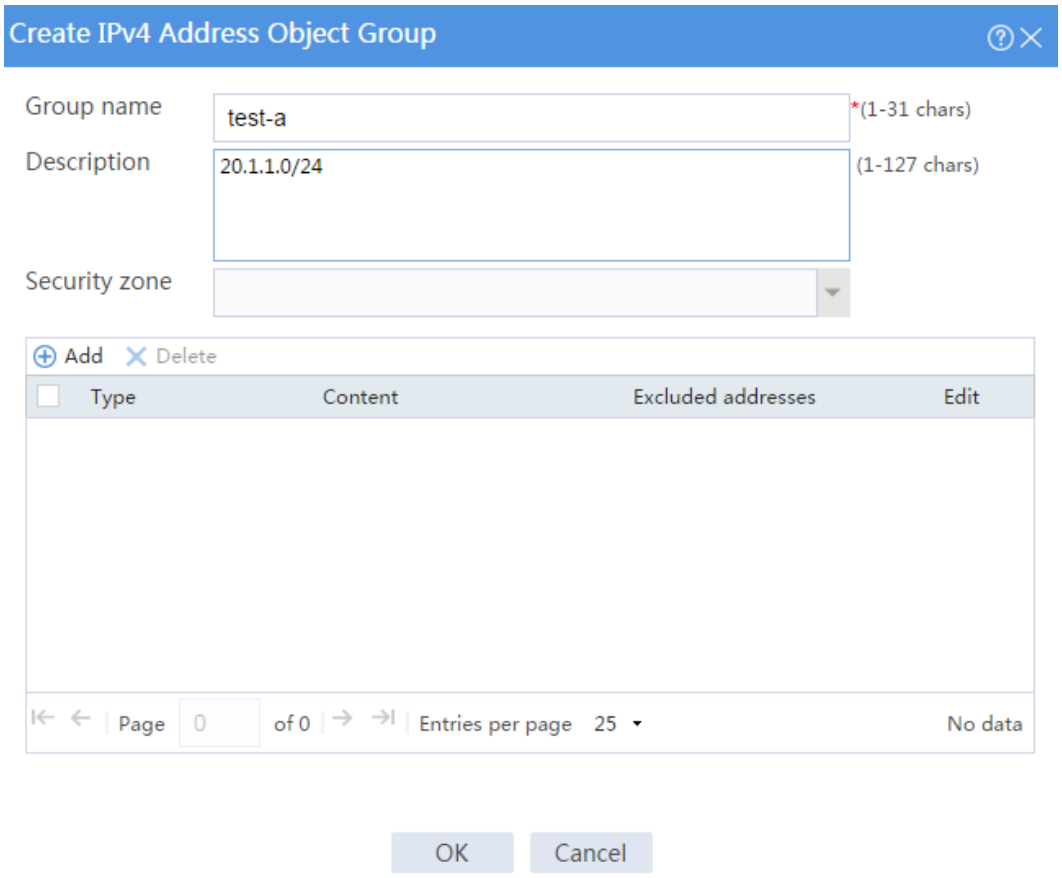
   # In the dialog box that opens, configure the IPv4 address object group:

   a. Enter a group name. In this example, enter **test-a**.

   b. Enter a description. In this example, enter **20.1.1.0/24**.

   c. Click **Add**.

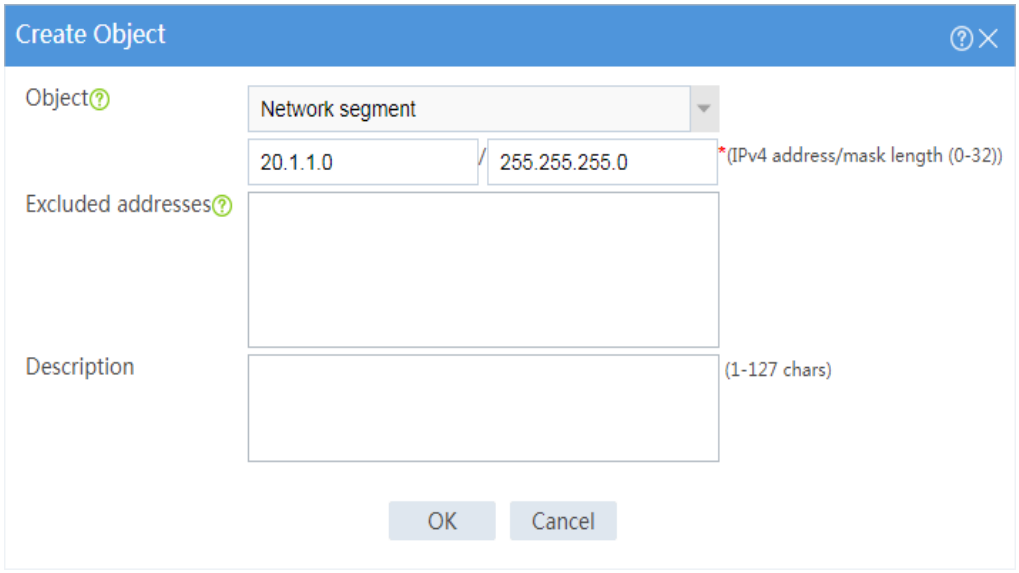
Figure 2 Create an IPv4 address object group



d. In the dialog box that opens, select the **Network segment** object, and enter the IPv4 address and mask length 20.1.1.0/24.

e. Click **OK**.

Figure 3 Create an object



f. On the **Create IPv4 Address Object Group** page, click **OK**.

3. Create a security policy from zone **Trust** to zone **Untrust**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that appears, configure a security policy:

- Enter policy name **test-a**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IP/MAC address **test-a**.

Click **OK**.

Verifying the configuration

Verify that you can ping Host 2 from Host 1 successfully.

```
C:\Users\abc> ping 30.1.1.10
```

Follow these steps to view the session information:

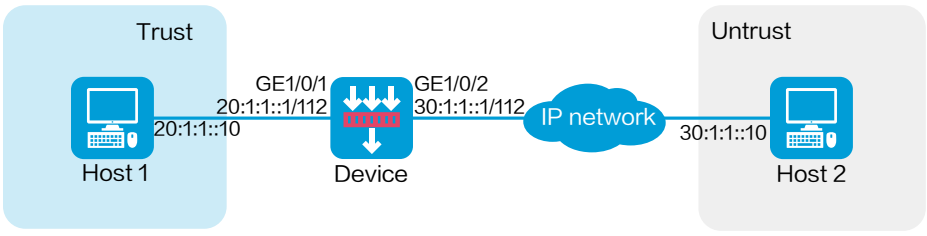
1. On the top navigation bar, click **Monitor**.
2. From the navigation pane, select **Sessions**.

Example: Configuring an IPv6 address object group

Network configuration

As shown in Figure 4, configure an IPv6 address object group on the device to allow Host 1 to communicate with Host 2.

Figure 4 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IPv6 addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv6 Address** tab, enter the IP address and mask of the interface. In this example, enter 20:1:1::1/112.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 30:1:1::1/112 in the same way you configure GE 1/0/1.

2. Create an IPv6 address object group.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Object Groups** > **IPv6 Address Object Groups**.

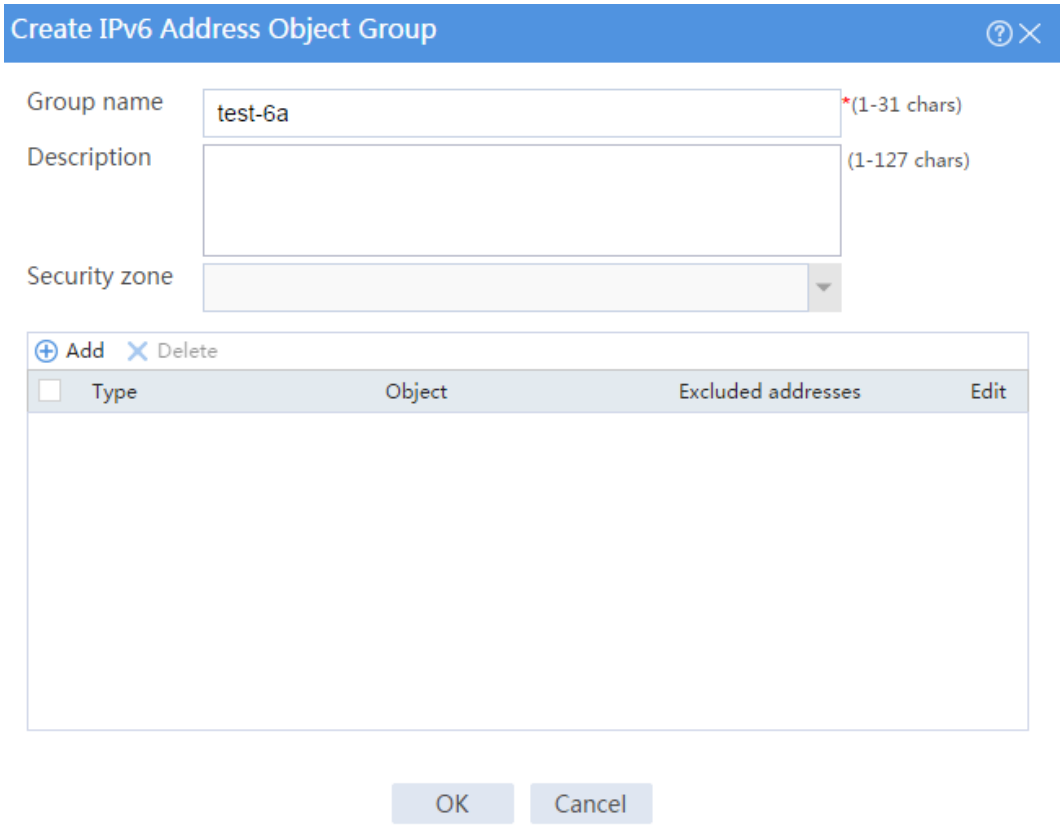
   # Click **Create**.

   # In the dialog box that opens, configure the IPv6 address object group:

   a. Enter a group name. In this example, enter **test-6a**.

b. Click **Add**.

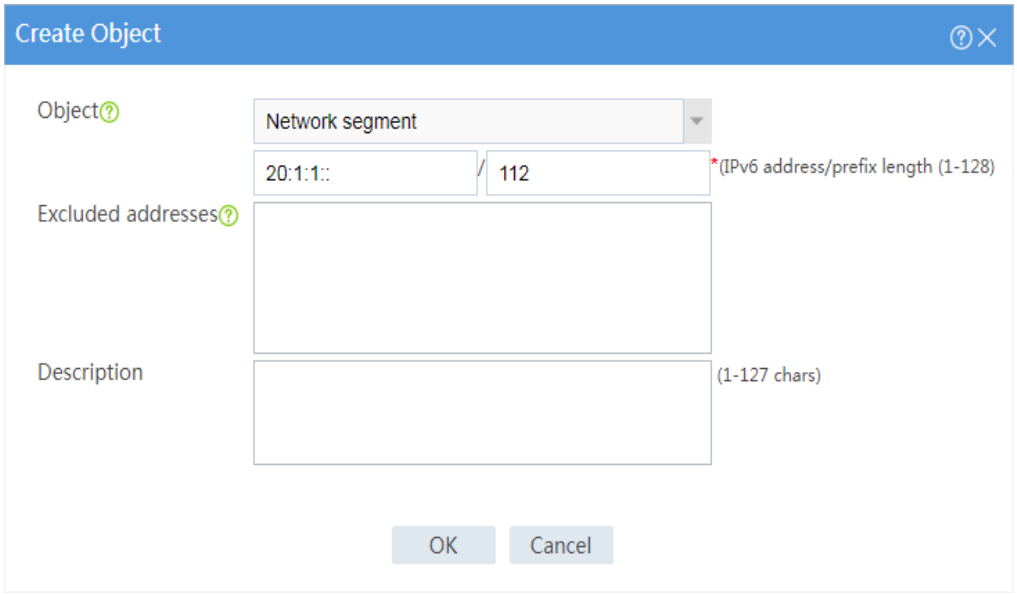
Figure 5 Create an IPv6 address object group



c. In the dialog box that opens, select the **Network segment** object, and enter the IPv6 address and prefix length 20:1:1::/112.

d. Click **OK**.

Figure 6 Create an object



e. On the **Create IPv6 Address Object Group** page, click **OK**.

3. Create a security policy from zone **Trust** to zone **Untrust**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that appears, configure a security policy:

- Enter policy name **test-6a**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv6**.
- Select action **Permit**.
- Select source IP/MAC address **test-6a**.

Click **OK**.

Verifying the configuration

Verify that you can ping Host 2 from Host 1 successfully.

```
C:\Users\abc> ping 30:1:1::10
```

Follow these steps to view the session information:

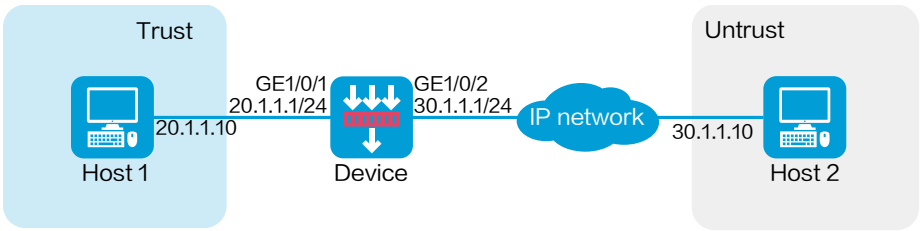
1. On the top navigation bar, click **Monitor**.
2. From the navigation pane, select **Sessions**.

Example: Configuring a MAC address object group

Network configuration

As shown in Figure 7, configure a MAC address object group on the device to allow Host 1 to communicate with Host 2. The MAC address of Host 1 is 3C-52-82-72-03-1F.

Figure 7 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 20.1.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 30.1.1.1/24 in the same way you configure GE 1/0/1.

2. Create a MAC address object group.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Object Groups** > **MAC Address Object Groups**.

   # Click **Create**.

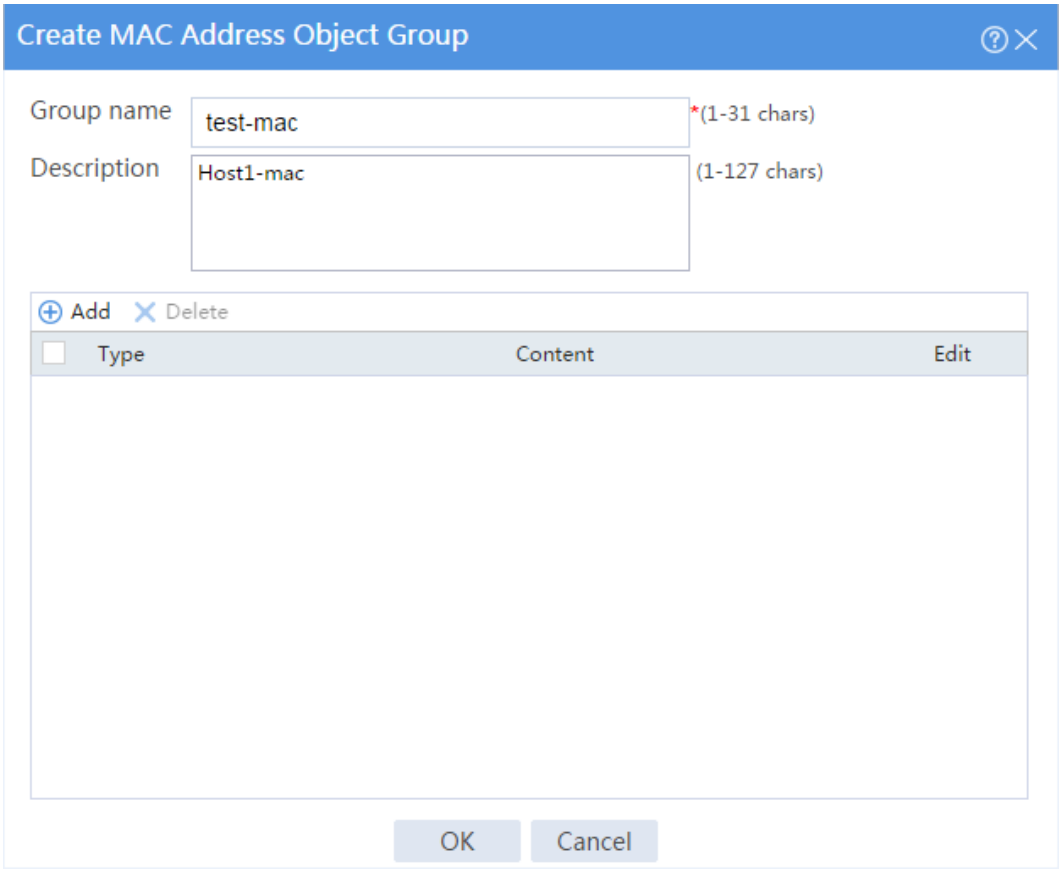
   # In the dialog box that opens, configure the MAC address object group:

   a. Enter a group name. In this example, enter **test-mac**.

b. Enter a description. In this example, enter **Host1-mac**.

c. Click **Add**.

Figure 8 Create a MAC address object group

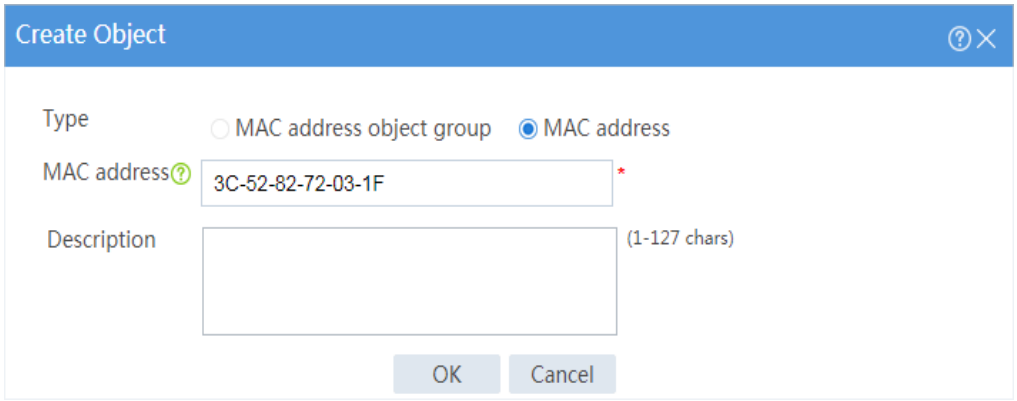


d. In the dialog box that opens, configure a MAC address object.

- Select type **MAC address**.
- Enter MAC address **3C-52-82-72-03-1F**.

e. Click **OK**.

Figure 9 Create an object



f. On the **Create MAC Address Object Group** page, click **OK**.

3. Create a security policy from zone **Trust** to zone **Untrust**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that appears, configure a security policy:

- Enter policy name **test-mac**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IP/MAC address **test-mac**.

Click **OK**.

Verifying the configuration

Verify that you can ping Host 2 from Host 1 successfully.

```
C:\Users\abc> ping 30.1.1.10
```

Follow these steps to view the session information:

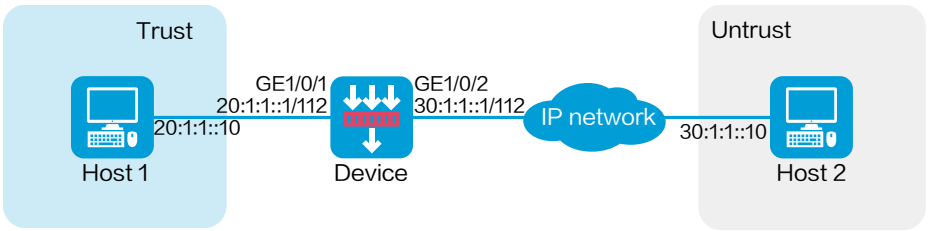
1. On the top navigation bar, click **Monitor**.
2. From the navigation pane, select **Sessions**.

Example: Configuring a service object group

Network configuration

As shown in Figure 10, configure a service object group on the device to allow Host 1 to communicate with Host 2 through ICMPv6.

Figure 10 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IPv6 addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv6 Address** tab, enter the IP address and mask of the interface. In this example, enter 20:1:1::1/112.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 30:1:1::1/112 in the same way you configure GE 1/0/1.

2. Create a service object group.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Object Groups** > **Service Object Groups**.

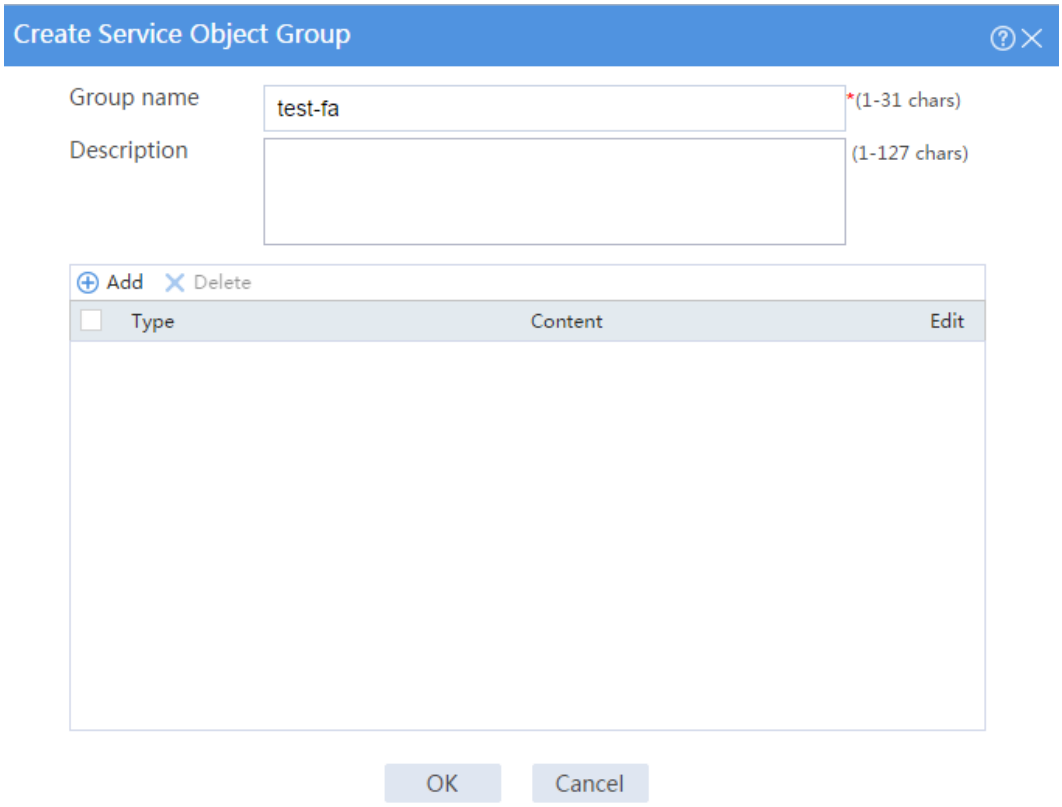
   # Click **Create**.

   # In the dialog box that opens, configure the service object group:

   a. Enter a group name. In this example, enter **test-fa**.

b. Click **Add**.

Figure 11 Create a service object group

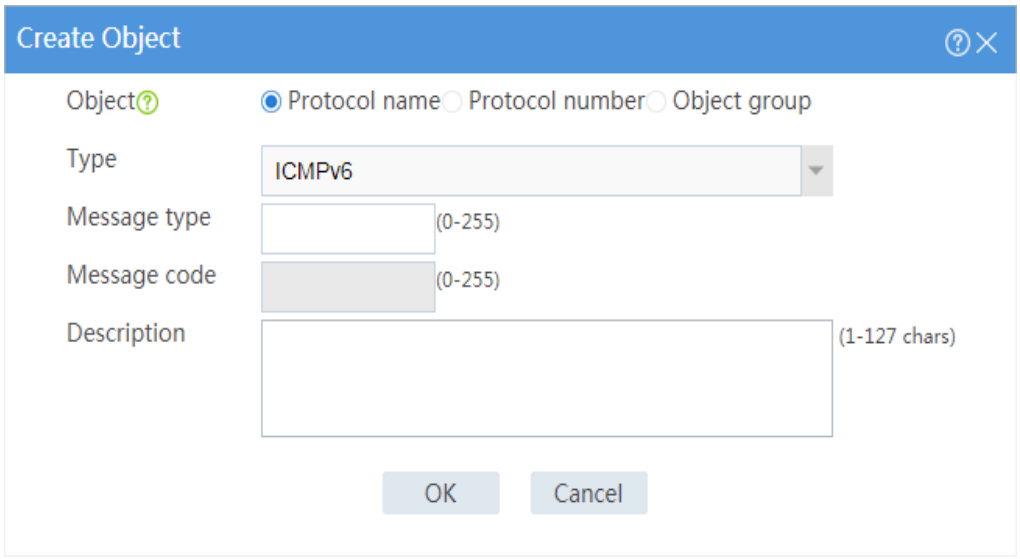


c. In the dialog box that opens, configure a service object.

- Select object **Protocol name**.
- Select type **ICMPv6**.

d. Click **OK**.

Figure 12 Create an object



e. On the **Create Service Object Group** page, click **OK**.

3. Create a security policy from zone **Trust** to zone **Untrust**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that appears, configure a security policy:

- Enter policy name **test-fa**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv6**.
- Select action **Permit**.
- Select service **test-fa**.

Click **OK**.

Verifying the configuration

Verify that you can ping Host 2 from Host 1 successfully.

```
C:\Users\abc> ping 30:1:1::10
```

Follow these steps to view the session information:

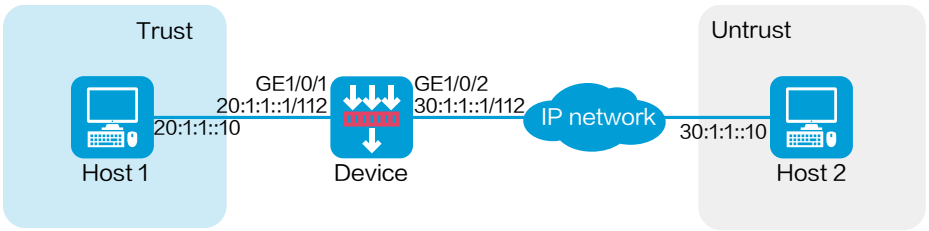
1. On the top navigation bar, click **Monitor**.
2. From the navigation pane, select **Sessions**.

Example: Configuring a time range

Network configuration

As shown in Figure 13, configure a service object group on the device to allow Host 1 to communicate with Host 2 through ICMPv6 in a specific time period.

Figure 13 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IPv6 addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv6 Address** tab, enter the IP address and mask of the interface. In this example, enter 20:1:1::1/112.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 30:1:1::1/112 in the same way you configure GE 1/0/1.

2. Create a service object group.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Object Groups** > **Service Object Groups**.

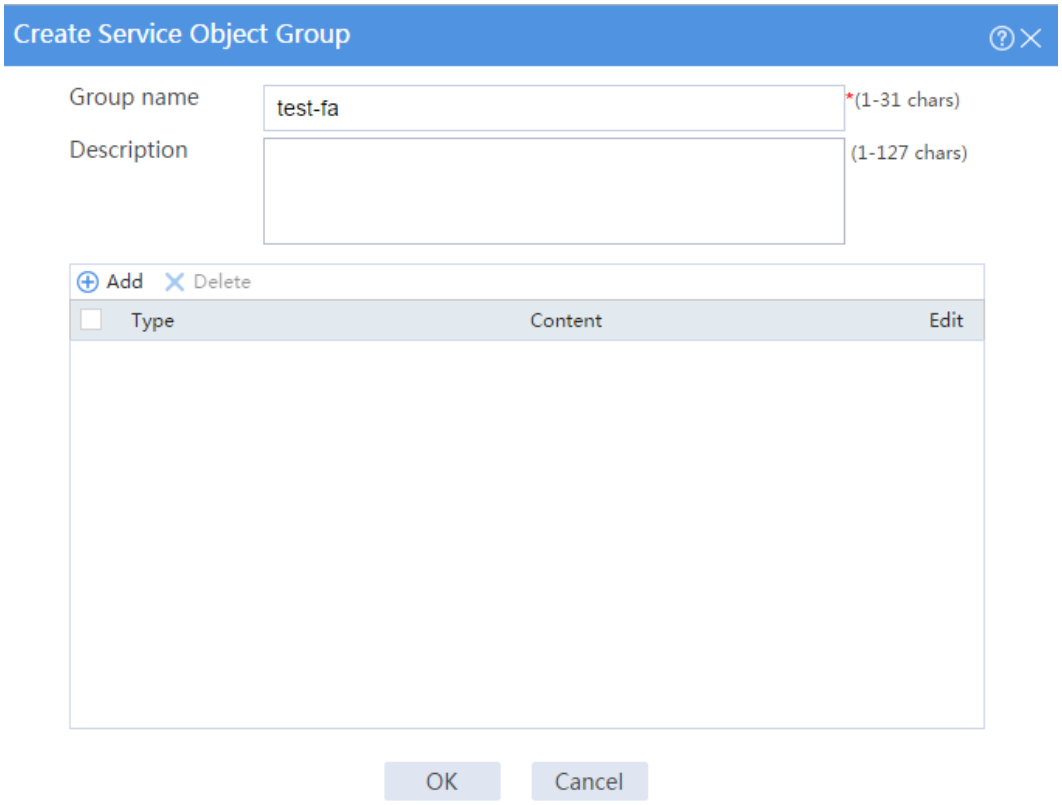
   # Click **Create**.

   # In the dialog box that opens, configure the service object group:

   a. Enter a group name. In this example, enter **test-fa**.

b. Click **Add**.

Figure 14 Create a service object group

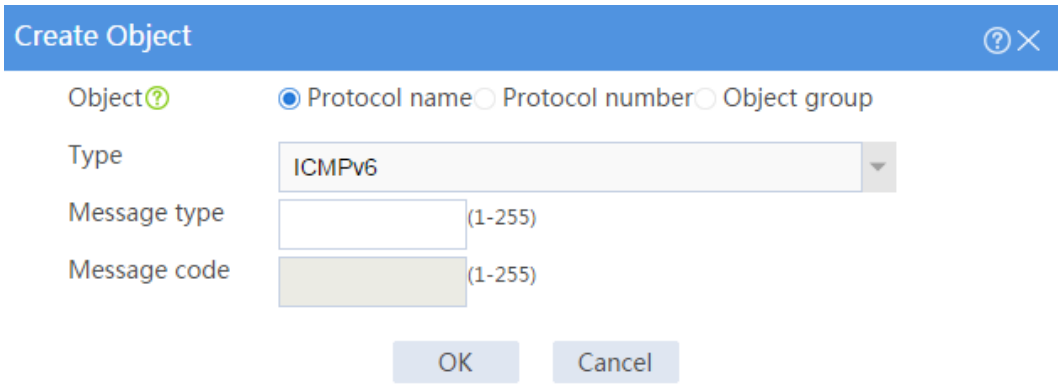


c. In the dialog box that opens, configure a service object.

- Select object **Protocol name**.
- Select type **ICMPv6**.

d. Click **OK**.

Figure 15 Create an object



e. On the **Create Service Object Group** page, click **OK**.

3. Create a time range.

On the top navigation bar, click **Object**.

From the navigation pane, select **Object Groups** > **Time Ranges**.

Click **Create**.

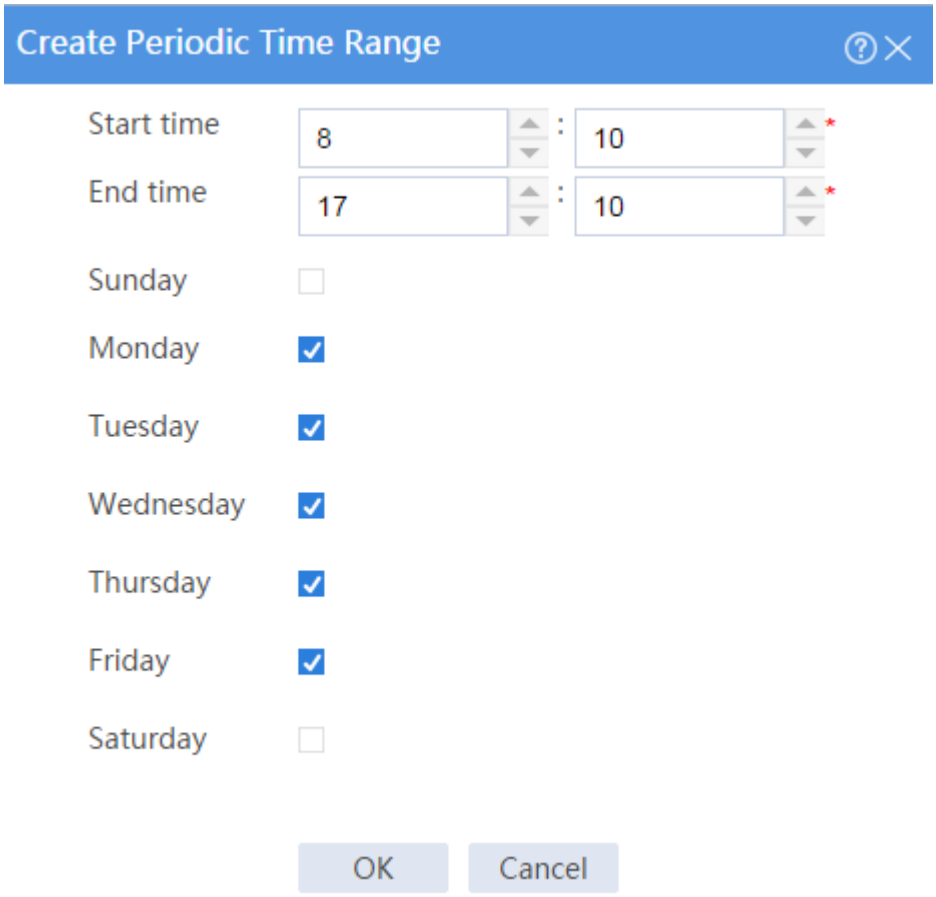
In the dialog box that appears, enter name **test-time** and then click **Create** for **Periodic time range**.

In the dialog box that appears, configure the time range:

- Set the start time to **08:10**.
- Set the end time to **17:10**.
- Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, and **Friday**.

Click **OK**.

Figure 16 Configure a time range



In the **Create Time Range** page, click **OK**.

4. Create a security policy from zone **Trust** to zone **Untrust**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that appears, configure a security policy:

   - Enter policy name **test-time**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.

- Select type **IPv6**.
- Select action **Permit**.
- Select service **test-fa**.
- Select time range **test-time**.

Click **OK**.

Verifying the configuration

Verify that you can ping Host 2 from Host 1 successfully in the time period specified by the time range.

```
C:\Users\abc> ping 30:1:1::10
```

Verify that you cannot ping Host 2 from Host 1 and the corresponding session does not exist at any time beyond the time period specified by the time range.

User identification configuration examples

Contents

Introduction

The following information provides user identification configuration examples.

The user identification feature identifies users by IP addresses. This feature works with other security features to control network access on a per-user basis.

The feature enables the device to perform the following tasks:

- Implements security policies on a per-user basis to improve the policy usability.
- Collects statistics and analysis for network attack behaviors and traffic flow on a per-user basis to track the user network access behaviors in real time.

- Implements policy control regardless of changes to the user IP addresses.

The RADIUS single sign-on service enables a RADIUS server to synchronize user identity information (for example, the username and IP address) to a security device (for example, a firewall) so the users can access the network without having to authenticate with the device after they pass authentication with the RADIUS server.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the portal, AAA, user identification, and security policy features.

General restrictions and guidelines

When you configure security policies and packet filtering policies, make sure they can take effect as you expected. Security policies process packets prior to packet filtering policies. Packet filtering policies will not process the packets that have matched security policies.

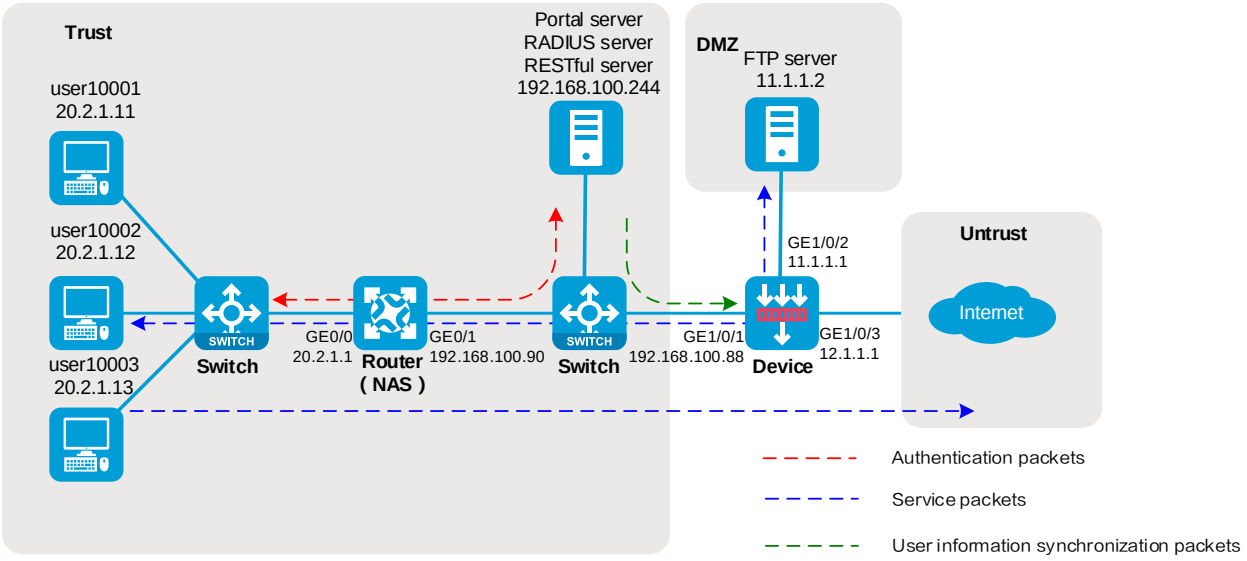
Example: Configuring user identification for portal users that pass RADIUS authentication (RADIUS single sign-on)

Network configuration

As shown in Figure 1:

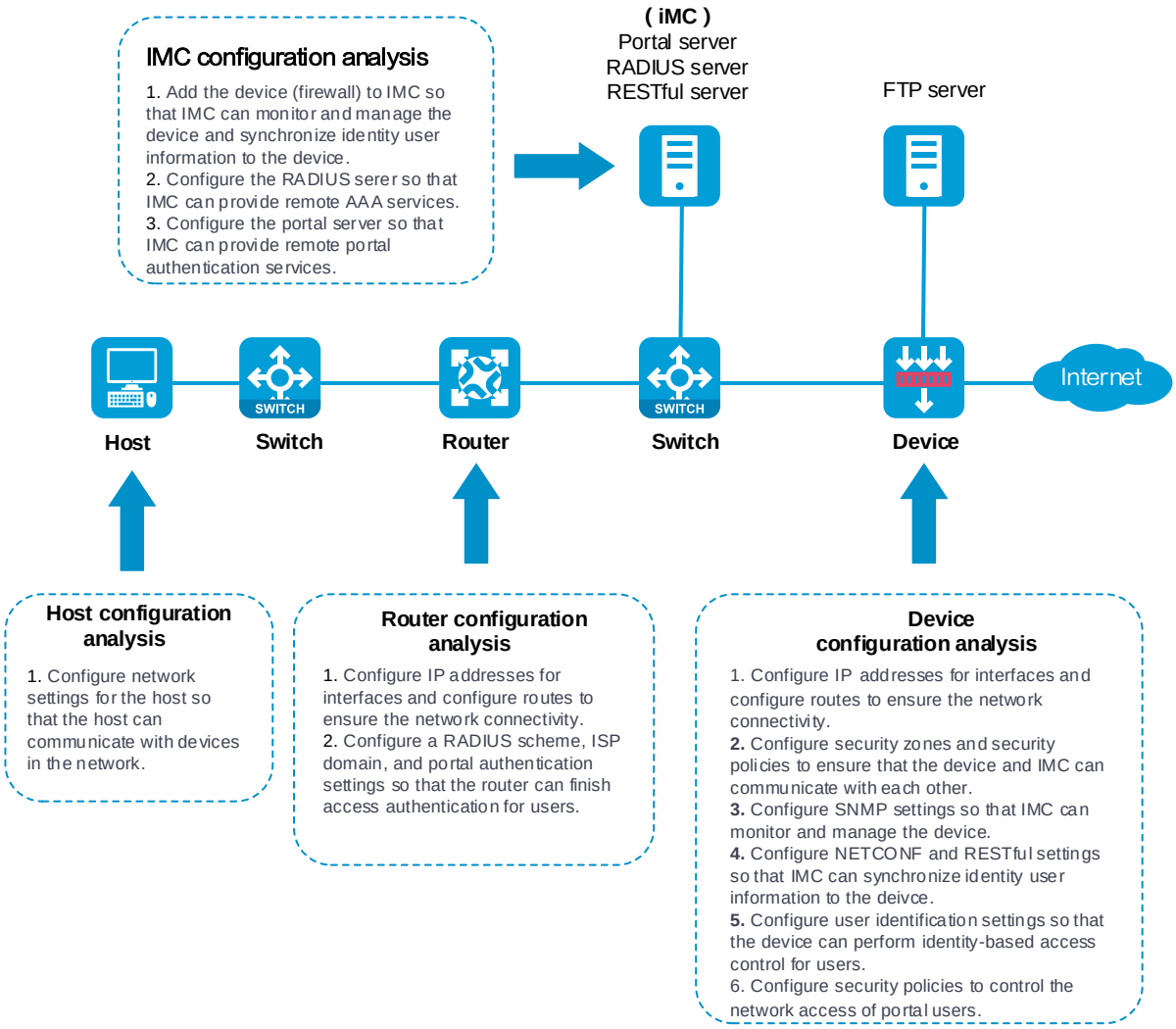
- Users **user10001**, **user10002**, and **user10003** use static IP addresses, and they must pass portal authentication to access the network.
- The router acts as a NAS for the users to access the network. The NAS uses the RADIUS server to authenticate the users.
- The RADIUS server is installed with IMC components. For portal authentication, the server acts as both the portal authentication server and portal Web server.
- The RESTful server stores user account information. The server can synchronize user identity information to Device.
- Device is a firewall. The users can access the network without having to authenticate with the firewall after they pass authentication with the RADIUS server.
- The firewall performs the following identity-based access control on the users that have passed portal authentication:
  - User **user10001** cannot access the FTP server or Internet.
  - User **user10002** can access the FTP server but cannot access the Internet.
  - User **user10003** can access the Internet but cannot access the FTP server.
  - Users from the Internet cannot access the hosts in the **Trust** and **DMZ** security zones.

Figure 1 Network diagram



Analysis

Figure 2 Analysis diagram



Software versions used

This configuration example was created and verified on the following software versions:

- R8560 of the NFNX3-HDB3080 device.
- Version 7.1.064, ESS 0701 of the MSR26-30 router.

The RADIUS and portal server is installed with IMC PLAT 7.3 (E0606), IMC UAM 7.3 (E0503), IMC CAMS 7.3 (E0501), and IMC EIA 7.3 (E0512).

Restrictions and guidelines

An IMC server logs off an online user only after it receives an accounting-stop request for that user. For the NAS to send accounting-stop requests to the server, you need to configure accounting settings in the authentication domain of the user on the NAS. However, you do not need to configure accounting parameters on the IMC server since accounting is not required.

Procedure

Configuring the router

Configuring IP addresses for interfaces and a default route to ensure the network connectivity of the router

Assign IP address 20.2.1.1 to GigabitEthernet 0/0.

```
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ip address 20.2.1.1 255.255.255.0
[Router-GigabitEthernet0/0] quit
```

Assign IP address 192.168.100.90 to GigabitEthernet 0/1.

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] ip address 192.168.100.90 255.255.255.0
[Router-GigabitEthernet0/1] quit
```

Configure a default route to ensure that the router can reach the FTP server and the Internet.

```
[Router] ip route-static 0.0.0.0 0.0.0.0 192.168.100.88
```

Configuring SNMP for the IMC server to monitor and manage the router

Enable the SNMP agent.

```
[Router] snmp-agent
```

Enable all SNMP versions, and create the read-only community **public** and the read and write community **private**.

```
[Router] snmp-agent sys-info version all
[Router] snmp-agent community read public
[Router] snmp-agent community write private
```

Configuring a RADIUS scheme

Create a RADIUS scheme named **rs1** and enter its view.

```
[Router] radius scheme rs1
```

Specify the server at 192.168.100.244 as the primary authentication server and the primary accounting server, and set the authentication shared key to **admin** in plaintext form for secure RADIUS communication.

```
[Router-radius-rs1] primary authentication 192.168.100.244
[Router-radius-rs1] primary accounting 192.168.100.244
[Router-radius-rs1] key authentication simple admin
```

Exclude domain names from the usernames sent to the RADIUS server.

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

Configuring an authentication domain

Create an ISP domain named **dm1** and enter its view.

```
[Router] domain dm1
```

Configure the ISP domain to use RADIUS scheme **rs1** for the authentication, authorization, and accounting of portal users.

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
```

```
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

Configuring portal authentication

Configure the portal authentication server.

```
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.100.244 key simple admin
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
```

Configure the portal Web server.

```
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.100.244:8080/portal
[Router-portal-websvr-newpt] quit
```

Enable direct portal authentication on GigabitEthernet 0/0.

```
[Router] interface gigabitethernet 0/0
[Router–GigabitEthernet0/0] portal enable method direct
```

Specify portal Web server **newpt** on GigabitEthernet 0/0.

```
[Router–GigabitEthernet0/0] portal apply web-server newpt
```

Specify domain **dm1** as the portal authentication domain on GigabitEthernet 0/0.

```
[Router–GigabitEthernet0/0] portal domain dm1
[Router–GigabitEthernet0/0] quit
```

Configuring Device (the firewall)

Configuring SNMP for the IMC server to monitor and manage the firewall

Enable the SNMP agent.

```
<Device> system-view
```

```
[Device] snmp-agent
```

Enable all SNMP versions, and create the read-only community **public** and the read and write community **private**.

```
[Device] snmp-agent sys-info version all
[Device] snmp-agent community read public
[Device] snmp-agent community write private
```

Configuring NETCONF over SOAP for the IMC server to issue configuration to the firewall

Enable NETCONF over SOAP over HTTP.

```
[Device] netconf soap http enable
```

Enable NETCONF over SOAP over HTTPS.

```
[Device] netconf soap https enable
```

Enabling RESTful for the firewall to communicate with the IMC RESTful server

Enable RESTful over HTTP.

```
[Device] restful http enable
```

Enable RESTful over HTTPS.

```
[Device] restful https enable
```

Assigning IP addresses to interfaces and adding the interfaces to security zones

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

1. Select the **Trust** security zone.
2. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 192.168.100.88/24.
3. Use the default settings for other parameters.

4. Click **OK**.

Add GE 1/0/2 to the **DMZ** security zone and set its IP address to 11.1.1.1/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Untrust** security zone and set its IP address to 12.1.1.1/24 in the same way you configure GE 1/0/1.

Configuring routing

1. Configure routes to ensure that the firewall and users can reach each other.

   This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure the IPv4 static route:

   - Enter **20.2.1.0** in the **Destination address** field.
   - Enter **24** in the **Mask length** field.
   - Enter **192.168.100.90** as the next hop address in the **Next hop** field.
   - Use the default settings for other parameters.

   # Click **OK**.

2. Configure a default route to ensure that the firewall can reach the Internet.

   This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure the IPv4 static route:

   - Enter **0.0.0.0** in the **Destination address** field.
   - Enter **0** in the **Mask length** field.
   - Enter **12.1.1.2** as the next hop address in the **Next hop** field.

- Use the default settings for other parameters.

Click **OK**.

Assigning the HTTP service to administrator admin

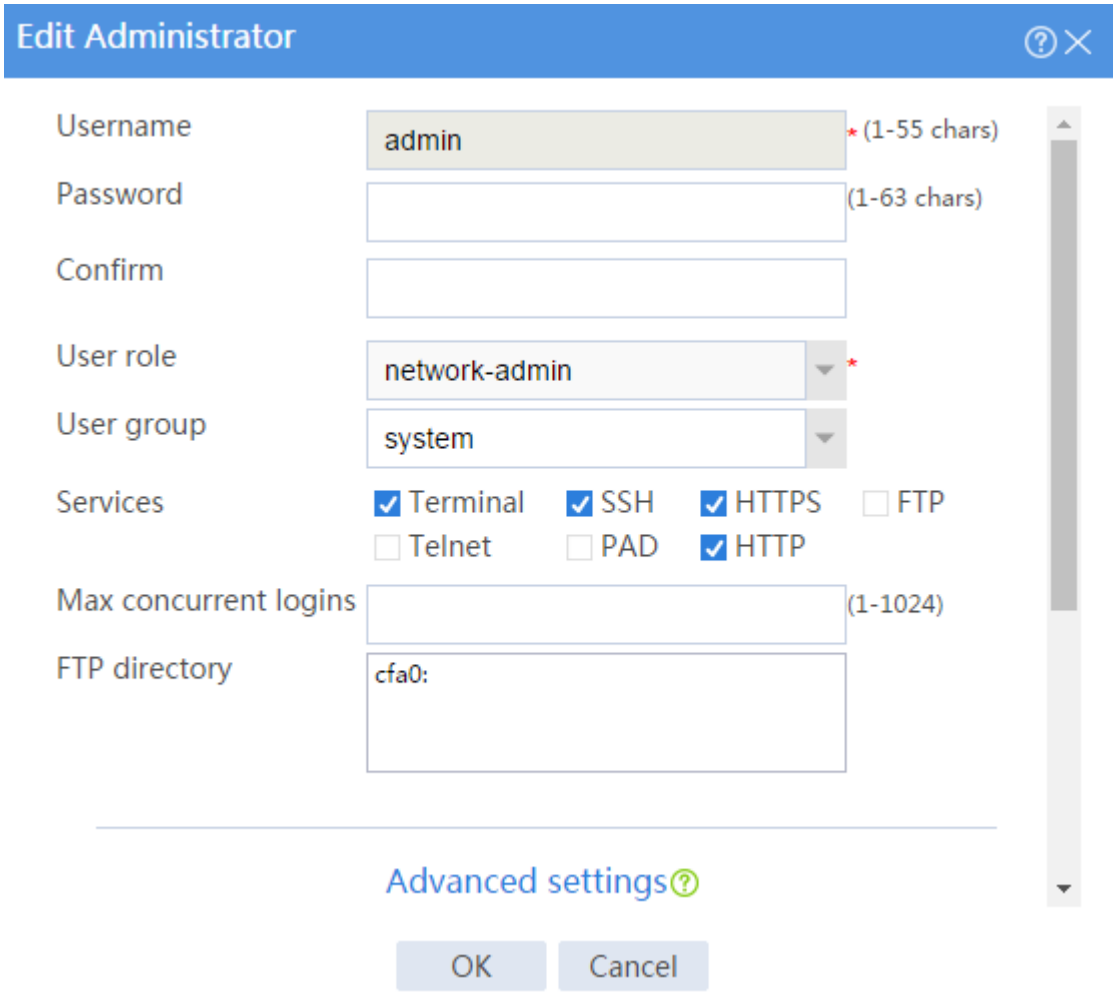
On the top navigation bar, click **System**.

From the navigation pane, select **Administrators** > **Administrators**.

Click the **Edit** icon for administrator **admin**.

In the dialog box that opens, select the HTTP service as shown in Figure 3.

Figure 3 Modifying administrator information



Click **OK**.

Configuring user identification

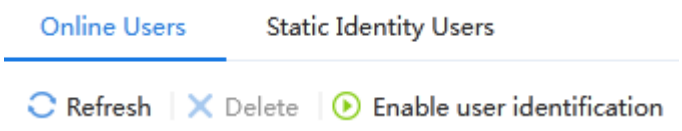
1. Enable user identification:

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **User** > **User Management** > **Online Users**.

   # On the **Online Users** tab, click **Enable user identification**.

   Figure 4 Enabling user identification

2. Create RESTful server **rest1**:

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **User** > **Authentication** > **RESTful Server**.

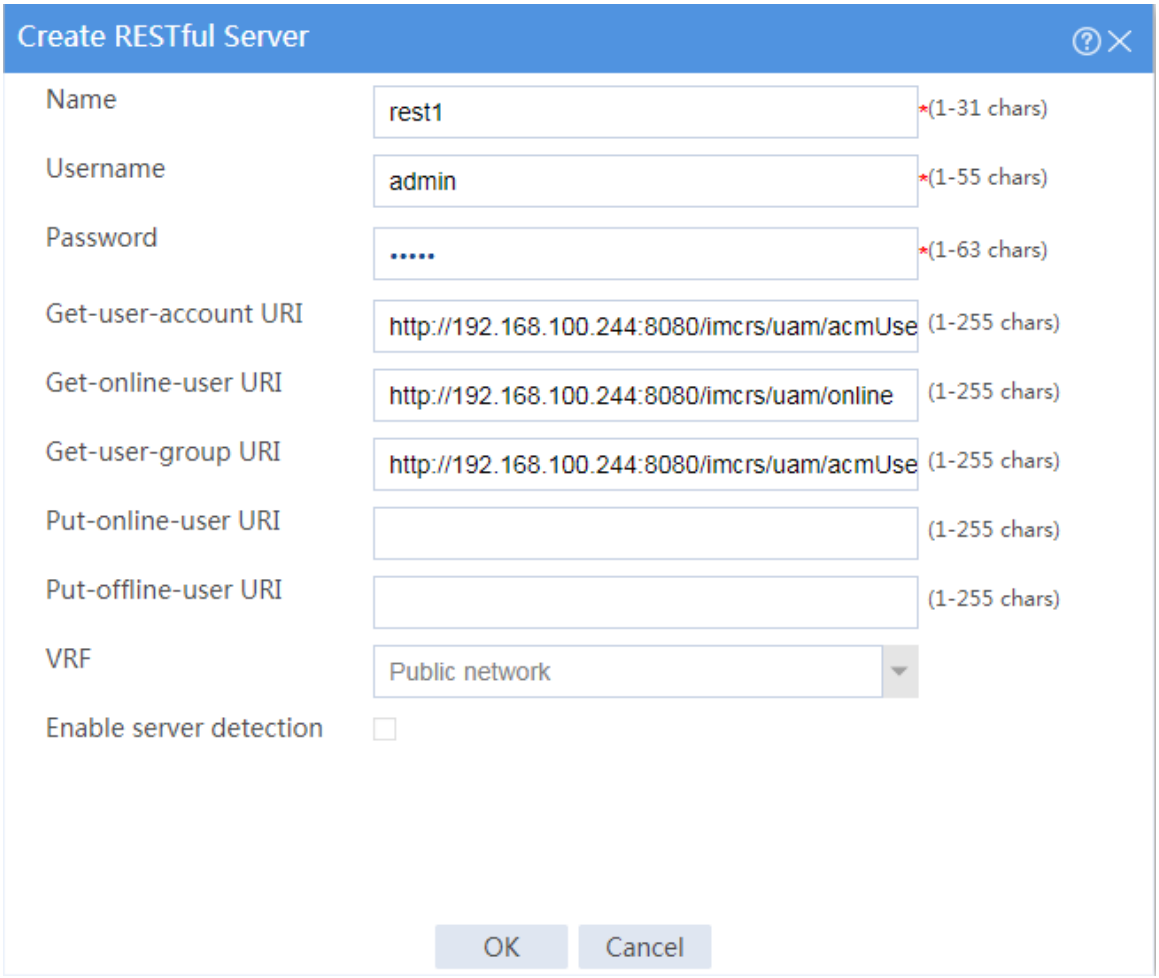
   # Click **Create**.

   # Configure the following parameters for the RESTful server:

   - Set the server name to **rest1**, the username to **admin**, and the password to **admin**.
   - Set the Get-user-account URI to **http://192.168.100.244:8080/imcrs/uam/acmUser/acmUserList**.
   - Set the Get-online-user URI to **http://192.168.100.244:8080/imcrs/uam/online**.
   - Set the Get-user-group URI to **http://192.168.100.244:8080/imcrs/uam/acmUser/userGroup**.

   For an IMC RESTful server, URIs are in a fixed format. You cannot modify any parameters in the above URIs except for the IP address.

Figure 5 Creating a RESTful server



Click **OK**.

3. Create user import policy **imc**:

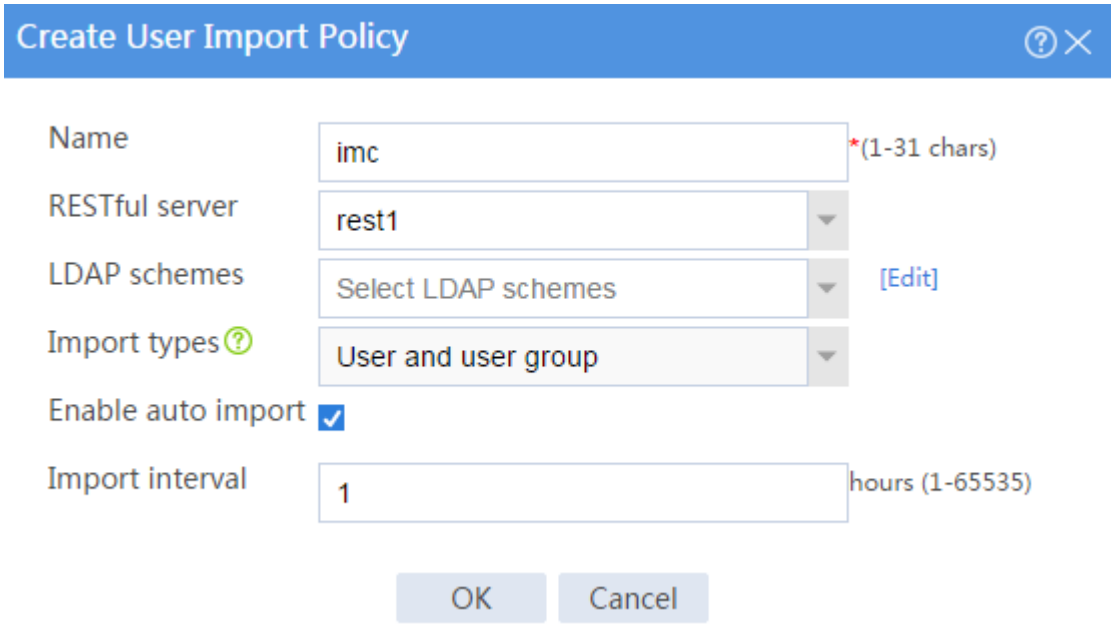
On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **User Import Policies**.

Click **Create**.

Configure parameters for the user import policy, as shown in Figure 6.

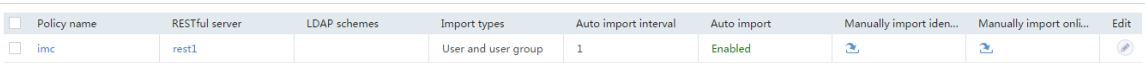
Figure 6 Creating a user import policy



Click **OK**.

After the firewall and the IMC server can communicate with each other, enter the **User Import Policies** page and select **imc** from the policy list. Then, click the **Manually import identity users** and **Manually import online users** icons to import the user accounts and online users on the IMC server to the firewall.

Figure 7 Importing user accounts and online users



Configuring security policies to ensure the network connectivity between the firewall and the IMC server

Perform the tasks in this section to ensure that the firewall can import identity user information from the IMC server.

.# On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** > **Create a policy**.

Configure security policy **trust-local** to permit traffic from zone **Trust** to zone **Local**:

- Enter security policy name **trust-local**.
- Select source security zone **Trust**.
- Select destination security zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Use the default settings for other parameters.

Click **OK**.

Configure security policy **local-trust** in the same way you configure security policy **trust-local** to permit traffic from zone **Local** to zone **Trust**:

- Enter security policy name **local-trust**.
- Select source security zone **Local**.
- Select destination security zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Use the default settings for other parameters.

Configure security policy **user10002** in the same way you configure security policy **trust-local** to permit user **user10002** to access the FTP server and deny other users from accessing the FTP server:

- Enter security policy name **user10002**.
- Select source security zones **Trust** and **DMZ**.
- Select destination security zones **Trust** and **DMZ**.
- Select type **IPv4**.
- Select action **Permit**.
- Select user **user10002**.
- Use the default settings for other parameters.

Configure security policy **user10003** in the same way you configure security policy **trust-local** to permit user **user10003** to access the Internet but denies users from the Internet from accessing the internal network:

- Enter security policy name **user10003**.
- Select source security zone **Trust**.
- Select destination security zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select user **user10003**.
- Use the default settings for other parameters.

Adding managed devices to IMC

Add the router and firewall to IMC so that IMC can monitor and manage the devices.

1. Log in to IMC:

Enter the IMC URL in the address bar of the Web browser. In this example, the URL is http://192.168.100.244:8080/imc/.

Enter username **admin** and password **admin**.

2. Add the firewall to IMC:

Click the **Resource** tab.

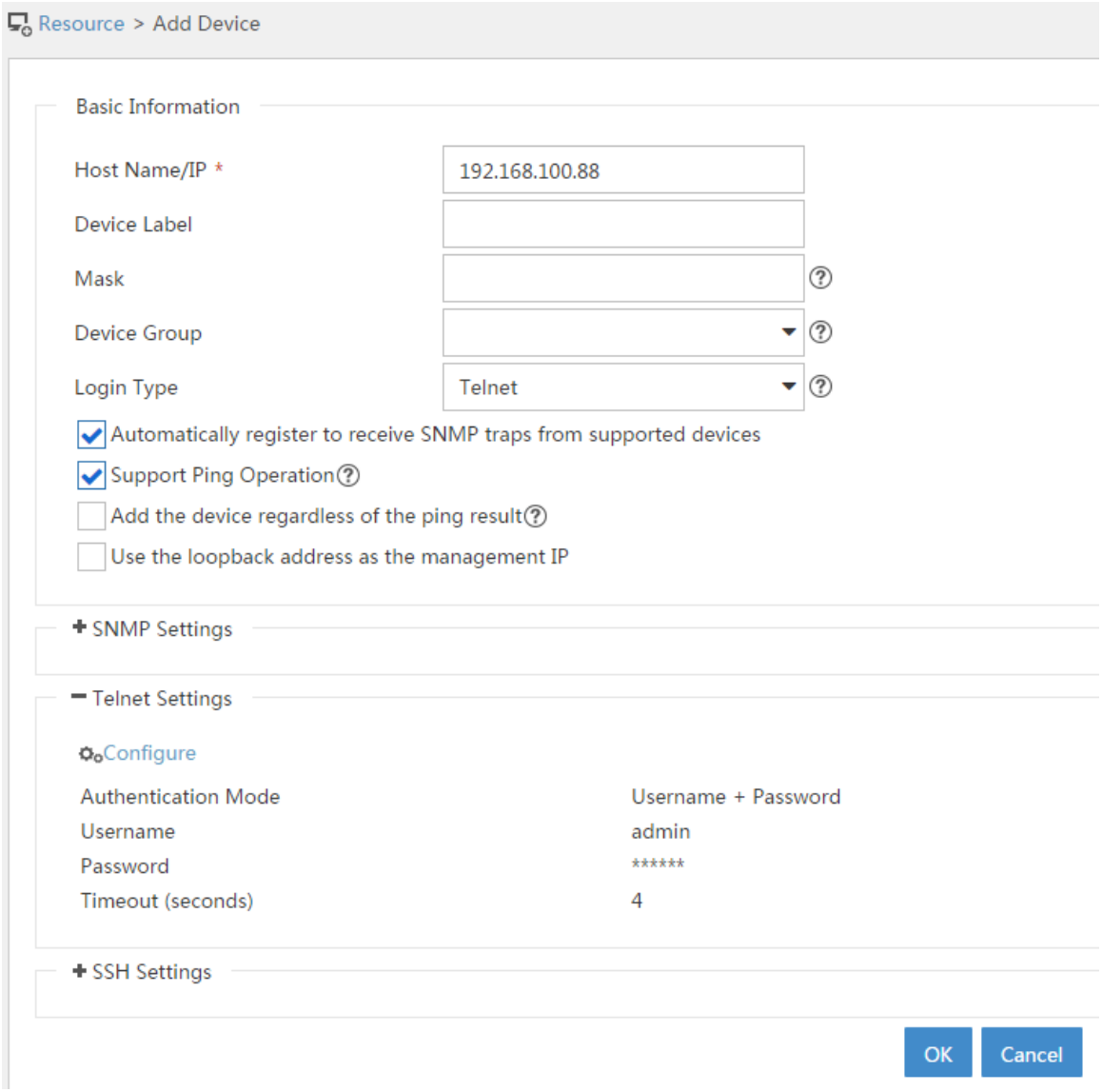
From the navigation tree, select **Resource Management** > **Add Device**.

On the page that opens, configure the parameters as shown in Figure 8:

- In the **Telnet Settings** area, set the username and password to **admin**.
- Use the default values for other parameters.

  By default, the read-only SNMP community string is **public** and the read and write SNMP community string is **private**.

Figure 8 Adding the firewall to IMC



Click **OK**.

Add the router (192.168.100.90) to IMC in the same way you add the firewall to IMC.

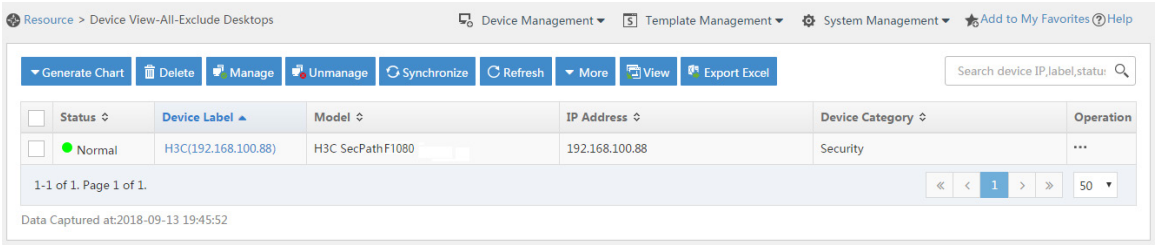
3. Modify NETCONF settings:

Click the **Resource** tab.

From the navigation tree, select **View Management** > **Device View**.

Click the link in the **Device Label** column for the target device.

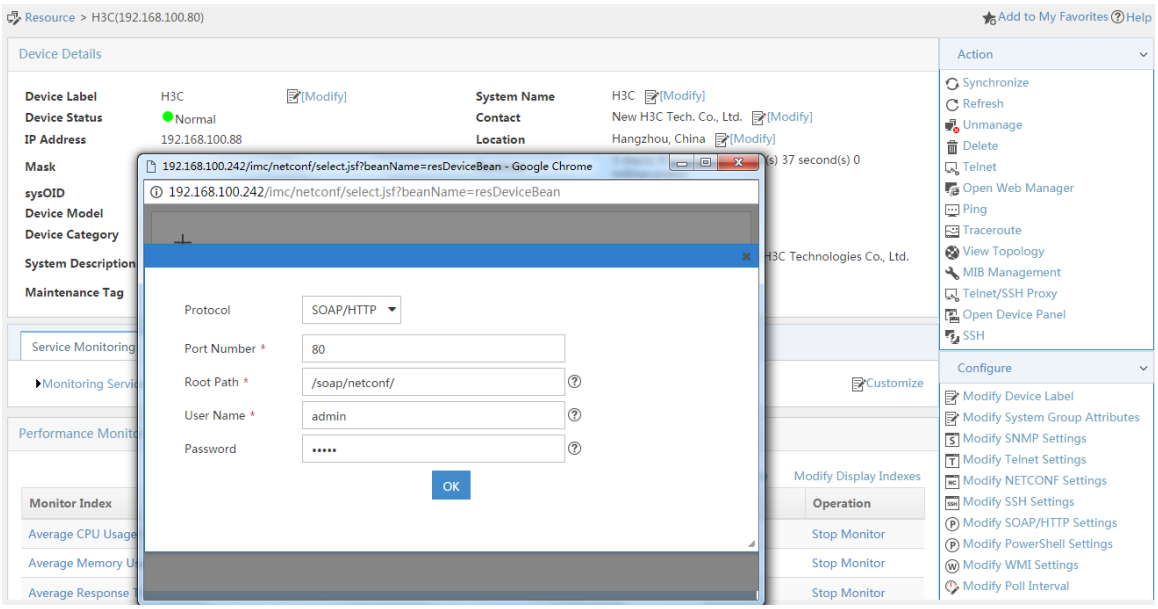
Figure 9 Device list



In the right pane, click **Configure** > **Modify NETCONF Settings**.

In the dialog box that opens, click the plus sign (+) to add a protocol as shown in Figure 10. In this example, set the username and password to **admin**.

Figure 10 Modifying NETCONF settings



Click **OK**.

Configuring security services (IMC)

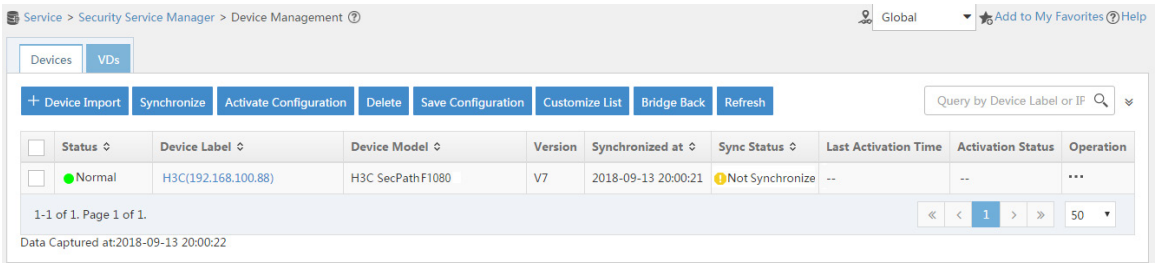
1. Synchronize security services from the firewall to the IMC server to ensure that the configuration and user information is consistent between the firewall and IMC server.

Click the **Service** tab.

From the navigation tree, select **Security Service Manager** > **Device Management**.

On the **Devices** tab, the firewall is displayed in the device list, as shown in Figure 11.

Figure 11 Page for security device management (not synchronized)



Select the firewall in the device list and click **Synchronize**. You can view the synchronization status from the **Sync Status** column, as shown in Figure 12 and Figure 13.

The synchronization process might take a long time. Please wait.

Figure 12 Page for security device management (synchronizing)

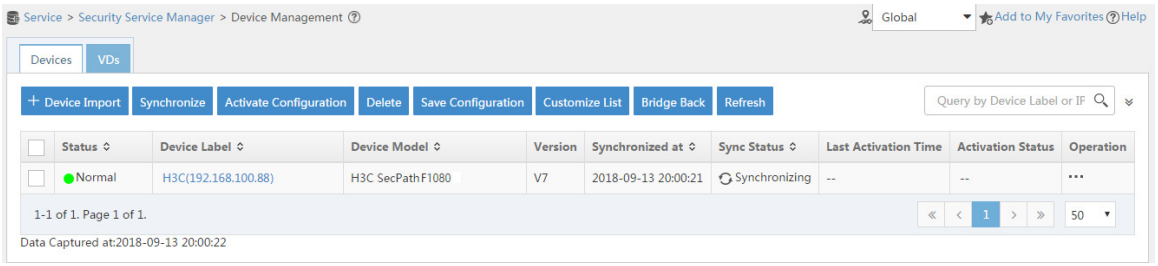
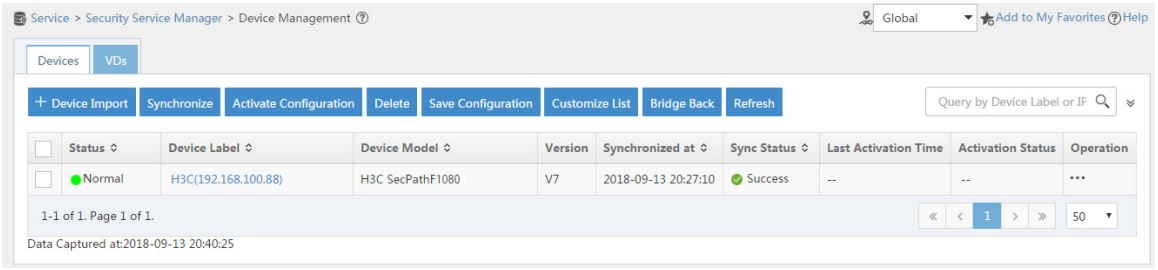


Figure 13 Page for security device management (synchronization succeeded)



2. Configure user authentication system parameters and user notification parameters to ensure

that the IMC server synchronizes user online and offline information to the firewall in real time.

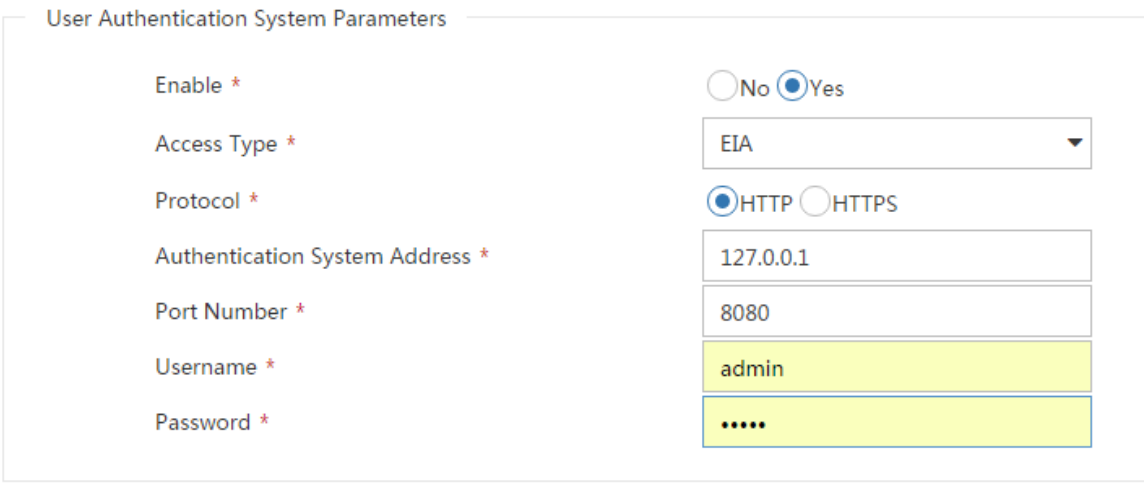
Click the **Service** tab.

From the navigation tree, select **Security Service Manager** > **Global Parameters**.

Configure the user authentication system parameters, as shown in Figure 14.

Select a protocol depending on the protocol of the portal authentication server. Make sure the username and password is the same as that used to log in to the IMC server.

Figure 14 Configuring user authentication system parameters



Click **OK**.

Click the **User** tab.

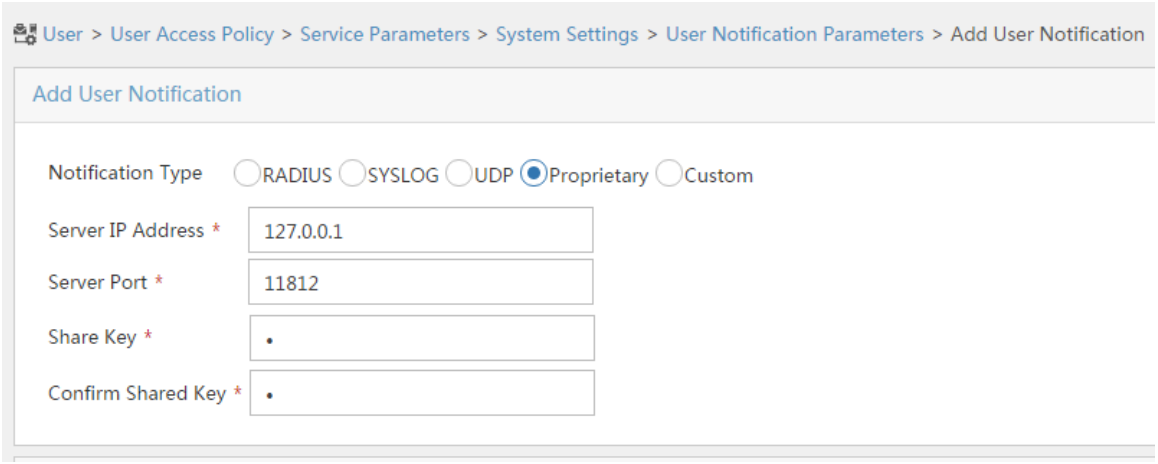
From the navigation tree, select **User Access Policy** > **Service Parameters** > **System Settings**.

Click the **Configure** icon for **User Notification Parameters**.

On the page that opens, click **Add**.

On the **Add User Notification** page, configure the parameters as shown in Figure 15. In this example, you can enter a shared key randomly.

Figure 15 Configuring user notification parameters



Click **OK**.

Configuring the RADIUS server (IMC)

1. Add the router to the server as an access device:

   # Click the **User** tab.

   # From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.

   # Click **Add**.

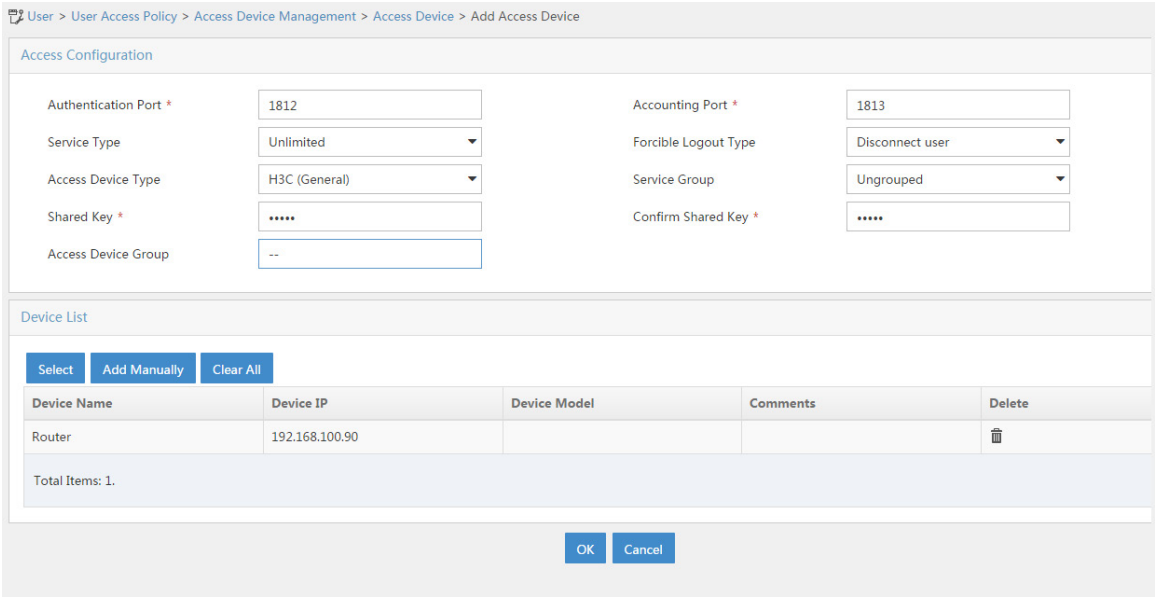
   # Set the shared key to **admin**, as shown in Figure 16.

   # In the **Device List** area, click **Select** or **Add Manually** to add the device at 192.168.100.90 as an access device.

   You must specify the source IP address of outgoing RADIUS packets on the router as the IP address of the access device on the server.

   On the router, the source IP address is configured by using the **`nas-ip`** or **`radius nas-ip`** command. The IP address configured by using the **`nas-ip`** command has a higher priority than the IP address configured by using the **`radius nas-ip`** command. If no IP address is specified as the source IP address, the IP address of the packet outbound interface is used as the source IP address. In this example, the IP address of the packet outbound interface is used, which is 192.168.100.90.

Figure 16 Adding an access device



Click **OK**.

2. Add an access policy:

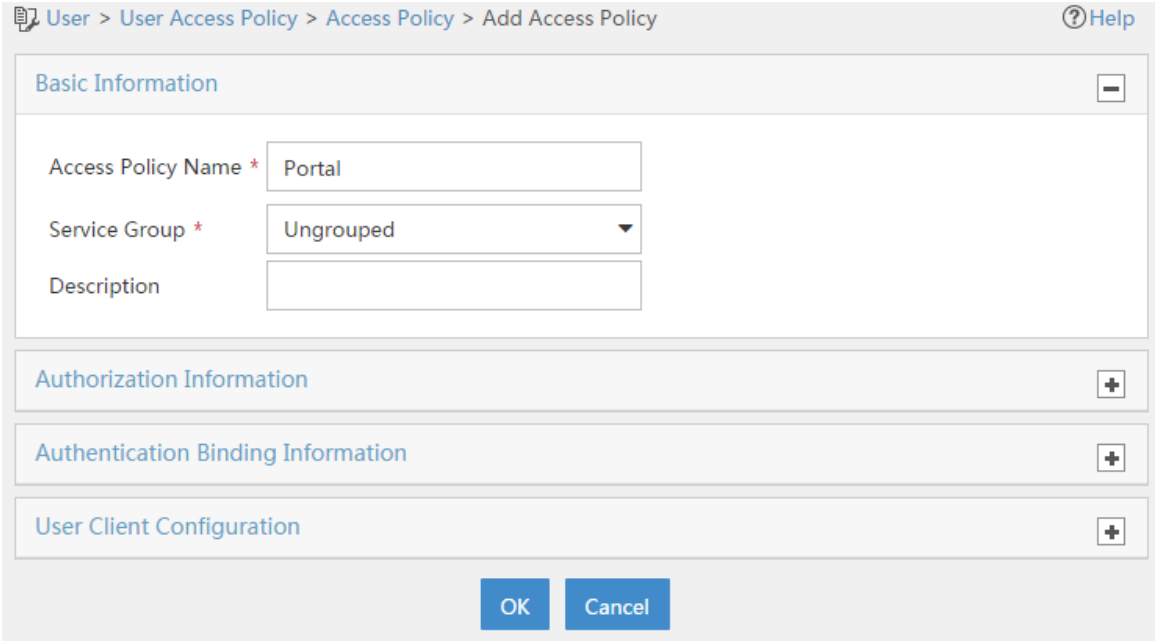
Click the **User** tab.

From the navigation tree, select **User Access Policy** > **Access Policy**.

Click **Add**.

Set the access policy name to **Portal**, as shown in Figure 17.

Figure 17 Adding an access policy



Click **OK**.

3. Add an access service:

Select the **User** tab.

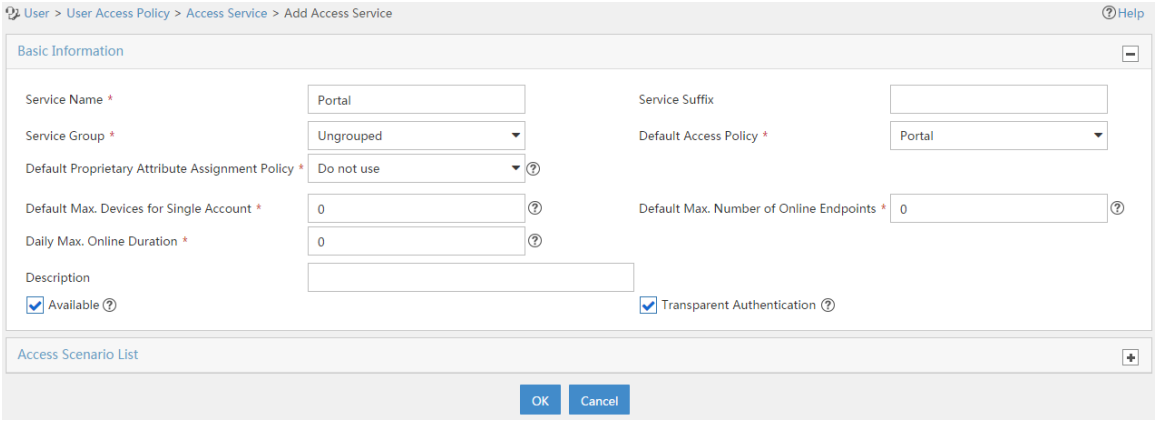
From the navigation tree, select **User Access Policy** > **Access Service**.

Click **Add**.

On the **Add Access Service** page, configure the following parameters:

- Enter service name to **Portal**.
- Select **Portal** from the **Default Access Policy** list.

Figure 18 Adding an access service



Click **OK**.

4. Add an access user:

Click the **User** tab.

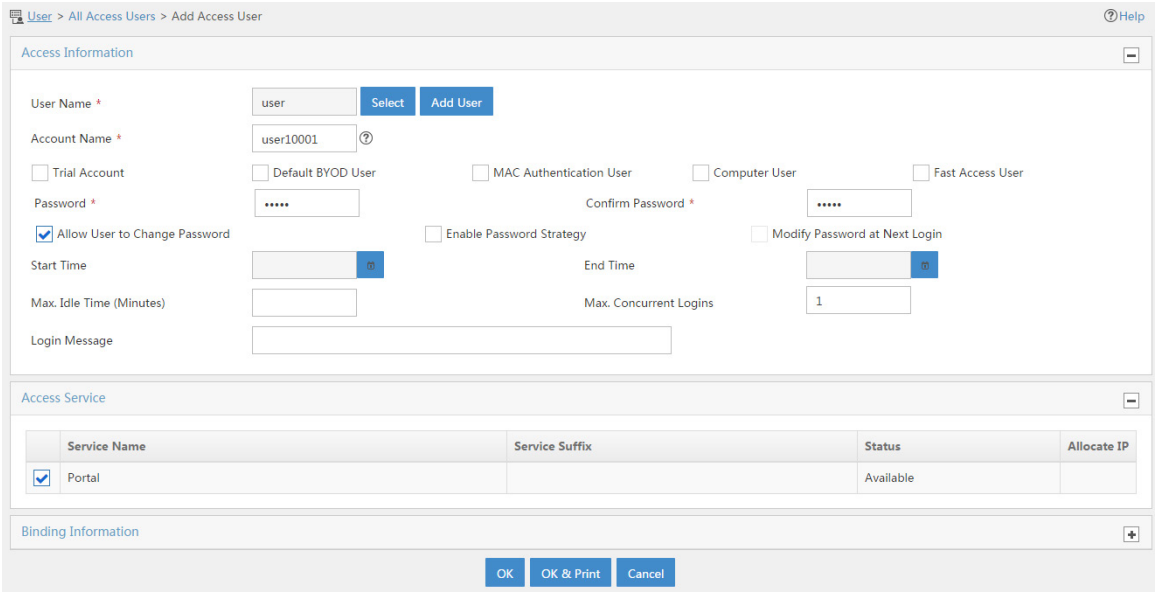
From the navigation tree, select **Access User** > **All Access Users**.

Click **Add**.

On the **Add Access User** page, configure parameters as shown in Figure 19.

- Enter **user** in the **User Name** field.
- Enter **user10001** in the **Account Name** field.
- Enter **admin** in the **Password** and **Confirm Password** fields.
- Select **Portal** in the **Access Service** area.

Figure 19 Adding an access user



Click **OK**.

Add user accounts **user10002** and **user10003** in the same way you add user account **user10001**.

Configuring the portal server (IMC)

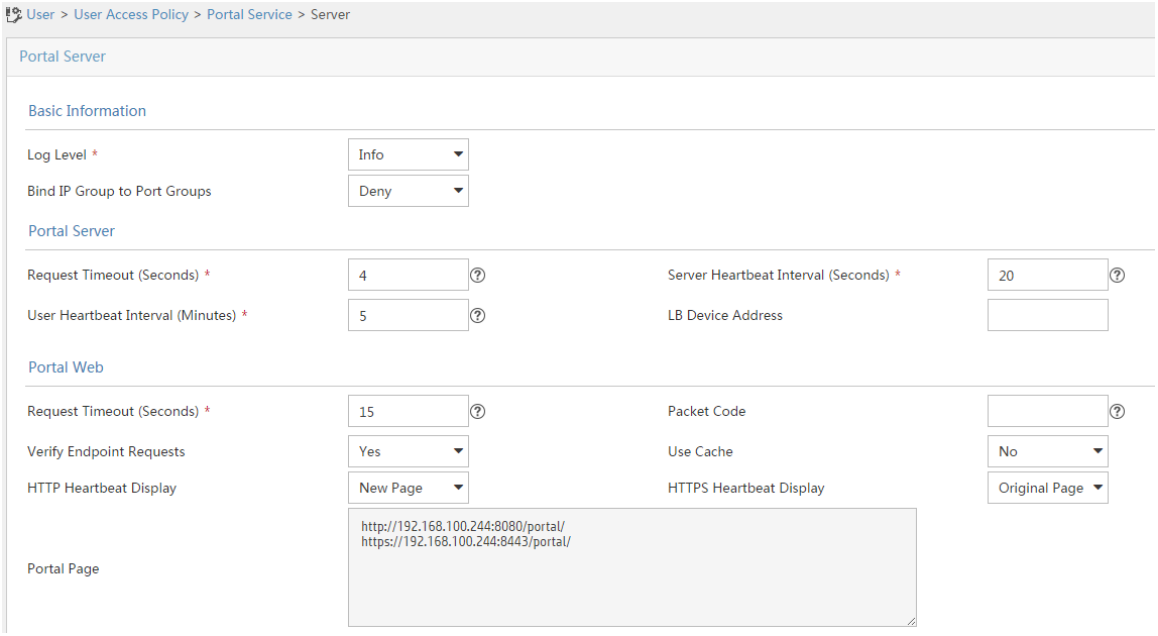
1. Configure the portal server:

   # Click the **User** tab.

   # From the navigation tree, select **User Access Policy** > **Portal Service** > **Server**.

   # Configure the parameters in Figure 20 depending on the network conditions. In this example, the default values are used.

Figure 20 Configuring the portal server



Click **OK**.

2. Add an IP group:

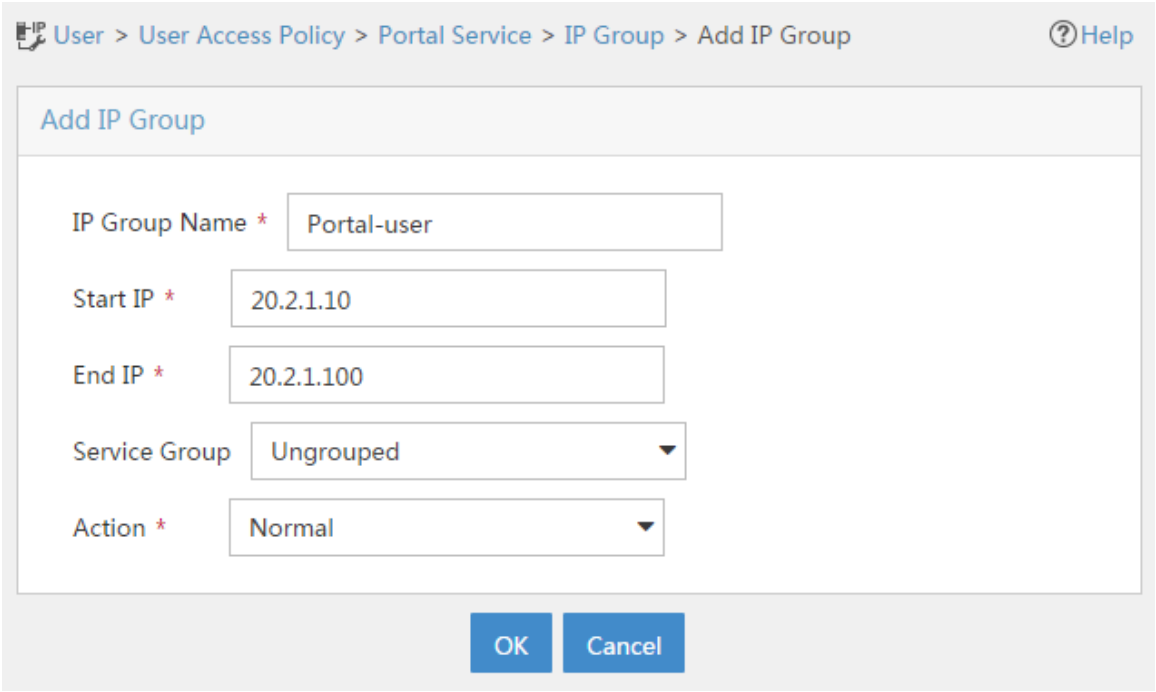
Click the **User** tab.

From the navigation tree, select **User Access Policy** > **Portal Service** > **IP Group**.

Click **Add**.

Configure parameters as shown in Figure 21.

Figure 21 Adding an IP group



Click **OK**.

3. Add a portal device:

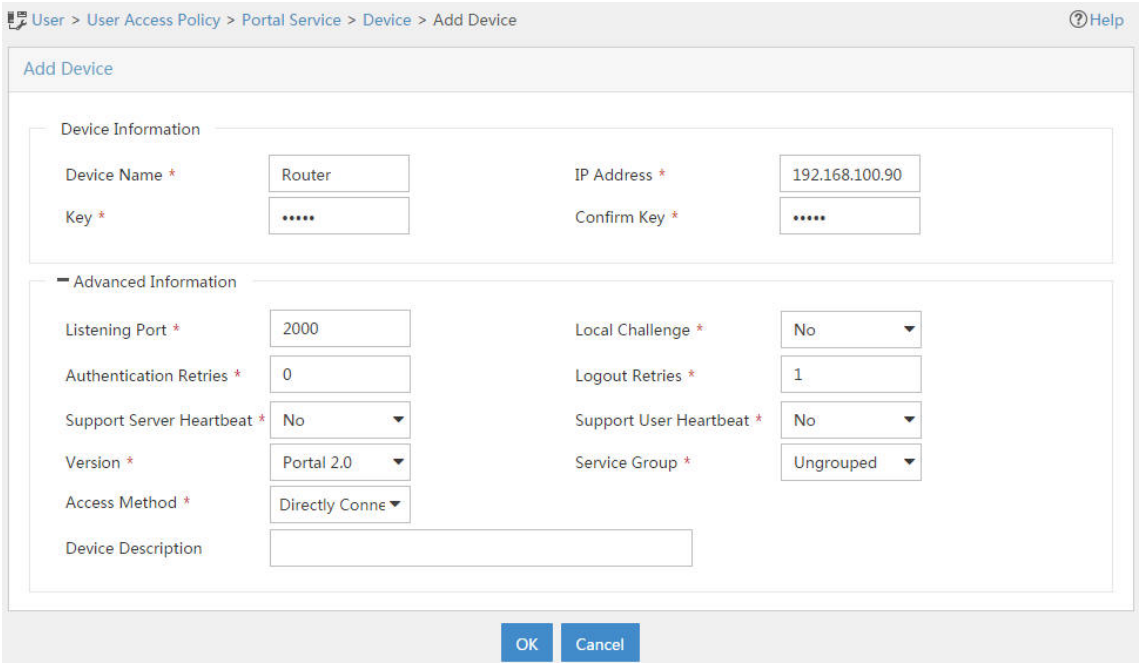
Click the **User** tab.

From the navigation tree, select **User Access Policy** > **Portal Service** > **Device**.

Click **Add**.

Set the shared key to **admin** and configure other parameters as shown in Figure 22.

Figure 22 Adding a portal device



Click **OK**.

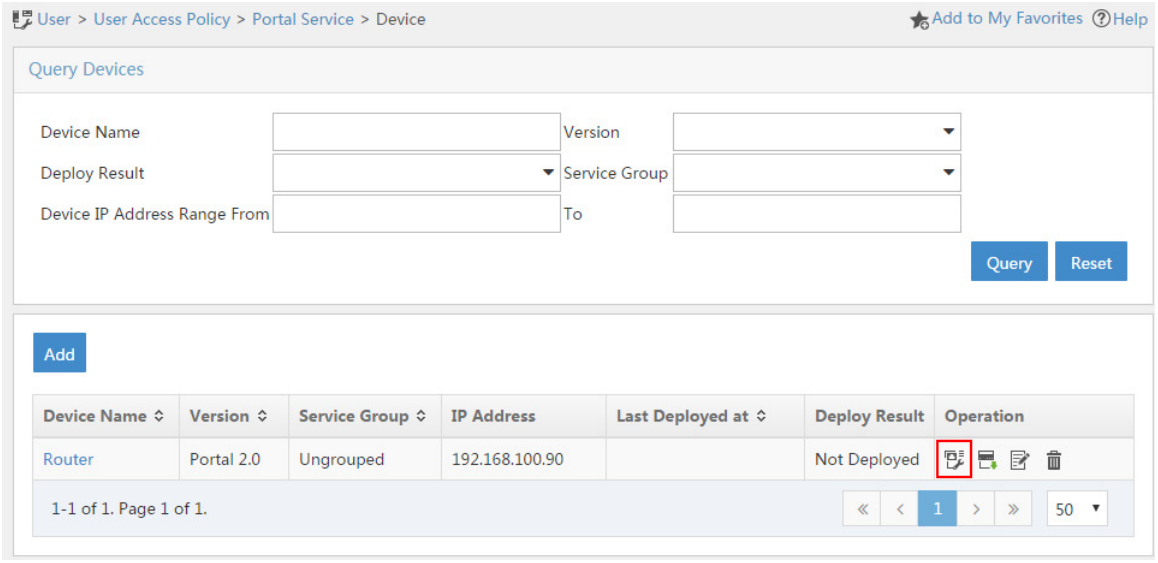
4. Associate the portal device with the IP group:

Click the **User** tab.

From the navigation tree, select **User Access Policy** > **Portal Service** > **Device**.

Click the **Port Group** icon in the **Operation** column for the router.

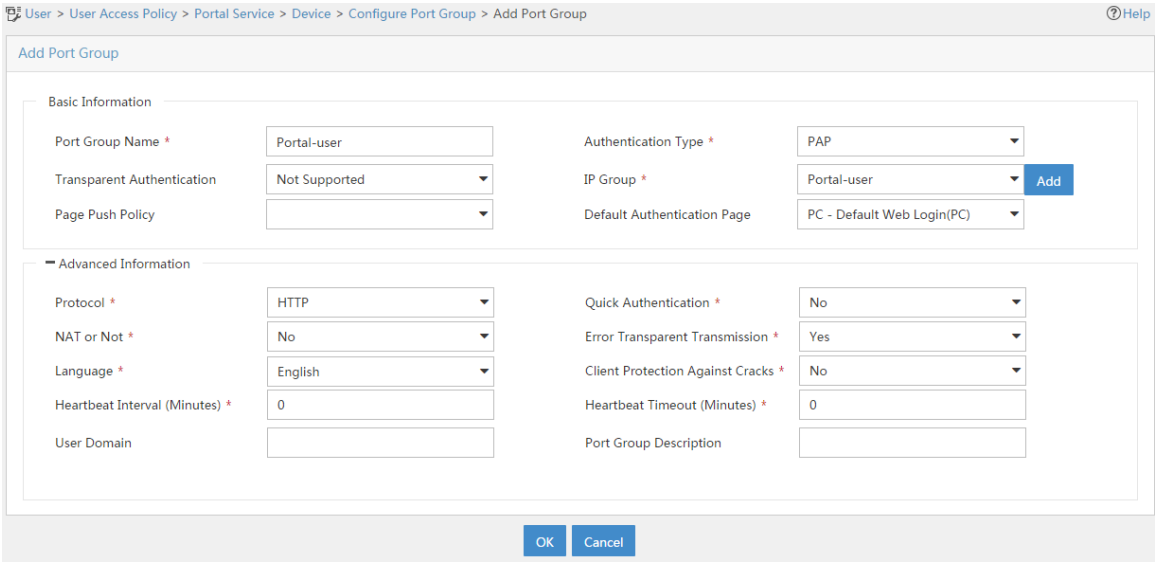
Figure 23 Device list



On the page that opens, click **Add**.

On the page that opens, configure a port group as shown in Figure 24.

Figure 24 Adding a port group



Click **OK**.

Configuring the hosts

Configure the IP address, network mask, and default gateway settings on each host. Make sure the hosts can communicate with the devices in the network. (Details not shown.)

Verifying the configuration

1. On the hosts, verify that the users can pass portal authentication.

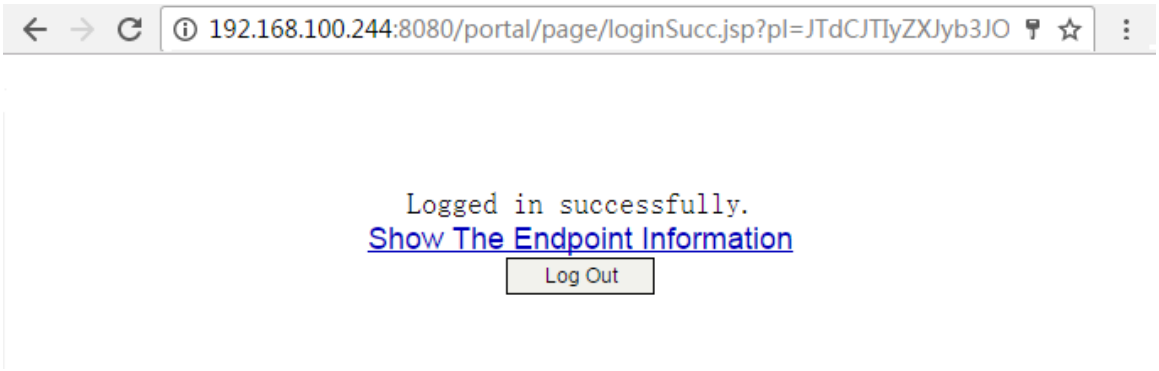
   # Enter the URL of the portal Web server in the address bar of the Web browser to log in to the portal authentication page. In this example, the URL is http://192.168.100.244:8080/portal.

   # Enter the username and password.

   # Click **Log In**.

   # Verify that the user has passed portal authentication.

   Figure 25 Portal authentication success page



2. On the IMC server, verify that users **user10001**, **user10002**, and **user10003** are in the online user list after they pass portal authentication. To view the online user list, click the **User** tab and select **Access User** > **Online Users** from the navigation tree.
3. On the firewall, display identity user information.

   # Display information about all identity users.

```
[Device] display user-identity all user
  User ID     Username
  0x2         user10001
  0x3         user10002
  0x4         user10003
```

Display information about online identity user **user10001**.

```
[Device] display user-identity online-user null-domain name user10001
User name: user10001
  IP  : 20.2.1.11
  MAC : 0011-95e4-4aa9
  Type: Dynamic

Total 1 records matched.
```

Display information about online identity user **user10002**.

```
[Device] display user-identity online-user null-domain name user10002
User name: user10002
  IP  : 20.2.1.12
  MAC : 0011-95e4-4aa3
  Type: Dynamic

Total 1 records matched.
```

Display information about online identity user **user10003**.

```
[Device] display user-identity online-user null-domain name user10003
User name: user10003
  IP  : 20.2.1.13
  MAC : 0011-95e4-4aa2
  Type: Dynamic

Total 1 records matched.
```

4. Verify that the firewall can perform identity-based access control on the users:

Verify that user **user10001** cannot ping the FTP server.

```
C:\>ping 11.1.1.2

Pinging 11.1.1.2 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.

Ping statistics for 11.1.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Verify that user **user10002** can ping the FTP server.

```
C:\>ping 11.1.1.2

Pinging 11.1.1.2 with 32 bytes of data:
Reply from 11.1.1.2: bytes=32 time=36ms TTL=253
Reply from 11.1.1.2: bytes=32 time<1ms TTL=253
Reply from 11.1.1.2: bytes=32 time<1ms TTL=253
Reply from 11.1.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 11.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

When user **user10002** pings the FTP server, verify that the firewall generates a message.

Verify that user **user10003** can ping hosts in the Internet. In this example, the user pings the host at 12.1.1.2.

```
C:\>ping 12.1.1.2
```

```
Pinging 12.1.1.2 with 32 bytes of data:
Reply from 12.1.1.2: bytes=32 time=37ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 12.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

When user **user10003** pings the host in the Internet, verify that the firewall generates a message.

Configuration files

Router

```
[Router] display current-configuration
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 20.2.1.1 255.255.255.0
 portal enable method direct
 portal domain dm1
 portal apply web-server newpt
#
```

```
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.100.90 255.255.255.0
#
interface GigabitEthernet3/0
 port link-mode route
 combo enable copper
#
 ip route-static 0.0.0.0 0 192.168.100.88
#
 snmp-agent
 snmp-agent local-engineid 800063A28074258A37B5F500000001
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
#
radius scheme rs1
 primary authentication 192.168.100.244
 primary accounting 192.168.100.244
 key authentication cipher $c$3$hhbEbD5Ycvw7VWqljAoMoU7hQRgcUjtg
 user-name-format without-domain
#
domain dm1
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal radius-scheme rs1
#
domain system
#
```

```
 domain default enable system
#
local-user admin class manage
 password                                                              hash
$h$6$UbIhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
 service-type telnet http
 authorization-attribute user-role network-admin
#
portal web-server newpt
 url http://192.168.100.244:8080/portal
#
portal server newpt
 ip 192.168.100.244 key cipher $c$3$+UmaGOco7eHsjOqlrp8lI4eYe0A8NpYU
#
return
```

Device

```
[Device] display current-configuration
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.100.88 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 11.1.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name DMZ
 import interface GigabitEthernet1/0/2
#
security-zone name Untrust
 import interface GigabitEthernet1/0/3
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
 ip route-static 0.0.0.0 0 12.1.1.2
 ip route-static 20.2.1.0 24 192.168.100.90
#
 snmp-agent
 snmp-agent local-engineid 800063A280487ADA9593B700000001
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 192.168.100.244 params
securityn
ame public v2c
```

```
#
local-user admin class manage
 password                                                        hash
$h$6$UbIhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
 service-type ssh telnet terminal http https
 authorization-attribute user-role level-3
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 netconf soap http enable
 netconf soap https enable
 restful http enable
 restful https enable
#
 user-identity enable
 user-identity user-account auto-import policy imc
#
user-identity restful-server rest1
 login-name admin password cipher $c$3$phGy00HA6OP6pIpGI0KOKZEOPuLVbtt/
 uri                                                  get-user-database
http://192.168.100.244:8080/imcrs/uam/acmUser/acmUserList
 uri                                              get-user-group-database
http://192.168.100.244:8080/imcrs/uam/acmUser/userGroup
 uri get-online-user http://192.168.100.244:8080/imcrs/uam/online
#
user-identity user-import-policy imc
 account-update-interval 1
 restful-server rest1
```

```
#
security-policy ip
 rule 0 name trust-local
  action pass
  source-zone trust
  destination-zone local
 rule 1 name local-trust
  action pass
  source-zone local
  destination-zone trust
 rule 2 name user10002
  action pass
  logging enable
  source-zone trust
  source-zone dmz
  destination-zone dmz
  destination-zone trust
  user user10002
 rule 3 name user10003
  action pass
  logging enable
  source-zone trust
  destination-zone untrust
  user user10003
#
return
```

Example: Configuring user identification for portal

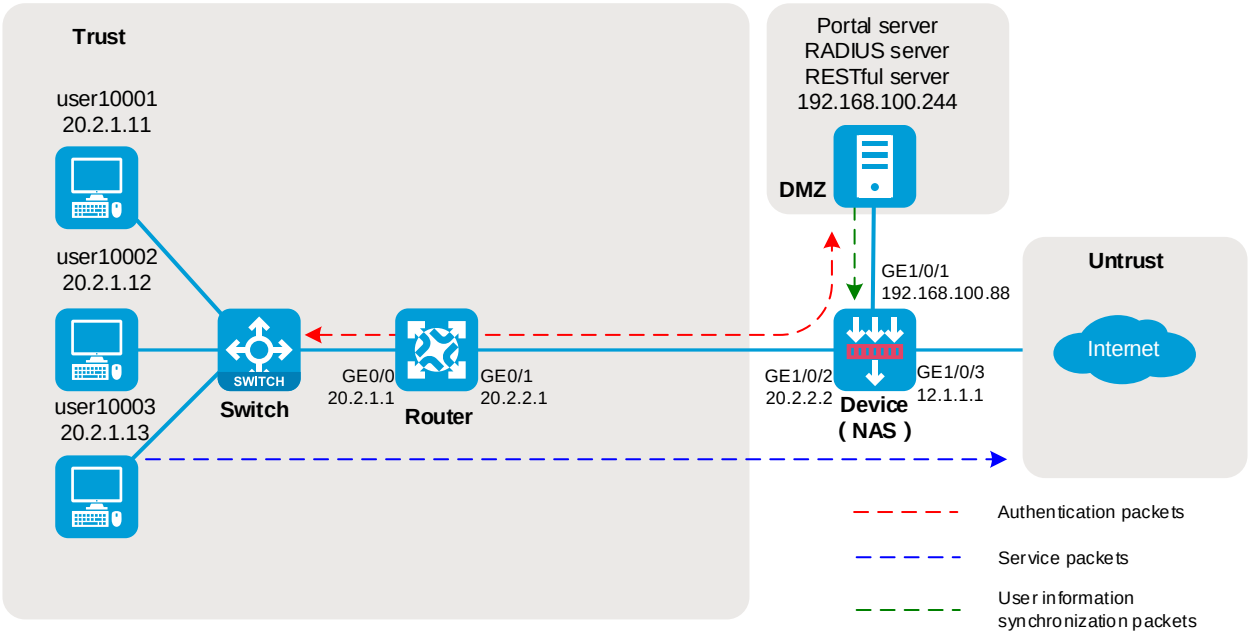
users that pass RADIUS authentication (non-RADIUS single sign-on)

Network configuration

As shown in Figure 26:

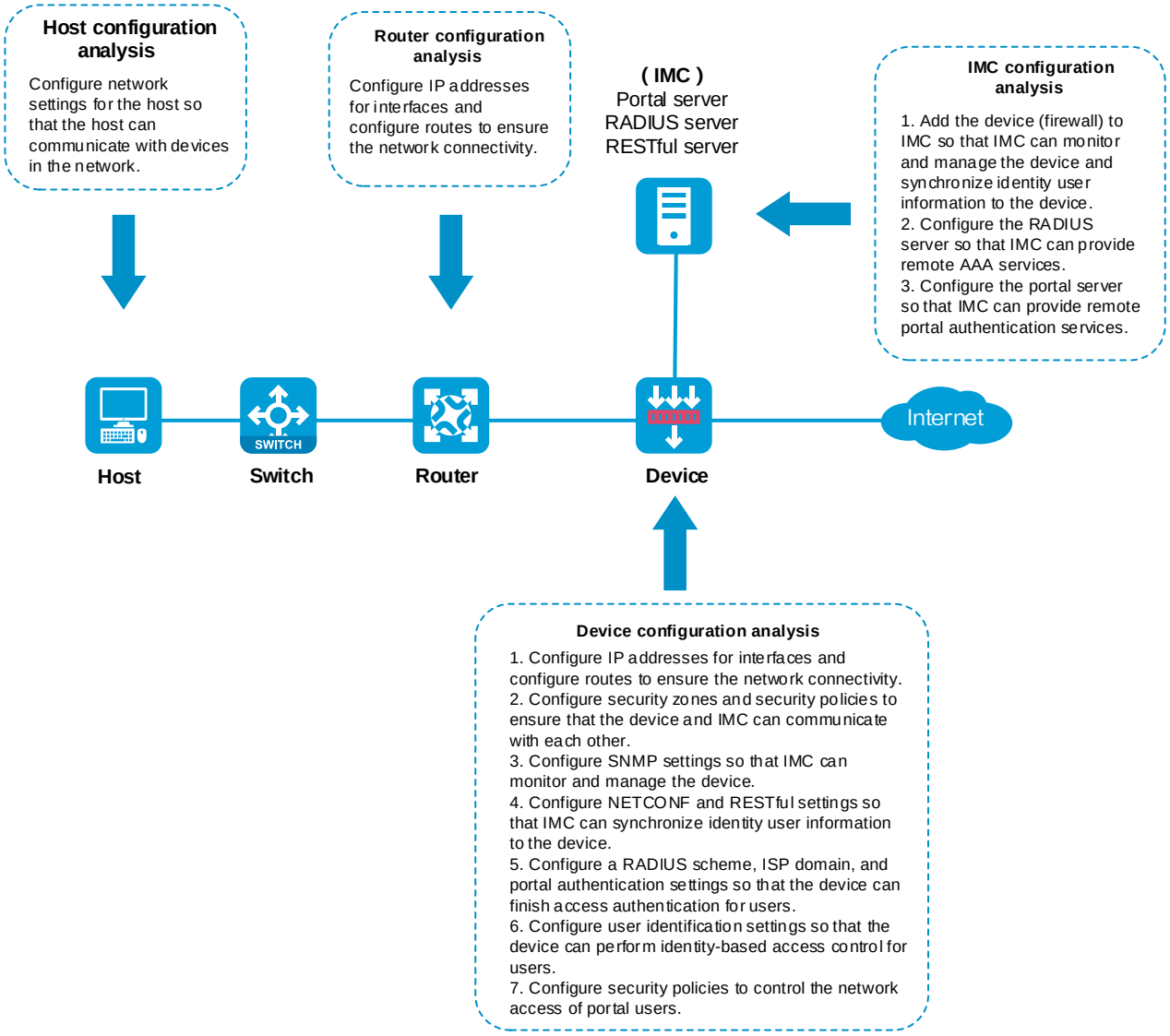
- Users **user10001**, **user10002**, and **user10003** use static IP addresses, and they must pass portal authentication to access the network.
- Device is a firewall and acts as a NAS for the users to access the network. The NAS uses the RADIUS server to authenticate the users.
- The RADIUS server is installed with IMC components. For portal authentication, the server acts as both the portal authentication server and portal Web server.
- The RESTful server stores user account information. The server can synchronize user identity information to Device (the firewall).
- The firewall performs the following identity-based access control on the users that have passed portal authentication:
  - Users **user10001** and **user10002** cannot access the Internet.
  - User **user10003** can access the Internet.
  - Users from the Internet cannot access the hosts in the **Trust** and **DMZ** security zones.

Figure 26 Network diagram



Analysis

Figure 27 Analysis diagram



Software versions used

This configuration example was created and verified on the following software versions:

- R8560 of the NFNX3-HDB3080 device.

- Version 7.1.064, ESS 0701 of the MSR26-30 router.

The RADIUS and portal server is installed with IMC PLAT 7.3 (E0606), IMC UAM 7.3 (E0503), IMC CAMS 7.3 (E0501), and IMC EIA 7.3 (E0512).

Restrictions and guidelines

An IMC server logs off an online user only after it receives an accounting-stop request for that user. For the NAS to send accounting-stop requests to the server, you need to configure accounting settings in the authentication domain of the user on the NAS. However, you do not need to configure accounting parameters on the IMC server since accounting is not required.

Procedure

Configuring the router

Perform the tasks in this section to ensure the network connectivity of the router.

Assign IP address 20.2.1.1 to GigabitEthernet 0/0.

```
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ip address 20.2.1.1 255.255.255.0
[Router-GigabitEthernet0/0] quit
```

Assign IP address 20.2.2.1 to GigabitEthernet 0/1.

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] ip address 20.2.2.1 255.255.255.0
[Router-GigabitEthernet0/1] quit
```

Configure a default route to ensure that the router can reach the Internet.

```
[Router] ip route-static 0.0.0.0 0.0.0.0 20.2.2.2
```

Configuring Device (the firewall)

Configuring SNMP for the IMC server to monitor and manage the firewall

Enable the SNMP agent.

```
<Device> system-view
[Device] snmp-agent
```

Enable all SNMP versions, create the read-only community **public** and the read and write community **private**.

```
[Device] snmp-agent sys-info version all
[Device] snmp-agent community read public
[Device] snmp-agent community write private
```

Configuring NETCONF over SOAP for the IMC server to issue configuration to the firewall

Enable NETCONF over SOAP over HTTP.

```
[Device] netconf soap http enable
```

Enable NETCONF over SOAP over HTTPS.

```
[Device] netconf soap https enable
```

Enabling RESTful for the firewall to communicate with the IMC RESTful server

Enable RESTful over HTTP.

```
[Device] restful http enable
```

Enable RESTful over HTTPS.

```
[Device] restful https enable
```

Assigning IP addresses to interfaces and adding the interfaces to security zones

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

1. Select the **DMZ** security zone.
2. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 192.168.100.88/24.
3. Use the default settings for other parameters.
4. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 20.2.2.2/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Untrust** security zone and set its IP address to 12.1.1.1/24 in the same way you configure GE 1/0/1.

Configuring routing

1. Configure a route to ensure that the firewall and the users can reach each other.

   This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure the IPv4 static route:

   - Enter **20.2.1.0** in the **Destination address** field.
   - Enter **24** in the **Mask length** field.
   - Enter **20.2.2.1** as the next hop address in the **Next hop** field.
   - Use the default settings for other parameters.

   # Click **OK**.

2. Configure a default route to ensure that the firewall can reach the Internet.

   This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure the IPv4 static route:

- Enter **0.0.0.0** in the **Destination address** field.
- Enter **0** in the **Mask length** field.
- Enter **12.1.1.2** as the next hop address in the **Next hop** field.

  Specify the IP address of the device that connects to the firewall in the Internet as the next hop address. In this example, the next hop address is 12.1.1.2.
- Use the default settings for other parameters.

Click **OK**.

Assigning the HTTP service to administrator admin

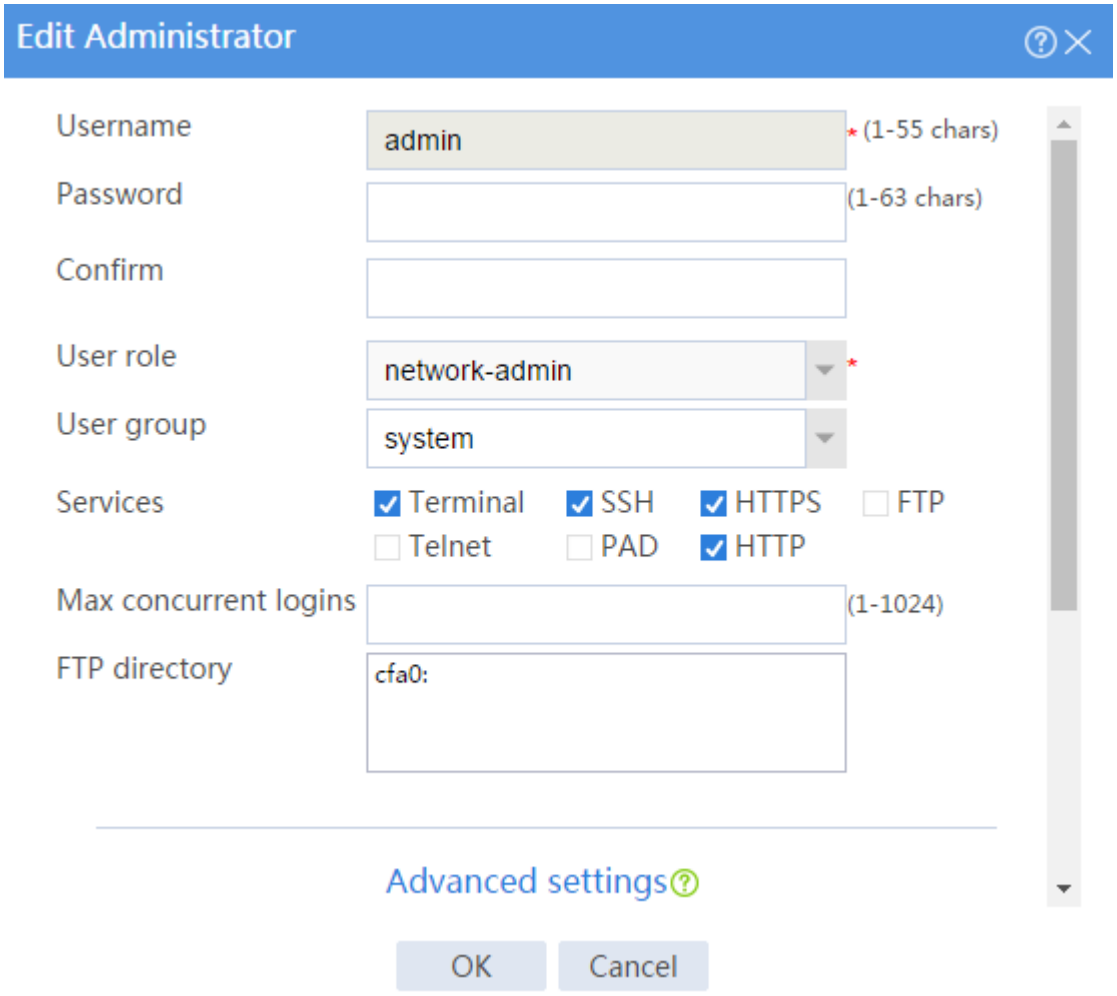
On the top navigation bar, click **System**.

From the navigation pane, select **Administrators** > **Administrators**.

Click the **Edit** icon for administrator **admin**.

In the dialog box that opens, select the HTTP service as shown in Figure 28.

Figure 28 Modifying administrator information



Click **OK**.

Configuring security policies to ensure the network connectivity between the firewall and the IMC server

Perform the tasks in this section to ensure that the firewall can import identity user information from the IMC server.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** > **Create a policy**.

Configure security policy **dmz-local** to permit traffic from zone **DMZ** to zone **Local**:

- Enter security policy name **dmz-local**.

- Select source security zone **DMZ**.
- Select destination security zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Use the default settings for other parameters.

Click **OK**.

Configure security policy **local-dmz** in the same way you configure security policy **dmz-local** to permit traffic from zone **Local** to zone **DMZ**:

- Enter security policy name **local-dmz**.
- Select source security zone **Local**.
- Select destination security zone **DMZ**.
- Select type **IPv4**.
- Select action **Permit**.
- Use the default settings for other parameters.

Configure security policy **trust-dmz** in the same way you configure security policy **dmz-local** to permit traffic between zone **Trust** and zone **DMZ**. This task allows the NAS to send and receive AAA and portal authentication packets for the users and IMC server.

- Enter security policy name **trust-dmz**.
- Select source security zones **Trust** and **DMZ**.
- Select destination security zones **Trust** and **DMZ**.
- Select type **IPv4**.
- Select action **Permit**.
- Use the default settings for other parameters.

Configuring RADIUS scheme rs1

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **Authentication** > **RADIUS**.

Click **Create**.

In the dialog box that opens, create a RADIUS authentication server and a RADIUS accounting

server and configure advanced settings, as shown in Figure 29, Figure 30, and Figure 31.

Figure 29 Creating a RADIUS scheme (authentication servers)

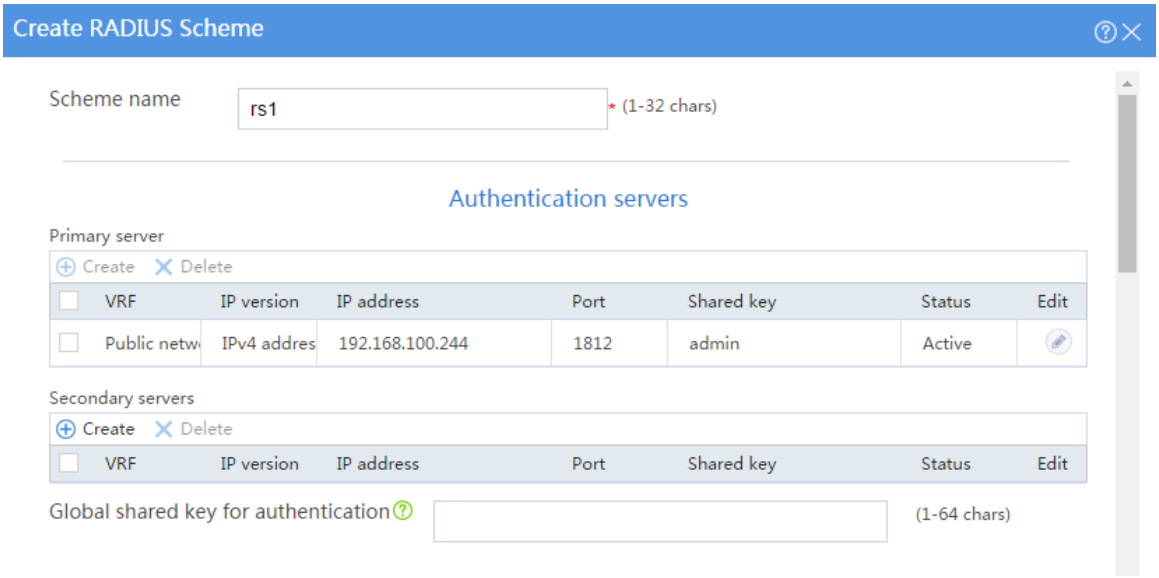


Figure 30 Creating a RADIUS scheme (accounting servers)

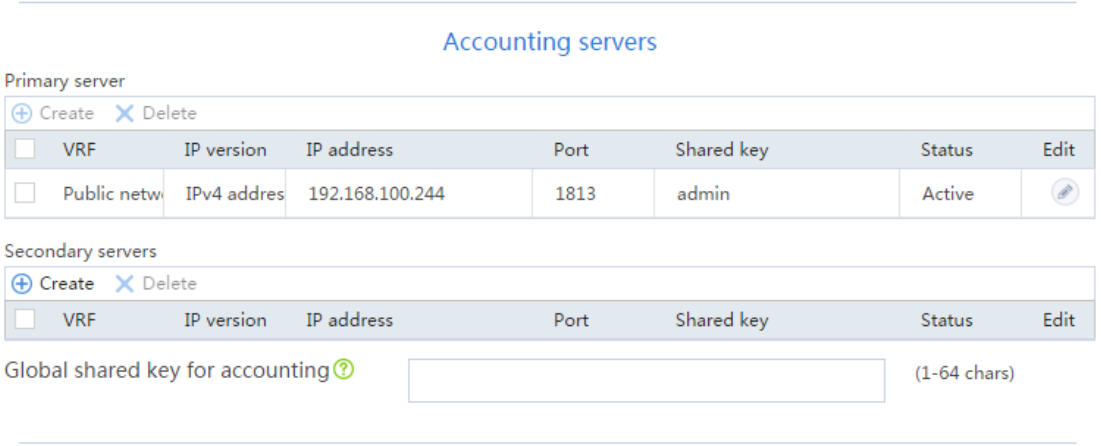
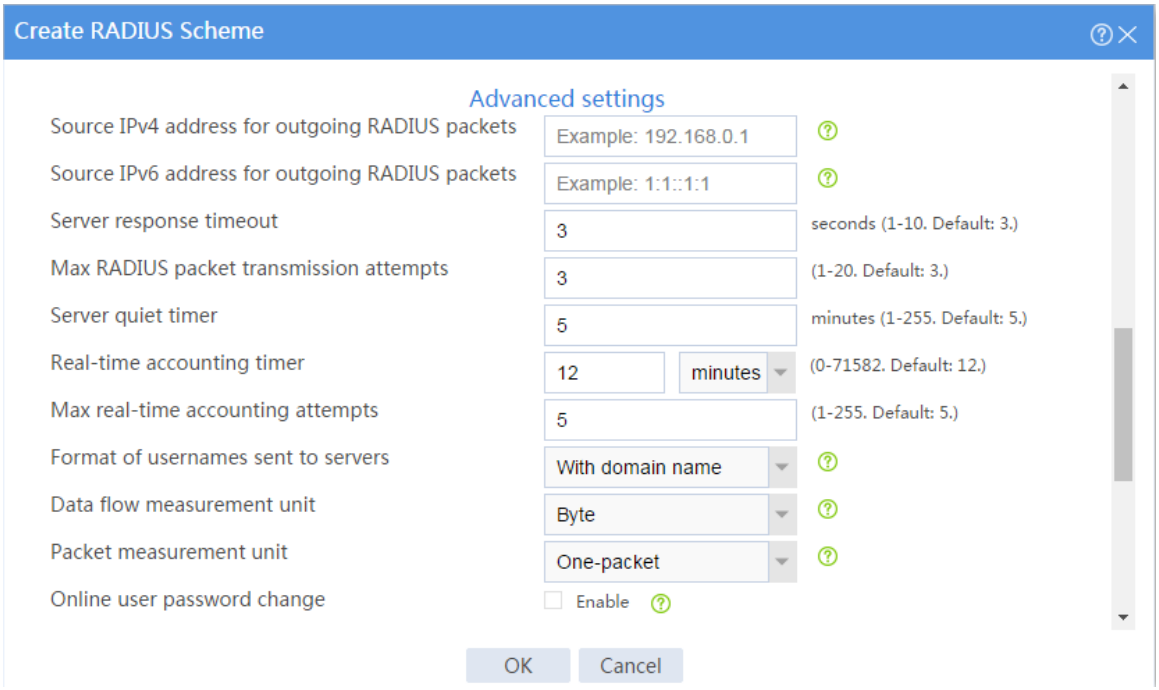


Figure 31 Creating a RADIUS scheme (advanced settings)



Click **OK**.

Configuring authentication domain dm1

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **Authentication** > **ISP Domains**.

Click **Create**.

In the dialog box that opens, configure the access types and the AAA methods for portal users, as shown in Figure 32 and Figure 33.

Figure 32 Adding ISP domain dm1 (access types)

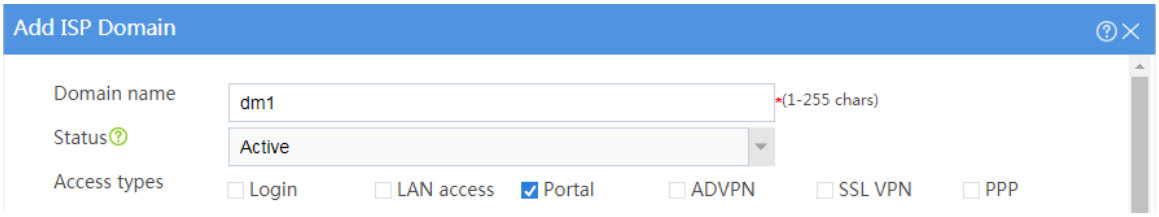
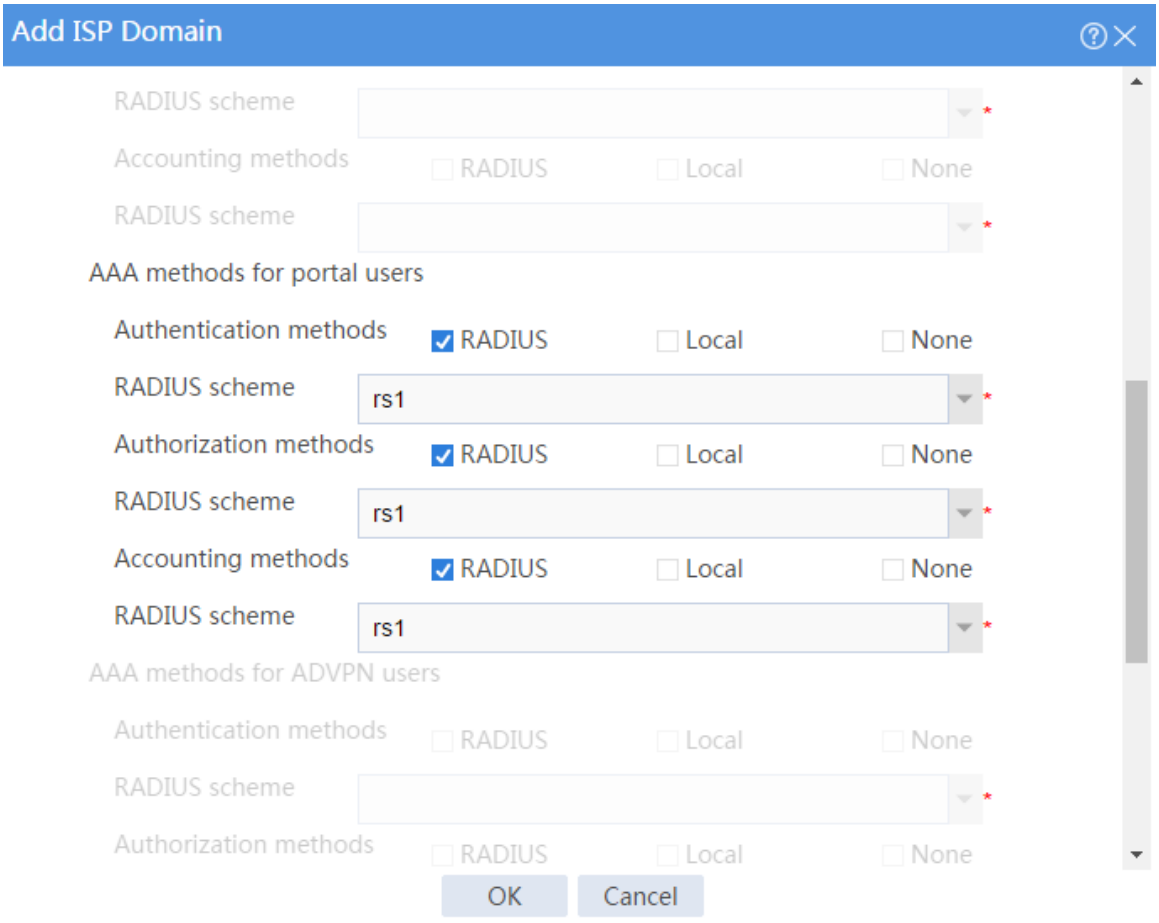


Figure 33 Adding ISP domain dm1 (AAA methods for portal users)



Click **OK**.

Configuring portal authentication

1. Configuring the portal authentication server:

On the top navigation bar, click **Objects**.

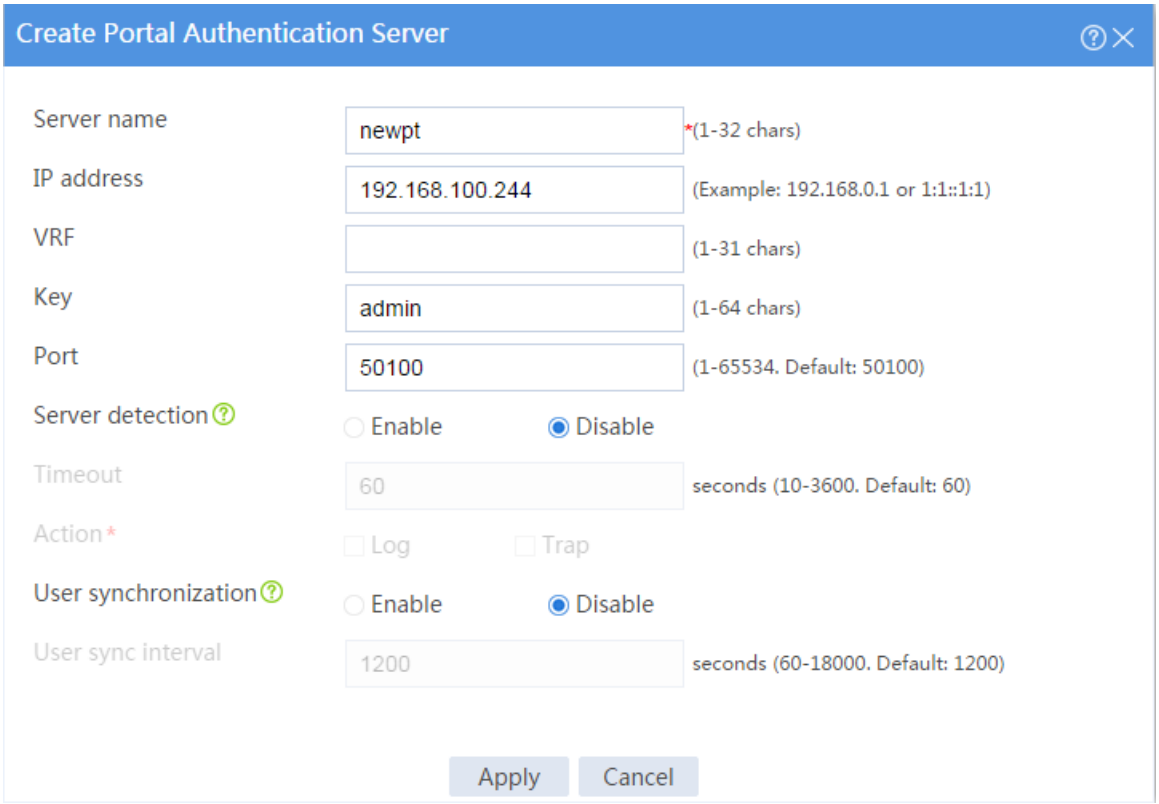
From the navigation pane, select **User** > **Access Control** > **Portal**.

On the **Portal Authentication Servers** tab, click **Create**.

In the dialog box that opens, configure the portal authentication server:

- Enter server name **newpt**.
- Set the IP address to 192.168.100.244.
- Enter key **admin**.
- Set the port to 50100.

Figure 34 Creating a portal authentication server



Click **OK**.

2. Configure the portal Web server:

On the top navigation bar, click **Objects**.

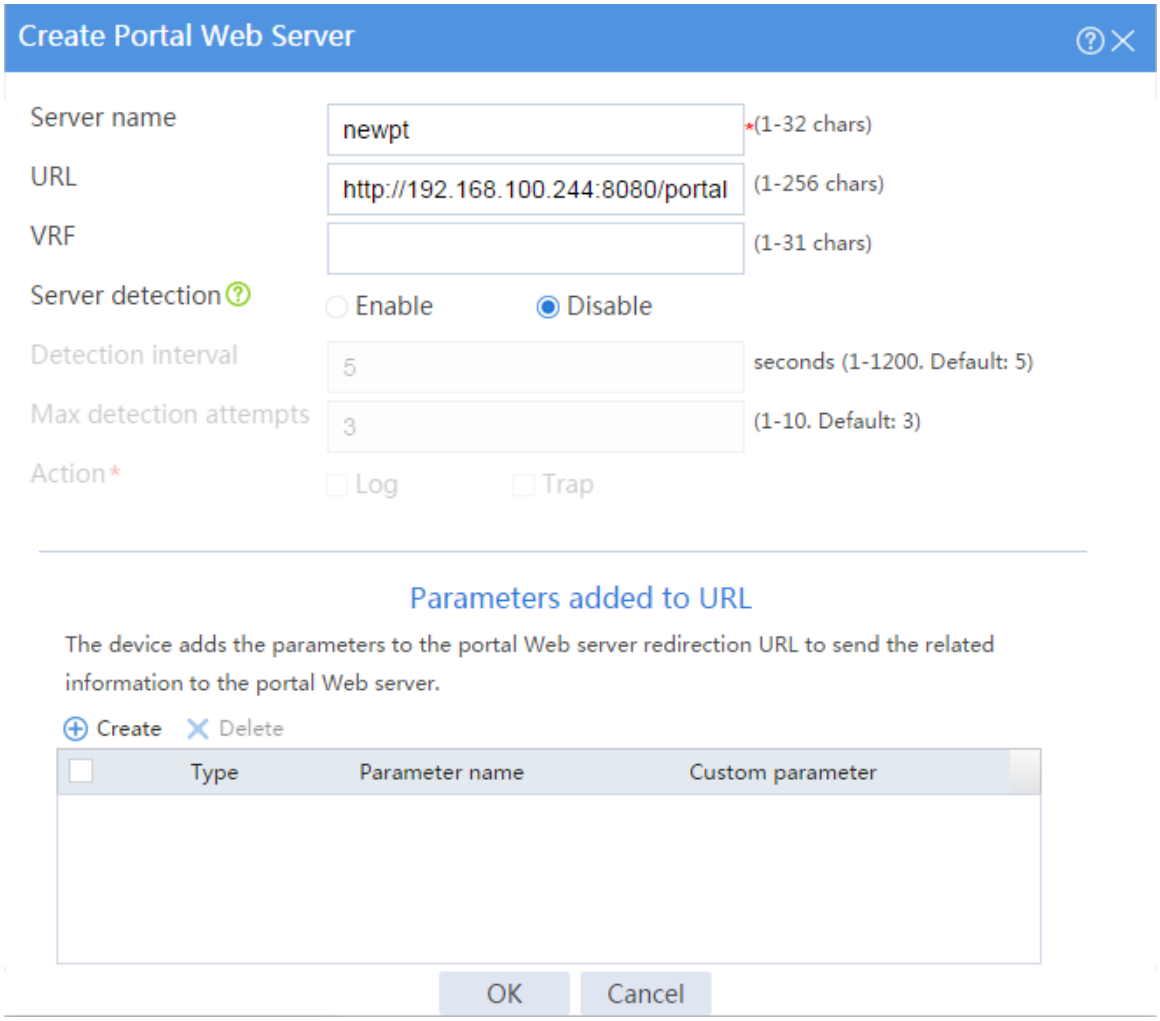
From the navigation pane, select **User** > **Access Control** > **Portal**.

Click the **Portal Web Servers** tab.

Click **Create**.

In the dialog box that opens, configure the server name and URL, as shown in Figure 35. In this example, the URL is http://192.168.100.244:8080/portal.

Figure 35 Creating a portal Web server



Click **OK**.

3. Configure an interface portal policy and enable IPv4 portal on GE 1/0/2:

On the top navigation bar, click **Objects**.

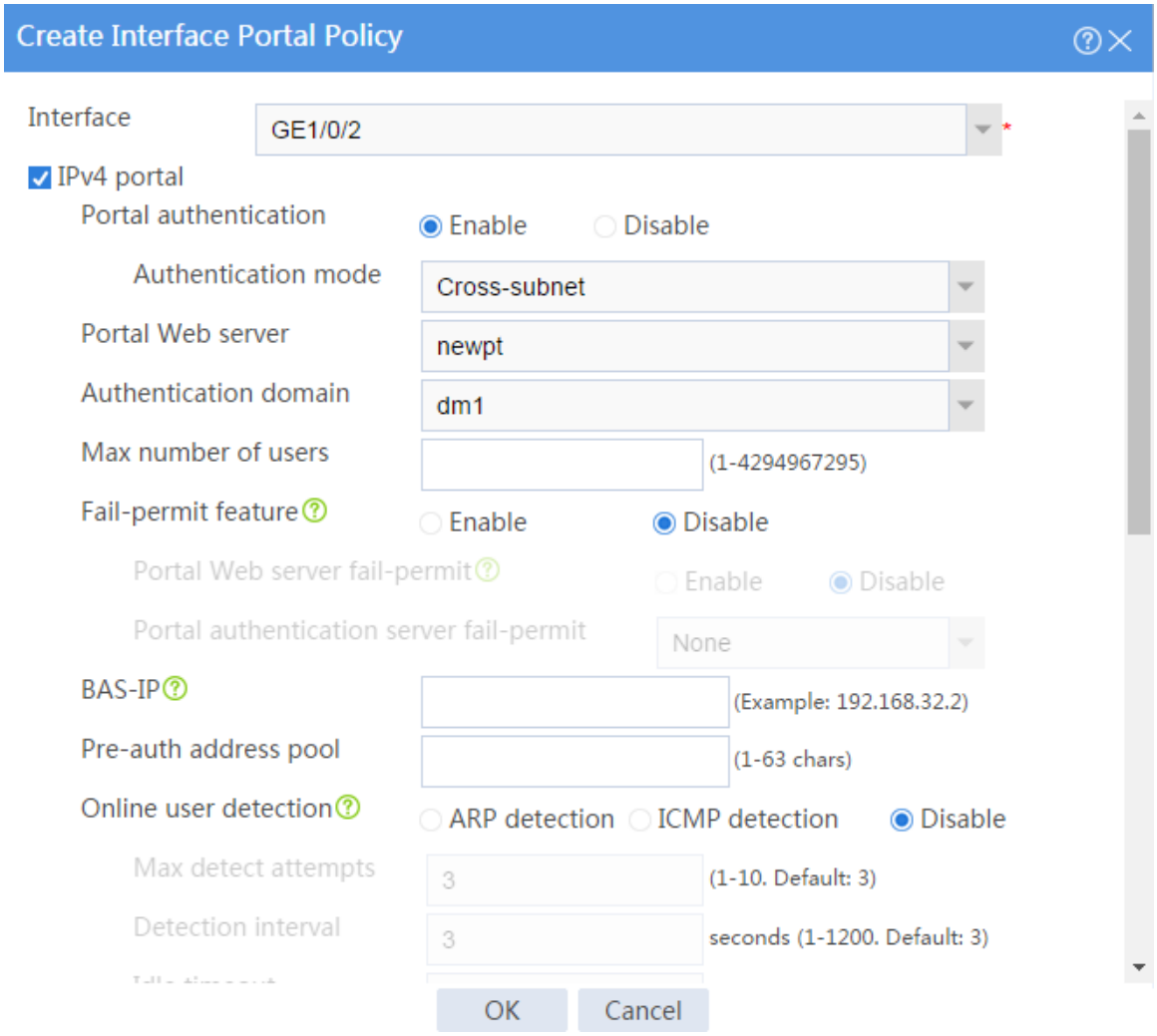
From the navigation pane, select **User** > **Access Control** > **Portal**.

Click the **Interface Portal Policies** tab.

Click **Create**.

In the dialog box that opens, configure the interface portal policy, as shown in Figure 36.

Figure 36 Creating an interface portal policy



Click **OK**.

Configuring user identification

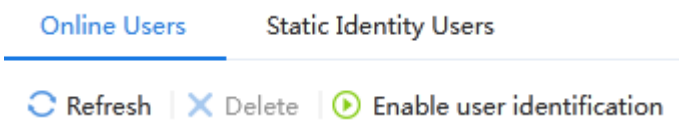
1. Enable user identification:

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **User** > **User Management** > **Online Users**.

   # On the **Online Users** tab, click **Enable user identification**.

Figure 37 Enabling user identification



2. Create RESTful server **rest1**:

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **User** > **Authentication** > **RESTful Server**.

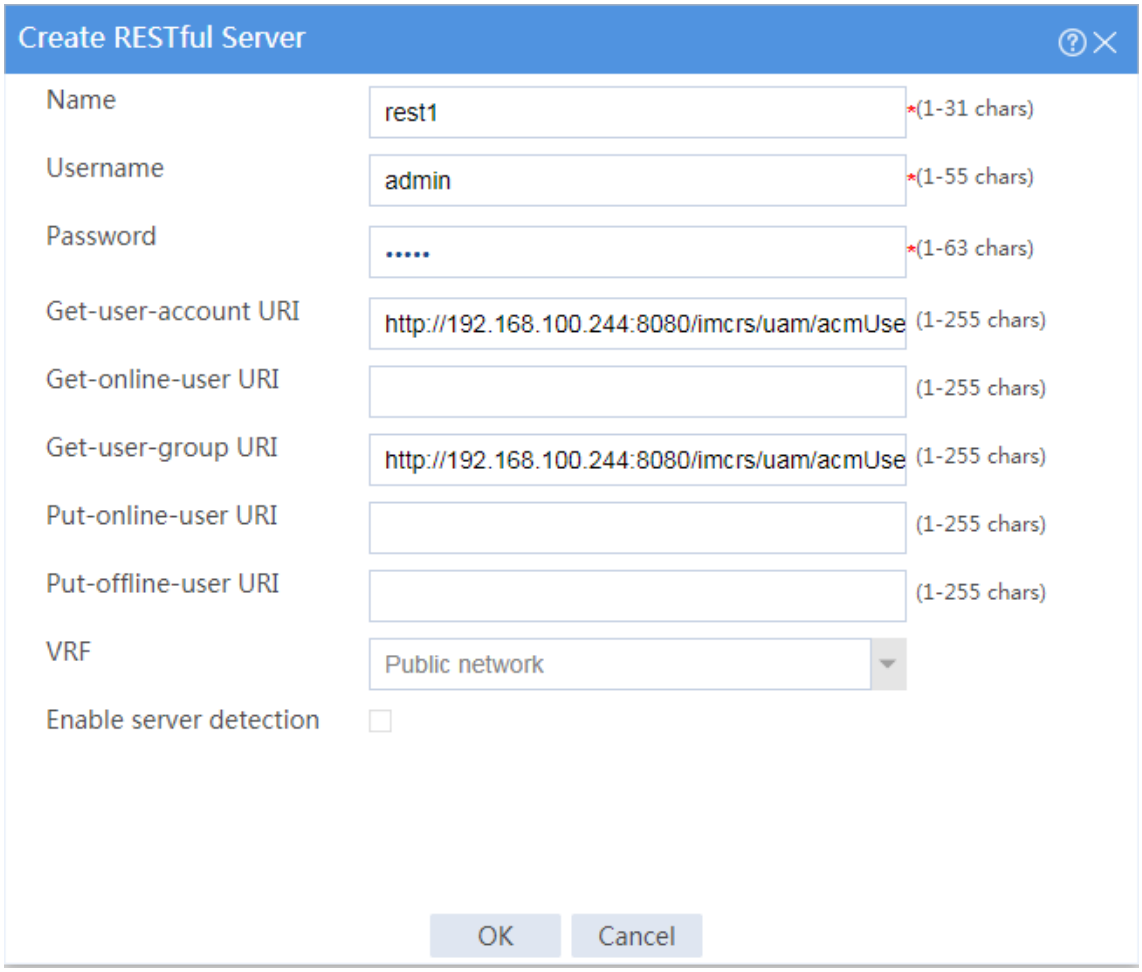
   # Click **Create**.

   # In the dialog box that opens, configure the following parameters for the RESTful server:

   - Enter server name **rest1**.
   - Enter username **admin**.
   - Enter password **admin**.
   - Set the Get-user-account URI to **http://192.168.100.244:8080/imcrs/uam/acmUser/acmUserList**.
   - Set the Get-online-user URI to **http://192.168.100.244:8080/imcrs/uam/online**.
   - Set the Get-user-group URI to **http://192.168.100.244:8080/imcrs/uam/acmUser/userGroup**.

   For an IMC RESTful server, URIs are in a fixed format. You cannot modify any parameters in the above URIs except for the IP address.

Figure 38 Creating the RESTful server



Click **OK**.

3. Create user import policy **imc**:

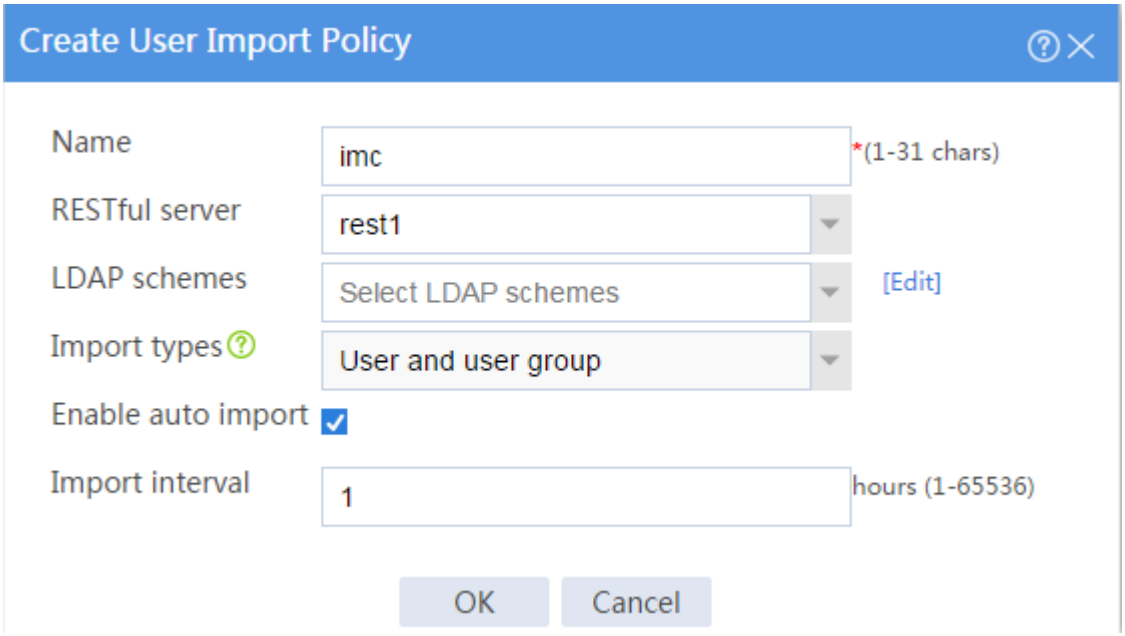
On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **User Import Policies**.

Click **Create**.

In the dialog box that opens, configure parameters for the user import policy, as shown in Figure 39.

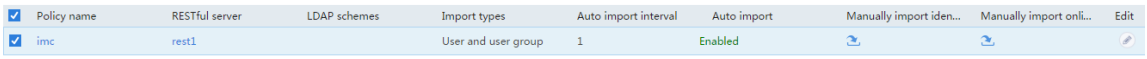
Figure 39 Creating user import policy imc



Click **OK**.

After the firewall and the IMC server can communicate with each other, enter the **User Import Policies** page and click the **Manually import identity users** icon for policy **imc** to import the user accounts on the IMC server to the firewall.

Figure 40 Importing user accounts



Configuring a security policy to permit user user10003 to access the Internet

Perform this task to create a security policy to permit user **user10003** to access the Internet and deny users from the Internet from accessing the internal network.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** > **Create a policy**.

In the dialog box that opens, configure the security policy:

- Enter security policy name **user10003**.
- Select source security zone **Trust**.
- Select destination security zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select user **user10003**.
- Use the default settings for other parameters.

Click **OK**.

Adding the firewall to IMC

Add the firewall to IMC for IMC to monitor and manage the firewall.

1. Log in to IMC:

Enter the IMC URL in the address bar of the Web browser. In this example, the URL is http://192.168.100.244:8080/imc/.

Enter username **admin** and password **admin**.

2. Add the firewall to IMC:

Click the **Resource** tab.

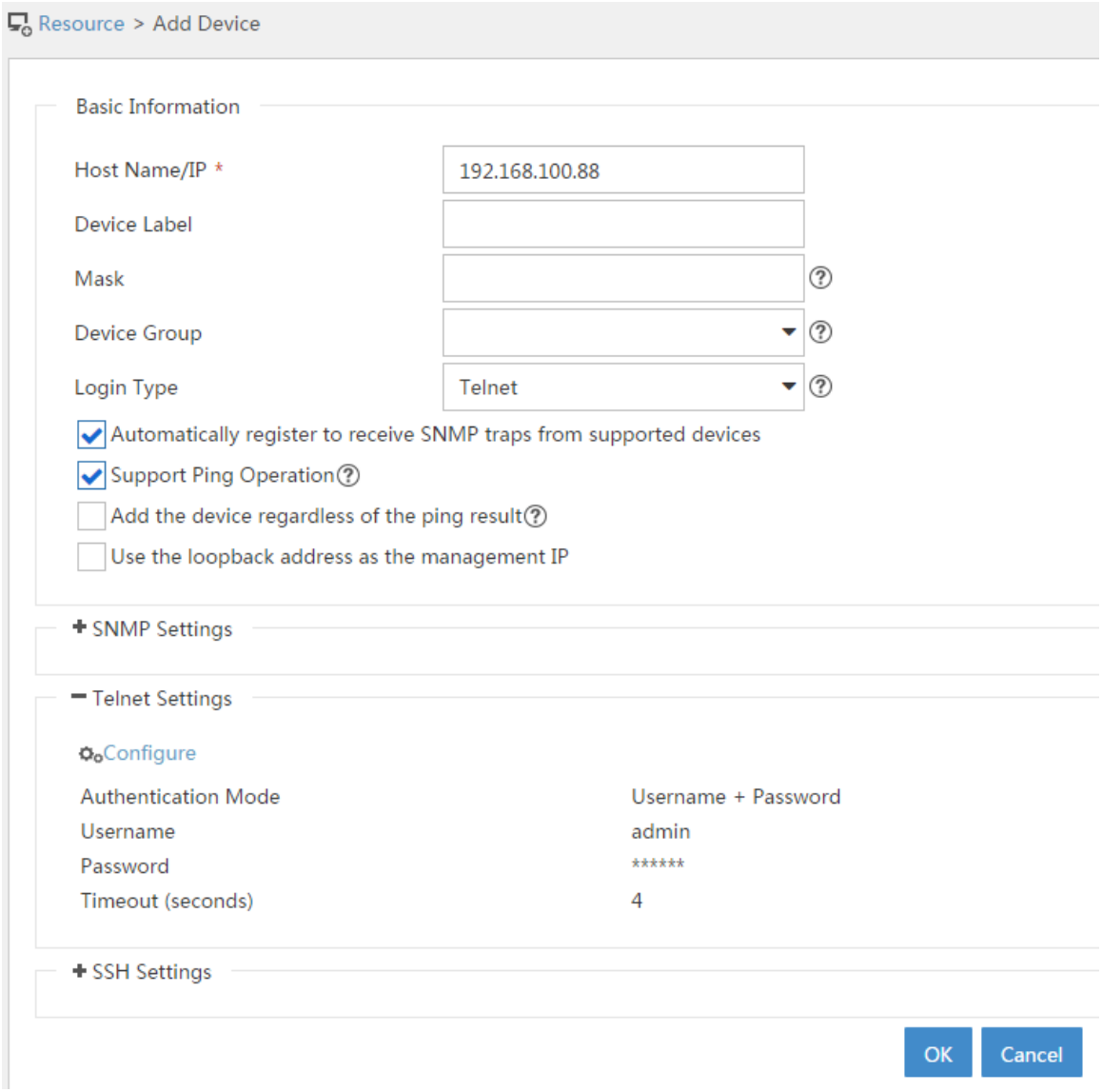
From the navigation tree, select **Resource Management** > **Add Device**.

On the page that opens, configure parameters as shown in Figure 41:

- Set the username and password to **admin** in the **Telnet Settings** area.
- Use the default values for other parameters.

  By default, the read-only SNMP community string is **public** and the read and write SNMP community string is **private**.

Figure 41 Adding the firewall to IMC



Click **OK**.

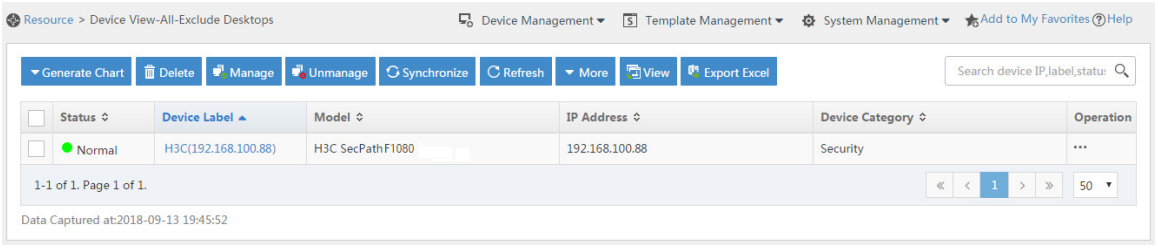
3. Modify NETCONF settings:

Click the **Resource** tab.

From the navigation tree, select **View Management** > **Device View**.

Click the link in the **Device Label** column for the target device.

Figure 42 Device list

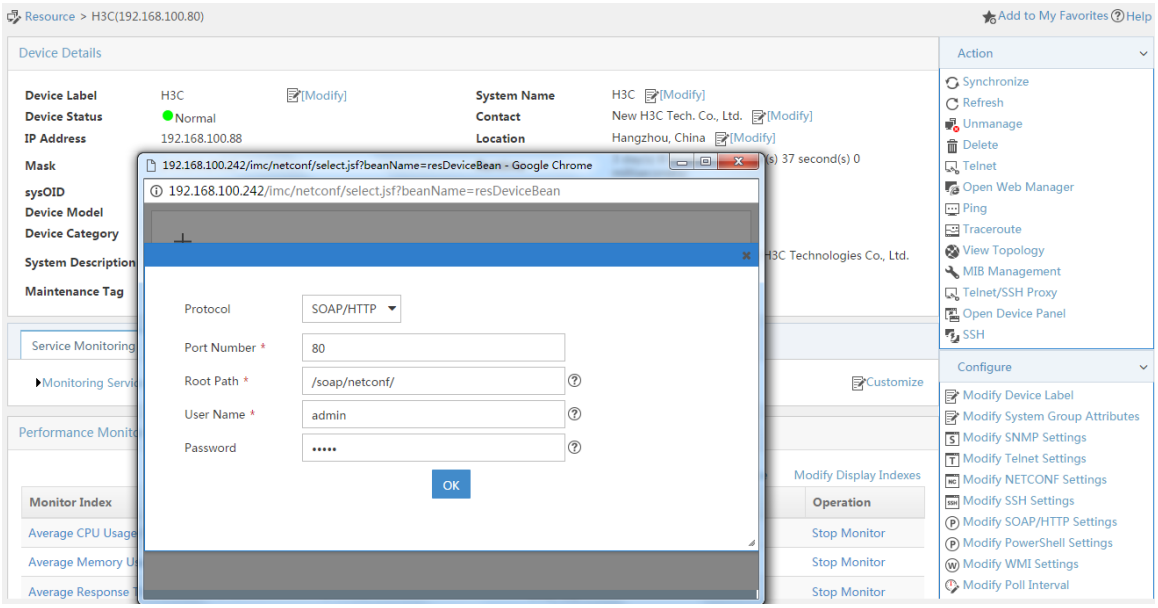


In the right pane, click **Configure** > **Modify NETCONF Settings**.

In the dialog box that opens, click the plus sign (+) to add a protocol as shown in Figure 43.

In this example, set the username and password to **admin**.

Figure 43 Modifying NETCONF settings



Click **OK**.

Configuring security services (IMC)

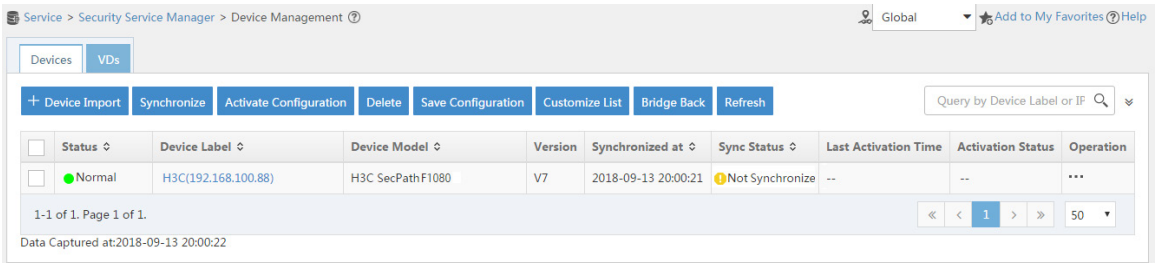
1. Synchronize security services from the firewall to the IMC server to ensure that the configuration and user information is consistent between the firewall and IMC server.

Click the **Service** tab.

From the navigation tree, select **Security Service Manager** > **Device Management**.

On the **Devices** tab, the firewall is displayed in the device list, as shown in Figure 44.

Figure 44 Page for security device management (not synchronized)



Select the firewall in the device list and click **Synchronize**. You can view the synchronization status from the **Sync Status** column, as shown in Figure 45 and Figure 46.

The synchronization process might take a long time. Please wait.

Figure 45 Page for security device management (synchronizing)

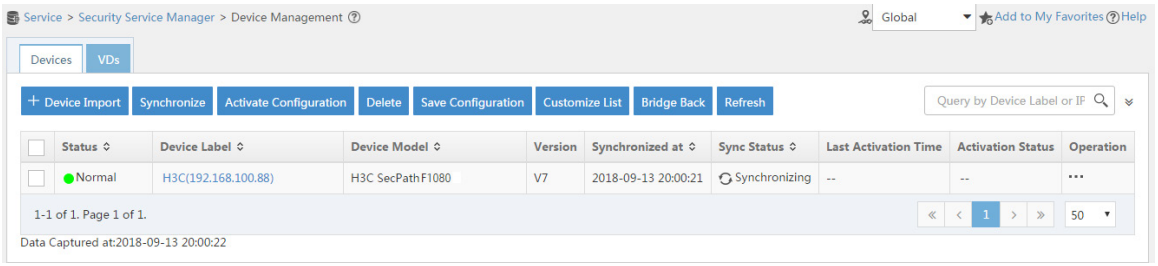
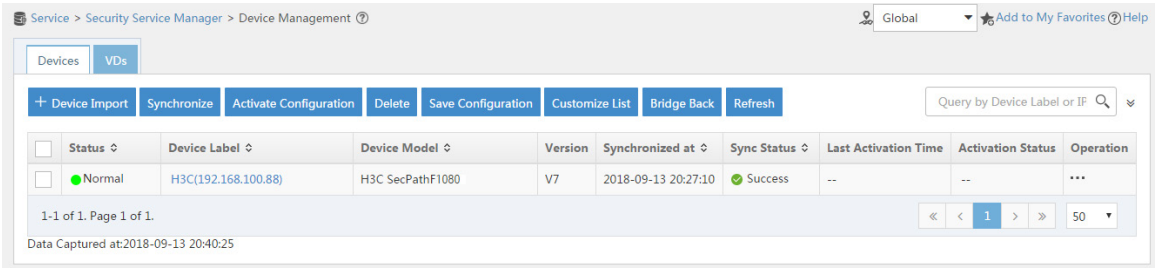


Figure 46 Page for security device management (synchronization succeeded)



2. Configure user authentication system parameters and user notification parameters to ensure

that the IMC server synchronizes user online and offline information to the firewall in real time.

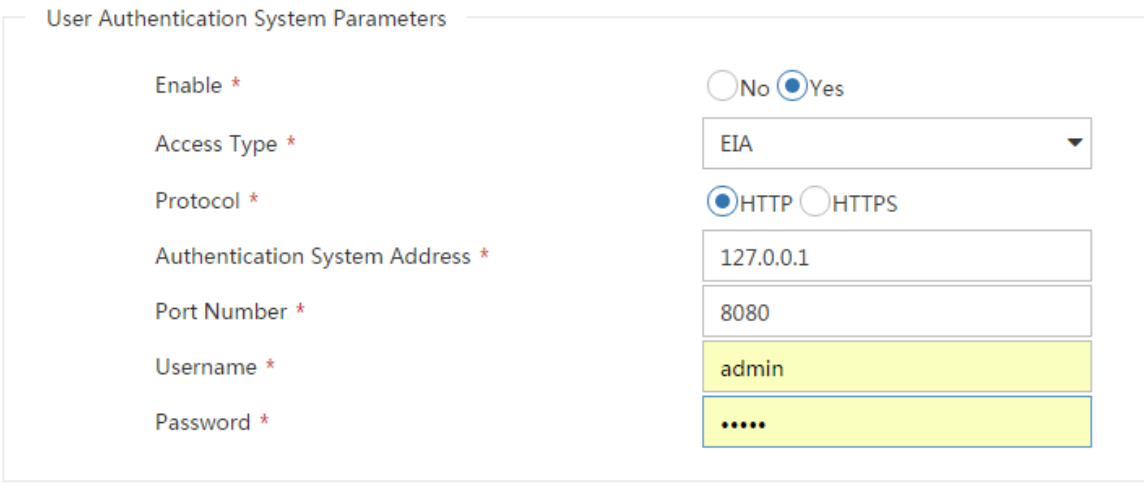
Click the **Service** tab.

From the navigation tree, select **Security Service Manager** > **Global Parameters**.

Configure the user authentication system parameters, as shown in Figure 47.

Select a protocol depending on the protocol of the portal authentication server. Make sure the username and password is the same as that used to log in to the IMC server.

Figure 47 Configuring user authentication system parameters



Click **OK**.

Click the **User** tab.

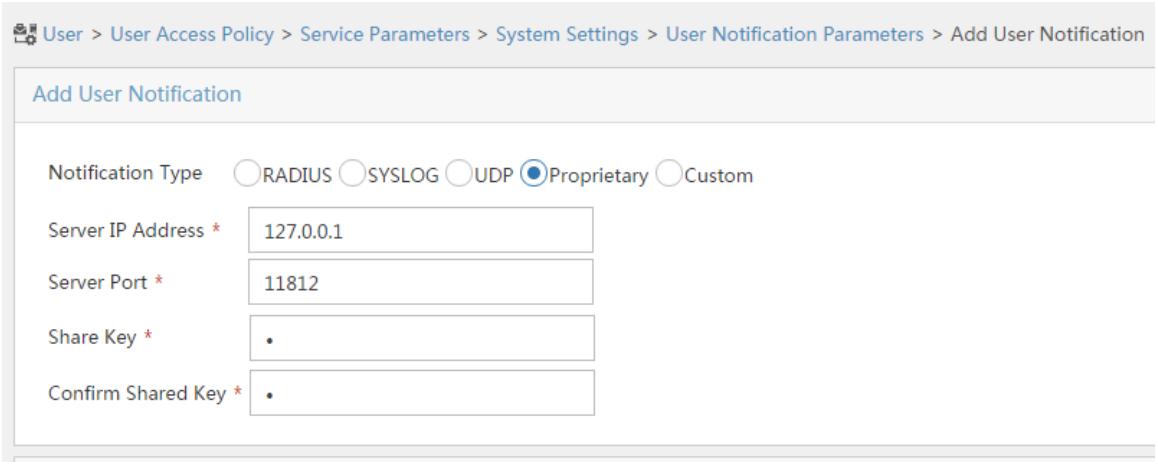
From the navigation tree, select **User Access Policy** > **Service Parameters** > **System Settings**.

Click the **Configure** icon for **User Notification Parameters**.

On the page that opens, click **Add**.

On the **Add User Notification** page, configure the parameters as shown in Figure 48. In this example, you can enter a shared key randomly.

Figure 48 Configuring user notification parameters



Click **OK**.

Configuring the RADIUS server (IMC)

1. Add the firewall to the IMC server as an access device:

   # Click the **User** tab.

   # From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.

   # Click **Add**.

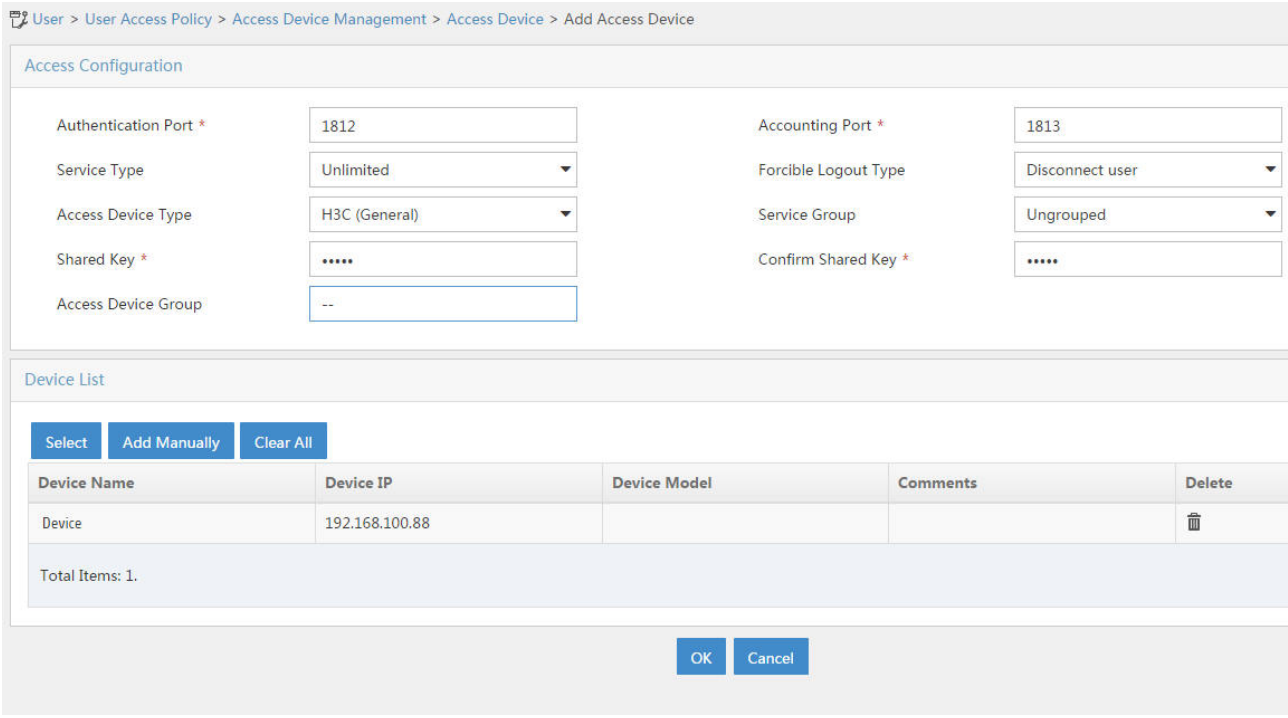
   # In the **Access Configuration** area, set the shared key to **admin**, as shown in Figure 49.

   # In the **Device List** area, click **Select** or **Add Manually** to add the device at 192.168.100.88 as an access device.

   You must specify the source IP address of outgoing RADIUS packets on the firewall as the IP address of the access device on the server.

   On the firewall, the source IP address is configured by using the **`nas-ip`** or **`radius nas-ip`** command. The IP address configured by using the **`nas-ip`** command has a higher priority than the IP address configured by using the **`radius nas-ip`** command. If no IP address is specified as the source IP address, the IP address of the packet outbound interface is used as the source IP address. In this example, the IP address of the packet outbound interface is used, which is 192.168.100.88.

Figure 49 Adding an access device



Click **OK**.

2. Add an access policy:

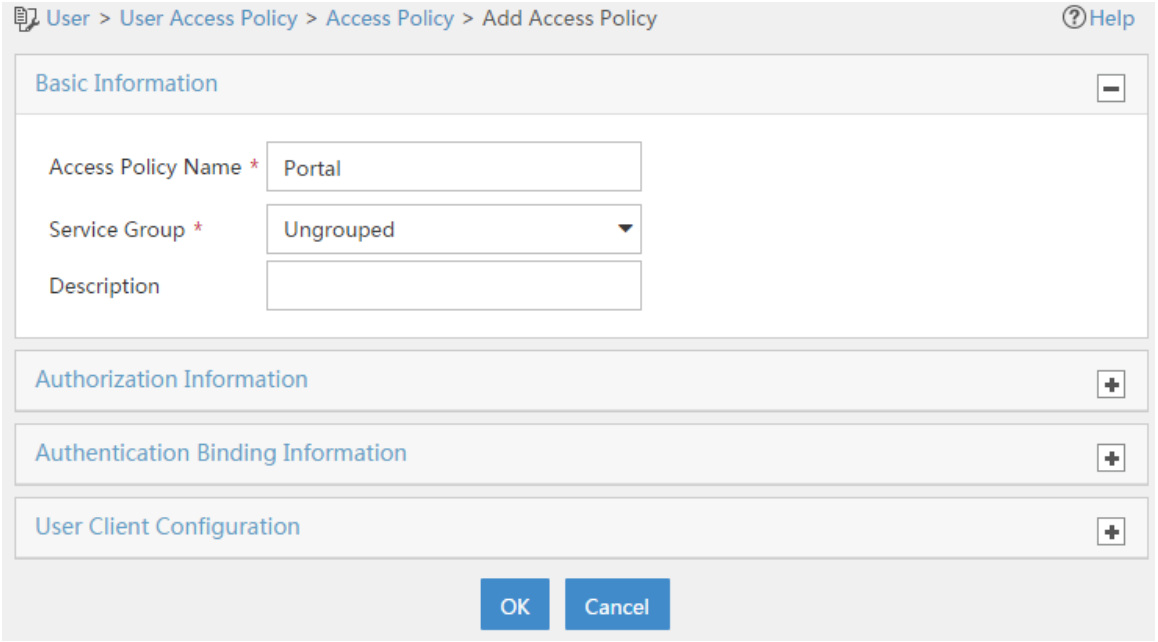
Click the **User** tab.

From the navigation tree, select **User Access Policy** > **Access Policy**.

Click **Add**.

On the **Add Access Policy** page, set the access policy name to **Portal**, as shown in Figure 50.

Figure 50 Adding an access policy



Click **OK**.

3. Add an access service:

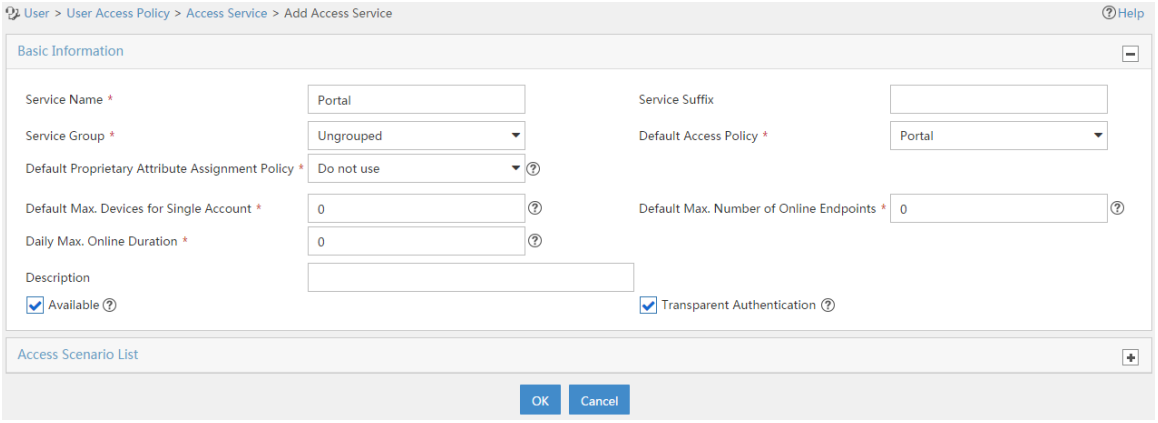
Select the **User** tab.

From the navigation tree, select **User Access Policy** > **Access Service**.

Click **Add**.

On the **Add Access Service** page, set the service name to **Portal** and select **Portal** from the **Default Access Policy** list.

Figure 51 Adding an access service



Click **OK**.

4. Add an access user:

Click the **User** tab.

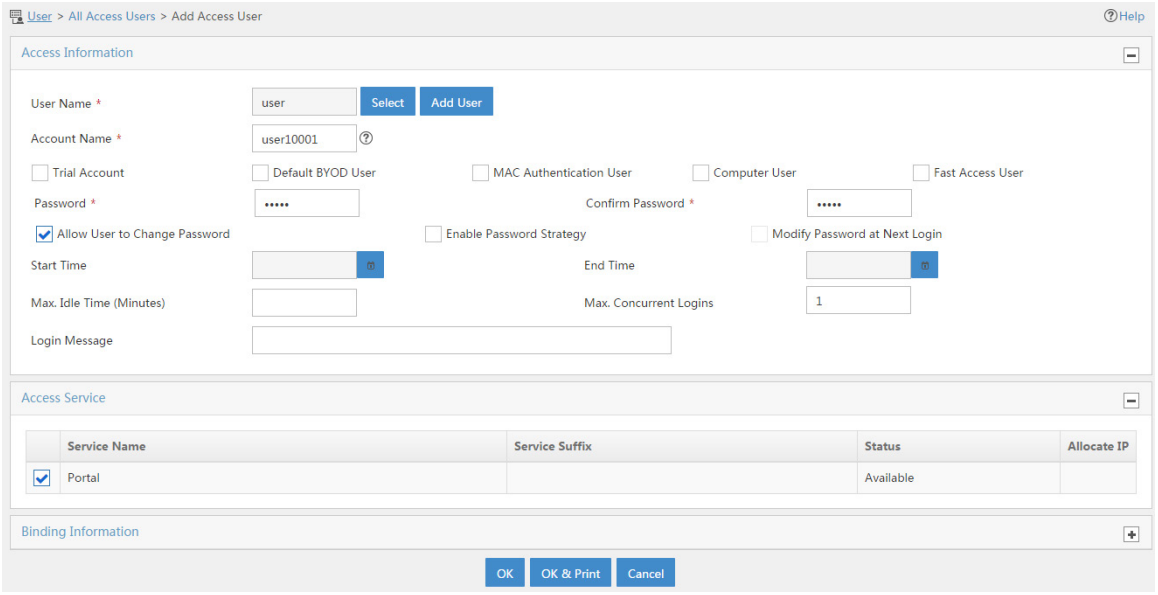
From the navigation tree, select **Access User** > **All Access Users**.

Click **Add**.

On the **Add Access User** page, configure parameters as shown in Figure 52.

- Enter **user** in the **User Name** field.
- Enter **user10001** in the **Account Name** field.
- Enter **admin** in the **Password** and **Confirm Password** fields.
- Select **Portal** in the **Access Service** area.

Figure 52 Adding an access user



Click **OK**.

Add user accounts **user10002** and **user10003** in the same way you add user account **user10001**.

Configuring the portal server (IMC)

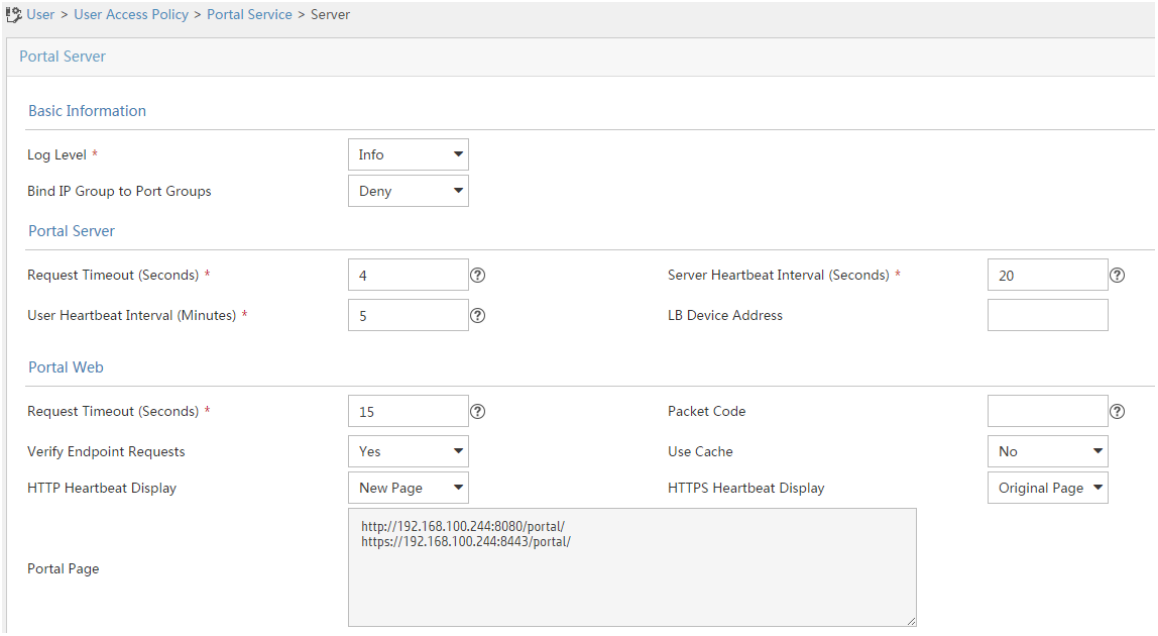
1. Configure the portal server:

   # Click the **User** tab.

   # From the navigation tree, select **User Access Policy** > **Portal Service** > **Server**.

   # Configure the parameters in Figure 53 depending on the network conditions. In this example, the default values are used.

Figure 53 Portal server configuration



Click **OK**.

2. Add an IP group:

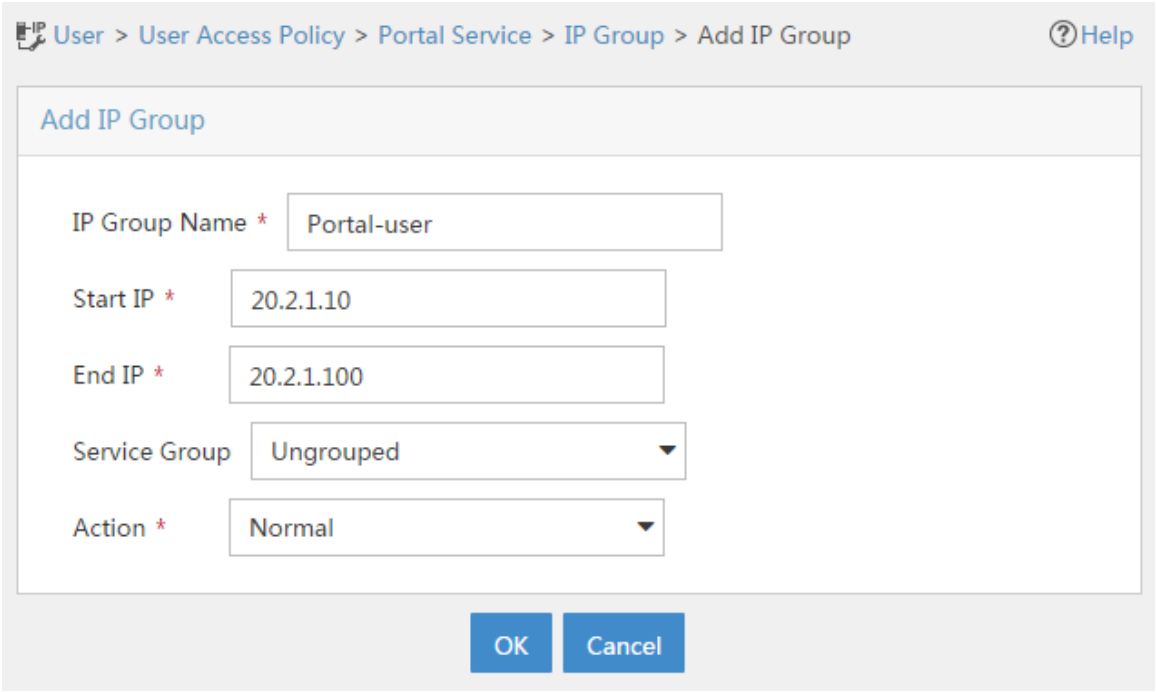
Click the **User** tab.

From the navigation tree, select **User Access Policy** > **Portal Service** > **IP Group**.

Click **Add**.

On the **Add IP Group** page, configure the IP group parameters as shown in Figure 54.

Figure 54 Adding an IP group



Click **OK**.

3. Add a portal device:

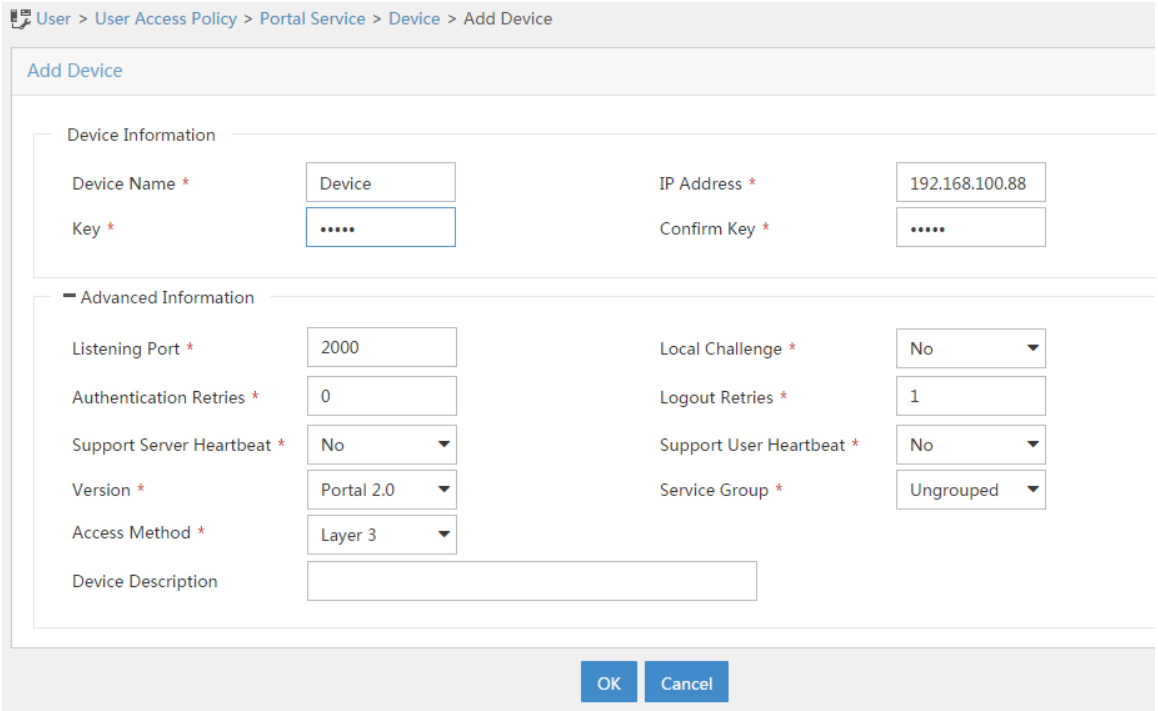
   # Click the **User** tab.

   # From the navigation tree, select **User Access Policy** > **Portal Service** > **Device**.

   # Click **Add**.

   # On the **Add Device** page, set the key to **admin** and configure other parameters as shown in Figure 55.

Figure 55 Adding portal device configuration



Click **OK**.

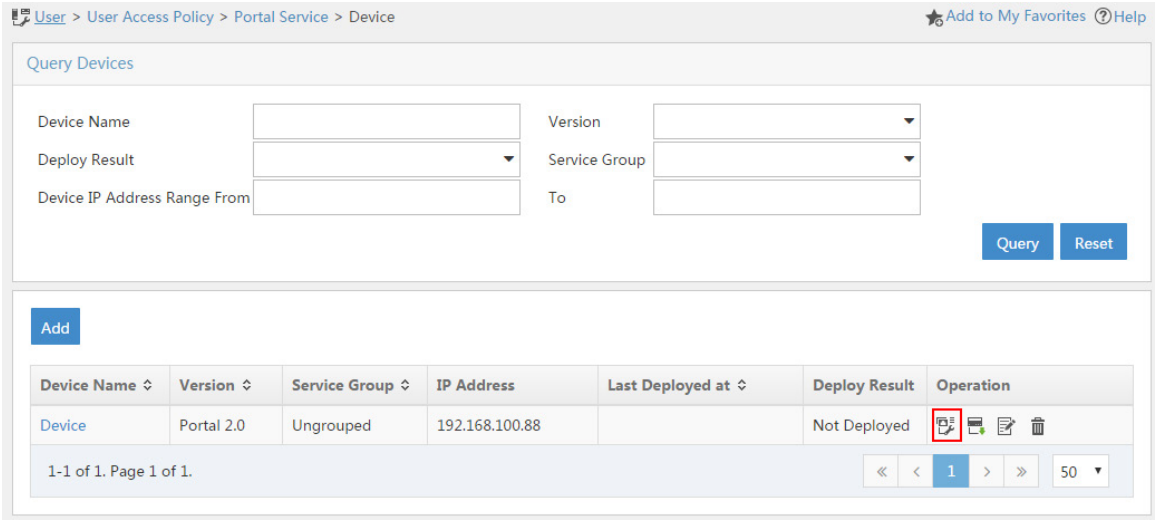
4. Associate the portal device with the IP group:

Click the **User** tab.

From the navigation tree, select **User Access Policy** > **Portal Service** > **Device**.

Click the **Port Group** icon in the **Operation** column for the firewall

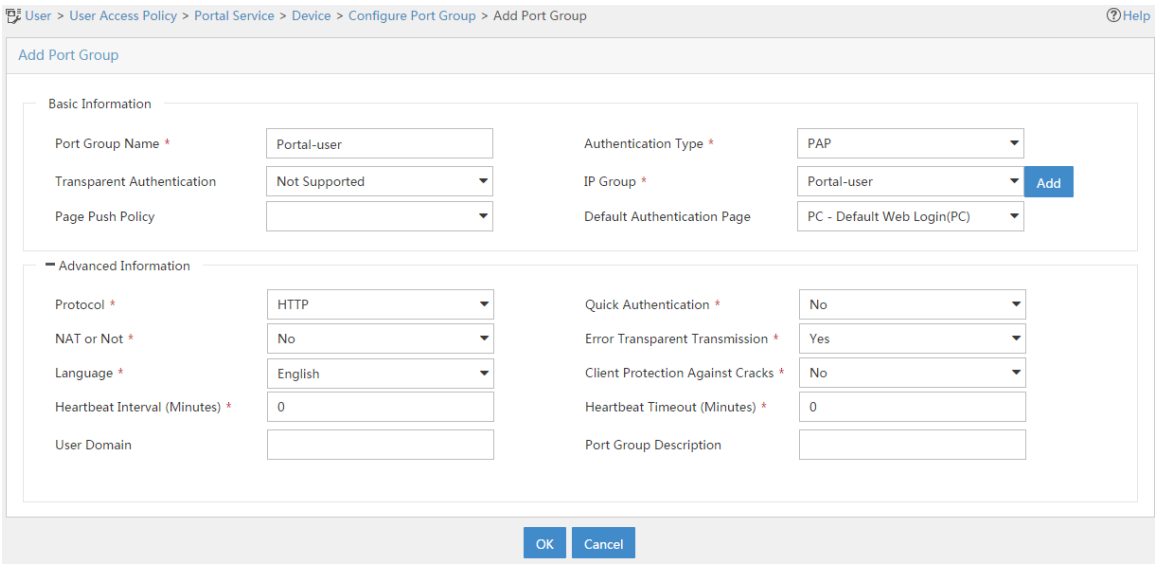
Figure 56 Device list



On the page that opens, click **Add**.

On the page that opens, configure a port group as shown in Figure 57.

Figure 57 Adding a port group



Click **OK**.

Configuring the hosts

Configure the IP address, network mask, and default gateway settings for each host. Make sure the hosts can communicate with the devices in the network. (Details not shown.)

Verifying the configuration

1. On the hosts, verify that the users can pass portal authentication.

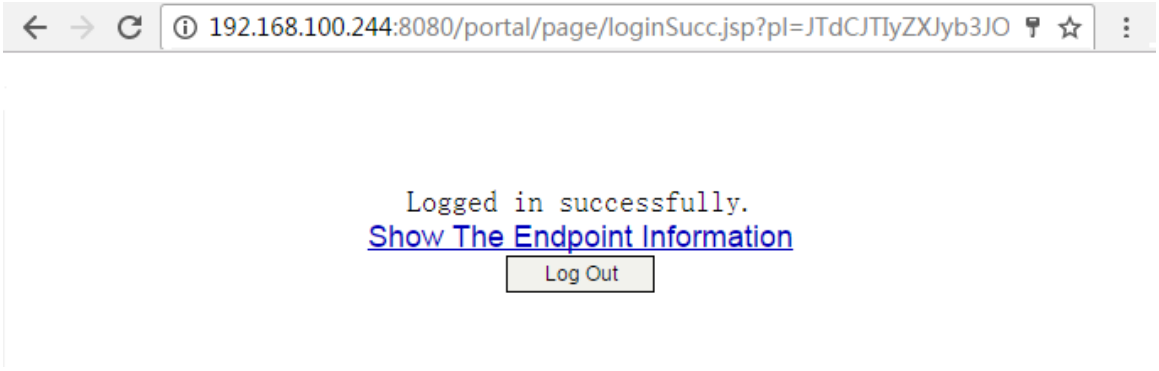
   # Enter the URL of the portal Web server in the address bar of the Web browser to log in to the portal authentication page. In this example, the URL is http://192.168.100.244:8080/portal.

   # Enter the username and password.

   # Click **Log In**.

   # Verify that the user has passed portal authentication.

   Figure 58 Portal authentication success page



2. On the IMC server, verify that users **user10001**, **user10002**, and **user10003** are in the online user list after they pass portal authentication. To view the online user list, click the **User** tab and select **Access User** > **Online Users** from the navigation tree.
3. On the firewall, display information about all portal users.

   ```
   [Device] display portal user all
   ```

```
Total portal users: 3
Username: user10001
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC             IP                    VLAN    Interface
  0011-95e4-4aa9  20.2.1.13            --      GigabitEthernet1/0/2
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
Outbound CAR: N/A

Username: user10002
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC             IP                    VLAN    Interface
  0011-95e4-4aa3  20.2.1.13            --      GigabitEthernet1/0/2
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

```
Username: user10003
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC             IP                    VLAN    Interface
  0011-95e4-4aa2  20.2.1.13             --      GigabitEthernet1/0/2
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

4. On the firewall, display identity user information.

Display information about all identity users.

```
[Device] display user-identity all user
  User ID     Username
  0x2         user10001
  0x3         user10002
  0x4         user10003
```

Display information about online identity user **user10001**.

```
[Device] display user-identity online-user null-domain name user10001
User name: user10001
  IP  : 20.2.1.11
  MAC : 0011-95e4-4aa9
  Type: Dynamic


Total 1 records matched.
```

Display information about online identity user **user10002**.

```
[Device] display user-identity online-user null-domain name user10002
User name: user10002
  IP  : 20.2.1.12
  MAC : 0011-95e4-4aa3
  Type: Dynamic

Total 1 records matched.
```

Display information about online identity user **user10003**.

```
[Device] display user-identity online-user null-domain name user10003
User name: user10003
  IP  : 20.2.1.13
  MAC : 0011-95e4-4aa2
  Type: Dynamic

Total 1 records matched.
```

5. Verify that the firewall can perform identity-based access control on the users:

Verify that user **user10001** cannot ping any host in the Internet. In this example, the user pings the host at 12.1.1.2.

```
C:\>ping 12.1.1.2

Pinging 12.1.1.2 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.

Ping statistics for 12.1.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Verify that user **user10003** can ping hosts in the Internet. In this example, the user pings

the host at 12.1.1.2.

```
C:\>ping 12.1.1.2

Pinging 12.1.1.2 with 32 bytes of data:
Reply from 12.1.1.2: bytes=32 time=36ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 12.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

When user **user10003** pings the host in the Internet, the firewall generates a message.

Configuration files

Router

```
[Router] display current-configuration
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 20.2.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
```

```
 ip address 20.2.2.1 255.255.255.0
#
interface GigabitEthernet3/0
 port link-mode route
 combo enable copper
#
 ip route-static 0.0.0.0 0 20.2.2.2
#
 snmp-agent
 snmp-agent local-engineid 800063A28074258A37B5F500000001
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
#
local-user admin class manage
 password                                                          hash
$h$6$UbIhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
 service-type telnet http
 authorization-attribute user-role network-admin
#
return
```

Device

```
[Device] display current-configuration
#
interface GigabitEthernet1/0/1
```

```
 port link-mode route
 ip address 192.168.100.88 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.2.2.2 255.255.255.0
 portal enable method direct
 portal domain dm1
 portal apply web-server newpt
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
#
security-zone name DMZ
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/3
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
 ip route-static 0.0.0.0 0 12.1.1.2
 ip route-static 20.2.1.0 24 20.2.2.1
```

```
#
 snmp-agent
 snmp-agent local-engineid 800063A280487ADA9593B700000001
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 192.168.100.244 params
securityn
ame public v2c
#
radius scheme rs1
 primary authentication 192.168.100.244
 primary accounting 192.168.100.244
 key authentication cipher $c$3$hhbEbD5Ycvw7VWqljAoMoU7hQRgcUjtg
 user-name-format without-domain
#
domain dm1
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal radius-scheme rs1
#
domain system
#
 domain default enable system
#
local-user admin class manage
 password                                                              hash
$h$6$UbIhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
```

```
 service-type ssh telnet terminal http https
 authorization-attribute user-role level-3
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
portal web-server newpt
 url http://192.168.100.244:8080/portal
#
portal server newpt
 ip 192.168.100.244 key cipher $c$3$+UmaGOco7eHsjOqlrp8lI4eYe0A8NpYU
#
 netconf soap http enable
 netconf soap https enable
 restful http enable
 restful https enable
#
 user-identity enable
 user-identity user-account auto-import policy imc
#
user-identity restful-server rest1
 login-name admin password cipher $c$3$phGy00HA6OP6pIpGI0KOKZEOPuLVbtt/
 uri                                                    get-user-database
http://192.168.100.244:8080/imcrs/uam/acmUser/acmUserList
 uri                                                get-user-group-database
http://192.168.100.244:8080/imcrs/uam/acmUser/userGroup
 uri get-online-user http://192.168.100.244:8080/imcrs/uam/online
#
user-identity user-import-policy imc
 account-update-interval 1
```

```
 restful-server rest1
#
security-policy ip
 rule 0 name dmz-local
  action pass
  source-zone dmz
  destination-zone local
 rule 1 name local-dmz
  action pass
  source-zone local
  destination-zone dmz
 rule 2 name trust-dmz
  action pass
  source-zone trust
  source-zone dmz
  destination-zone dmz
  destination-zone trust
 rule 3 name user10003
  action pass
  logging enable
  source-zone trust
  destination-zone untrust
  user user10003
#
return
```

Example: Configuring user identification for users obtained from a Dr.Com server (Dr.Com server

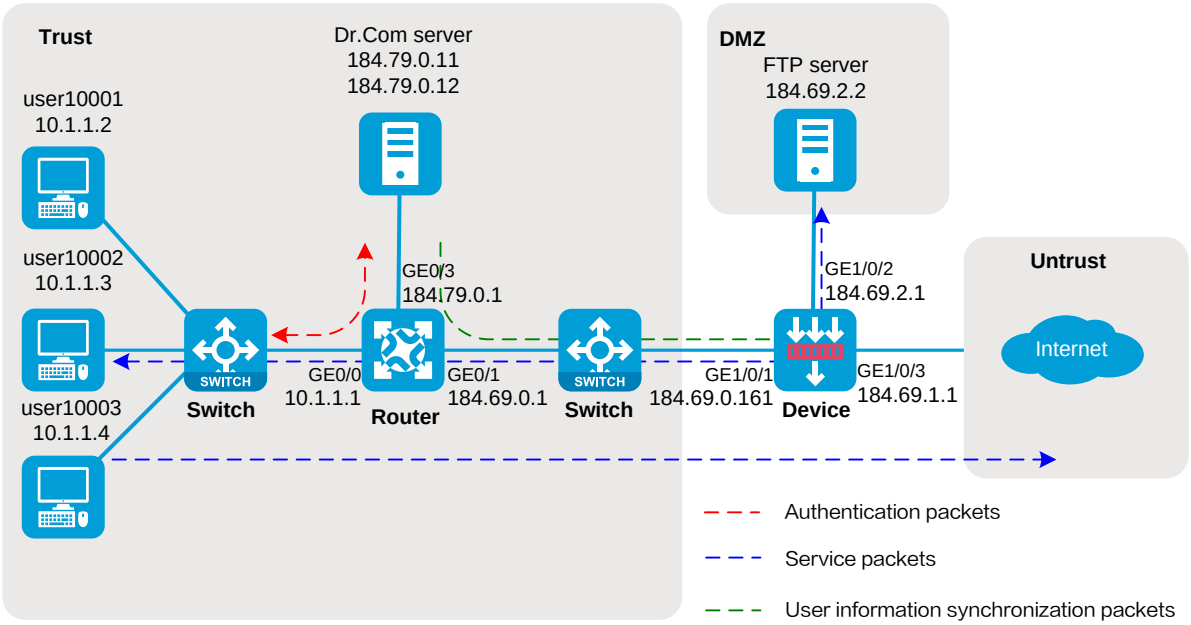
single sign-on)

Network configuration

As shown in Figure 59:

- A Dr.Com server is deployed for user authentication, authorization, and accounting in the campus network.
- Device (firewall) acts as a gateway to control access between the campus network and the Internet.
- Device obtains all user accounts, online users, and user online and offline messages from the server.
- Device performs the following identity-based access control on online users based on the information synchronized from the server:
  - User **user10001** cannot access the FTP server or Internet.
  - User **user10002** can access the FTP server but cannot access the Internet.
  - User **user10003** can access the Internet but cannot access the FTP server.
  - Users from the Internet cannot access the hosts in the **Trust** and **DMZ** security zones.
- The Dr.Com server has two IP addresses:
  - One IP address is 184.79.0.12 for communication with users, user identity authentication, and authorization.
  - The other IP address is 184.79.0.11 for communication with Device and user information synchronization.

Figure 59 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Prerequisites

Create the users on the Dr.Com server.

Configure access authentication settings on the network access devices to ensure that the users can pass authentication on the Dr.Com server and obtain authorization information from the server.

Procedure

Configuring the Dr.Com server

1. Add the IP address and port number of Device to the server:

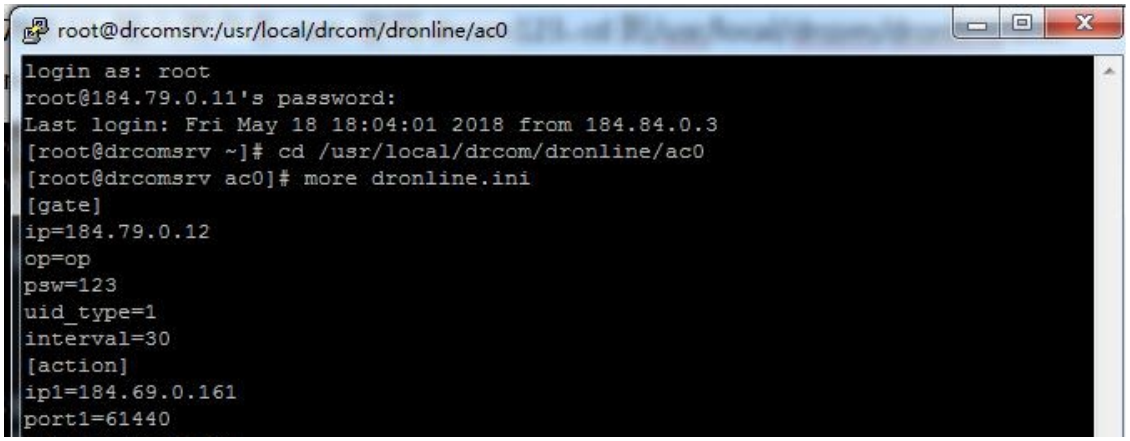
Use SSH to access 184.79.0.11/24 and enter the username and password to log in to the CLI of the DR.Com server.

Change the work directory to /usr/local/drcom/dronline/ac0.

Configure the following parameters under the **action** title in the **dronline.ini** file:

- Set the value for the **ip1** parameter to 184.69.0.161 (IP address of Device).
- Set the value for the **port1** parameter to 61440.

Figure 60 Adding the IP address and port number of Device



2. Enable UDP interface process and get interface process on the server:

Enable UDP interface process for pushing user online and offline messages.

```
cd /usr/local/drcom/dronline/ac0
./dronline
```

Enable get interface process for responding to the requests from Device for importing user accounts and online users in bulk.

```
cd /usr/local/drcom/DrcomSup
java -jar DrcomSup.jar --server.port=8003
```

Verify that the server can push user online and offline messages to Device and respond to the requests from Device. (Details not shown.)

Configuring Device (the firewall)

1. Assign IP addresses to interfaces and add the interfaces to security zones:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Trust** security zone.

b. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 184.69.0.161/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **DMZ** security zone and set its IP address to 184.69.2.1/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Untrust** security zone and set its IP address to 184.69.1.1/24 in the same way you configure GE 1/0/1.

2. Configure routing:

This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure the IPv4 static route:

- Enter 184.79.0.0 in the **Destination address** field.
- Enter 24 in the **Mask length** field.
- Enter 184.69.0.1 as the next hop address in the **Next hop** field.
- Use the default settings for other parameters.

Click **OK**.

Configure a static route destined for 10.1.1.0/24 in the same way the static route destined for 184.79.0.0/24 is configured.

Configure a static route destined for the Internet in the same way the static route destined for 184.79.0.0/24 is configured.

3. Configure security policies to permit traffic between the Dr.Com server and Device:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** > **Create a policy**.

Configure the following parameters in the security policy for Device to import user information from the Dr.Com server:

- Set the name to **trust-local**.
- Select **Trust** as the source security zone.
- Select **Local** as the destination security zone.
- Set the type to IPv4.
- Select action **Permit**.
- Specify 184.79.0.0/24 as the source IPv4 address.
- Use the default settings for other parameters.

Click **OK**.

Configure security policy **local-trust** for Device to send traffic to the Dr.Com server in the same way security policy **trust-local** is configured. Configure the following parameters for security policy **local-trust**:

- Set the name to **local-trust**.
- Select **Local** as the source security zone.
- Select **Trust** as the destination security zone.
- Set the type to IPv4.
- Select action **Permit**.
- Specify 184.79.0.0/24 as the destination IPv4 address.
- Use the default settings for other parameters.

Click **OK**.

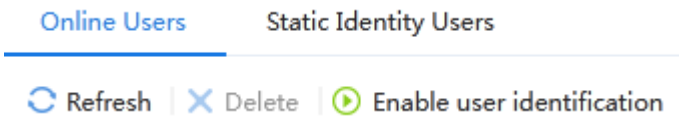
4. Enable user identification:

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **User** > **User Management** > **Online Users**.

   # On the **Online Users** tab, click **Enable user identification**.

   Figure 61 Enabling user identification

5. Configure a RESTful server for synchronizing user accounts and online users from the Dr.Com server:

   # On the top navigation bar, click **Objects**.

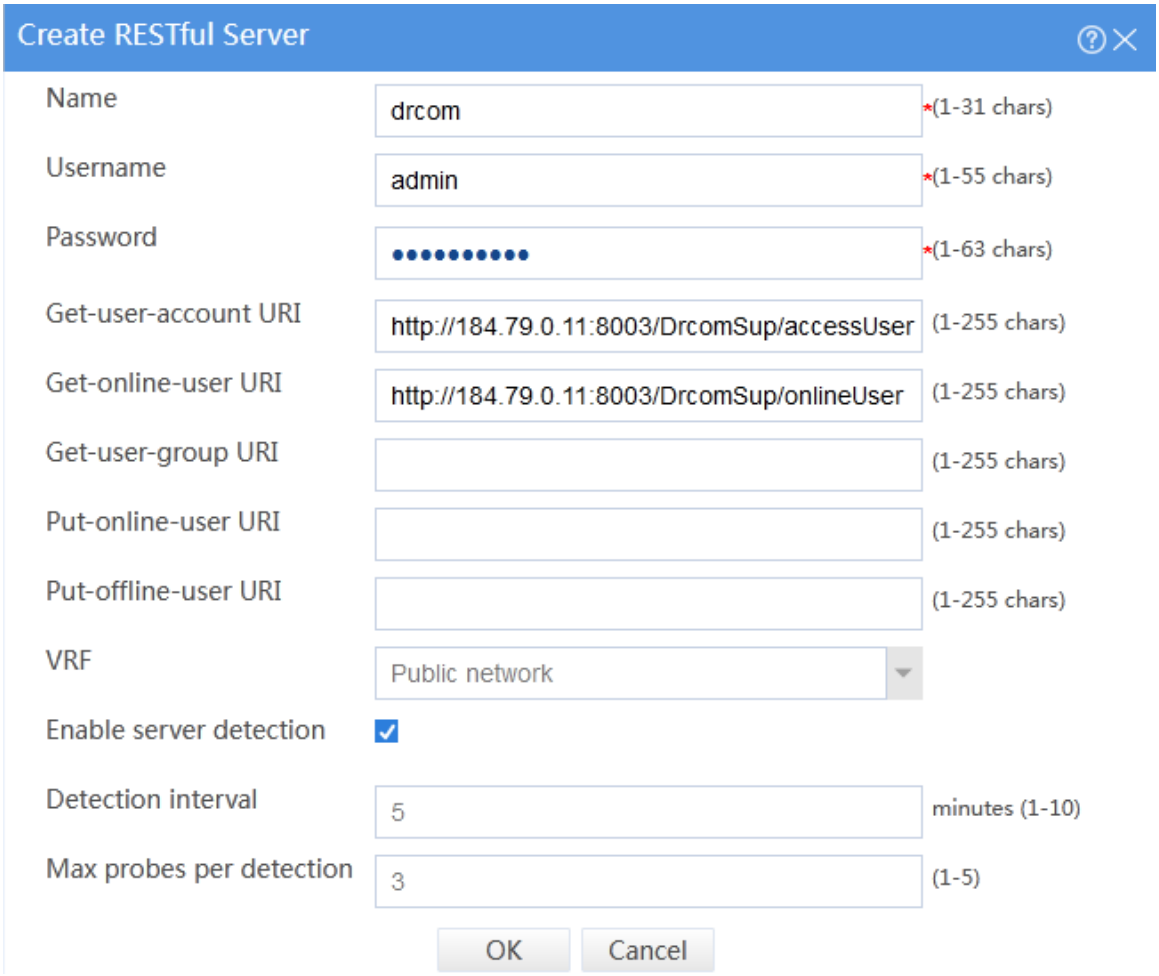
   # From the navigation pane, select **User** > **Authentication** > **RESTful Server**.

   # Click **Create**.

   # Configure the following parameters for the RESTful server:

   - Set the name to **drcom**.
   - Set the username to the username used to access the Dr.Com server.
   - Set the password to the password used to access the Dr.Com server.
   - Set the Get-user-account URI to http://184.79.0.11:8003/DrcomSup/accessUser.
   - Set the Get-online-user URI to http://184.79.0.11:8003/DrcomSup/onlineUser.
   - Enable server detection.
   - Use the default settings for other parameters.

Figure 62 Configuring a RESTful server



Click **OK**.

6. Configure a security management server set to receive user online and offline messages pushed from the Dr.Com server:

   # On the top navigation bar, click **Objects**.

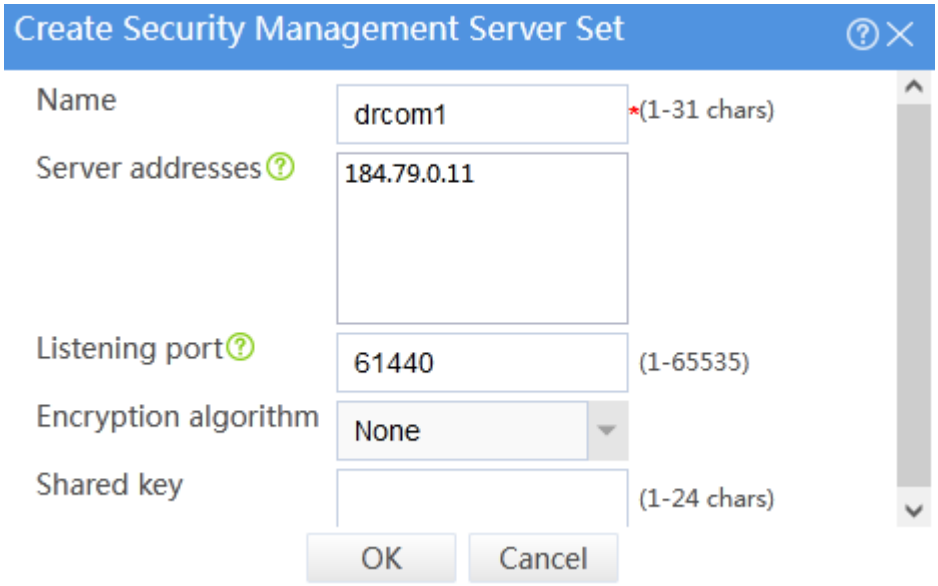
   # From the navigation pane, select **User** > **Authentication** > **Sec Mgt Server Set**.

   # Click **Create**.

   # Configure the following parameters for the security management server set:

   - Set the name to **drcom1**.
   - Set the server address to 184.79.0.11.
   - Set the listening port to 61440.
   - Use the default settings for other parameters.

Figure 63 Configuring a security management server set



Click **OK**.

7. Configure a user import policy:

   # On the top navigation bar, click **Objects**.

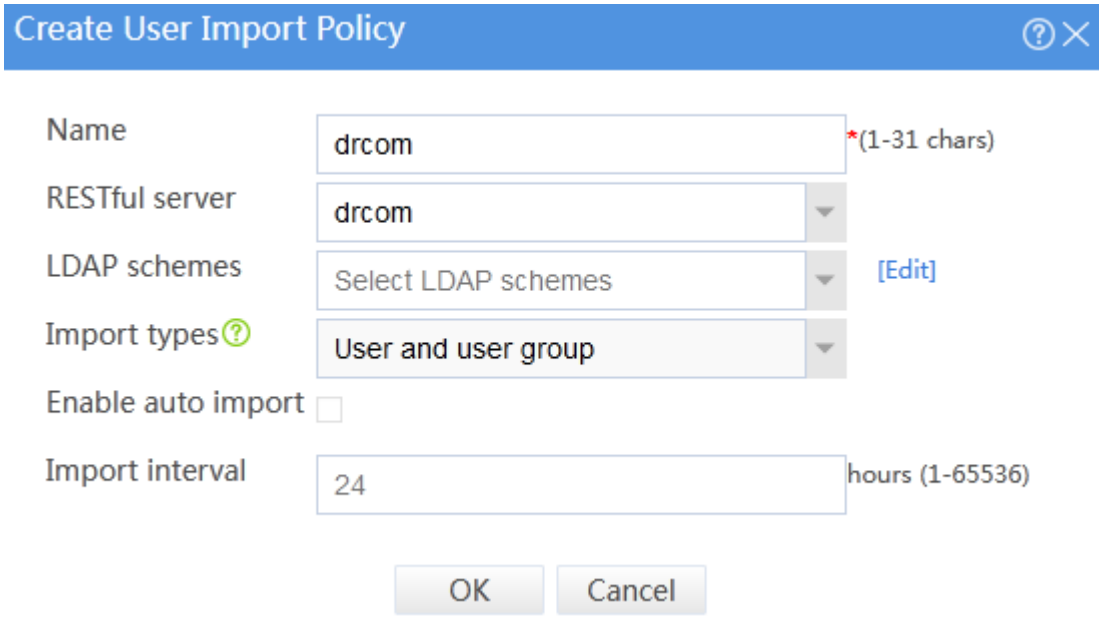
   # From the navigation pane, select **User** > **User Management** > **User Import Policies**.

   # Click **Create**.

   # Configure the following parameters for the user import policy:

   - Set the name to **drcom**.
   - Select RESTful server **drcom**.
   - Select **User and user group** as the import type.
   - Enable auto import.
   - Use the default settings for other parameters.

Figure 64 Configuring a user import policy



Click **OK**.

8. Manually import user accounts and online users:

   # On the **User Import Policies** page, select **drcom** from the policy list.

   # Click the **Manually import identity users** and **Manually import online users** icons for the policy to import the user accounts and online users on the Dr.Com server to the firewall.

9. Configure security policies to control user traffic:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create** > **Create a policy**.

   # Configure the following parameters in the security policy to permit only user **user10002** to access the FTP server:

   - Set the name to **user10002**.
   - Select **Trust** as the source security zone.
   - Select **DMZ** as the destination security zone.
   - Set the type to IPv4.
   - Select action **Permit**.
   - Specify user **user10002**.

- Use the default settings for other parameters.

Click **OK**.

Create security policy **user10003** to permit only user **user10003** to access the Internet and prevent Internet users from accessing the internal network.

- Set the name to **user10003**.
- Select **Trust** as the source security zone.
- Select **Untrust** as the destination security zone.
- Set the type to IPv4.
- Select action **Permit**.
- Specify user **user10003**.
- Use the default settings for other parameters.

Click **OK**.

Verifying the configuration

1. On the top navigation bar, click **Objects**. From the navigation pane, select **User** > **User Management** > **Static Identity Users**. On the page that opens, verify that you can view user information imported from the Dr.Com server.
2. On the top navigation bar, click **Objects**. From the navigation pane, select **User** > **User Management** > **Online Users**. On the page that opens, verify that you can view online user information pushed from the Dr.Com server.
3. Verify that user **user10001** cannot ping the FTP server.

```
C:\>ping 184.69.2.2


Pinging 184.69.2.2 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.
```

```
Ping statistics for 184.69.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4. Verify that user **user10002** can ping the FTP server.

```
C:\>ping 184.69.2.2

Pinging 184.69.2.2 with 32 bytes of data:
Reply from 184.69.2.2: bytes=32 time=36ms TTL=253
Reply from 184.69.2.2: bytes=32 time<1ms TTL=253
Reply from 184.69.2.2: bytes=32 time<1ms TTL=253
Reply from 184.69.2.2: bytes=32 time<1ms TTL=253

Ping statistics for 184.69.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

5. Verify that user **user10003** can ping a host on the Internet. In this example, the user pings the host at 12.1.1.2.

```
C:\>ping 12.1.1.2

Pinging 12.1.1.2 with 32 bytes of data:
Reply from 12.1.1.2: bytes=32 time=37ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 12.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

Attack defense configuration examples

Contents

Introduction

The following information describes attack defense configuration examples.

The following attack defense features are supported:

Scanning attack defense

Scanning attack detection inspects the incoming packet rate of connections to the target system. Apply a scanning attack defense policy to the security zone that is connected to the external network.

Global flood attack defense

Apply a flood attack defense policy to the security zone that is connected to the external network to protect internal servers. Flood attack detection monitors the rate at which connections are initiated to the internal servers.

IP-specific flood attack defense

You can configure flood attack detection and defense for specific IP addresses. For non-specific IP addresses, the device uses the global flood attack defense settings.

Well-known single-packet attack defense

Single-packet attack detection inspects incoming packets based on the packet signature. Apply the single-packet attack defense policy to the security zone that is connected to the external network.

User-defined single-packet attack defense

The device supports detecting attack packets with user-defined signatures.

Exemption list

The attack defense policy uses an ACL to identify exempted packets. The policy does not check the packets permitted by the ACL.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

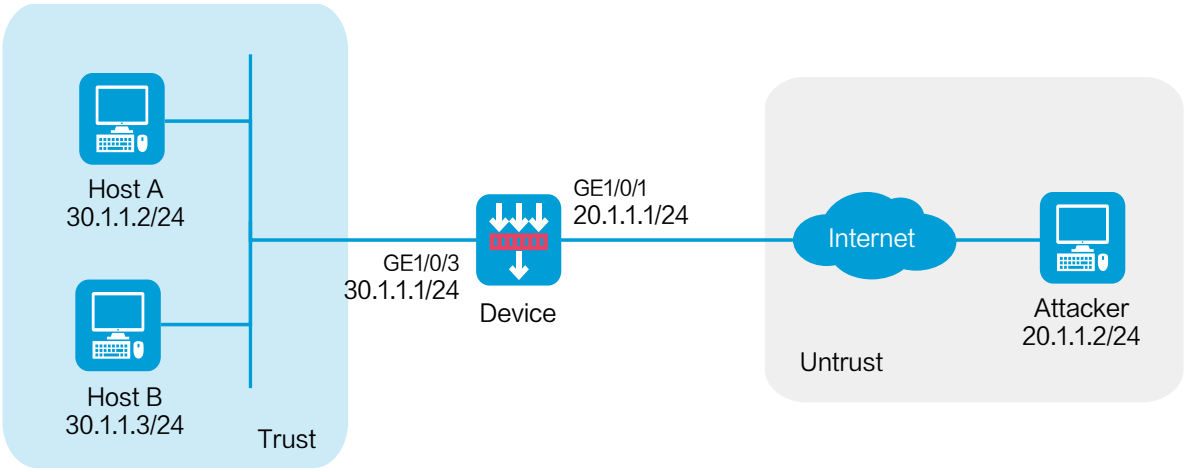
The following information is provided based on the assumption that you have basic knowledge of attack detection and defense.

Example: Configuring scanning attack defense

Network configuration

As shown in Figure 1, configure middle-level scanning attack detection and defense on the **Untrust** security zone where GigabitEthernet 1/0/1 resides to protect internal hosts from scanning attacks. The defense actions are logging and dropping attack packets.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 20.1.1.1/24.

c. Click **OK**.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 30.1.1.1/24 in the same way you configure GE 1/0/1.

2. Create a security policy from zone **Untrust** to zone **Trust**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy:

- Enter policy name **Secpolicy**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Set the action to **Permit**.
- Specify **20.1.1.0/24** as the source IPv4 address.
- Specify **30.1.1.0/24** as the destination IPv4 address.
- Use the default settings for other parameters.

Click **OK**.

3. Configure a scanning attack defense policy.

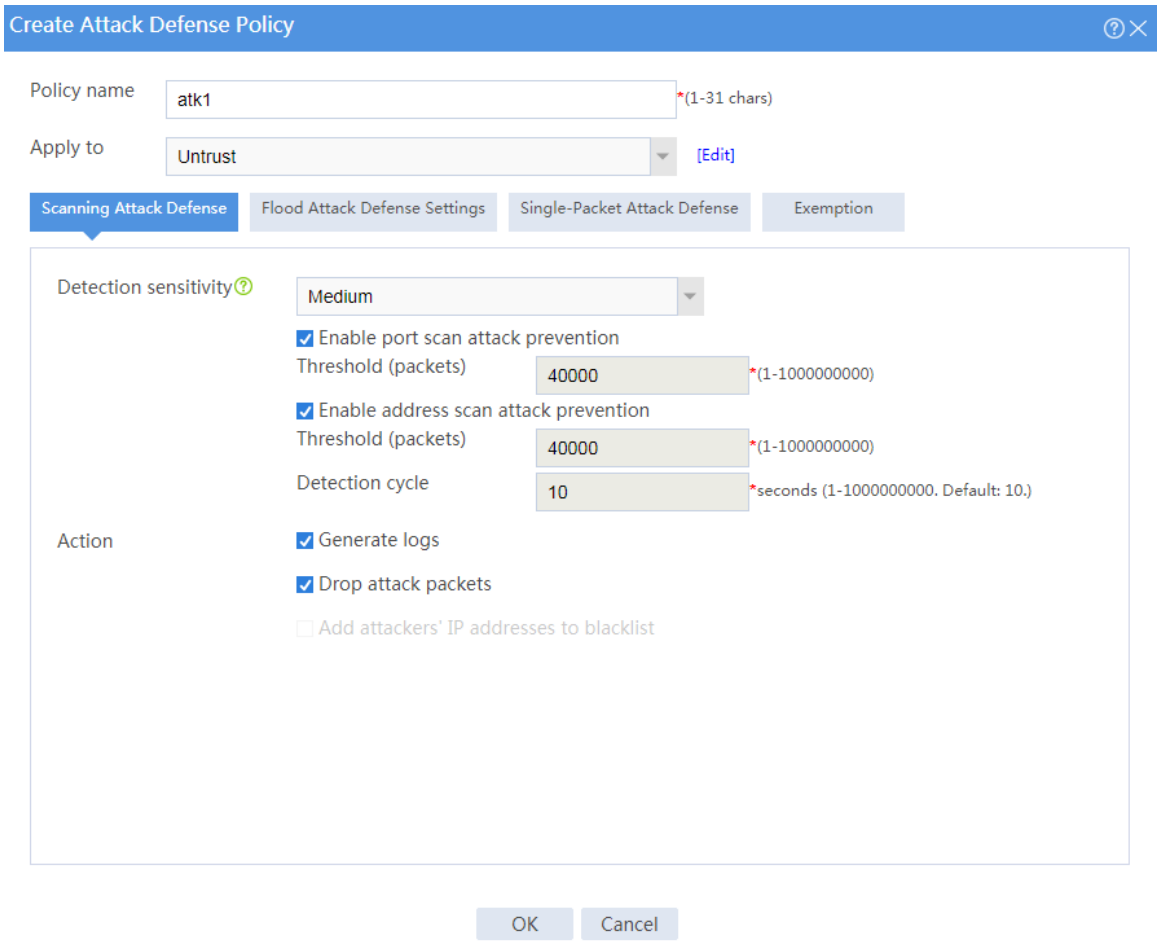
On the top navigation bar, click **Policies**.

From the navigation pane, select **Attack Defense** > **Attack Defense Policies**.

Click **Create**.

Create a scanning attack defense policy, as shown in Figure 2.

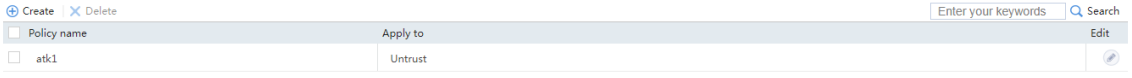
Figure 2 Creating a scanning attack defense policy



Click **OK**.

The attack defense policy is displayed on the attack defense policy list, as shown in Figure 3.

Figure 3 Attack defense policy list



Verifying the configuration

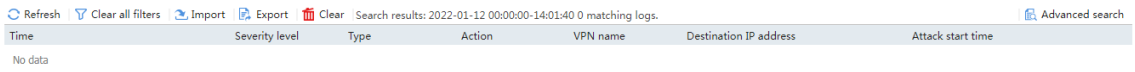
1. On the host at 20.1.1.2, simulate an attack to send a large number of SYN packets with different destination port numbers to destination address 30.1.1.2.

2. On the firewall, view the attack defense log information.

   # On the top navigation bar, click **Monitor**.

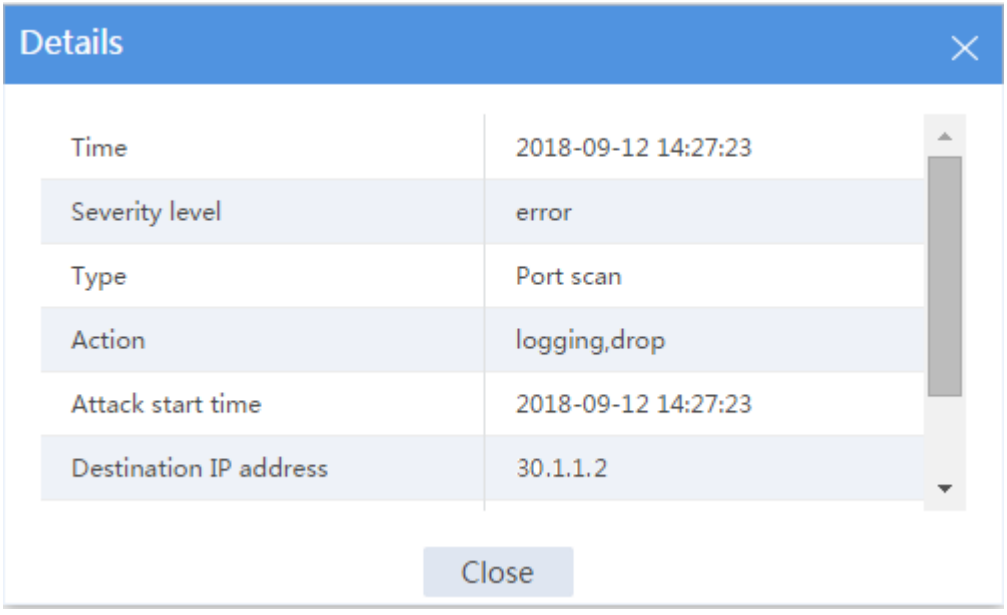
   # From the navigation pane, select **Security Logs** > **Scanning Attack Logs**.

Figure 4 Scanning attack log list



3. Double-click the attack log to view its details.

Figure 5 Detailed information about the scanning attack log



4. Verify that no sessions are created for SYN packets because these packets have been dropped.

   # On the top navigation bar, click **Monitor**.

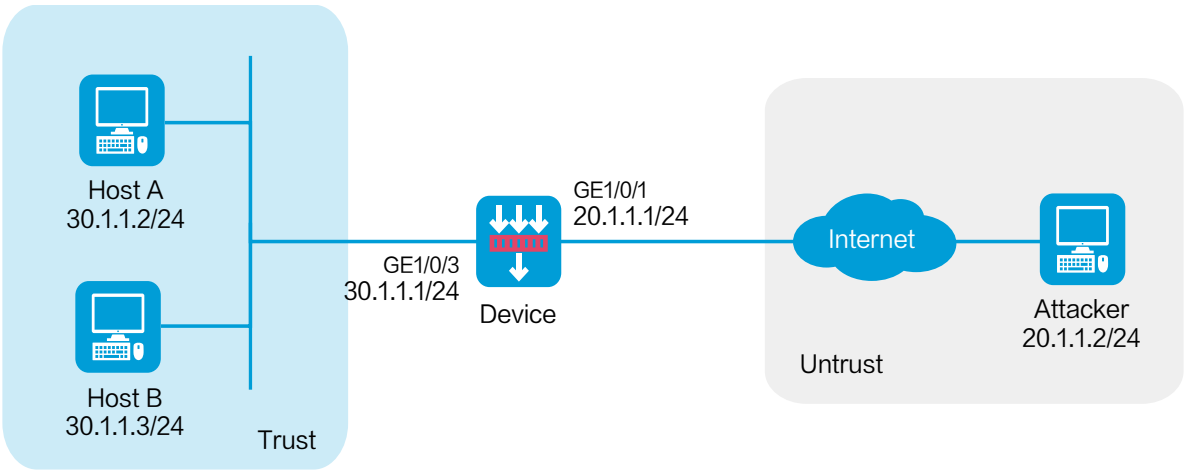
   # From the navigation pane, select **Sessions**.

Example: Configuring flood attack defense

Network configuration

As shown in Figure 6, configure SYN flood attack detection and defense on the security zone where GigabitEthernet 1/0/1 resides to protect internal network hosts from SYN flood attacks. When the firewall detects that the number of packets sent by the attacker reaches or exceeds 10000 per second, the firewall outputs logs and drops attack packets.

Figure 6 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 20.1.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/3 to the **Trust** security zone and set its IP address to 30.1.1.1/24 in the same way you configure GE 1/0/1.

2. Create a security policy from zone **Untrust** to zone **Trust**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **Secpolicy**.

- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Set the action to **Permit**.
- Specify **20.1.1.0/24** as the source IPv4 address.
- Specify **30.1.1.0/24** as the destination IPv4 address.
- Use the default settings for other parameters.

Click **OK**.

3. Configuring flood attack defense global settings.

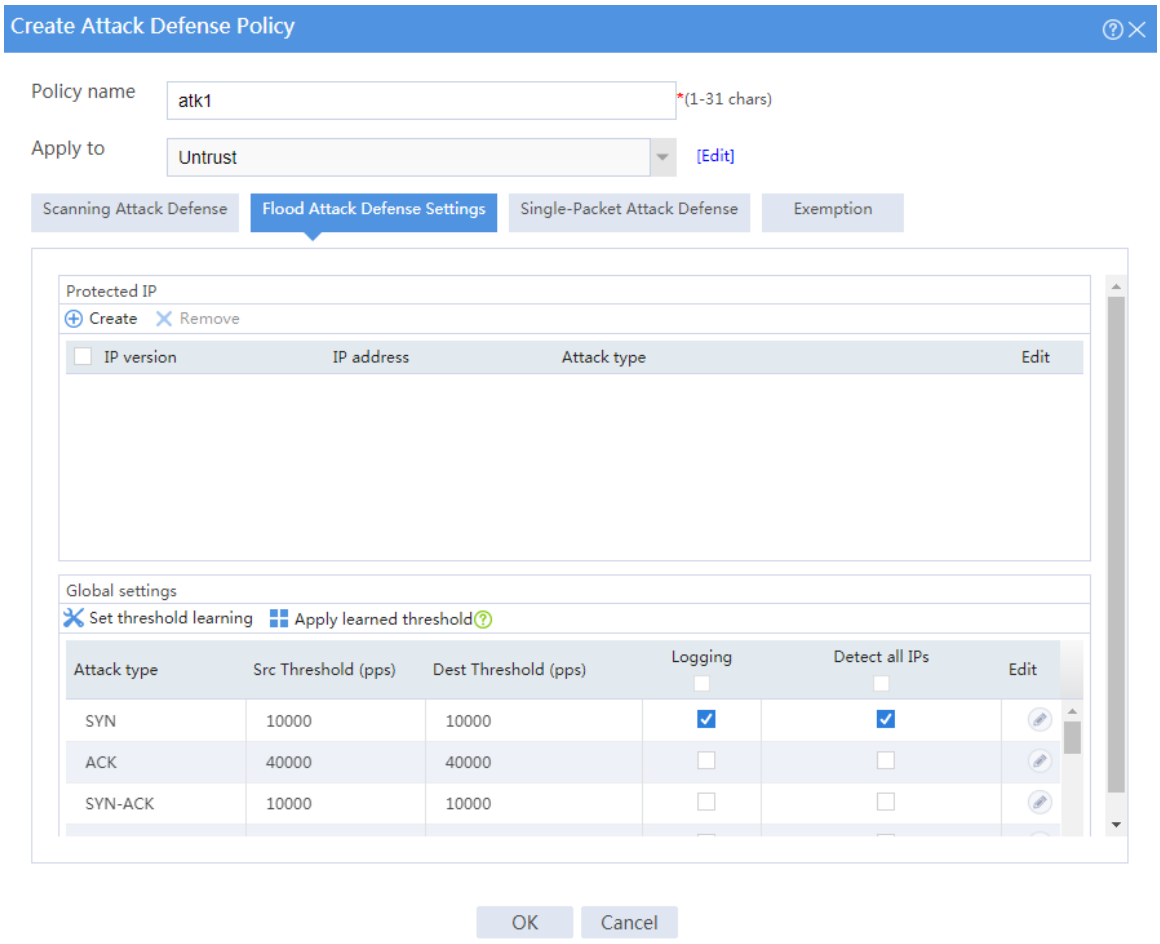
On the top navigation bar, click **Policies**.

From the navigation pane, select **Attack Defense** > **Attack Defense Policies**.

Click **Create**.

In the dialog box that opens, create an attack defense policy, as shown in Figure 7.

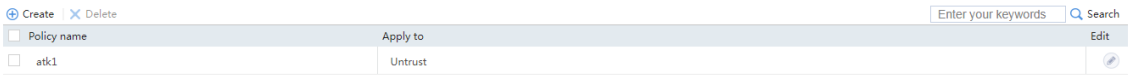
Figure 7 Creating an attack defense policy



Click **OK**.

The attack defense policy is displayed on the attack defense policy list, as shown in Figure 8.

Figure 8 Attack defense policy list



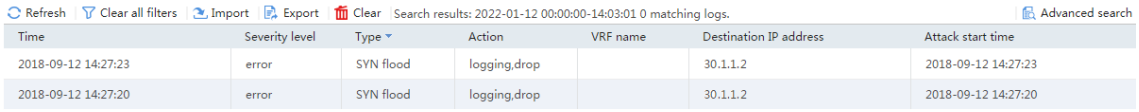
Verifying the configuration

1. On the host at 20.1.1.2, simulate a SYN flood attack by sending a large number of SYN packets with different source port numbers to destination address 30.1.1.2.
2. On the firewall, view the flood attack log information.

   # On the top navigation bar, click **Monitor**.

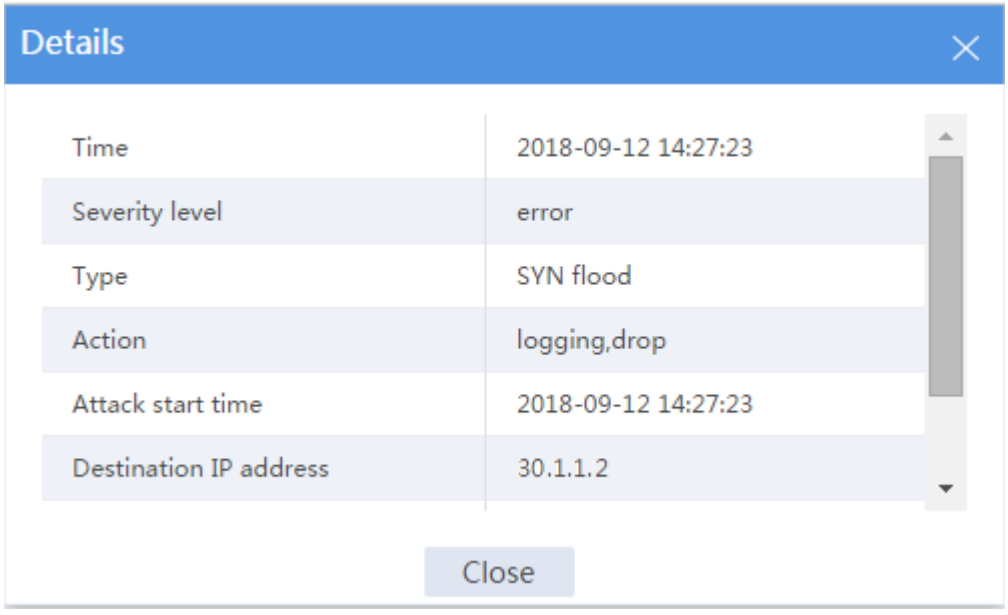
   # From the navigation pane, select **Security Logs** > **Flood Attack Logs**.

Figure 9 Flood attack log list



3. Double-click the flood attack log to view its details.

Figure 10 Flood attack log details



4. Verify that no session is created for SYN packets because these packets have been dropped.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Device Logs** > **Traffic Logs**.

IPCAR configuration examples

Contents

Introduction

The following information provides IPCAR configuration examples.

IPCAR can limit the new connection establishment rate on the device. It can be used to prevent DDoS attacks from decreasing the device performance.

The device can use IPCAR to protect the public network or internal network:

- **Public network protection**—Limits the rate of connection establishment requests from the public network to the internal network. The device monitors the number of connection establishment requests based on the destination IP address of packets. If the number reaches the connection rate threshold, the device will take the specified action on subsequent packets.
- Internal network protection—Limits the rate of connection establishment requests from the internal network to the public network. The device monitors the number of connection establishment requests based on the source IP address of packets. If the number reaches the connection rate threshold, the device will take the specified action on subsequent packets.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

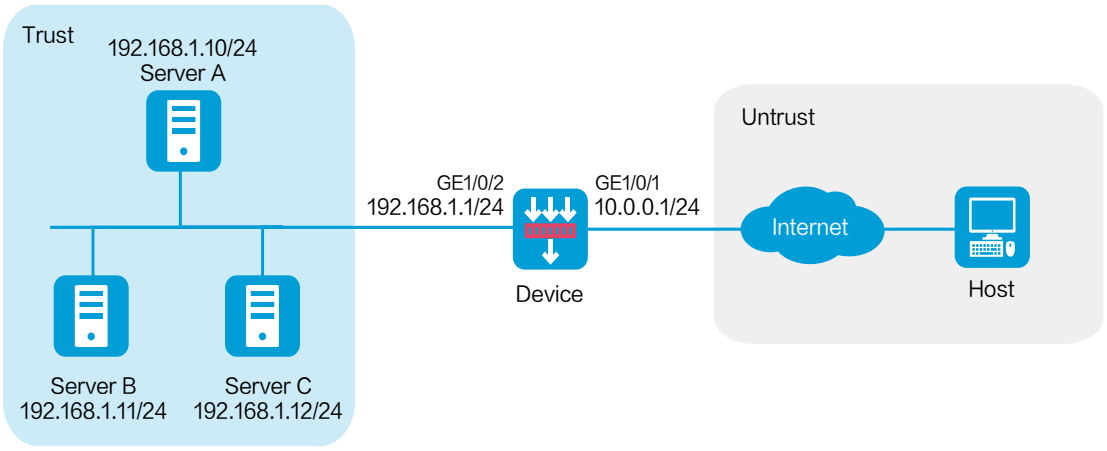
The following information is provided based on the assumption that you have basic knowledge of the IP CAR feature.

Example: Configuring IPCAR for public network protection

Network configuration

As shown in Figure 1, configure IPCAR for public network protection on the device to limit the rate to 10 for connection requests from the public network to each internal server.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on the R8560 of the NFNX3-HDB3080 device.

Procedure

Assigning IP addresses to interfaces and adding the interfaces to security zones

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

1. Select the **Trust** security zone.
2. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 10.0.0.1/24.

3. Use the default settings for other parameters.
4. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 192.168.1.1/24 in the same way you configure GE 1/0/1.

Configuring a security policy

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** > **Create a policy**.

Configure security policy **Secpolicy**:

- Enter security policy name **trust-local**.
- Select source security zone **Untrust**.
- Select destination security zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Set destination IPv4 addresses to 192.168.1.10, 192.168.1.11, and 192.168.1.12.
- Use the default settings for other parameters.

Click **OK**.

Configuring IPCAR

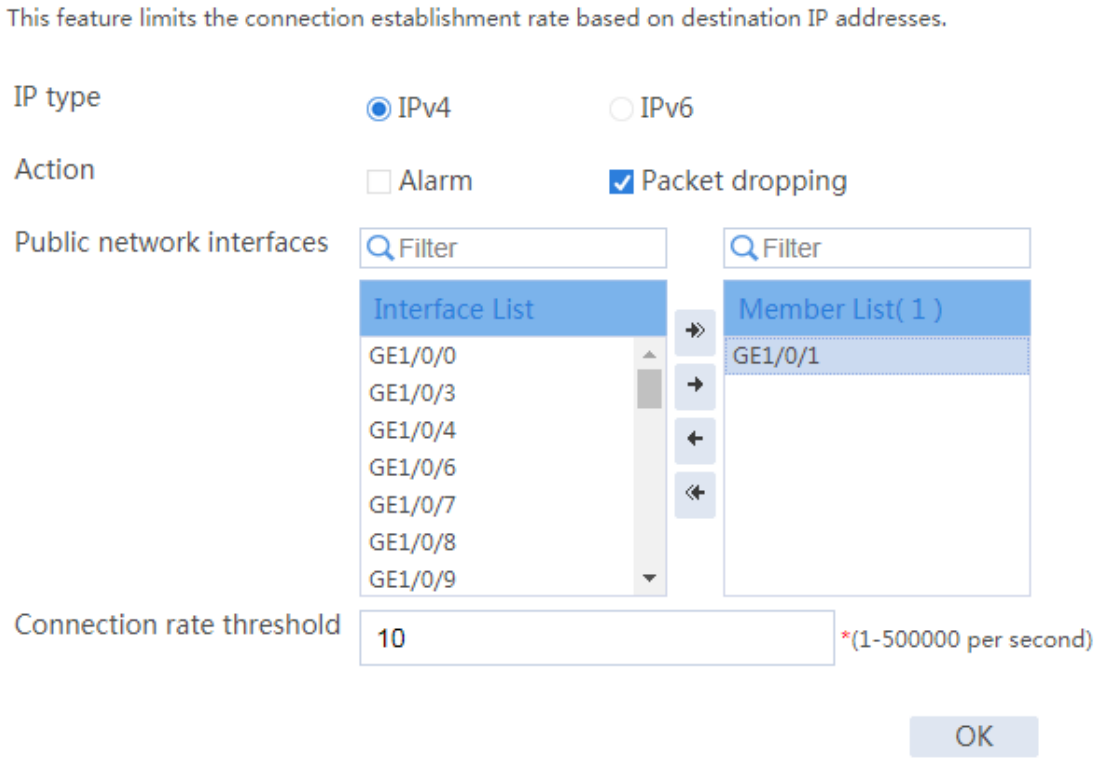
On the top navigation bar, click **Policies**.

From the navigation pane, select **Attack Defense** > **IPCAR**.

Configure the following IPCAR parameters:

- Select IP type **IPv4**.
- Select action **Packet dropping**.
- Select public network interface GE1/0/1.
- Set the connection rate threshold to 10.

Figure 2 Configuring IPCAR



Verifying the configuration

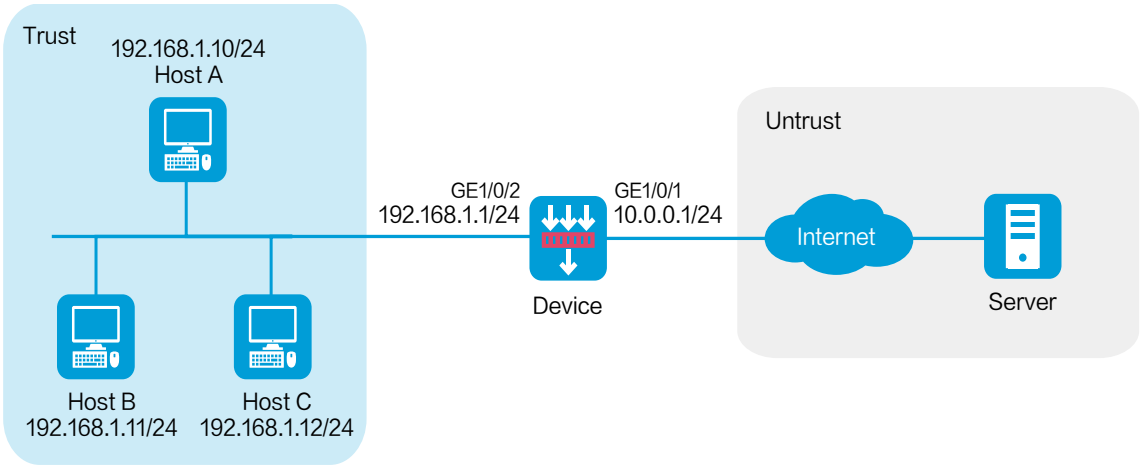
Verify that each internal server can receive a maximum of 10 connection requests from the external network.

Example: Configuring IPCAR for internal network protection

Network configuration

As shown in Figure 3, configure IPCAR for internal network protection on the device to limit the rate to 10 for connection requests initiated from each internal server to the public network.

Figure 3 Network diagram



Software versions used

This configuration example was created and verified on the R8560 of the NFNX3-HDB3080 device.

Procedure

Assigning IP addresses to interfaces and adding the interfaces to security zones

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

1. Select the **Trust** security zone.
2. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 10.0.0.1/24.
3. Use the default settings for other parameters.
4. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 192.168.1.1/24 in the same way you configure GE 1/0/1.

Configuring a security policy

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** > **Create a policy**.

Configure security policy **Secpolicy**:

- Enter security policy name **trust-local**.
- Select source security zone **Untrust**.
- Select destination security zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Set destination IPv4 addresses to 192.168.1.10, 192.168.1.11, and 192.168.1.12.

- Use the default settings for other parameters.

Click **OK**.

Configuring IPCAR

On the top navigation bar, click **Policies**.

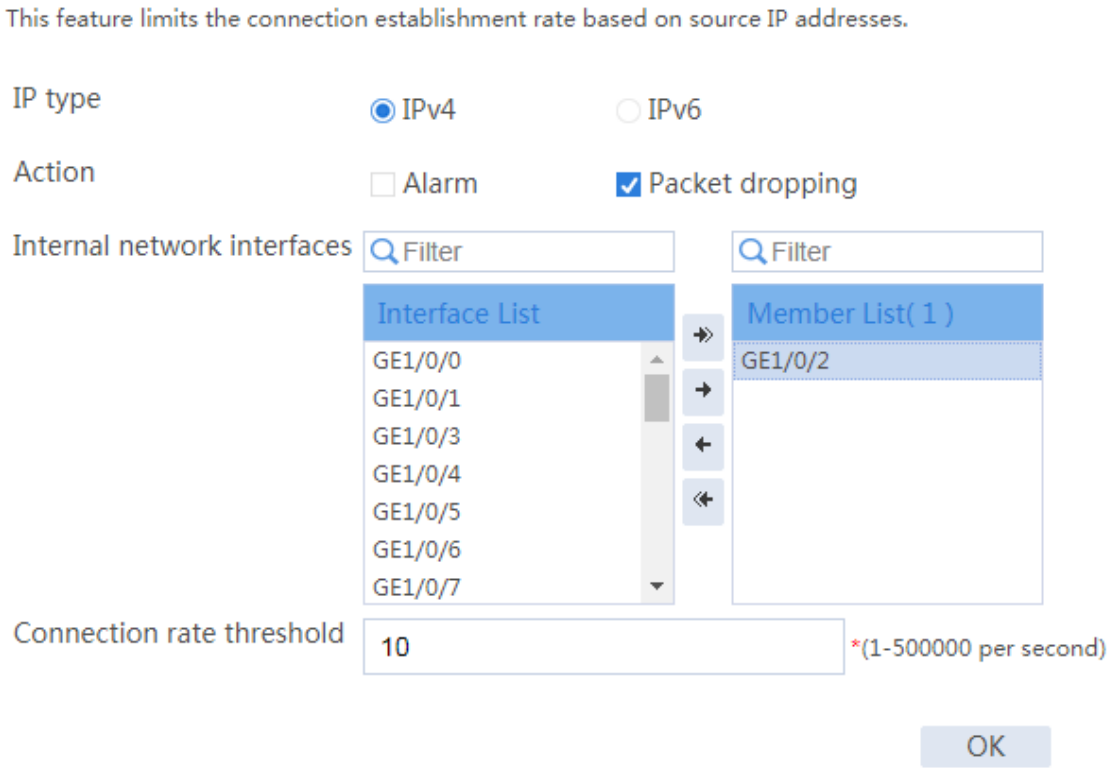
From the navigation pane, select **Attack Defense** > **IPCAR**.

Click the **Internal Network Protection** tab.

Configure the following IPCAR parameters:

- Select IP type **IPv4**.
- Select action **Packet dropping**.
- Select internal network interface GE1/0/2.
- Set the connection rate threshold to 10.

Figure 4 Configuring IPCAR



Verifying the configuration

Verify that each internal server can initiate a maximum of 10 connections to the external network.

IPS configuration examples

Contents

Introduction

The following information provides IPS configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the IPS feature.

Restrictions and guidelines

The IPS feature requires a license to run on the device. After the license expires, IPS can use the existing IPS signature library on the device, but the library cannot be updated.

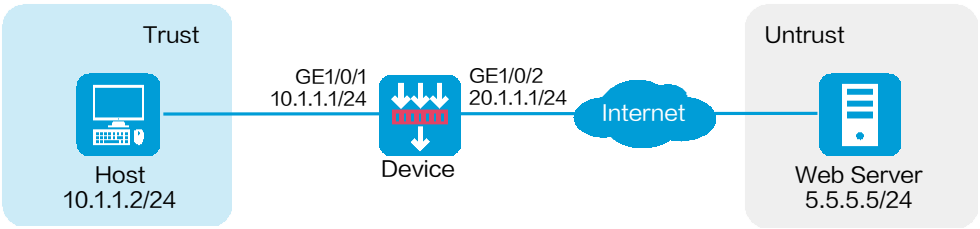
Example: Configuring IPS

Network configuration

As shown in Figure 1, the device acts as the security gateway. Configure the IPS feature to meet the following requirements:

- Protect the internal network from the vulnerability attacks from the Internet.
- Allow the internal users to use the application that matches the IPS signature with signature ID 936.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask length of the interface. In this example, enter 10.1.1.1/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure routing settings.

   This example configures a static route. To use dynamic routing, configure dynamic routing protocols as required.

   Configure the next hop IP address to reach the Web server in the external network according to the actual network conditions. In this example, the next hop IP address is 20.1.1.2.

To configure a static route:

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static IPv4 route to reach 0.0.0.0:

- Enter destination IP address **5.5.5.0**.
- Enter mask length **24**.
- Enter next hop address **20.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

3. Update the IPS signature library to the latest version. (Details not shown.)

4. Configure an IPS profile:

On the top navigation bar, click **Objects**.

From the navigation pane, select **APP Security** > **IPS** > **Profiles**.

Click **Create**.

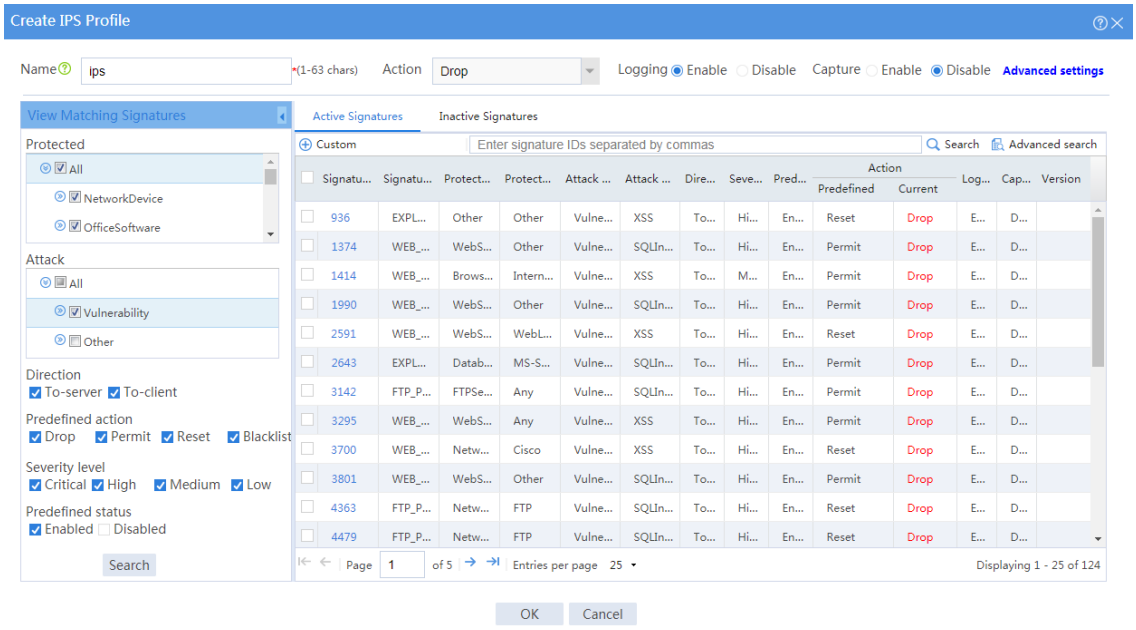
In the dialog box that opens, configure an IPS profile:

- Enter the name **ips**.
- In the **View Matching Signatures** area, configure the following settings:
  - Select **All** for the protected target.
  - Select **Vulnerability** for the attack categories.
  - Set **To-server** and **To-client** for the direction.
  - Set the predefined action to drop, permit, reset and blacklist.
  - Set the severity level to critical, high, medium, and low.

- Enable the predefined status.

- In the **Action** area on the top of the page, configuration the actions:
  - Select **Drop** from the action list.
  - Enable logging.
  - Use the default settings for other parameters.

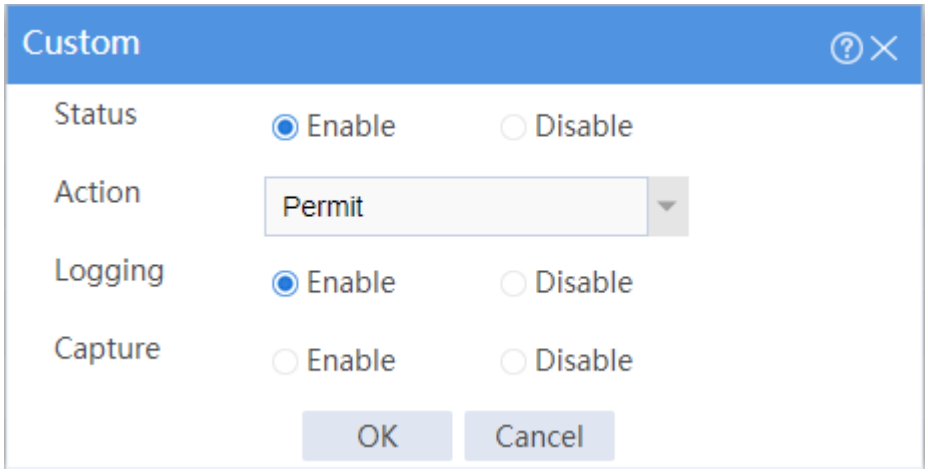
Figure 2 Creating an IPS profile



In the active signature list, select signature 936, and click **Custom**. In the dialog box that opens, configure the following parameters:

- Set the status to **Enable**.
- Select **Permit** from the action list.
- Enable logging.
- Use the default settings for other parameters.

Figure 3 Customizing the signature



Click **OK**.

Click **OK**.

5. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** , and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-trust** to permit the specified traffic from the **Untrust** to **Trust** security zones:

- Enter policy name **untrust-trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select destination IP address **10.1.1.0/24**.
- Select IPS profile **ips** in the **Content security** area.

- Use the default settings for other parameters.

Click **OK**.

Create security policy **trust-untrust** to permit the specified traffic from the **Trust** to **Untrust** security zones:

- Enter policy name **trust-untrust**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IP address **10.1.1.0/24**.
- Select IPS profile **ips** in the **Content security** area.
- Use the default settings for other parameters.

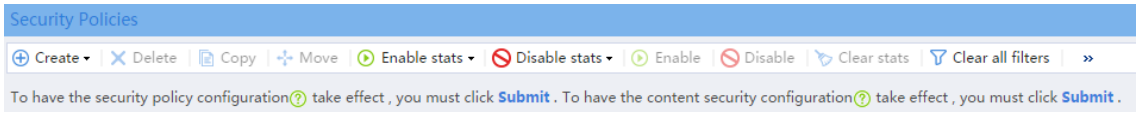
Click **OK**.

6. Activate the settings on the **Security Policies** page:

After you apply the IPS profile to the security policy, click **Submit** (the second **Submit** in Figure 4) to have the content security configuration take effect.

Click **Activate** (the first **Submit** in Figure 4) to activate security policy matching acceleration.

Figure 4 Activate security policy settings



7. Enable logging:

On the top navigation bar, click **System**.

From the navigation pane, select **Log Settings** > **Basic Settings**.

Click the **Storage Space Settings** tab.

Edit the storage space settings for the IPS service and enable logging for the service.

Verifying the configuration

Verify that IPS can implement the following protection for the internal network:

- Log and block the vulnerability attacks.
- Allow the internal users to use the application that matches IPS signature 936.

To view the logs generated for these events, click **Monitor** on the top navigation bar, and then select **Security Logs** > **Threat Logs** from the navigation pane.

URL filtering configuration examples

Contents

Introduction

The following information provides URL filtering configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the URL filtering feature.

Restrictions and guidelines

The URL filtering feature requires a license to run on the device. After the license expires, URL filtering can use the existing URL filtering signature library on the device, but the library cannot be updated.

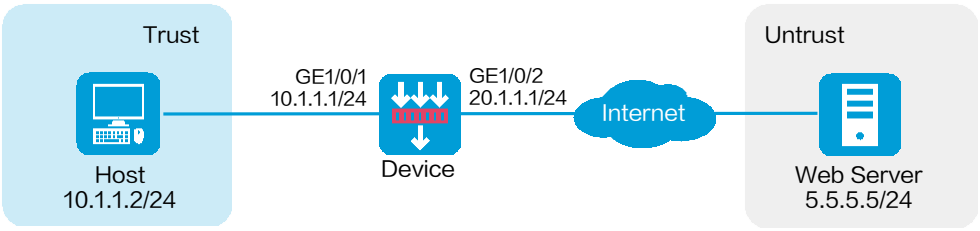
Example: Configuring URL filtering

Network configuration

As shown in Figure 1, a security gateway device is deployed at the border of the enterprise network. Configure URL filtering on the device to block and log the following Internet access behaviors of internal users:

- Access to shopping website **taobao** and adult websites.
- Access to the **www.tudou.com** website.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask length of the interface. In this example, enter 10.1.1.1/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure routing settings.

   This example configures a static route. To use dynamic routing, configure dynamic routing protocols as required.

   Configure the next hop IP address to reach the Web server in the external network according to the actual network conditions. In this example, the next hop IP address is 20.1.1.2.

   To configure a static route:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static IPv4 route to reach 0.0.0.0:

   - Enter destination IP address **5.5.5.0**.
   - Enter mask length **24**.
   - Enter next hop address **20.1.1.2**.
   - Use the default settings for other parameters.

   # Click **OK**.

3. Update the URL filtering signature library to the latest version. (Details not shown.)

4. Configure a URL category:

   # On the top navigation bar, click **Objects**.

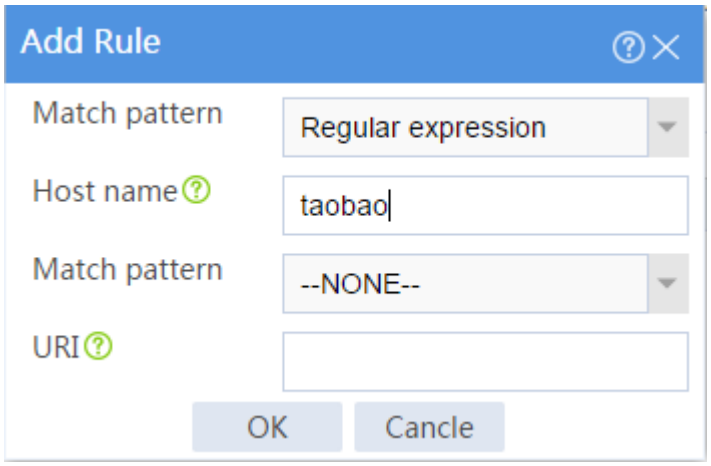
   # From the navigation pane, select **APPSecurity** > **URL Filtering** > **URL Categories**.

   # Click **Create**.

   # In the dialog box that opens, configure a URL category:

- Enter **shopping** in the **Name** field.
- Set the severity level to 2000.
- Click **Add**.
- In the dialog box that opens, select **Regular expression** from the **Match pattern** list and enter **taobao** in the **Host name** field, and then click **OK**.

Figure 2 Adding a rule to the URL category



Click **OK**.

5. Configure a URL filtering profile:

On the top navigation bar, click **Objects**.

From the navigation pane, select **APPSecurity** > **URL Filtering** > **Profiles**.

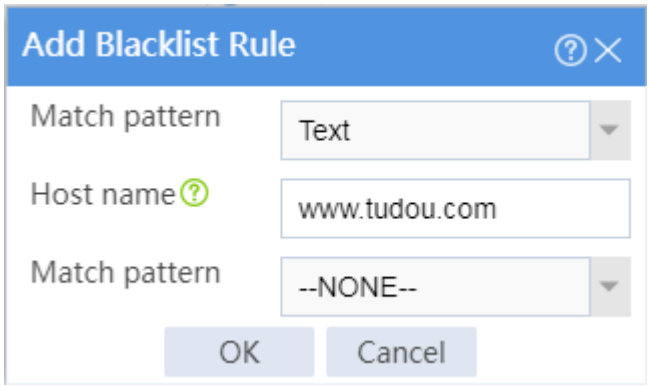
Click **Create**.

In the dialog box that opens, configure a URL filtering profile:

- Enter the name **urlfilter**.
- Select **Permit** as the default action.
- Select the **Logging** option.

- Use the default settings for other parameters.
- In the **Blacklist** area, click **Add**.
- In the dialog box that opens, select **Text** from the **Match pattern** list and enter **www.tudou.com** in the **Host name** field, and then click **OK**.

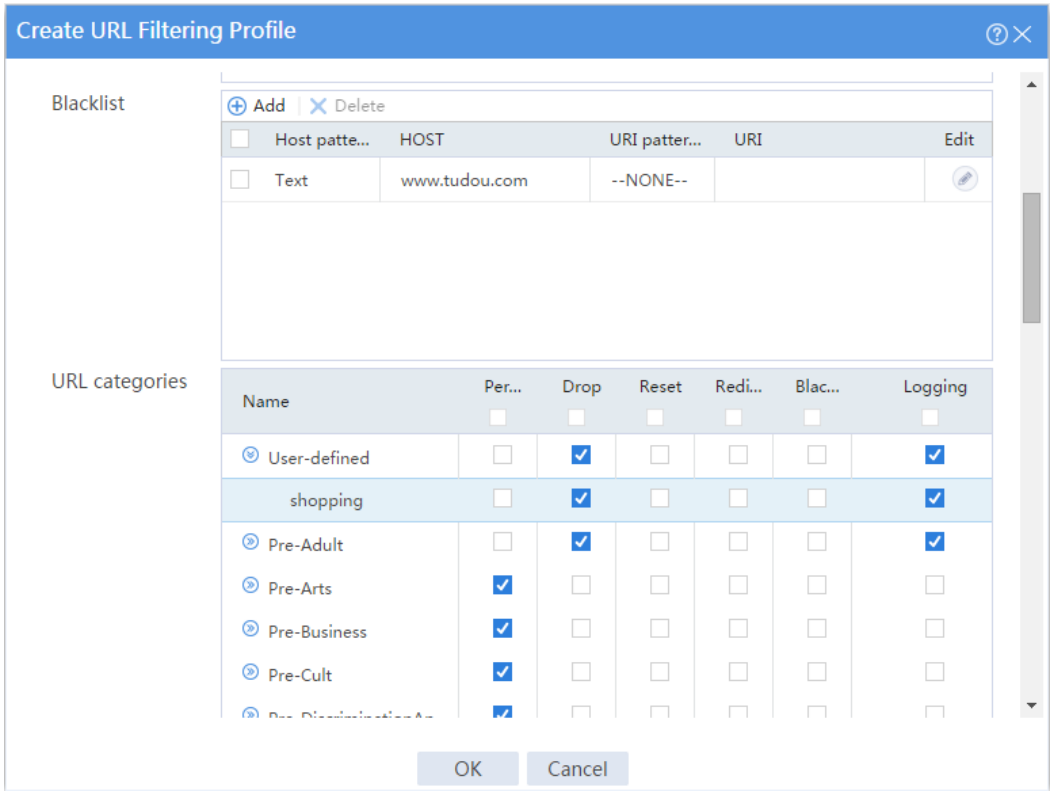
Figure 3 Adding a blacklist rule



- In the **URL categories** area, select the **Drop** and **Logging** actions for user-defined URL category **shopping** and predefined URL category **Pre-Adult**.

Click **OK**.

Figure 4 Configuring a URL filtering profile



6. Create a security policy:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**, and then click **Create a policy**.

   # In the dialog box that opens, configure a security policy named **urlfilter** to permit the specified traffic from the **Untrust** to **Trust** security zones:

   - Enter policy name **urlfilter**.
   - Select source zone **Untrust**.
   - Select destination zone **Trust**.
   - Select type **IPv4**.
   - Select action **Permit**.

- Select source IP address **10.1.1.0/24**.
- Select URL filtering profile **urlfilter** in the **Content security** area.
- Use the default settings for other parameters.

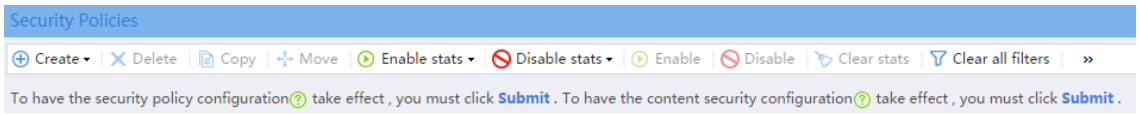
Click **OK**.

7. Activate the settings on the **Security Policies** page:

   # After you apply the URL filtering profile to the security policy, click **Submit** (the second **Submit** in Figure 5) to have the content security configuration take effect.

   # Click **Activate** (the first **Submit** in Figure 5) to activate security policy matching acceleration.

   Figure 5 Activate security policy settings



8. Enable logging:

   # On the top navigation bar, click **System**.

   # From the navigation pane, select **Log Settings** > **Basic Settings**.

   # Click the **Storage Space Settings** tab.

   # Edit the storage space settings for the URL filtering service and enable logging for the service.

Verifying the configuration

Verify that URL filtering can log and block the following Internet access behaviors of internal users:

- Access to shopping website taobao and adult websites.

- Access to the **www.tudou.com** website.

To view the logs generated for these behaviors, click **Monitor** on the top navigation bar, and then select **Security Logs** > **URL Filtering Logs** from the navigation pane.

Anti-virus configuration examples

Contents

Introduction

The following information provides anti-virus configuration examples.

The anti-virus feature supports the following application protocols:

- FTP.
- HTTP.
- IMAP.
- NFS.
- POP3.
- SMB.
- SMTP.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the anti-virus feature.

Restrictions and guidelines

For anti-virus to inspect HTTPS protocol packets, you must also configure the application proxy feature. To configure the application proxy feature, access the **Policies** > **Application Proxy** page.

The anti-virus feature requires a license to run on the device. After the license expires, anti-virus can use the existing virus signature library on the device, but the library cannot be updated.

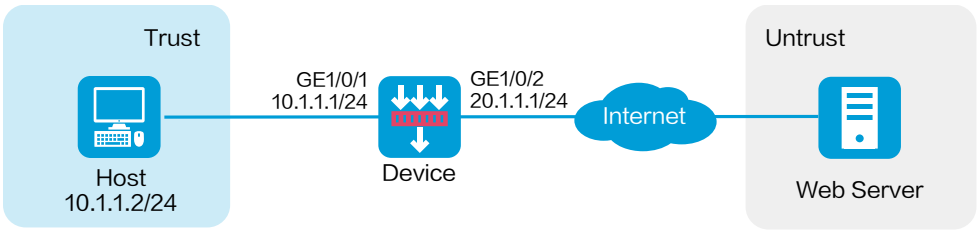
Example: Configuring anti-virus

Network configuration

As shown in Figure 1, a security gateway device is deployed at the border of the enterprise network. Internal users need to transfer files and emails by using the Web server and email server on the Internet.

Configure anti-virus on the device to perform virus detection on the files and emails transferred by the internal users to protect the enterprise network.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask length of the interface. In this example, use 10.1.1.1/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

   This example configures a static route. If dynamic routes are used, configure a routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, create an IPv4 static route:

   - Enter destination address **0.0.0.0**.
   - Enter mask length **0**.

- Enter next hop address **20.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

3. Update the virus signature library to the latest version. (Details not shown.)

4. Configure an anti-virus profile.

On the top navigation bar, click **Objects**.

From the navigation pane, select **APP Security** > **Anti-Virus** > **Profile**.

Click **Create**.

In the dialog box that opens, configure an anti-virus profile:

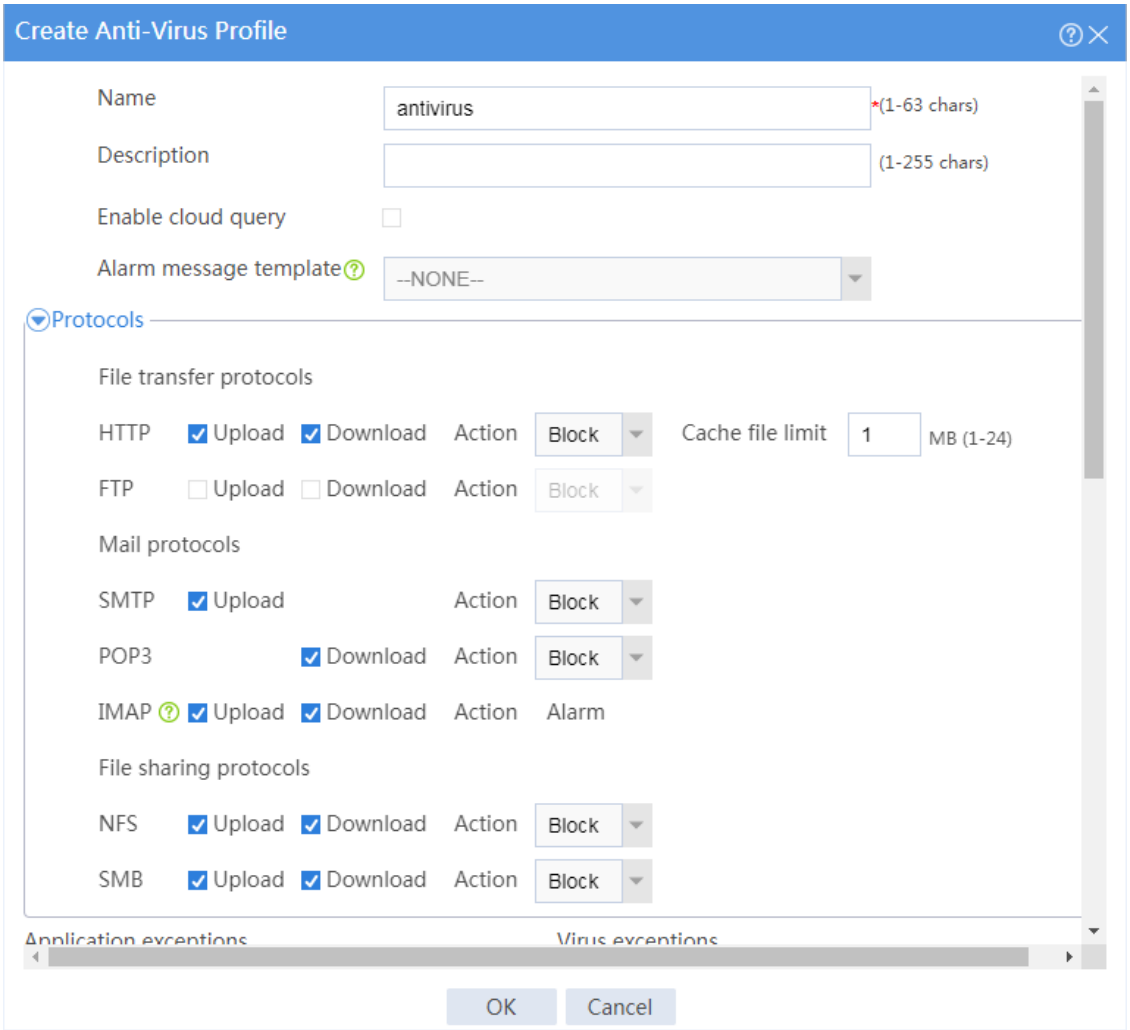
a. Enter the name **antivirus**.

b. In the **Protocols** area, configure anti-virus protection for file transfer protocols and mail protocols, as shown in Figure 2.

- Clear the check boxes for the **Upload** and **Download** options of the FTP protocol.
- Set the action to **Block** for the SMTP and POP3 mail protocols.

c. Click **OK**.

Figure 2 Creating an anti-virus profile



5. Configure security policies:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**, and then click **Create a policy**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **trust-untrust**.
   - Select source zone **Trust**.

- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IP address **10.1.1.0/24**.
- Select anti-virus profile **antivirus** in the **Content security** area.

Click **OK**.

Create security policy **untrust-trust** in the same way you create security policy **trust-untrust**:

- Enter policy name **untrust-trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select destination IP address **10.1.1.0/24**.
- Select anti-virus profile **antivirus** in the **Content security** area.

Click **OK**.

6. On the **Anti-Virus Profile** page, click **Submit** to make the anti-virus profile take effect.

Verifying the configuration

Verify that anti-virus detect and block virus-infected files and emails transmitted by internal users to protect the enterprise network.

To view the threat logs generated by anti-virus, click **Monitor** on the top navigation bar, and then select **Security Logs** > **Threat Logs** from the navigation pane.

File filtering configuration examples

Contents

Introduction

The following information provides file filtering configuration examples.

The file filtering feature filters files based on file extensions. You can configure file filtering to perform actions on files based on the file extensions.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the file filtering feature.

Restrictions and guidelines

File filtering supports filtering packets of the following protocols:

- HTTP.
- FTP.
- SMTP.
- IMAP.
- NFS.
- POP3.
- RTMP.
- SMB.

For file filtering to inspect HTTPS protocol packets, you must also configure the application proxy feature. To configure the application proxy feature, access the **Policies** > **Application Proxy** page.

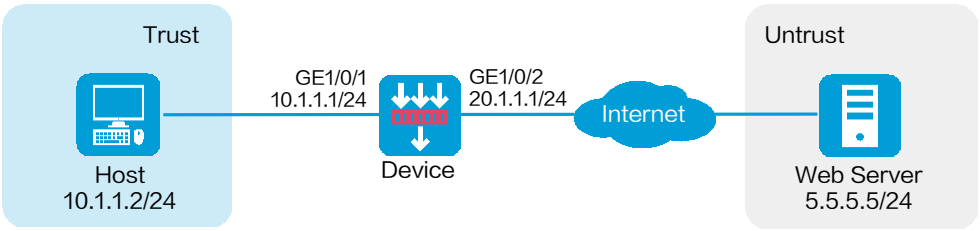
Example: Configuring file filtering

Network configuration

As shown in Figure 1, a security gateway device is deployed at the border of the enterprise network. Configure file filtering on the device to control the file transfer behaviors of internal users as follows:

- Block uploading of common files and compressed files to the Internet to reduce the risk of internal information leakage.
- Block downloading of script files from Web servers to reduce the risk of virus entering the enterprise network.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure a route:

   This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

   Configure the next hop IP address to reach the Web server in the external network according to the actual network conditions. In this example, the next hop IP address is 20.1.1.2.

   To configure a static route:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, create an IPv4 static route:

- Enter destination address **5.5.5.0**.
- Enter mask length **24**.
- Enter next hop address **20.1.1.2**.

Click **OK**.

3. Configure file type groups.

Create file type group **filetype1** as follows:

a. On the top navigation bar, click **Objects**.

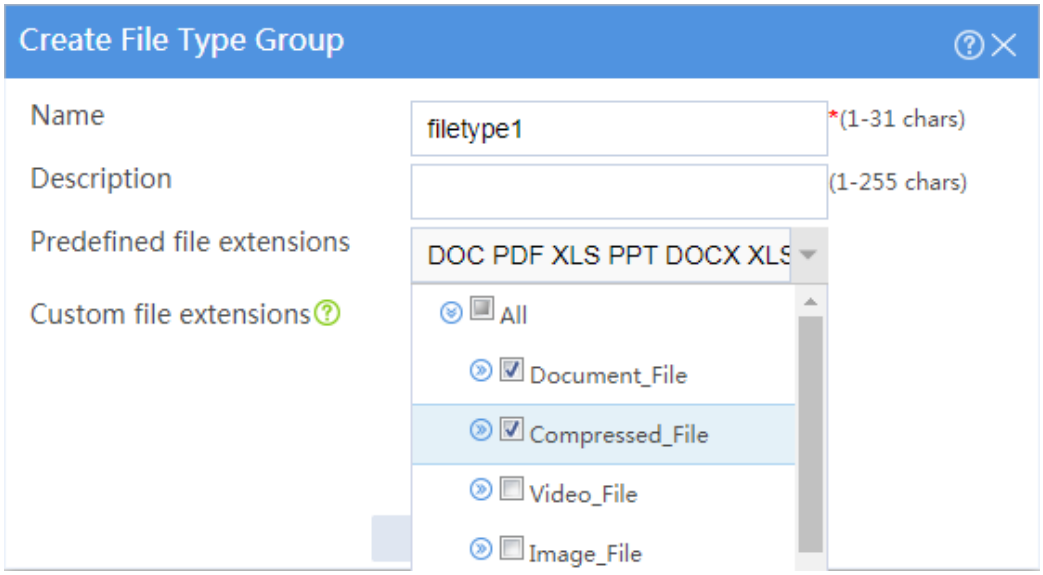
b. From the navigation pane, select **APP Security** > **File Filtering** > **File Type Groups**.

c. Click **Create**.

d. In the dialog box that opens, configure the file type group:

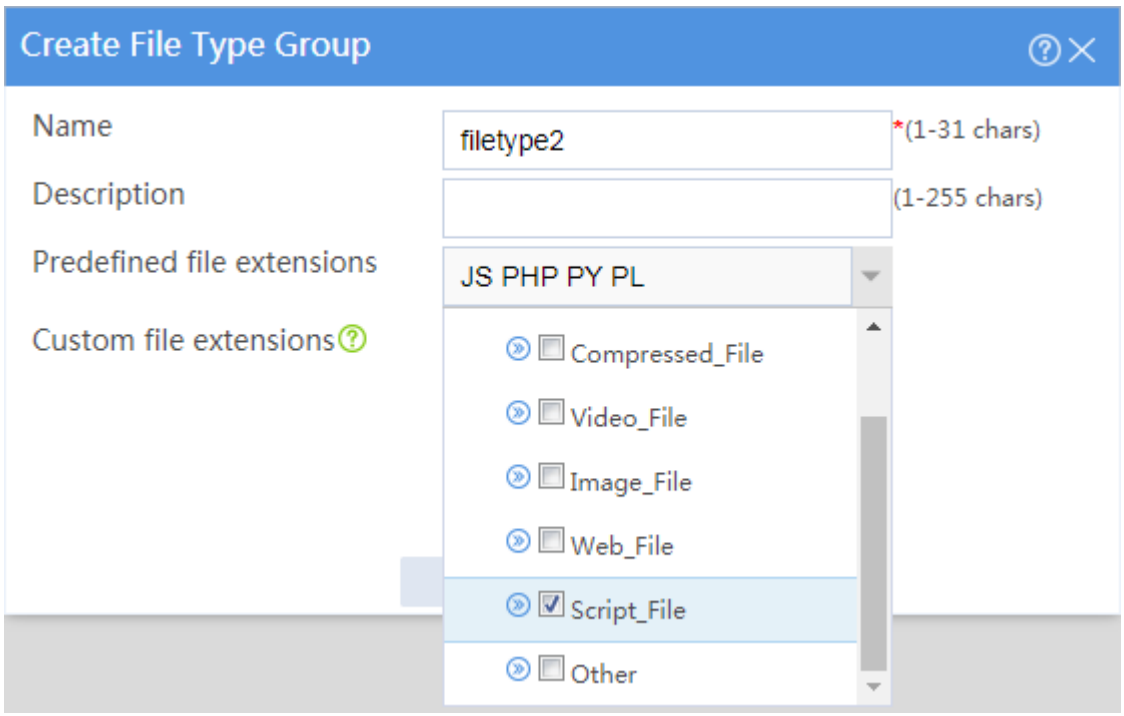
- Enter **filetype1** in the **Name** field.
- From the **Predefined file extensions** list, select **Compressed_File** and **Docmument_File**.
- Click **OK**.

Figure 2 Creating file type group filetype1



Create file type group **filetype2** with the **Script_File** predefined file extension selected.

Figure 3 Creating file type group filetype2



4. Configure a file filtering profile.

On the top navigation bar, click **Objects**.

From the navigation pane, select **APP Security** > **File Filtering** > **Profiles**.

Click **Create**.

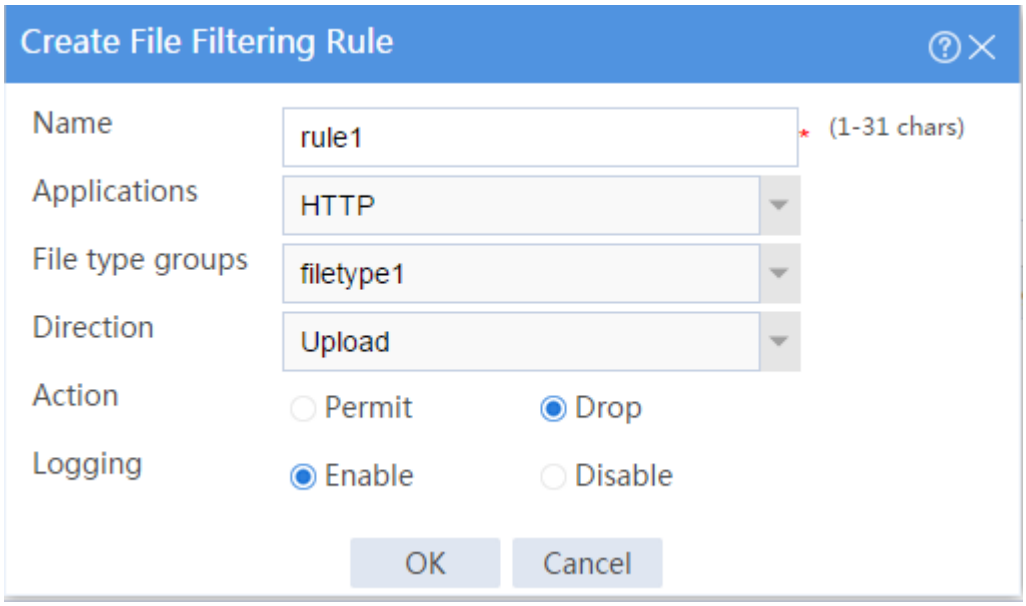
In the dialog box that opens, configure a file filtering profile:

a. Enter the name **filefilter**.

b. In the **File filtering rules** area, click **Create**.

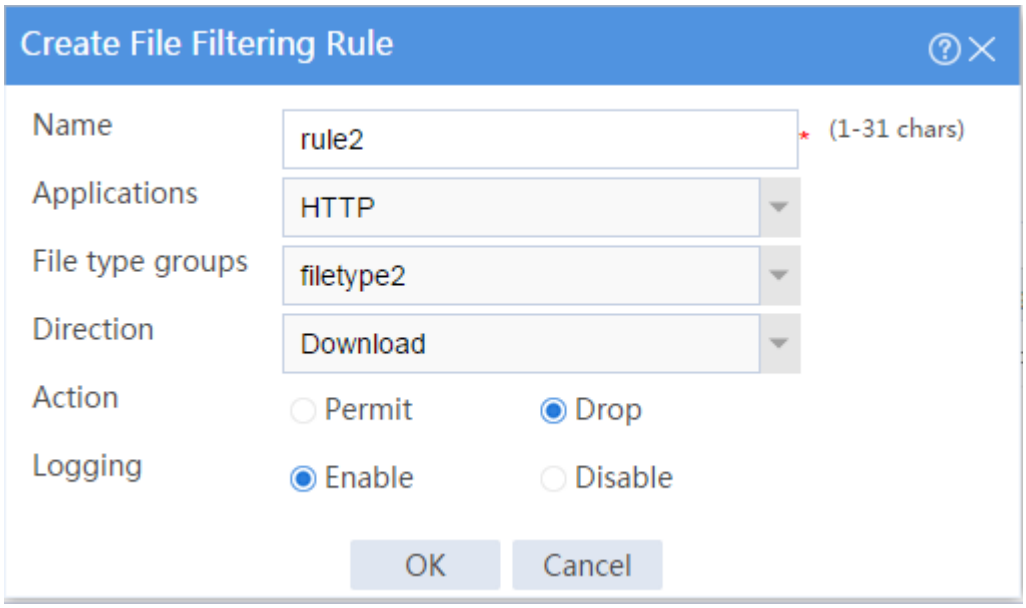
c. In the dialog box that opens, configure file filtering rule **rule1** as shown in Figure 4, and then click **OK**.

Figure 4 Creating file filtering rule rule1



d. Create file filtering rule **rule2** (as shown in Figure 5) in the same way you configure file filtering rule **rule1**.

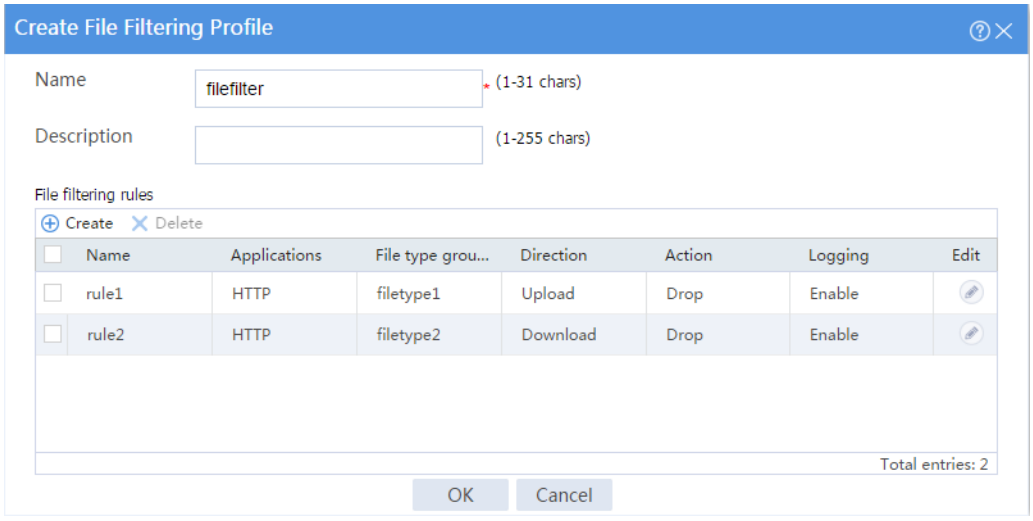
Figure 5 Creating file filtering rule rule2



The file filtering rules are displayed in the **Create File Filtering Profile** dialog box, as shown in Figure 6.

e. Click **OK**.

Figure 6 Creating a file filtering profile



5. Create a security policy:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **filefilter**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select type **IPv4**.
   - Select action **Permit**.
   - Select source IP address **10.1.1.0/24**.
   - Select file filtering profile **filefilter** in the **Content security** area.

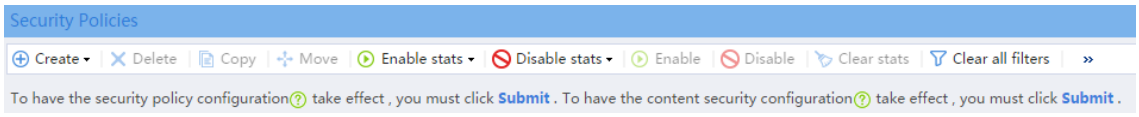
   # Cilck **OK**.

6. Activate the settings on the **Security Policies** page:

   # After you apply the file filtering profile to the security policy, click **Submit** (the second **Submit** in Figure 7) to have the content security configuration take effect.

   # Click **Activate** (the first **Submit** in Figure 7) to activate security policy matching acceleration.

   Figure 7 Activate security policy settings



7. Enable logging:

On the top navigation bar, click **System**.

From the navigation pane, select **Log Settings** > **Basic Settings**.

Click the **Storage Space Settings** tab.

Edit the storage space settings for the file filtering service and enable logging for the service.

Verifying the configuration

Verify that internal users cannot upload document files or compressed files to the Internet, or download script files from Web servers.

To view the file filtering logs, click **Monitor** on the top navigation bar, and then select **Security Logs** > **File Filtering Logs** from the navigation pane.

Data filtering configuration examples

Contents

Introduction

The following information provides data filtering configuration examples.

Data filtering filters packets based on application layer information. You can use data filtering to effectively prevent leakage of internal information, distribution of illegal information, and unauthorized access to the Internet.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the data filtering feature.

Restrictions and guidelines

Data filtering supports filtering packets of the following protocols:

- HTTP.
- FTP.
- SMTP.
- IMAP.
- NFS.
- POP3.
- RTMP.
- SMB.

For data filtering to inspect HTTPS protocol packets, you must also configure the application proxy feature. To configure the application proxy feature, access the **Policies** > **Application Proxy** page.

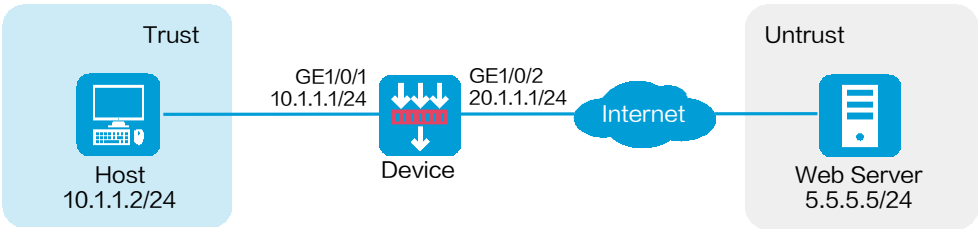
Example: Configuring data filtering

Network configuration

As shown in Figure 1, a security gateway device is deployed at the border of the enterprise network. Configure data filtering on the device to block and log the following Internet access behaviors of internal users:

- Browsing, publishing, or downloading information containing the **illegal** keyword on the Internet.
- Transferring files marked as for internal use only on the Internet.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter **10.1.1.1/24**.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure a route:

   This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

   Configure the next hop IP address to reach the external Web server according to the actual network conditions. In this example, the next hop IP address is 20.1.1.2.

   To configure a static route:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, create an IPv4 static route:

- Enter destination address **5.5.5.0**.
- Enter mask length **24**.
- Enter next hop address **20.1.1.2**.

Click **OK**.

3. Configure keyword groups.

Create keyword group **keywordgroup1**.

a. On the top navigation bar, click **Objects**.

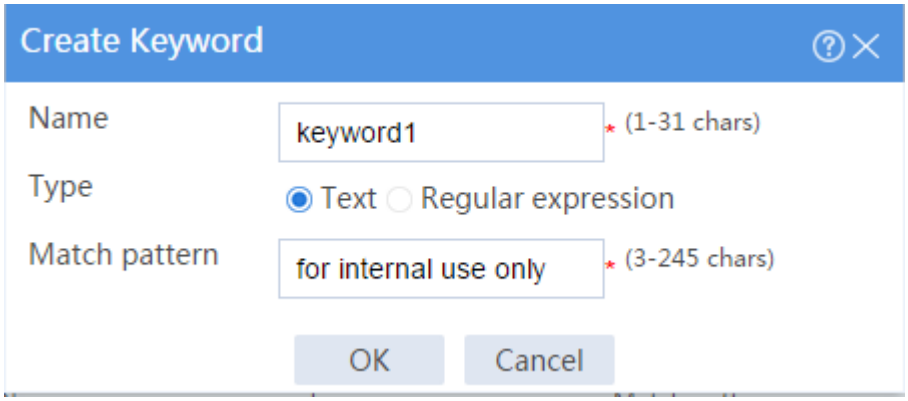
b. From the navigation pane, select **APP Security** > **Data Filtering** > **Keyword Groups**.

c. Click **Create**.

d. In the dialog box that opens, configure the keyword group:

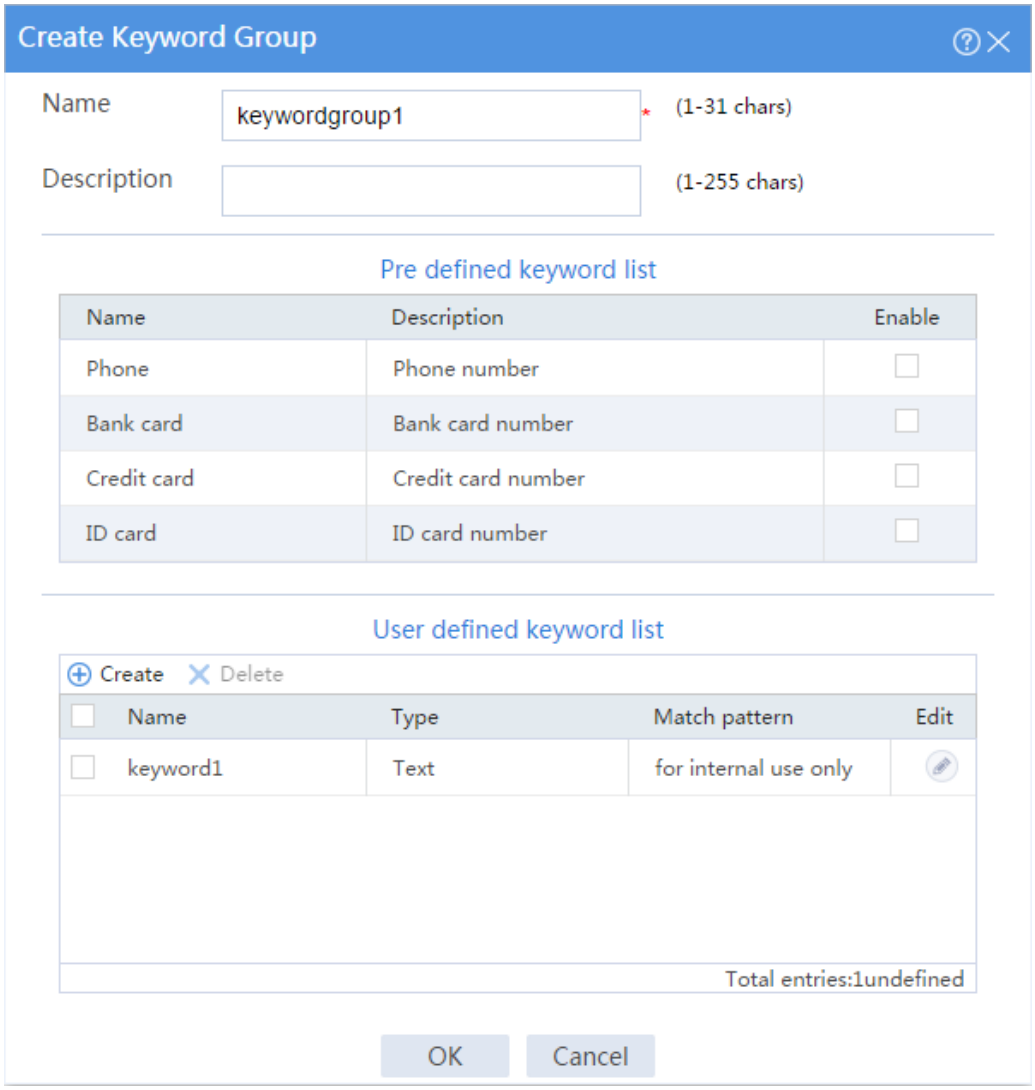
- Enter **keywordgroup1** in the **Name** field.
- In the **User defined keyword list** area, click **Create**.
- In the **Create Keyword** dialog box, enter **keyword1** in the **Name** field, select the **Text** type, and enter **for internal use only** in the **Match pattern** field.
- Click **OK**.

Figure 2 Creating a keyword



The newly created keyword **keyword1** is displayed in the **Create Keyword Group** dialog box.

Figure 3 Creating keyword group keywordgroup1



e. Click **OK**.

Create keyword group **keywordgroup2**.

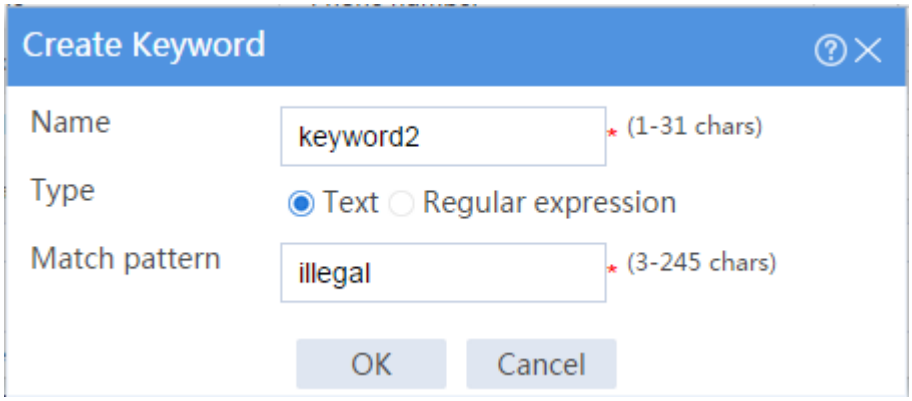
a. On the **Keyword Group** page, click **Create**.

b. In the dialog box that opens, configure the keyword group:

- Enter **keywordgroup2** in the **Name** field.
- In the **User defined keyword list** area, click **Create**.
- In the **Create Keyword** dialog box, enter **keyword2** in the **Name** field, select the **Text** type, and enter **illegal** in the **Match pattern** field.

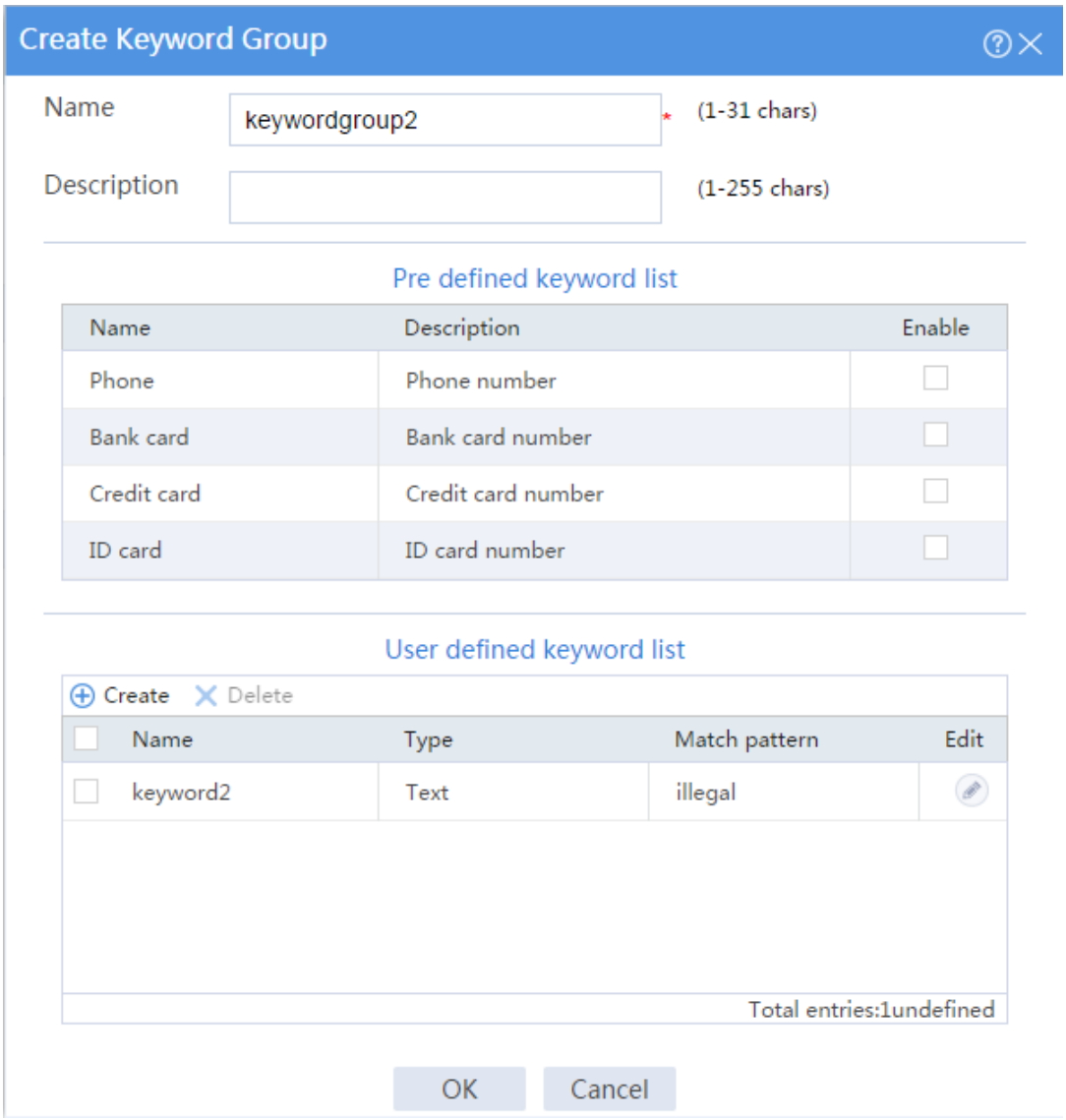
- Click **OK**.

Figure 4 Creating a keyword



The newly created keyword **keyword2** is displayed in the **Create Keyword Group** dialog box.

Figure 5 Creating keyword group keywordgroup2



c. Click **OK**.

4. Configure a data filtering profile.

On the top navigation bar, click **Objects**.

From the navigation pane, select **APP Security** > **Data Filtering** > **Profiles**.

Click **Create**.

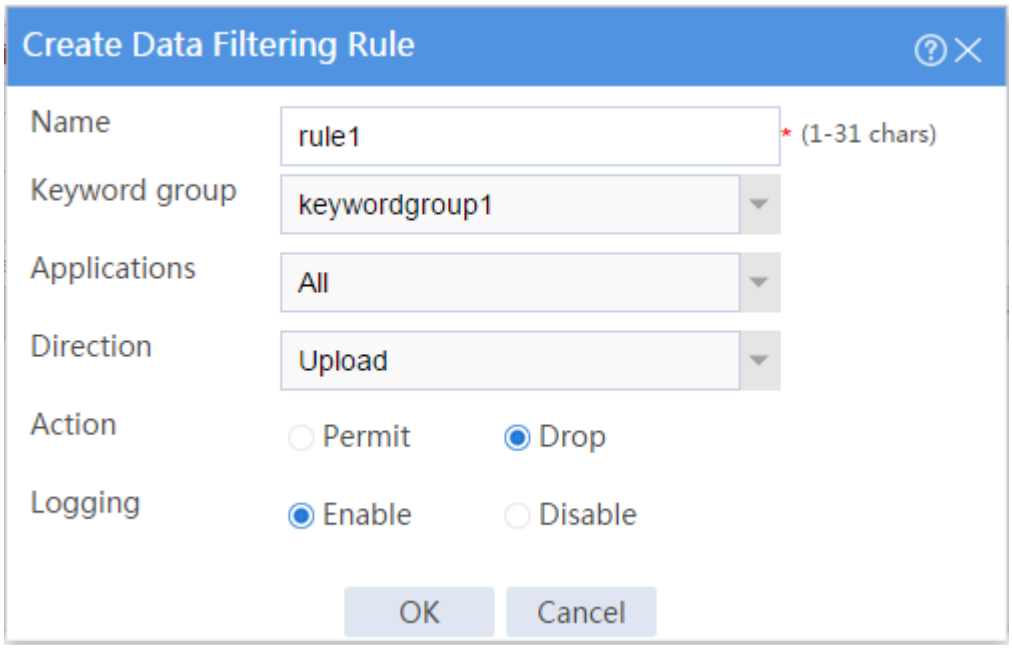
In the dialog box that opens, configure a data filtering profile.

a. Enter the name **datafilter**.

b. In the **Data filtering rules** area, click **Create**.

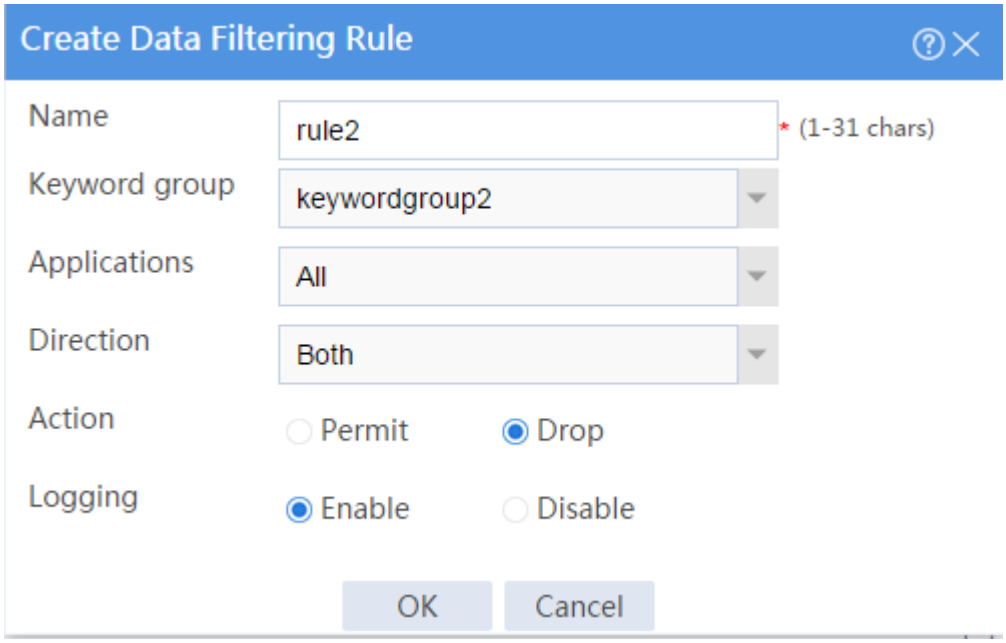
c. In the dialog box that opens, create data filtering rule **rule1** as shown in Figure 6, and then click **OK**.

Figure 6 Creating data filtering rule rule1



d. Create data filtering rule **rule2** (as shown in Figure 7) in the same way you configure data filtering rule **rule1**.

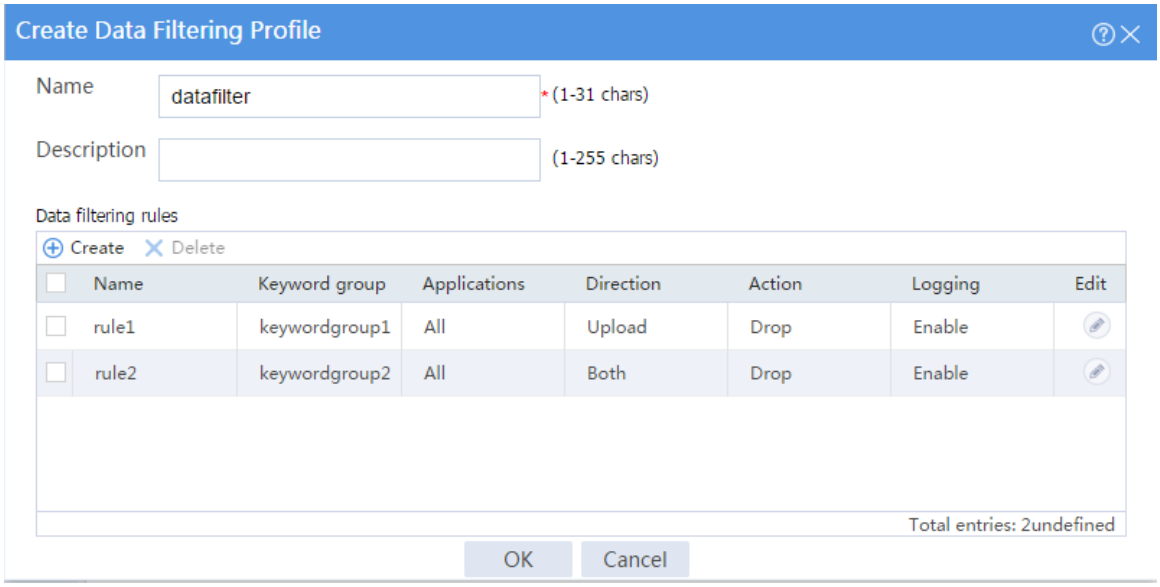
Figure 7 Creating data filtering rule rule2



The data filtering rules are displayed in the **Create Data Filtering Profile** dialog box, as shown in Figure 8.

e. Click **OK**.

Figure 8 Creating a data filtering profile



5. Create a security policy:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy:

- Enter policy name **datafilter**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IP address **10.1.1.0/24**.
- Select data filtering profile **datafilter** in the **Content security** area.

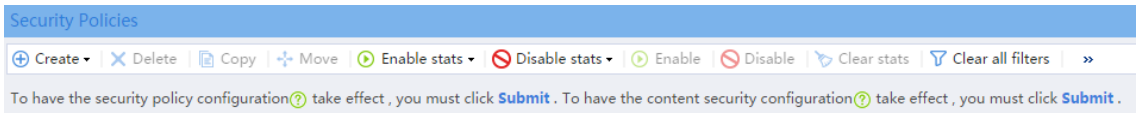
Cilck **OK**.

6. Activate the settings on the **Security Policies** page:

   # After you apply the data filtering profile to the security policy, click **Submit** (the second **Submit** in Figure 9) to have the content security configuration take effect.

   # Click **Activate** (the first **Submit** in Figure 9) to activate security policy matching acceleration.

Figure 9 Activate security policy settings



Verifying the configuration

Verify that data filtering can log and block the following Internet access behaviors of internal users:

- Browsing, publishing, or downloading information containing the **illegal** keyword on the Internet.
- Transferring files marked as for internal use only on the Internet.

To view the logs generated for these behaviors, perform either of the following tasks:

- At the CLI, execute the **`display logbuffer module dfilter`** command to view the data filtering logs.
- On the Web interface, click **System** on the top navigation bar, and then select **Log Settings** > **Basic Settings** from the navigation pane. On the **Syslog Settings** tab, create a log host to receive the logs. You can access the log host to view data filtering logs.

NetShare control configuration examples

Contents

Introduction

The following information provides NetShare control configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the NetShare control feature.

General restrictions and guidelines

The device supports only one NetShare control policy.

Example: Configuring NetShare control

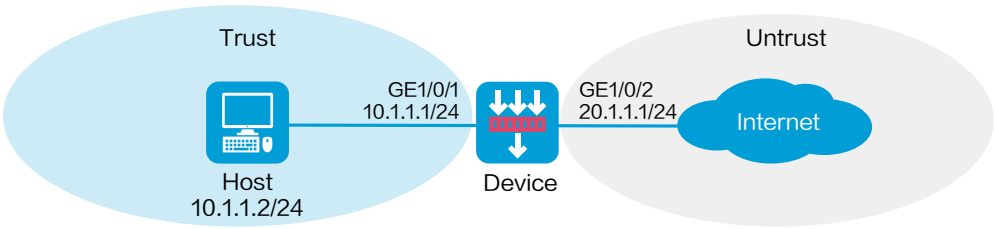
Network configuration

As shown in Figure 1, the device connects to the LAN and Internet through security zones **Trust** and **Untrust**, respectively.

Configure NetShare control on the device to meet the following requirements:

- Monitor the packets sent by the hosts on the LAN to the Internet based on the APR-based packet analysis for network sharing behavior inspection.
- If an IP address is detected to be shared by more than one host for Internet access, NetShare control will freeze the IP address for an hour and logs the event.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Create a security policy:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **test-a**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select type **IPv4**.
   - Select action **Permit**.
   - Select source IP address **10.1.1.2/24**.

   # Click **OK**.

3. Update the APR signature library to the latest version. (Details not shown.)

4. Configure a NetShare control policy.

   # On the top navigation bar, click **Policies**.

From the navigation pane, select **Netshare Control** > **Netshare Policy**.

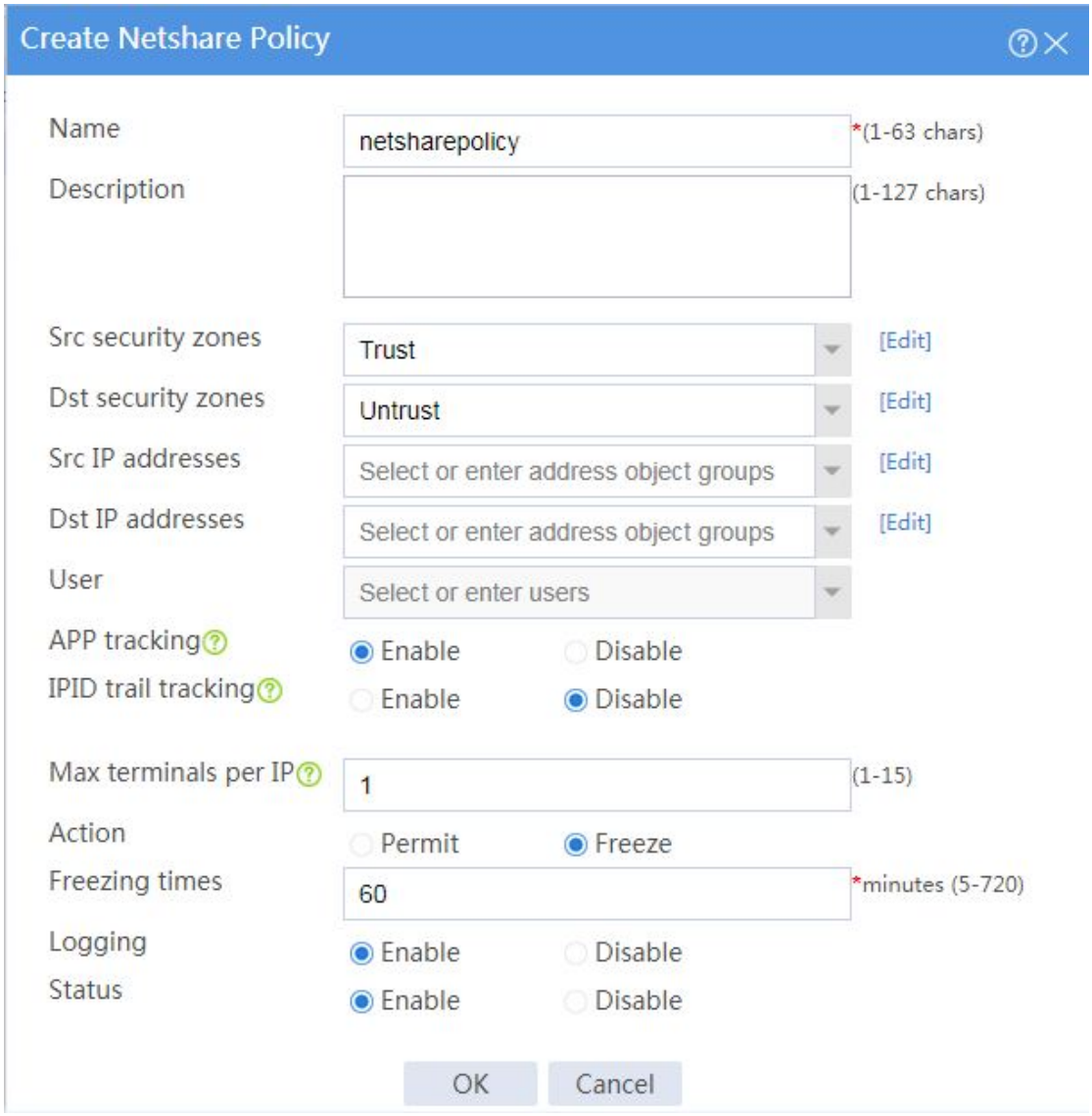
Click **Create**.

In the dialog box that appears, configure a NetShare policy:

- Enter policy name **netsharepolicy**.
- Select source security zone **Trust**.
- Select destination security zone **Untrust**.
- Enable APP tracking.
- Disable IPID trail tracking.
- Allow a maximum of one terminal per IP.
- Select action **Freeze**.
- Set the freezing times to 60.
- Enable logging.
- Enable the NetShare policy.

Cilck **OK**.

Figure 2 Creating a NetShare policy



5. Click **Submit** to have the NetShare policy configuration take effect.

Verifying the configuration

If a host on the LAN accesses the Internet by using a shared IP address through a proxy, the device can detect the network sharing behavior and will freeze the shared IP address for an hour and log the event.

To view the IP address with the network sharing behavior, click **Policies** on the top navigation bar and select **Netshare Control** > **Netshare List** from the navigation pane.

Bandwidth management configuration examples

Contents

Introduction

The following information provides bandwidth management configuration examples.

Bandwidth management provides fine-grained control over traffic that flows through the device by using the following information:

- Source and destination security zones.
- Source and destination IP addresses.
- Users and user groups.
- Applications and application groups.

- DSCP priorities.
- Time ranges.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of bandwidth management.

Restrictions and guidelines

When you configure bandwidth management, follow these restrictions and guidelines:

- Traffic policies support nesting, and can be nested for up to four levels.
- The maximum bandwidth for a child traffic policy must be smaller than or equal to that for its parent traffic policy.
- The guaranteed bandwidth for a child traffic policy must be smaller than or equal to that for its parent traffic policy.
- The traffic profiles cannot be the same for the child and parent traffic policies.

- An interface with small default expected bandwidth might experience traffic loss if the following conditions exist:
    - There is a large amount of traffic on the interface.
    - The interface uses the default expected bandwidth.

  To avoid traffic loss, implicitly set the expected bandwidth to a large value for such an interface. For example, you can set the expected bandwidth of a tunnel interface to a value greater than 64 kbps (the default) if there is a large amount of traffic on the interface.
- If a traffic policy to be copied has child traffic policies, only the parent traffic policy is copied.

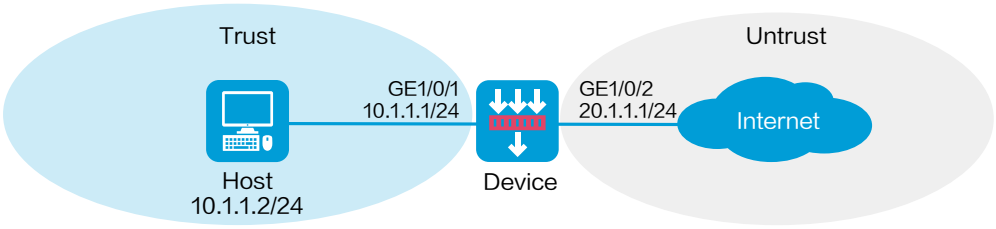
Example: Configuring a single traffic profile

Network configuration

As shown in Figure 1, configure bandwidth management on the device to meet the following requirements:

- The maximum bandwidth is limited to 30 Mbps for both upstream and downstream iQiYiPPS application traffic of the host in the intranet.
- The guaranteed bandwidth is 30 Mbps for both upstream and downstream FTP traffic of the host .
- The bandwidth of the interface to the Internet is limited to 100 Mbps.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Trust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.
   - Use the default settings for other parameters.
   - Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure security policies.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **Trust-Untrust**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Enter source IPv4 address **10.1.1.2/24**.
   - Select action **Permit**.
   - Use the default settings for other parameters.
   - Click **OK**.

3. Configure traffic profiles.

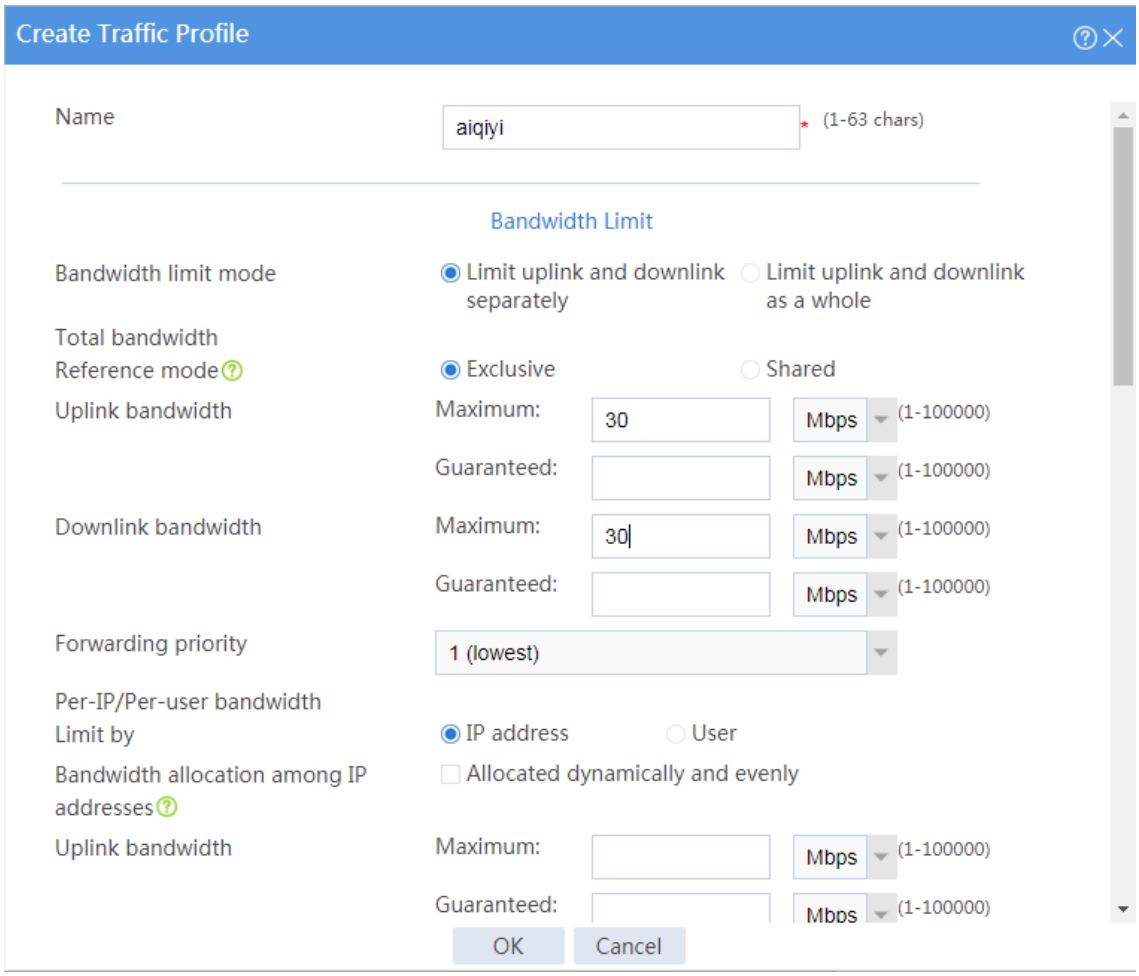
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Bandwidth Management** > **Traffic Profiles**.

   # Click **Create**.

   # In the dialog box that opens, create a traffic profile named **aiqiyi** as shown in Figure 2.

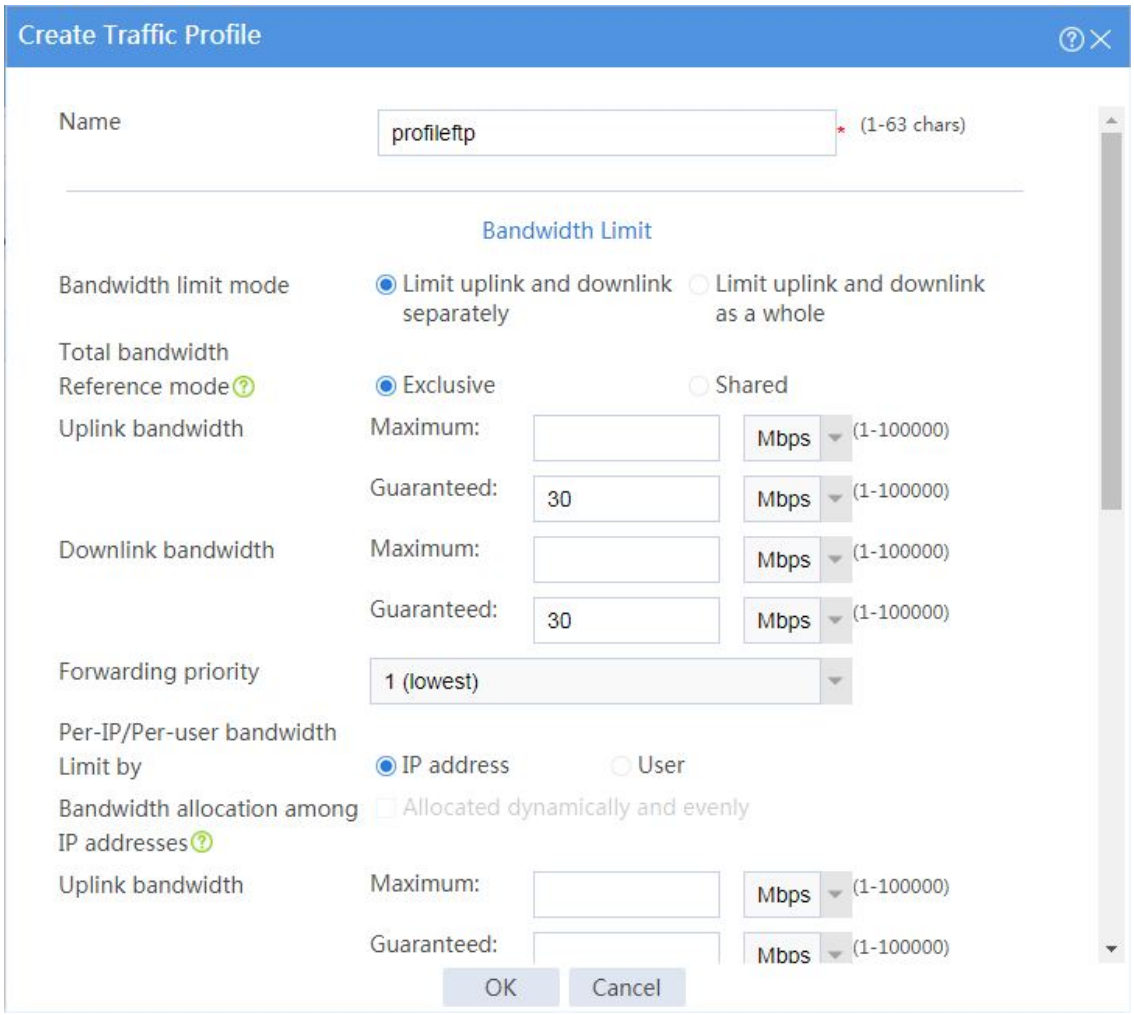
Figure 2 Creating a traffic profile named aiqiyi



Click **OK**.

Create a traffic profile named **profileftp** in the same way you create traffic profile **aiqiyi**, as shown in Figure 3.

Figure 3 Creating a traffic profile named profileftp



Click **OK**.

4. Configure traffic policies.

On the top navigation bar, click **Policies**.

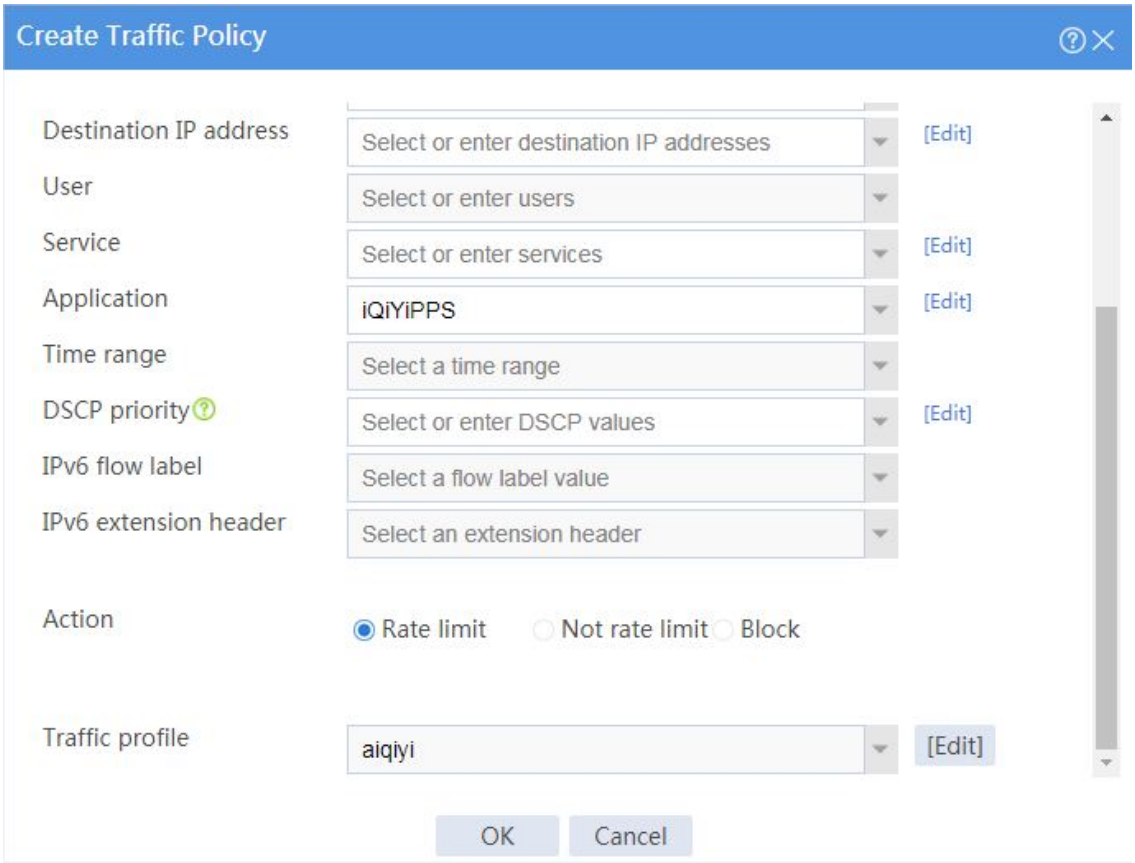
From the navigation pane, select **Bandwidth Management** > **Traffic Policies**.

Click **Create**.

In the dialog box that opens, create a traffic policy named **aiqiyi**, as shown in Figure 4.

Figure 4 Creating a traffic policy named aiqiyi

Figure 5 Creating a traffic policy named aiqiyi (continued)

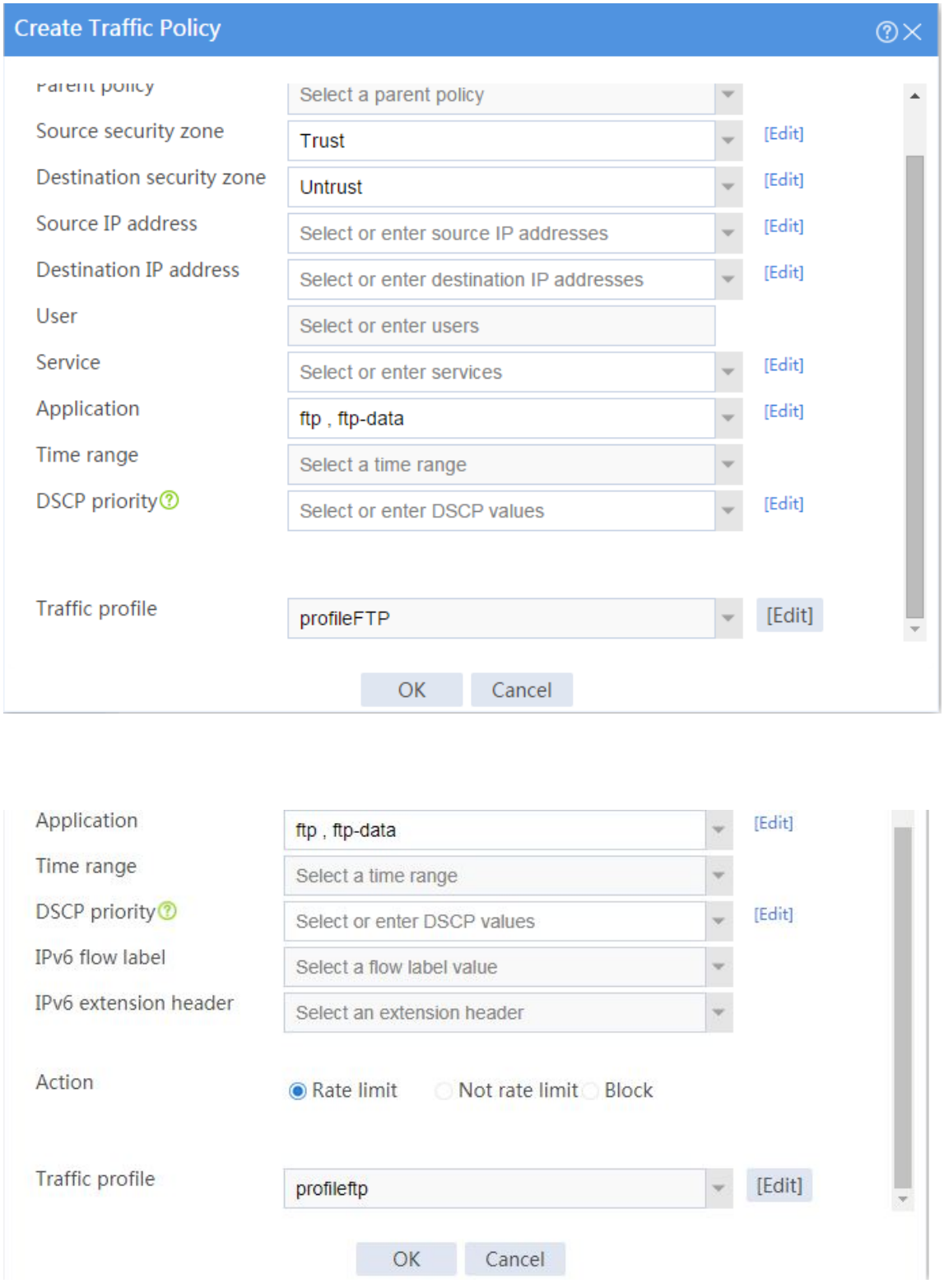


Click **OK**.

After creating the traffic policy, select the policy and click **Enable** to enable the policy.

Create a traffic policy **FTP** in the same way you create traffic policy **aiqiyi**, as shown in Figure 6.

Figure 6 Creating a traffic policy named FTP



Click **OK**.

After creating the traffic policy, select the policy and click **Enable** to enable the policy.

5. Configure interface bandwidth.

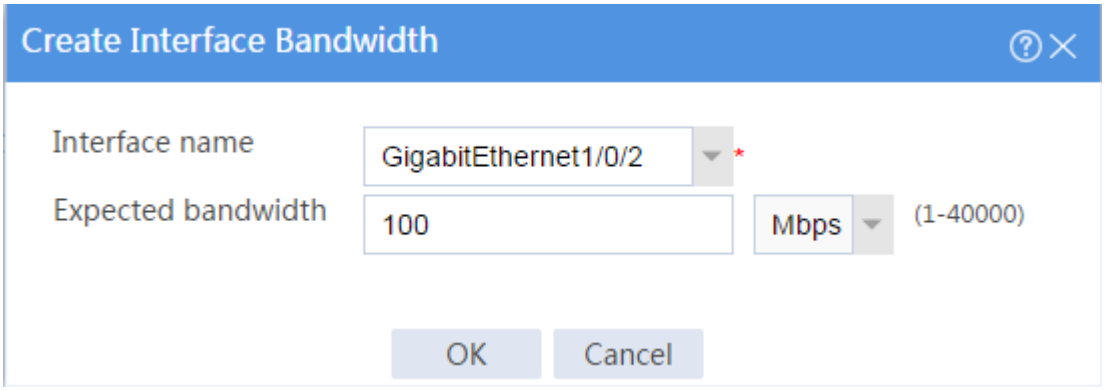
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Bandwidth Management** > **Interface Bandwidth**.

   # Click **Create**.

   # In the dialog box that opens, configure interface bandwidth as shown in Figure 7.

   Figure 7 Configuring interface bandwidth



   # Click **OK**.

Verifying the configuration

Verify that the iQiYiPPS application traffic rate cannot exceed 30 Mbps and the FTP traffic rate can reach a minimum of 30 Mbps when the total traffic rate on GigabitEthernet 1/0/2 reaches 100 Mbps.

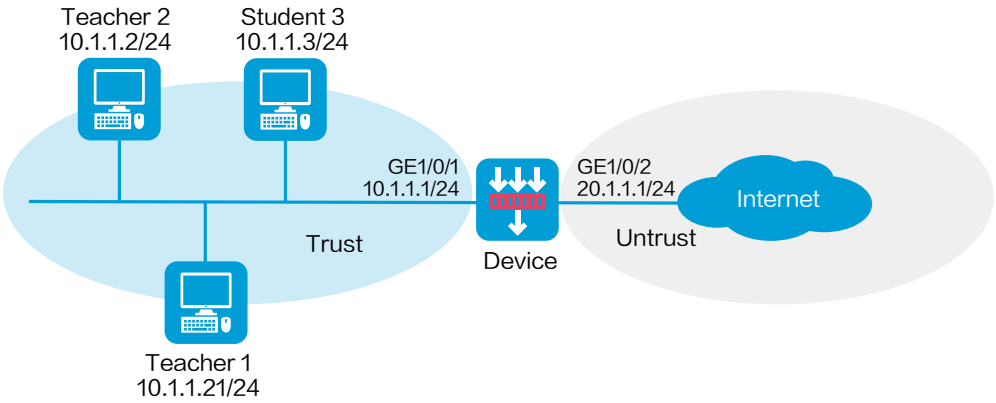
Example: Configuring parent/child traffic profiles

Network configuration

As shown in Figure 8, configure bandwidth management on the device to meet the following requirements:

- The maximum bandwidth is limited to 30 Mbps for both upstream and downstream iQiYiPPS application traffic of the host in the intranet.
- The guaranteed bandwidth is 30 Mbps for both upstream and downstream FTP traffic of the host .
- The total traffic rate of the host is limited to 50 Mbps.

Figure 8 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure security policies.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **Trust-Untrust**.

- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select action **Permit**.
- Enter source IPv4 address **10.1.1.2/24**.

Click **OK**.

3. Configure traffic profiles.

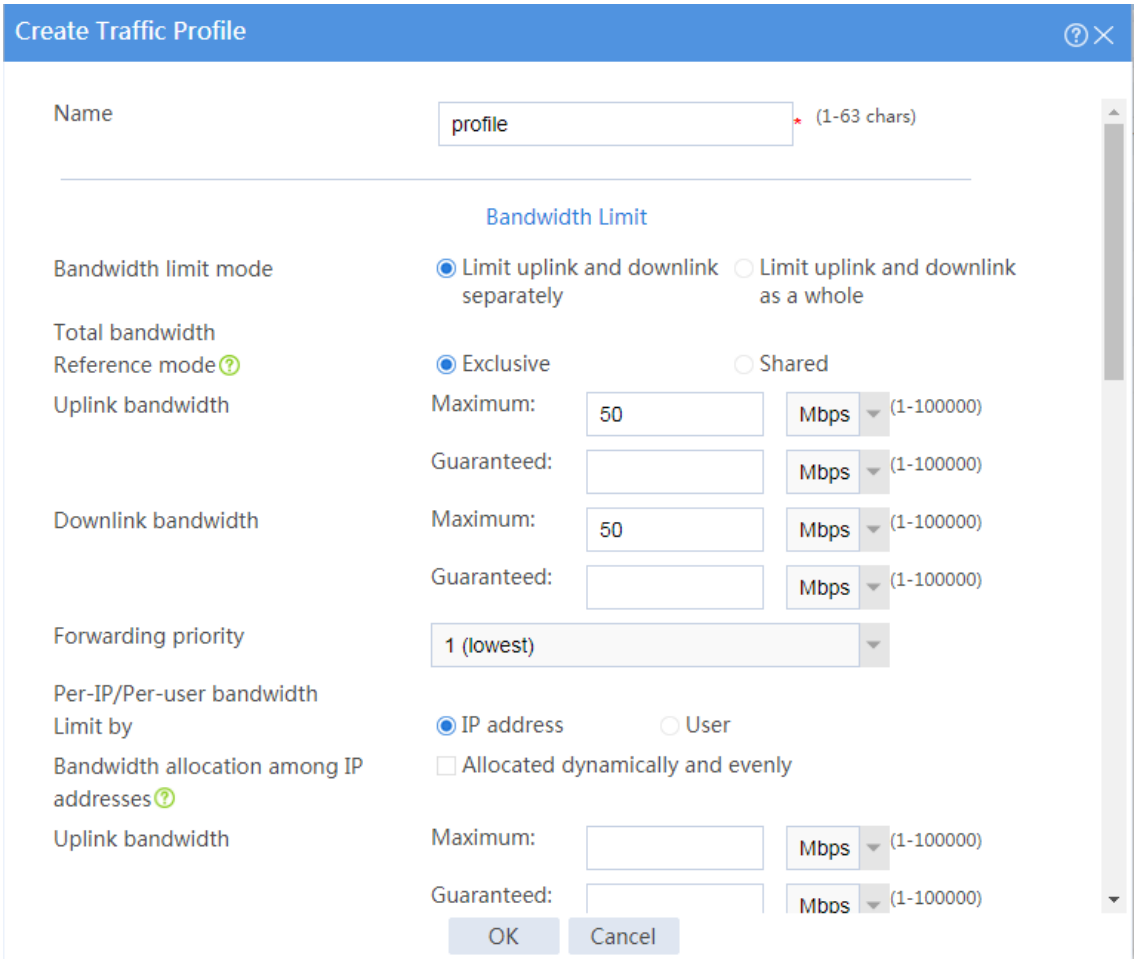
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Bandwidth Management** > **Traffic Profiles**.

   # Click **Create**.

   # In the dialog box that opens, configure a traffic profile as shown in Figure 9.

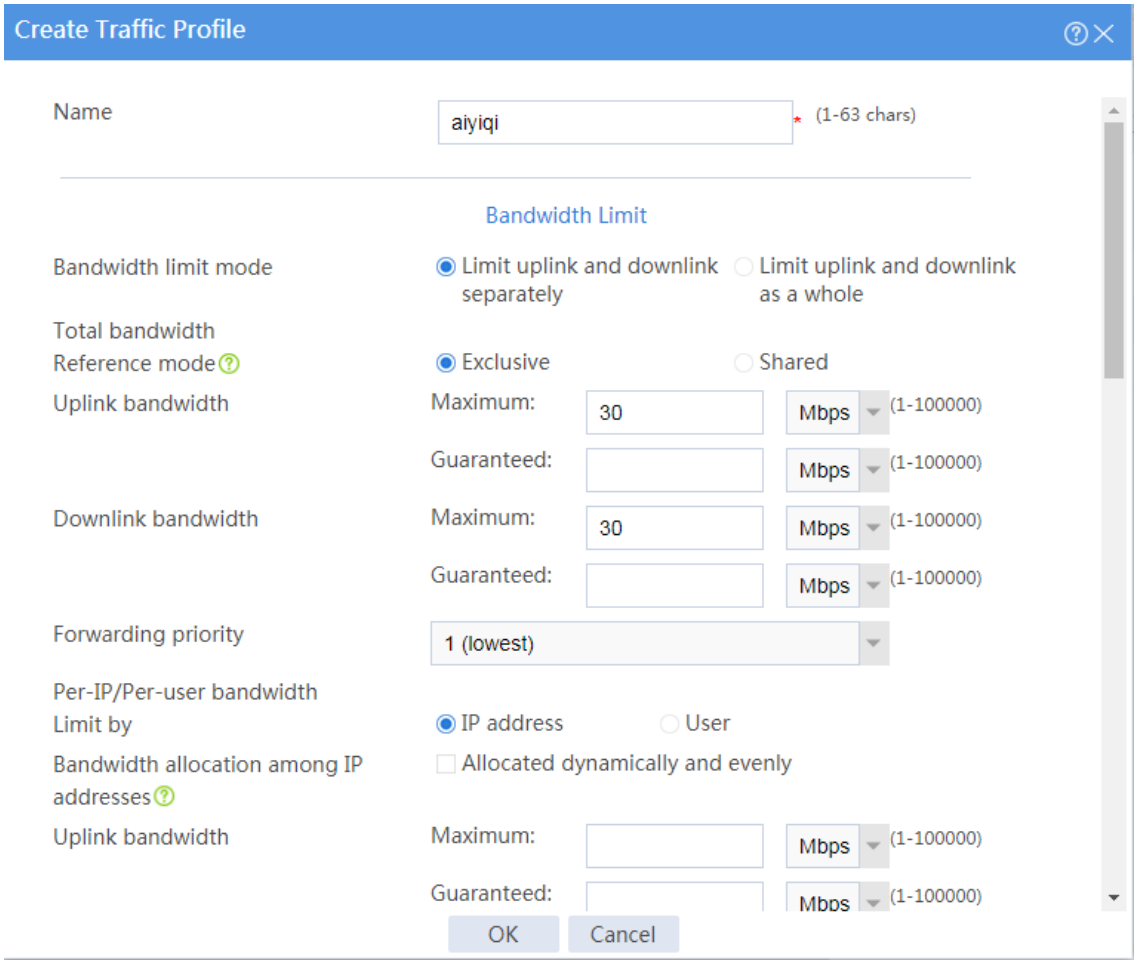
Figure 9 Creating a traffic profile named profile



Click **OK**.

Create a traffic profile named **aiqiyi** in the same way you create the traffic profile named **profile**, as shown in Figure 10.

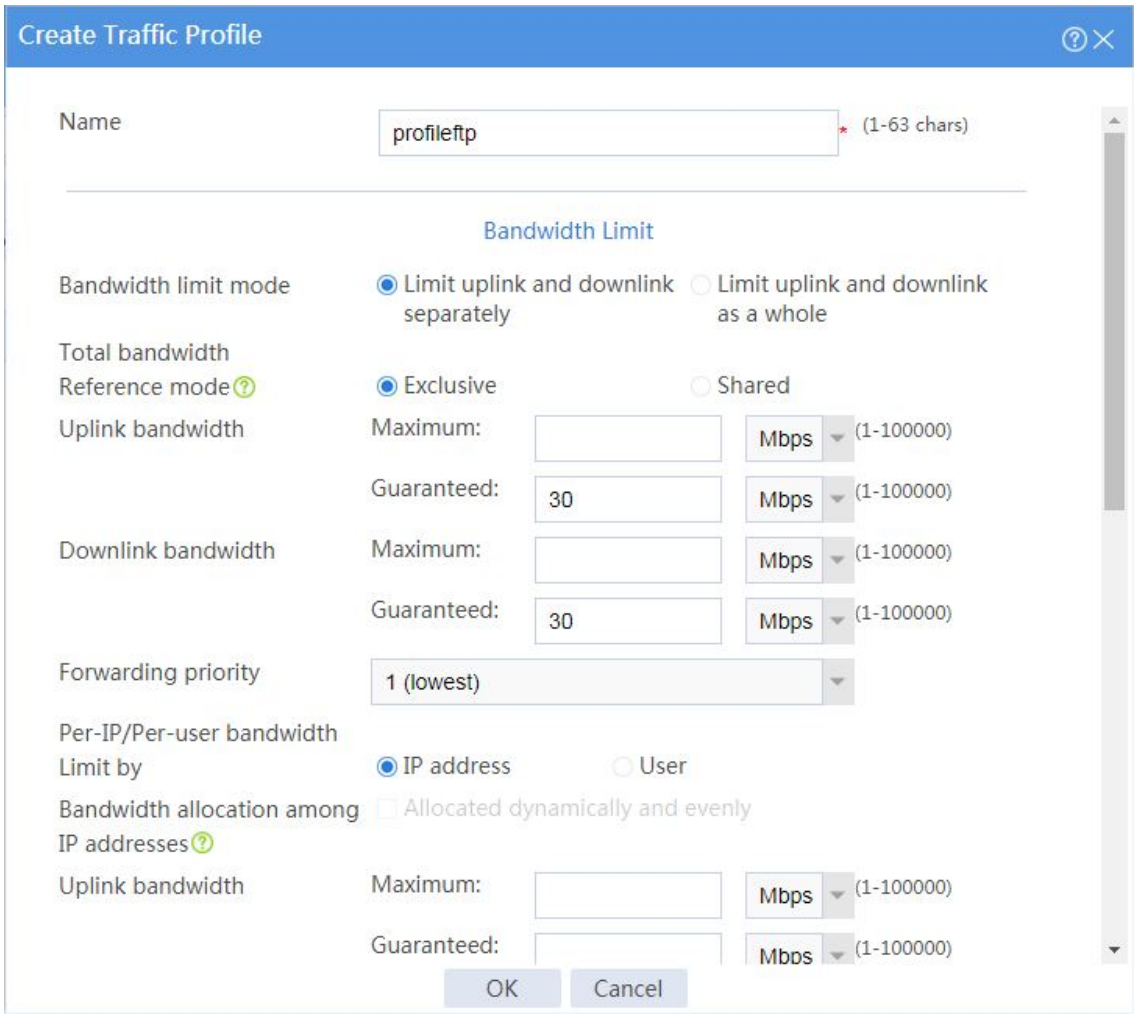
Figure 10 Creating a traffic profile named aiqiyi



Click **OK**.

Create a traffic profile named **profileftp** in the same way you create the traffic profile named **profile**, as shown in Figure 11.

Figure 11 Creating a traffic profile named profileftp



Click **OK**.

4. Configure the parent traffic policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Bandwidth Management** > **Traffic Policies**.

Click **Create**.

In the dialog box that opens, create a traffic policy named **policy** as shown in Figure 12.

Figure 12 Creating a traffic policy named policy

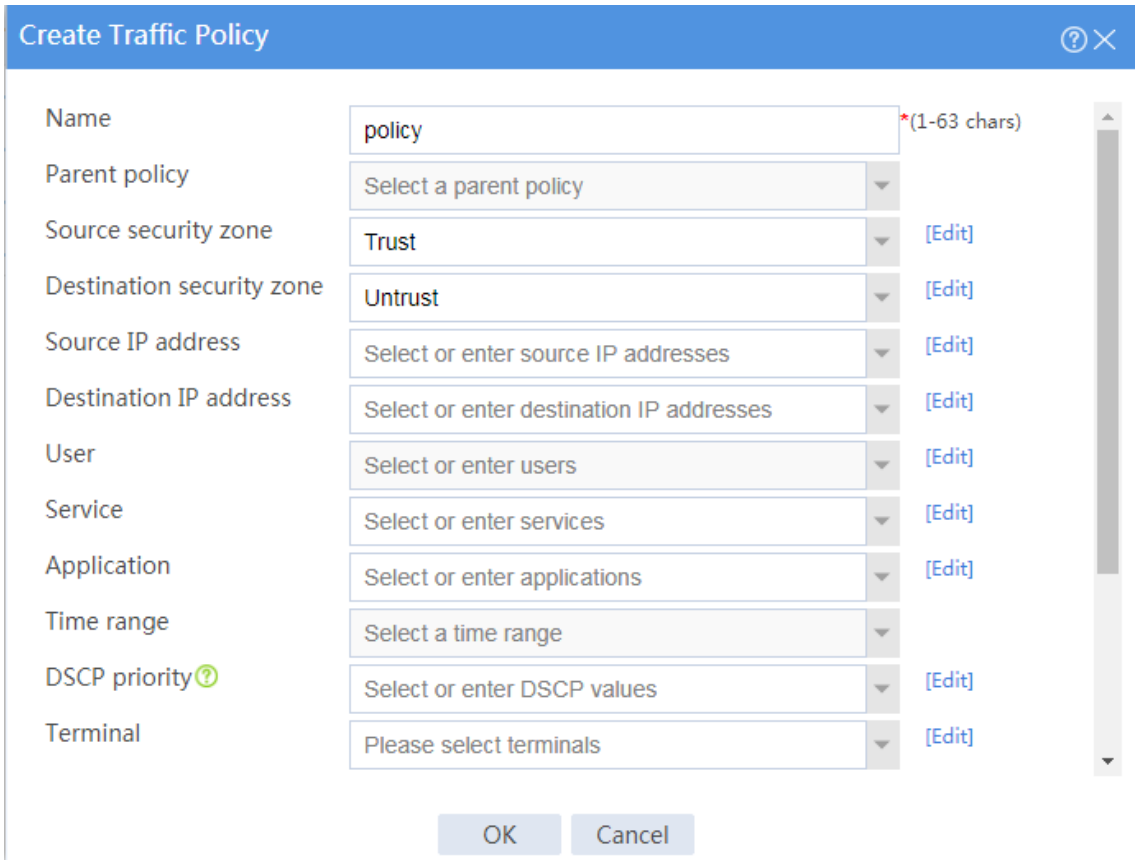
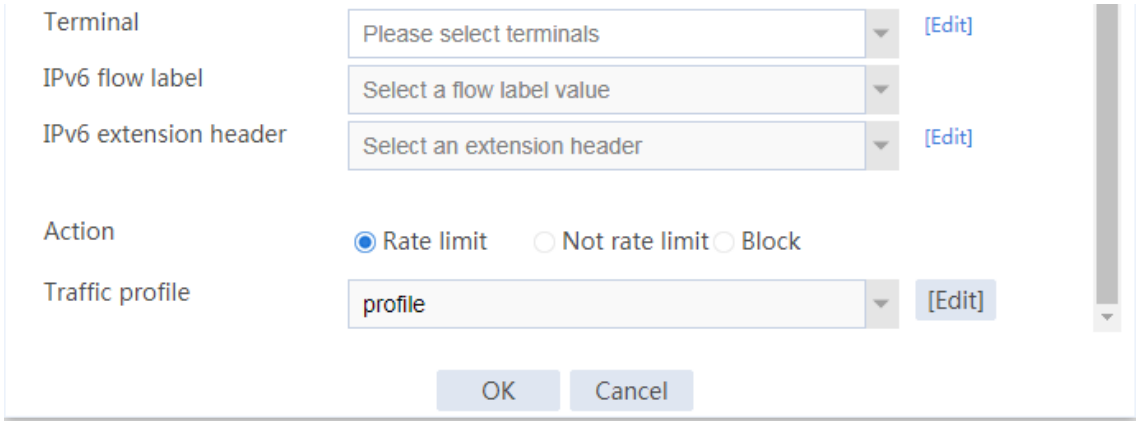


Figure 13 Creating a traffic policy named policy (continued)



Click **OK**.

After creating the traffic policy, select the policy and click **Enable** to enable the policy.

5. Configure child traffic policies.

On the top navigation bar, click **Policies**.

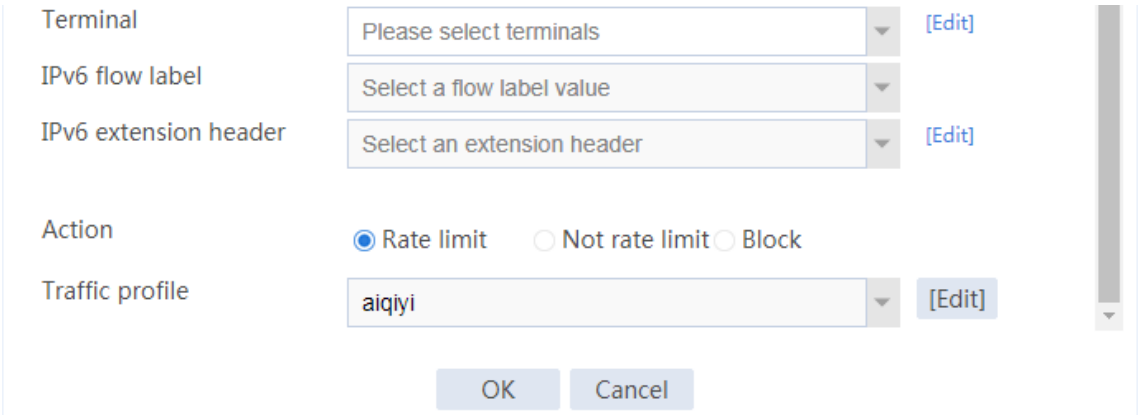
From the navigation pane, select **Bandwidth Management** > **Traffic Policies**.

Click **Create**.

In the dialog box that opens, create a traffic policy named **aiqiyi** as shown in Figure 14.

Figure 14 Creating a traffic policy named aiqiyi

Figure 15 Creating a traffic policy named aiqiyi (continued)



Click **OK**.

After creating the traffic policy, select the policy and click **Enable** to enable the policy.

Create a traffic policy named **FTP** in the same way you create the traffic policy named **policy**, as shown in Figure 16.

Figure 16 Creating a traffic policy named FTP

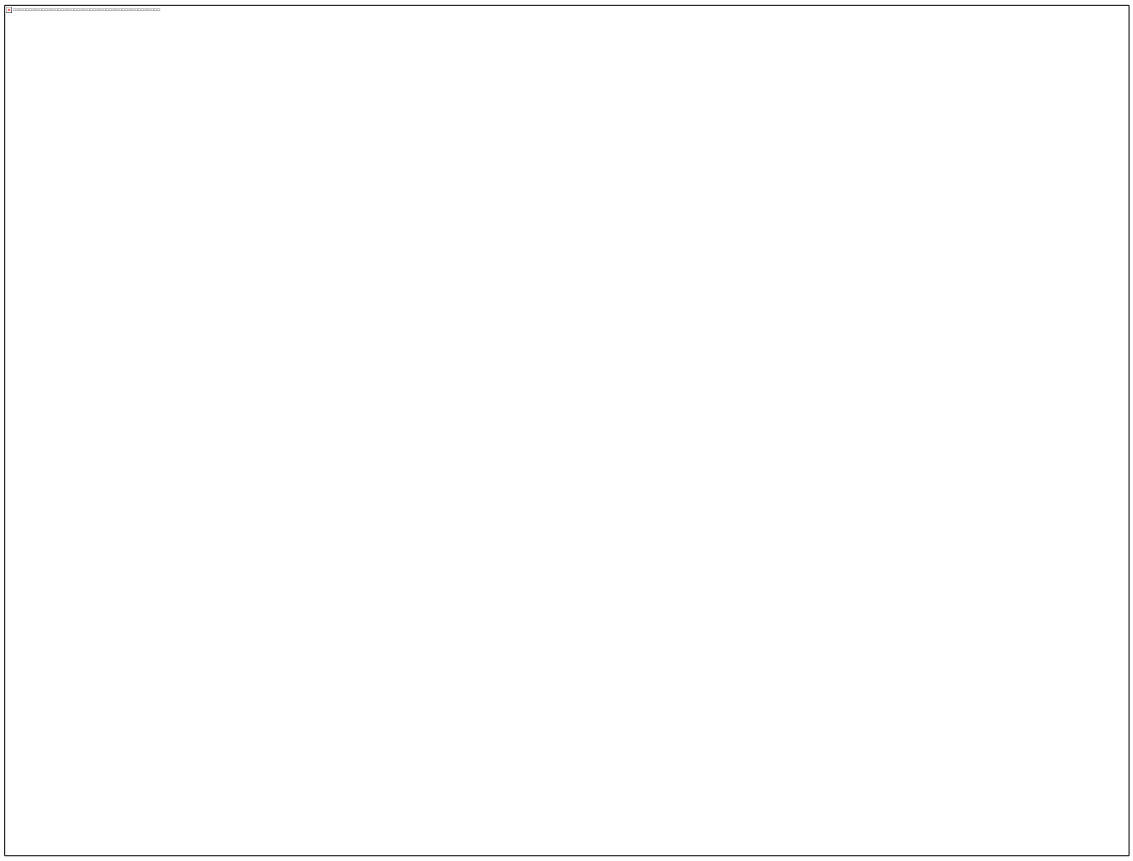
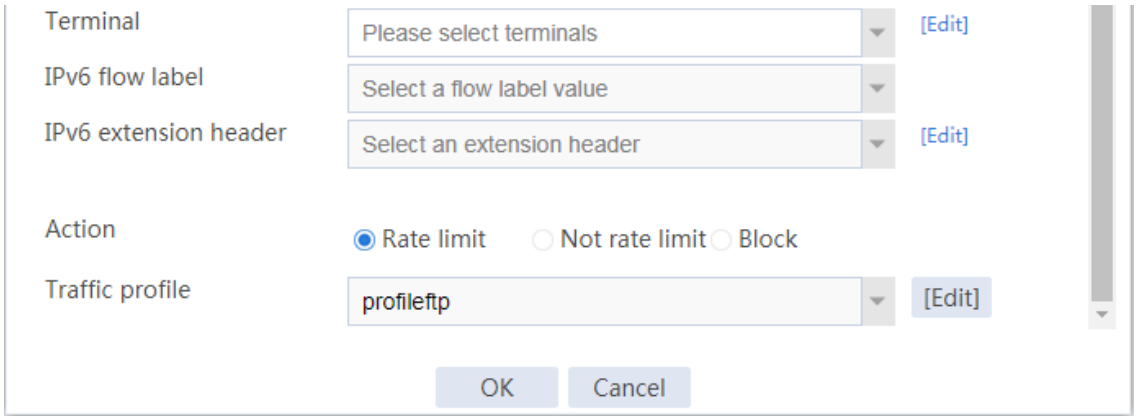


Figure 17 Creating a traffic policy named FTP (continued)



Click **OK**.

After creating the traffic policy, select the policy and click **Enable** to enable the policy.

Verifying the configuration

Verify that the total traffic rate of the host is limited to 50 Mbps, and that the iQiYiPPS application traffic rate is limited to 30 Mbps. When congestion occurs, bandwidth of 30 Mbps is guaranteed for FTP traffic.

Example: Configuring a user-based traffic profile

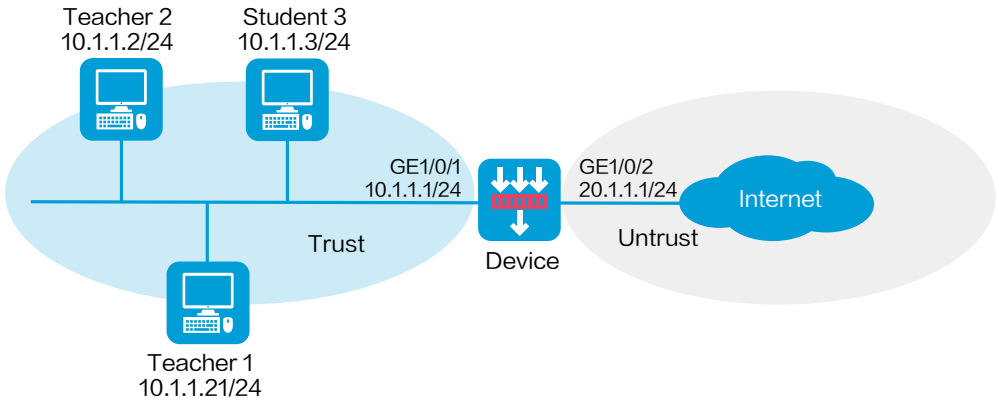
Network configuration

As shown in Figure 18, an intranet has two user groups: a teacher group with two teachers and a student group with five students.

Configure per-user bandwidth management on the device to meet the following requirements:

- The bandwidth is limited to 10 Mbps for each teacher in both the upstream and downstream directions, and the bandwidth is limited to 2 Mbps for each student in both the upstream and downstream directions.
- Teachers have higher priority over students to access the Internet.

Figure 18 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Trust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.1.1/24.

c. Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

2. Configure security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy:

- Enter policy name **Trust-Untrust**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Enter source IPv4 address **10.1.1.0/24**.
- Select action **Permit**.

Click **OK**.

3. Create identity users.

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **Local Users**.

On the **User** tab, click **Create**.

In the dialog box that opens, configure the username as **student1**.

Click **OK**.

Create users **student2**, **student3**, **student4**, **student5**, **teacher1**, and **teacher2** in the same way the user **student1** is created.

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **Local Users**.

On the **User Group** tab, click **Create**.

In the dialog box that opens, configure the group name as **student** and configure identity users **student1**, **student2**, **student3**, **student4**, and **student5** for the group.

Click **OK**.

Create a group named **teacher** and configure identity users **teacher1** and **teacher2** for the group in the same way the group **student** is configured.

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **Online Users**.

On the **Static Identity Users** tab, click **Create**.

In the dialog box that opens, configure the username as **student1**, configure the IP address type as IPv4, and configure the IP address as 10.1.1.11.

Click **OK**.

Create static identity users **student2**, **student3**, **student4**, **student5**, **teacher1**, and **teacher2** in the same way the static identity user **student1** is configured.

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **Online Users**.

On the **Online Users** tab, click **Enable user identification**.

4. Configure traffic profiles.

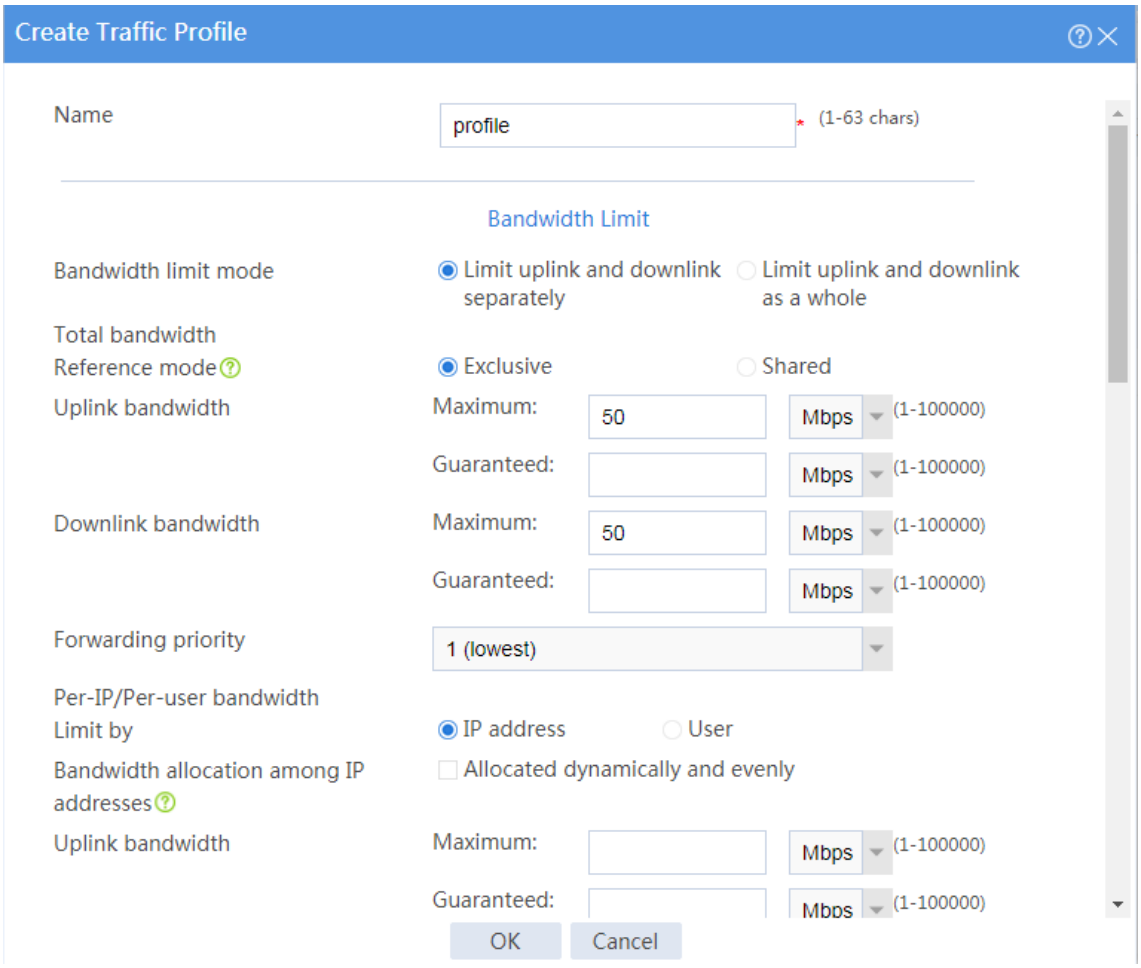
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Bandwidth Management** > **Traffic Profiles**.

   # Click **Create**.

   # In the dialog box that opens, create a traffic profile named **profile-teacher** as shown in Figure 19.

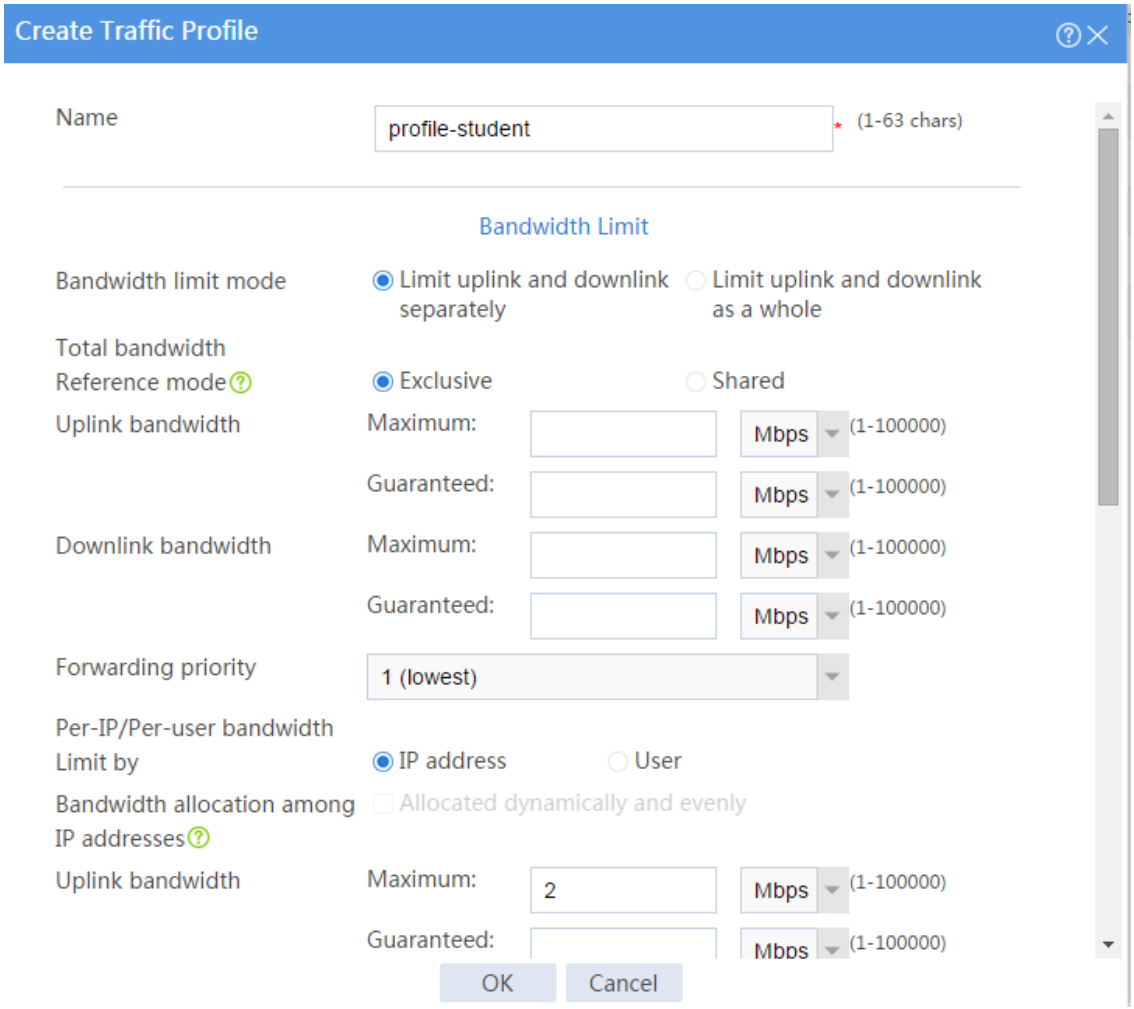
Figure 19 Creating a traffic profile named profile-teacher



Click **OK**.

Create a traffic profile named **profile-student** as shown in Figure 20.

Figure 20 Creating a traffic profile named profile-student



Click **OK**.

5. Configure traffic policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Bandwidth Management** > **Traffic Policies**.

Click **Create**.

In the dialog box that opens, create a traffic policy named **policy-teacher** as shown in Figure 21.

Figure 21 Creating a traffic policy named policy-teacher

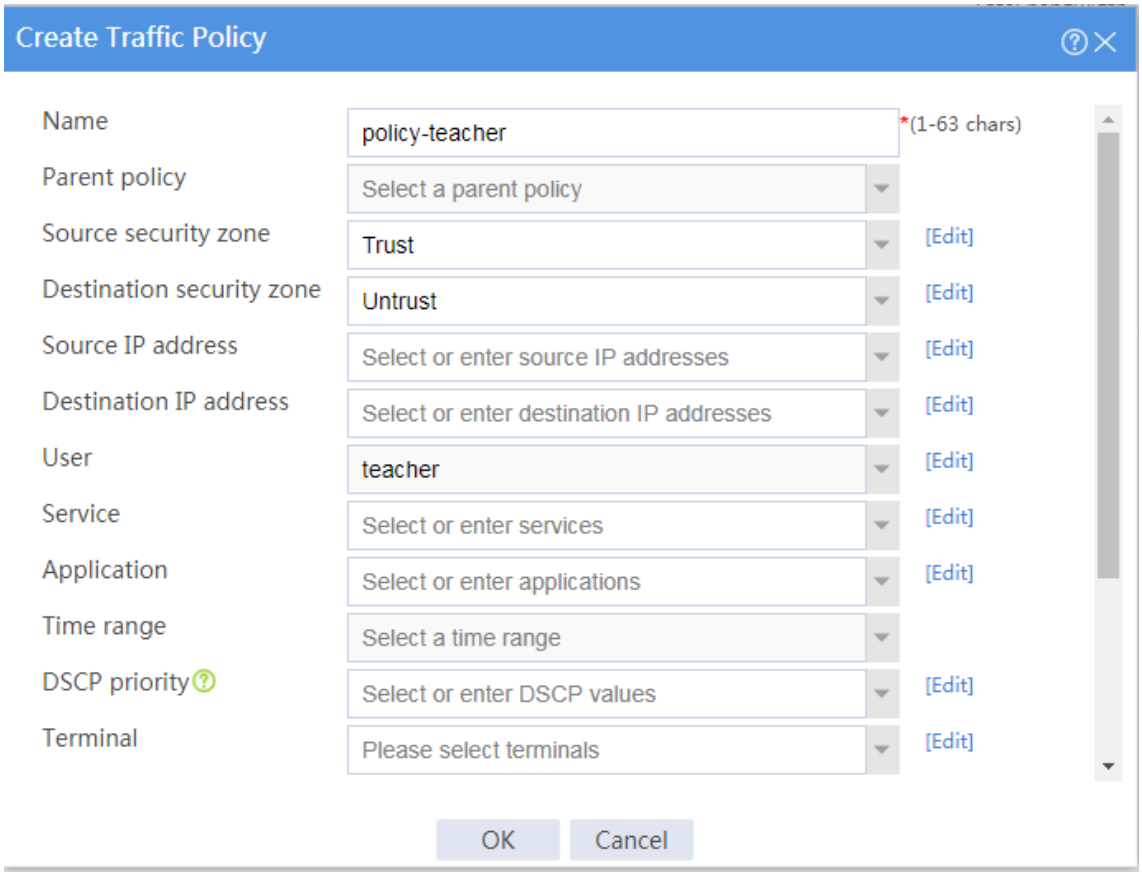
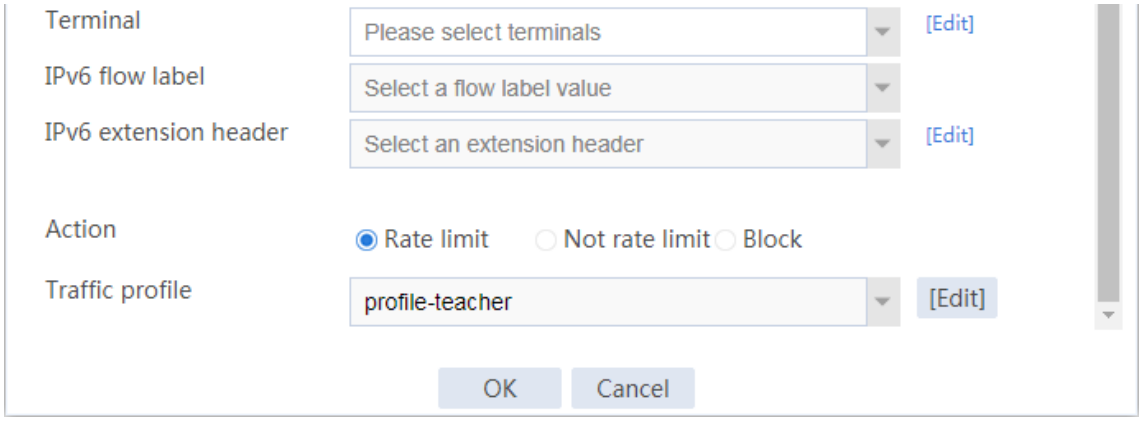


Figure 22 Creating a traffic policy named policy-teacher (continued)



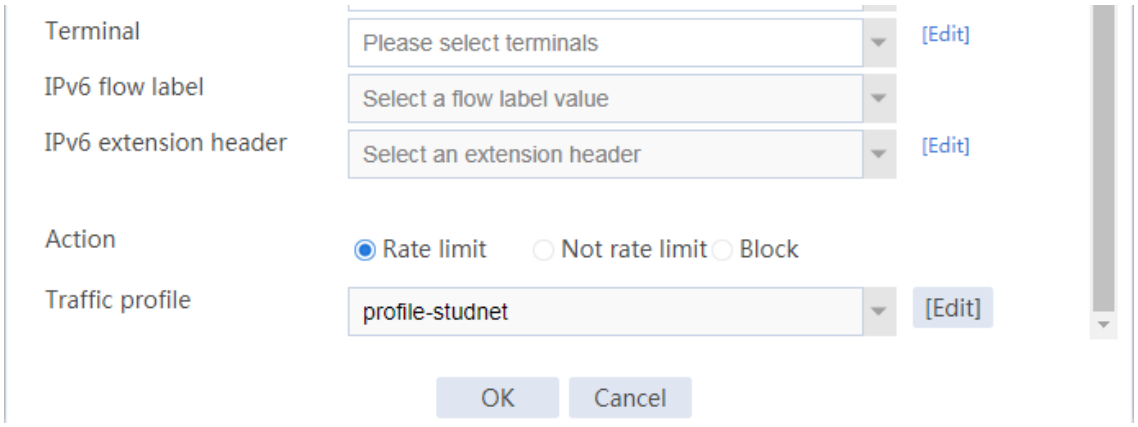
Click **OK**.

After creating the traffic policy, select the policy and click **Enable** to enable the policy.

Create a traffic policy named **policy-student** in the same way you create the traffic policy named **policy-teacher**, as shown in Figure 23.

Figure 23 Creating a traffic policy named policy-student

Figure 24 Creating a traffic policy named policy-student (continued)



Click **OK**.

After creating the traffic policy, select the policy and click **Enable** to enable the policy.

Verifying the configuration

Verify that the bandwidth is limited to 10 Mbps for each teacher, and that the bandwidth is limited to 2 Mbps for each student.

Verify that the connection counts are limited for both students and teachers.

IPsec configuration examples

Contents

Introduction

The following information provides IPsec configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the IPsec feature.

Restrictions and guidelines

- When you specify the remote host name in an IPsec policy, follow these restrictions and guidelines:
  - If the remote host name is resolved by a DNS server, the local device gets the latest IP address corresponding to the host name by sending a query to the DNS server when the cached DNS entry ages. The DNS entry aging information is obtained from the DNS server.
  - If the remote host name is resolved by a locally configured static DNS entry and the IP address in the entry is changed, you must respecify the remote host name in the IPsec policy to get the new IP address.
- To make sure SAs can be set up and the traffic protected by IPsec can be processed correctly between two IPsec peers, create mirror image ACLs on the IPsec peers. If the ACL rules on IPsec peers do not form mirror images of each other, SAs can be set up only when both of the following requirements are met:
  - The range specified by an ACL rule on one peer is covered by its counterpart ACL rule on the other peer.
  - The peer with the narrower rule initiates SA negotiation.

    If a wider ACL rule is used by the SA initiator, the negotiation request might be rejected because the matching traffic is beyond the scope of the responder.
- If you do not configure the local identity in an IPsec policy, the policy uses the global local identity settings configured in the advanced settings.

- Modifications to the following settings in an IPsec policy take effect only on IPsec SAs set up after the modifications:
  - Encapsulation mode.
  - Security protocol.
  - Security algorithms.
  - PFS.
  - IPsec SA lifetimes.
  - IPsec SA idle timeout.

  For the modifications to take effect on existing IPsec SAs, you must reset the IPsec SAs.
- The IPsec peers of an IPsec tunnel must have IPsec policies that use the same security protocols, security algorithms, and encapsulation mode.
- When IKE negotiates IPsec SAs, it uses the IPsec SA lifetime settings configured in the IPsec policy to negotiate the IPsec SA lifetime with the peer. If the IPsec SA lifetime settings are not configured in the IPsec policy, the global IPsec SA lifetime settings are used. IKE uses the local lifetime settings or those proposed by the peer, whichever are smaller.

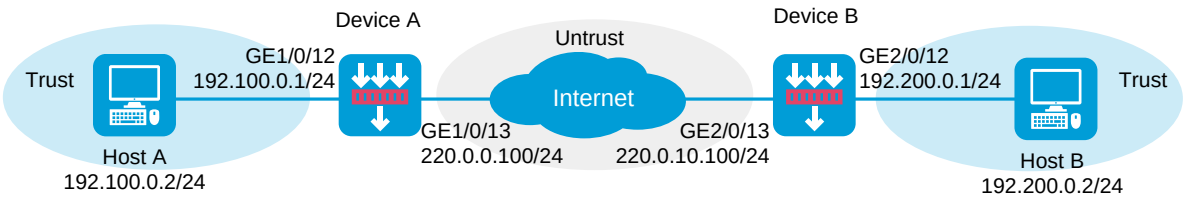
Example: Configuring an IPsec tunnel for IPv4 subnets

Network configuration

As shown in Figure 1, establish an IPsec tunnel between Device A and Device B to protect data flows between the subnets of Host A and Host B. Configure the tunnel as follows:

- Set up SAs through IKE negotiation.
- Configure IKE to use the 3DES-CBC encryption algorithm, the SHA256 authentication algorithm, and the preshared key authentication method.
- Specify the IPsec encapsulation mode as tunnel and the security protocol as ESP

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/13.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. Click the **IPv4 Address** tab. Enter the IP address and mask length of the interface. In this example, use 220.0.0.100/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/12 to the **Trust** security zone and set its IP address to 192.100.0.1/24 in the same way you configure GE 1/0/13.

2. Configure settings for routing:

This example configures static routes.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static route to reach 220.0.10.100:

a. Set the destination IP address to 220.0.10.100.

b. Set the mask length to 24.

c. Set the next hop address to 220.0.0.2.

d. Use the default settings for other parameters.

e. Click **OK**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static route to reach 192.200.0.2:

a. Set the destination IP address to 192.200.0.2.

b. Set the mask length to 24.

c. Set the next hop address to 220.0.0.2.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Configure security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

Configure a security policy named **trust-untrust** to permit specific traffic from the **Trust** to **Untrust** security zones:

a. Set the security policy name to **trust-untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **192.100.0.0/24**.

g. Enter destination IPv4 address **192.200.0.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-trust** to permit specific traffic from the **Untrust** to **Trust** security zones:

a. Set the security policy name to **untrust-trust**.

b. Select source zone **Untrust**.

c. Select destination zone **Trust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **192.200.0.0/24**.

g. Enter destination IPv4 address **192.100.0.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **local-untrust** to permit specific traffic from the **Local** to **Untrust** security zones:

a. Set the security policy name to **local-untrust**.

b. Select source zone **Local**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **220.0.0.100**.

g. Enter destination IPv4 address **220.0.10.100**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-local** to permit specific traffic from the **Untrust** to **Local** security zones:

a. Set the security policy name to **untrust-local**.

b. Select source zone **Untrust**.

c. Select destination zone **Local**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **220.0.10.100**.

g. Enter destination IPv4 address **220.0.0.100**.

h. Use the default settings for other parameters.

i. Click **OK**.

4. Create an IKE proposal:

On the top navigation bar, click **Network**.

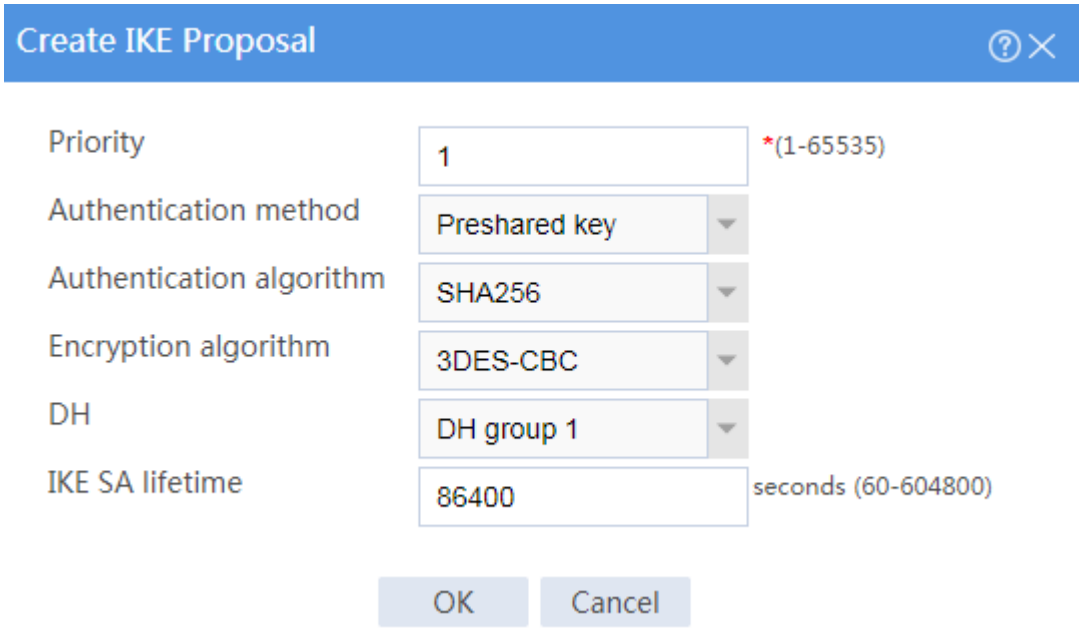
From the navigation pane, select **VPN** > **IPsec** > **IKE Proposals**.

Click **Create**.

- Set the priority to 1.
- Select the preshared key authentication method.
- Select the SHA256 authentication algorithm.
- Select the 3DES-CBC encryption algorithm.
- Use the default settings for other parameters.

Click **OK**.

Figure 2 Creating an IKE proposal



5. Configure the IPsec policy:

   # On the top navigation bar, click **Network**.

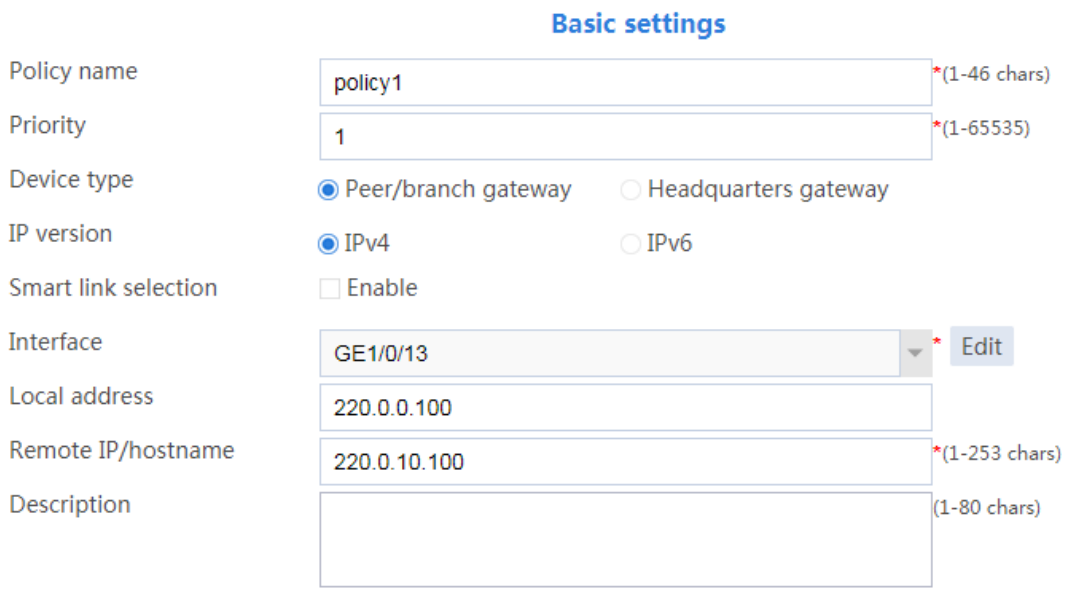
   # From the navigation pane, select **VPN** > **IPsec** > **IPsec Policies**.

   # Click **Create**.

   # Configure the basic settings as follows:

   - Set the policy name to **policy1**.
   - Set the priority to 1.
   - Set the device type to **Peer/branch gateway**.
   - Set the IP version to **IPv4**.
   - Select interface GE1/0/13.
   - Configure the local address as 220.0.0.100.
   - Configure the remote address/host name as 220.0.10.100.

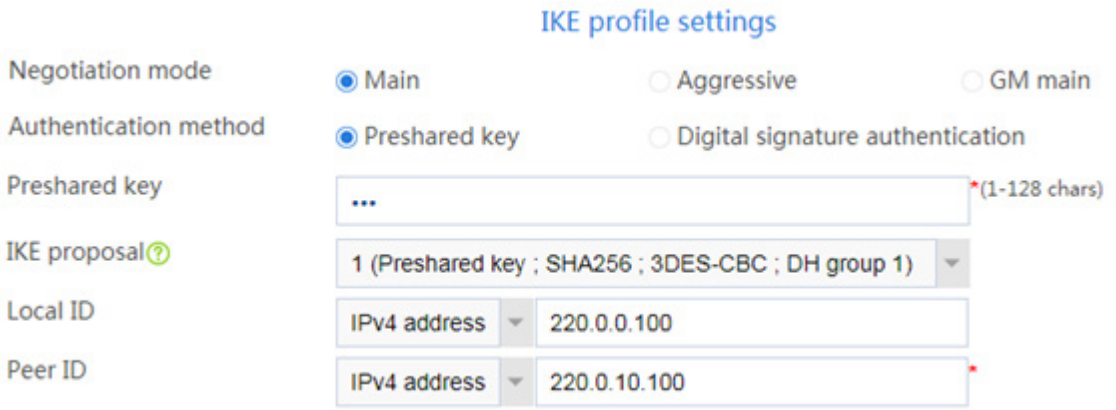
Figure 3 Basic settings



Configure the IKE profile settings as follows:

- Set the negotiation mode as **Main**.
- Set the authentication method as **Preshared key**.
- Enter the preshared key string.
- Select IKE proposal **1 (Preshared key; SHA256; 3DES-CBC; DH group 1)**.
- Set the local ID as IPv4 address 220.0.0.100.
- Set the peer ID as IPv4 address 220.0.10.100.

Figure 4 IKE profile settings

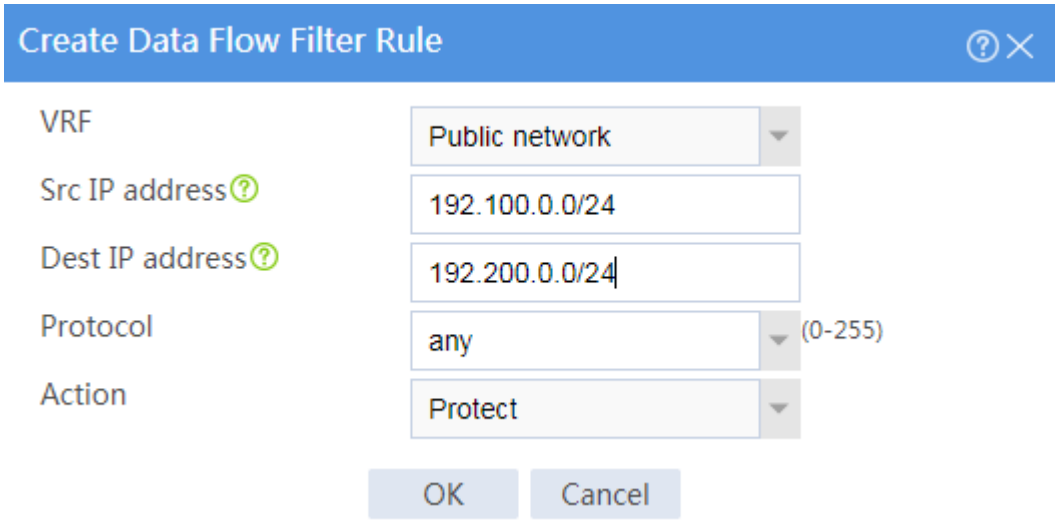


Configure the data flow filter rules as follows:

- Click **Create**.
- Set the source IP address as 192.100.0.0/24.
- Set the destination IP address as 192.200.0.0/24.

Click **OK**.

Figure 5 Creating a data flow filter rule



Set the IPsec SA triggering mode to **Traffic-based**.

Configure the IPsec advanced settings as follows:

- Select the **Tunnel** encapsulation mode.
- Select the **ESP** security protocol.

Click **OK**.

Configuring Device B

1. Assign IP addresses to interfaces and add the interfaces to security zones:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 2/0/13.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. Click the **IPv4 Address** tab, and then enter the IP address and mask length of the interface. In this example, use 220.0.10.100/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 2/0/12 to the **Trust** security zone and set its IP address to 192.200.0.2/24 in the same way you configure GE 2/0/13.

2. Configure settings for routing:

This example configures static routes.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static route to reach 220.0.0.100:

a. Set the destination IP address to 220.0.0.100.

b. Set the mask length to 24.

c. Set the next hop address to 220.0.10.2.

d. Use the default settings for other parameters.

e. Click **OK**.

On the **IPv4 Static Routing** tab, click **Create**.

Configure a static route to reach 192.100.0.2:

a. Set the destination IP address to 192.100.0.2.

b. Set the mask length to 24.

c. Set the next hop address to 220.0.10.2.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Configure security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

Configure a security policy named **trust-untrust** to permit specific traffic from the **Trust** to **Untrust** security zones:

a. Set the security policy name to **trust-untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **192.200.0.0/24**.

g. Enter destination IPv4 address **192.100.0.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-trust** to permit specific traffic from the **Untrust** to **Trust** security zones:

a. Set the security policy name to **untrust-trust**.

b. Select source zone **Untrust**.

c. Select destination zone **Trust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **192.100.0.0/24**.

g. Enter destination IPv4 address **192.200.0.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **local-untrust** to permit specific traffic from the **Local** to **Untrust** security zones:

a. Set the security policy name to **local-untrust**.

b. Select source zone **Local**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **220.0.10.100**.

g. Enter destination IPv4 address **220.0.0.100**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-local** to permit specific traffic from the **Untrust** to **Local** security zones:

a. Set the security policy name to **untrust-local**.

b. Select source zone **Untrust**.

c. Select destination zone **Local**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **220.0.0.100**.

g. Enter destination IPv4 address **220.0.10.100**.

h. Use the default settings for other parameters.

i. Click **OK**.

4. Create an IKE proposal:

On the top navigation bar, click **Network**.

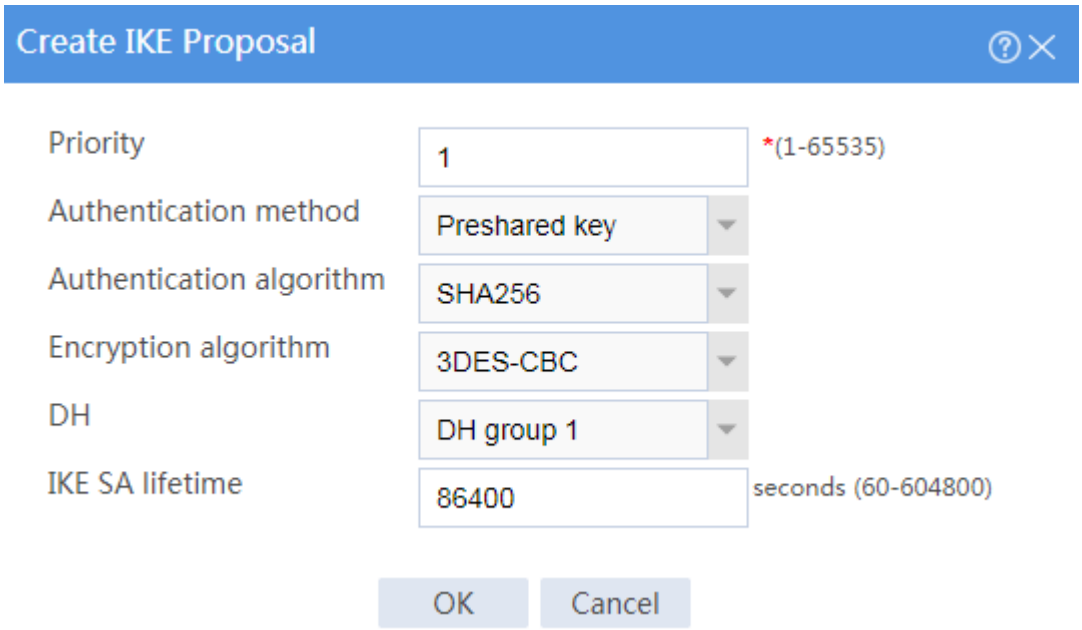
From the navigation pane, select **VPN** > **IPsec** > **IKE Proposals**.

Click **Create**.

- Set the priority to 1.
- Select the preshared key authentication method.
- Select the SHA256 authentication algorithm.
- Select the 3DES-CBC encryption algorithm.
- Use the default settings for other parameters.

Click **OK**.

Figure 6 Creating an IKE proposal



5. Configure the IPsec policy:

On the top navigation bar, click **Network**.

From the navigation pane, select **VPN** > **IPsec** > **IPsec Policies**.

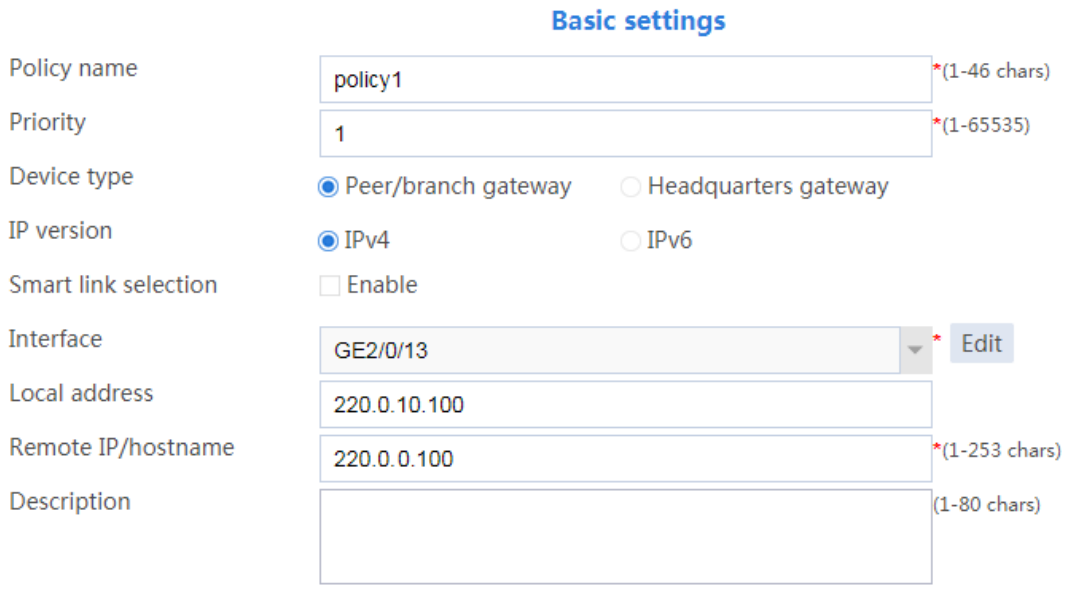
Click **Create**.

Configure the basic settings as follows:

- Set the policy name to **policy1**.

- Set the priority to 1.
- Set the device type to **Peer/branch gateway**.
- Set the IP version to **IPv4**.
- Select interface GE2/0/13.
- Configure the local address as 220.0.10.100.
- Configure the remote address/host name as 220.0.0.100.

Figure 7 Basic settings

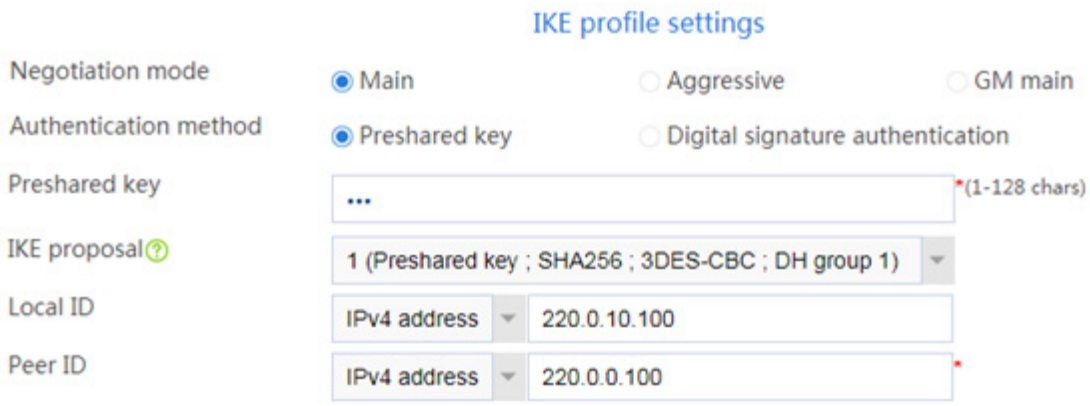


Configure the IKE profile settings as follows:

- Set the negotiation mode as **Main**.
- Set the authentication method as **Preshared key**.
- Enter the preshared key string.
- Select IKE proposal **1 (Preshared key; SHA256; 3DES-CBC; DH group 1)**.
- Set the local ID as IPv4 address 220.0.10.100.

- Set the peer ID as IPv4 address 220.0.0.100.

Figure 8 IKE profile settings

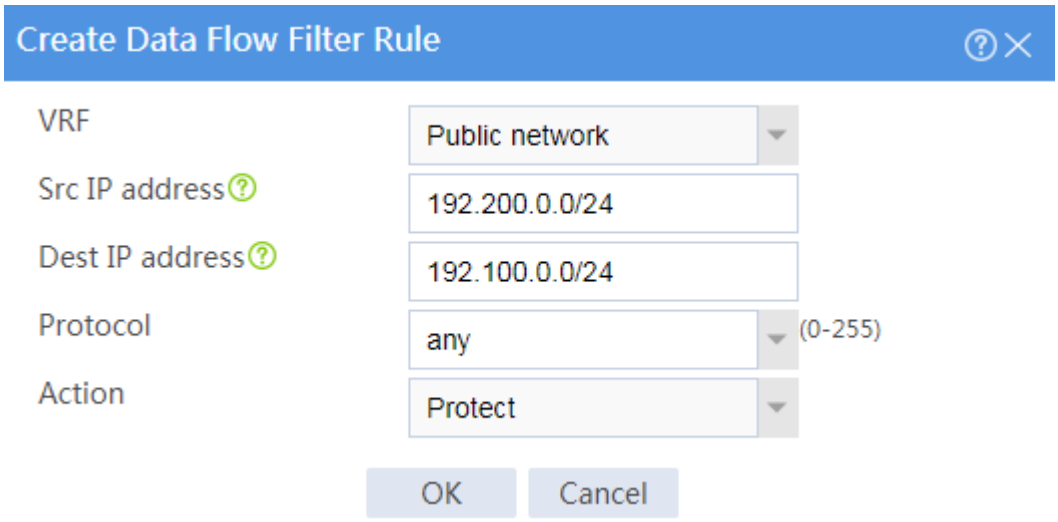


Configure the data flow filter rules as follows:

- Click **Create**.
- Set the source IP address as 192.200.0.0/24.
- Set the destination IP address as 192.100.0.0/24.

Click **OK**.

Figure 9 Creating a data flow filter rule



Set the IPsec SA triggering mode to **Traffic-based**.

Configure the IPsec advanced settings as follows:

- Select the **Tunnel** encapsulation mode.
- Select the **ESP** security protocol.

Click **OK**.

Verifying the configuration

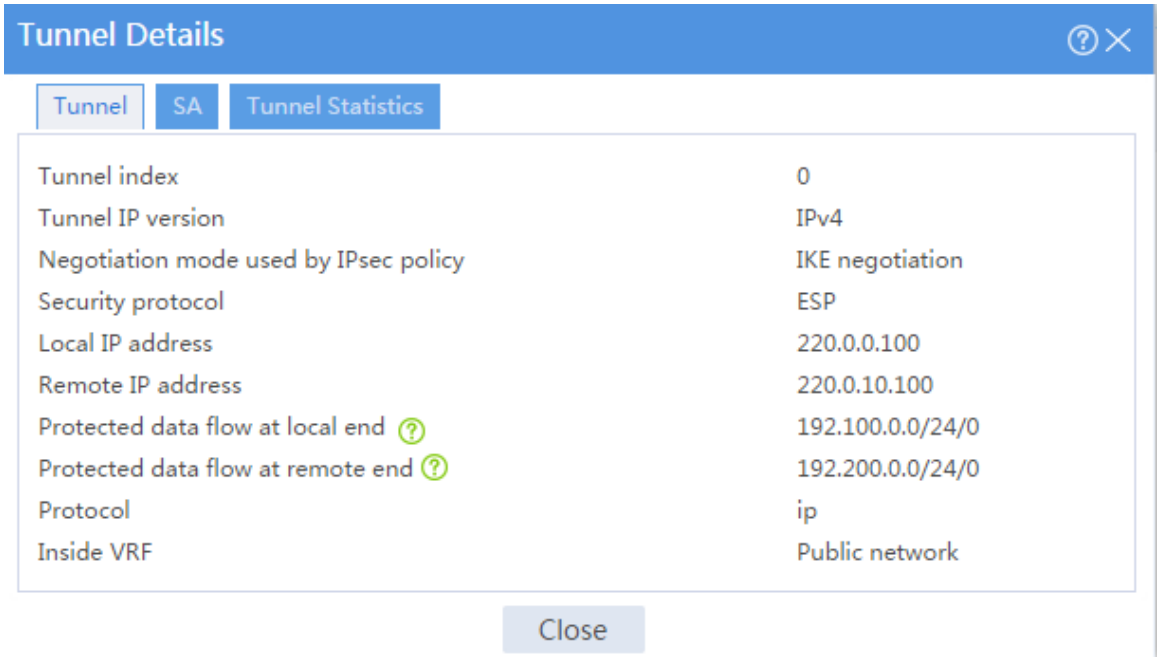
1. Verify that Device A and Device B can communicate with each other.
2. On Device A, display IPsec tunnel information:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **VPN** > **IPsec** > **IPsec Tunnels**. The established IPsec tunnel is displayed.

Click the **Details** icon for the IPsec tunnel. The **Tunnel Details** page displays tunnel information, SA information, and tunnel statistics.

Figure 10 Details of the IPsec tunnel on Device A



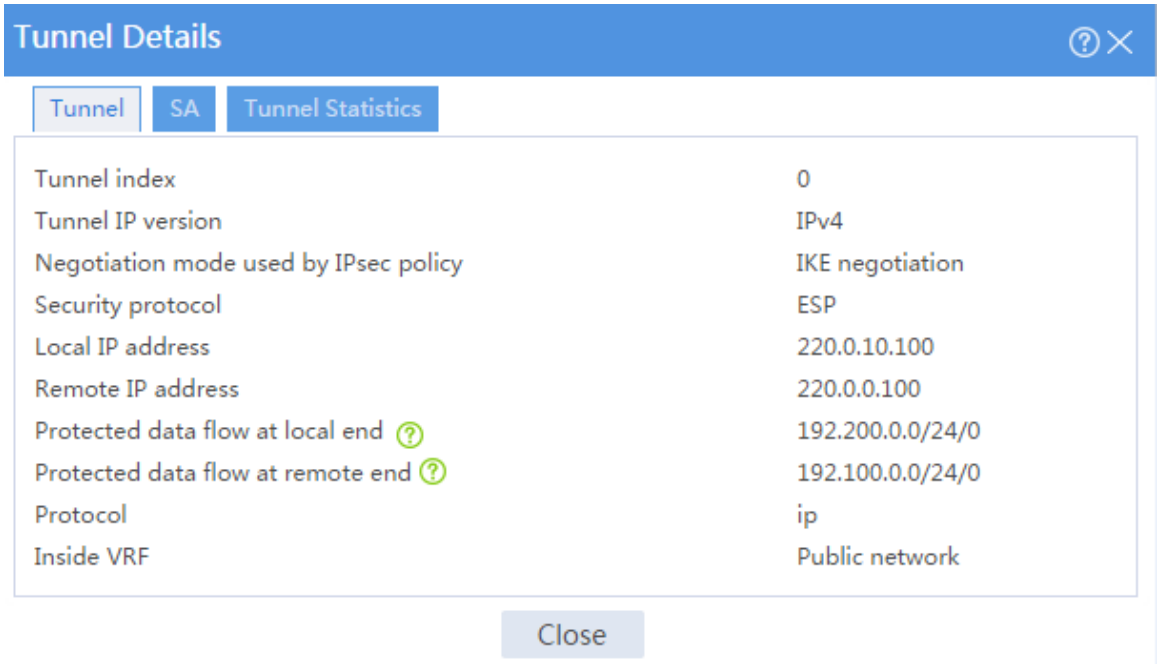
3. On Device B, display IPsec tunnel information:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **VPN** > **IPsec** > **IPsec Tunnels**. The established IPsec tunnel is displayed.

   # Click the **Details** icon for the IPsec tunnel. The **Tunnel Details** page displays tunnel information, SA information, and tunnel statistics.

Figure 11 Details of the IPsec tunnel on Device B



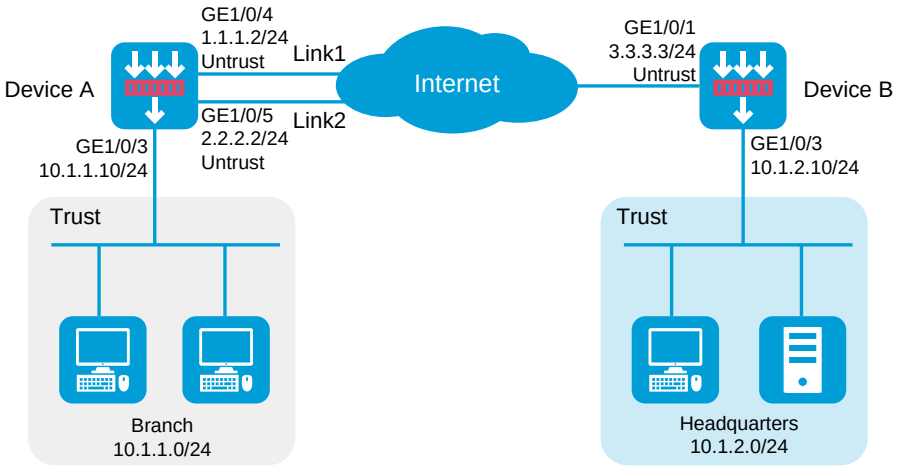
Example: Configuring IPsec smart link selection

Network configuration

As shown in Figure 12, Device A is the IPsec gateway of the branch. Device B is the IPsec gateway of the headquarters. Configure IPsec smart link selection so the branch can establish an IPsec tunnel to the headquarters over link 1 or link 2, whichever has a better link quality.

- Device A first uses link 1 to establish the IPsec tunnel.
- When link 1 suffers high packet loss ratio or delay, Device A automatically switches traffic to the IPsec tunnel established based on link 2.

Figure 12 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/4.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. Click the **IPv4 Address** tab. Enter the IP address and mask length of the interface. In this example, use 1.1.1.2/24. Specify the gateway address for the interface as 1.1.1.3.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/5 to the **Trust** security zone and set its IP address to 2.2.2.2/24 and its gateway address to 2.2.2.3 in the same way you configure GE 1/0/4.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 10.1.1.10/24 in the same way you configure GE 1/0/4.

2. Configure security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

Configure a security policy named **trust-untrust** to permit specific traffic from the **Trust** to **Untrust** security zones:

a. Set the security policy name to **trust-untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **10.1.1.0/24**.

g. Enter destination IPv4 address **10.1.2.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-trust** to permit specific traffic from the **Untrust** to **Trust** security zones:

a. Set the security policy name to **untrust-trust**.

b. Select source zone **Untrust**.

c. Select destination zone **Trust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **10.1.2.0/24**.

g. Enter destination IPv4 address **10.1.1.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **local-untrust** to permit specific traffic from the **Local** to **Untrust** security zones:

a. Set the security policy name to **local-untrust**.

b. Select source zone **Local**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **1.1.1.2,2.2.2.2**.

g. Enter destination IPv4 address **3.3.3.3**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-local** to permit specific traffic from the **Untrust** to **Local** security zones:

a. Set the security policy name to **untrust-local**.

b. Select source zone **Untrust**.

c. Select destination zone **Local**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **3.3.3.3**.

g. Enter destination IPv4 address **1.1.1.2,2.2.2.2**.

h. Use the default settings for other parameters.

i. Click **OK**.

3. Create an IKE proposal:

On the top navigation bar, click **Network**.

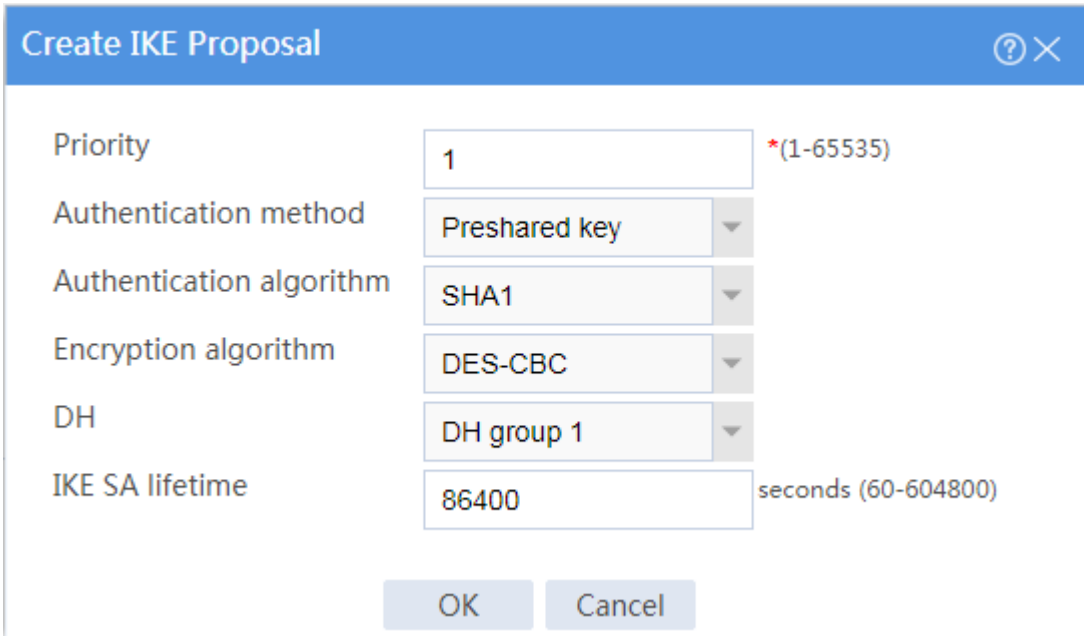
From the navigation pane, select **VPN** > **IPsec** > **IKE Proposals**.

Click **Create**.

- Set the priority to 1.
- Select the preshared key authentication method.
- Select the SHA1 authentication algorithm.
- Select the DES-CBC encryption algorithm.
- Use the default settings for other parameters.

Click **OK**.

Figure 13 Creating an IKE proposal



4. Configure the IPsec policy:

   # On the top navigation bar, click **Network**.

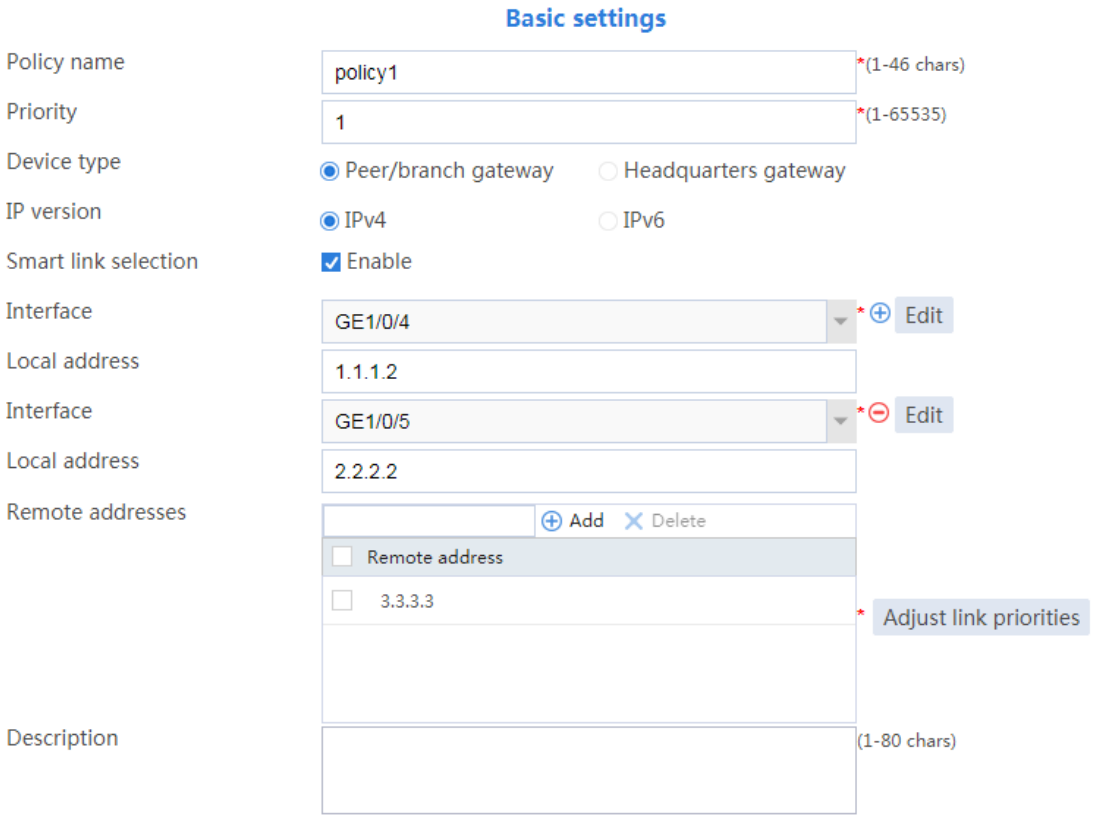
   # From the navigation pane, select **VPN** > **IPsec** > **IPsec Policies**.

   # Click **Create**.

   # Configure the basic settings as follows:

   - Set the policy name to **policy1**.
   - Set the priority to 1.
   - Set the device type to **Peer/branch gateway**.
   - Set the IP version to **IPv4**.
   - Select interface GE1/0/4 and GE1/0/5.

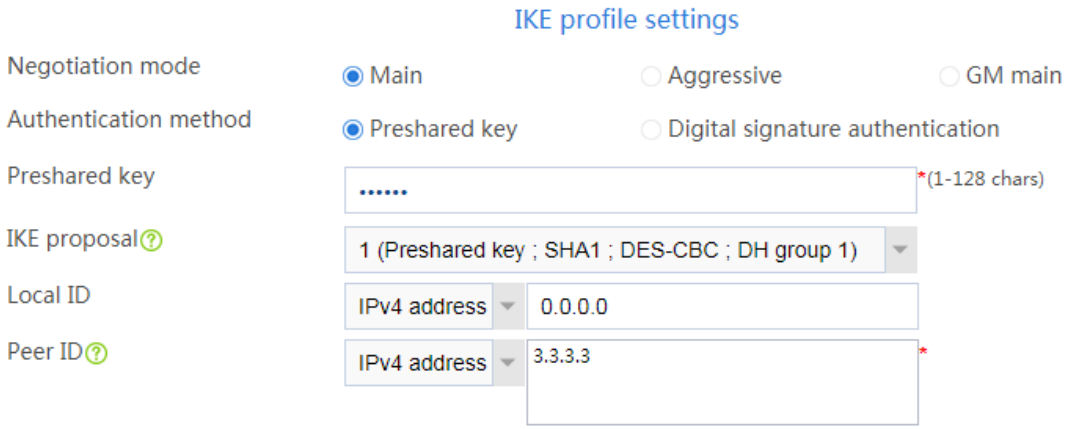
Figure 14 Basic settings



Configure the IKE profile settings as follows:

- Set the negotiation mode as **Main**.
- Set the authentication method as **Preshared key**.
- Enter the preshared key string.
- Select IKE proposal **1 (Preshared key; SHA1; DES-CBC; DH group 1)**.
- Set the local ID as IPv4 address 0.0.0.0.
- Set the peer ID as IPv4 address 3.3.3.3.

Figure 15 IKE profile settings



Configure the data flow filter rules as follows:

- Click **Create**.
- Set the source IP address as 10.1.1.0/24.
- Set the destination IP address as 10.1.2.0/24.

Click **OK**.

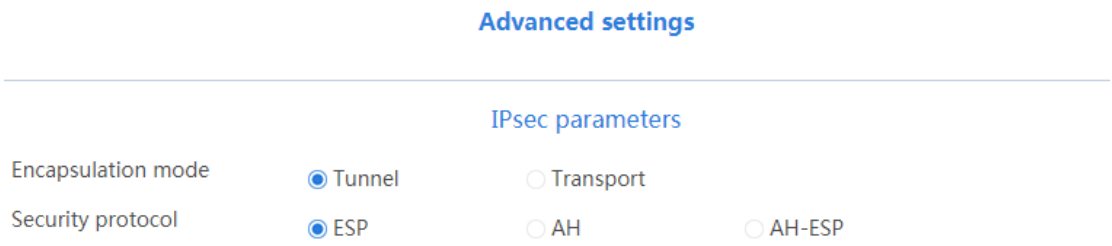
Figure 16 Creating a data flow filter rule

Configure the IPsec advanced settings as follows:

- Select the **Tunnel** encapsulation mode.
- Select the **ESP** security protocol.

Click **OK**.

Figure 17 Advanced settings



Configuring Device B

1. Assign IP addresses to interfaces and add the interfaces to security zones:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. Click the **IPv4 Address** tab. Enter the IP address and mask length of the interface. In this example, use 3.3.3.3/24. Specify the gateway address for the interface as 3.3.3.4.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 10.1.2.10/24 in the same way you configure GE 1/0/1.

2. Configure security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

Configure a security policy named **trust-untrust** to permit specific traffic from the **Trust** to **Untrust** security zones:

a. Set the security policy name to **trust-untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **10.1.2.0/24**.

g. Enter destination IPv4 address **10.1.1.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-trust** to permit specific traffic from the **Untrust** to **Trust** security zones:

a. Set the security policy name to **untrust-trust**.

b. Select source zone **Untrust**.

c. Select destination zone **Trust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **10.1.1.0/24**.

g. Enter destination IPv4 address **10.1.2.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **local-untrust** to permit specific traffic from the **Local** to **Untrust** security zones:

a. Set the security policy name to **local-untrust**.

b. Select source zone **Local**.

c. Select destination zone **Untrust**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 address **3.3.3.3**.

g. Enter destination IPv4 addresses **1.1.1.2,2.2.2.2**.

h. Use the default settings for other parameters.

i. Click **OK**.

On the **Security Policies** page, click **Create**.

Configure a security policy named **untrust-local** to permit specific traffic from the **Untrust** to **Local** security zones:

a. Set the security policy name to **untrust-local**.

b. Select source zone **Untrust**.

c. Select destination zone **Local**.

d. Select **IPv4** as the type.

e. Select action **Permit**.

f. Enter source IPv4 addresses **1.1.1.2,2.2.2.2**.

g. Enter destination IPv4 address **3.3.3.3**.

h. Use the default settings for other parameters.

i. Click **OK**.

3. Create an IKE proposal:

On the top navigation bar, click **Network**.

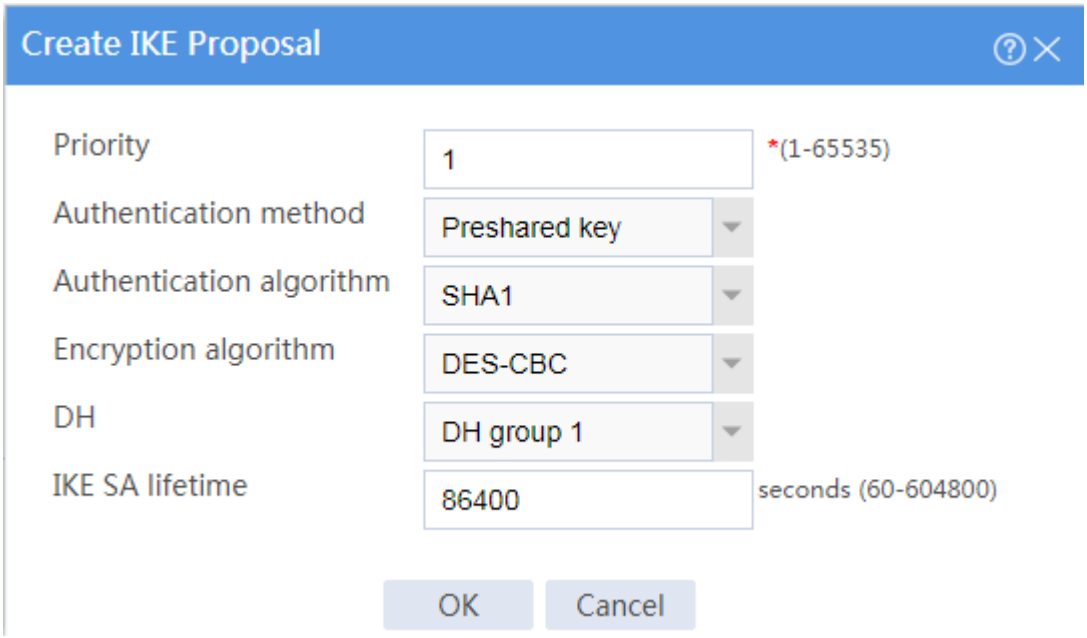
From the navigation pane, select **VPN** > **IPsec** > **IKE Proposals**.

Click **Create**.

- Set the priority to 1.
- Select the preshared key authentication method.
- Select the SHA1 authentication algorithm.
- Select the DES-CBC encryption algorithm.
- Use the default settings for other parameters.

Click **OK**.

Figure 18 Creating an IKE proposal



4. Configure the IPsec policy:

   # On the top navigation bar, click **Network**.

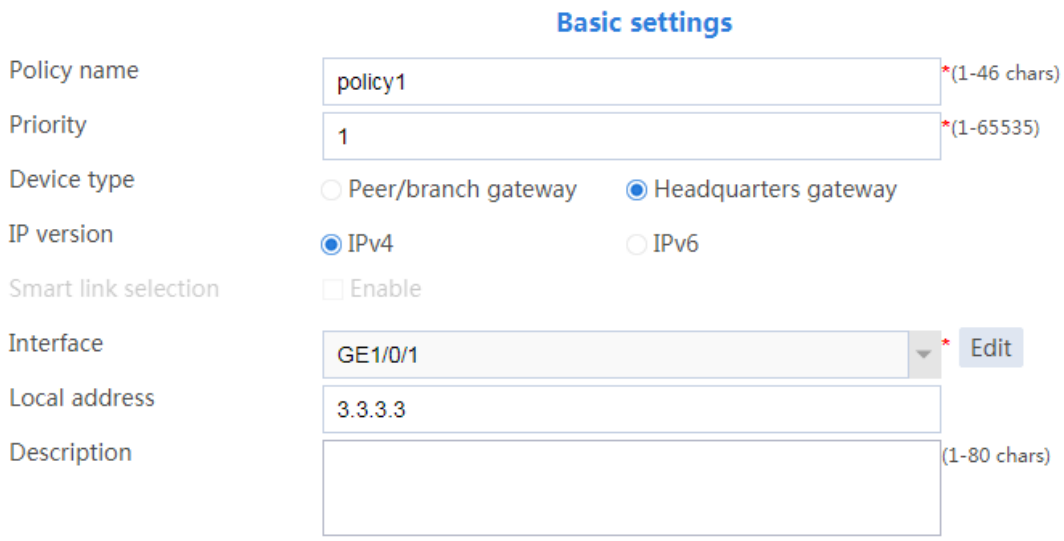
   # From the navigation pane, select **VPN** > **IPsec** > **IPsec Policies**.

   # Click **Create**.

   # Configure the basic settings as follows:

   - Set the policy name to **policy1**.
   - Set the priority to 1.
   - Set the device type to **Headquarters gateway**.
   - Set the IP version to **IPv4**.
   - Select interface GE1/0/1.

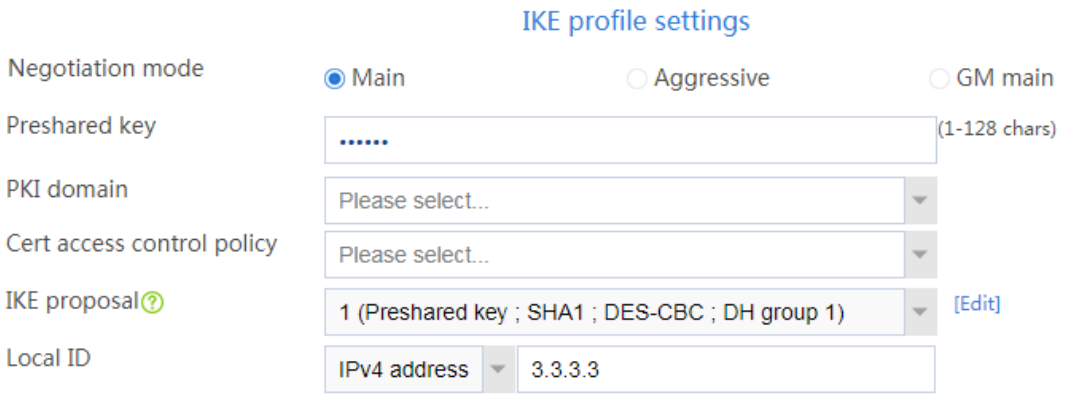
Figure 19 Basic settings



Configure the IKE profile settings as follows:

- Set the negotiation mode as **Main**.
- Set the authentication method as **Preshared key**.
- Enter the preshared key string.
- Select IKE proposal **1 (Preshared key; SHA1; DES-CBC; DH group 1)**.
- Set the local ID as IPv4 address 3.3.3.3.

Figure 20 IKE profile settings

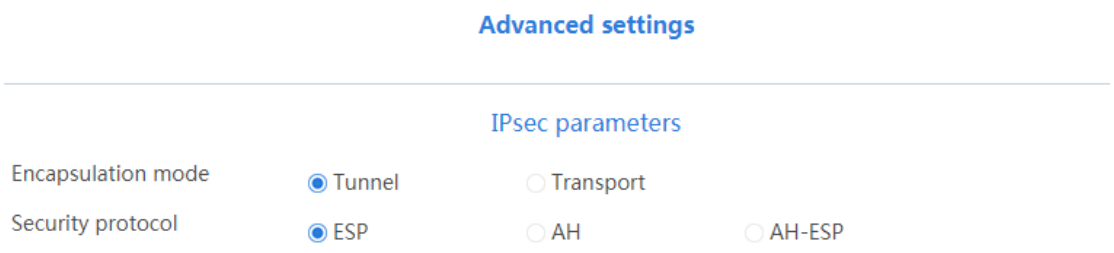


Configure the IPsec advanced settings as follows:

- Select the **Tunnel** encapsulation mode.
- Select the **ESP** security protocol.

Click **OK**.

Figure 21 Advanced settings



Verifying the configuration

1. Verify that Device A and Device B can communicate with each other.

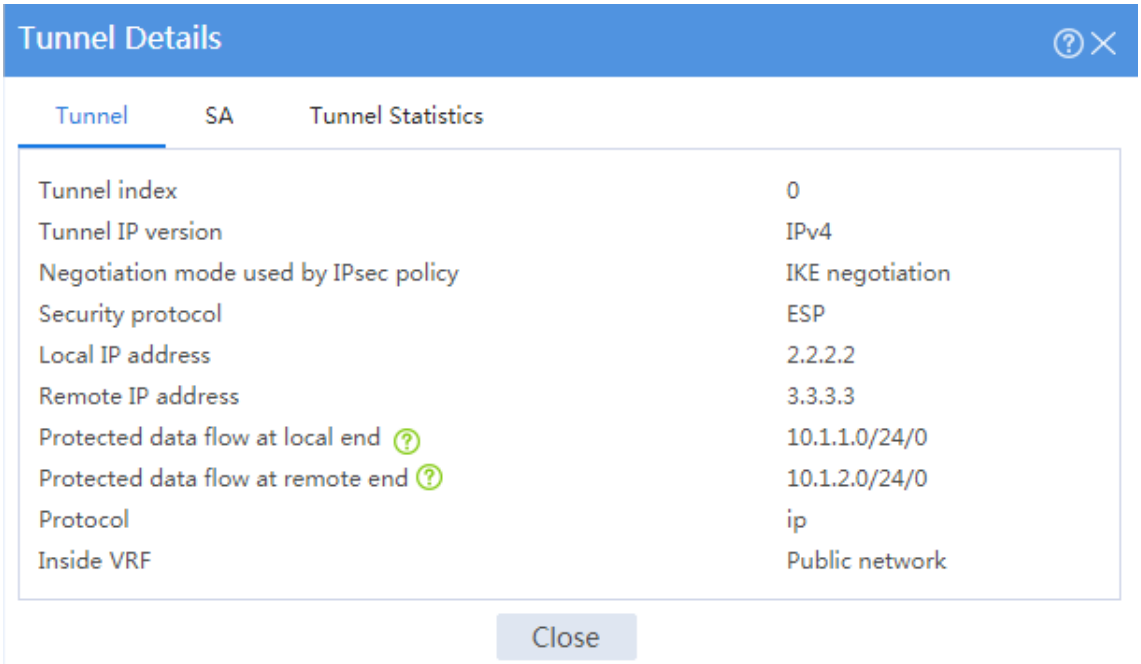
2. On Device A, display IPsec tunnel information:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **VPN** > **IPsec** > **IPsec Tunnels**. The established IPsec tunnel is displayed.

   # Click the **Details** icon for the IPsec tunnel. The **Tunnel Details** page displays tunnel information, SA information, and tunnel statistics.

Figure 22 Details of the IPsec tunnel on Device A



3. On Device A, automatically or manually switch links:

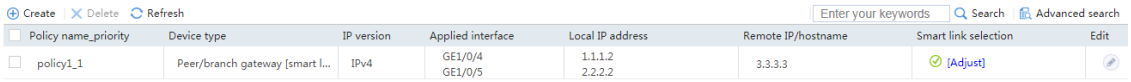
   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **VPN** > **IPsec** > **IPsec Policies**. In this example, the created IPsec policy **policy1_1** is displayed, and IPsec smart link selection is enabled in the policy.

   IPsec smart link selection enables the branch gateway to monitor the real-time packet loss ratio and delay of the active link over which the IPsec tunnel is established. The branch

gateway can dynamically select a link with desired transmission quality to establish the IPsec tunnel to the headquarters.

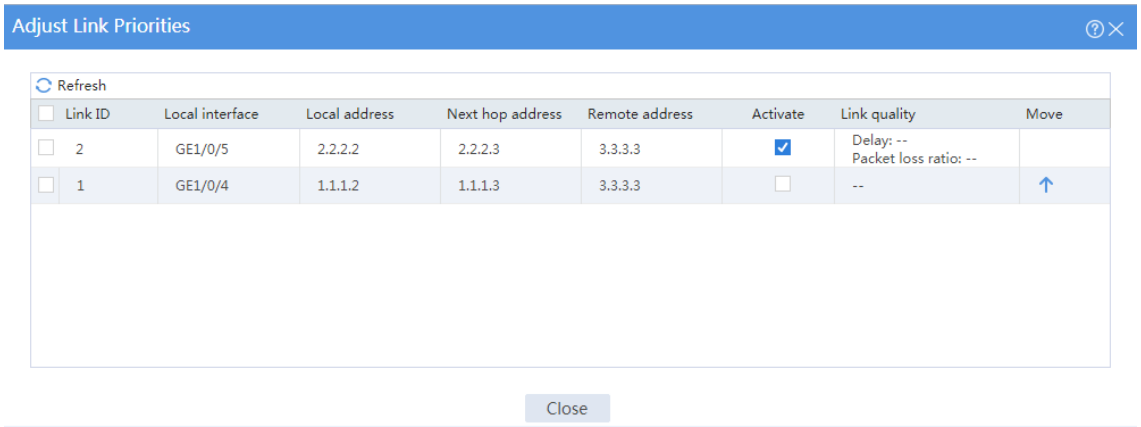
Figure 23 IPsec policies



Click **Adjust** in the **Smart link selection** column to open the **Adjust Link Priorities** page.

Select the check box in the **Activate** column of a link to manually activate the link.

Figure 24 Adjust link priorities



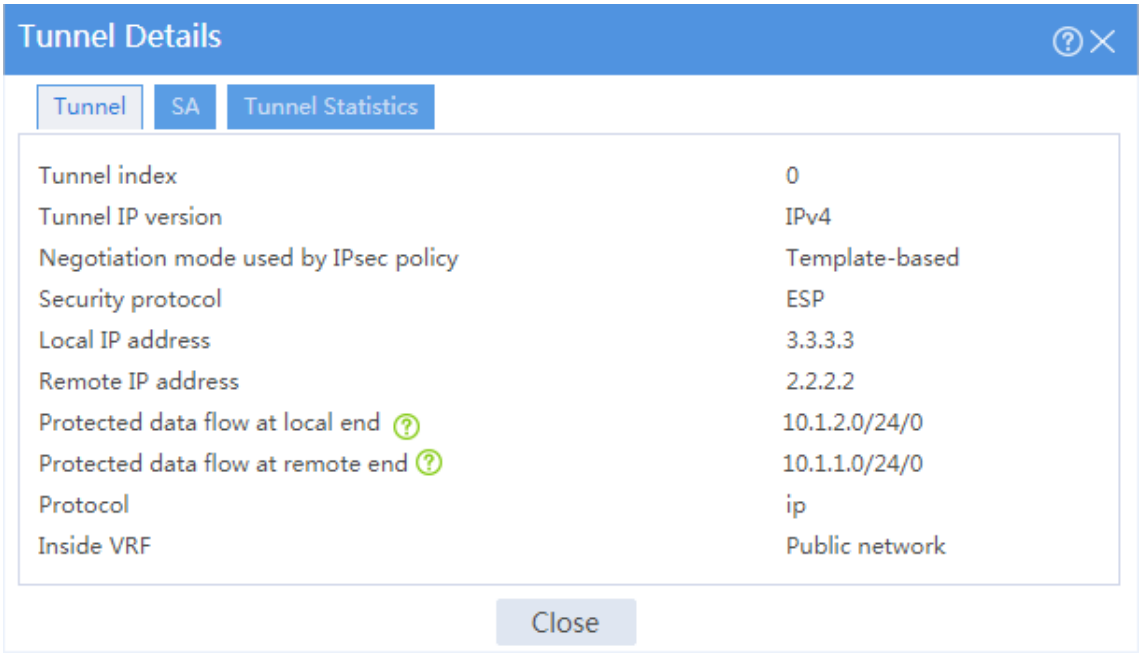
4. On Device B, display IPsec tunnel information:

On the top navigation bar, click **Network**.

From the navigation pane, select **VPN** > **IPsec** > **IPsec Tunnels**. The established IPsec tunnel is displayed.

Click the **Details** icon for the IPsec tunnel. The **Tunnel Details** page displays tunnel information, SA information, and tunnel statistics.

Figure 25 Details of the IPsec tunnel on Device B



SSL VPN IP access configuration examples

Contents

Introduction

The following information provides SSL VPN IP access configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedure and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of SSL VPN.

Example: Configuring IP access with RADIUS authentication

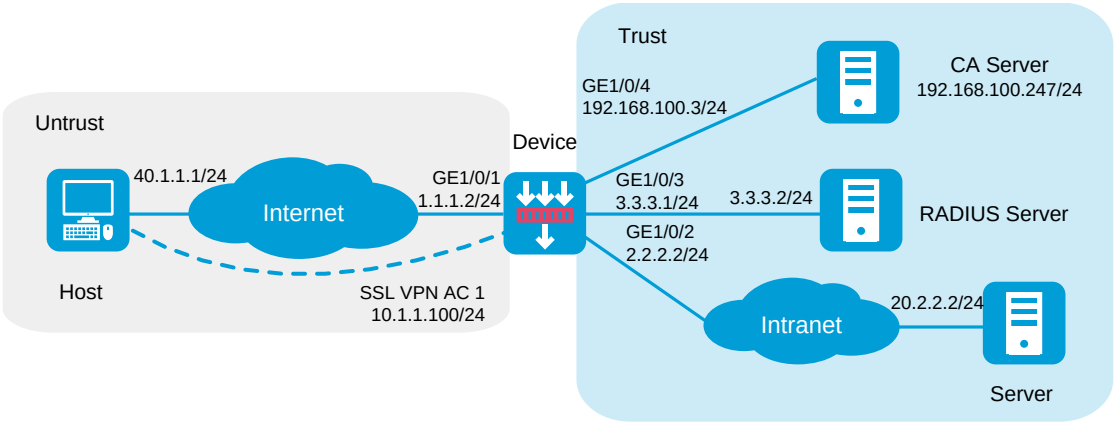
Network configuration

As shown in Figure 1, the device acts as an SSL VPN gateway that connects the public network and the private network. On the private network, a Windows Server 2008 R2 CA server and a RADIUS server that runs IMC PLAT 7.3 (E0504) are deployed. Users need secure access to the internal server (20.2.2.2/24) in IP access mode.

Perform the following tasks:

- Request an SSL server certificate for the device from the CA server.
- Configure the device to require that users pass certificate authentication for IP access.
- Configure the device to use the RADIUS server to perform remote authentication and authorization for IP access users.
- Configure the SSL VPN IP access service on the device to allow users to access the internal server in IP access mode.

Figure 1 Network diagram (RADIUS authentication)



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

- The IP address pool configured for client address allocation must meet the following requirements:
  - The address range of the address pool cannot be on the same subnet as the IP address used on the client host.
  - The IP addresses in the address pool do not conflict with the IP addresses used on the device.
  - The address range of the address pool cannot be on the same subnet as the IP address of the internal server.
- The SSL VPN AC interface must be added to the correct security zone (**Untrust**, in this example).

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click the **Network** tab.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

   # Add GE 1/0/3 to the **Trust** security zone and set its IP address to 3.3.3.1/24 in the same way you configure GE 1/0/1.

   # Add GE 1/0/4 to the **Trust** security zone and set its IP address to 192.168.100.3/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

   This example configures static routes.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static IPv4 route to reach 40.1.1.1:

   a. Enter destination IP address **40.1.1.1**.

   b. Enter mask length **24**.

   c. Enter next hop address **1.1.1.3**.

   d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 20.2.2.2:

a. Enter destination IP address **20.2.2.2**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.

- Select source IPv4 addresses **2.2.2.2**, **3.3.3.1**, and **192.168.100.3**.
- Select destination IPv4 addresses **20.2.2.2**, **3.3.3.2**, and **192.168.100.247**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **untrust-trust** to permit the specified traffic from the **Untrust** to **Trust** security zones:

- Enter policy name **untrust-trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.0/24**.
- Select destination IPv4 address **20.2.2.2/24**.
- Use the default settings for other parameters.

Click **OK**.

4. Request a server certificate for the device:

a. Create a certificate subject:

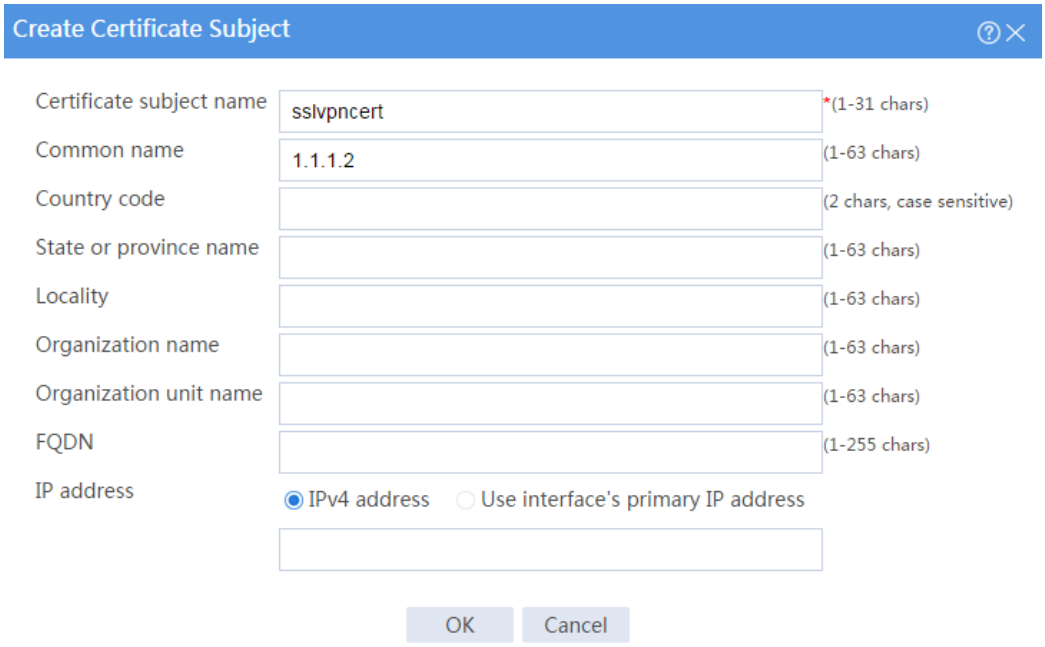
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate Subject**.

Click **Create**.

Create a certificate subject as shown in Figure 2, and the click **OK**.

Figure 2 Creating a certificate subject

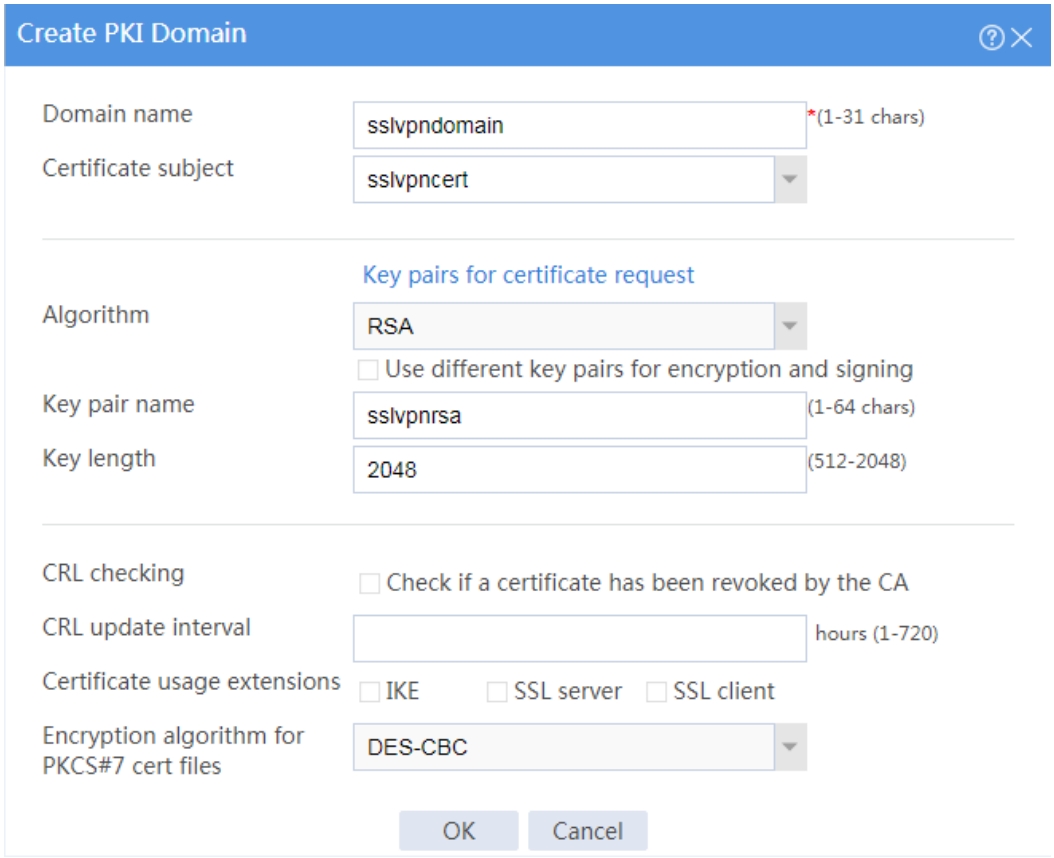


b. Create a PKI domain:

On the **Certificate** page, click **Create PKI domain**.

Create a PKI domain as shown in Figure 3, and then click **OK**.

Figure 3 Creating a PKI domain

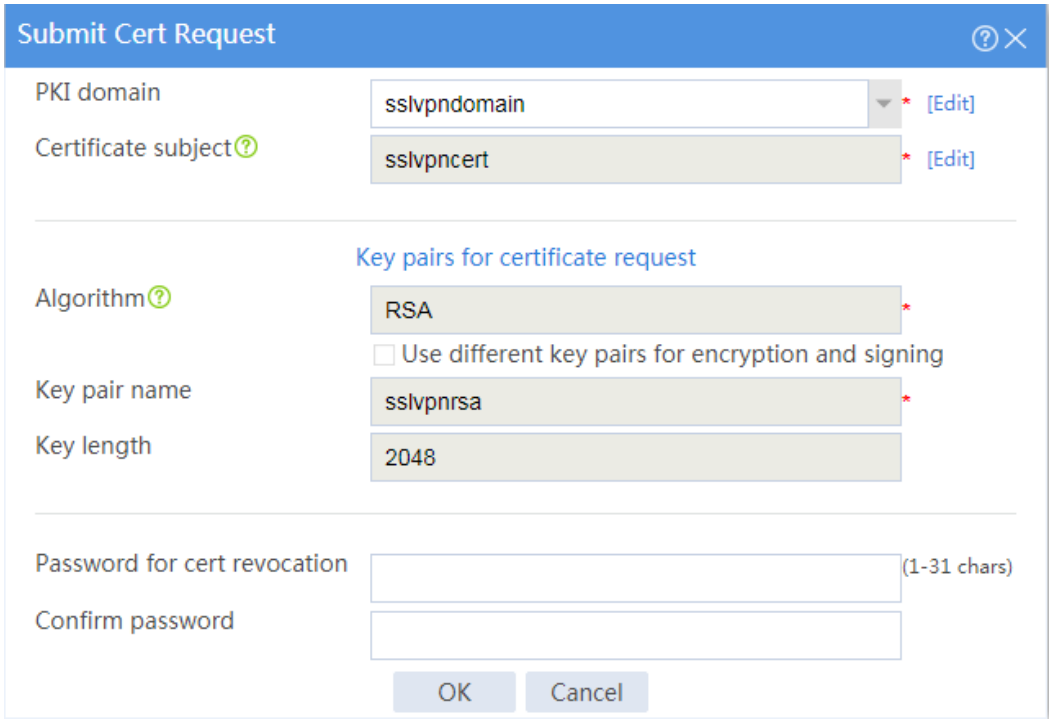


c. Create a certificate request:

On the **Certificate** page, click **Submit Cert Request**.

Configure the certificate request settings as shown in Figure 4.

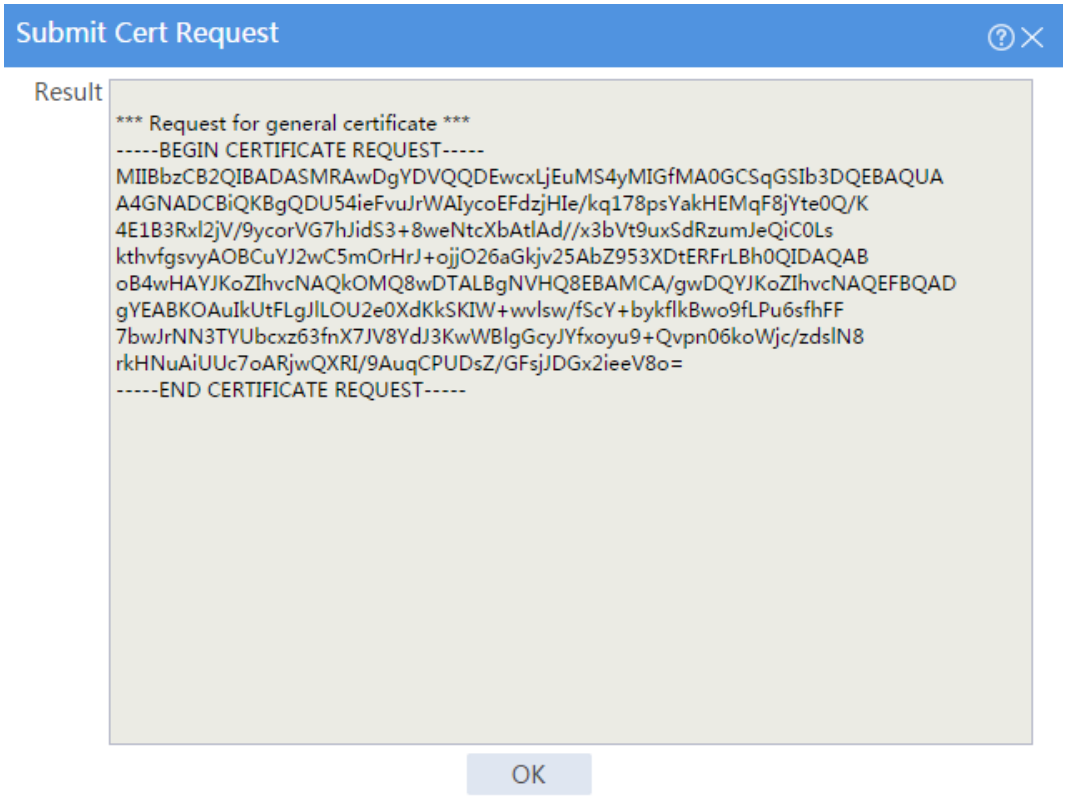
Figure 4 Creating a certificate request



Click **OK**.

The certificate request content will be displayed, as shown in Figure 5.

Figure 5 Certificate request content



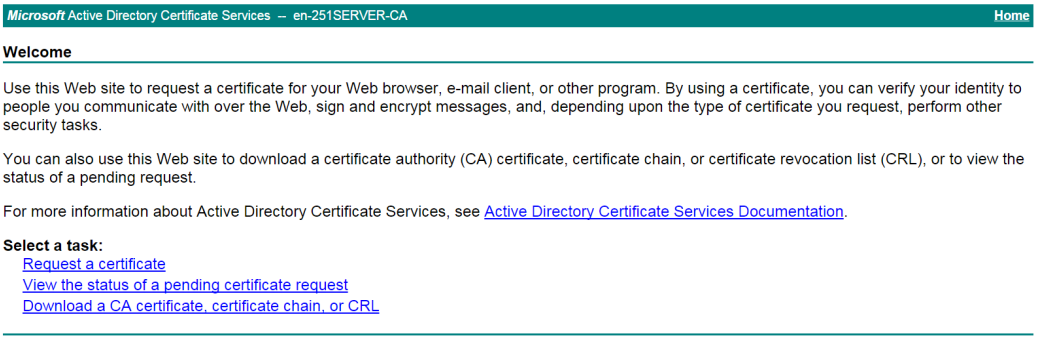
Copy the certificate request content and click **OK**.

d. Request a server certificate from the CA:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 6, click **Request a certificate**.

Figure 6 Certificate service home page

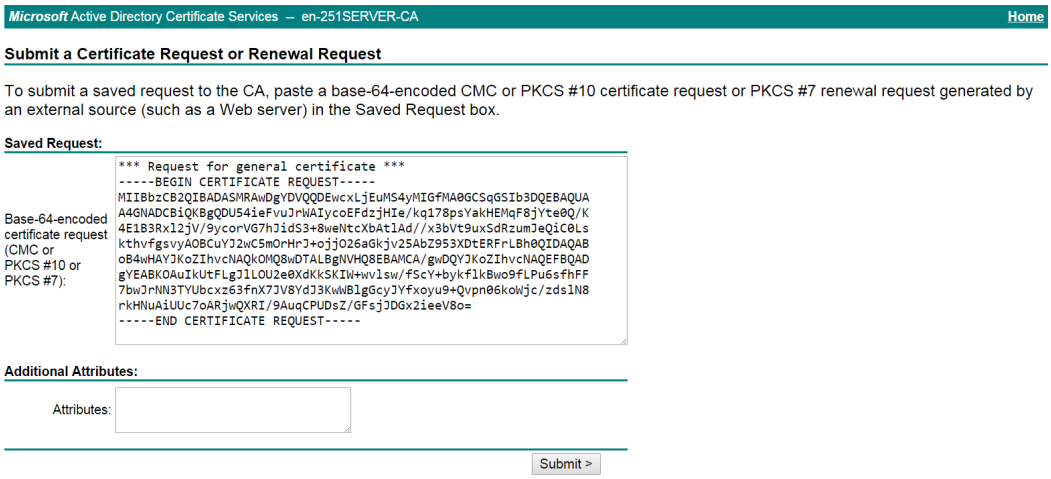


On the **Request a Certificate** page shown in Figure 7, click **advanced certificate request**.

Figure 7 Request a Certificate page

Paste the previously copied certificate request content in the **Base-64-encoded certificate request CMC or PKCS # 10 or PKCS # 7)** field, as shown in Figure 8.

Figure 8 Pasting the certificate request content

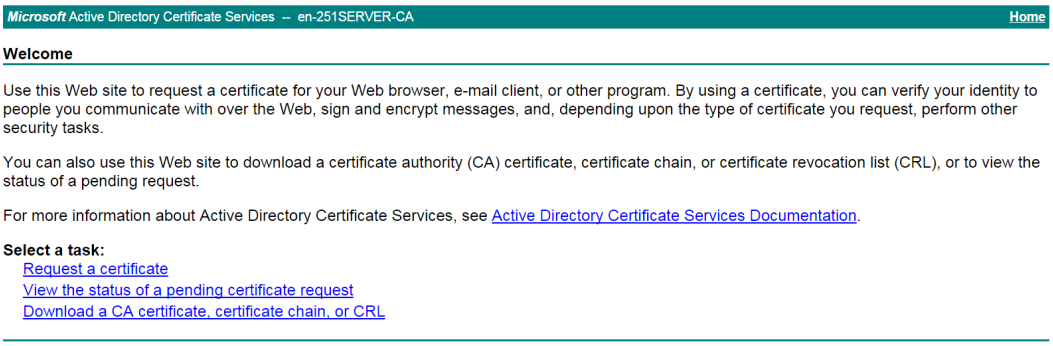


Click **Submit**.

After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 9, click **View the status of a pending certificate request**.

Figure 9 Certificate service home page



Select the certificate request you want to view.

Figure 10 View the Status of a Pending Certificate Request page

The **Certificate Issued** page opens, indicating that the requested server certificate has been issued, as shown in Figure 11.

Figure 11 Certificate Issued page

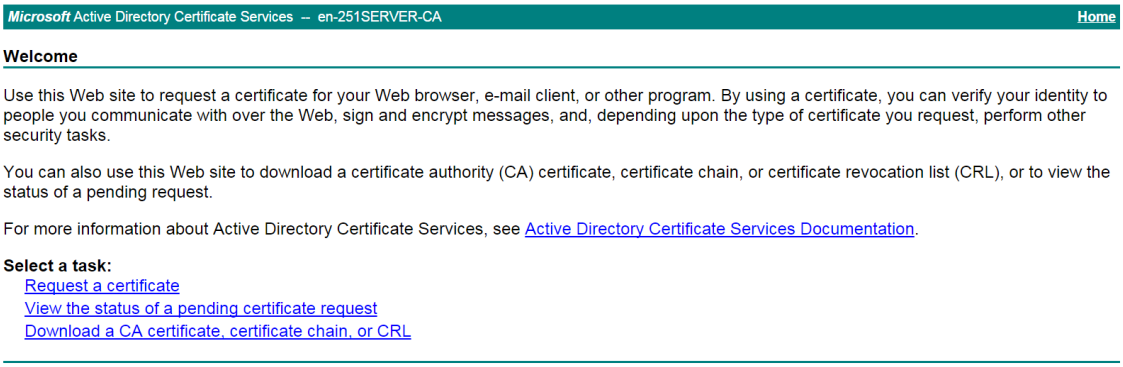
Click **Download certificate** to download the server certificate and save it locally.

5. Download the CA certificate:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

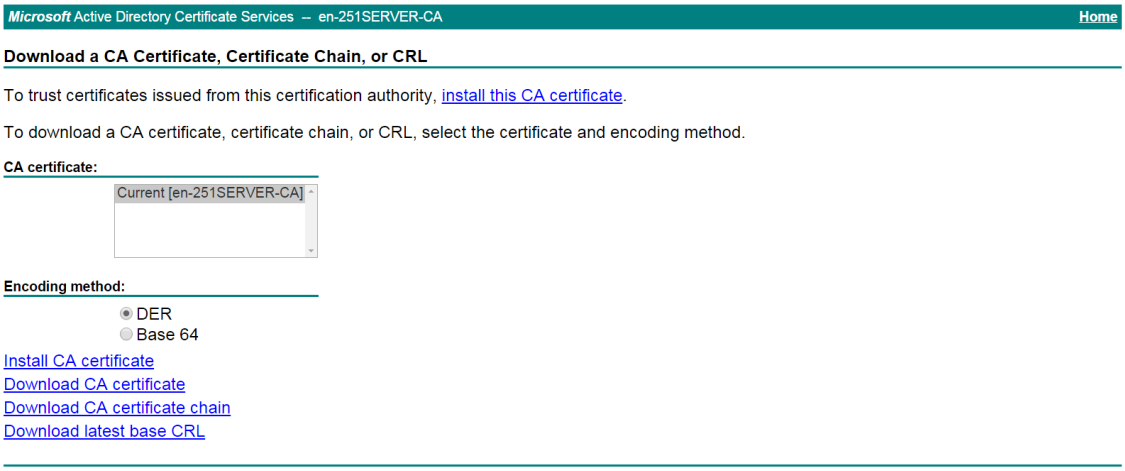
On the certificate service home page shown in Figure 12, click **Download a CA certificate, certificate chain, or CRL**.

Figure 12 Certificate service home page



On the **Download a CA certificate, certificate chain, or CRL** page shown in Figure 13, click **Download CA certificate**.

Figure 13 Download a CA certificate, certificate chain, or CRL page



Save the downloaded CA certificate locally.

6. Import the CA certificate and server certificate to the PKI domain:

a. Import the CA certificate:

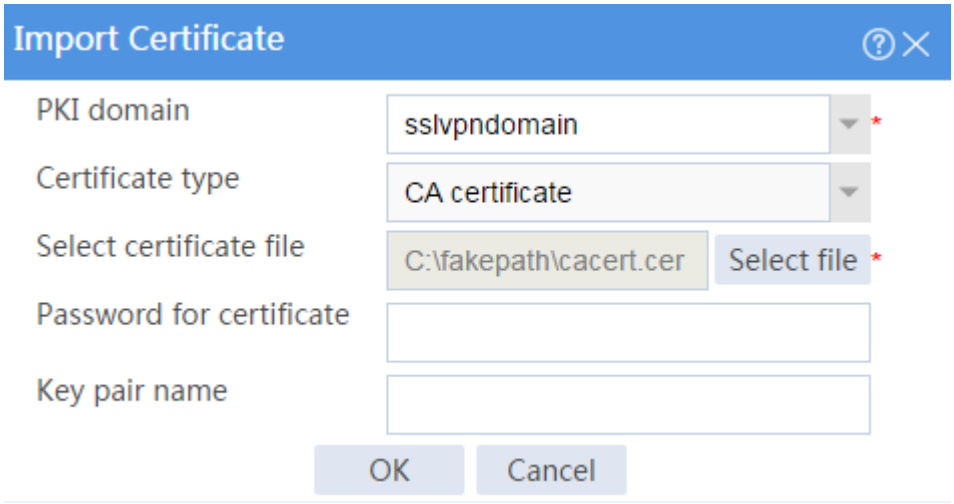
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate**.

Click **Import certificate**.

Import the locally saved CA certificate, as shown in Figure 14, and then click **OK**.

Figure 14 Importing the CA certificate

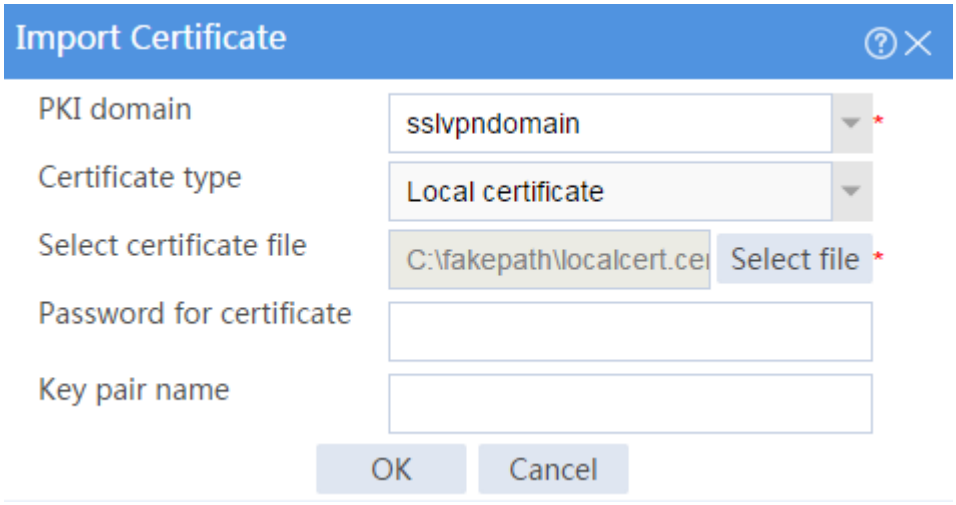


b. Import the server certificate:

On the **Certificate** page, click **Import certificate**.

Import the locally saved server certificate, as shown in Figure 15, and then click **OK**.

Figure 15 Importing the server certificate



7. Configure an SSL server policy:

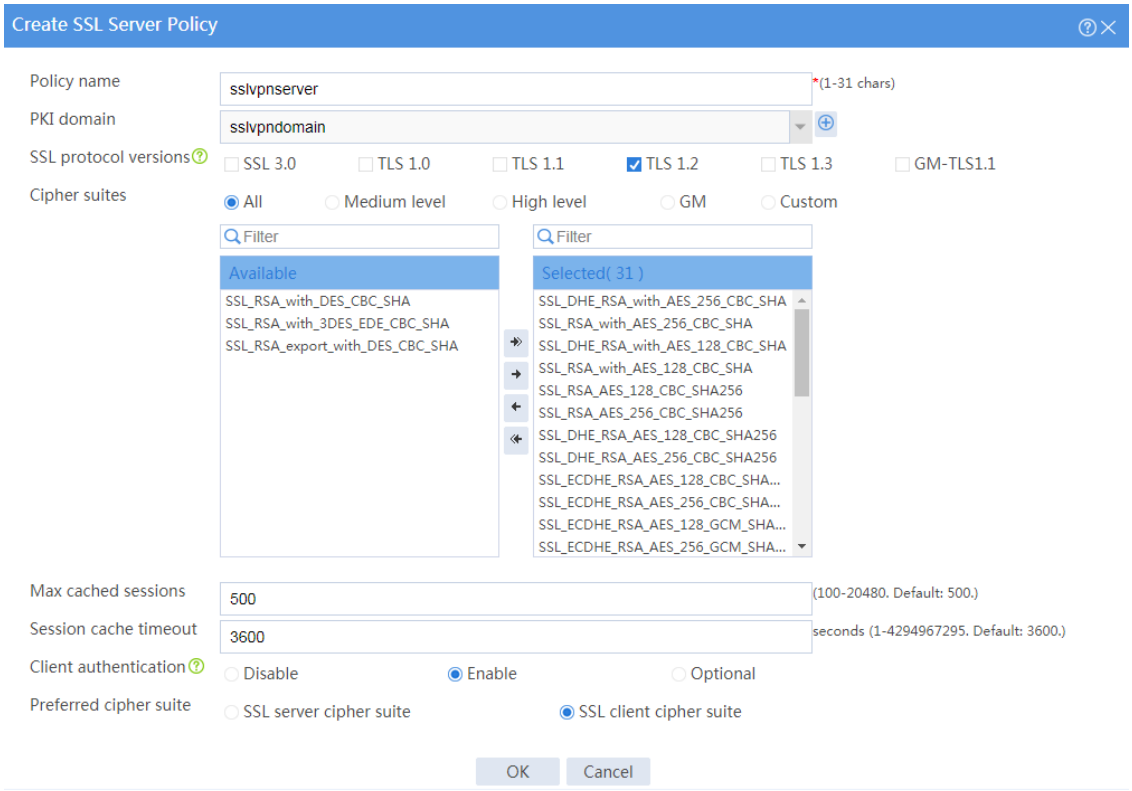
On the top navigation bar, click **Objects**.

From the navigation pane, select **SSL** > **SSL Server Policies**.

Click **Create**.

Configure an SSL server policy as shown in Figure 16, and then click **OK**.

Figure 16 Creating an SSL server policy



8. Configure an SSL client policy:

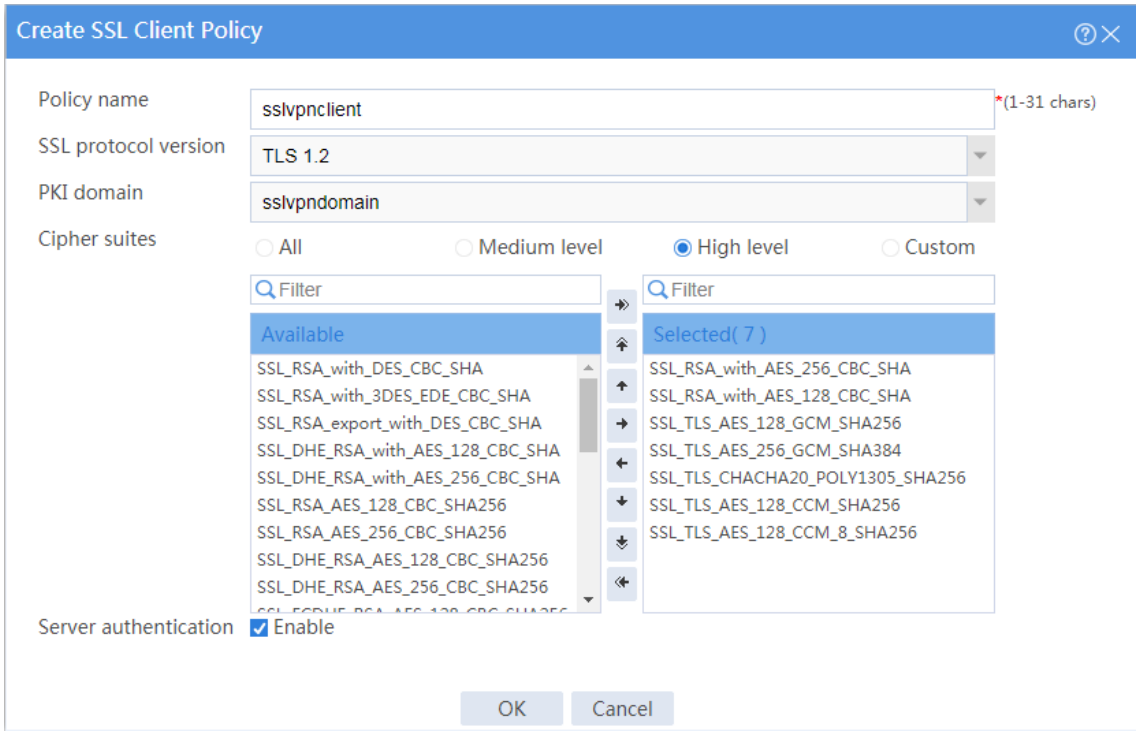
   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **SSL** > **SSL Client Policies**.

   # Click **Create**.

   # Configure an SSL client policy as shown in Figure 17, and then click **OK**.

Figure 17 Creating an SSL client policy



9. Configure a RADIUS scheme:

On the top navigation bar, click **Objects**.

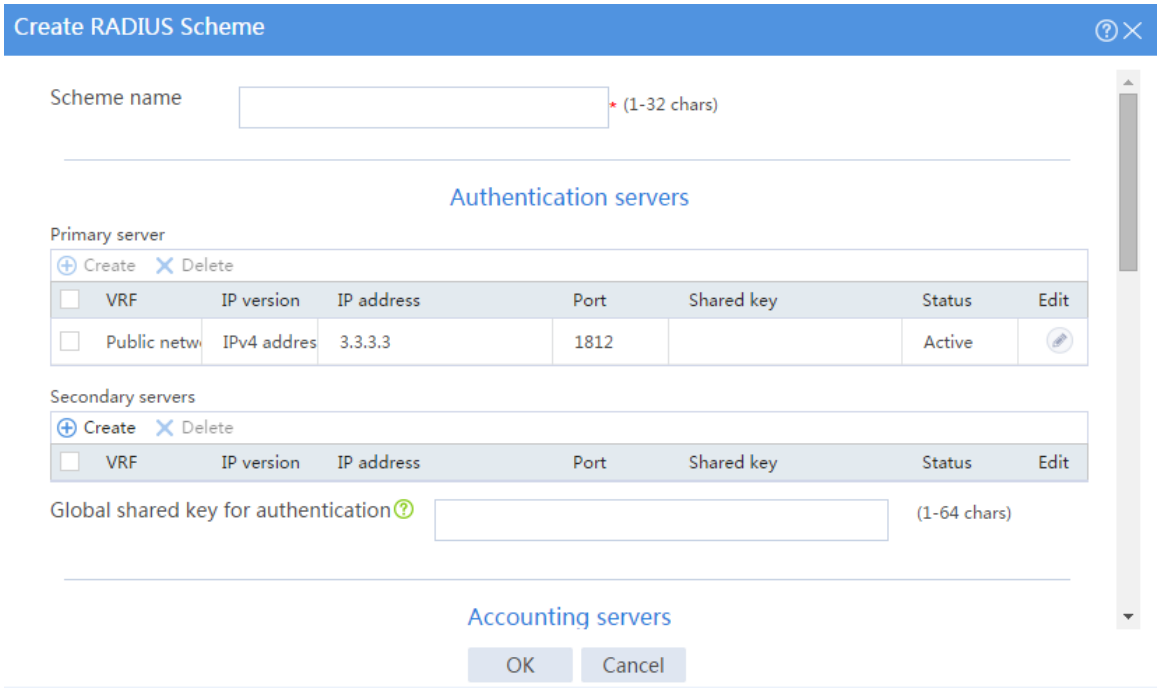
From the navigation pane, select **User** > **Authentication** > **RADIUS**.

Click **Create**.

Configure a RADIUS scheme named **radius**:

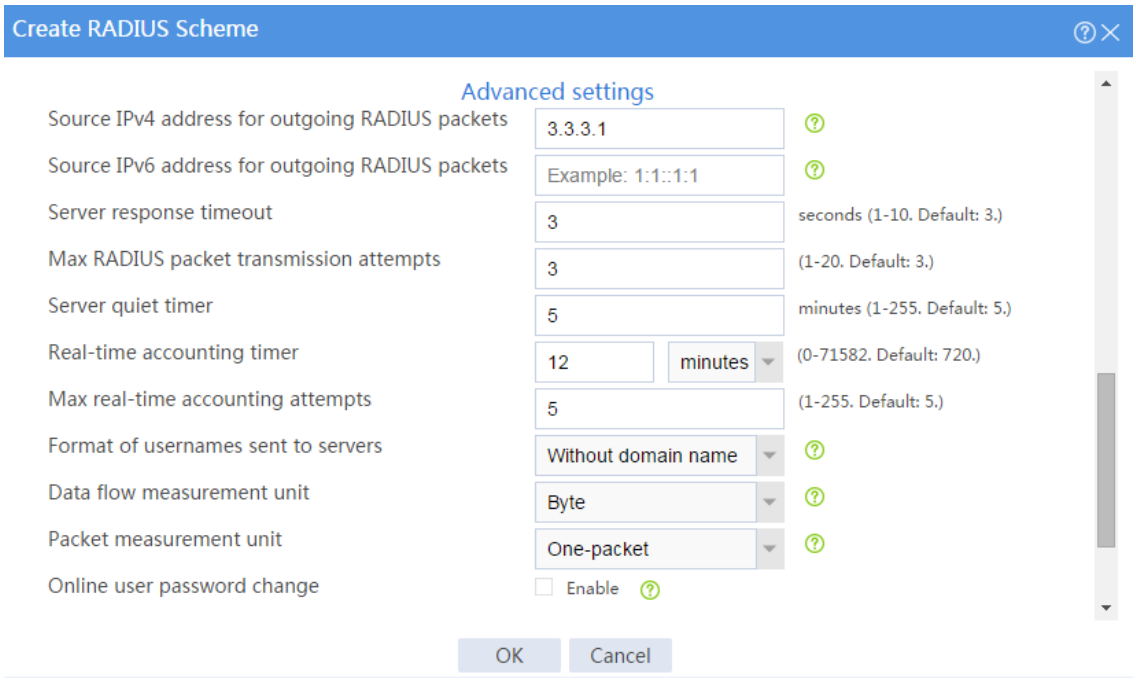
- Set the authentication server as shown in Figure 18.
- Set the global shared key for authentication to 123456.

Figure 18 Configuring a RADIUS scheme



Configure the advanced settings for the RADIUS scheme in the **Advanced settings** area, as shown in Figure 19.

Figure 19 Configuring the advanced settings for the RADIUS scheme



Click **OK**.

10. At the CLI, create ISP domain **sslvpn**, specify RADIUS scheme **radius** for the authentication and authorization methods, and set the accounting method to none.

```
<Device> system-view
[Device] domain sslvpn
[Device-isp-sslvpn] authentication sslvpn radius-scheme radius
[Device-isp-sslvpn] authorization sslvpn radius-scheme radius
[Device-isp-sslvpn] accounting sslvpn none
[Device-isp-sslvpn] quit
```

11. Create a user group:

    # On the top navigation bar, click **Objects**.

    # From the navigation pane, select **User** > **User Management** > **Local Users**.

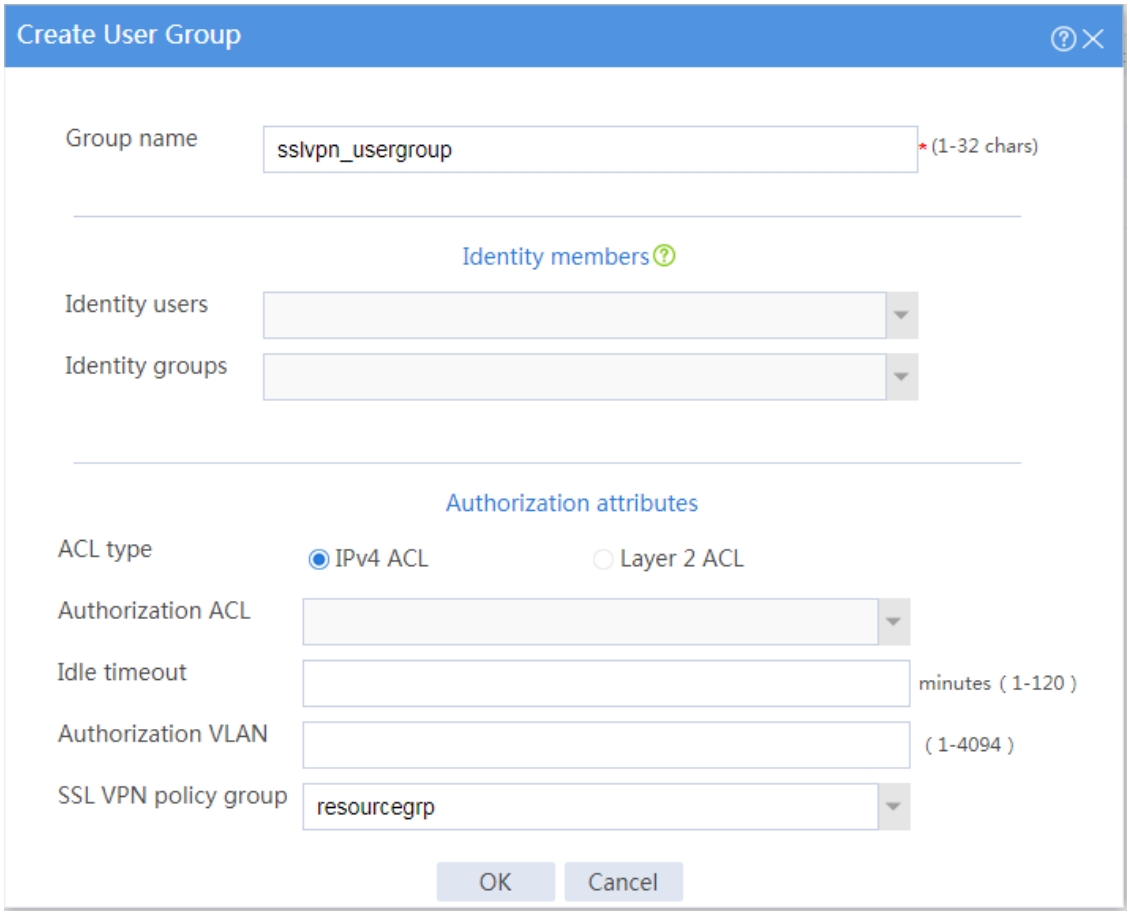
    # Click the **User Group** tab.

    # Click **Create**.

    # Create a user group named **sslvpn_usergroup** and specify SSL VPN resource group **resourcegrp** for the user group, as shown in Figure 20.

    # Click **OK**.

Figure 20 Creating a user group



12. Configure the SSL VPN gateway:

On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

Click **Create**.

Create an SSL VPN gateway as shown in Figure 21, and then click **OK**.

Figure 21 Creating an SSL VPN gateway

13. Create an SSL VPN AC interface:

On the top navigation bar, click **Network**.

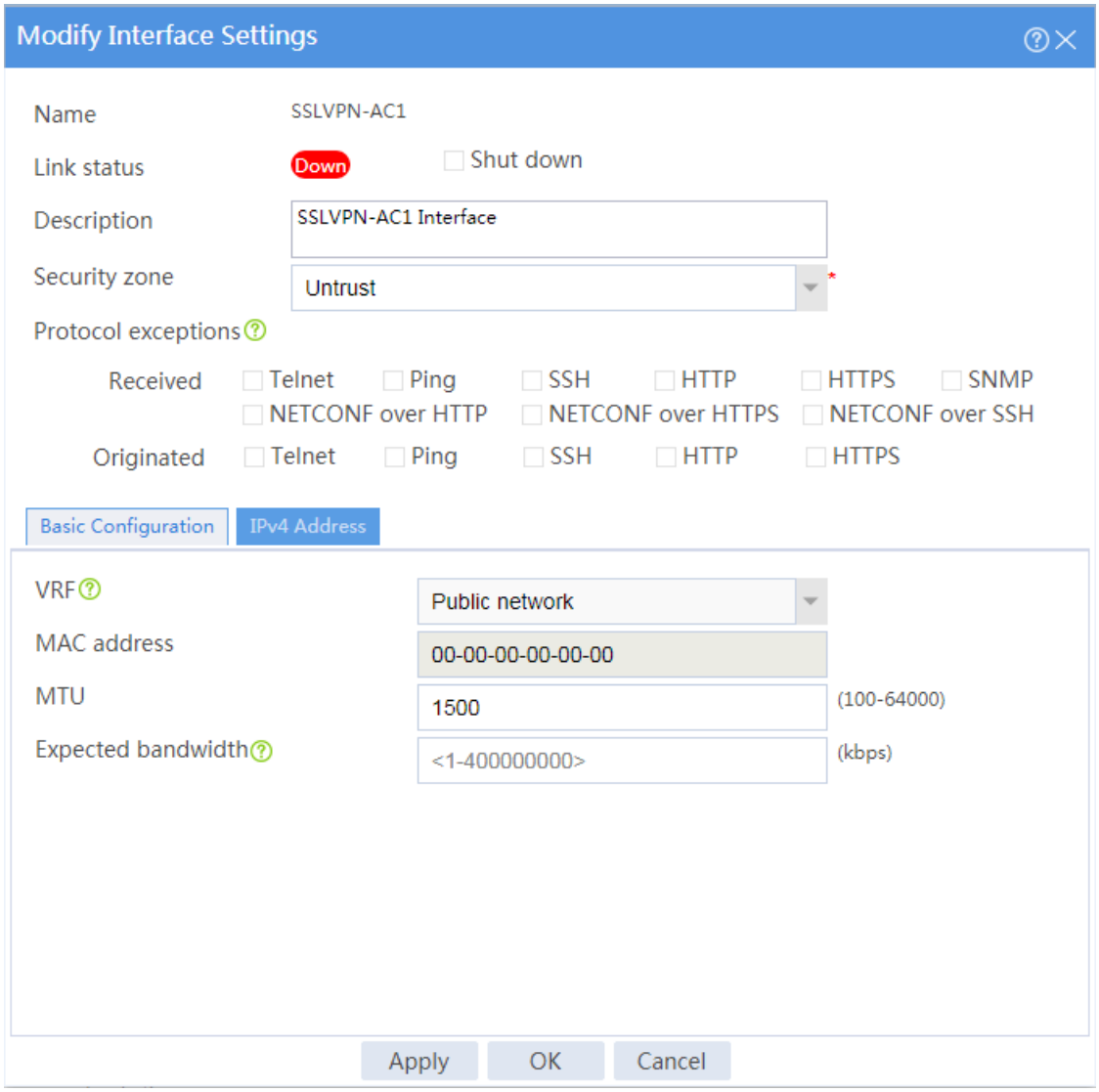
From the navigation pane, select **SSL VPN** > **SSL VPN AC Interfaces**.

Click **Create**.

In the **Create Interfaces** dialog box that opens, enter **1** in the **Interface number** field and click **OK**.

In the **Modify Interface Settings** dialog box, configure the basic settings for the SSL VPN AC interface as shown in Figure 22.

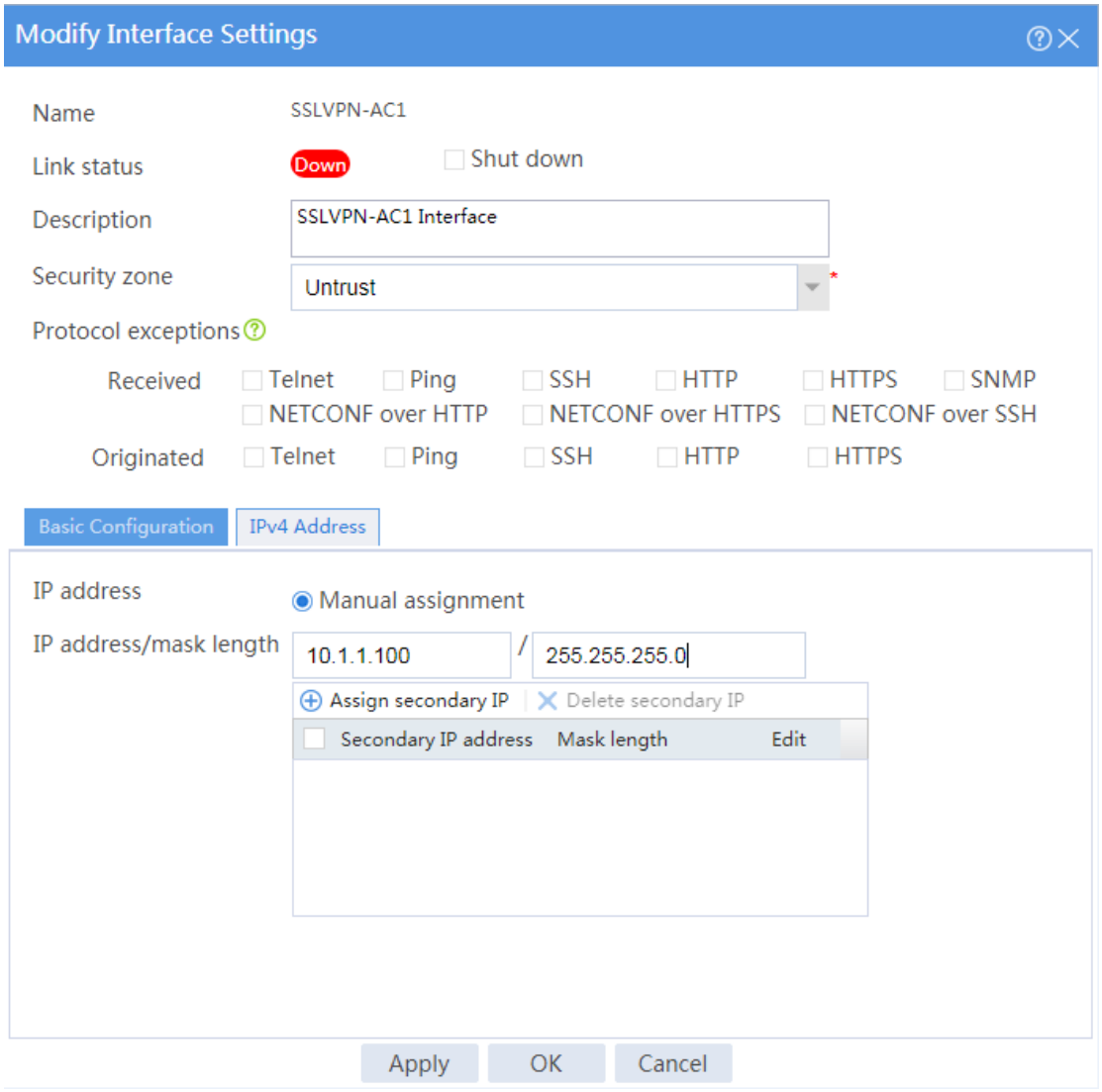
Figure 22 Configuring basic settings for the SSL VPN AC interface



Click the **IPv4 Address** tab and configure the IPv4 address settings for the SSL VPN AC interface as shown in Figure 23.

Click **OK**.

Figure 23 Configuring IPv4 address settings for the SSL VPN AC interface



14. Create an address pool for IP access users:

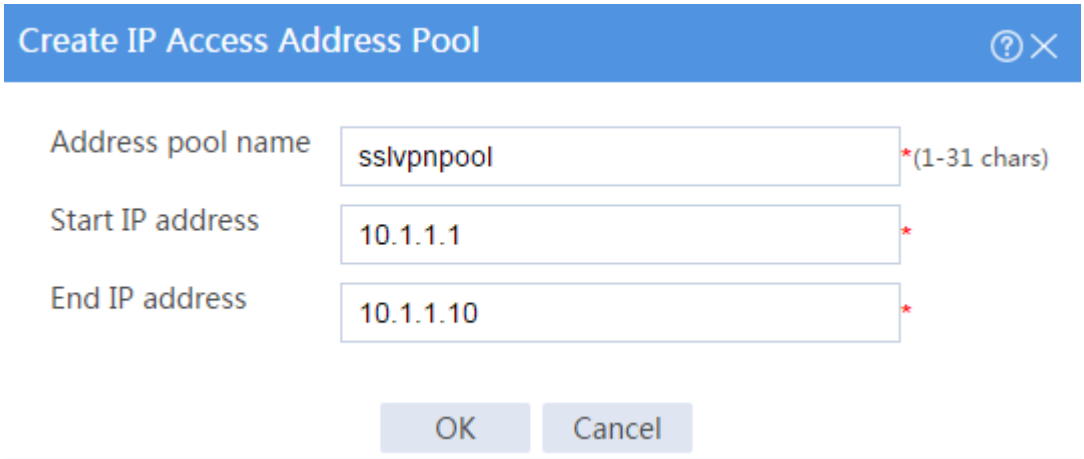
On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **IP Access Address Pools**.

Click **Create**.

Create an IP access address pool as shown in Figure 24, and then click **OK**.

Figure 24 Creating an IP access address pool



15. Configure an SSL VPN context:

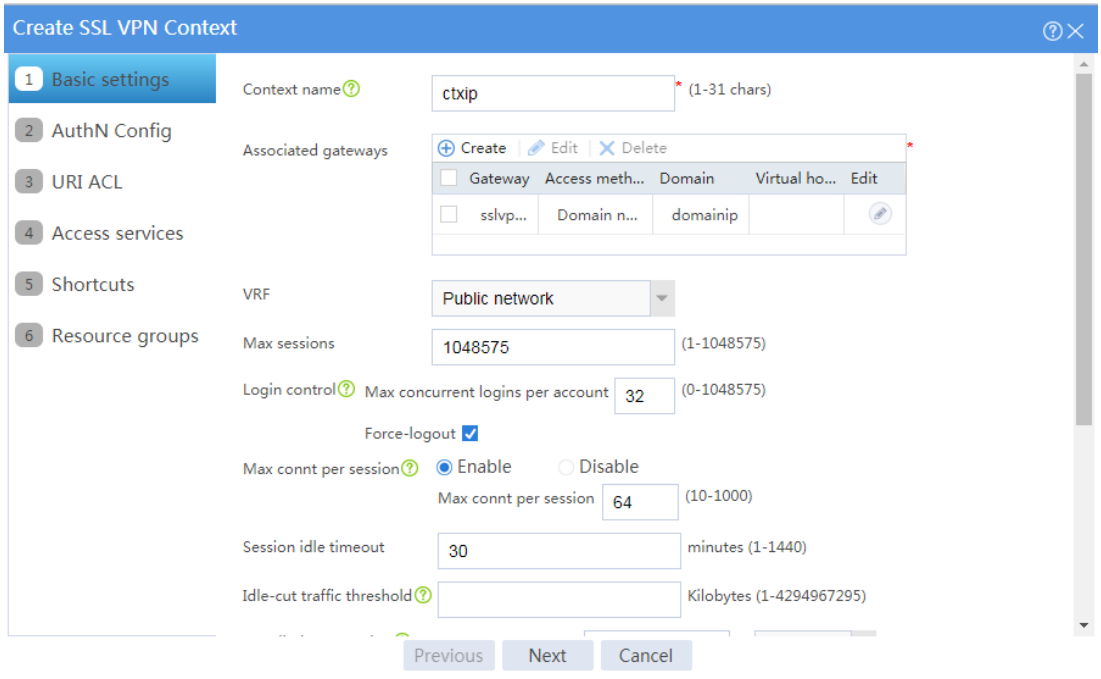
On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

Click **Create**.

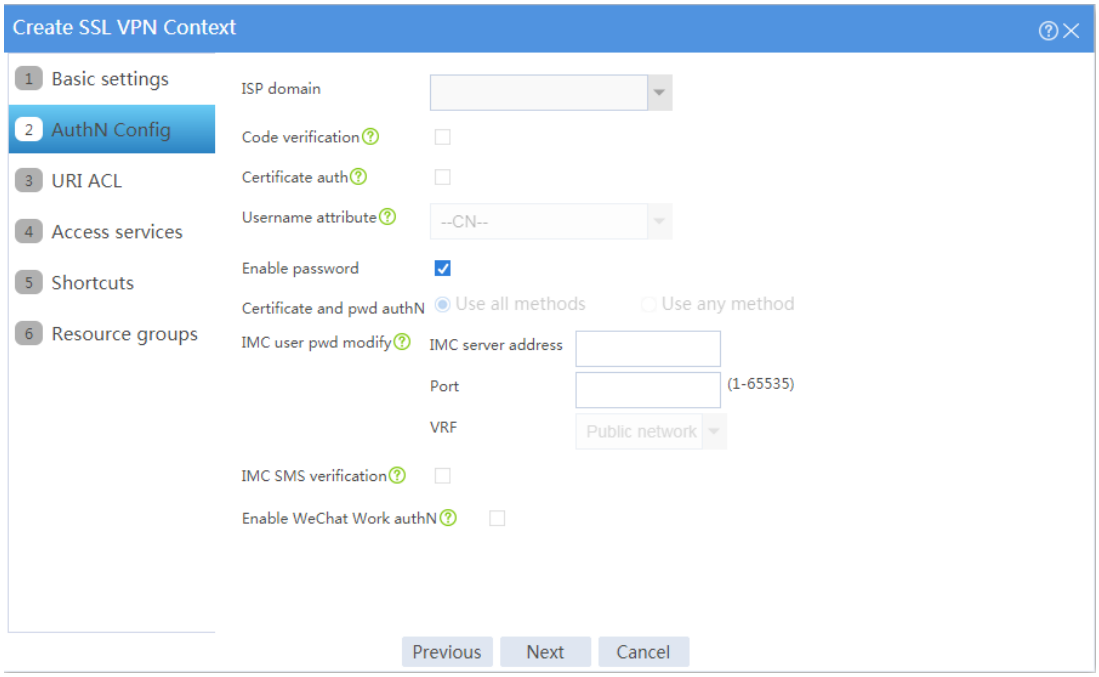
Configure the basic settings for the SSL VPN context as shown in Figure 25.

Figure 25 Configuring basic settings for an SSL VPN context



Click **Next** to configure authentication settings, as shown in Figure 26.

Figure 26 Configuring authentication settings



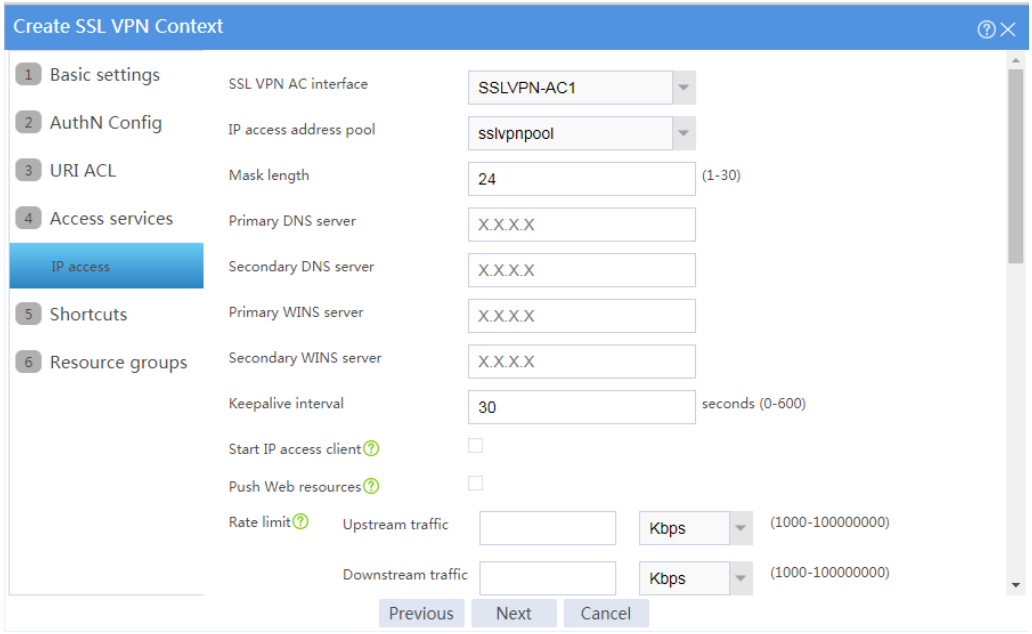
Click **Next** to open the URI ACL page. On the **URI ACL** page, click **Next**.

On the **Access services** page, select **IP access** and click **Next**.

On the **IP access** page, configure the IP access service as follows:

a. Configure the IP access parameters as shown in Figure 27 and click **Next**.

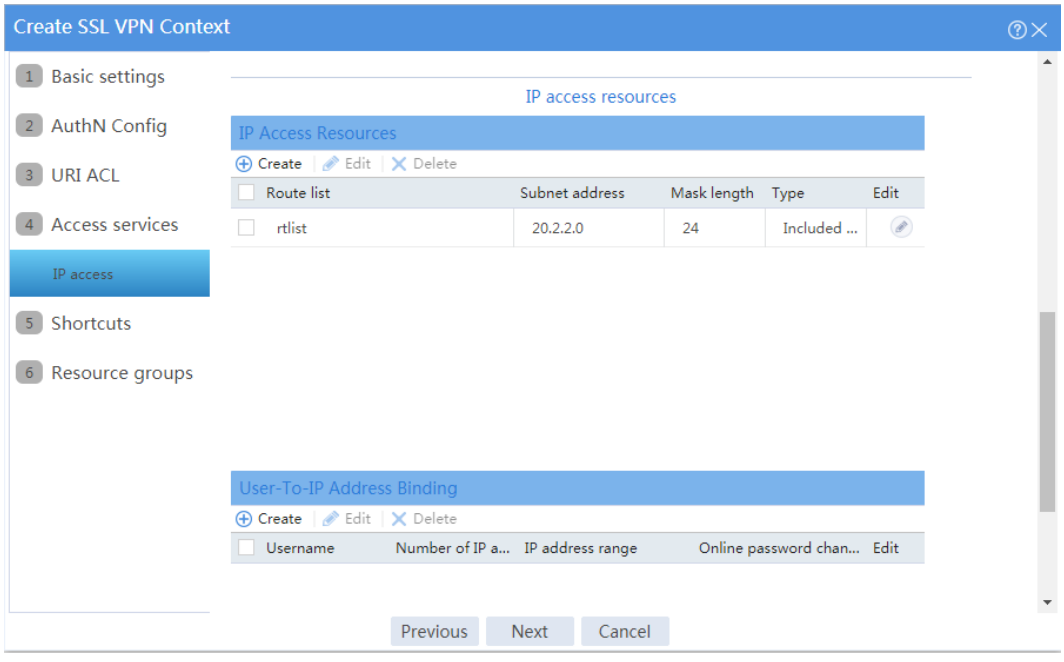
Figure 27 Configuring IP access parameters for the IP access service



b. In the **IP access resources** area, configure route list **rtlist** with an included route entry for 20.2.2.0/24, as shown in Figure 28.

c. Click **Next**.

Figure 28 Configuring IP access resources for the IP access service

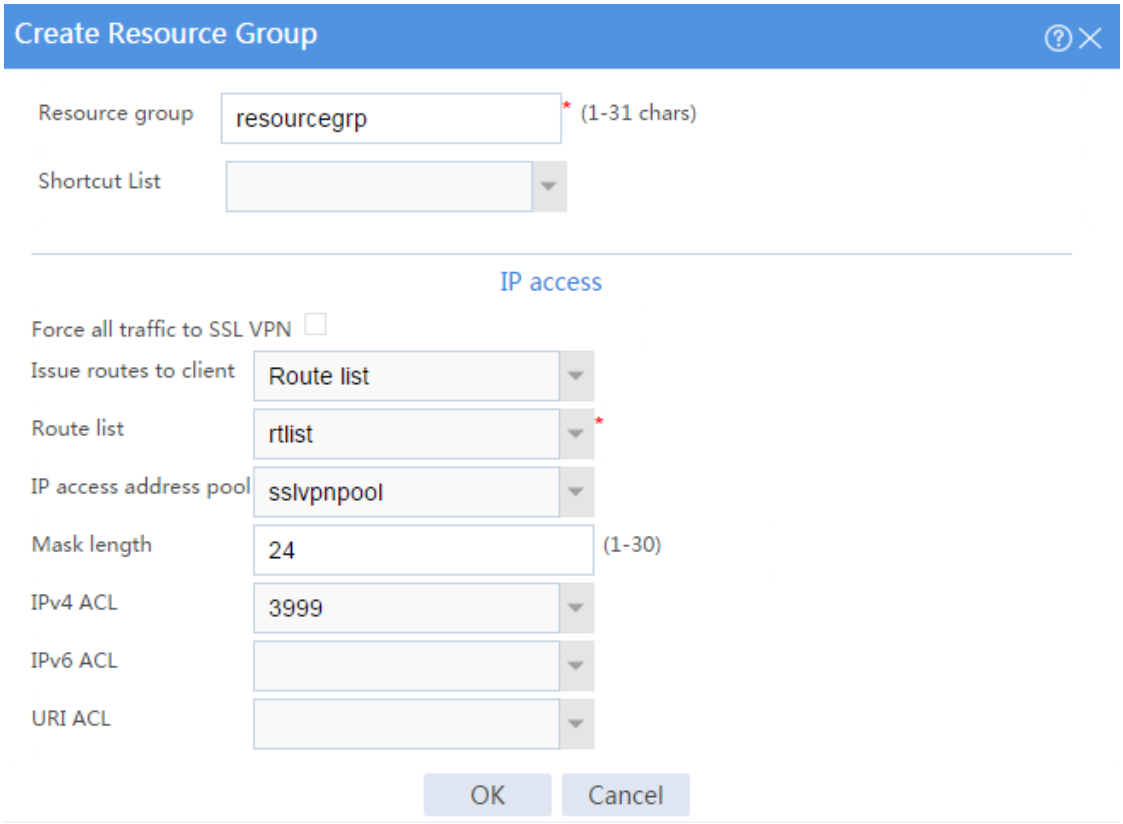


Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp**, as shown in Figure 29. In this example, select route list **rtlist** as the accessible IP resources and use IPv4 ACL 3999 (which permits all traffic) for IP access request filtering.

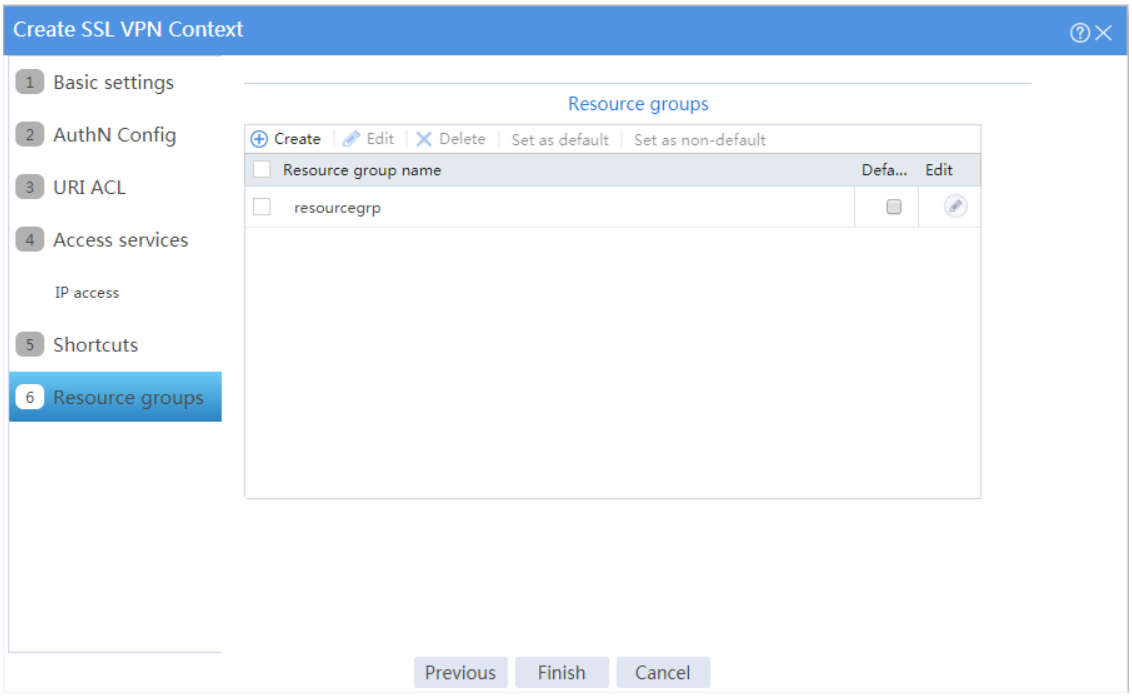
Figure 29 Creating an SSL VPN resource group



Click **OK**.

The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 30.

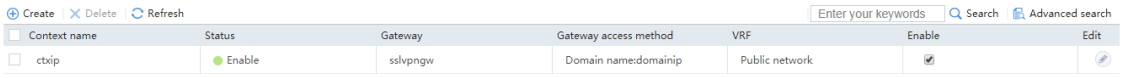
Figure 30 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 31.

Figure 31 Enabling the SSL VPN context



Configuring the RADIUS server

1. Configure an access policy named **resourcegrp**:

Log in to IMC.

On the top navigation bar, click **User**.

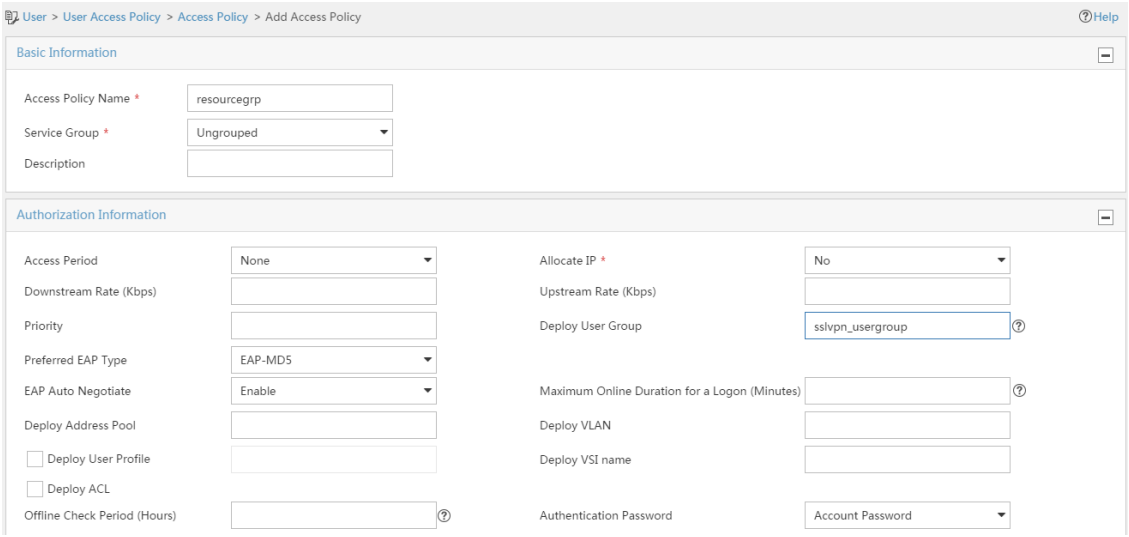
From the navigation pane, select **User Access Policy** > **Access Policy**.

Click **Add**.

Add an access policy as shown in Figure 32.

Click **OK**.

Figure 32 Creating an access policy



2. Configure an access service named **sslvpnservice**:

   # On the top navigation bar, click **User**.

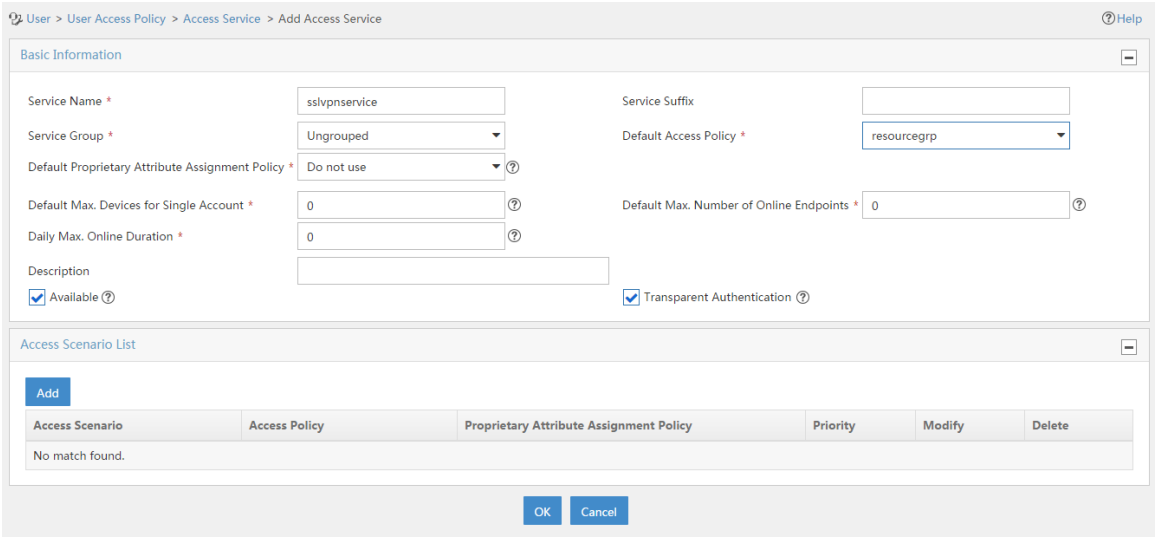
   # From the navigation pane, select **User Access Policy** > **Access Service**.

   # Click **Add**.

   # Add an access service as shown in Figure 33. In this example, specify access policy **resourcegrp** as the default access policy.

   # Click **OK**.

Figure 33 Creating an access service



3. Configure an access device:

   # On the top navigation bar, click **User**.

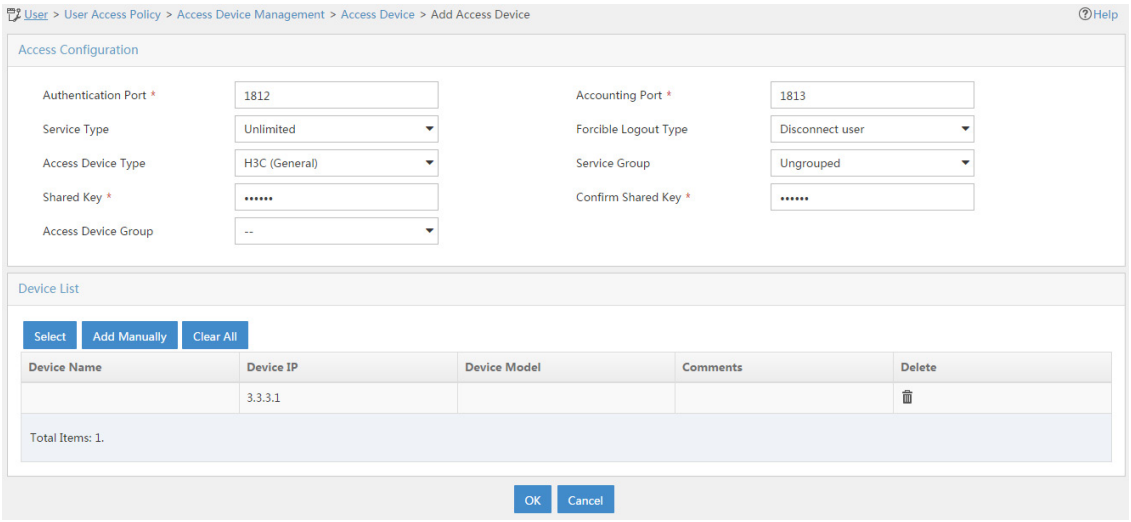
   # From the navigation pane, select **User Access Policy** > **Access Device Management** > **Access Device**.

   # Click **Add**.

   # Add an access device as shown in Figure 34. In this example, set the shared key to **123456**.

   # Click **OK**.

Figure 34 Configuring an access device



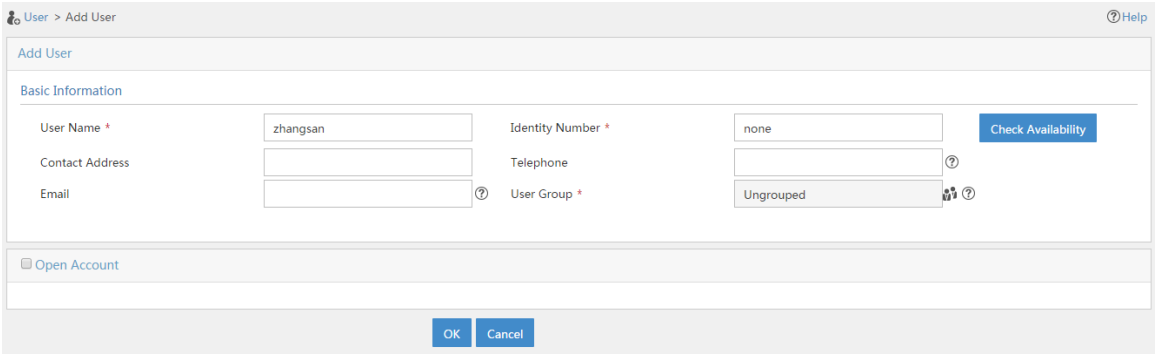
4. Configure an access user:

Access the **User** > **Add User** page.

Add a platform user as shown in Figure 35.

Click **OK**.

Figure 35 Adding a platform user



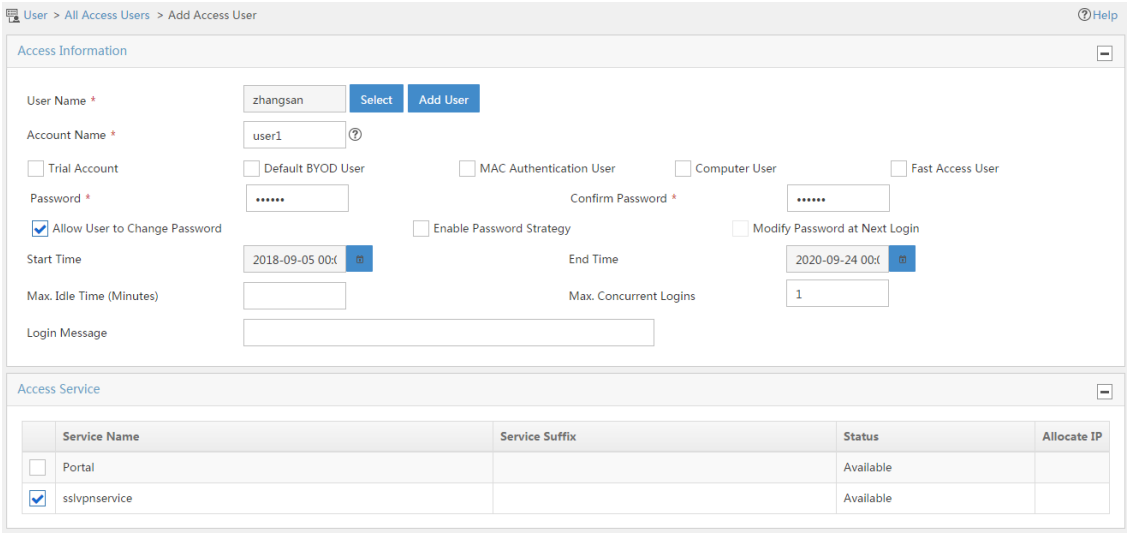
From the navigation pane, select **Access User** > **All Access Users**.

Click **Add**.

Add an access user and assign access service **sslvpnservice** to the user, as shown in Figure 36.

Click **OK**.

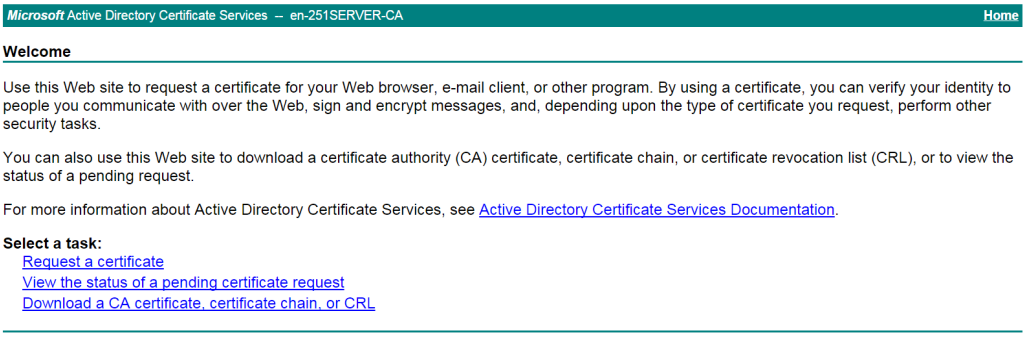
Figure 36 Adding an access user



Configuring the host

1. Configure the IP address and gateway address settings for the host and make sure it can reach the SSL VPN gateway and the CA server.
2. Submit a client certificate request to the CA server:
   a. Enter **http://192.168.100.247/certsrv** in the browser address bar.
   b. On the certificate service home page shown in Figure 37, click **Request a certificate**.

Figure 37 Certificate service home page

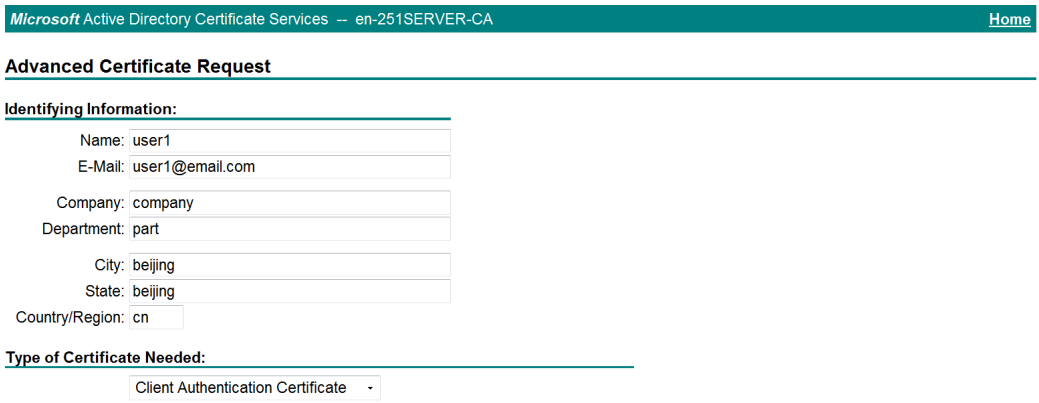


   c. On the **Request a Certificate** page shown in Figure 38, click **advanced certificate request**.

Figure 38 Request a Certificate page

d. Create a client certificate request, as shown in Figure 39.

Figure 39 Creating a client certificate request



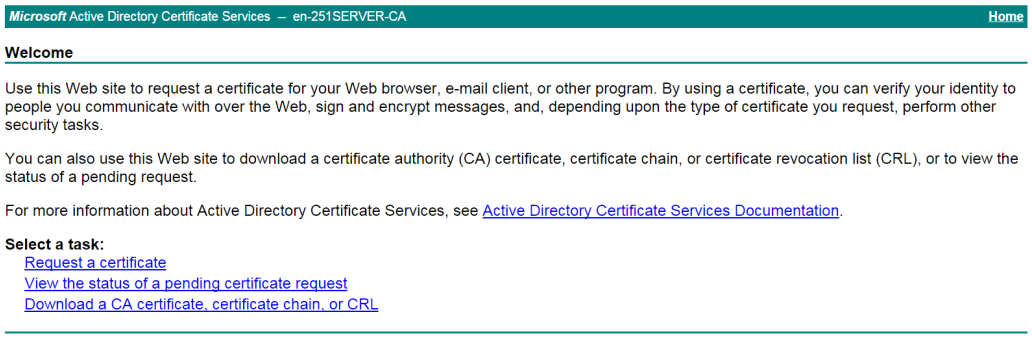
e. Click **Submit**.

3. Install the client certificate on the host:

a. After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

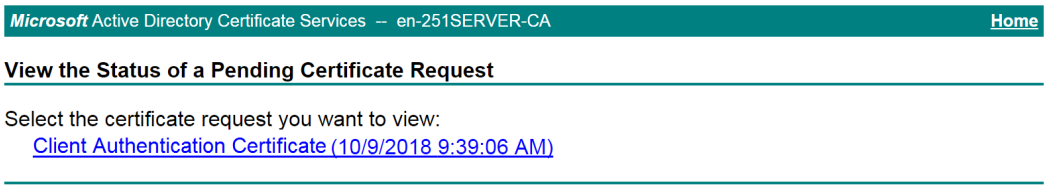
b. On the certificate service home page shown in Figure 40, click **View the status of a pending certificate request**.

Figure 40 Certificate service home page



The **View the Status of a Pending Certificate Request** page opens, as shown in Figure 41.

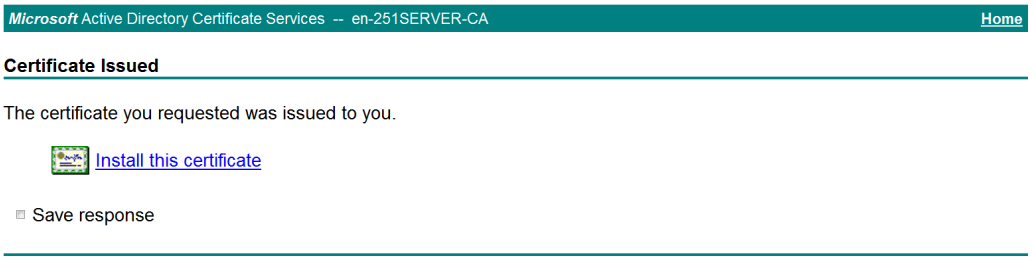
Figure 41 View the Status of a Pending Certificate Request page



c. Click the client certificate whose status you want to view.

d. On the **Certificate Issued** page shown in Figure 42, click **Install this certificate** to install the client certificate.

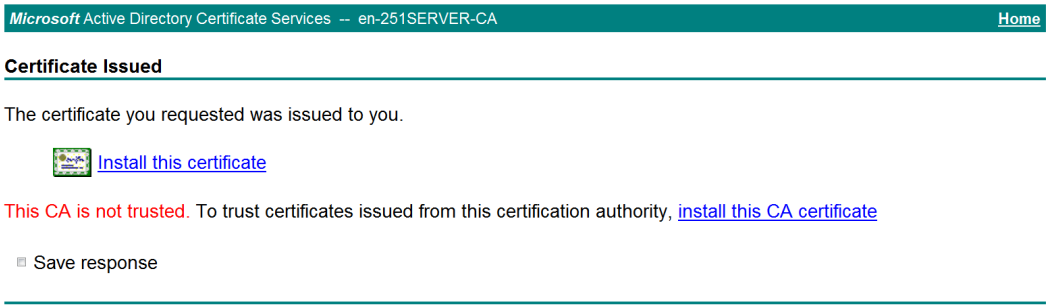
Figure 42 Installing the client certificate



If the host does not have a CA certificate, the page shown in Figure 43 opens. You must install the CA certificate first.

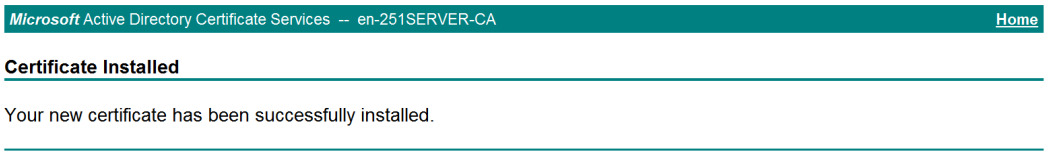
e. Click **install this CA certificate** to install the CA certificate. Then, click **Install this certificate** to install the client certificate.

Figure 43 Installing the CA certificate and then the client certificate



After the client certificate is installed, the **Certificate Installed** page shown in Figure 44 opens.

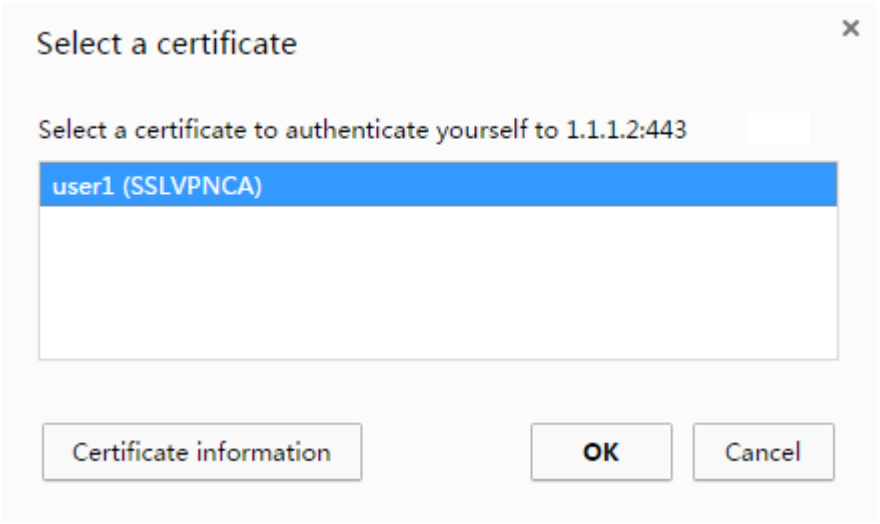
Figure 44 Certificate Installed page



Verifying the configuration

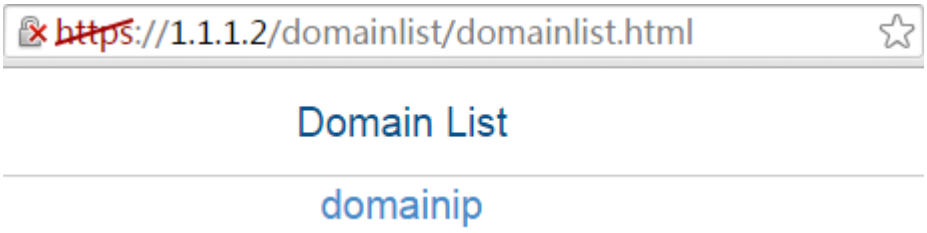
1. In the browser address bar of the host, enter **https://1.1.1.2** and press **Enter**.
2. On the **Select a certificate** page, select the client certificate for authentication, as shown in Figure 45.

Figure 45 Select a certificate page



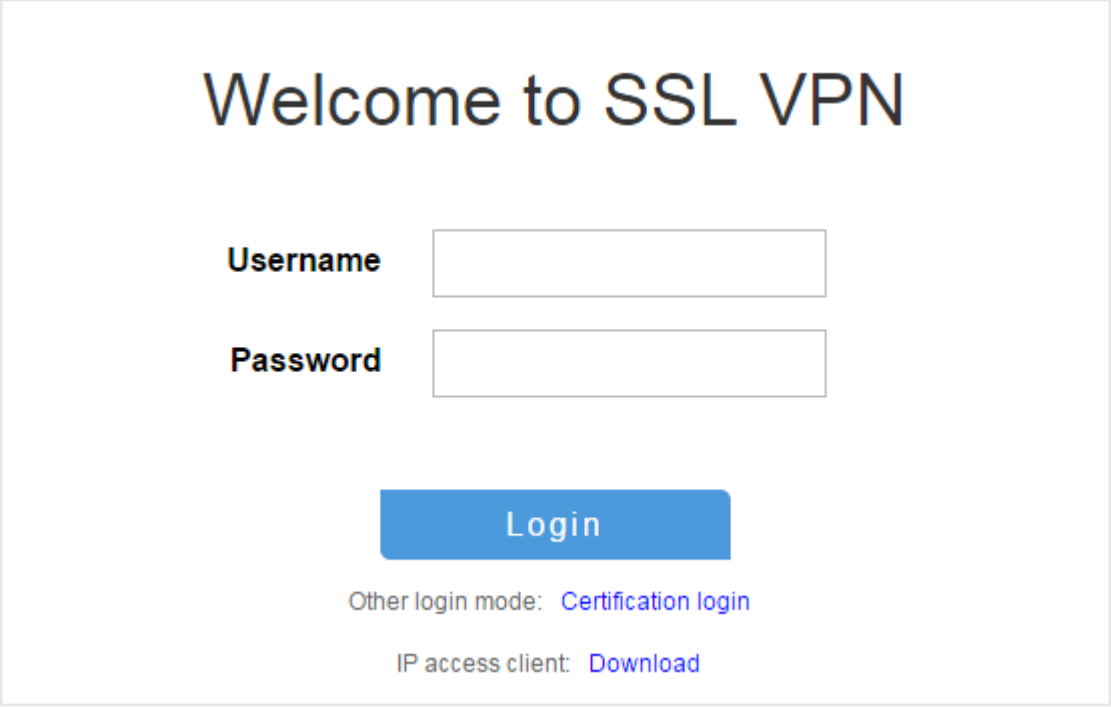
3. Click **OK**.
4. On the **Domain List** page shown in Figure 46, select **domainip** to access the login page.

Figure 46 Domain list page



5. On the login page, enter username **user1** and password **123456**, and then click **Login**.

Figure 47 Login page



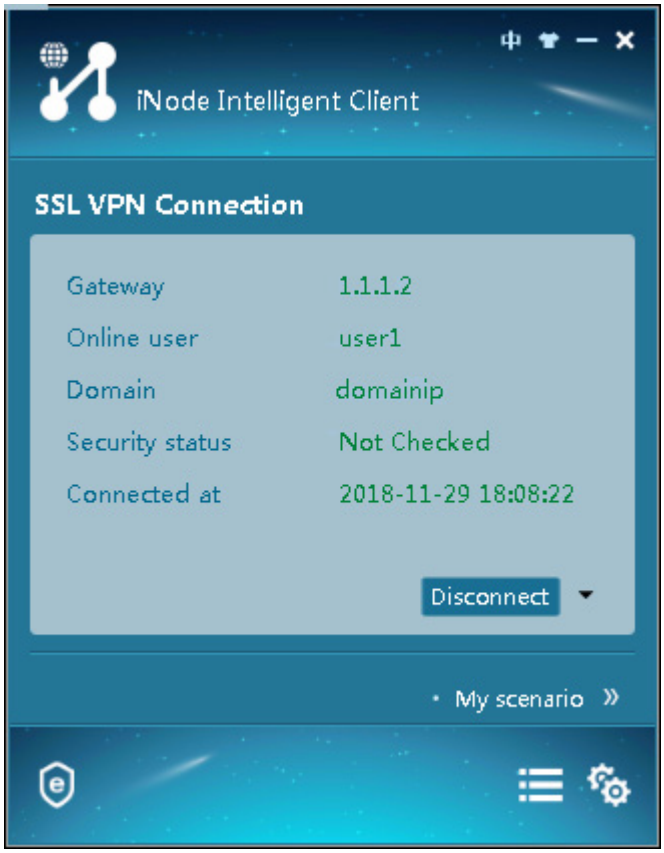
6. Click **START** to start the IP client application.

   If the host does not have an iNode client installed, the system installs the iNode client, and then starts and connects the iNode client to the SSL VPN gateway.

   If the host already has an iNode client installed, the system starts the iNode client and connects it to the SSL VPN gateway directly.

   Figure 48 shows that the iNode client is successfully connected to the SSL VPN gateway.

Figure 48 Connecting the iNode client to the SSL VPN gateway



Example: Configuring IP access with LDAP authentication

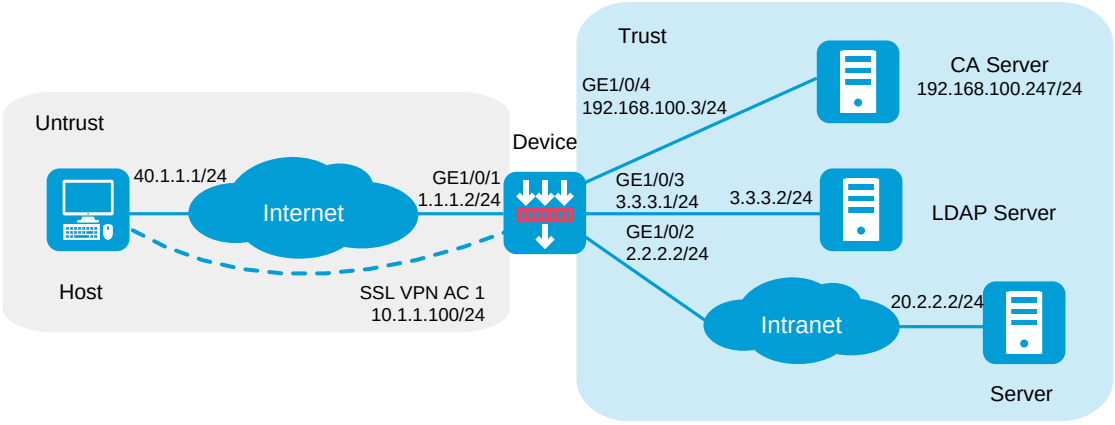
Network configuration

As shown in Figure 49, the device acts as an SSL VPN gateway that connects the public network and the private network. On the private network, a CA server and an LDAP server are deployed and both servers run the Windows Server 2008 R2 operating system. Users need secure access to the internal server (20.2.2.2/24) in IP access mode.

Perform the following tasks:

- Request an SSL server certificate for the device from the CA server.
- Configure the device to require that users pass both password and certificate authentication for IP access.
- Configure the device to use the LDAP server to perform remote authentication and authorization for IP access users.
- Configure the SSL VPN IP access service on the device to allow users to access the internal server in IP access mode.

Figure 49 Network diagram (LDAP authentication)



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

- The IP address pool configured for client address allocation must meet the following requirements:
  - The address range of the address pool cannot be on the same subnet as the IP address used on the client host.

- The IP addresses in the address pool do not conflict with the IP addresses used on the device.
- The address range of the address pool cannot be on the same subnet as the IP address of the internal server.

- The SSL VPN AC interface must be added to the correct security zone (**Untrust**, in this example).

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click the **Network** tab.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 3.3.3.1/24 in the same way you configure GE 1/0/1.

Add GE 1/0/4 to the **Trust** security zone and set its IP address to 192.168.100.3/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

This example configures static routes.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static IPv4 route to reach 40.1.1.1:

a. Enter destination IP address **40.1.1.1**.

b. Enter mask length **24**.

c. Enter next hop address **1.1.1.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 20.2.2.2:

a. Enter destination IP address **20.2.2.2**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 addresses **2.2.2.2**, **3.3.3.1**, and **192.168.100.3**.
- Select destination IPv4 addresses **20.2.2.2**, **3.3.3.2**, and **192.168.100.247**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **untrust-trust** to permit the specified traffic from the **Untrust** to **Trust** security zones:

- Enter policy name **untrust-trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.0/24**.
- Select destination IPv4 address **20.2.2.2/24**.
- Use the default settings for other parameters.

Click **OK**.

4. Request a server certificate for the device:

a. Create a certificate subject:

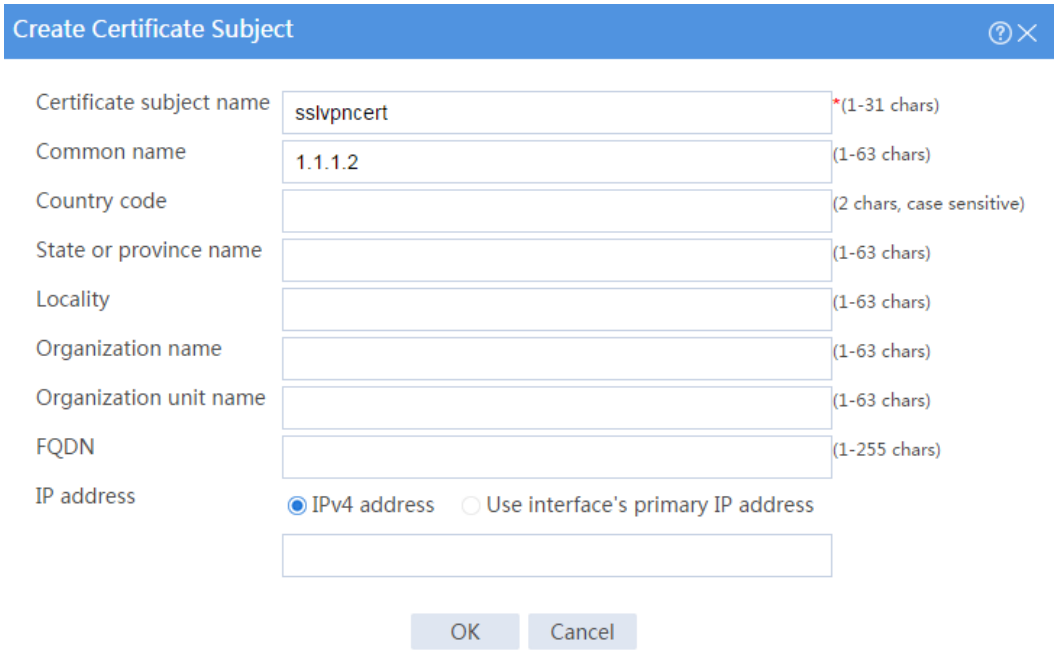
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate Subject**.

Click **Create**.

Create a certificate subject as shown in Figure 50, and the click **OK**.

Figure 50 Creating a certificate subject

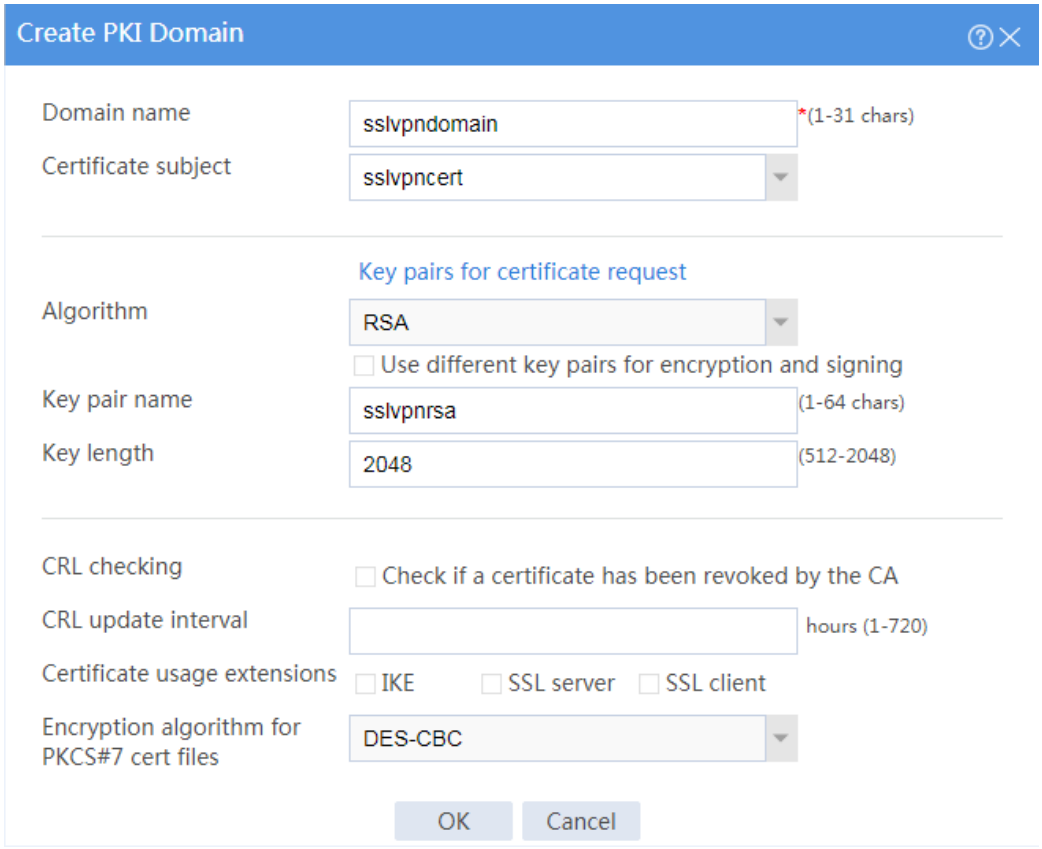


b. Create a PKI domain:

On the **Certificate** page, click **Create PKI domain**.

Create a PKI domain as shown in Figure 51, and then click **OK**.

Figure 51 Creating a PKI domain

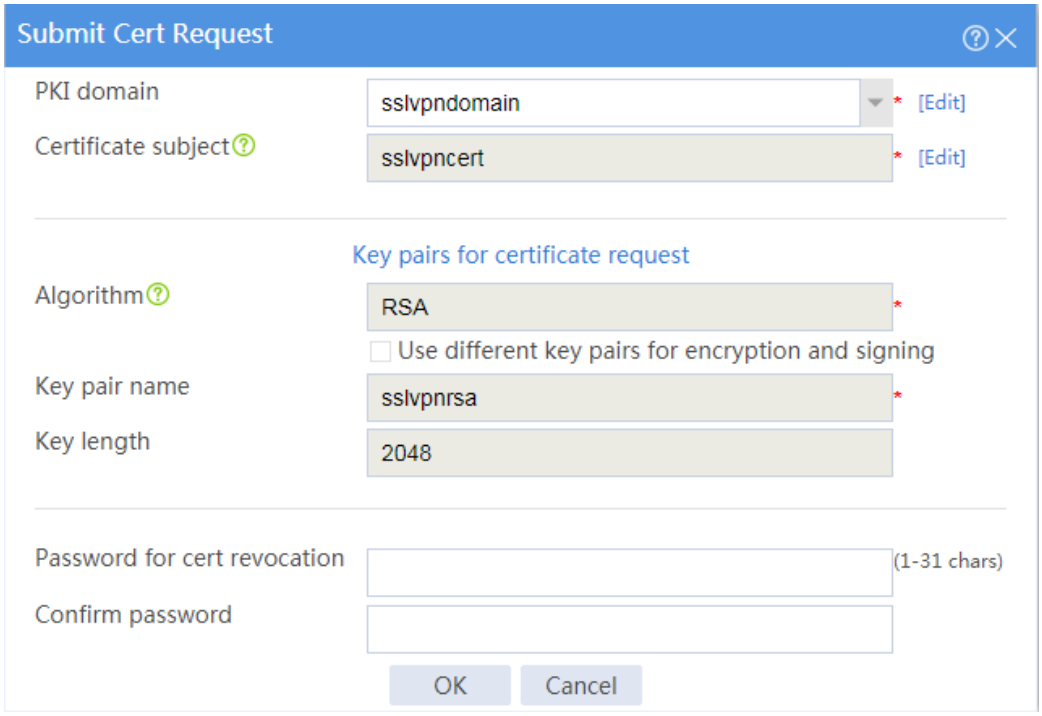


c. Create a certificate request:

On the **Certificate** page, click **Submit Cert Request**.

Configure the certificate request settings as shown in Figure 52.

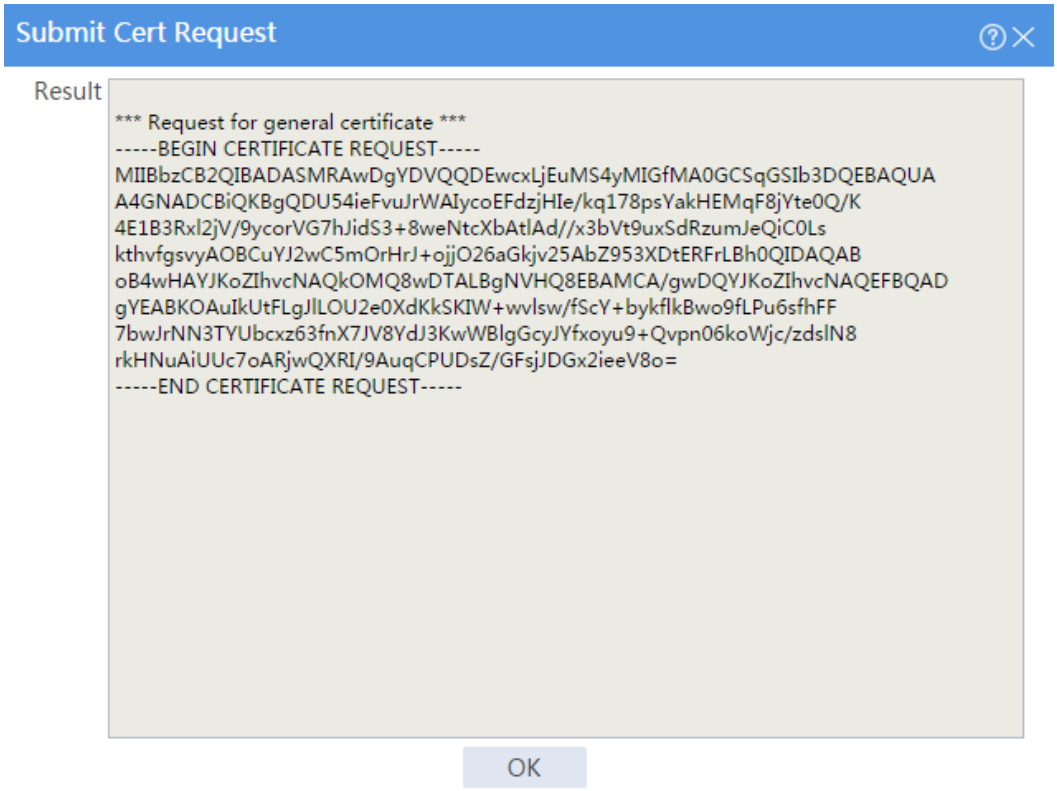
Figure 52 Creating a certificate request



Click **OK**.

The certificate request content will be displayed, as shown in Figure 53.

Figure 53 Certificate request content



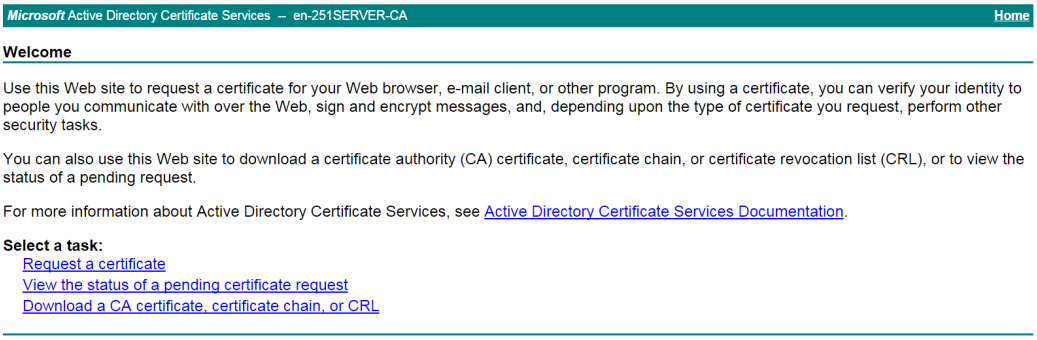
Copy the certificate request content and click **OK**.

d. Request a server certificate from the CA:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 54, click **Request a certificate**.

Figure 54 Certificate service home page

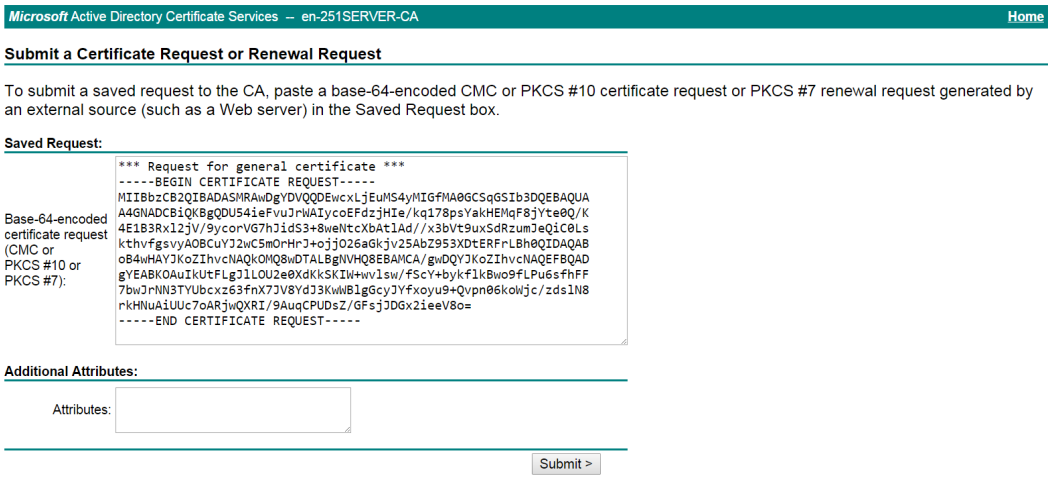


On the **Request a Certificate** page shown in Figure 55, click **advanced certificate request**.

Figure 55 Request a Certificate page

Paste the previously copied certificate request content in the **Base-64-encoded certificate request CMC or PKCS # 10 or PKCS # 7)** field, as shown in Figure 56.

Figure 56 Pasting the certificate request content

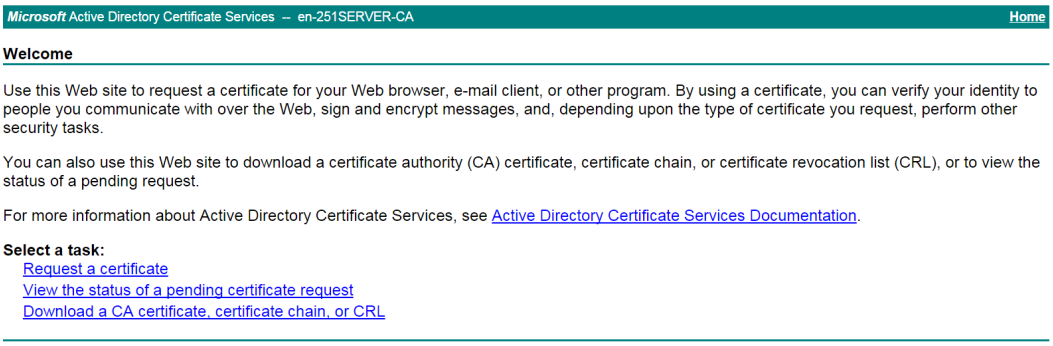


Click **Submit**.

After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 57, click **View the status of a pending certificate request**.

Figure 57 Certificate service home page



Select the certificate request you want to view.

Figure 58 View the Status of a Pending Certificate Request page

The **Certificate Issued** page opens, indicating that the requested server certificate has been issued, as shown in Figure 59.

Figure 59 Certificate Issued page

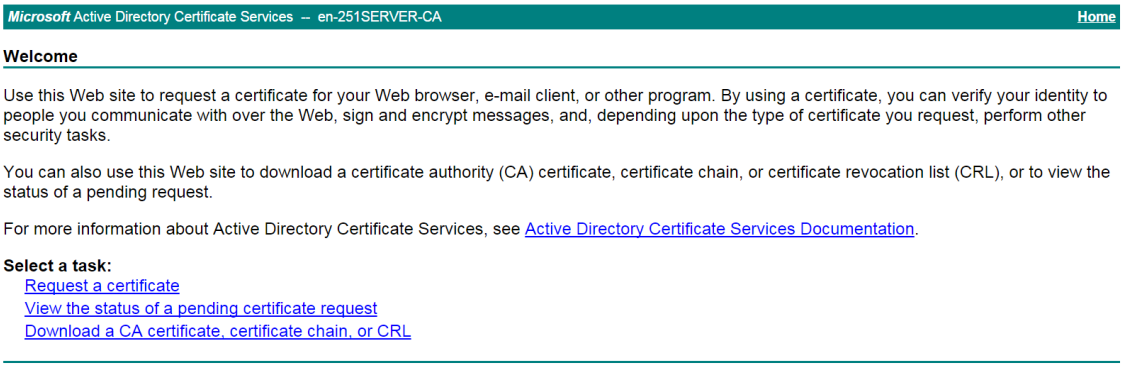
Click **Download certificate** to download the server certificate and save it locally.

5. Download the CA certificate:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

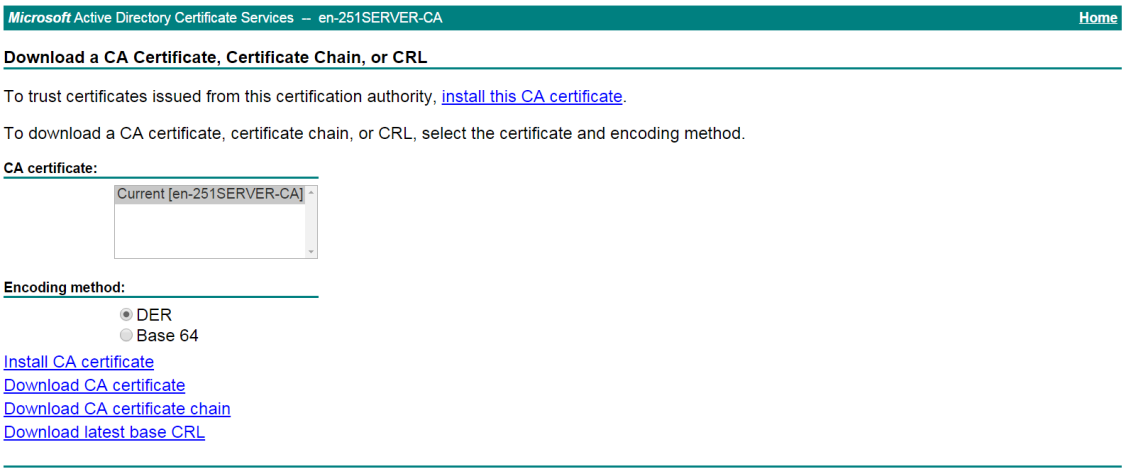
On the certificate service home page shown in Figure 60, click **Download a CA certificate, certificate chain, or CRL**.

Figure 60 Certificate service home page



On the **Download a CA certificate, certificate chain, or CRL** page shown in Figure 61, click **Download CA certificate**.

Figure 61 Download a CA certificate, certificate chain, or CRL page



Save the downloaded CA certificate locally.

6. Import the CA certificate and server certificate to the PKI domain:

a. Import the CA certificate:

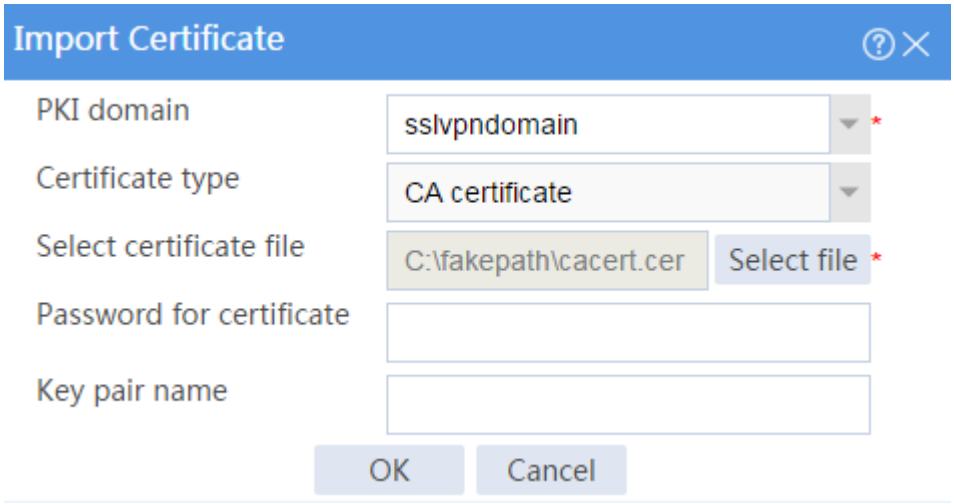
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate**.

Click **Import certificate**.

Import the locally saved CA certificate, as shown in Figure 62, and then click **OK**.

Figure 62 Importing the CA certificate

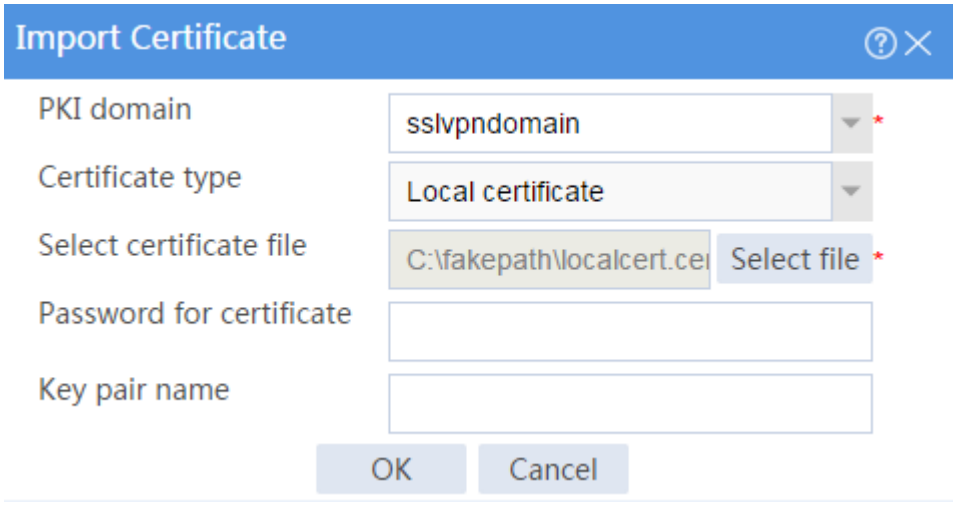


b. Import the server certificate:

On the **Certificate** page, click **Import certificate**.

Import the locally saved server certificate, as shown in Figure 63, and then click **OK**.

Figure 63 Importing the server certificate



7. Configure an SSL server policy:

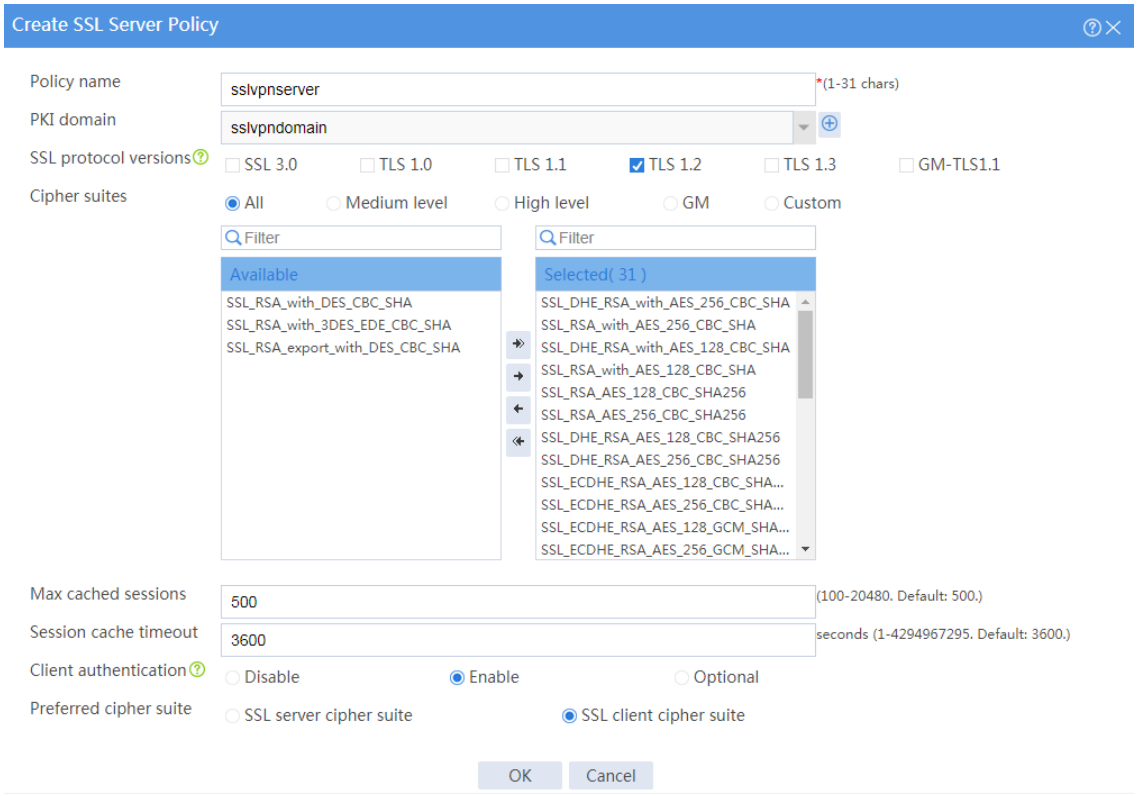
On the top navigation bar, click **Objects**.

From the navigation pane, select **SSL** > **SSL Server Policies**.

Click **Create**.

Configure an SSL server policy as shown in Figure 64, and then click **OK**.

Figure 64 Creating an SSL server policy



8. Configure an SSL client policy:

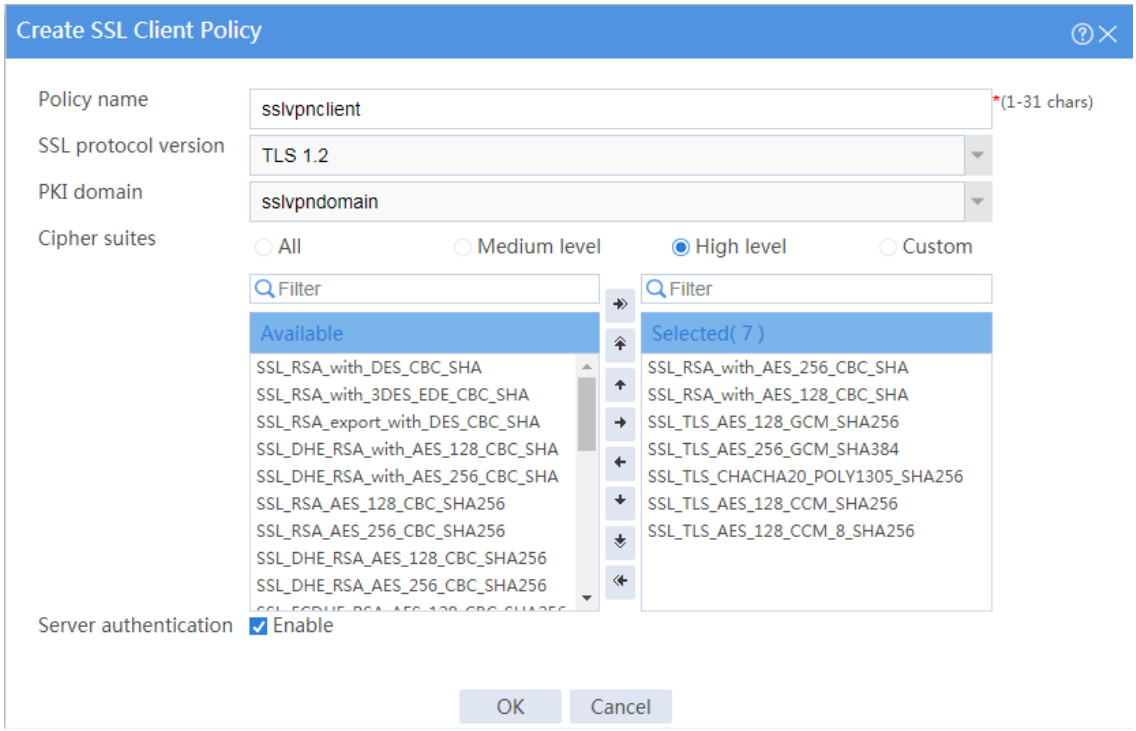
   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **SSL** > **SSL Client Policies**.

   # Click **Create**.

   # Configure an SSL client policy as shown in Figure 65, and then click **OK**.

Figure 65 Creating an SSL client policy



9. Configure LDAP settings at the CLI:

Configure LDAP server **ldap1**.

```
<Device> system-view
[Device] ldap server ldap1
[Device-ldap-server-ldap1] login-dn
cn=administrator,cn=users,dc=ldap,dc=com
[Device-ldap-server-ldap1] search-base-dn
ou=sslvpn_usergroup,dc=ldap,dc=com
[Device-ldap-server-ldap1] ip 3.3.3.3
[Device-ldap-server-ldap1] login-password simple 123456
[Device-ldap-server-ldap1] quit
```

Configure LDAP attribute map **test**.

```
[Device] ldap attribute-map test
[Device-ldap-attr-map-test] map ldap-attribute memberof prefix cn=
delimiter , aaa-attribute user-group
```

```
[Device-ldap-attr-map-test] quit
```

Configure LDAP scheme **shm1**.

```
[Device] ldap scheme shm1
[Device-ldap-shm1] authentication-server ldap1
[Device-ldap-shm1] authorization-server ldap1
[Device-ldap-shm1] attribute-map test
[Device-ldap-shm1] quit
```

Configure ISP domain **sslvpn**.

```
[Device] domain sslvpn
[Device-isp-sslvpn] state active
[Device-isp-sslvpn] authentication sslvpn ldap-scheme shm1
[Device-isp-sslvpn] authorization sslvpn ldap-scheme shm1
[Device-isp-sslvpn] accounting sslvpn none
[Device-isp-sslvpn] quit
```

10. Create a user group:

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **Local Users**.

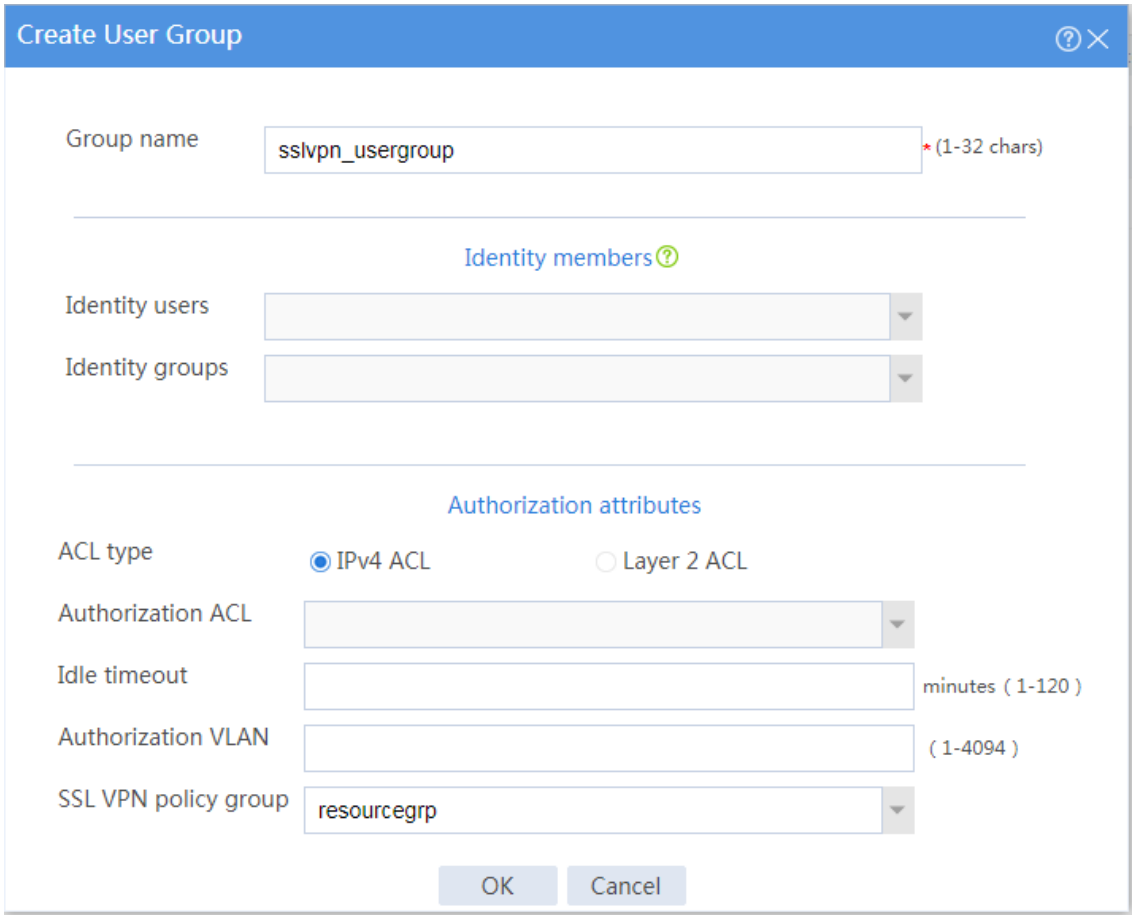
Click the **User Group** tab.

Click **Create**.

Create a user group named **sslvpn_usergroup** and specify SSL VPN resource group **resourcegrp** for the user group, as shown in Figure 66.

Click **OK**.

Figure 66 Creating a user group



11. Configure the SSL VPN gateway:

On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

Click **Create**.

Create an SSL VPN gateway as shown in Figure 67, and then click **OK**.

Figure 67 Creating an SSL VPN gateway

12. Create an SSL VPN AC interface:

On the top navigation bar, click **Network**.

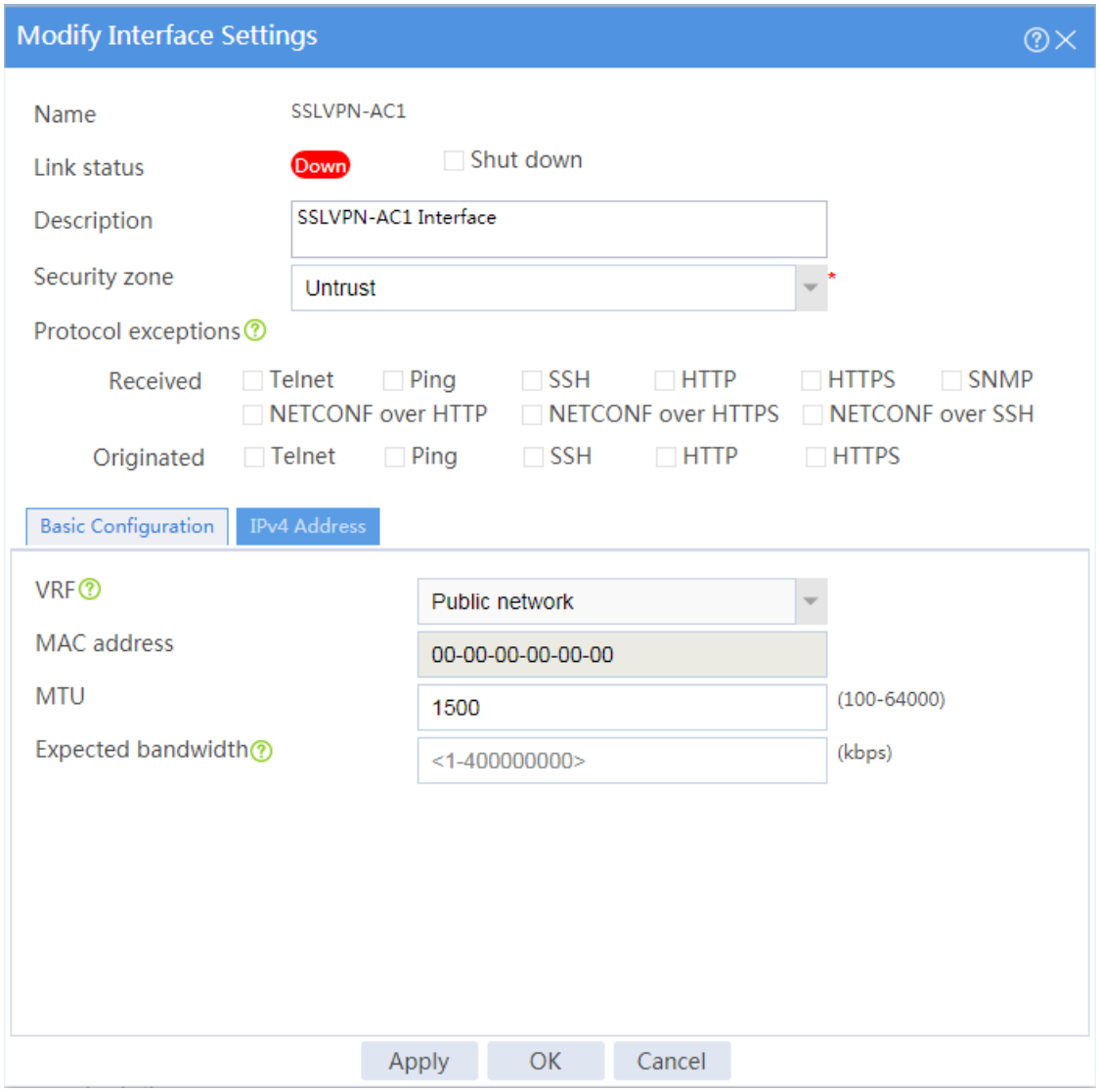
From the navigation pane, select **SSL VPN** > **SSL VPN AC Interfaces**.

Click **Create**.

In the **Create Interfaces** dialog box that opens, enter **1** in the **Interface number** field and click **OK**.

In the **Modify Interface Settings** dialog box, configure the basic settings for the SSL VPN AC interface as shown in Figure 68.

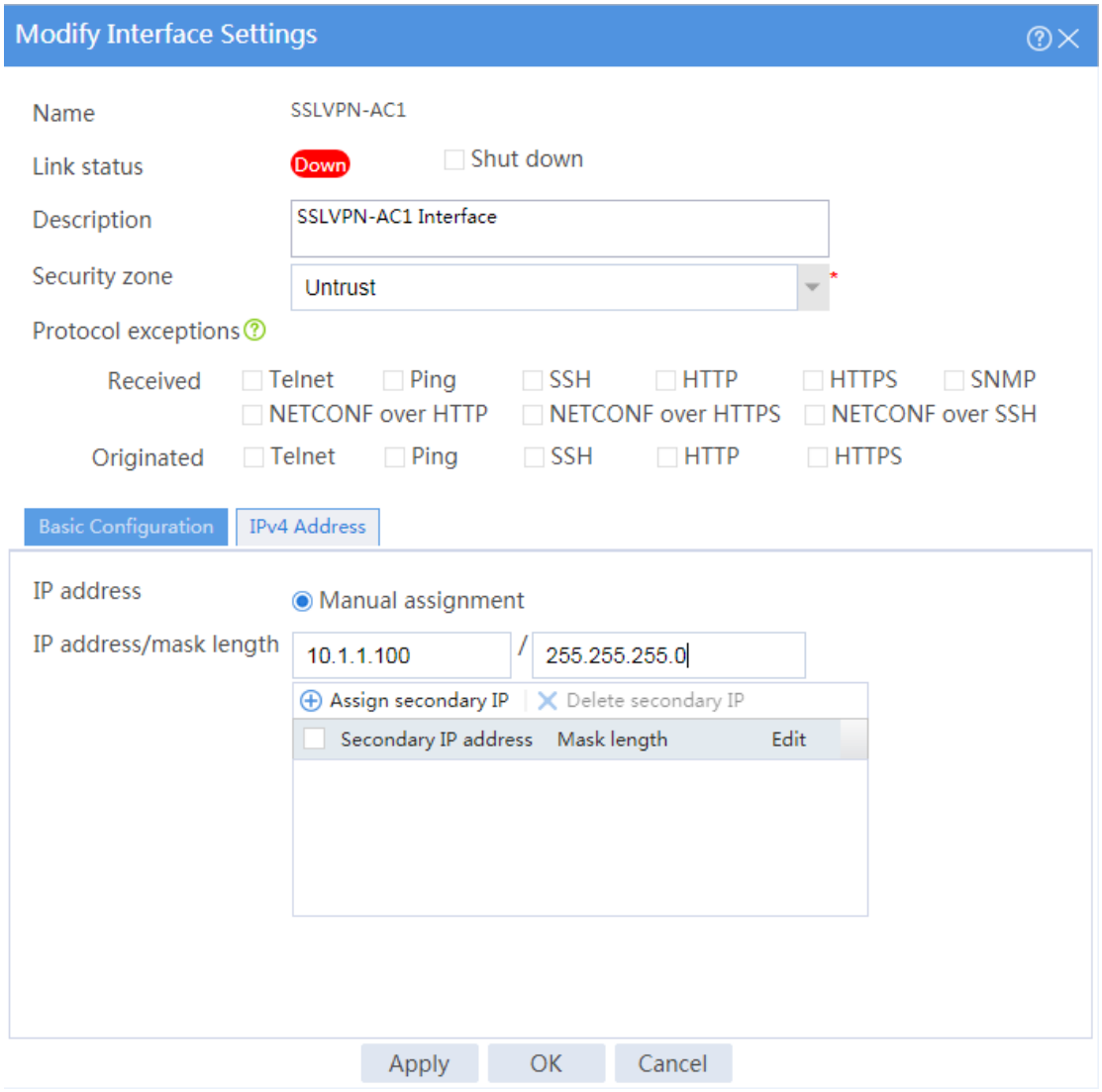
Figure 68 Configuring basic settings for the SSL VPN AC interface



Click the **IPv4 Address** tab and configure the IPv4 address settings for the SSL VPN AC interface as shown in Figure 69.

Click **OK**.

Figure 69 Configuring IPv4 address settings for the SSL VPN AC interface



13. Create an address pool for IP access users:

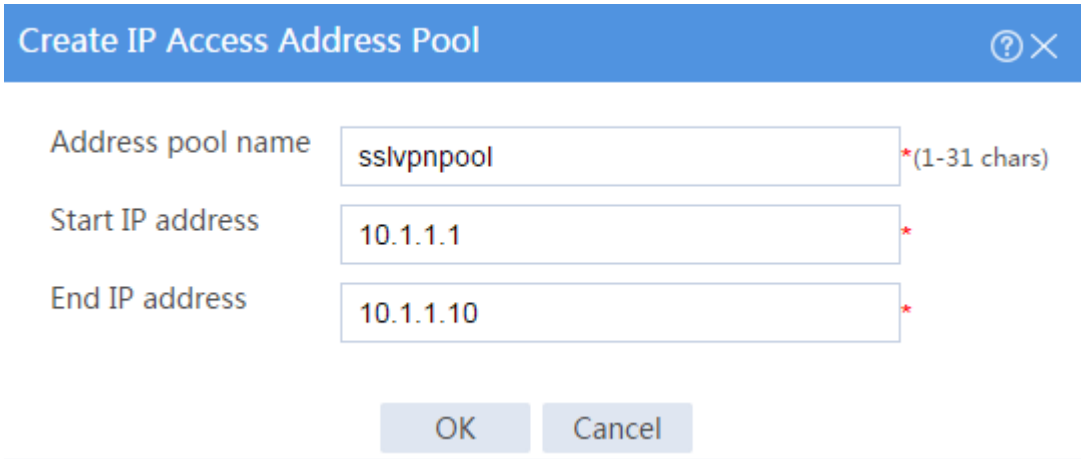
On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **IP Access Address Pools**.

Click **Create**.

Create an IP access address pool as shown in Figure 70, and then click **OK**.

Figure 70 Creating an IP access address pool



14. Configure an SSL VPN context:

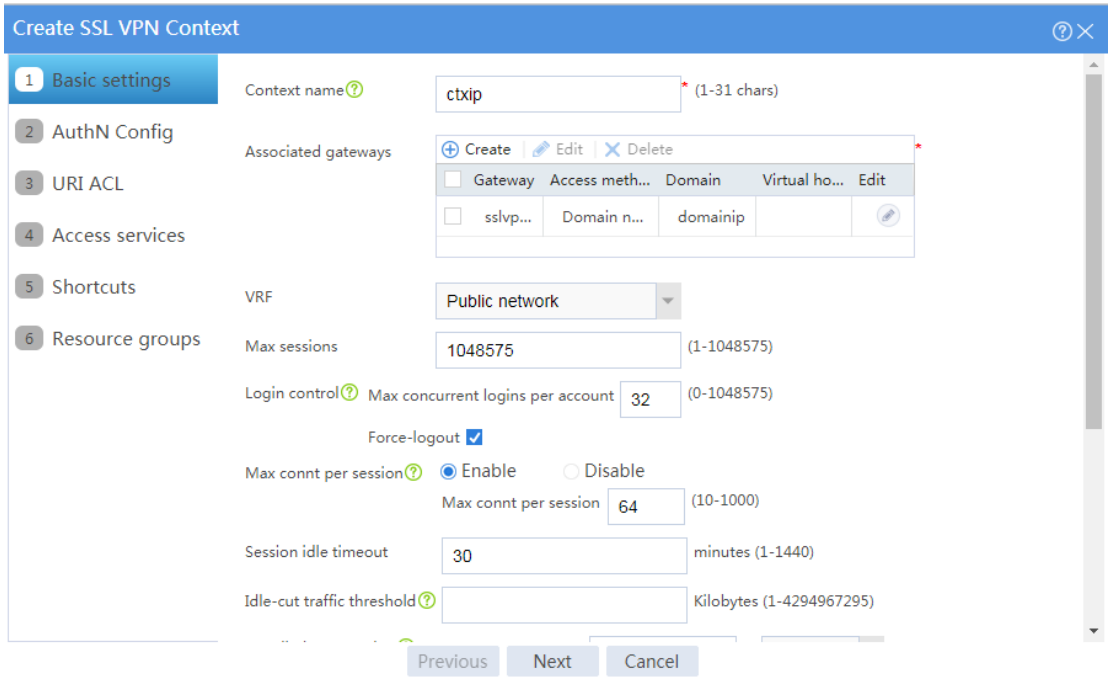
    # On the top navigation bar, click **Network**.

    # From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

    # Click **Create**.

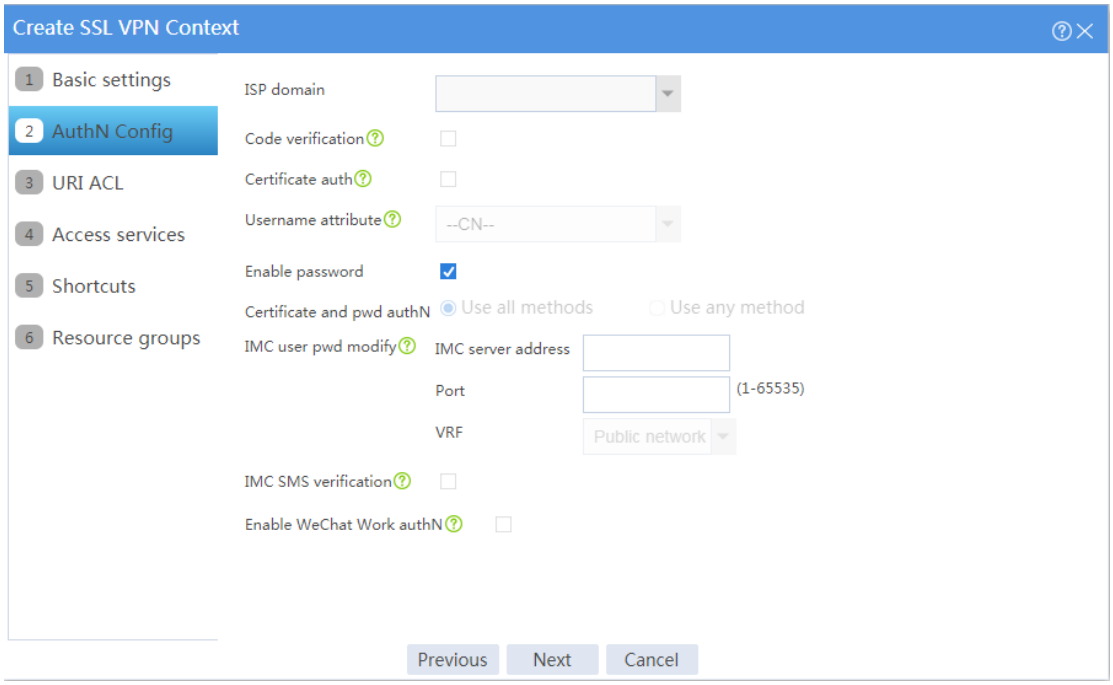
    # Configure the basic settings for the SSL VPN context as shown in Figure 71.

Figure 71 Configuring basic settings for an SSL VPN context



Click **Next** to configure authentication settings for the SSL VPN context as shown in Figure 72.

Figure 72 Configuring authentication settings



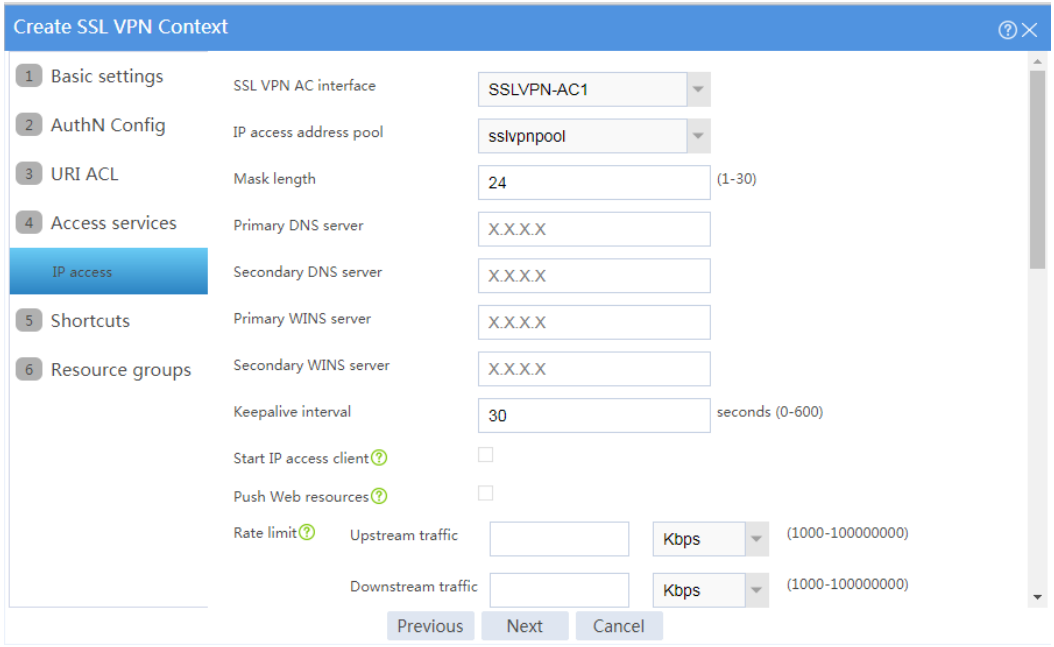
Click **Next**. On the **URI ACL** page that opens, click **Next**.

On the **Access services** page, select **IP access** and click **Next**.

On the **IP access** page, configure the IP access service as follows:

a. Configure the IP access parameters as shown in Figure 73 and click **Next**.

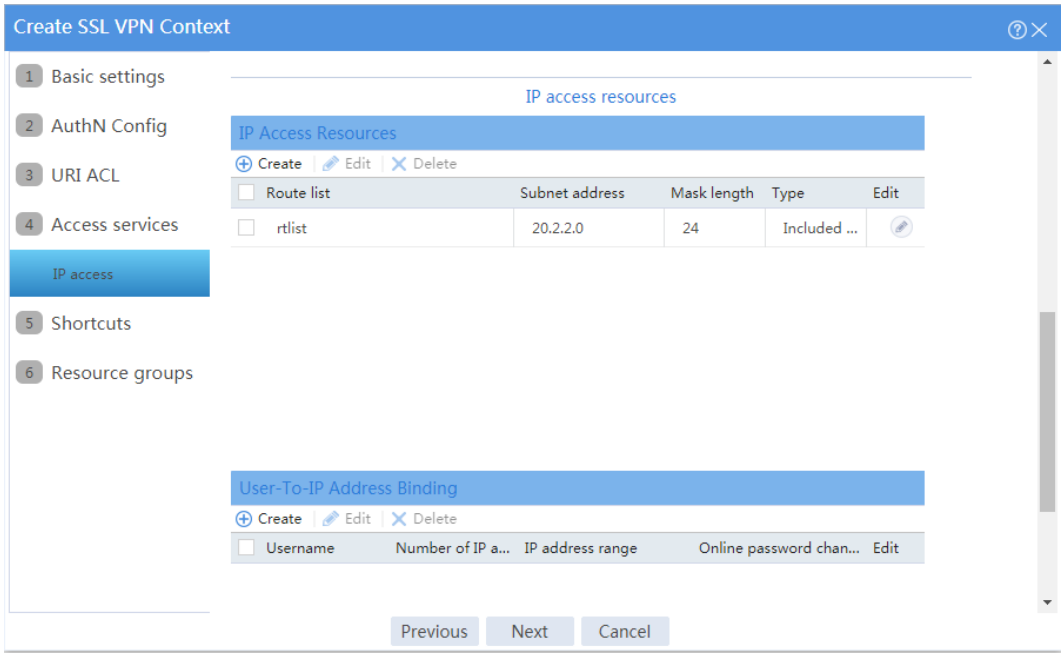
Figure 73 Configuring IP access parameters for the IP access service



b. In the **IP access resources** area, configure route list **rtlist** with an included route entry for 20.2.2.0/24, as shown in Figure 74.

c. Click **Next**.

Figure 74 Configuring IP access resources for the IP access service

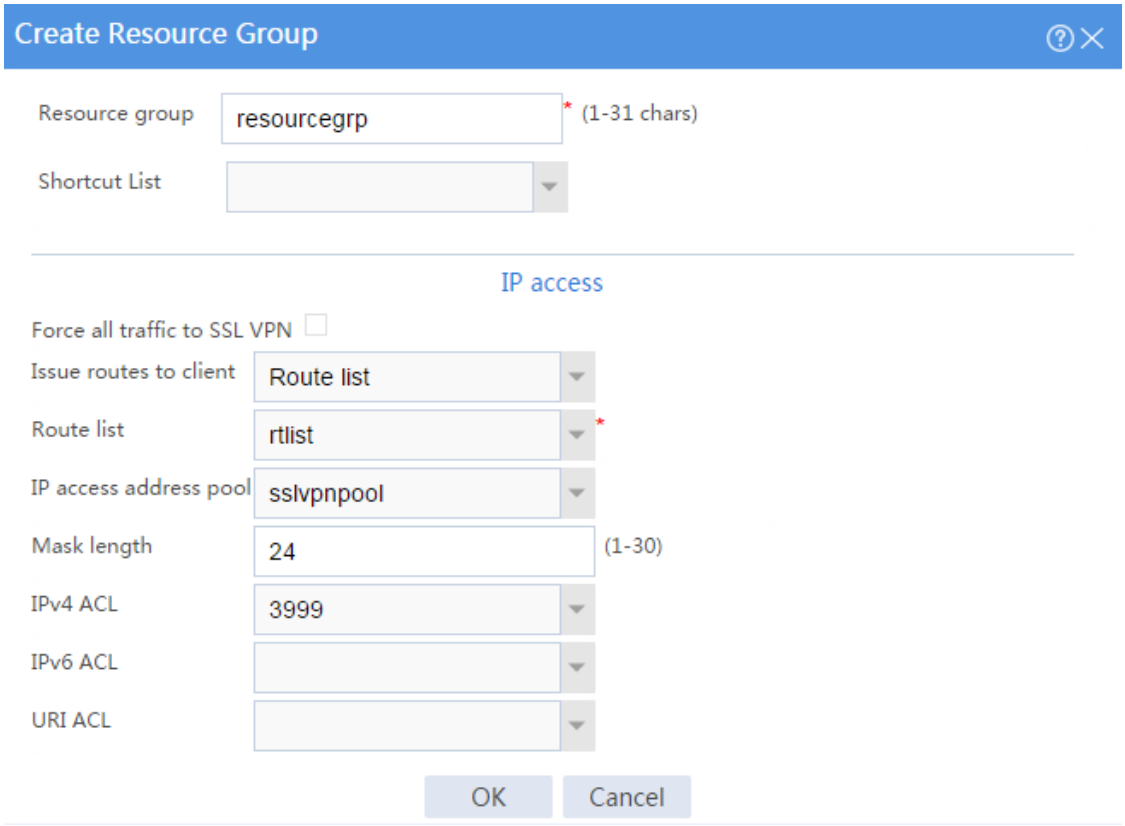


Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp**, as shown in Figure 75. In this example, select route list **rtlist** as the accessible IP resources and use IPv4 ACL 3999 (which permits all traffic) for IP access request filtering.

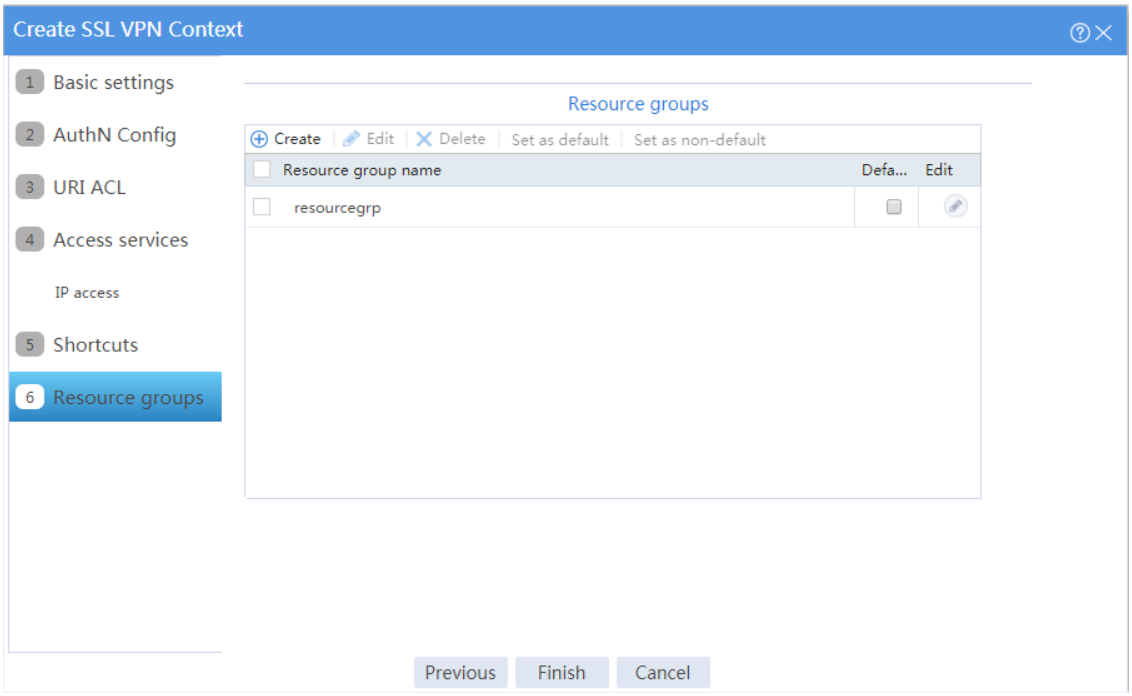
Figure 75 Creating an SSL VPN resource group



Click **OK**.

The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 76.

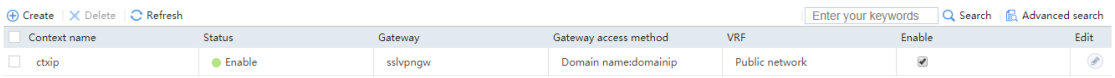
Figure 76 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 77.

Figure 77 Enabling the SSL VPN context



Configuring the LDAP server

1. Create user group **sslvpn_usergroup**:

On the LDAP server, start the Server Manager by selecting **Start** > **Administrative Tools** > **Server Manager**.

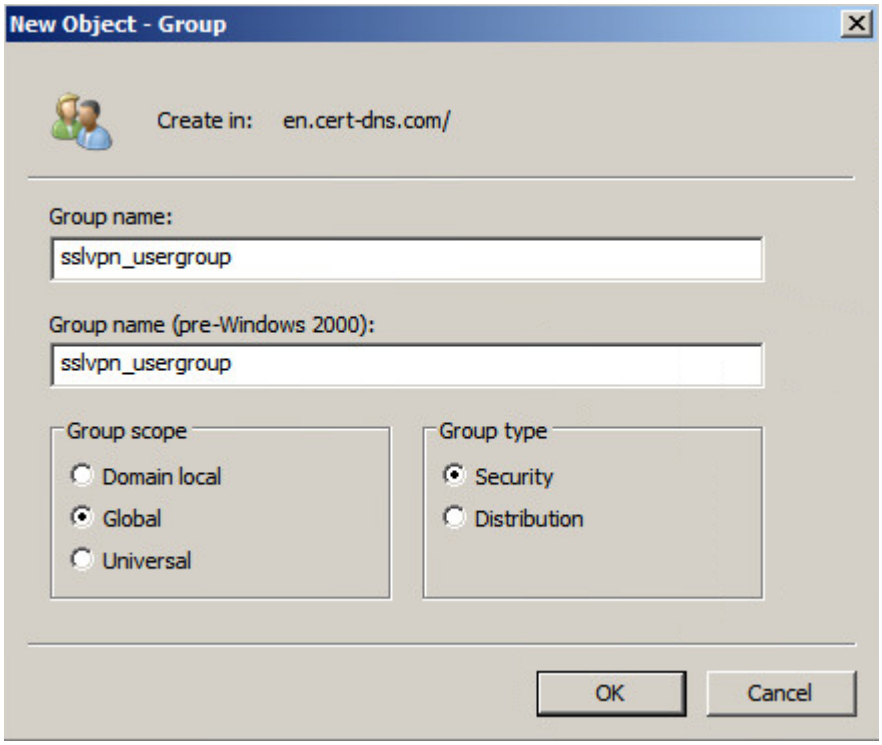
From the navigation pane, select **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers**.

Right-click **Users** under the **en.cert-dns.com** node, and then select **New** > **Group** from the shortcut menus.

Create user group **sslvpn_usergroup** as shown in Figure 78.

Click **OK**.

Figure 78 Creating a user group



2. Create user **user1** and add the user to user group **sslvpn_usergroup**:

   # On the LDAP server, start the Server Manager by selecting **Start** > **Administrative Tools** > **Server Manager**.

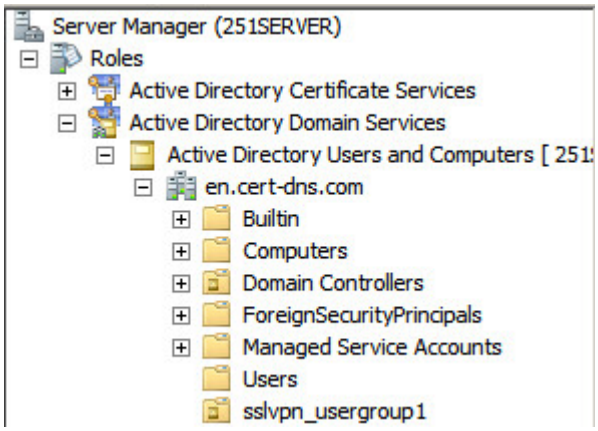
   # From the navigation pane, select **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers**.

   # Right-click the **en.cert-dns.com** node, and then select **New** > **Organizational Unit** from the shortcut menus.

   # Create organizational unit **sslvpn_usergroup**, as shown in Figure 79.

   # Click **OK**.

Figure 79 Creating an organizational unit

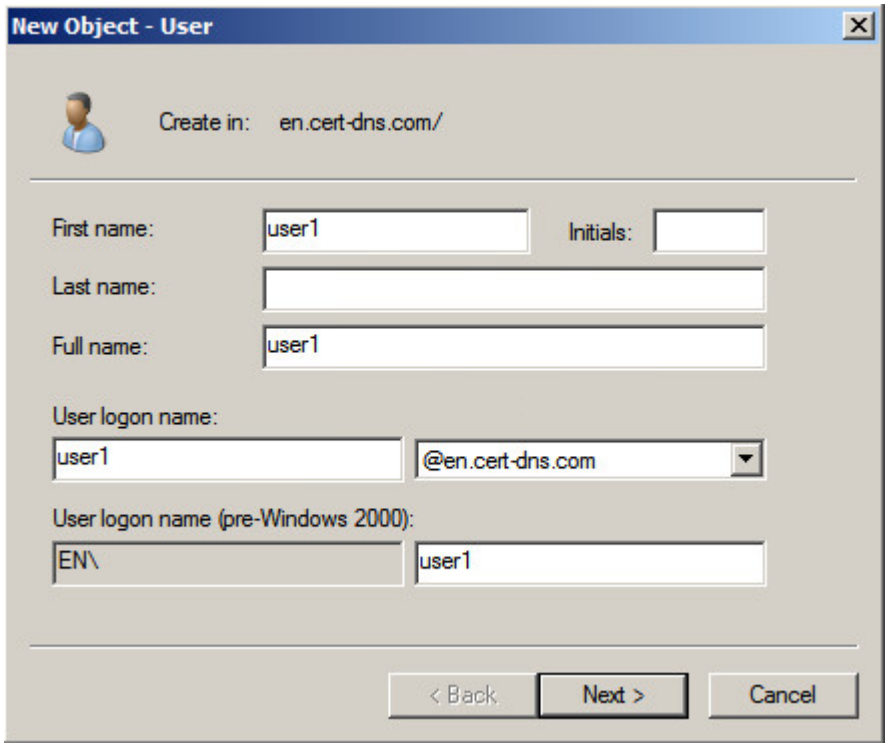


Right-click **sslvpn_usergroup**, and then select **New** > **User** from the shortcut menus.

Add user **user1** as shown in Figure 80.

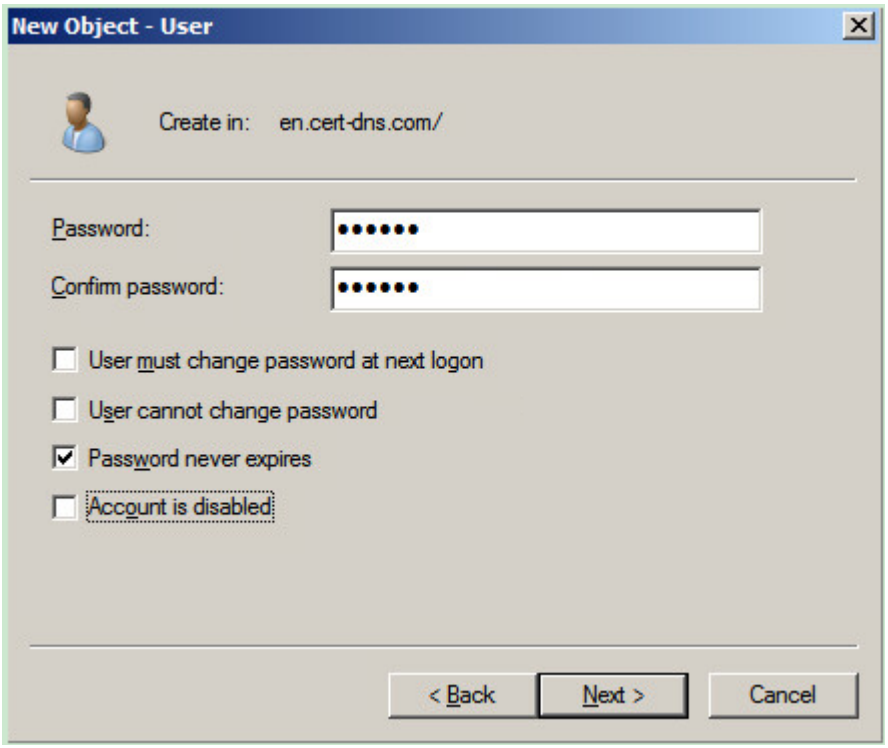
Click **Next**.

Figure 80 Adding LDAP user user1



On the page shown in Figure 81, enter password **123456**, select options as needed, and click **Next**.

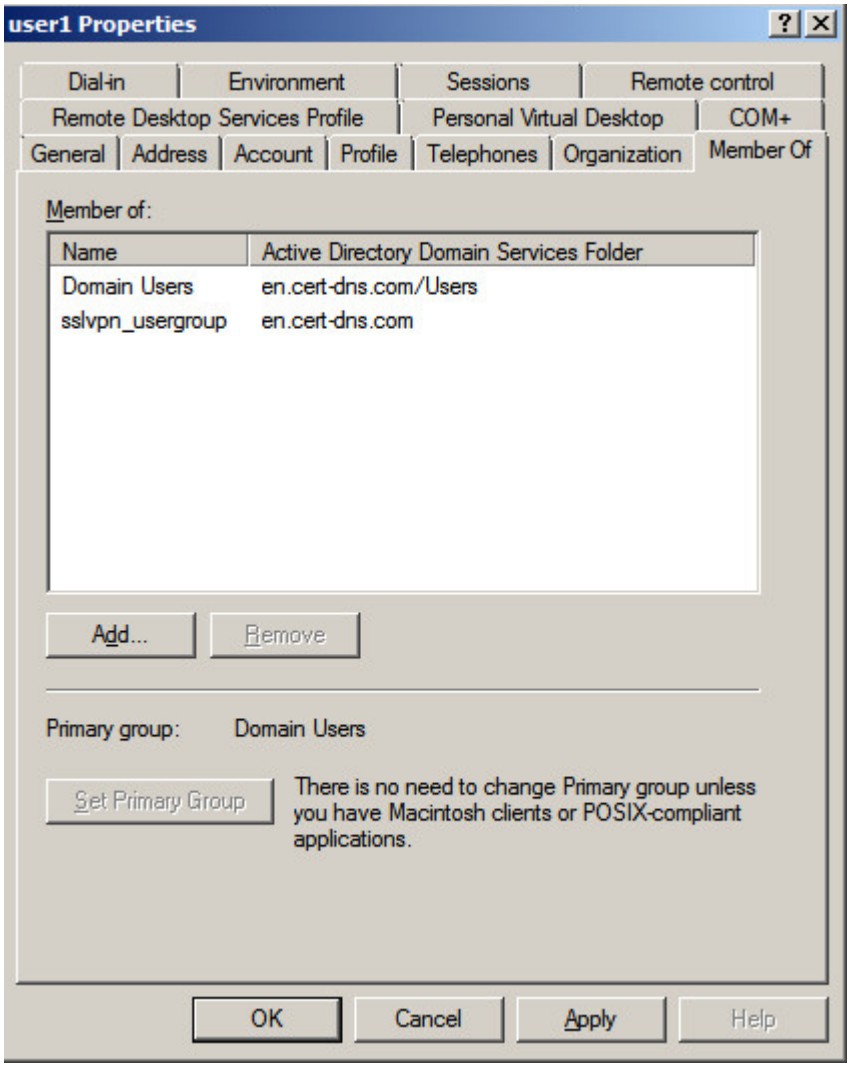
Figure 81 Setting the user's password



Right-click user **user1** and select **Properties**.

In the dialog box that opens, click the **Member Of** tab and add **user1** to user group **sslvpn_usergroup**, as show in Figure 82.

Figure 82 Modifying user properties

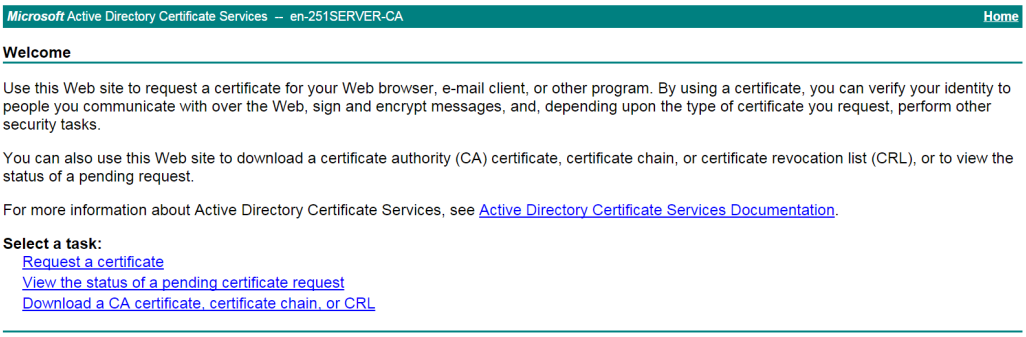


Click **OK**.

Configuring the host

1. Configure the IP address and gateway address settings for the host and make sure it can reach the SSL VPN gateway and the CA server.
2. Submit a client certificate request to the CA server:
   a. Enter **http://192.168.100.247/certsrv** in the browser address bar.
   b. On the certificate service home page shown in Figure 83, click **Request a certificate**.

Figure 83 Certificate service home page

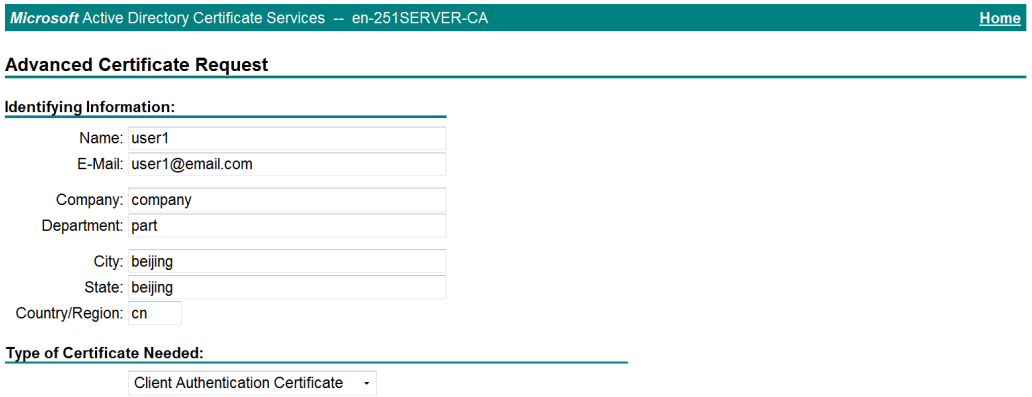


c. On the **Request a Certificate** page shown in Figure 84, click **advanced certificate request**.

Figure 84 Request a Certificate page

d. Create a client certificate request, as shown in Figure 85.

Figure 85 Creating a client certificate request



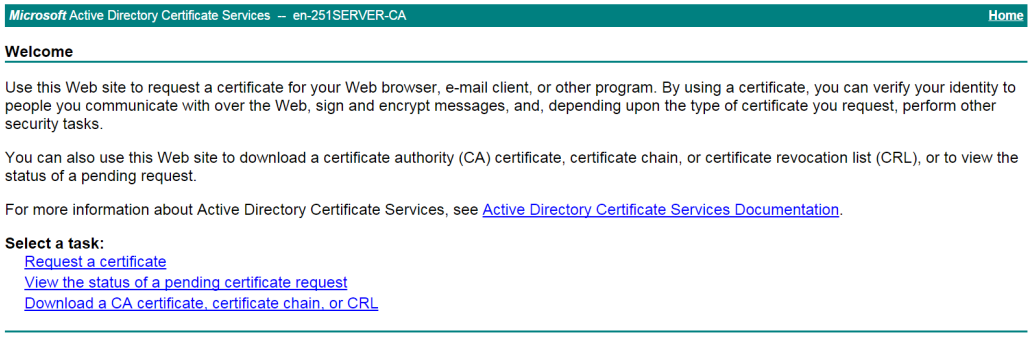
e. Click **Submit**.

3. Install the client certificate on the host:

a. After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

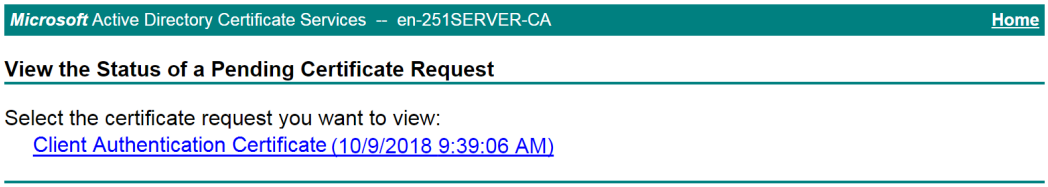
b. On the certificate service home page shown in Figure 86, click **View the status of a pending certificate request**.

Figure 86 Certificate service home page



The **View the Status of a Pending Certificate Request** page opens, as shown in Figure 87.

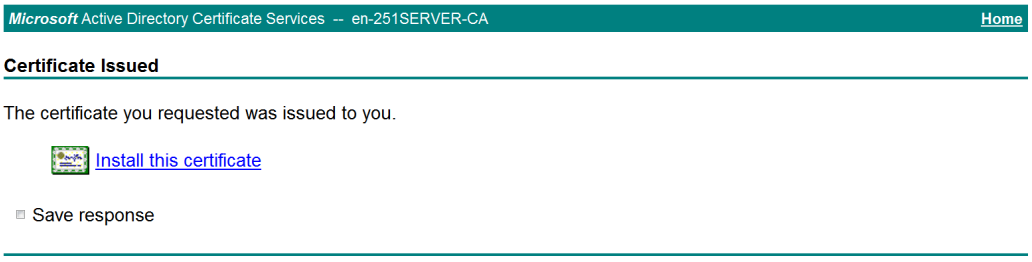
Figure 87 View the Status of a Pending Certificate Request page



c. Click the client certificate whose status you want to view.

d. On the **Certificate Issued** page shown in Figure 88, click **Install this certificate** to install the client certificate.

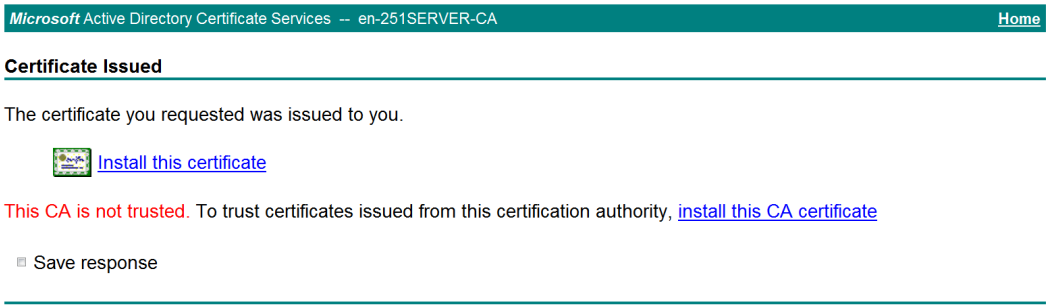
Figure 88 Installing the client certificate



If the host does not have a CA certificate, the page shown in Figure 89 opens. You must install the CA certificate first.

e. Click **install this CA certificate** to install the CA certificate. Then, click **Install this certificate** to install the client certificate.

Figure 89 Installing the CA certificate and then the client certificate



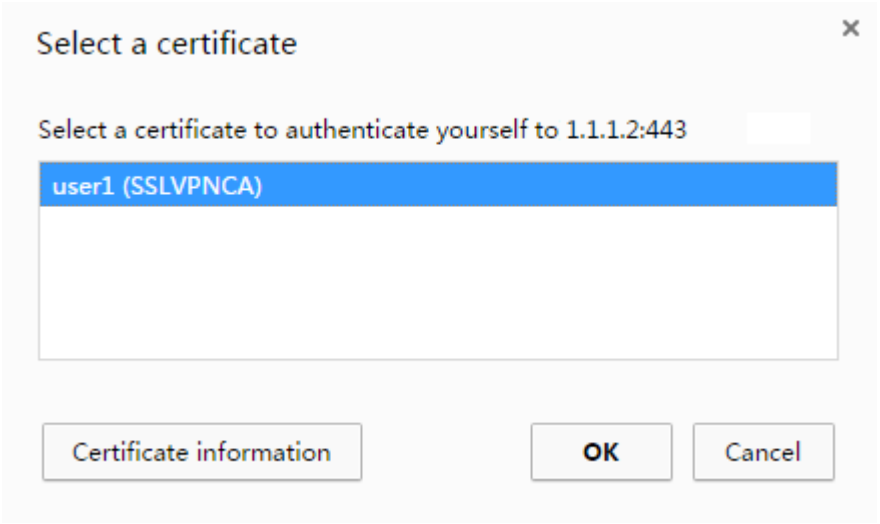
After the client certificate is installed, the **Certificate Installed** page shown in Figure 90 opens.

Figure 90 Certificate Installed page

Verifying the configuration

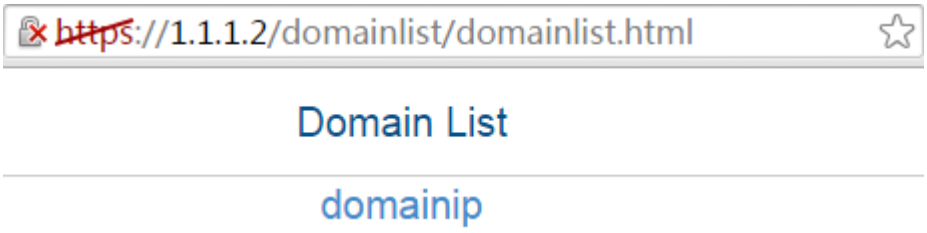
1. In the browser address bar of the host, enter **https://1.1.1.2** and press **Enter**.
2. On the **Select a certificate** page, select the client certificate for authentication, as shown in Figure 91.

Figure 91 Select a certificate page



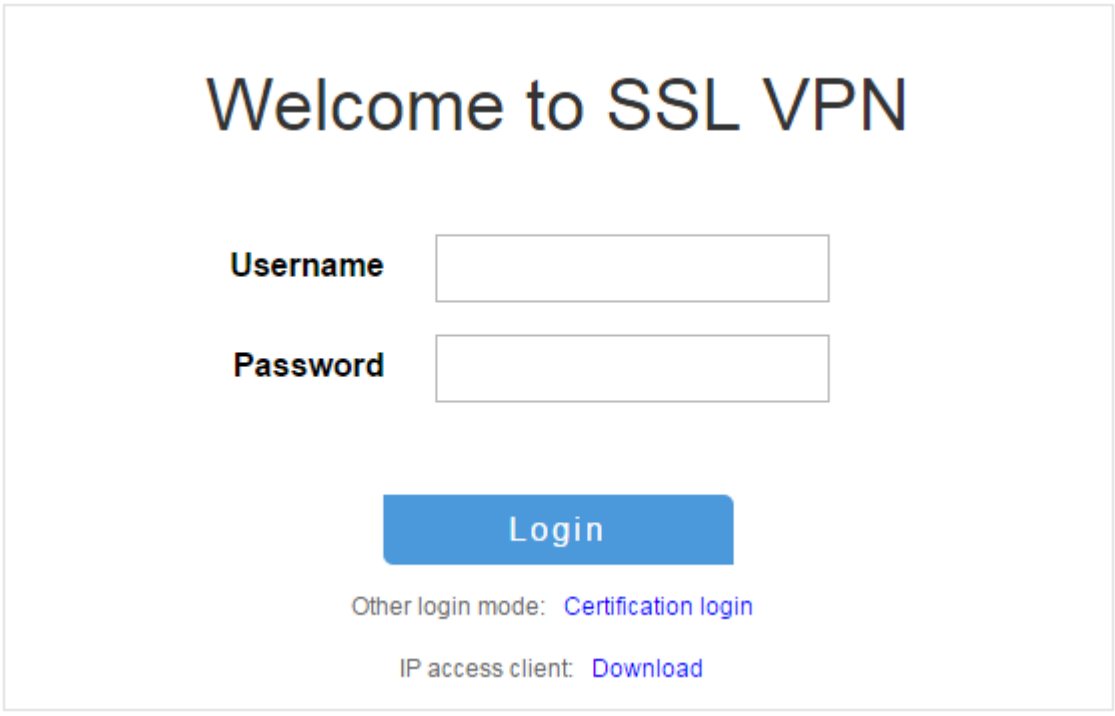
3. Click **OK**.
4. On the **Domain List** page shown in Figure 92, select **domainip** to access the login page.

Figure 92 Domain list page



5. Select **domainip** to access the login page.
6. On the login page, enter username **user1** and password **123456**, and then click **Login**.

Figure 93 Login page



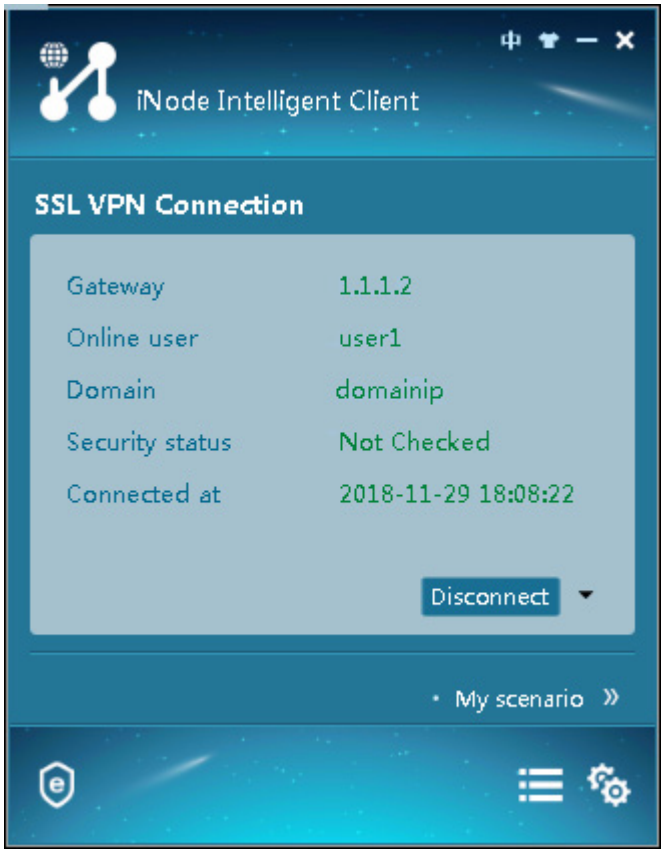
7. Click **START** to start the IP client application.

   If the host does not have an iNode client installed, the system installs the iNode client, and then starts and connects the iNode client to the SSL VPN gateway.

   If the host already has an iNode client installed, the system starts the iNode client and connects it to the SSL VPN gateway directly.

   Figure 94 shows that the iNode client is successfully connected to the SSL VPN gateway.

Figure 94 Connecting the iNode client to the SSL VPN gateway



Example: Configuring IP access with local authentication and a self-signed certificate

Network configuration

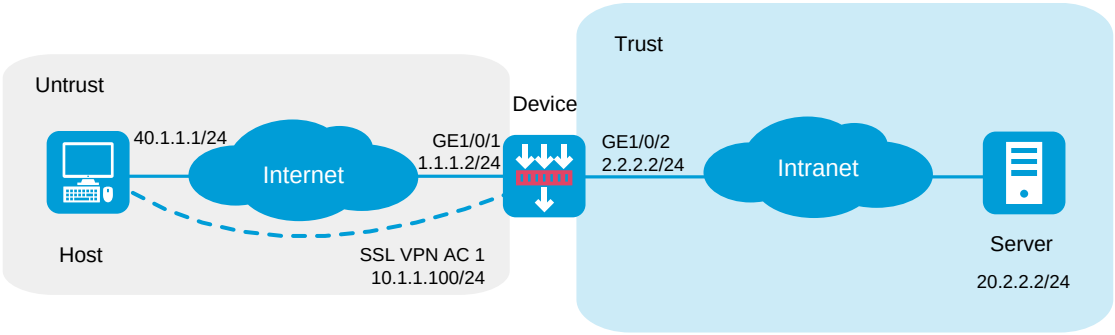
As shown in Figure 95, the device acts as an SSL VPN gateway that connects the public network and the private network. Users need secure access to the internal server in IP access mode.

The device uses a self-signed server certificate.

Perform the following tasks:

- Configure the SSL VPN IP access service on the device to allow users to access the internal server in IP access mode.
- Configure the device to perform local authentication and authorization for IP access users.

Figure 95 Network diagram (local authentication)



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

- The IP address pool configured for client address allocation must meet the following requirements:
  - The address range of the address pool cannot be on the same subnet as the IP address used on the client host.
  - The IP addresses in the address pool do not conflict with the IP addresses used on the device.
  - The address range of the address pool cannot be on the same subnet as the IP address of the internal server.
- The SSL VPN AC interface must be added to the correct security zone (**Untrust**, in this example).

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click the **Network** tab.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

   # Add GE 1/0/3 to the **Trust** security zone and set its IP address to 3.3.3.1/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

   This example configures static routes.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static IPv4 route to reach 40.1.1.1:

   a. Enter destination IP address **40.1.1.1**.

   b. Enter mask length **24**.

   c. Enter next hop address **1.1.1.3**.

   d. Use the default settings for other parameters.

   e. Click **OK**.

Configure a static IPv4 route to reach 20.2.2.2:

a. Enter destination IP address **20.2.2.2**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **2.2.2.2**.

- Select destination IPv4 address **20.2.2.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **untrust-trust** to permit the specified traffic from the **Untrust** to **Trust** security zones:

- Enter policy name **untrust-trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.0/24**.
- Select destination IPv4 address **20.2.2.0/24**.
- Use the default settings for other parameters.

Click **OK**.

4. Configure the SSL VPN gateway:

On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

Click **Create**.

Create an SSL VPN gateway as shown in Figure 96, and then click **OK**.

Figure 96 Creating an SSL VPN gateway

5. Create an SSL VPN AC interface:

   # On the top navigation bar, click **Network**.

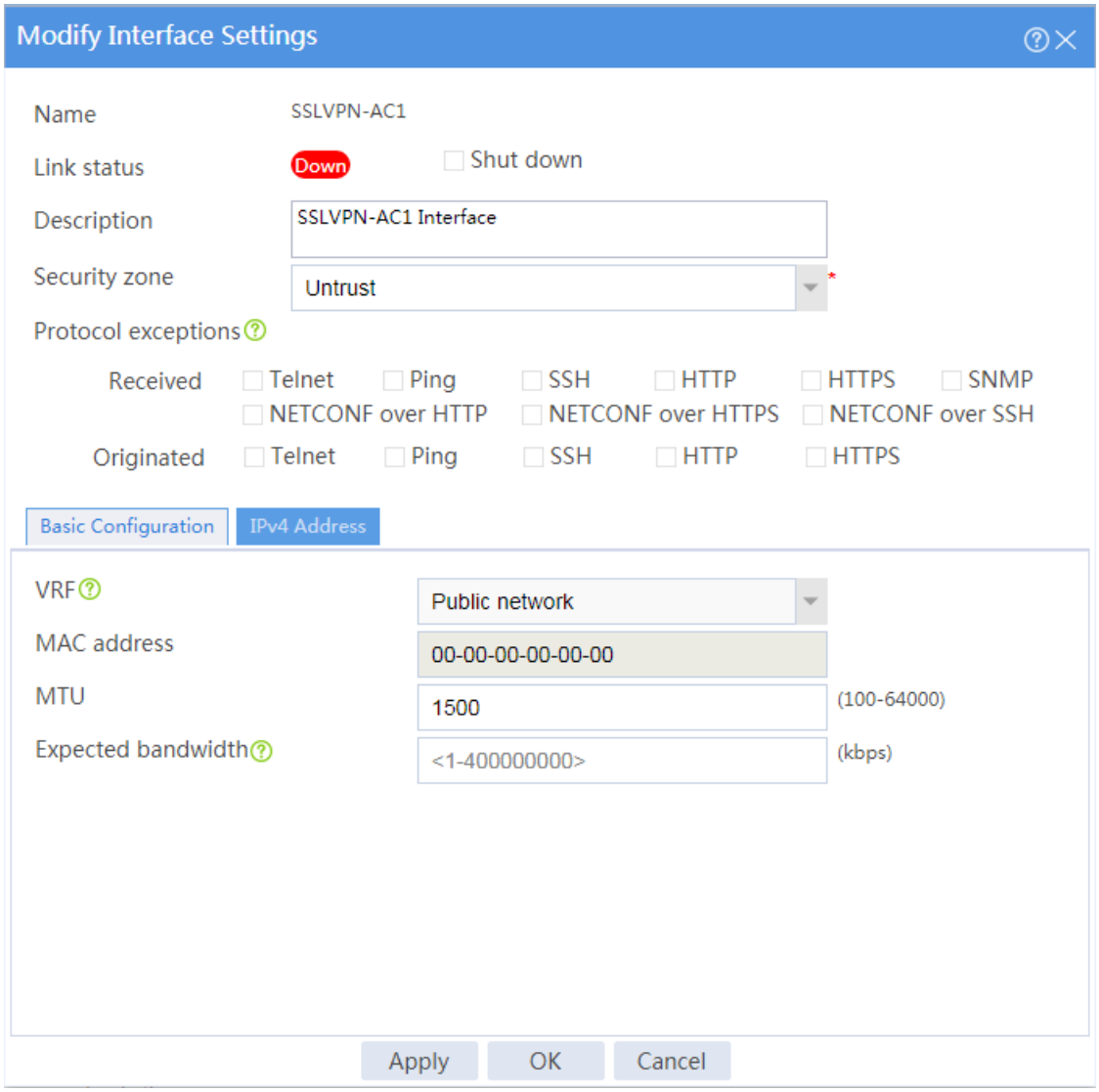
   # From the navigation pane, select **SSL VPN** > **SSL VPN AC Interfaces**.

   # Click **Create**.

   # In the **Create Interfaces** dialog box that opens, enter **1** in the **Interface number** field and click **OK**.

   # In the **Modify Interface Settings** dialog box, configure the basic settings for the SSL VPN AC interface as shown in Figure 97.

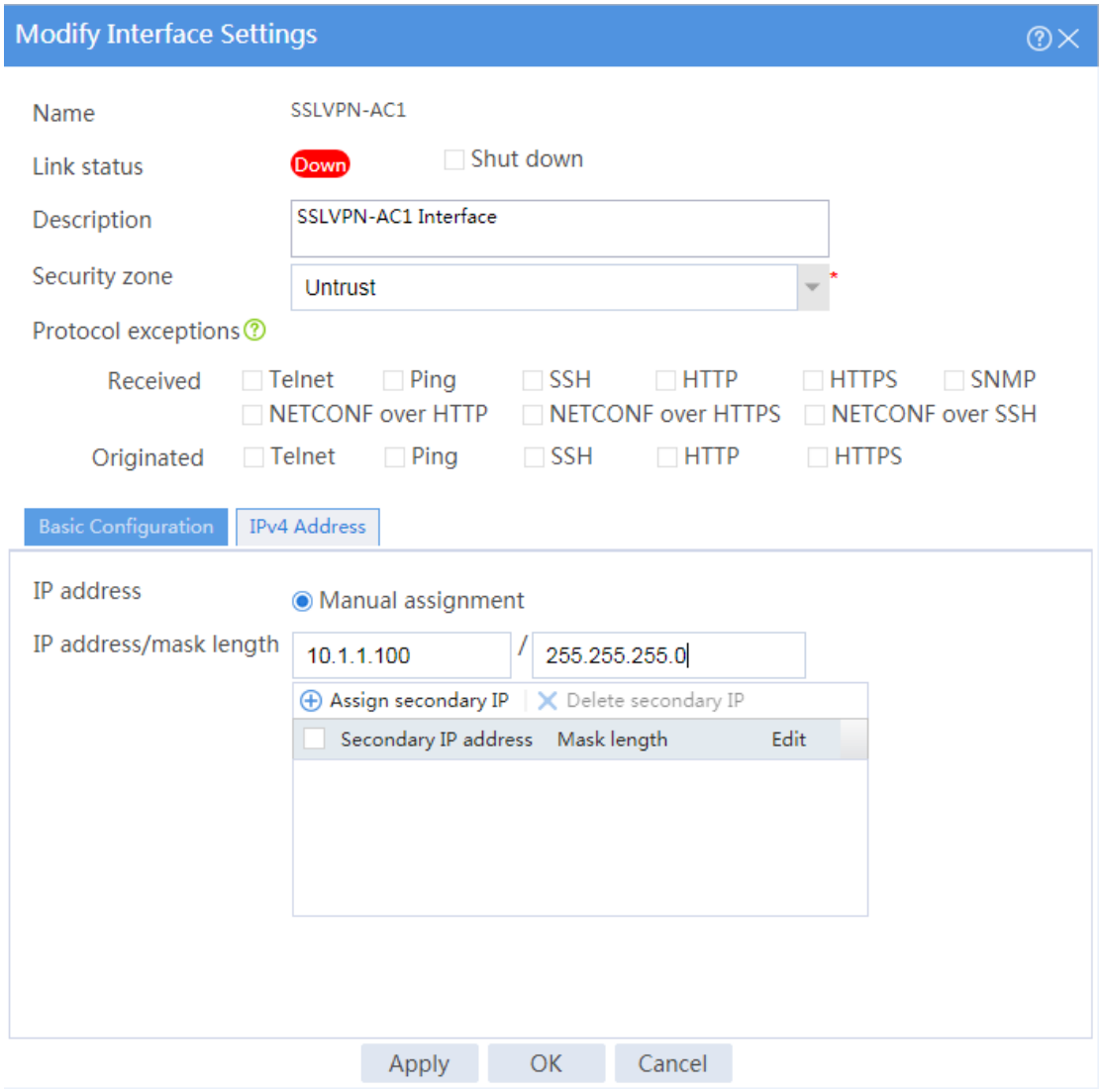
Figure 97 Configuring basic settings for the SSL VPN AC interface



Click the **IPv4 Address** tab and configure the IPv4 address settings for the SSL VPN AC interface as shown in Figure 98.

Click **OK**.

Figure 98 Configuring IPv4 address settings for the SSL VPN AC interface



6. Create an address pool for IP access users:

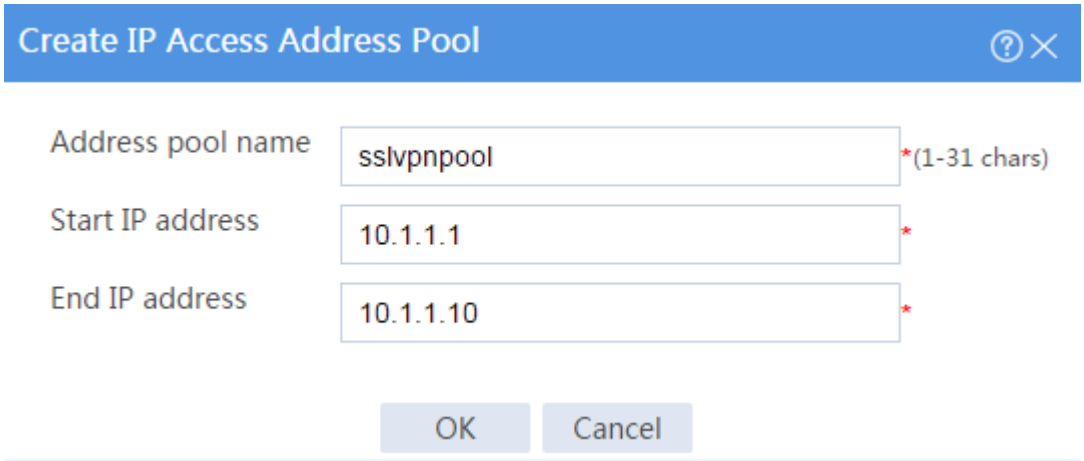
   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **SSL VPN** > **IP Access Address Pools**.

   # Click **Create**.

   # Create an IP access address pool as shown in Figure 99, and then click **OK**.

Figure 99 Creating an IP access address pool



7. Configure an SSL VPN context:

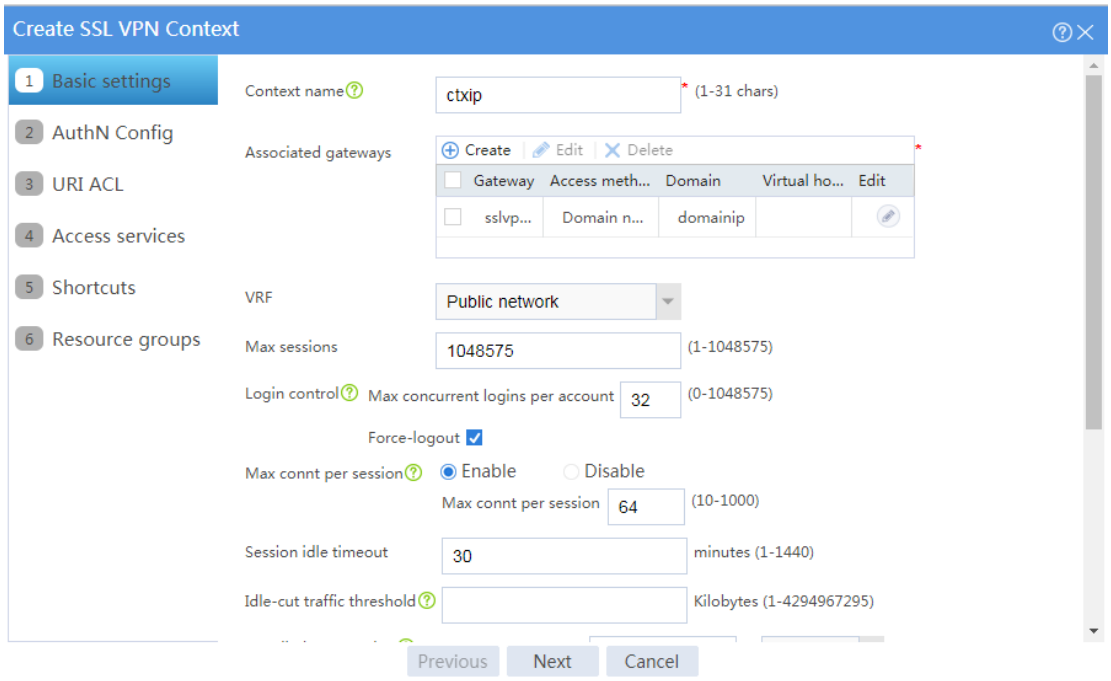
   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

   # Click **Create**.

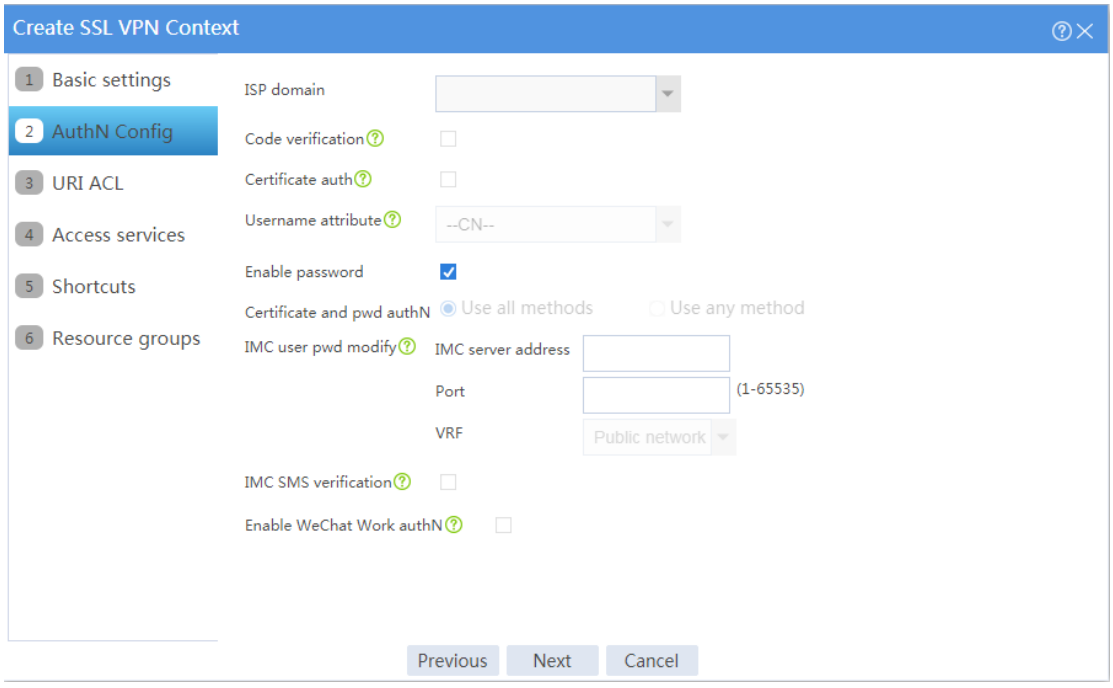
   # Configure the basic settings for the SSL VPN context as shown in Figure 100, and then click **Next**.

Figure 100 Configuring basic settings for an SSL VPN context



Click **Next** to configure authentication settings for the SSL VPN context as shown in Figure 101.

Figure 101 Configuring authentication settings



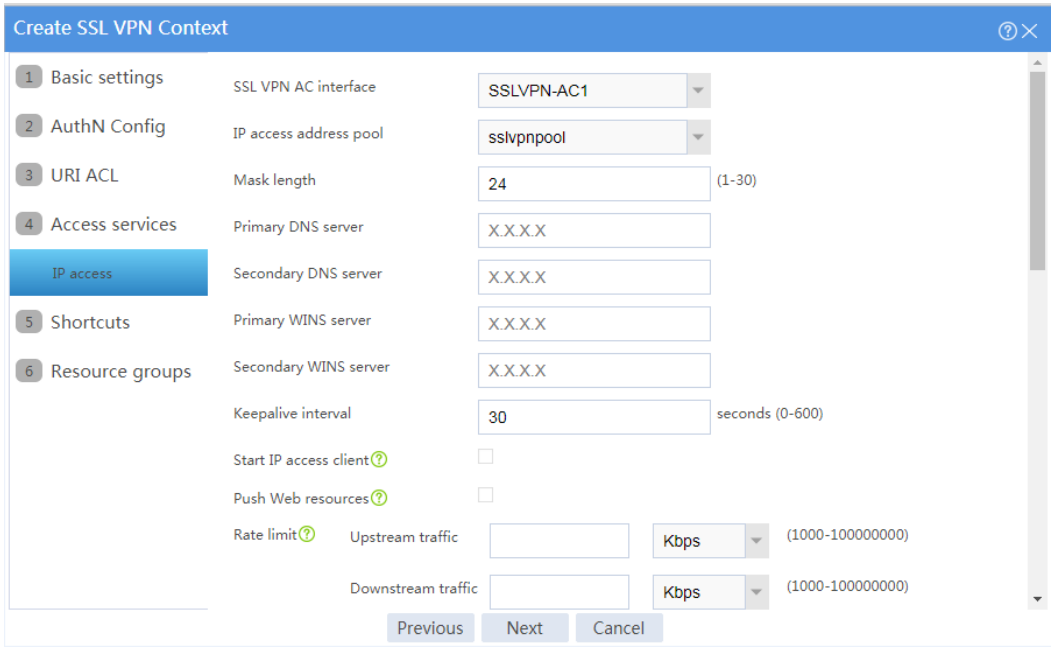
Click **Next**. On the **URI ACL** page that opens, click **Next**.

On the **Access services** page, select **IP access** and click **Next**.

On the **IP access** page, configure the IP access service as follows:

a. Configure the IP access parameters as shown in Figure 102 and click **Next**.

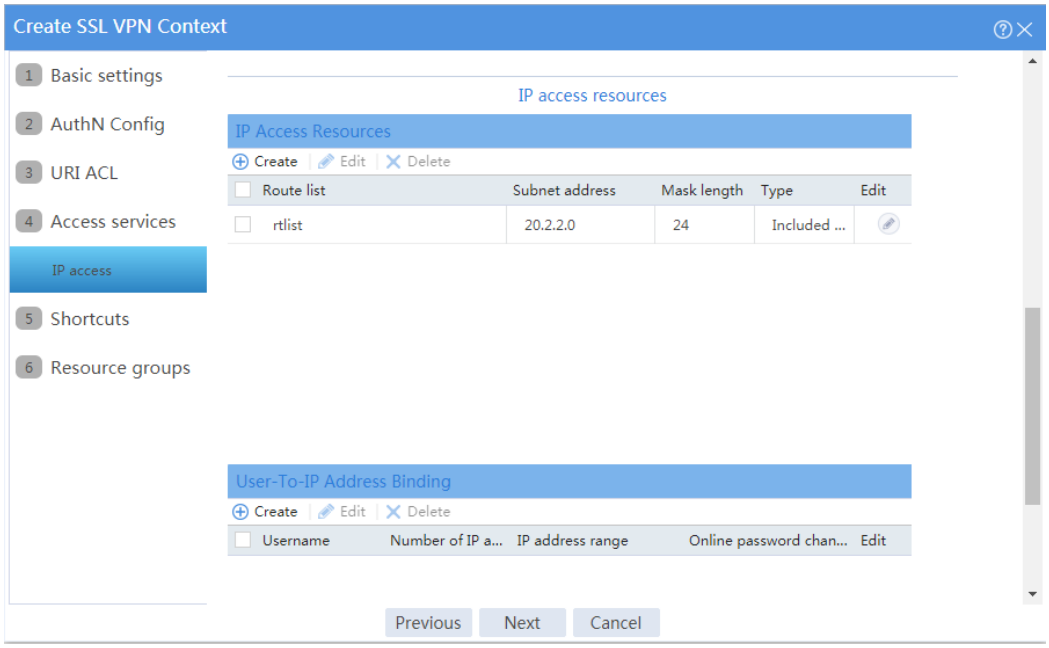
Figure 102 Configuring IP access parameters for the IP access service



b. In the **IP access resources** area, configure route list **rtlist** with an included route entry for 20.2.2.0/24, as shown in Figure 103.

c. Click **Next**.

Figure 103 Configuring IP access resources for the IP access service

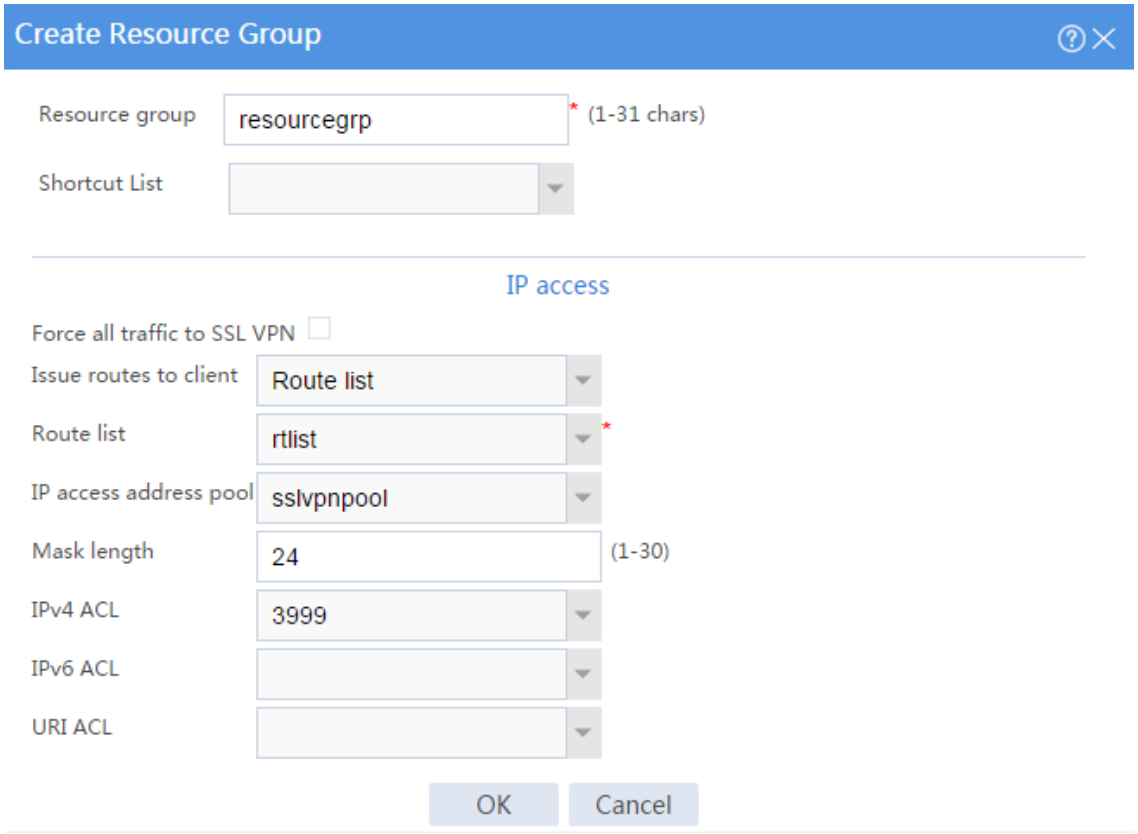


Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp**, as shown in Figure 104. In this example, select route list **rtlist** as the accessible IP resources and use IPv4 ACL 3999 (which permits all traffic) for IP access request filtering.

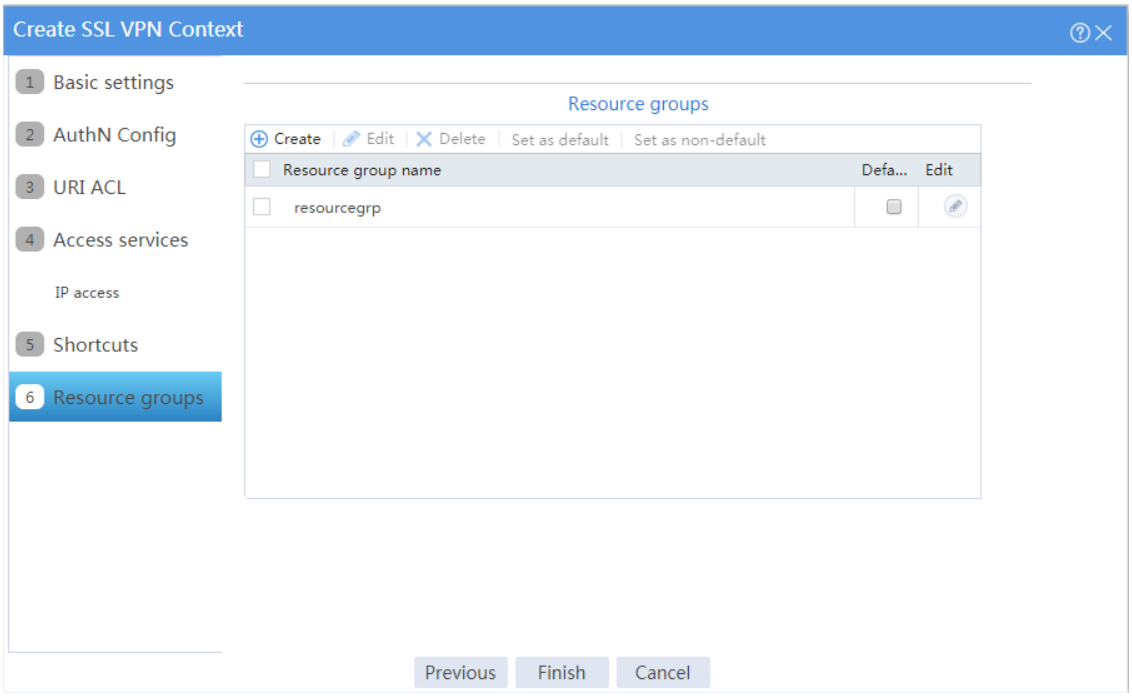
Figure 104 Creating an SSL VPN resource group



Click **OK**.

The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 105.

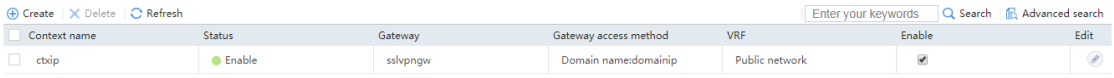
Figure 105 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 106.

Figure 106 Enabling the SSL VPN context



8. Create an SSL VPN user:

On the top navigation bar, click **Objects**.

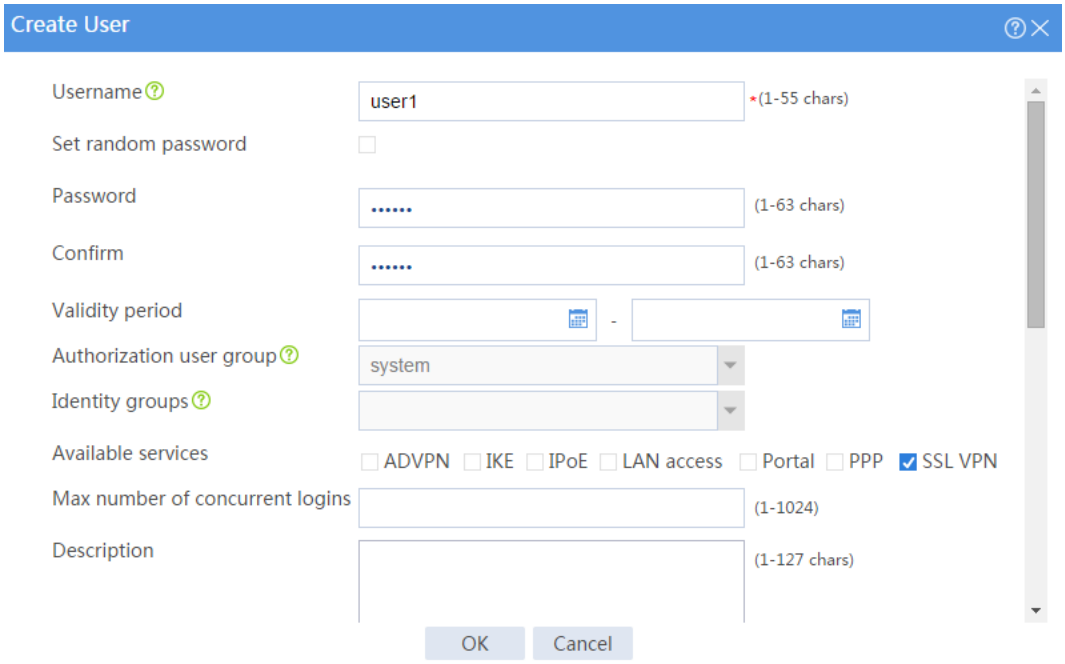
From the navigation pane, select **User** > **User Management** > **Local Users**.

Click **Create**.

Create an SSL VPN user:

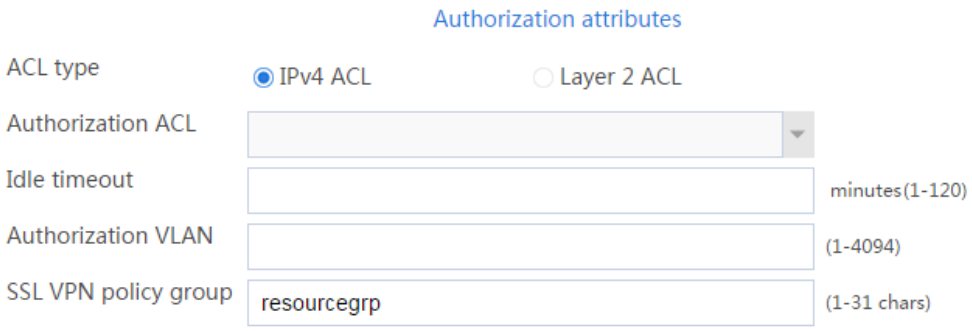
a. Set the username to **user1** and password to **123456**, and select **SSL VPN** as the available service, as shown in Figure 107.

Figure 107 Creating an SSL VPN user



b. In the **Authorization Attributes** area, authorize the user to use SSL VPN resource group **resourcegrp**, as shown in Figure 108.

Figure 108 Setting the authorization attributes for the SSL VPN user



c. Click **OK**.

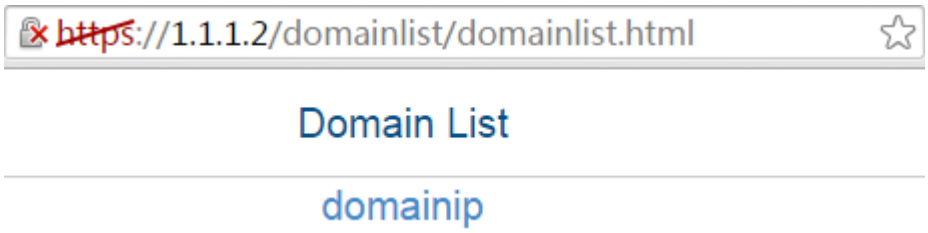
Configuring the host

Configure the IP address and gateway address settings for the host and make sure it can reach the SSL VPN gateway.

Verifying the configuration

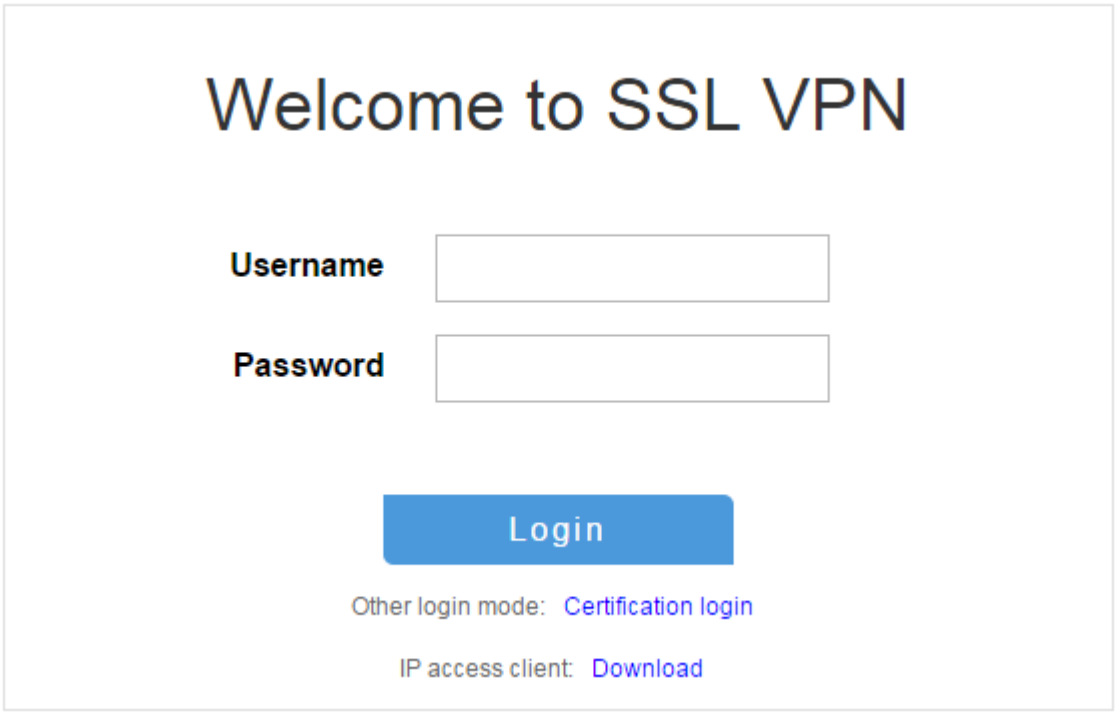
1. In the browser address bar of the host, enter **https://1.1.1.2** and press **Enter** to open the domain list page.

Figure 109 Domain list page



2. Select **domainip** to access the login page.
3. On the login page, enter username **user1** and password **123456**, and then click **Login**.

Figure 110 Login page



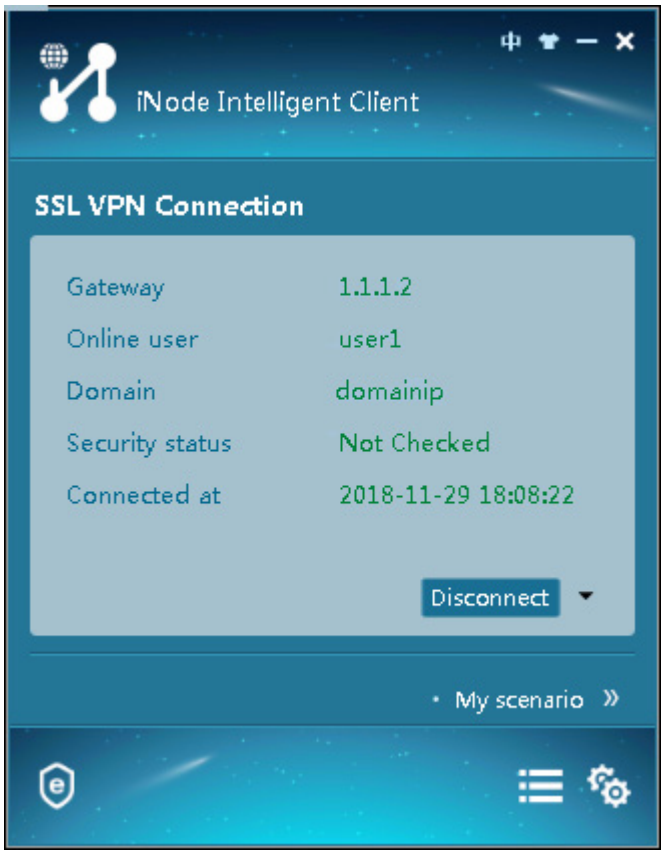
4. Click **START** to start the IP client application.

   If the host does not have an iNode client installed, the system installs the iNode client and connects the iNode client to the SSL VPN gateway.

   If the host already has an iNode client installed, the system starts the iNode client and connects it to the SSL VPN gateway directly.

   Figure 111 shows that the iNode client is successfully connected to the SSL VPN gateway.

Figure 111 Connecting the iNode client to the SSL VPN gateway



Example: Configuring IP access with USB key certificate authentication

Network configuration

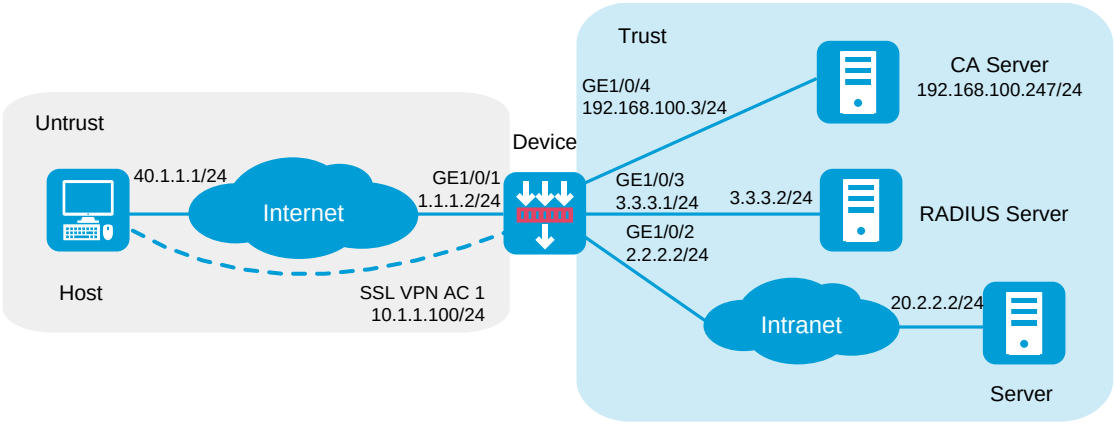
As shown in Figure 112, the device acts as an SSL VPN gateway that connects the public network and the private network. Users need secure access to the internal server in IP access mode.

The device uses a RADIUS server to perform remote authentication and authorization for IP access users.

To enhance security, configure the device to authenticate the client certificate. The client certificate is provided by a USB key.

To enhance security, the device uses a CA-signed server certificate instead of a self-signed server certificate.

Figure 112 Network diagram (USB key authentication)



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

- The IP address pool configured for client address allocation must meet the following requirements:
  - The address range of the address pool cannot be on the same subnet as the IP address used on the client host.
  - The IP addresses in the address pool do not conflict with the IP addresses used on the device.
  - The address range of the address pool cannot be on the same subnet as the IP address of the internal server.
- The SSL VPN AC interface must be added to the correct security zone (**Untrust**, in this example).
- Install the driver for the USB key to ensure availability of the USB key.
- The specified attribute (CN attribute by default) in the client certificate of the USB key is the same as the username of the SSL VPN user.

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click the **Network** tab.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 3.3.3.1/24 in the same way you configure GE 1/0/1.

Add GE 1/0/4 to the **Trust** security zone and set its IP address to 192.168.100.3/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

This example configures static routes.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static IPv4 route to reach 40.1.1.1:

a. Enter destination IP address **40.1.1.1**.

b. Enter mask length **24**.

c. Enter next hop address **1.1.1.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 20.2.2.2:

f. Enter destination IP address **20.2.2.2**.

g. Enter mask length **24**.

h. Enter next hop address **2.2.2.3**.

i. Use the default settings for other parameters.

j. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 addresses **2.2.2.2**, **3.3.3.1**, and **192.168.100.3**.
- Select destination IPv4 address **20.2.2.2**, **3.3.3.2**, and **192.168.100.247**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **untrust-trust** to permit the specified traffic from the **Untrust** to **Trust** security zones:

- Enter policy name **untrust-trust**.
- Select source zone **Untrust**.

- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.0/24**.
- Select destination IPv4 address **20.2.2.0/24**.
- Use the default settings for other parameters.

Click **OK**.

4. Request a server certificate for the device:

a. Create a certificate subject:

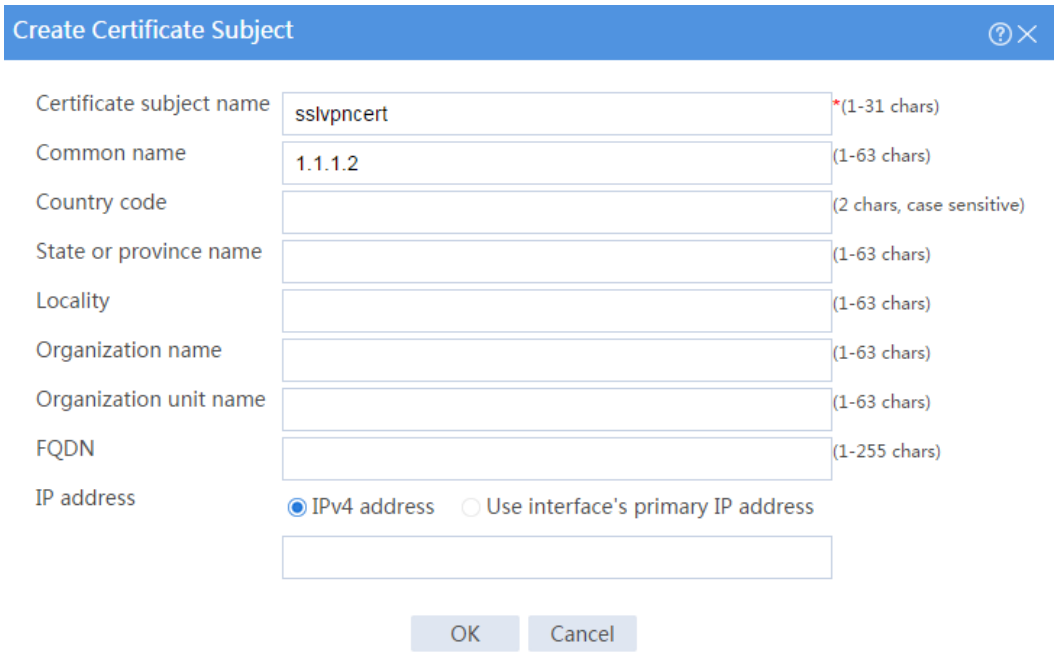
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate Subject**.

Click **Create**.

Create a certificate subject as shown in Figure 113, and the click **OK**.

Figure 113 Creating a certificate subject

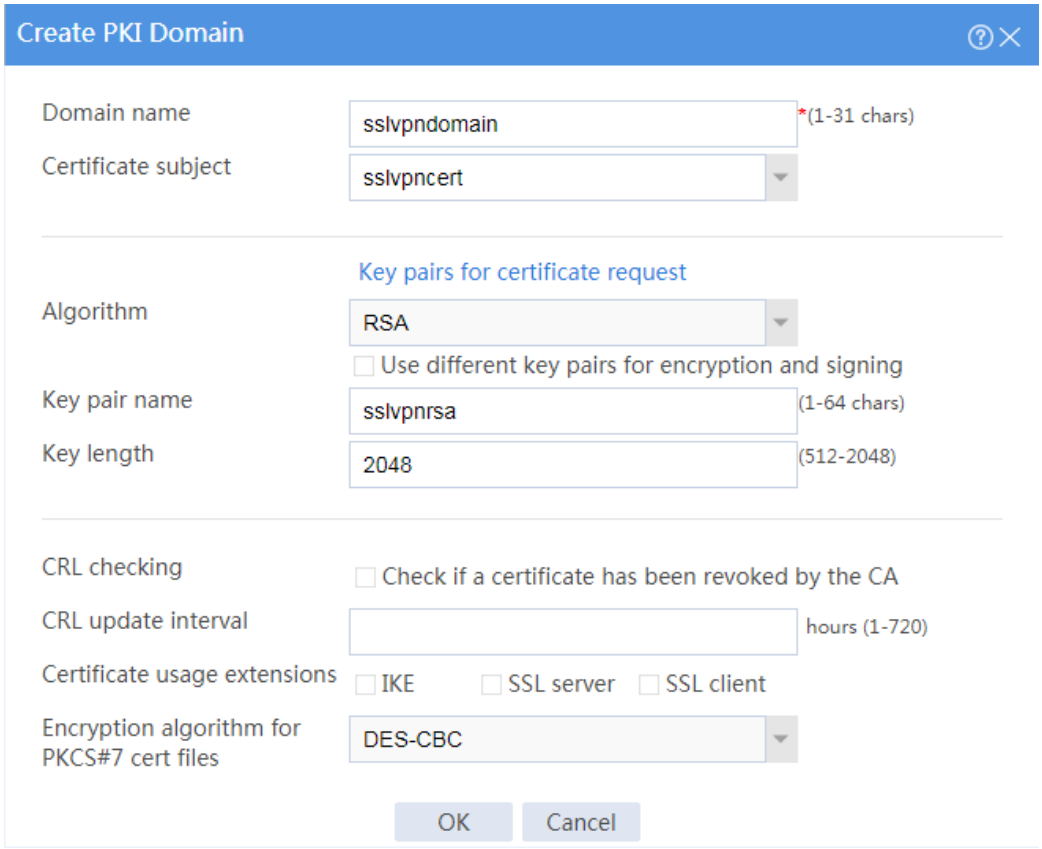


b. Create a PKI domain:

On the **Certificate** page, click **Create PKI domain**.

Create a PKI domain as shown in Figure 114, and then click **OK**.

Figure 114 Creating a PKI domain

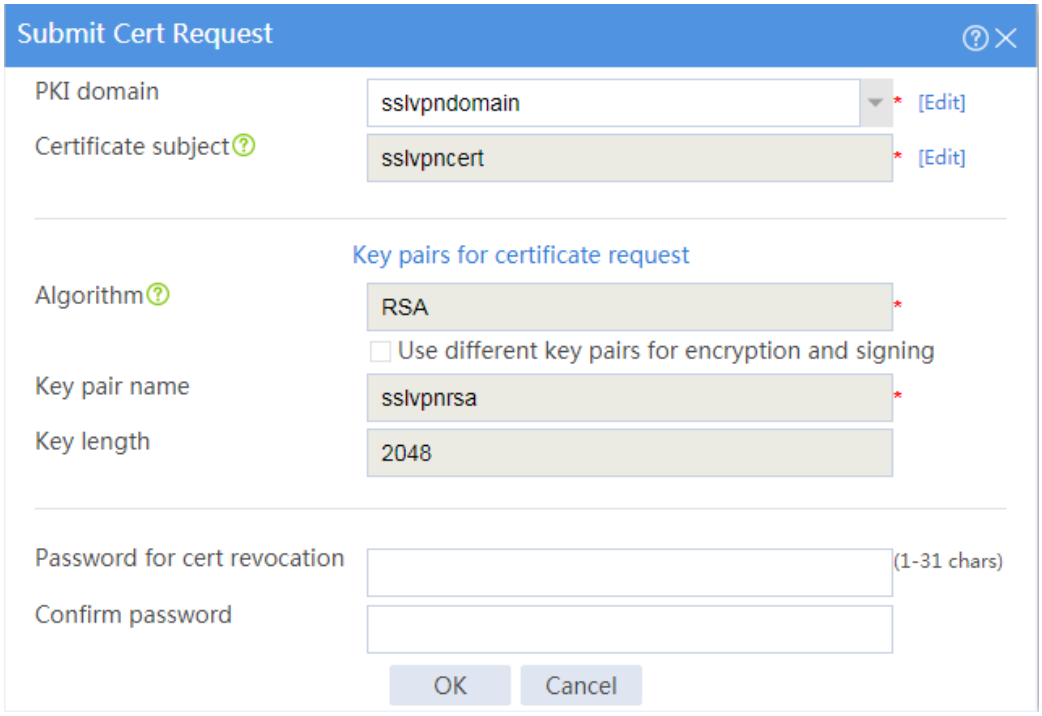


c. Create a certificate request:

On the **Certificate** page, click **Submit Cert Request**.

Configure the certificate request settings as shown in Figure 115.

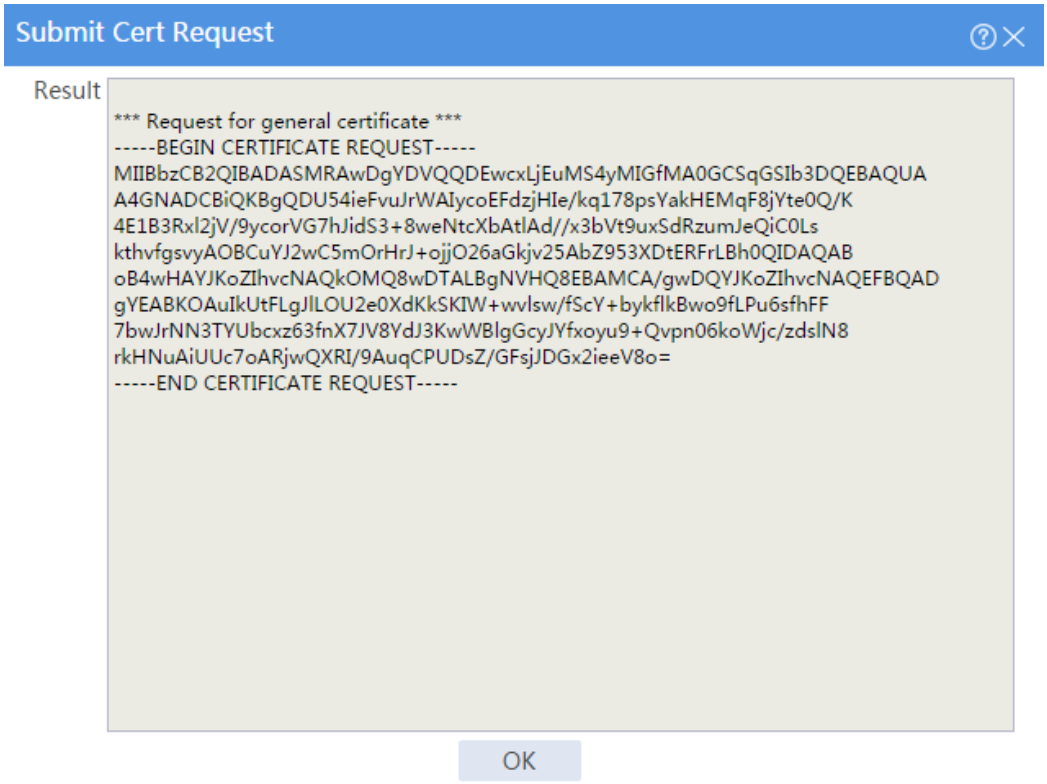
Figure 115 Creating a certificate request



Click **OK**.

The certificate request content will be displayed, as shown in Figure 116.

Figure 116 Certificate request content



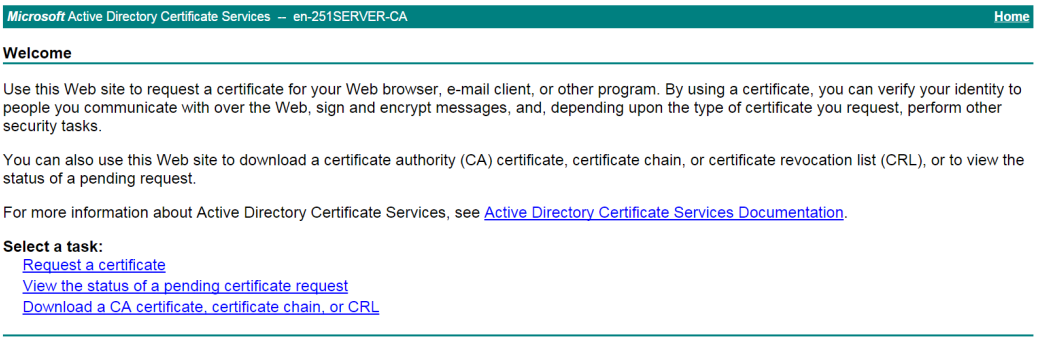
Copy the certificate request content and click **OK**.

d. Request a server certificate from the CA (Windows Server 2008 R2 in this example):

Enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 117, click **Request a certificate**.

Figure 117 Certificate service home page

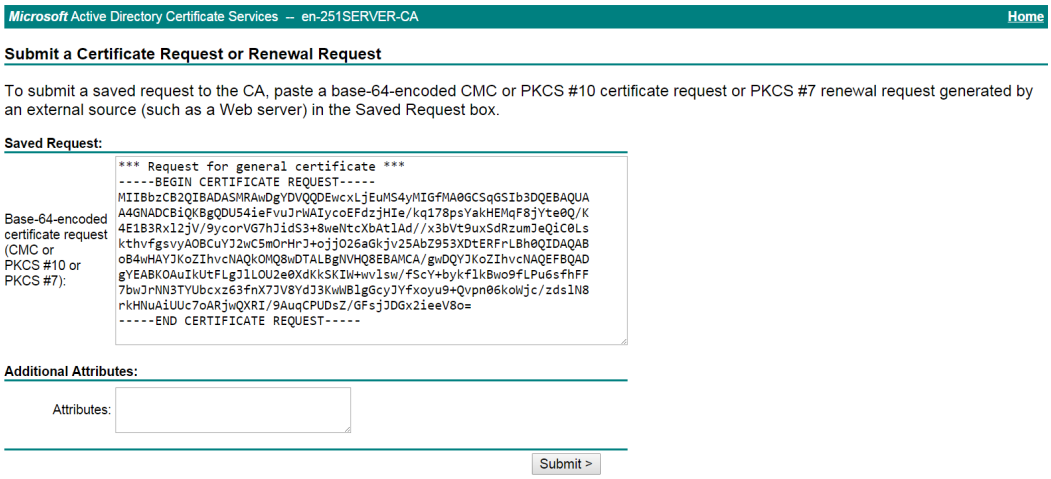


On the **Request a Certificate** page shown in Figure 118, click **advanced certificate request**.

Figure 118 Request a Certificate page

Paste the previously copied certificate request content in the **Base-64-encoded certificate request CMC or PKCS # 10 or PKCS # 7)** field, as shown in Figure 119.

Figure 119 Pasting the certificate request content

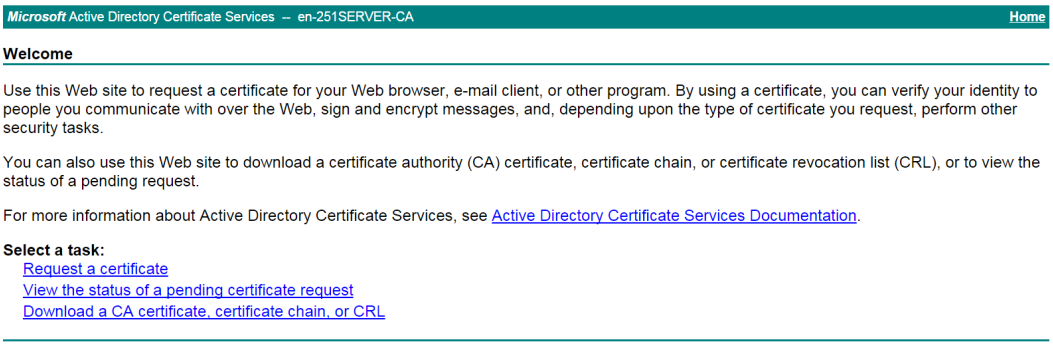


Click **Submit**.

After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 57, click **View the status of a pending certificate request**.

Figure 120 Certificate service home page



Select the certificate request you want to view.

Figure 121 View the Status of a Pending Certificate Request

The **Certificate Issued** page opens, indicating that the requested server certificate has been issued, as shown in Figure 122.

Figure 122 Certificate Issued page

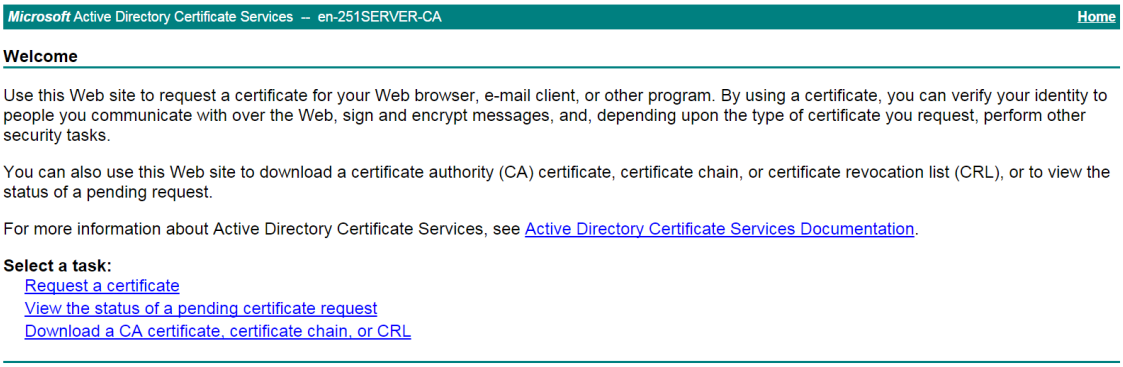
Click **Download certificate** to download the server certificate and save it locally.

5. Download the CA certificate:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

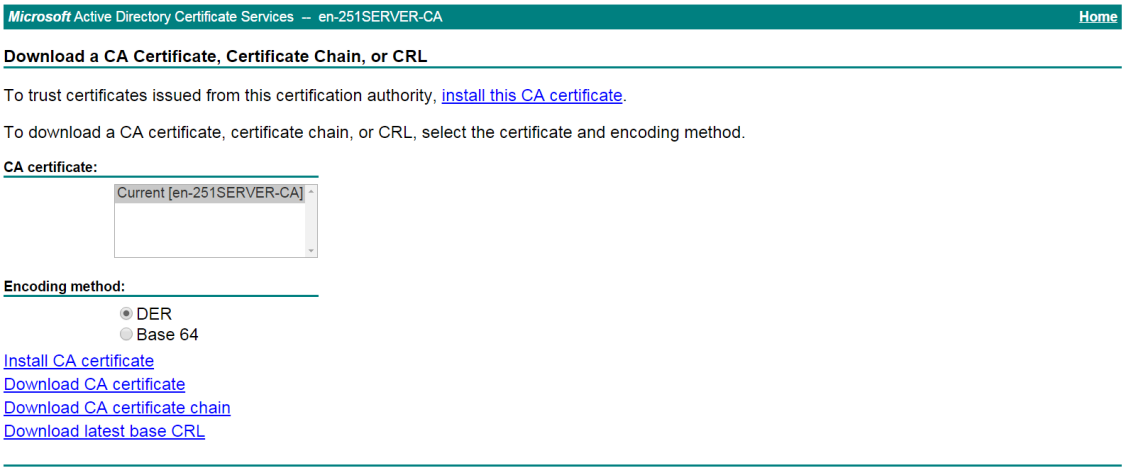
On the certificate service home page shown in Figure 123, click **Download a CA certificate, certificate chain, or CRL**.

Figure 123 Certificate service home page



On the **Download a CA certificate, certificate chain, or CRL** page shown in Figure 124, click **Download CA certificate**.

Figure 124 Download a CA certificate, certificate chain, or CRL page



Save the downloaded CA certificate locally.

6. Import the CA certificate and server certificate to the PKI domain:

a. Import the CA certificate:

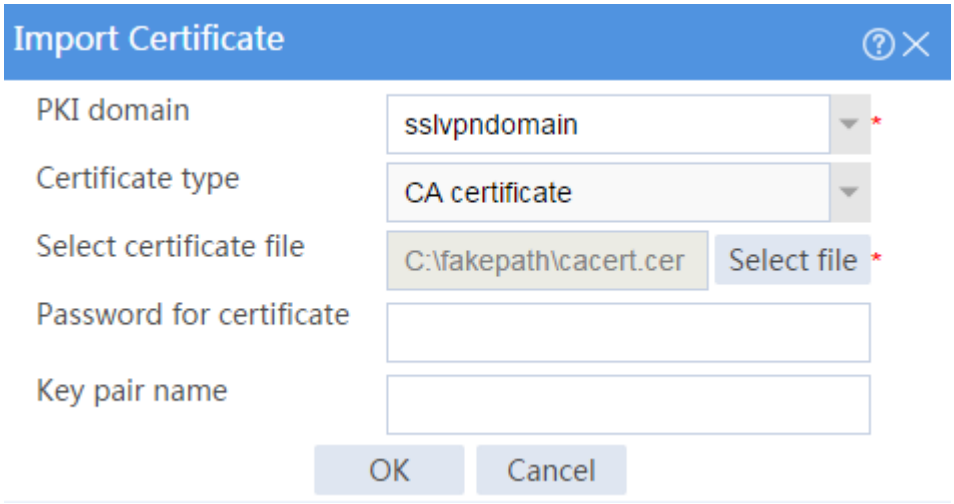
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate**.

Click **Import certificate**.

Import the locally saved CA certificate, as shown in Figure 125, and then click **OK**.

Figure 125 Importing the CA certificate

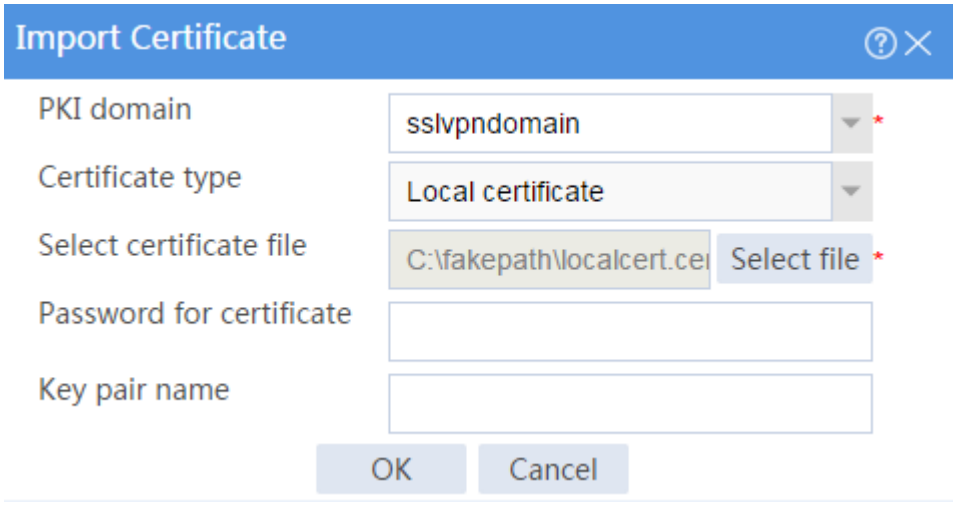


b. Import the server certificate:

On the **Certificate** page, click **Import certificate**.

Import the locally saved server certificate, as shown in Figure 126, and then click **OK**.

Figure 126 Importing the server certificate



7. Configure an SSL server policy:

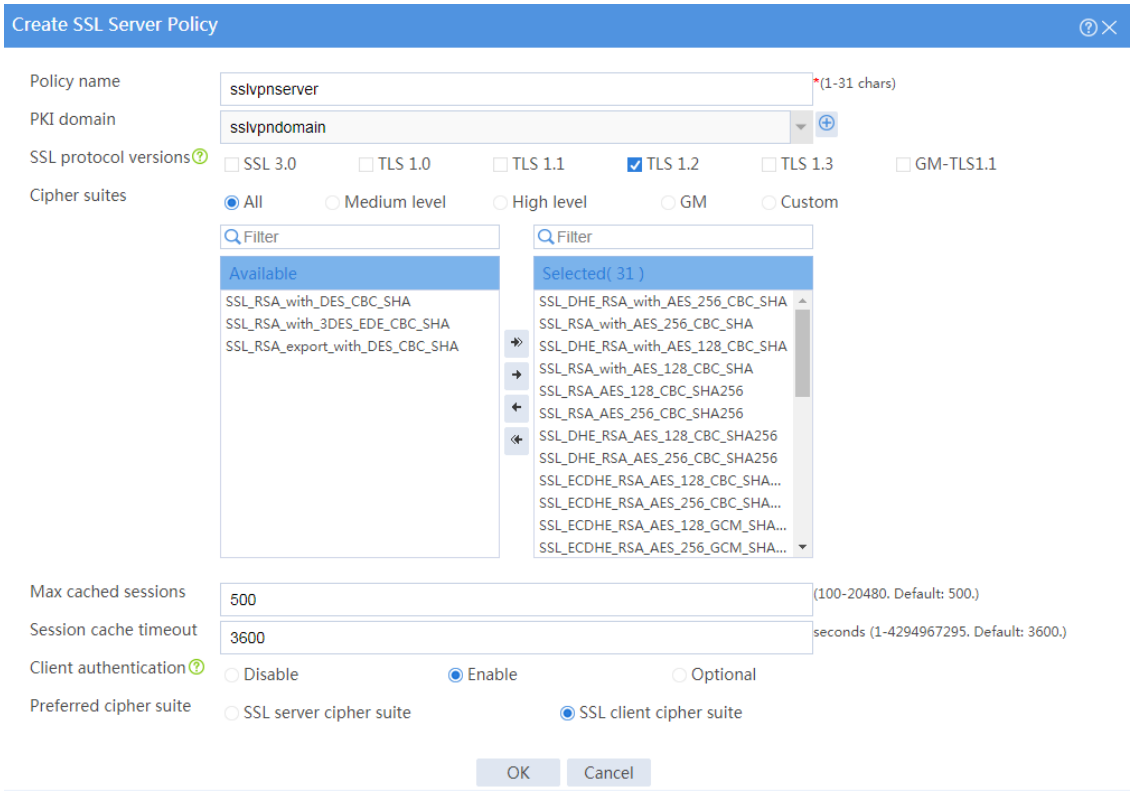
On the top navigation bar, click **Objects**.

From the navigation pane, select **SSL** > **SSL Server Policies**.

Click **Create**.

Configure an SSL server policy as shown in Figure 127, and then click **OK**.

Figure 127 Creating an SSL server policy



8. Configure an SSL client policy:

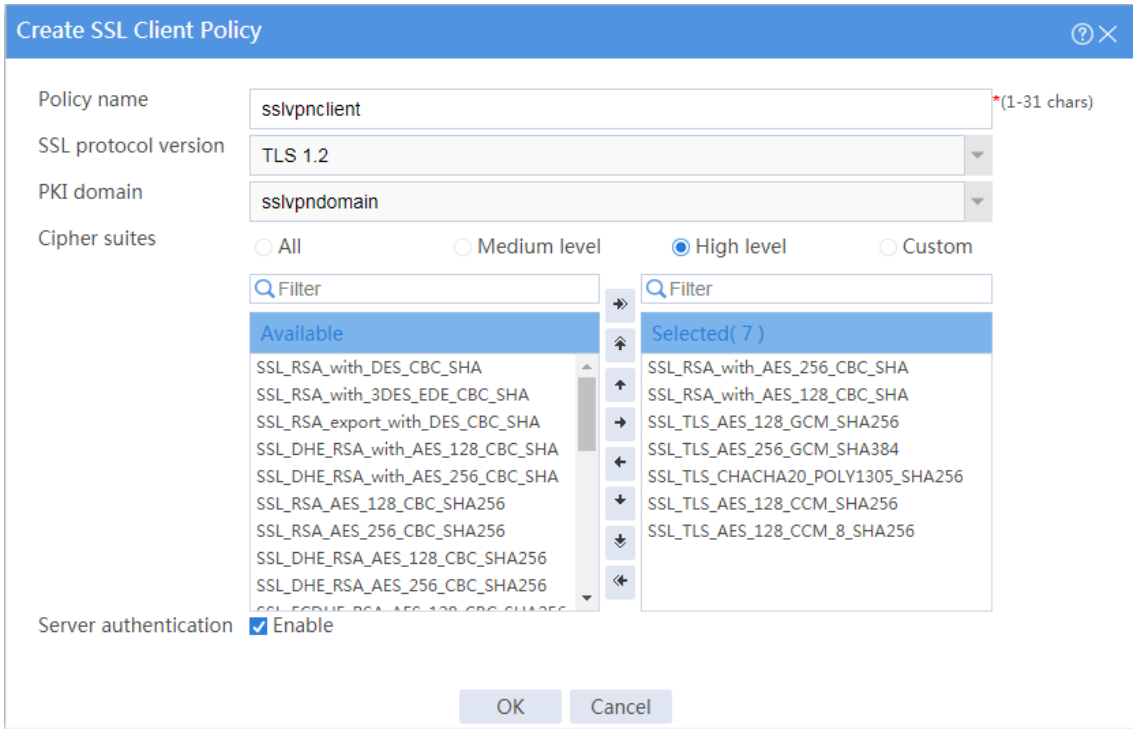
   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **SSL** > **SSL Client Policies**.

   # Click **Create**.

   # Configure an SSL client policy as shown in Figure 128, and then click **OK**.

Figure 128 Creating an SSL client policy



9. Configure a RADIUS scheme:

On the top navigation bar, click **Objects**.

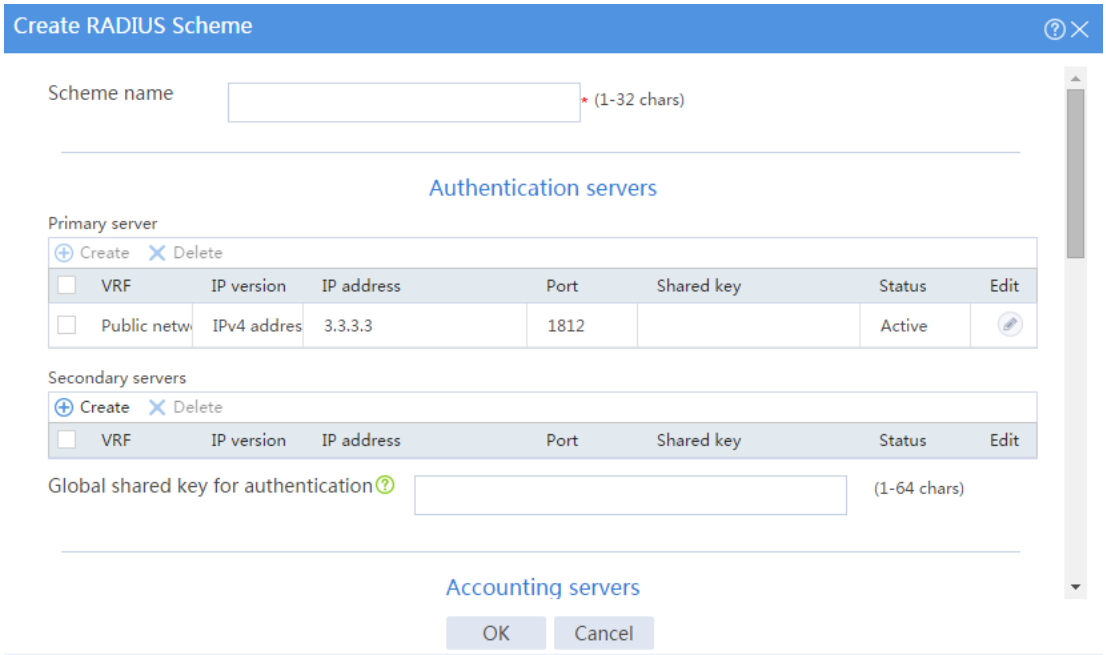
From the navigation pane, select **User** > **Authentication** > **RADIUS**.

Click **Create**.

Configure a RADIUS scheme named **radius**:

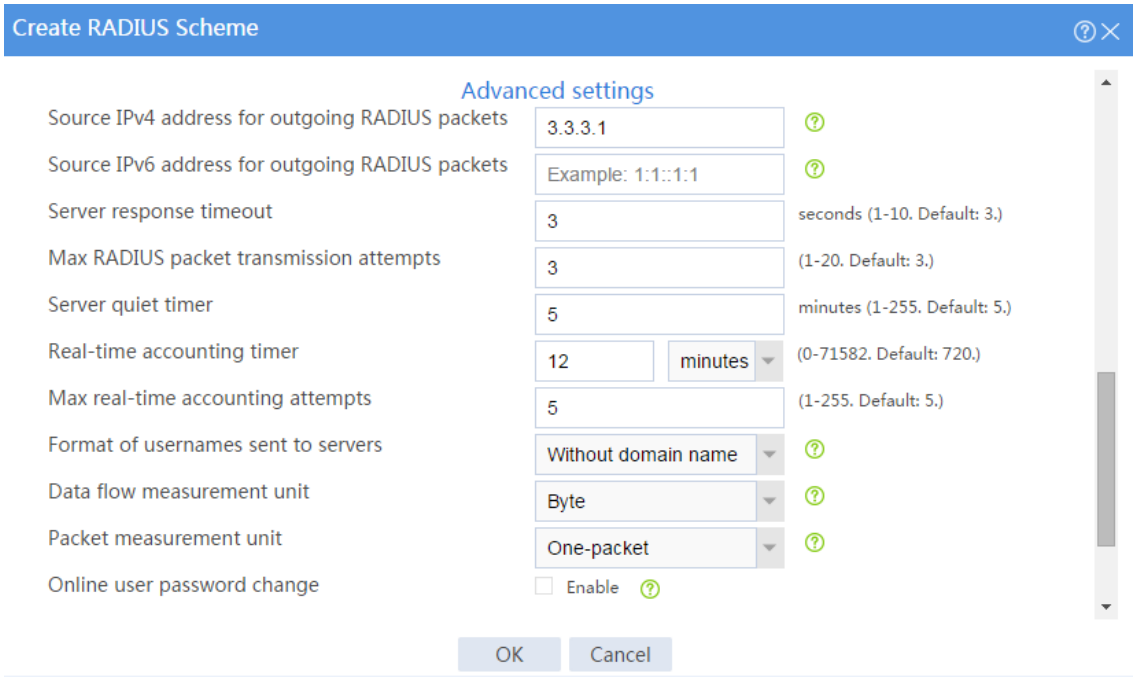
- Set the authentication server as shown in Figure 129.
- Set the global shared key for authentication to 123456.

Figure 129 Configuring a RADIUS scheme



Configure the advanced settings for the RADIUS scheme in the **Advanced settings** area, as shown in Figure 130.

Figure 130 Configuring the advanced settings for the RADIUS scheme



Click **OK**.

10. Configure an ISP domain:

    # On the top navigation bar, click **Objects**.

    # From the navigation pane, select **User** > **Authentication** > **ISP Domains**.

    # Click **Create**.

    # Configure an ISP domain named for SSL VPN.

    - Specify the domain name as **sslvpn**.
    - Select the access type **SSL VPN**.
    - Select **RADIUS** for authentication and authorization methods and select a RADIUS scheme.
    - Select **None** for the accounting method.

Figure 131 Configuring an ISP domain

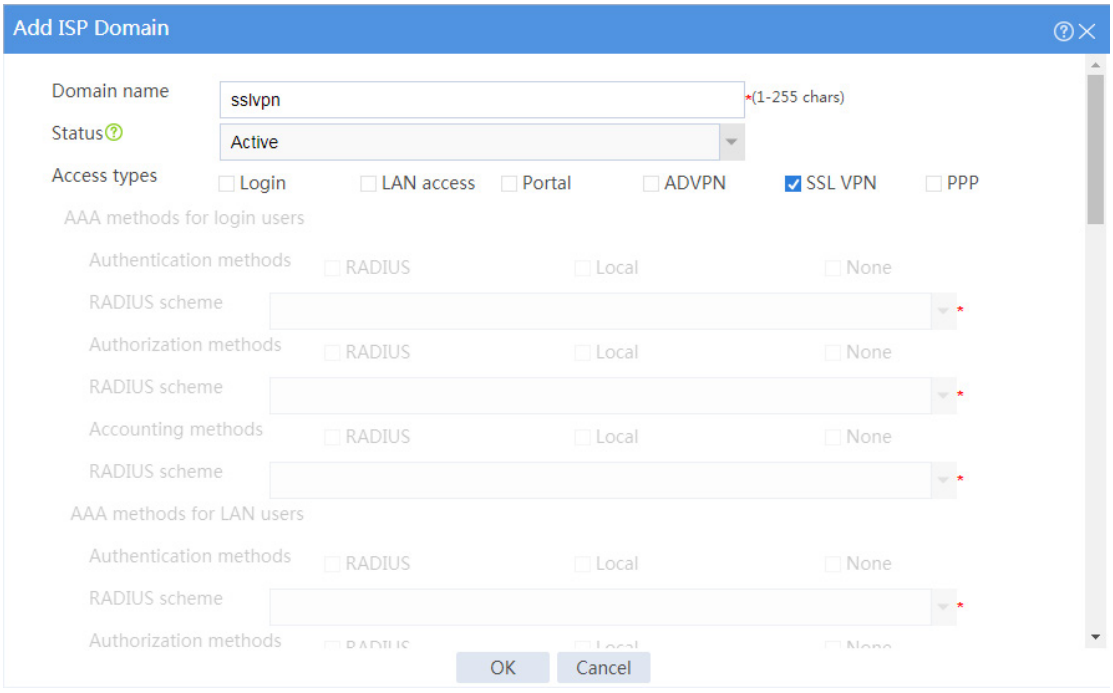
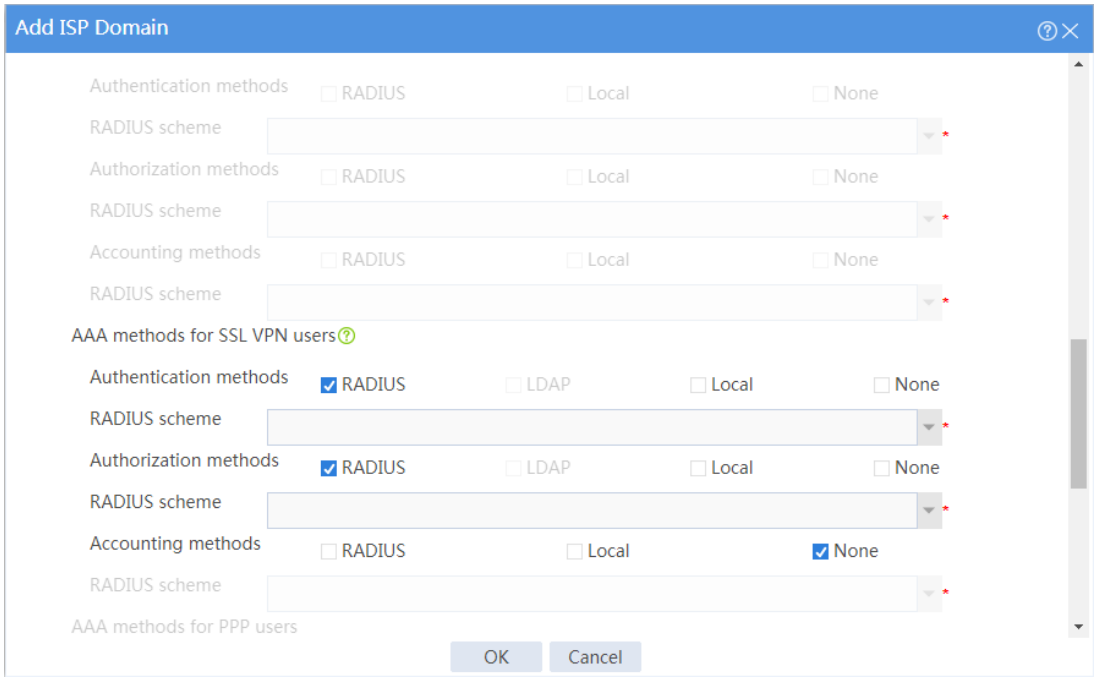


Figure 132 Configuring an ISP domain



11. Create a user group:

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **Local Users**.

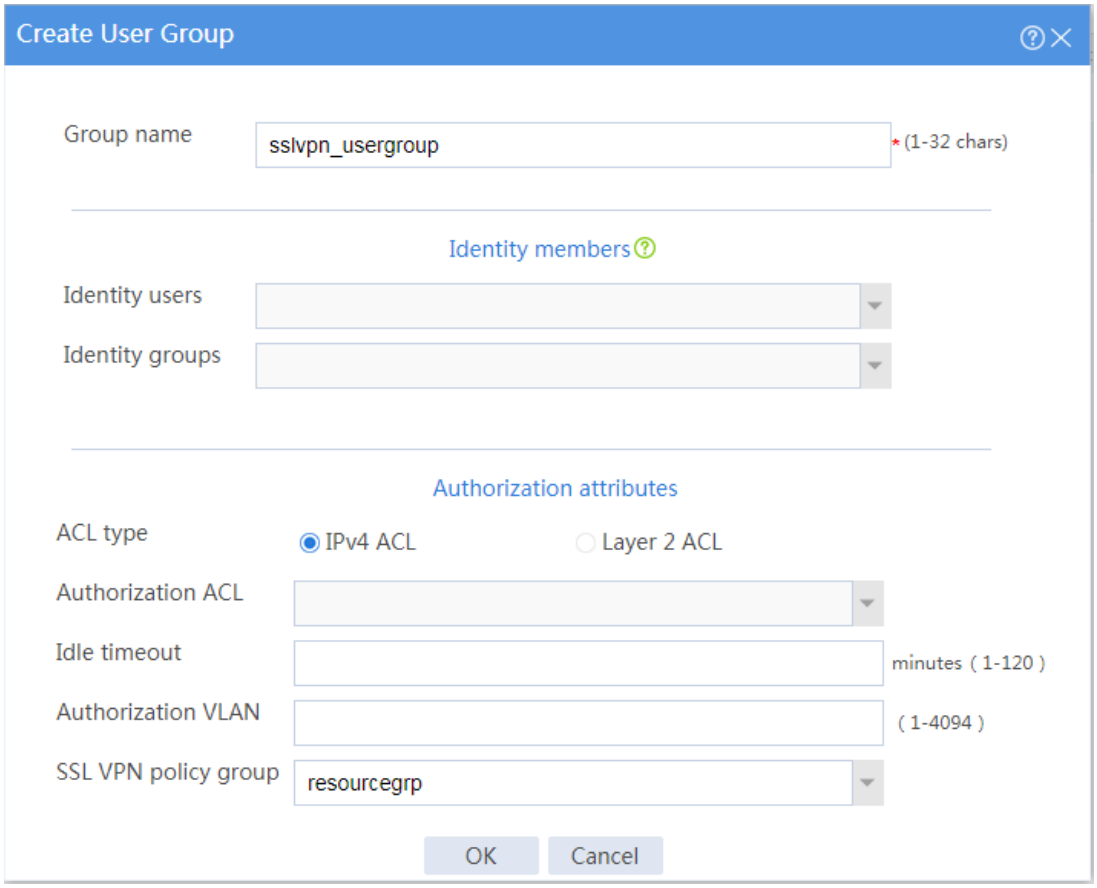
Click the **User Group** tab.

Click **Create**.

Create a user group named **sslvpn_usergroup** and specify SSL VPN resource group **resourcegrp** for the user group, as shown in Figure 133.

Click **OK**.

Figure 133 Creating a user group



12. Configure the SSL VPN gateway:

On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

Click **Create**.

Create an SSL VPN gateway as shown in Figure 134, and then click **OK**.

Figure 134 Creating an SSL VPN gateway

13. Create an SSL VPN AC interface:

    # On the top navigation bar, click **Network**.

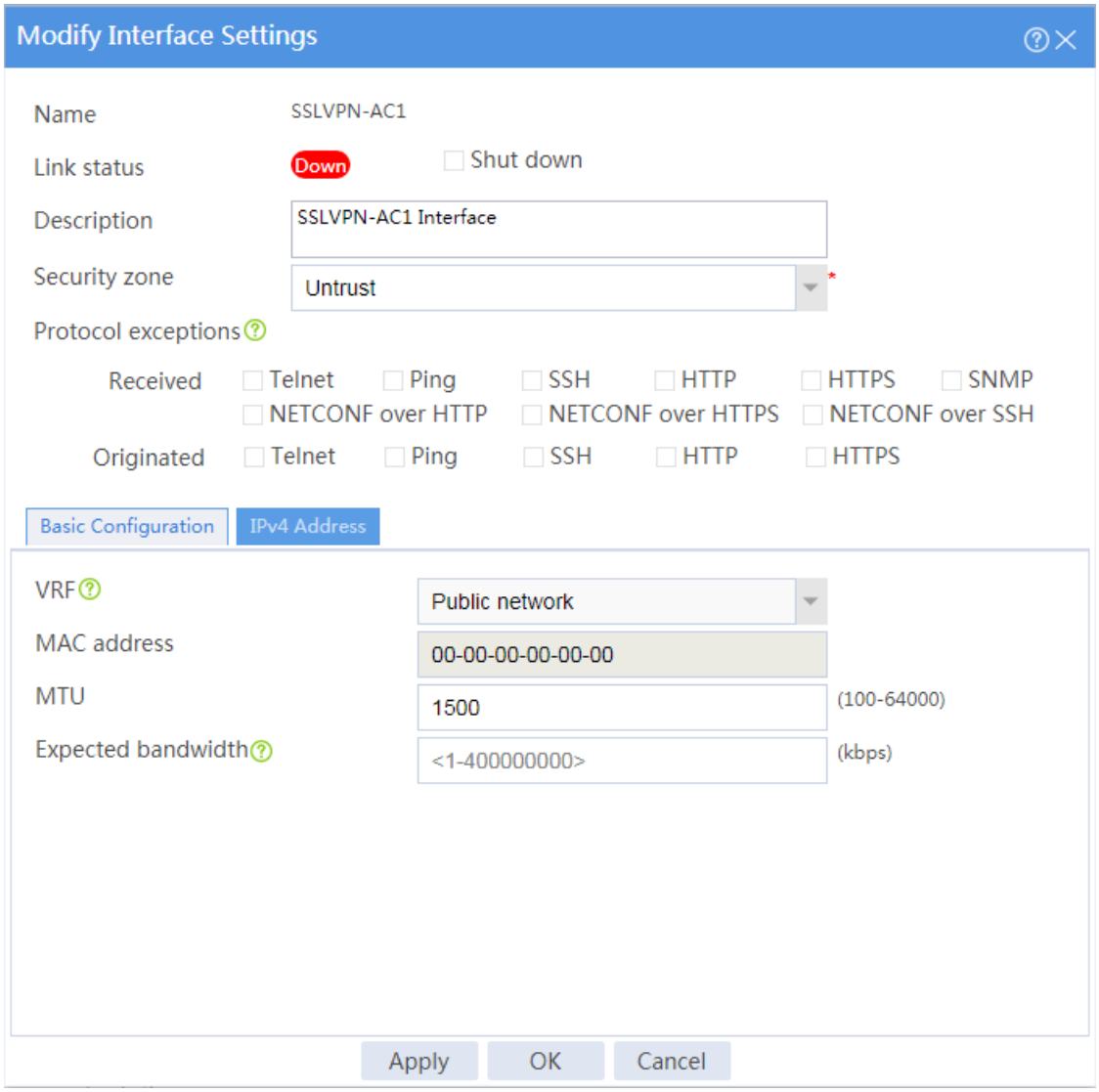
    # From the navigation pane, select **SSL VPN** > **SSL VPN AC Interfaces**.

    # Click **Create**.

    # In the **Create Interfaces** dialog box that opens, enter **1** in the **Interface number** field and click **OK**.

    # In the **Modify Interface Settings** dialog box, configure the basic settings for the SSL VPN AC interface as shown in Figure 135.

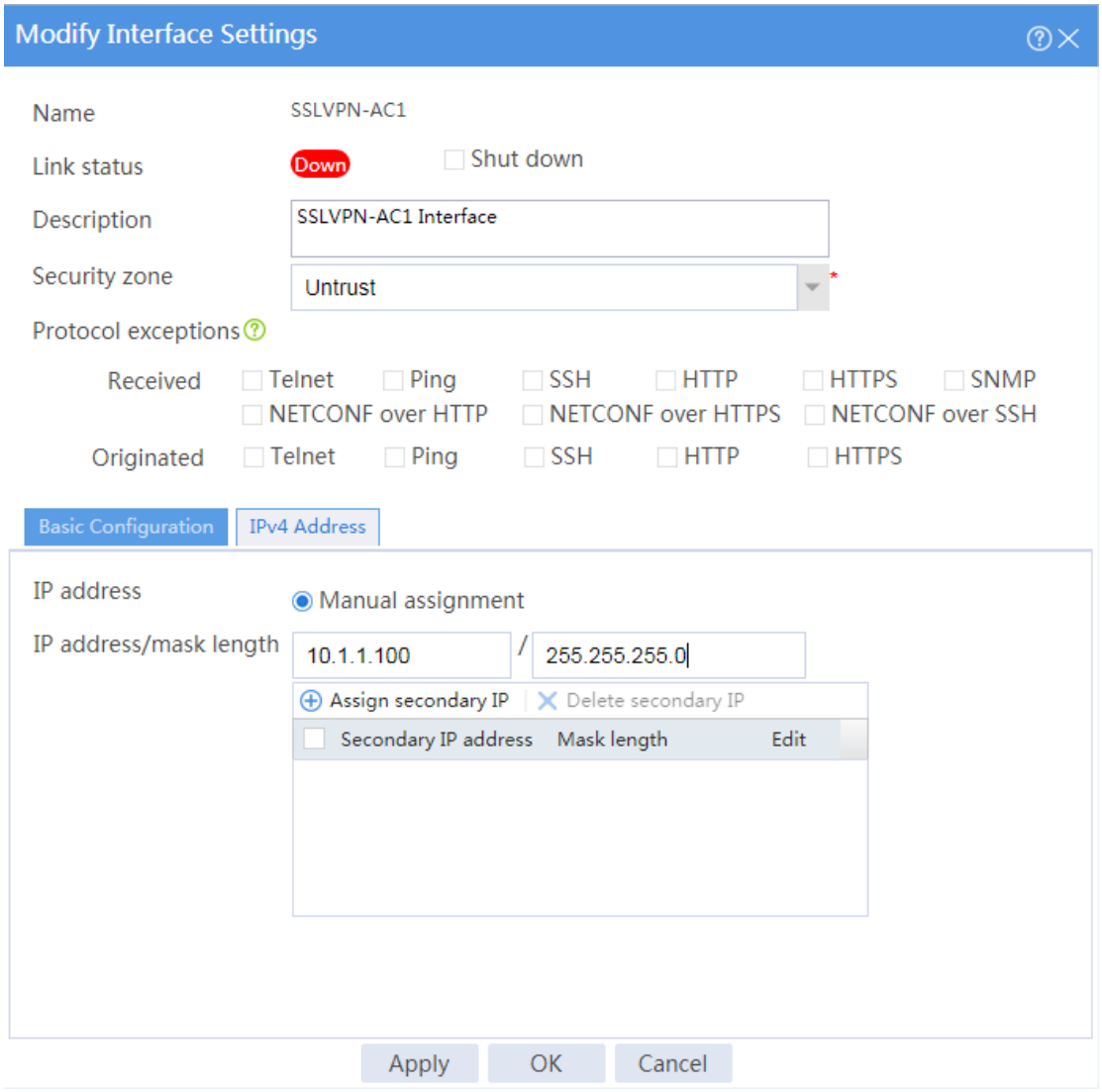
Figure 135 Configuring basic settings for the SSL VPN AC interface



Click the **IPv4 Address** tab and configure the IPv4 address settings for the SSL VPN AC interface as shown in Figure 136.

Click **OK**.

Figure 136 Configuring IPv4 address settings for the SSL VPN AC interface



14. Create an address pool for IP access users:

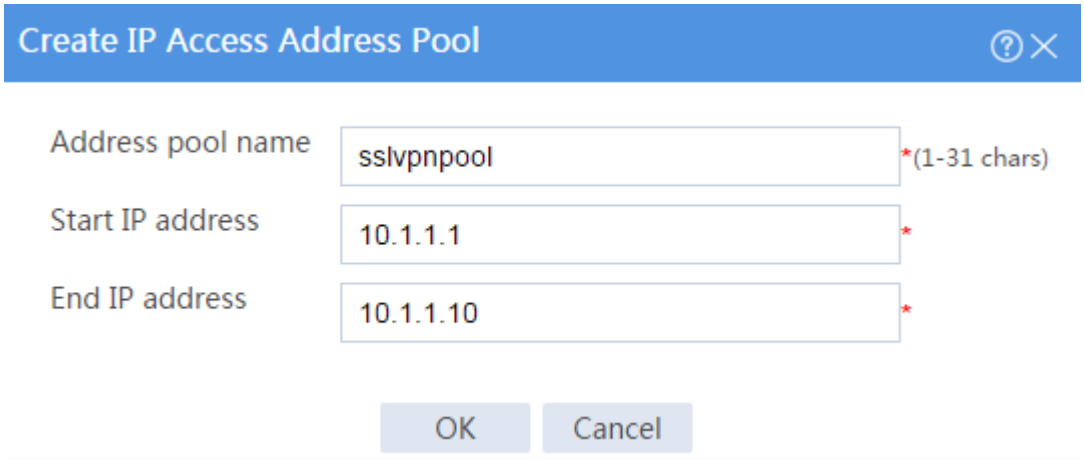
On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **IP Access Address Pools**.

Click **Create**.

Create an IP access address pool as shown in Figure 137, and then click **OK**.

Figure 137 Creating an IP access address pool



15. Configure an SSL VPN context:

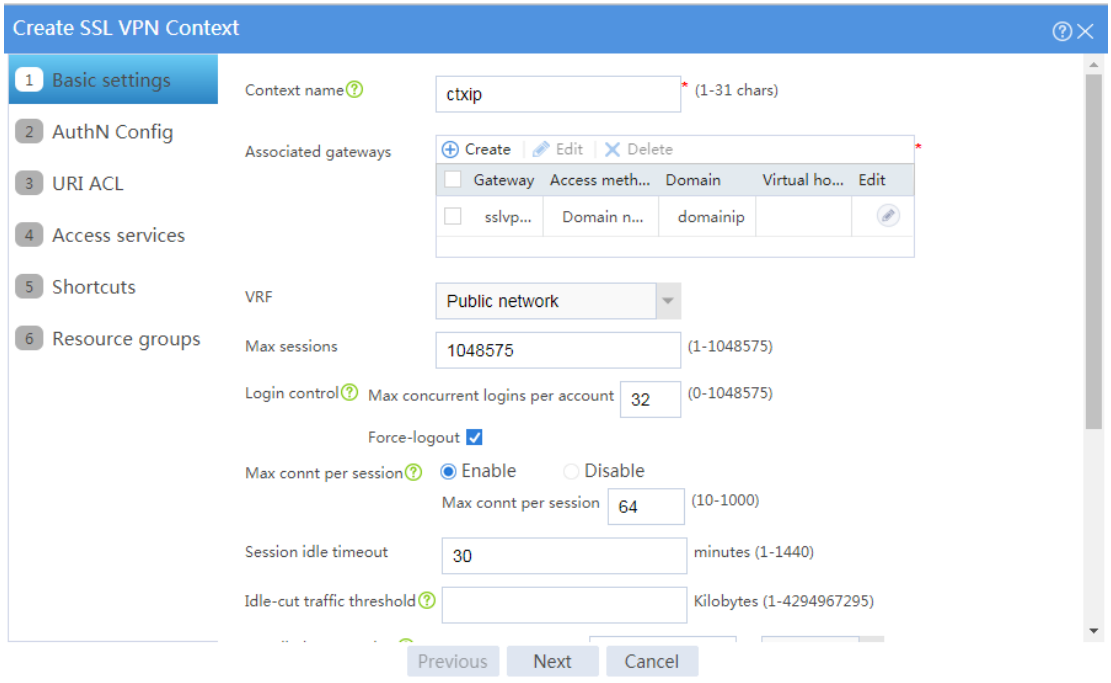
    # On the top navigation bar, click **Network**.

    # From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

    # Click **Create**.

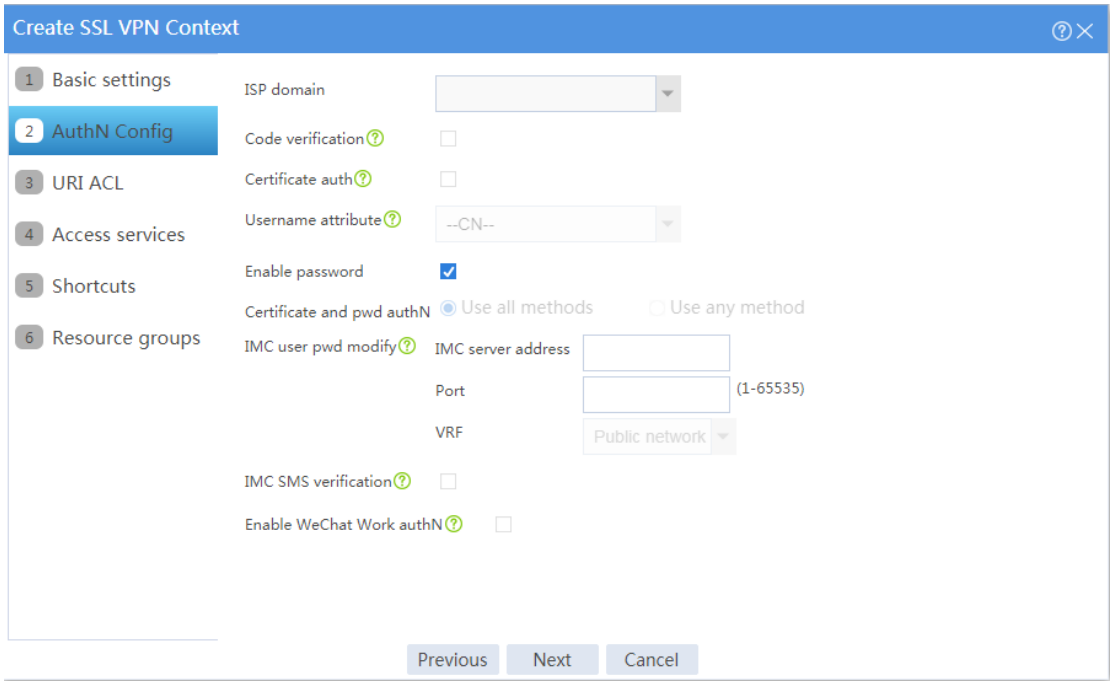
    # Configure the basic settings for the SSL VPN context as shown in Figure 138.

Figure 138 Configuring basic settings for an SSL VPN context



Click **Next** to configure authentication settings for the SSL VPN context as shown in Figure 139.

Figure 139 Configuring authentication settings



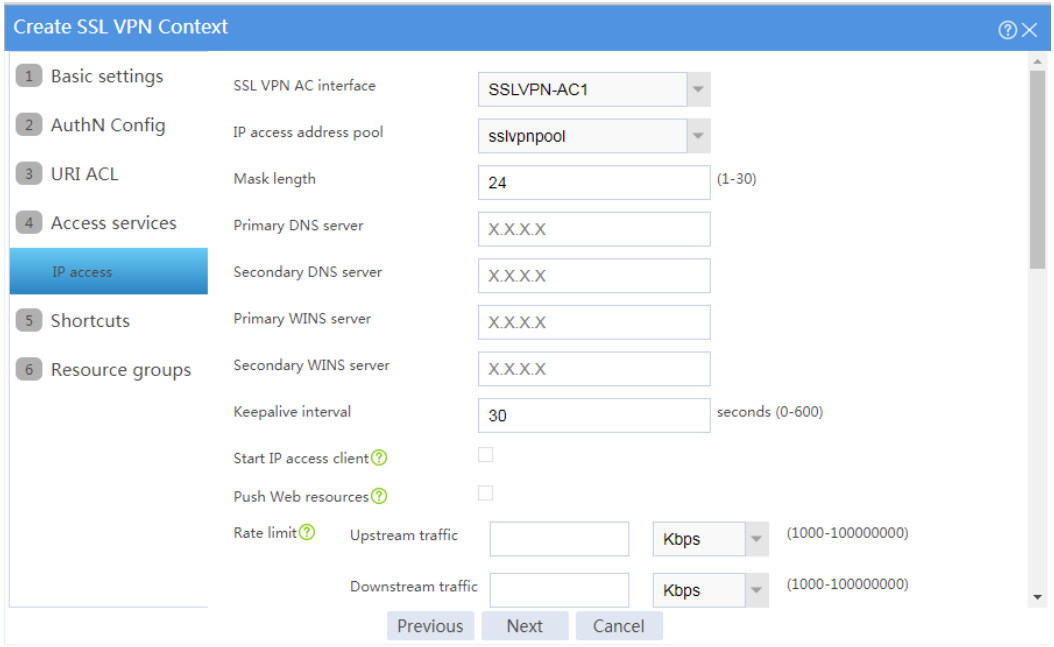
Click **Next**. On the **URI ACL** page that opens, click **Next**.

On the **Access services** page, select **IP access** and click **Next**.

On the **IP access** page, configure the IP access service as follows:

a. Configure the IP access parameters as shown in Figure 140 and click **Next**.

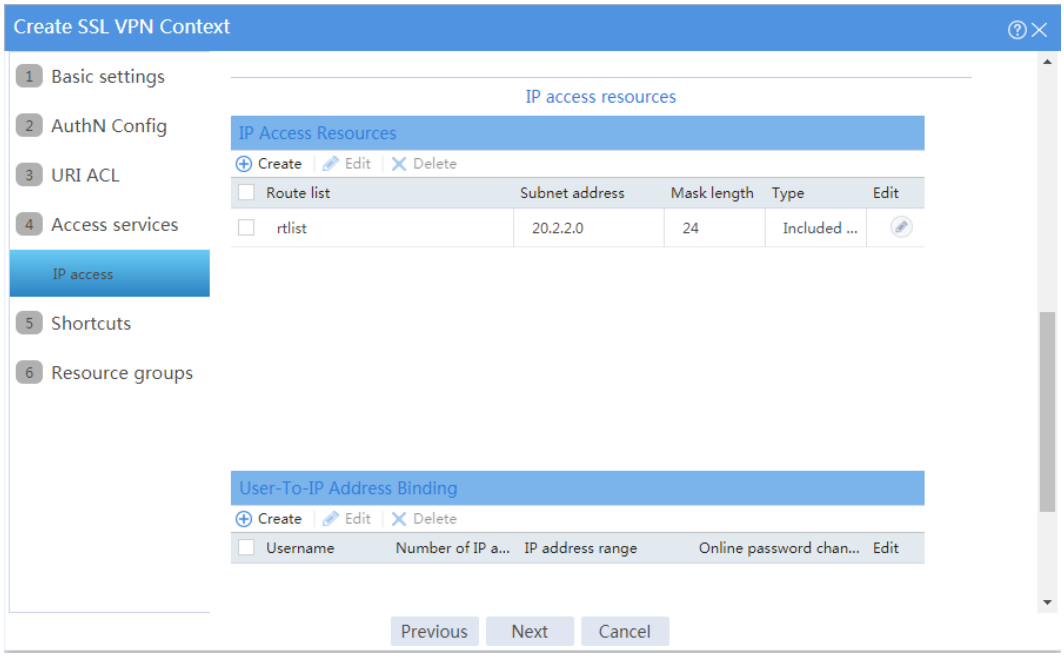
Figure 140 Configuring IP access parameters for the IP access service



b. In the **IP access resources** area, configure route list **rtlist** with an included route entry for 20.2.2.0/24, as shown in Figure 141.

c. Click **Next**.

Figure 141 Configuring IP access resources for the IP access service

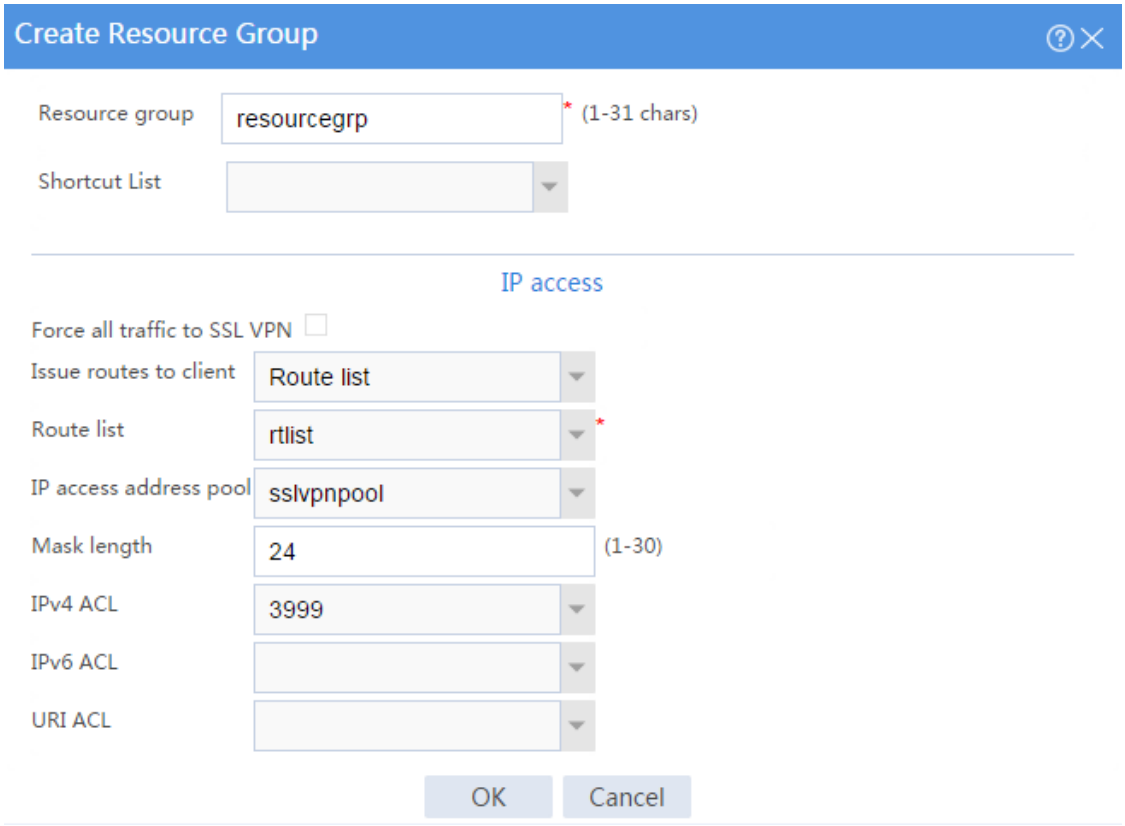


Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp**, as shown in Figure 142. In this example, select route list **rtlist** as the accessible IP resources and use IPv4 ACL 3999 (which permits all traffic) for IP access request filtering.

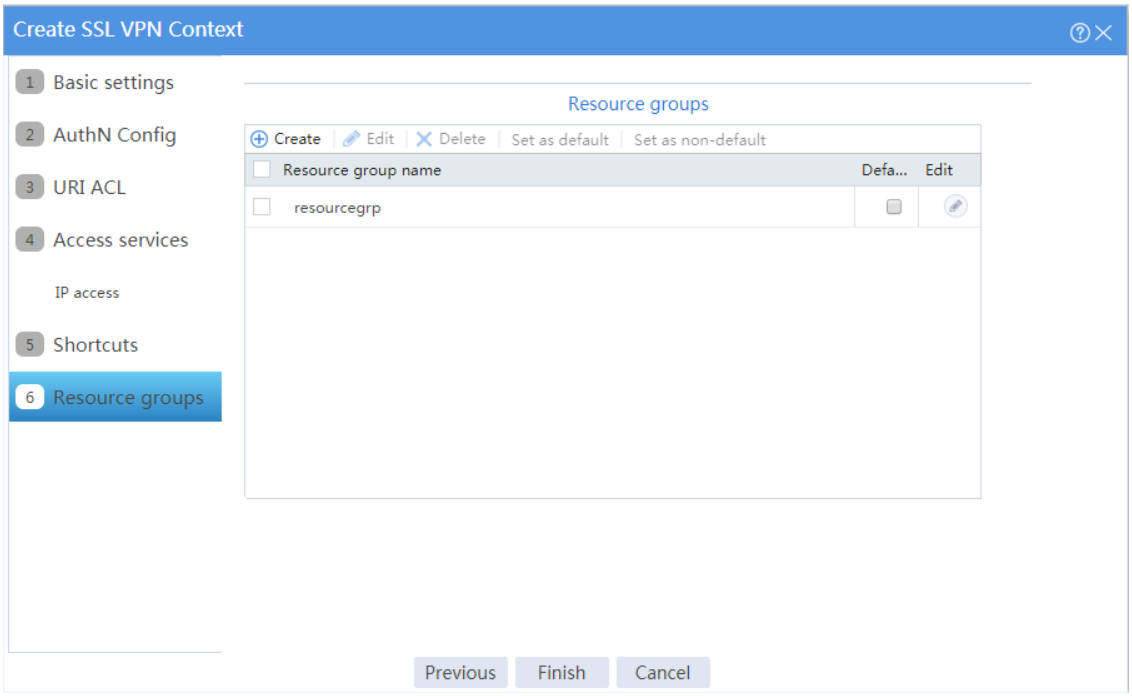
Figure 142 Creating an SSL VPN resource group



Click **OK**.

The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 143.

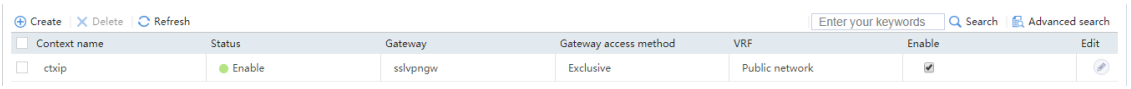
Figure 143 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 144.

Figure 144 Enabling the SSL VPN context



Configuring the RADIUS server

In this example, the IMC version is iMC PLAT 7.3 (E0504).

1. Configure an access policy named **resourcegrp**:

Log in to IMC.

On the top navigation bar, click **User**.

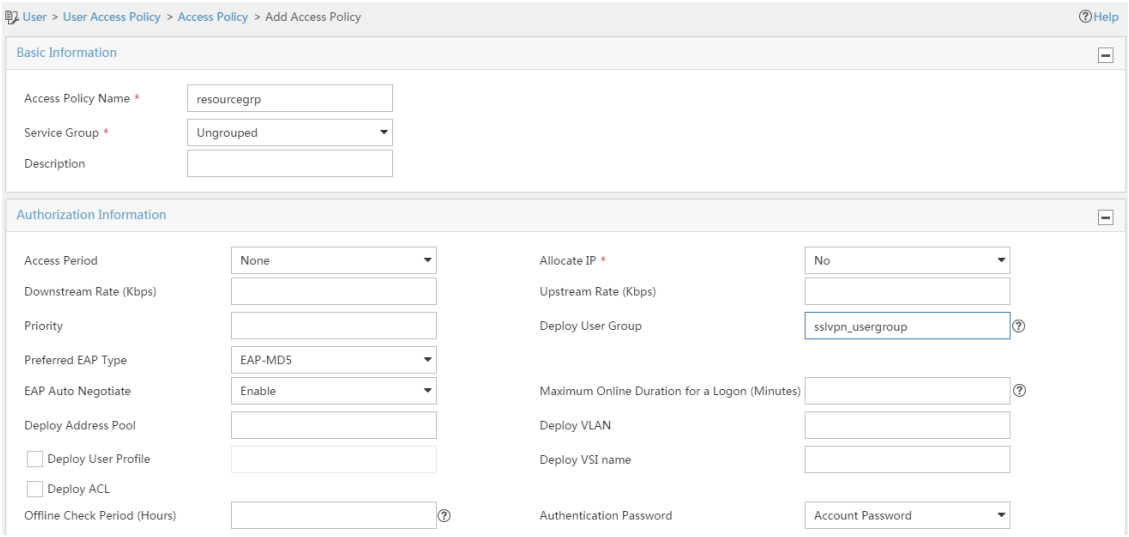
From the navigation pane, select **User Access Policy** > **Access Policy**.

Click **Add**.

Add an access policy as shown in Figure 145.

Click **OK**.

Figure 145 Creating an access policy



2. Configure an access service named **sslvpnservice**:

   # On the top navigation bar, click **User**.

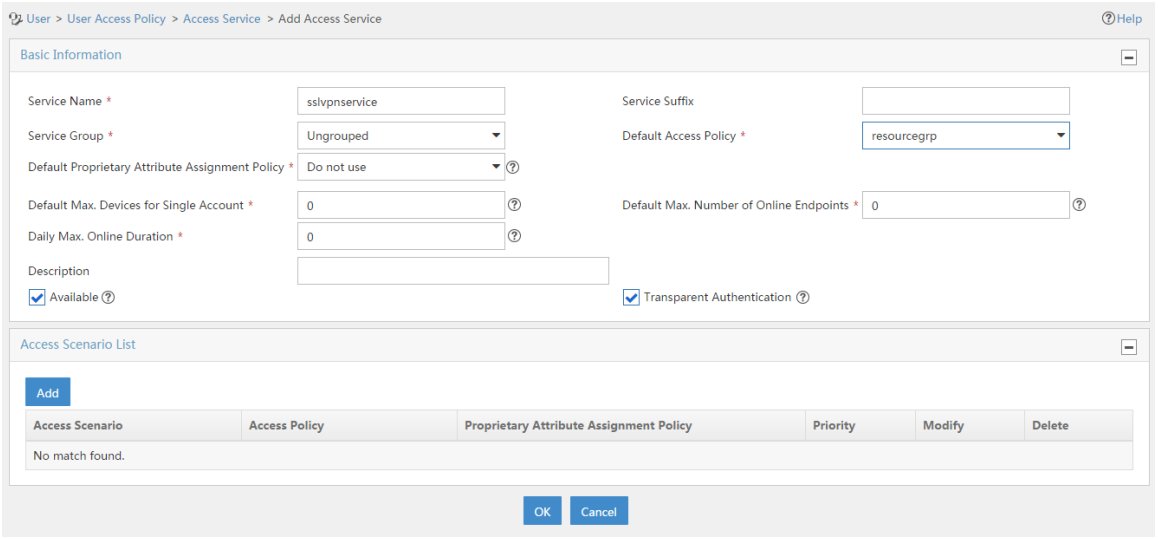
   # From the navigation pane, select **User Access Policy** > **Access Service**.

   # Click **Add**.

   # Add an access service as shown in Figure 146. In this example, specify access policy **resourcegrp** as the default access policy.

   # Click **OK**.

Figure 146 Creating an access service



3. Configure an access device:

   # On the top navigation bar, click **User**.

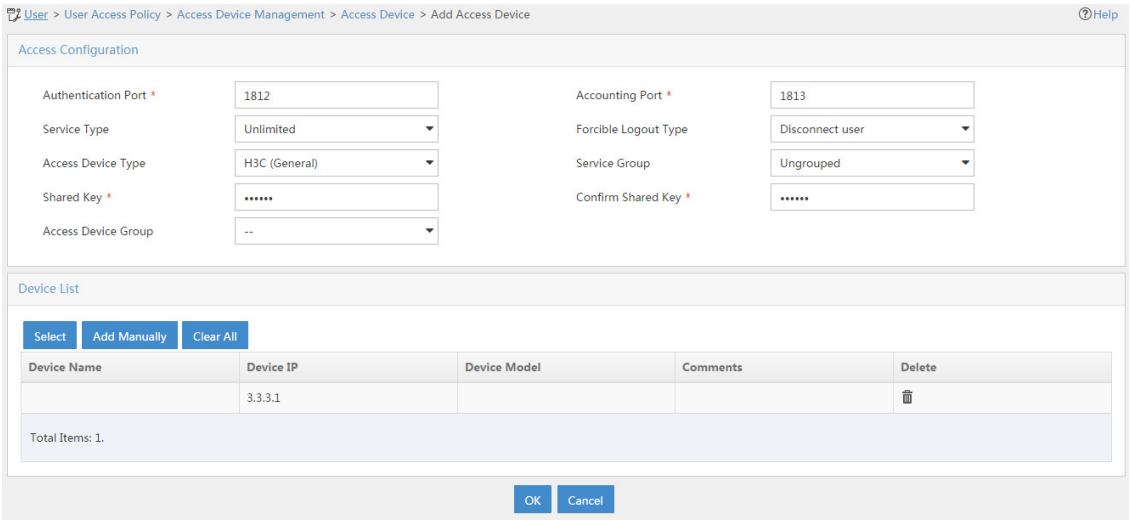
   # From the navigation pane, select **User Access Policy** > **Access Device Management** > **Access Device**.

   # Click **Add**.

   # Add an access device as shown in Figure 147. In this example, set the shared key to **123456**.

   # Click **OK**.

Figure 147 Configuring an access device



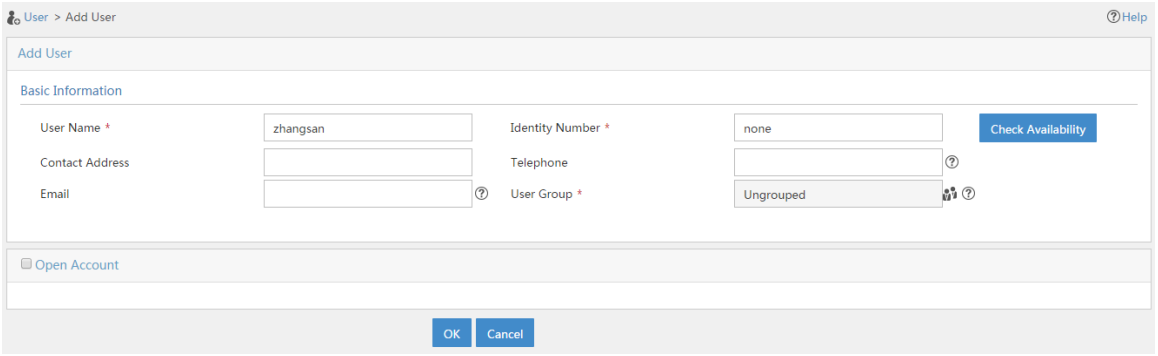
4. Configure an access user:

Access the **User** > **Add User** page.

Add a platform user as shown in Figure 148.

Click **OK**.

Figure 148 Adding a platform user



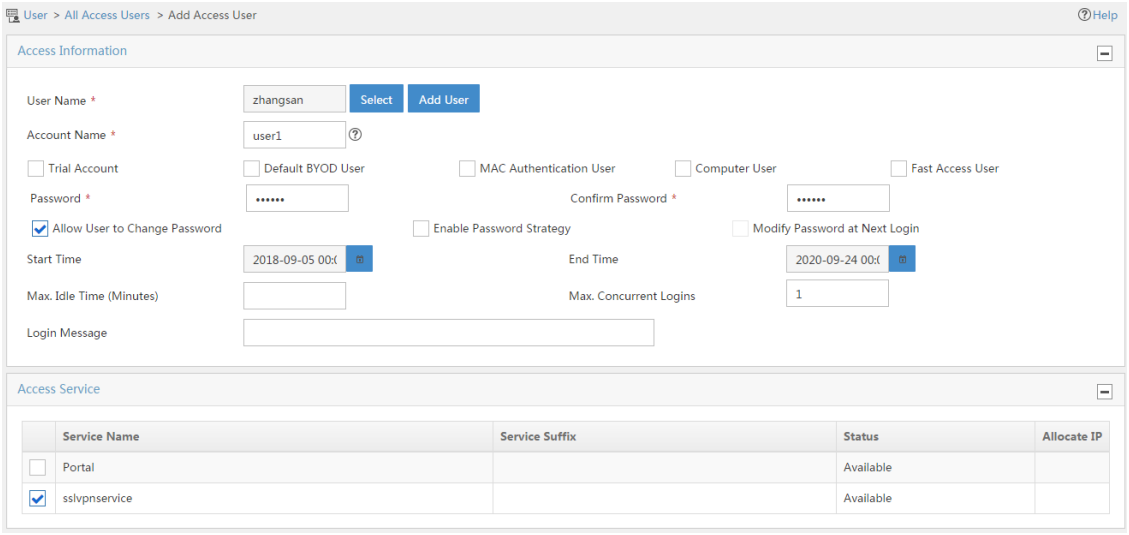
From the navigation pane, select **Access User** > **All Access Users**.

Click **Add**.

Add an access user and assign access service **sslvpnservice** to the user, as shown in Figure 149.

Click **OK**.

Figure 149 Adding an access user



Configuring the server

Make sure the server has a route to subnet 10.1.1.0/24.

Verifying the configuration

1. Install the USB key on the host.

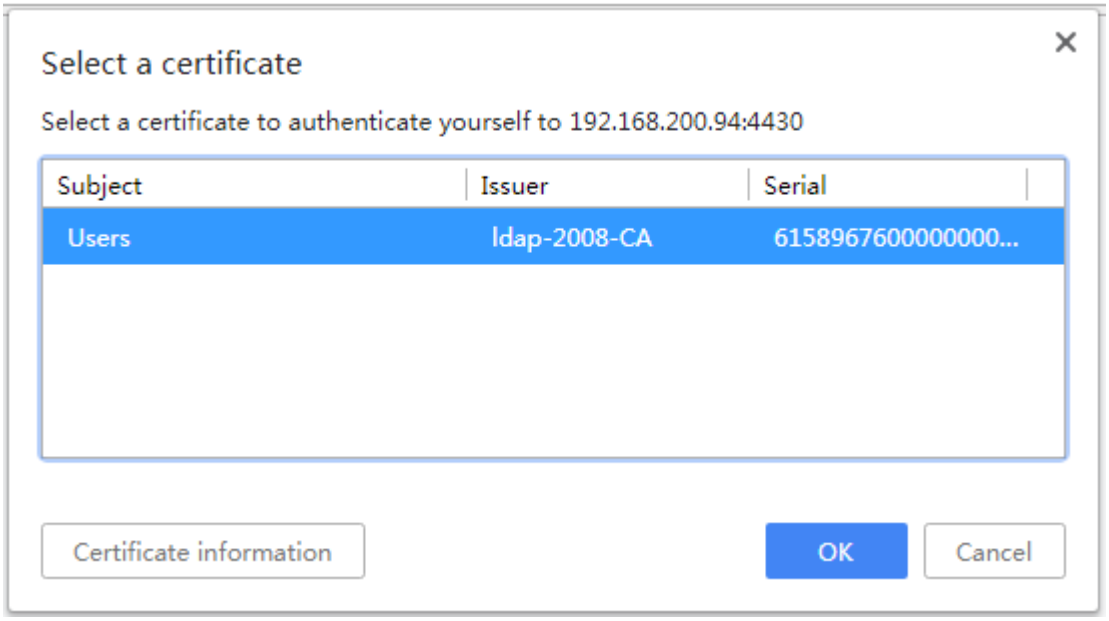
   Obtain the USB key from the administrator, and install the USB key on the host. For information about how to make a USB key, see the appendix in the following section.

2. Log in to the SSL VPN gateway from the host:

   # In the browser address bar of the host, enter **https://1.1.1.2:4430/** and press **Enter**.

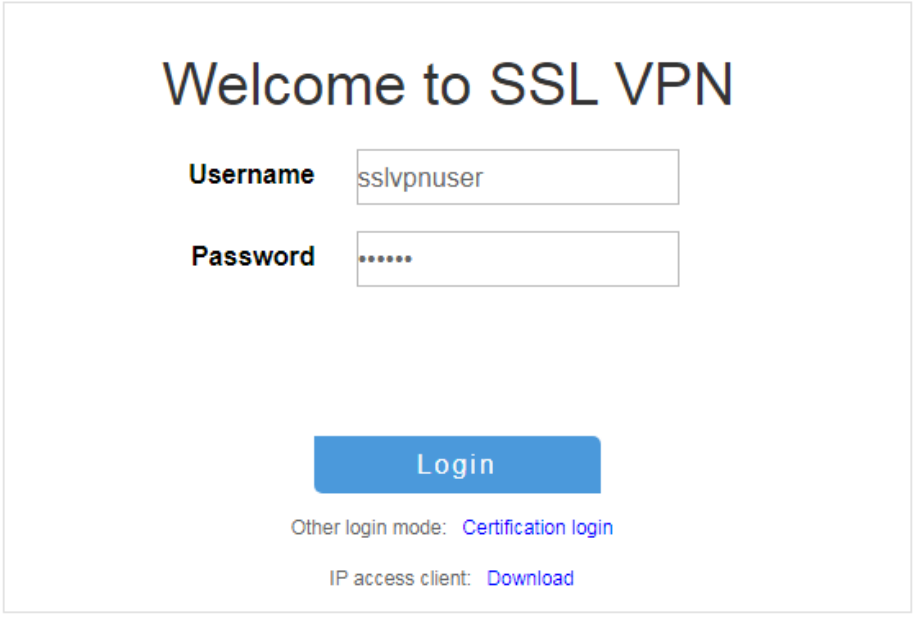
   # On the **Select a certificate** page, select the client certificate for authentication, as shown in Figure 150.

Figure 150 Select a certificate page



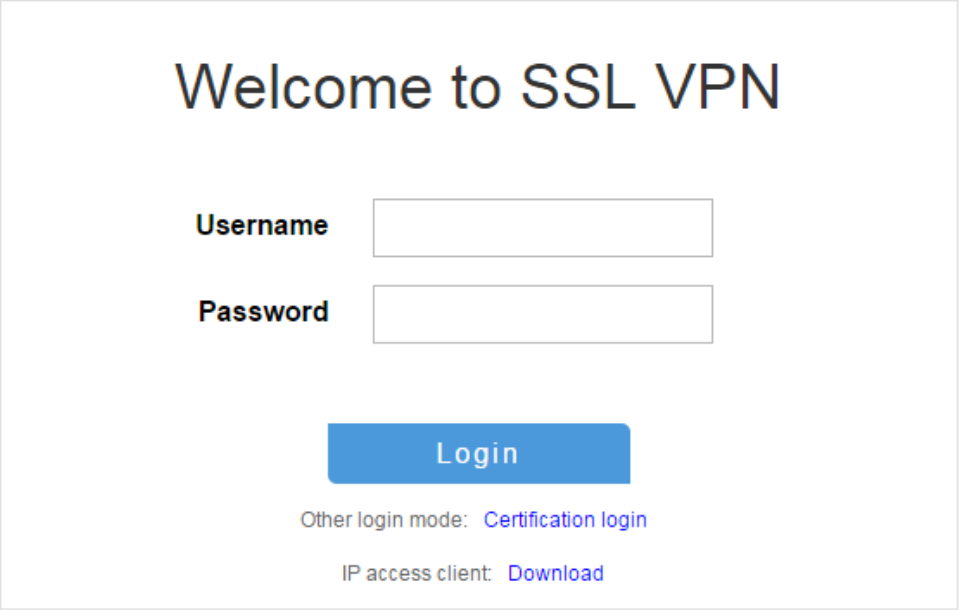
3. Click **OK**.
4. On the page that opens, enter username **sslvpnuser** and password **123456TESTplat&!**, and then click **Login** as shown in Figure 151.

Figure 151 SSL VPN login page



5. On the login page, enter username **user1** and password **123456**, and then click **Login**.

Figure 152 Login page



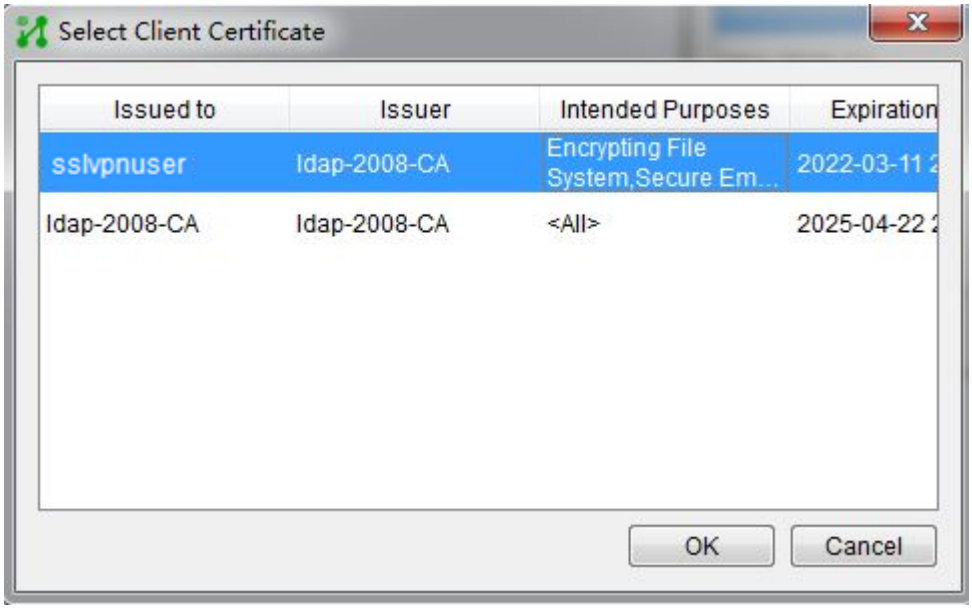
6. Click **START** to start the IP client application.

Launch the installed IP client and configure it as follows:

Figure 153 Connecting the iNode client to the SSL VPN gateway

Click the icon next the **Password** box. In the dialog box that opens, select the client certificate in the USB key, and then click **OK**.

Figure 154 Selecting the client certificate



Click **Connect** on the iNode client. You log in to the SSL VPN gateway successfully.

Figure 155 Logging into the SSL VPN gateway successfully

After the SSL VPN user logs in, the user can ping the server IP address 20.2.2.2 from the host.

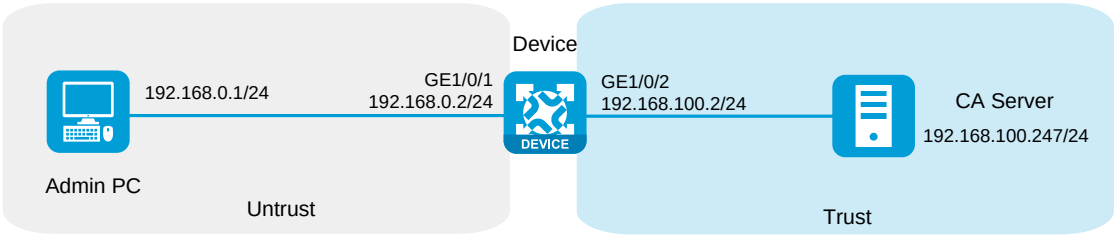
```
C:\>ping 20.2.2.2

Pinging 20.2.2.2 with 32 bytes of data:

Reply from 20.2.2.2: bytes=32 time=31ms TTL=254

Reply from 20.2.2.2: bytes=32 time=18ms TTL=254

Reply from 20.2.2.2: bytes=32 time=15ms TTL=254

Reply from 20.2.2.2: bytes=32 time=16ms TTL=254


Ping statistics for 20.2.2.2:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 15ms, Maximum = 31ms, Average = 20ms
```

Appendix—Making a USB key

Make a USB key in the following procedure:

1. Configure an IP address and gateway on the administrator's PC to ensure the PC can reach the CA server. This example uses Windows 2008 server as the CA server.

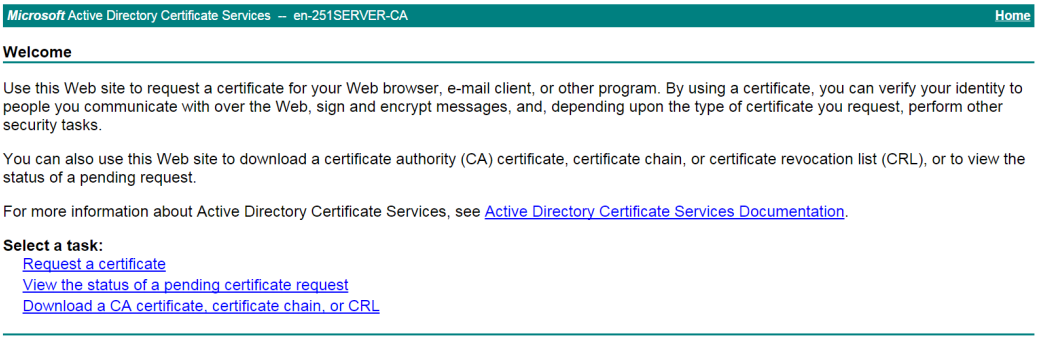
Figure 156 Network diagram



2. Request the USB key client certificate:

   # Enter **http://192.168.100.247/certsrv** in the address bar of a browser to open the certificate service page.

Figure 157 Certificate services



   # Click **Request a certificate**. The certificate request page opens.

Figure 158 Requesting a certificate

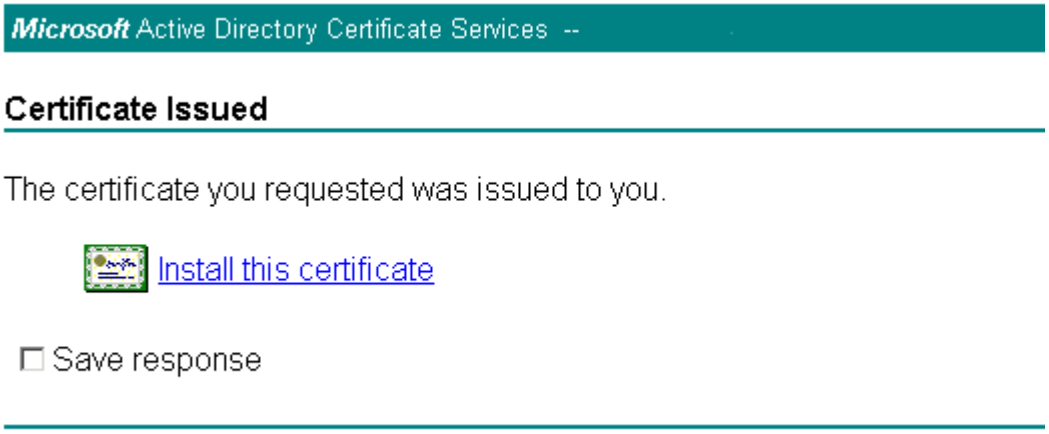
Click **advanced certificate request**. On the page that opens, select **Create and submit a request to this CA** to request a client certificate.

Configure the client certificate request parameters, and then click **Submit** at the bottom of the page.

In the dialog box that opens, enter the USB key password, and then log in.

Click **Install this certificate** to install the client certificate to the USB key.

Figure 159 Installing the client certificate to the USB key



After a possible conflict warning about installing a certificate, click **Yes** to install the client certificate into the USB key.

The USB key is made successfully.

SSL VPN TCP access configuration examples

Contents

Introduction

The following information provides SSL VPN TCP access configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedure and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of SSL VPN.

Example: Configuring TCP access with a CA-signed server certificate

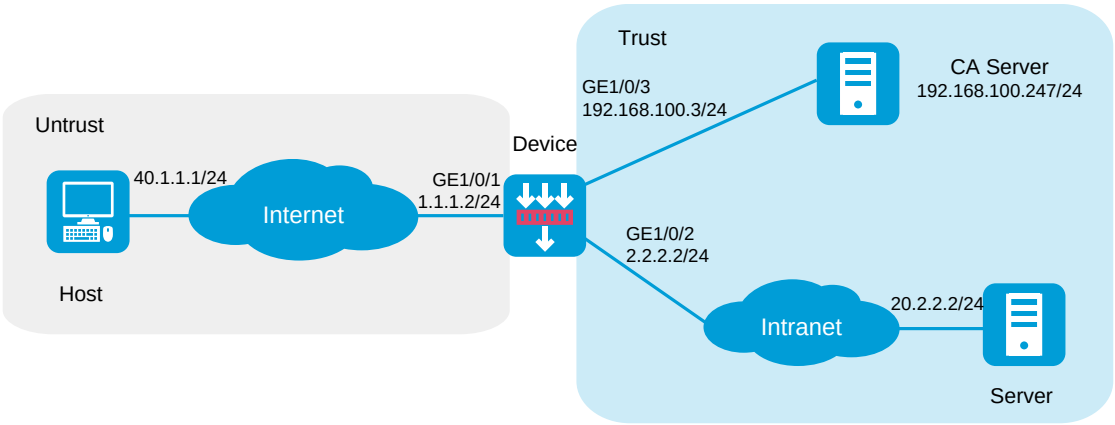
Network configuration

As shown in Figure 1, the device acts as the SSL VPN gateway that connects the public network and the private network. A Windows Server 2008 R2 CA server is deployed on the private network. Users need secure access to the internal Telnet server in TCP access mode.

Perform the following tasks:

- Request a server certificate for the device from the CA server.
- Configure the SSL VPN TCP access service on the device to allow users to access the server in TCP access mode.
- Configure the device to perform local authentication and authorization for TCP access users.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

- Certificate-based client authentication is not available in TCP access mode.
- To start the TCP client from the Web interface, make sure the Java Runtime Environment is installed on the client host.
- To access internal resources in TCP access mode from the host, modifications to the **Hosts** file on the host might be required. Make sure you log in to the host with administrative privileges.

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click the **Network** tab.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 192.168.100.3/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

This example configures static routes.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static IPv4 route to reach 40.1.1.1:

a. Enter destination IP address **40.1.1.1**.

b. Enter mask length **24**.

c. Enter next hop address **1.1.1.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 20.2.2.2:

a. Enter destination IP address **20.2.2.2**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.

- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 addresses **2.2.2.2** and **192.168.100.3**.
- Select destination IPv4 addresses **20.2.2.2** and **192.168.100.247**.
- Use the default settings for other parameters.

Click **OK**.

4. Request a server certificate for the device:

a. Create a certificate subject:

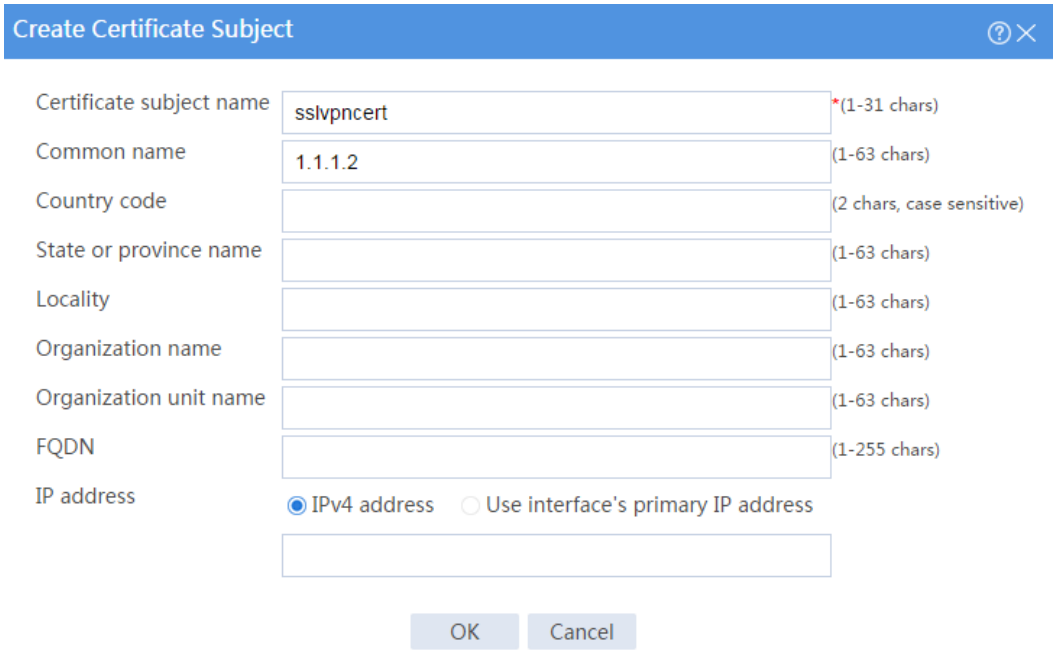
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate Subject**.

Click **Create**.

Create a certificate subject as shown in Figure 2, and the click **OK**.

Figure 2 Creating a certificate subject



b. Create a PKI domain:

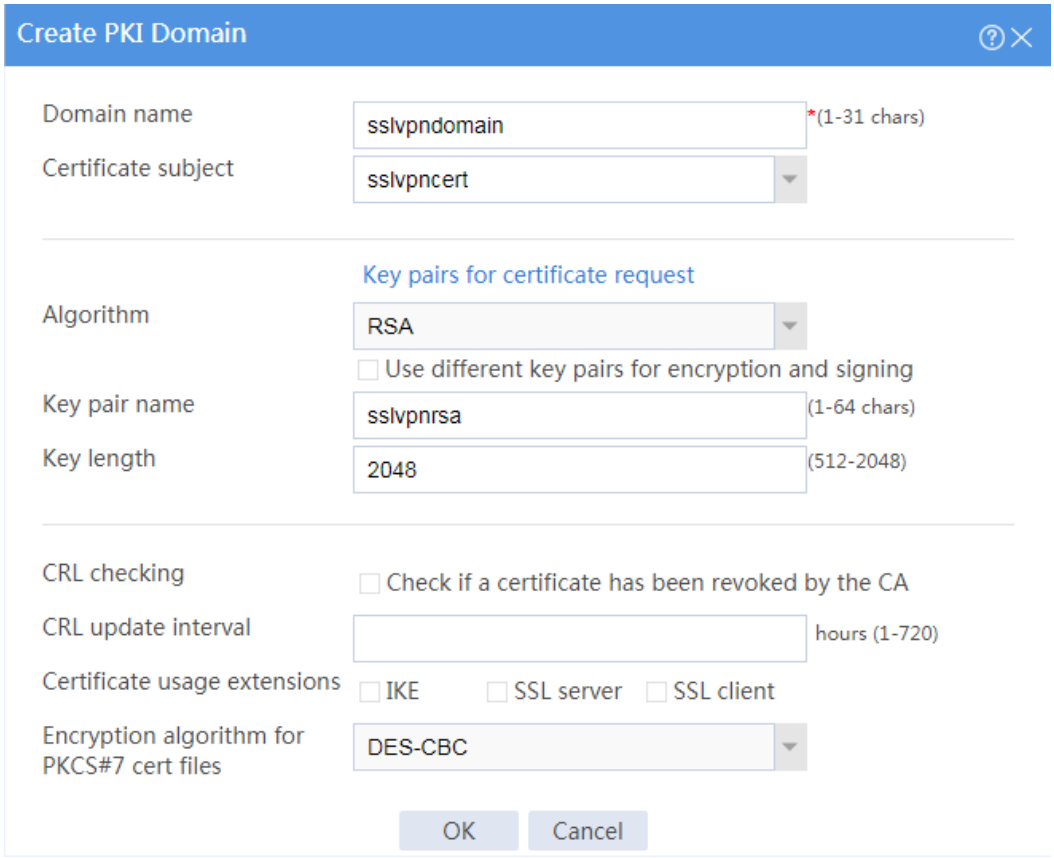
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate**.

Click **Create PKI domain**.

Create a PKI domain as shown in Figure 3, and then click **OK**.

Figure 3 Creating a PKI domain

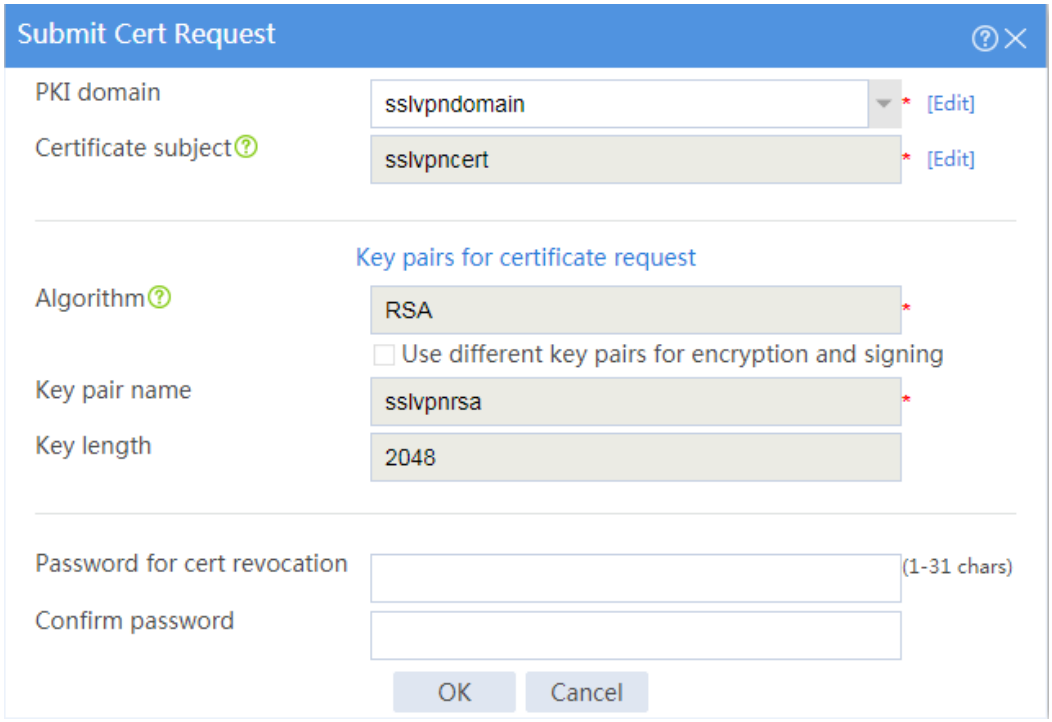


c. Create a certificate request:

On the **Certificate** page, click **Submit Cert Request**.

Configure the certificate request settings as shown in Figure 4.

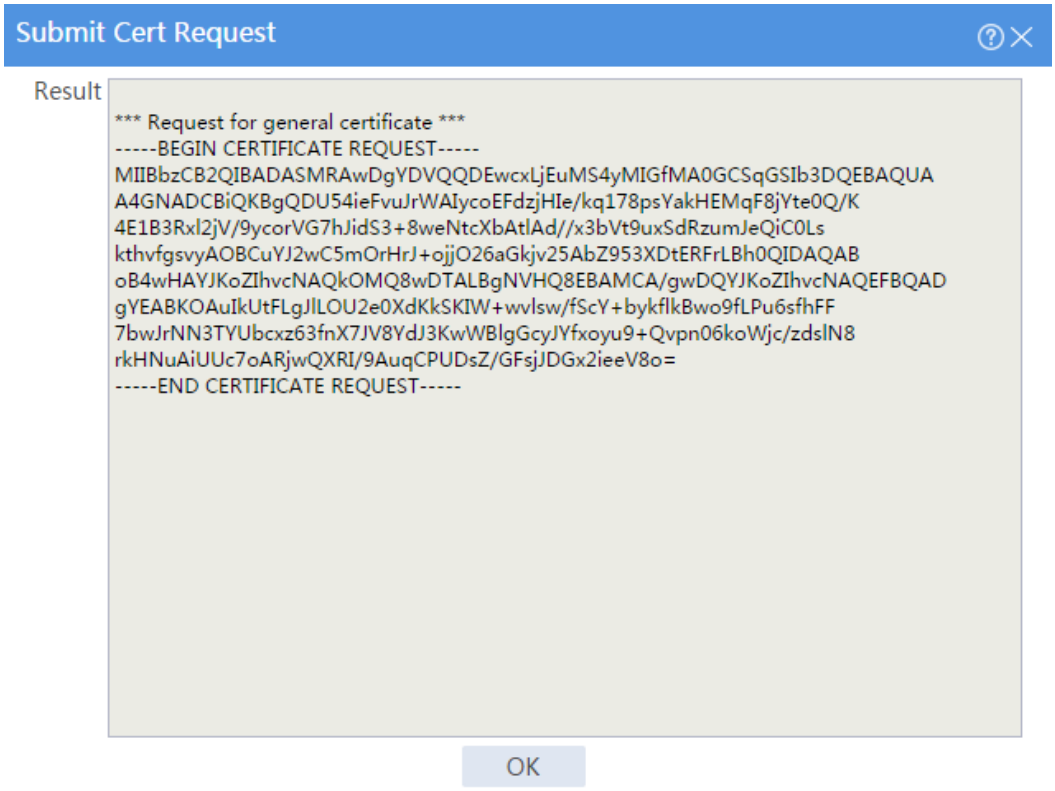
Figure 4 Creating a certificate request



Click **OK**.

The certificate request content will be displayed, as shown in Figure 5.

Figure 5 Certificate request content



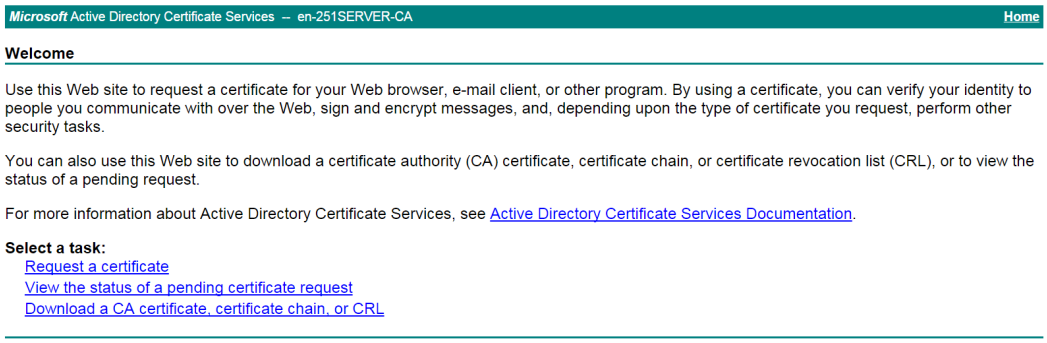
Copy the certificate request content and click **OK**.

d. Request a server certificate from the CA:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 6, click **Request a certificate**.

Figure 6 Certificate service home page

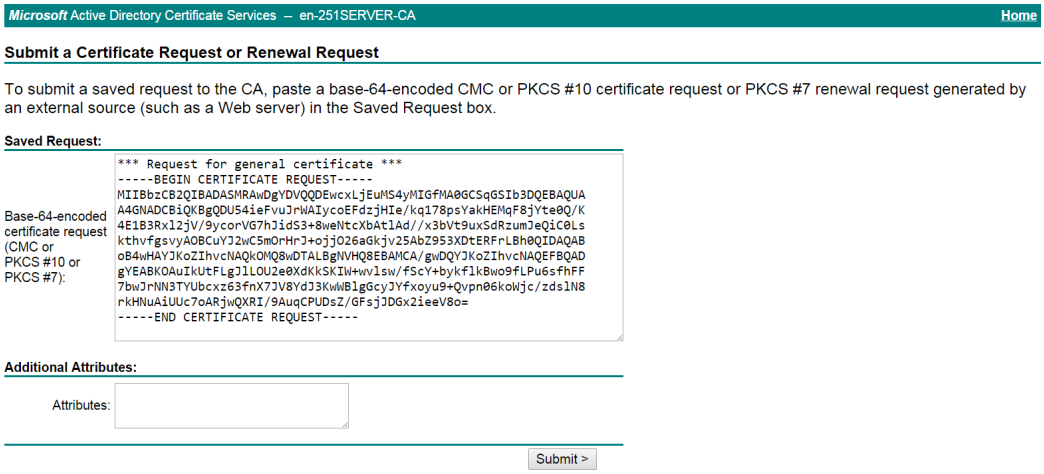


On the **Request a Certificate** page shown in Figure 7, click **advanced certificate request**.

Figure 7 Request a Certificate page

Paste the previously copied certificate request content in the **Base-64-encoded certificate request CMC or PKCS # 10 or PKCS # 7)** field, as shown in Figure 8.

Figure 8 Pasting the certificate request content

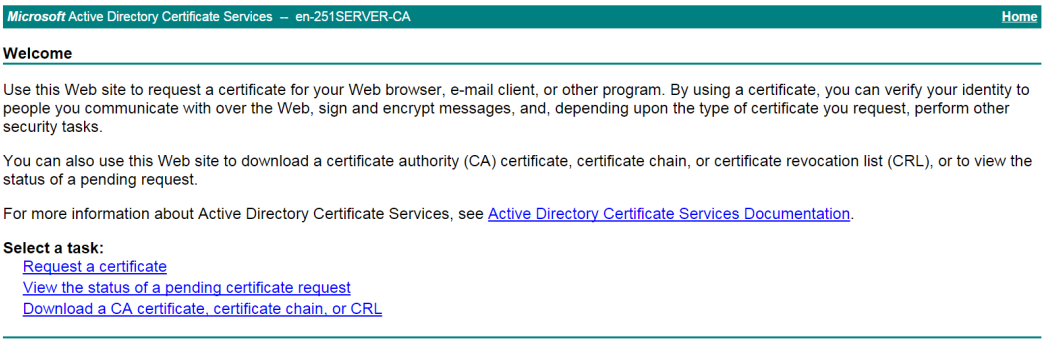


Click **Submit**.

After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 9, click **View the status of a pending certificate request**.

Figure 9 Certificate service home page

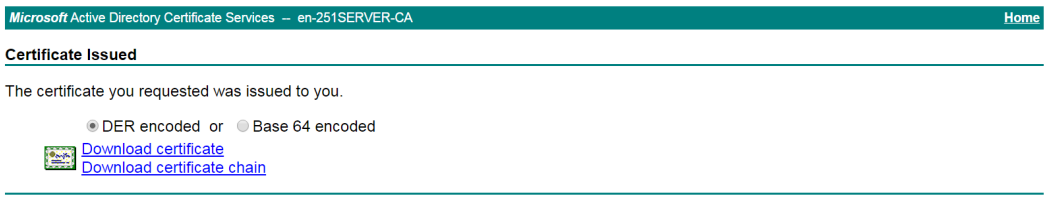


Select the certificate request you want to view. In this example, select **Saved-Request Certificate (9/24/2018 9:53:57 AM)**, as shown in Figure 10.

Figure 10 View the Status of a Pending Certificate Request page

The **Certificate Issued** page opens, indicating that the requested server certificate has been issued, as shown in Figure 11.

Figure 11 Certificate Issued page



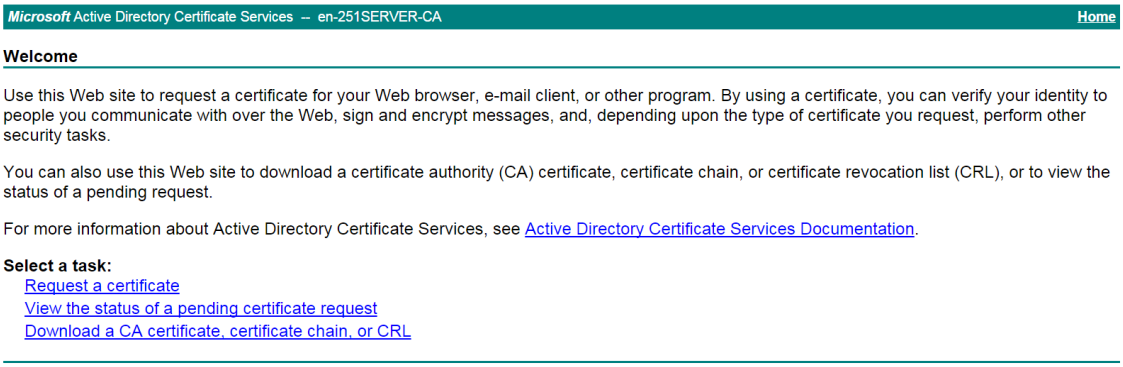
Click **Download certificate** to download the server certificate and save it locally.

5. Download the CA certificate:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

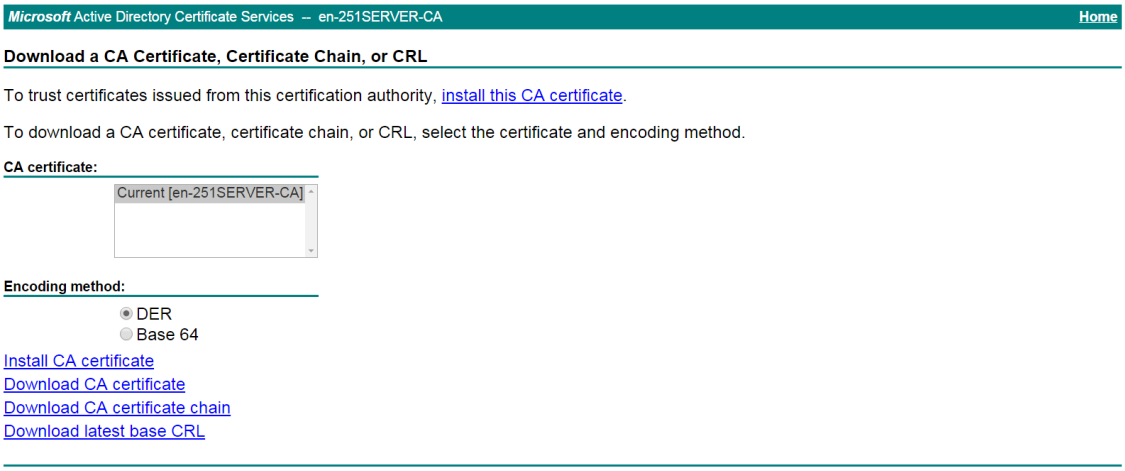
On the certificate service home page shown in Figure 12, click **Download a CA certificate, certificate chain, or CRL**.

Figure 12 Certificate service home page



On the **Download a CA certificate, certificate chain, or CRL** page, click **Download CA certificate**.

Figure 13 Download a CA certificate, certificate chain, or CRL page



Save the downloaded CA certificate locally.

6. Import the CA and server certificates:

a. Import the CA certificate:

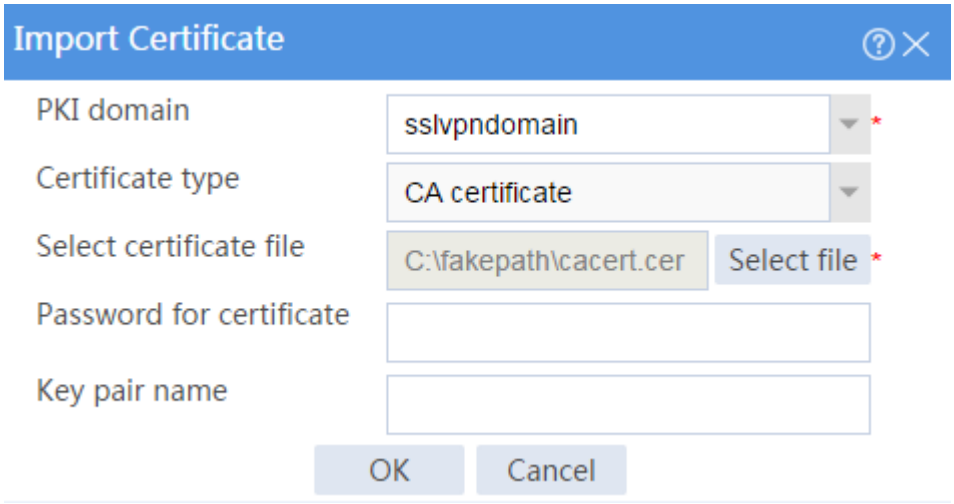
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate**.

Click **Import certificate**.

Import the locally saved CA certificate, as shown in Figure 14, and then click **OK**.

Figure 14 Importing the CA certificate

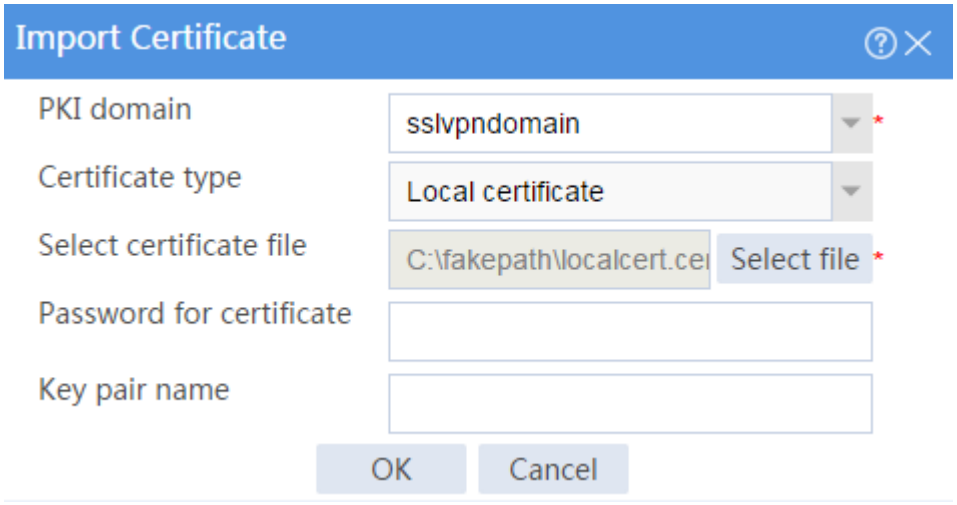


b. Import the server certificate:

On the **Certificate** page, click **Import certificate**.

Import the locally saved server certificate, as shown in Figure 15, and then click **OK**.

Figure 15 Importing the server certificate



7. Configure an SSL server policy:

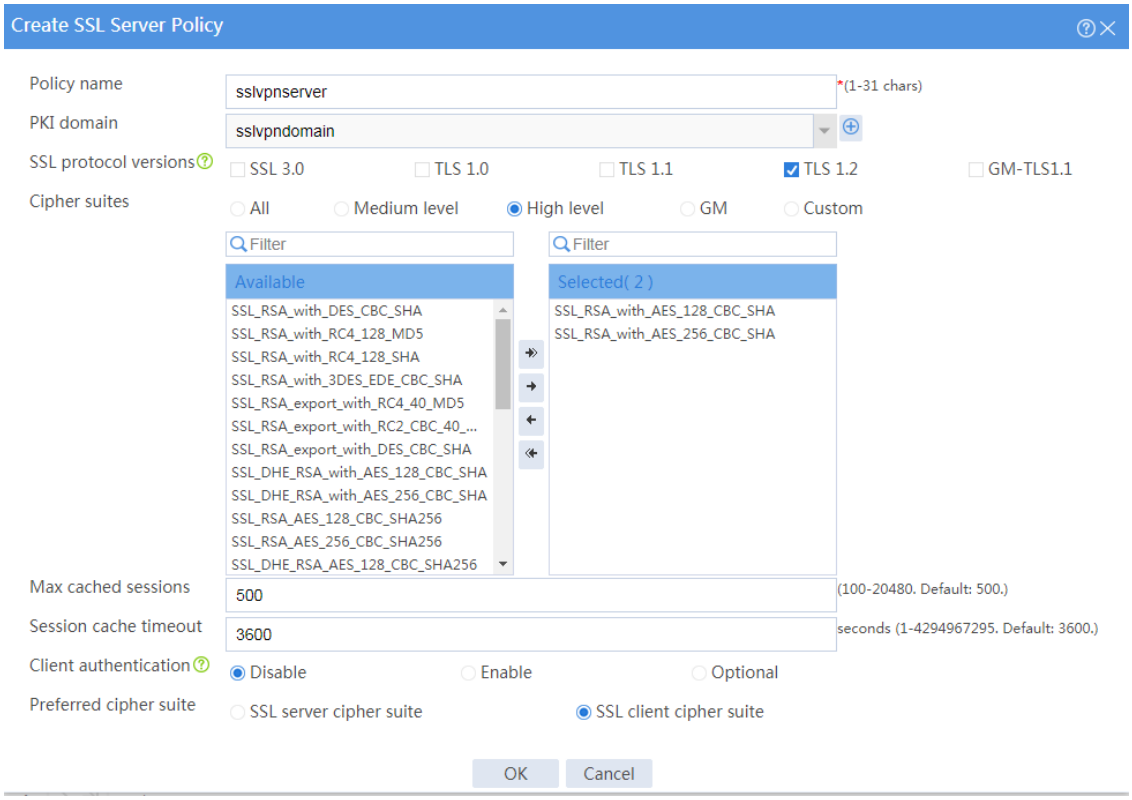
On the top navigation bar, click **Objects**.

From the navigation pane, select **SSL** > **SSL Server Policies**.

Click **Create**.

Configure an SSL server policy as shown in Figure 16, and then click **OK**.

Figure 16 Creating an SSL server policy



8. Configure the SSL VPN gateway:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

   # Click **Create**.

   # Create an SSL VPN gateway as shown in Figure 17, and then click **OK**.

Figure 17 Creating an SSL VPN gateway

9. Configure an SSL VPN context:

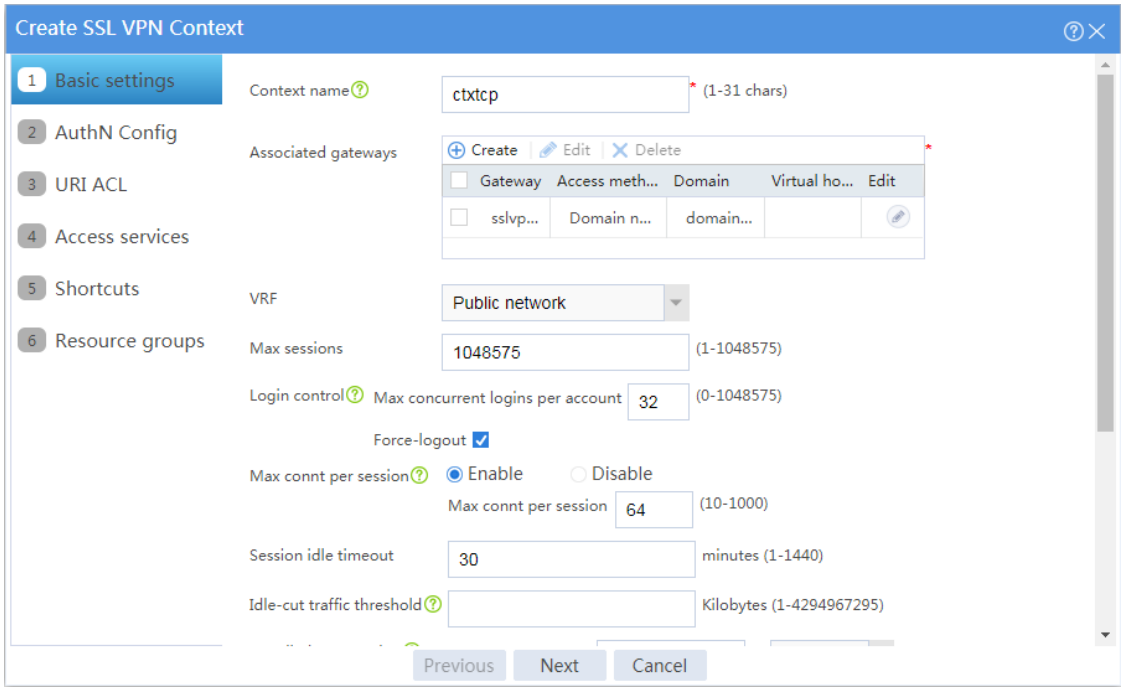
On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

Click **Create**.

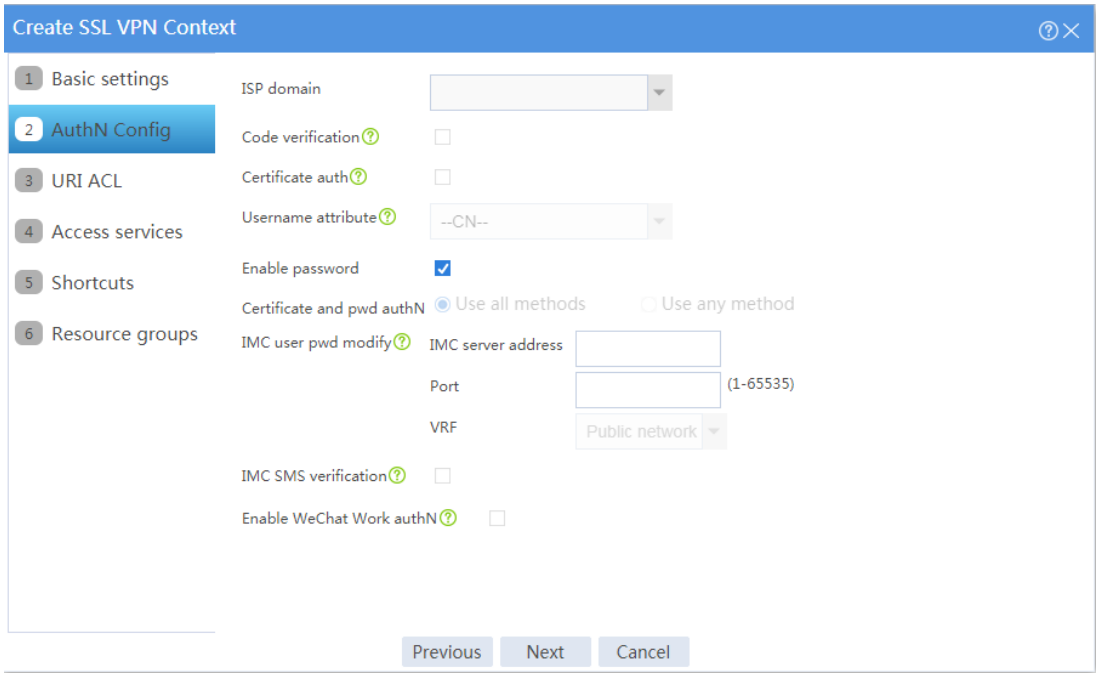
Configure the basic settings for the SSL VPN context as shown in Figure 18, and then click **Next**.

Figure 18 Creating an SSL VPN context



Configure authentication settings, as shown in Figure 19, and then click **Next**.

Figure 19 Configuring authentication settings



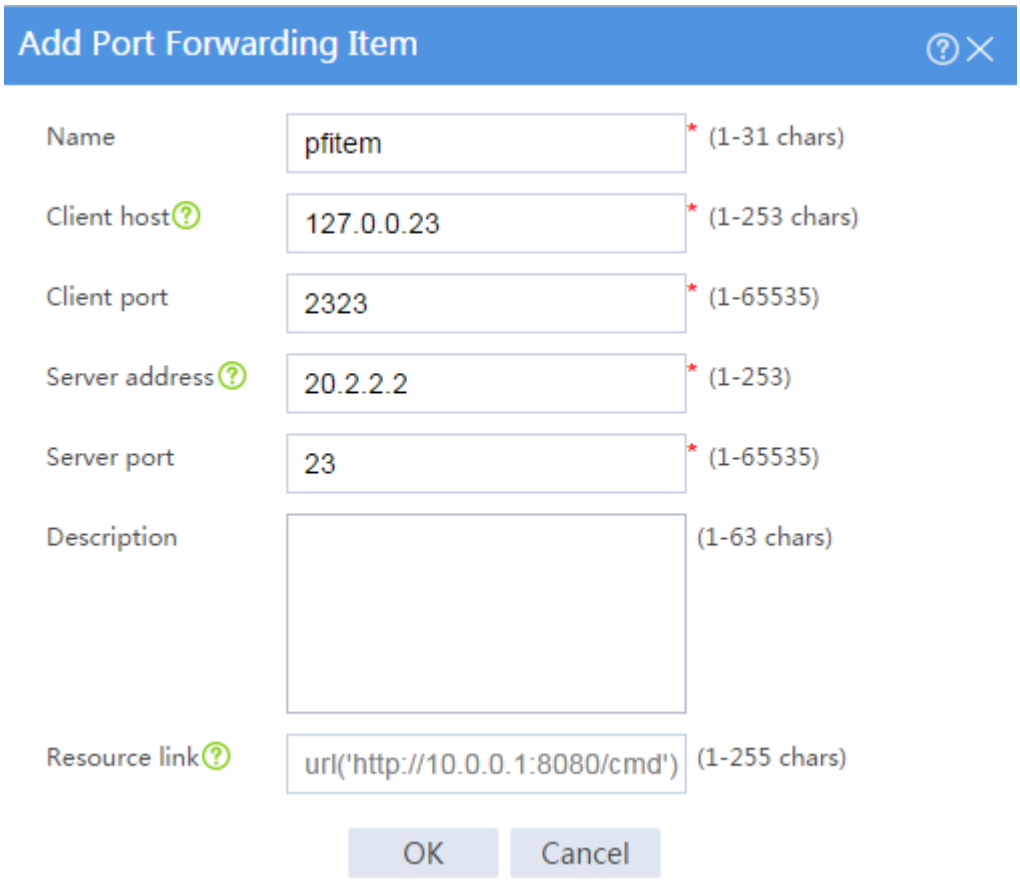
On the **URI ACL** page, click **Next**.

On the **Access services** page, select **TCP access** and click **Next**.

On the **TCP access** page, click **Create** in the **Port Forwarding Item** area.

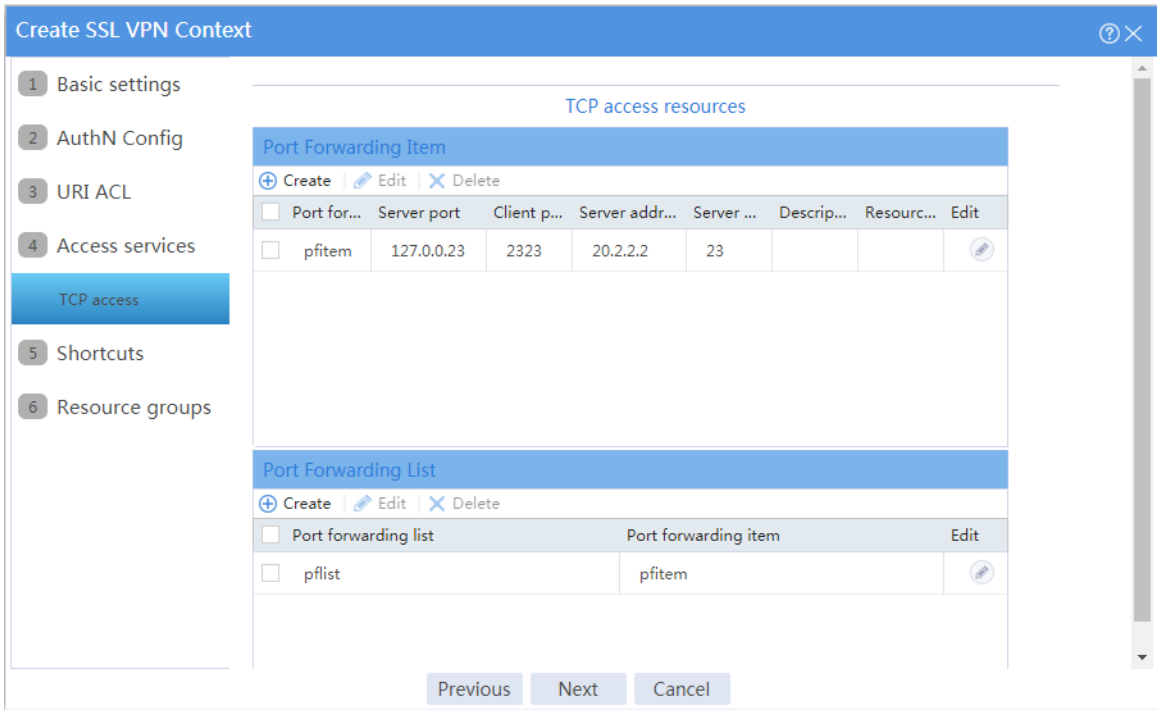
Create a port forwarding item named **pfitem** as shown in Figure 20, and then click **OK**.

Figure 20 Creating a port forwarding item



Create a port forwarding list named **pflist** and assign port forwarding item **pfitem** to it, as shown in Figure 21.

Figure 21 Configuring TCP access resources

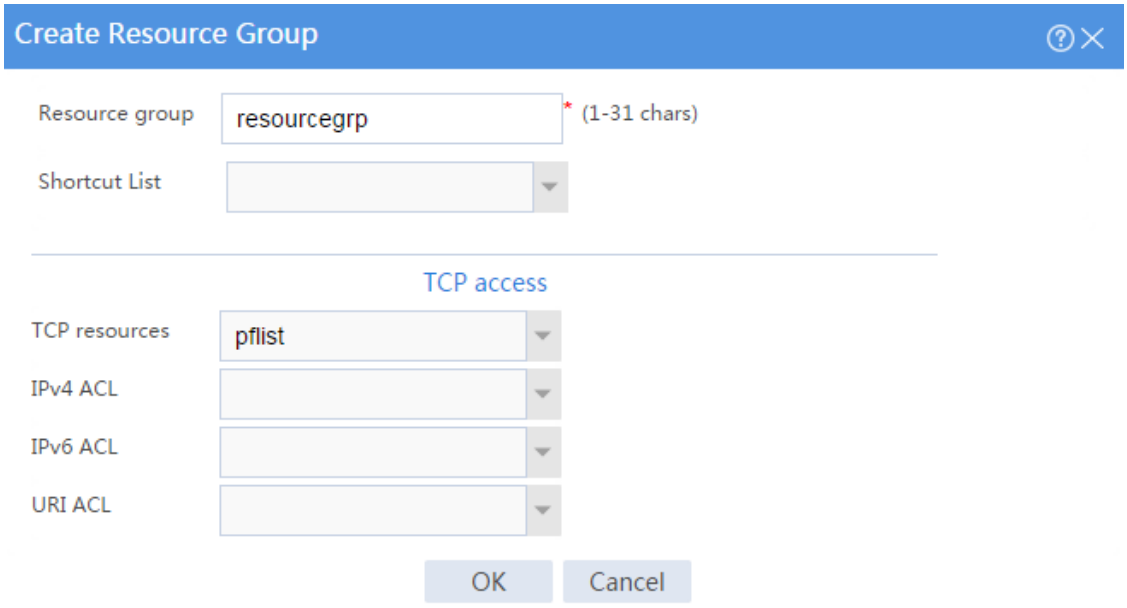


Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp** and select port forwarding list **pflist** from the **TCP resources** list, as shown in Figure 22.

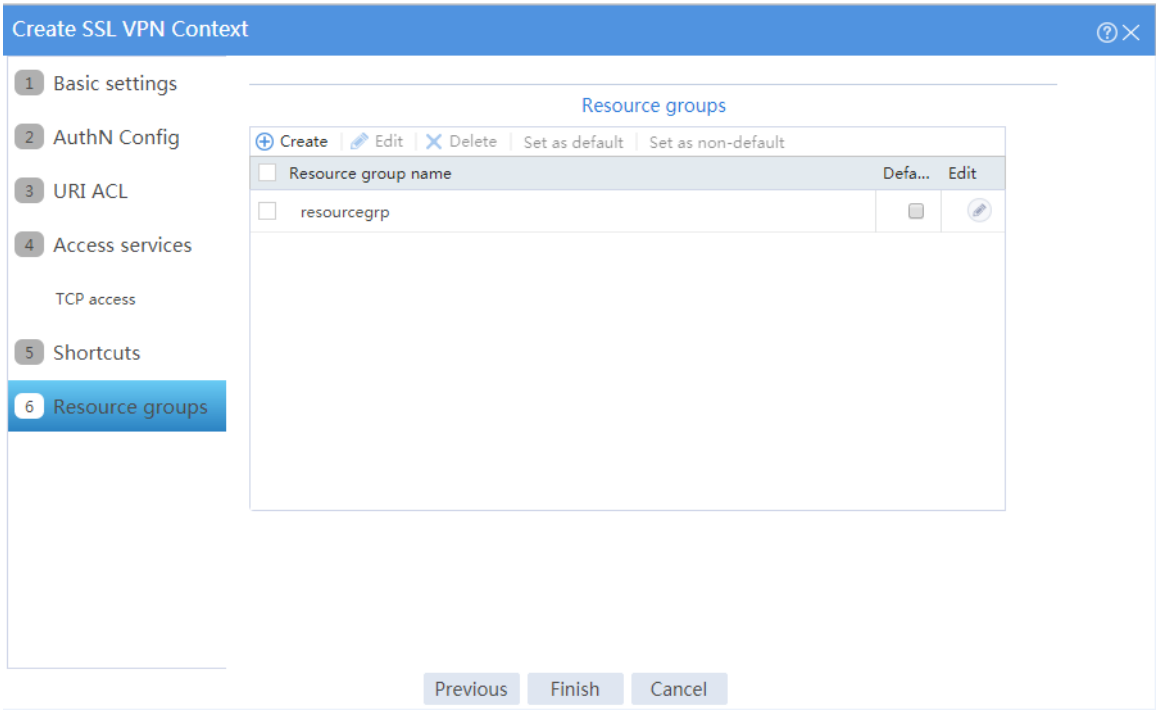
Figure 22 Creating an SSL VPN resource group



Click **OK**.

The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 23.

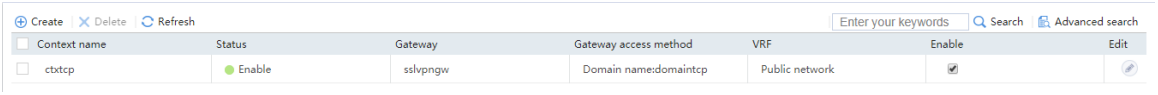
Figure 23 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 24.

Figure 24 Enabling the SSL VPN context



10. Create an SSL VPN user:

On the top navigation bar, click **Objects**.

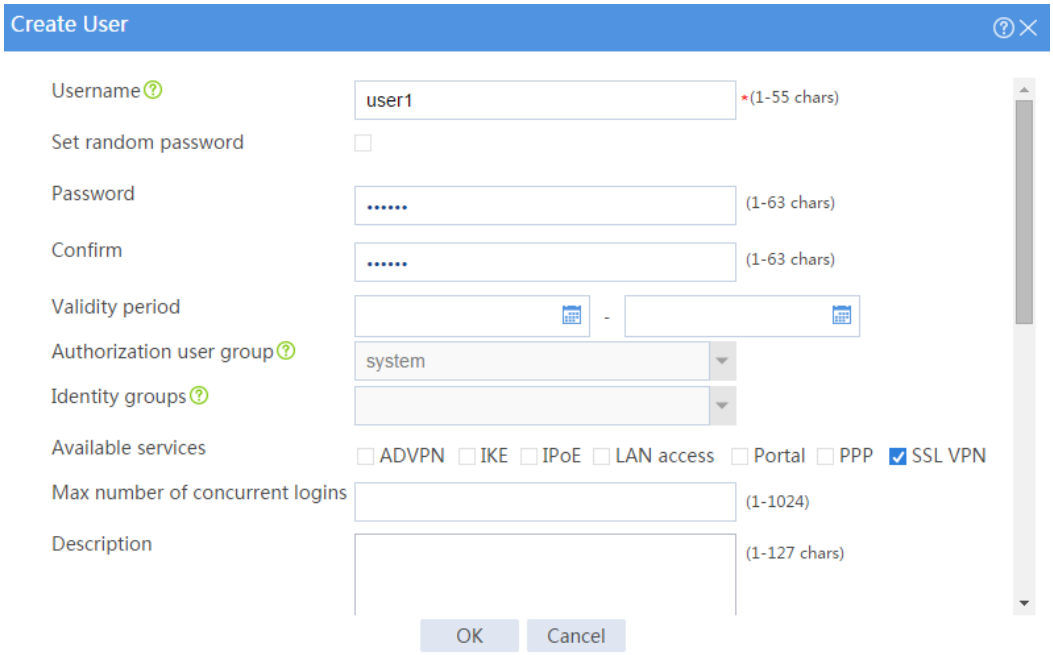
From the navigation pane, select **User** > **User Management** > **Local Users**.

Click **Create**.

Create an SSL VPN user:

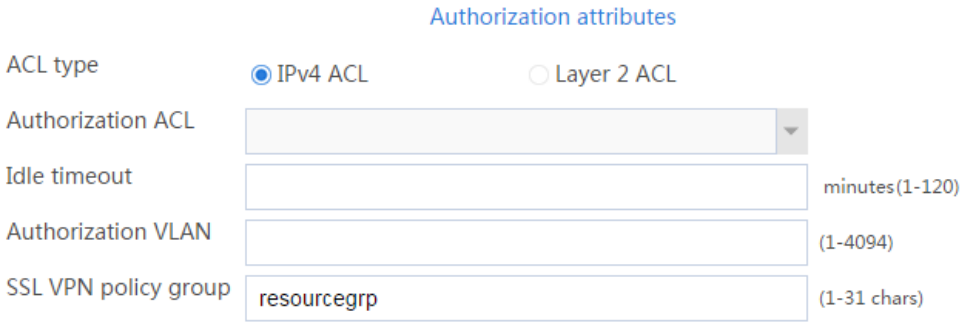
a. Set the username to **user1** and password to **123456**, and select **SSL VPN** as the available service, as shown in Figure 25.

Figure 25 Creating an SSL VPN user



b. In the **Authorization Attributes** area, authorize the user to use SSL VPN resource group **resourcegrp**, as shown in Figure 26.

Figure 26 Setting the authorization attributes for the SSL VPN user



c. Click **OK**.

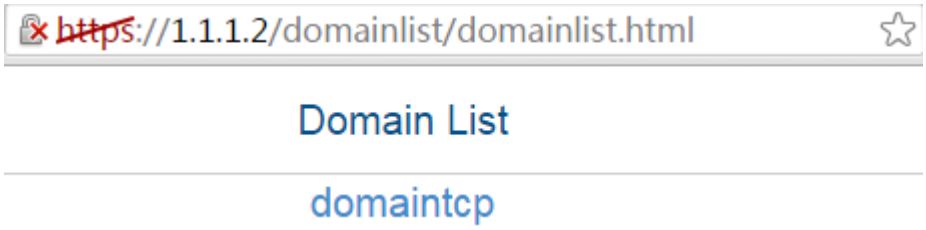
Configuring the host

Configure the IP address and gateway address settings for the host and make sure it can reach the SSL VPN gateway.

Verifying the configuration

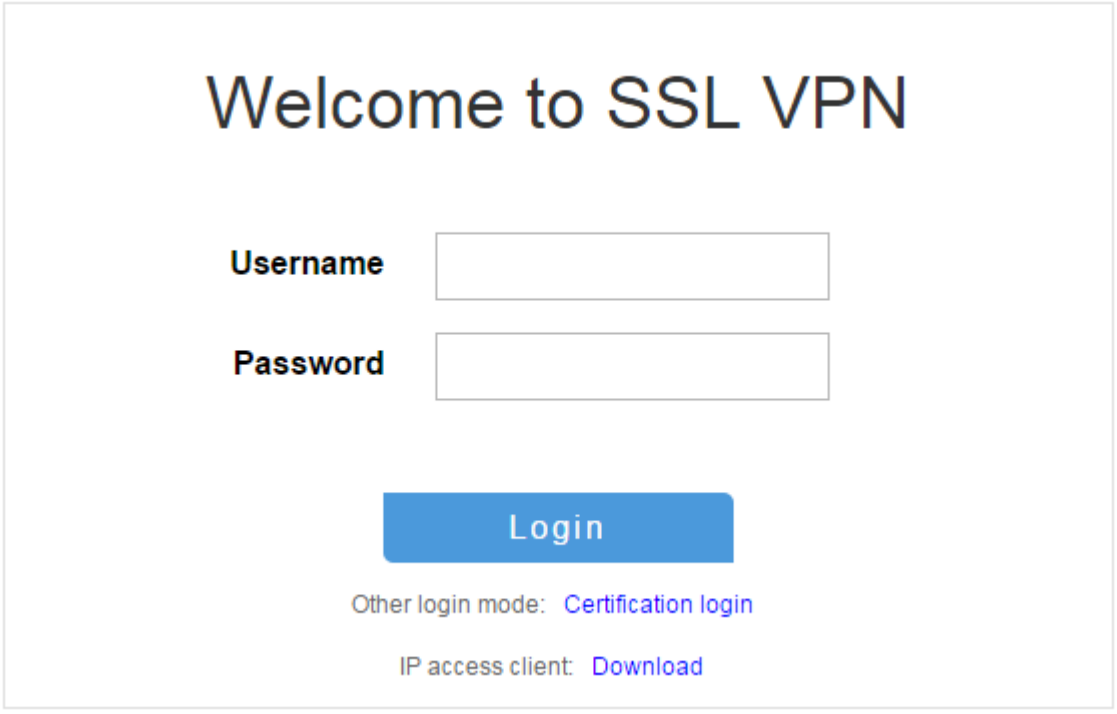
1. In the browser address bar of the host, enter **https://1.1.1.2** and press **Enter** to open the domain list page.

Figure 27 Domain list page



2. Select **domaintcp** to access the login page.
3. On the login page, enter username **user1** and password **123456**, and then click **Login**.

Figure 28 Login page



The SSL VPN home page opens, displaying the TCP resources the user can access in the **TCP Resource** area.

Figure 29 Accessible TCP resources

4. Click **START** to start the TCP client application.

   You cannot start the TCP client application by double-clicking it.

5. Telnet to local address 127.0.0.1 and local port 2323 to access the server.

Example: Configuring TCP access with a self-signed server certificate

Network configuration

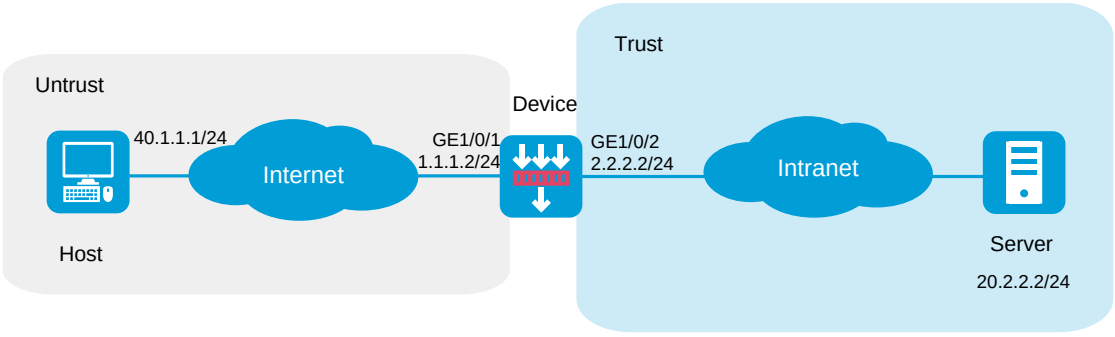
As shown in Figure 30, the device acts as the SSL VPN gateway that connects the public network and the private network. Users need secure access to the internal Telnet server in TCP access mode.

Configure the SSL VPN TCP access service on the device to allow users to access the server in TCP access mode.

Configure the device to perform local authentication and authorization for TCP access users.

The device uses a self-signed SSL server certificate.

Figure 30 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

When you configure TCP access with a self-signed server certificate, follow these restrictions and guidelines:

- Certificate-based client authentication is not available in TCP access mode.
- To start the TCP client from the Web interface, make sure the Java Runtime Environment is installed on the client host.
- To access internal resources in TCP access mode from the host, modifications to the **Hosts** file on the host might be required. Make sure you log in to the host with administrative privileges.

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click the **Network** tab.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

   This example configures static routes.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static IPv4 route to reach 40.1.1.1:

   a. Enter destination IP address **40.1.1.1**.

   b. Enter mask length **24**.

   c. Enter next hop address **1.1.1.3**.

   d. Use the default settings for other parameters.

   e. Click **OK**.

   # Configure a static IPv4 route to reach 20.2.2.2:

   a. Enter destination IP address **20.2.2.2**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **2.2.2.2**.
- Select destination IPv4 address **20.2.2.2**.
- Use the default settings for other parameters.

Click **OK**.

4. Configure the SSL VPN gateway:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

   # Click **Create**.

   # Create an SSL VPN gateway as shown in Figure 31, and then click **OK**.

Figure 31 Creating an SSL VPN gateway

5. Configure an SSL VPN context:

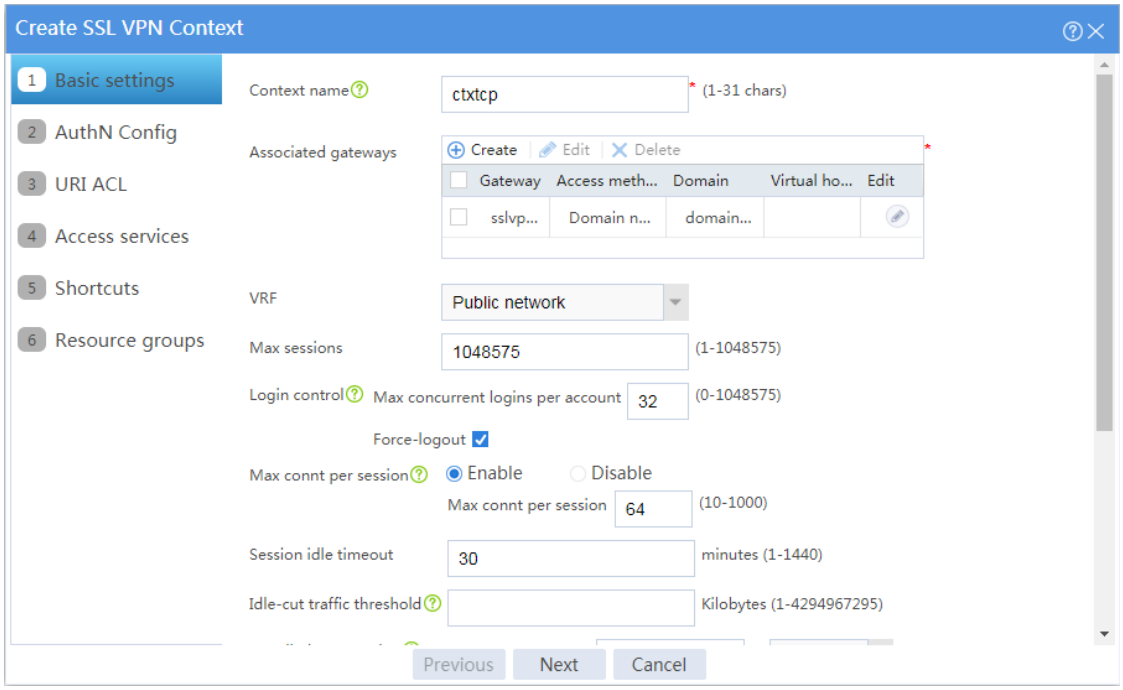
   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

   # Click **Create**.

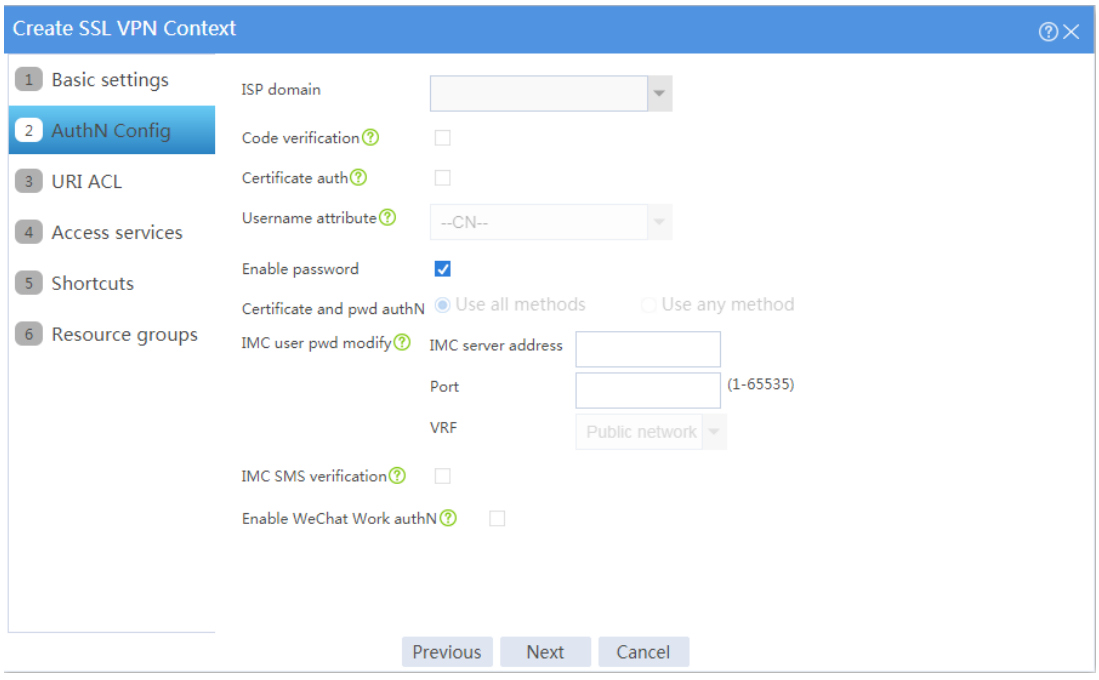
   # Configure the basic settings for the SSL VPN context as shown in Figure 32, and then click **Next**.

Figure 32 Creating an SSL VPN context



Configure authentication settings, as shown in Figure 33, and then click **Next**.

Figure 33 Configuring authentication settings



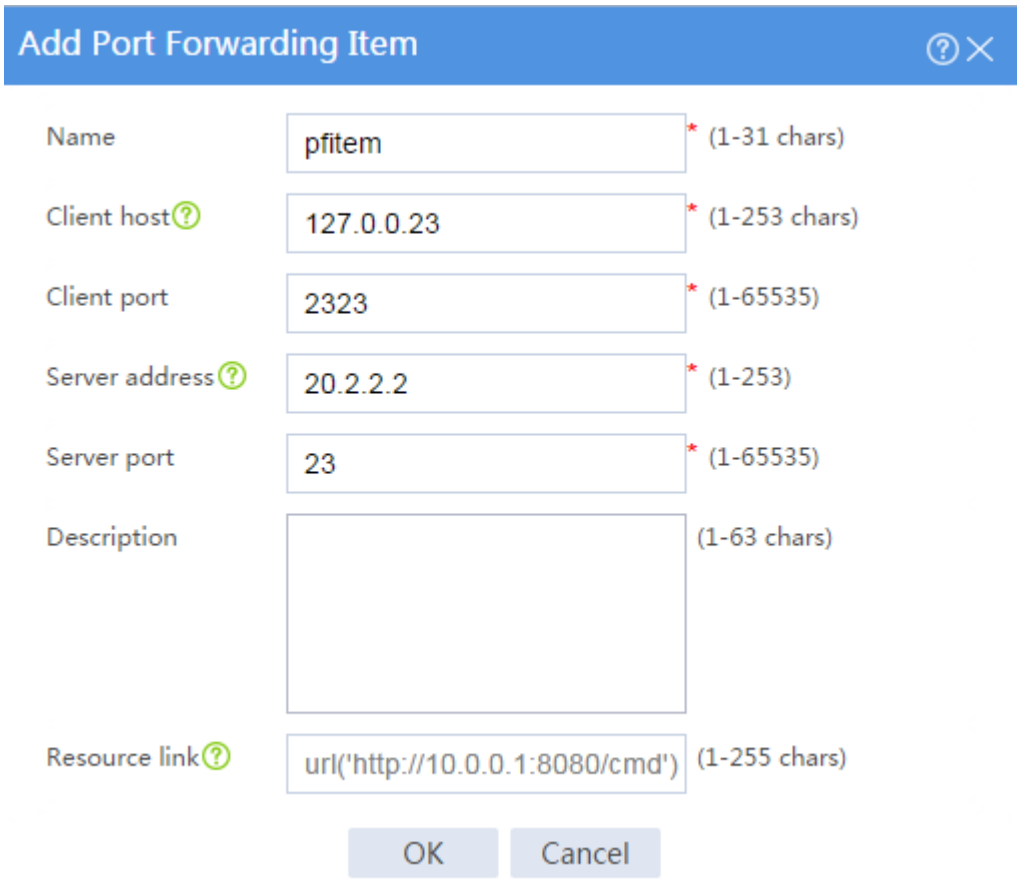
On the **URI ACL** page, click **Next**.

On the **Access services** page, select **TCP access** and click **Next**.

On the **TCP access** page, click **Create** in the **Port Forwarding Item** area.

Create a port forwarding item named **pfitem** as shown in Figure 34, and then click **OK**.

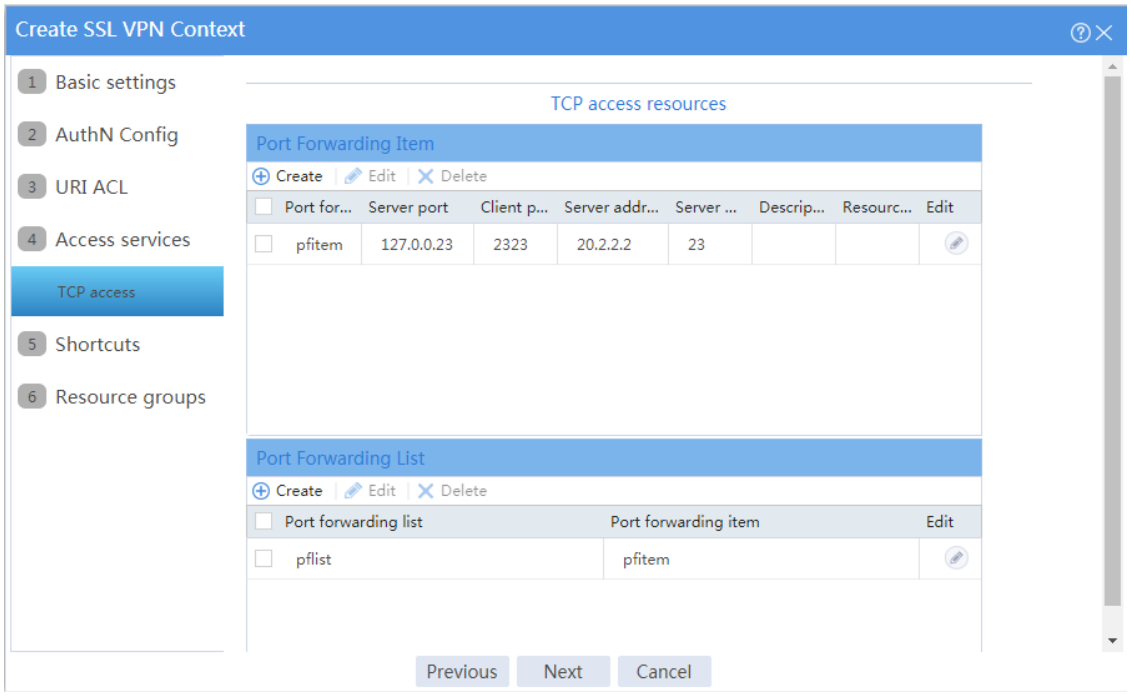
Figure 34 Creating a port forwarding item



Click **Create** in the **Port Forwarding List** area.

Create a port forwarding list named **pflist** and assign port forwarding item **pfitem** to it, as shown in Figure 35.

Figure 35 Configuring TCP access resources

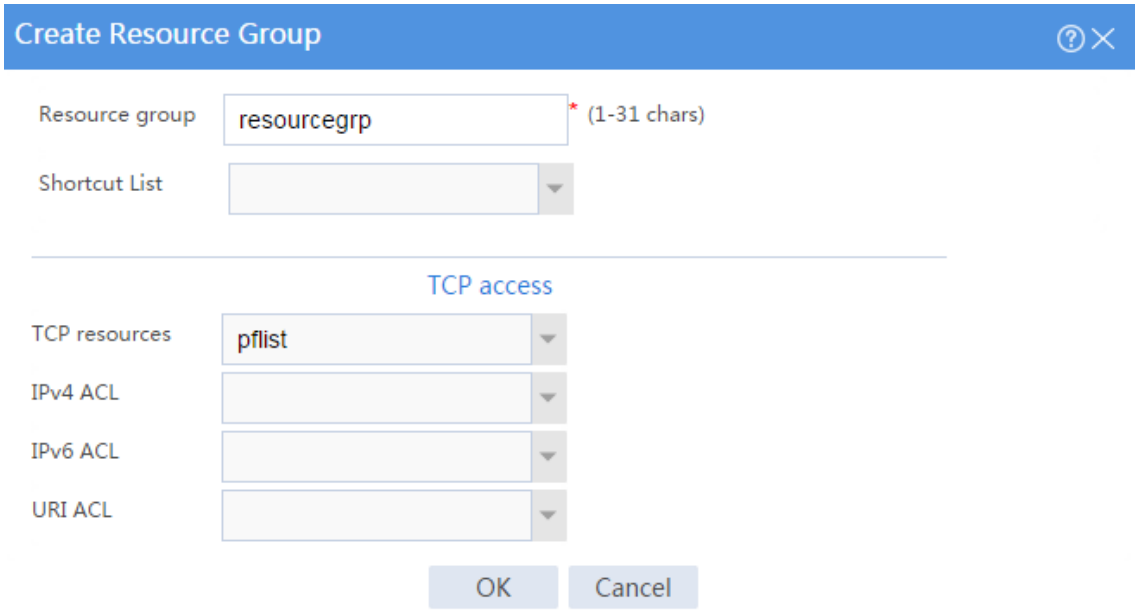


Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp** and select port forwarding list **pflist** from the **TCP resources** list, as shown in Figure 36.

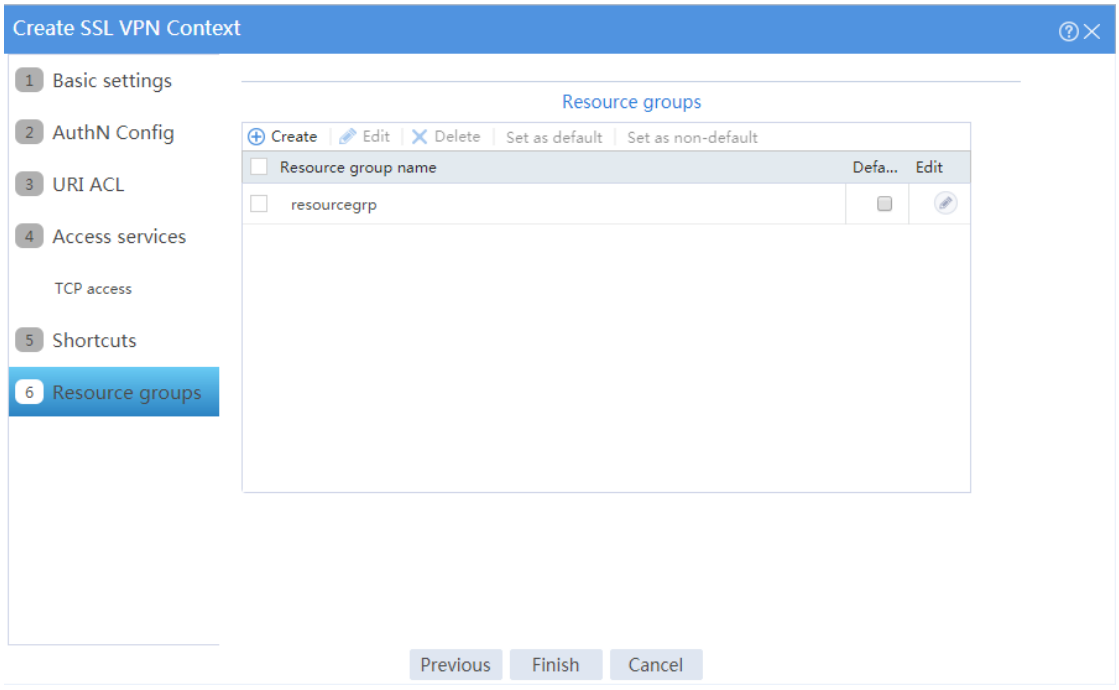
Figure 36 Creating an SSL VPN resource group



Click **OK**.

The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 37.

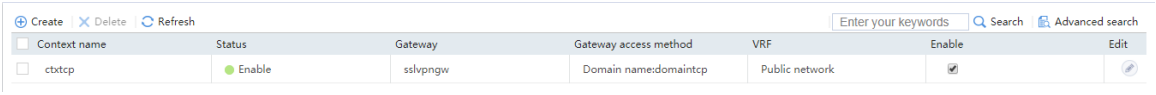
Figure 37 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 38.

Figure 38 Enabling the SSL VPN context



6. Create an SSL VPN user:

On the top navigation bar, click **Objects**.

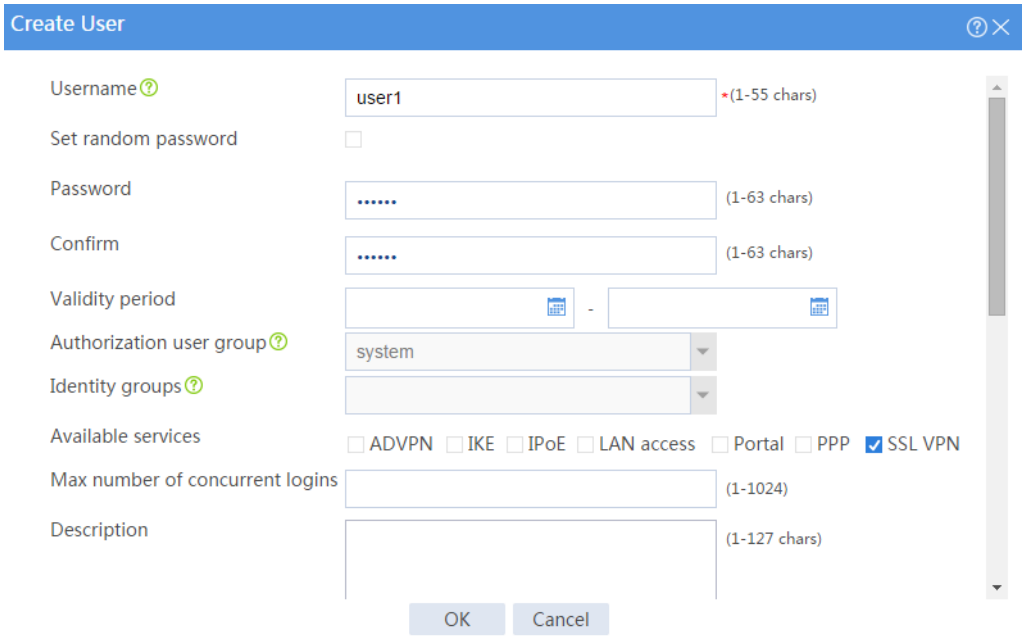
From the navigation pane, select **User** > **User Management** > **Local Users**.

Click **Create**.

Create an SSL VPN user:

a. Set the username to **user1** and password to **123456**, and select **SSL VPN** as the available service, as shown in Figure 39.

Figure 39 Creating an SSL VPN user



b. In the **Authorization Attributes** area, authorize the user to use SSL VPN resource group **resourcegrp**, as shown in Figure 40.

Figure 40 Setting the authorization attributes for the SSL VPN user

c. Click **OK**.

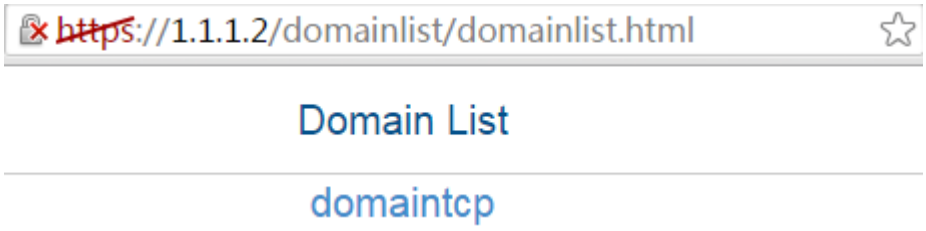
Configuring the host

Configure the IP address and gateway address settings for the host and make sure it can reach the SSL VPN gateway.

Verifying the configuration

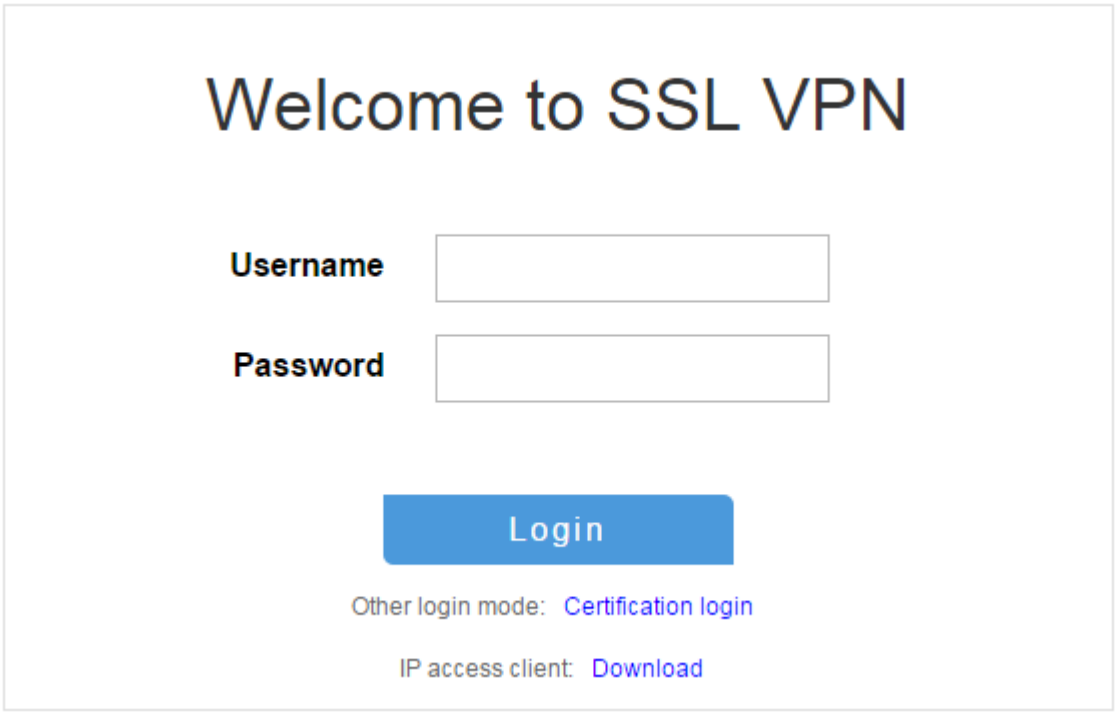
1. In the browser address bar of the host, enter **https://1.1.1.2** and press **Enter** to open the domain list page.

Figure 41 Domain list page



2. Select **domaintcp** to access the login page.
3. On the login page, enter username **user1** and password **123456**, and then click **Login**.

Figure 42 Login page



The SSL VPN home page opens, displaying the TCP resources the user can access in the **TCP Resource** area.

Figure 43 Accessible TCP resources

4. Click **START** to start the TCP client application.

   You cannot start the TCP client application by double-clicking it.

5. Telnet to local address 127.0.0.1 and local port 2323 to access the server.

SSL VPN Web access configuration examples

Contents

Introduction

The following information provides SSL VPN Web access configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedure and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of SSL VPN.

Example: Configuring Web access with mutual certificate authentication

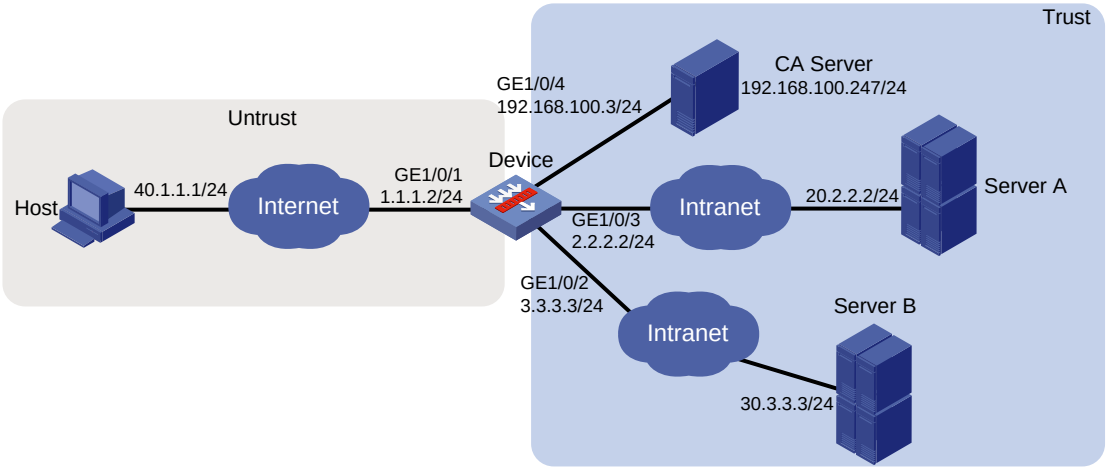
Network configuration

As shown in Figure 1, the device acts as the SSL VPN gateway that connects the public network and the private network. A Windows Server 2008 R2 CA server is deployed on the private network. Users need to access resources on internal Web servers Server A and Server B. Both Web servers use HTTP over port 80.

Configure the SSL VPN Web access service on the device to allow users to access Server A and Server B in Web access mode.

Configure the device to perform local authentication and authorization for Web access users. Require users to pass both password and certificate authentication for Web access. To enhance security, request an SSL server certificate for the device from the CA server rather than use the default certificate.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click the **Network** tab.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 3.3.3.3/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

Add GE 1/0/4 to the **Trust** security zone and set its IP address to 192.168.100.3/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

This example configures static routes.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static IPv4 route to reach 40.1.1.1:

a. Enter destination IP address **40.1.1.1**.

b. Enter mask length **24**.

c. Enter next hop address **1.1.1.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 20.2.2.2:

a. Enter destination IP address **20.2.2.2**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 30.3.3.3:

a. Enter destination IP address **30.3.3.3**.

b. Enter mask length **24**.

c. Enter next hop address **3.3.3.4**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 addresses **2.2.2.2**, **3.3.3.3**, and **192.168.100.3**.
- Select destination IPv4 addresses **20.2.2.2**, **30.3.3.3**, and **192.168.100.247**.
- Use the default settings for other parameters.

Click **OK**.

4. Request a server certificate for the device:

a. Create a certificate subject:

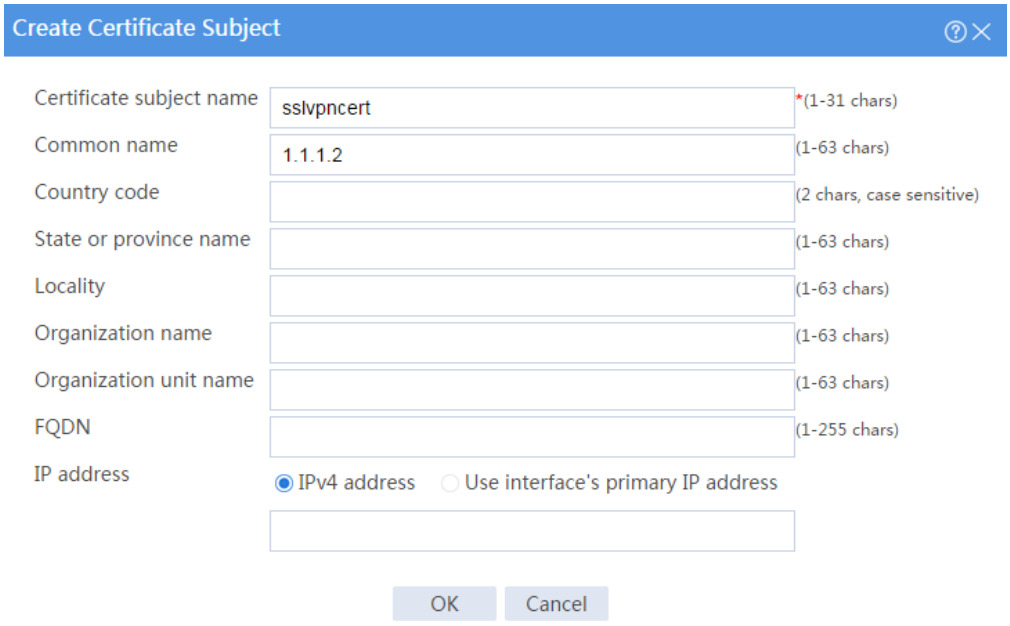
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate Subject**.

Click **Create**.

Create a certificate subject as shown in Figure 2, and the click **OK**.

Figure 2 Creating a certificate subject

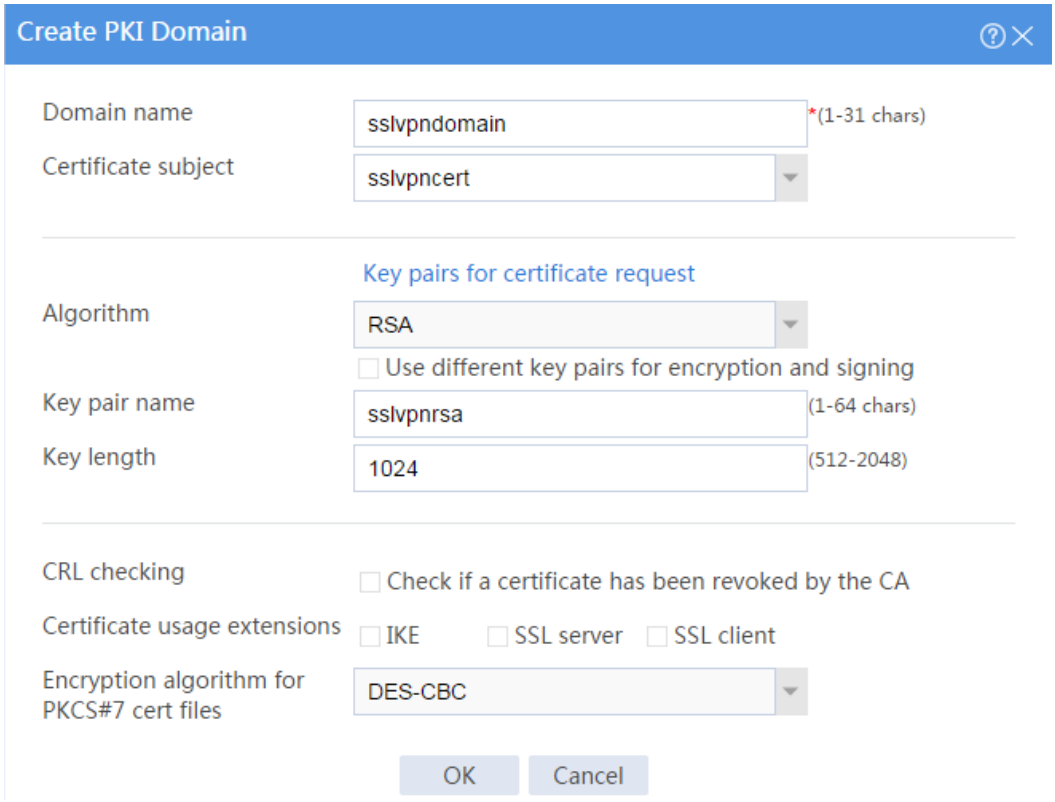


b. Create a PKI domain:

On the **Certificate** page, click **Create PKI domain**.

Create a PKI domain as shown in Figure 3, and then click **OK**.

Figure 3 Creating a PKI domain

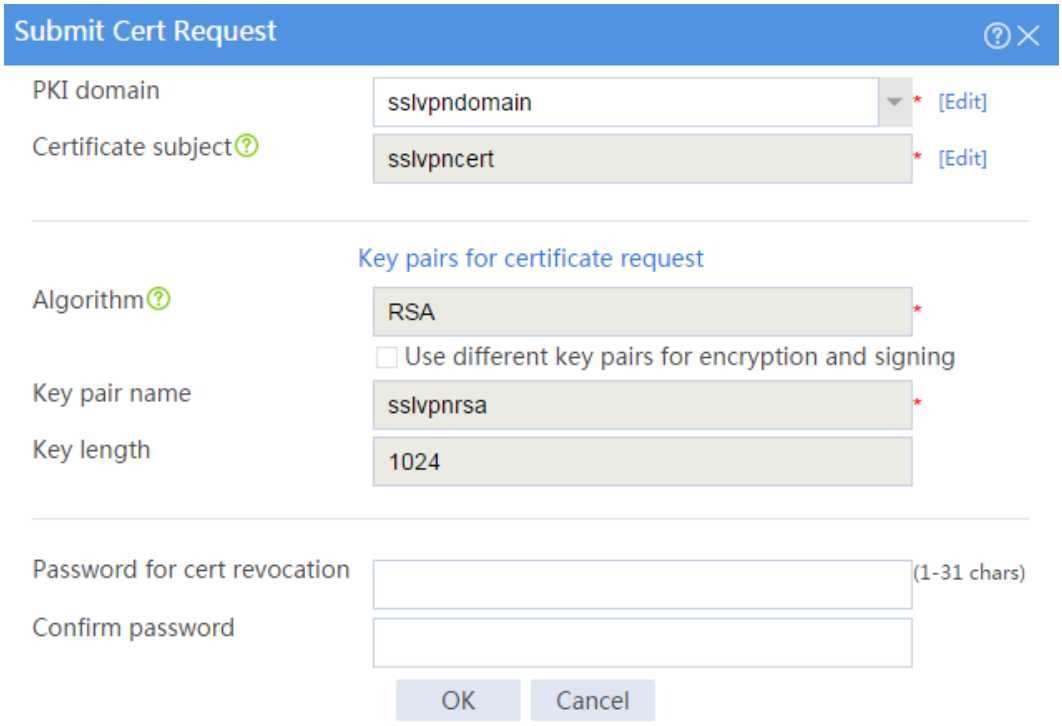


c. Create a certificate request:

On the **Certificate** page, click **Submit Cert Request**.

Configure the certificate request settings as shown in Figure 4.

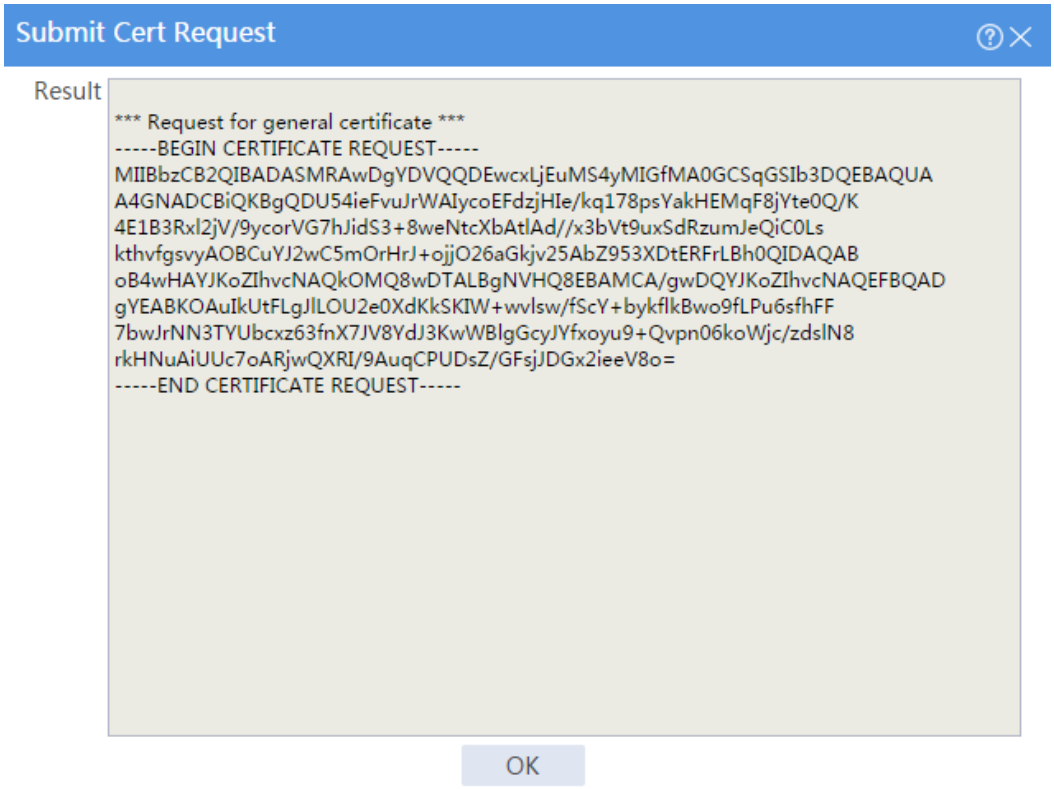
Figure 4 Creating a certificate request



Click **OK**.

The certificate request content will be displayed, as shown in Figure 5.

Figure 5 Certificate request content



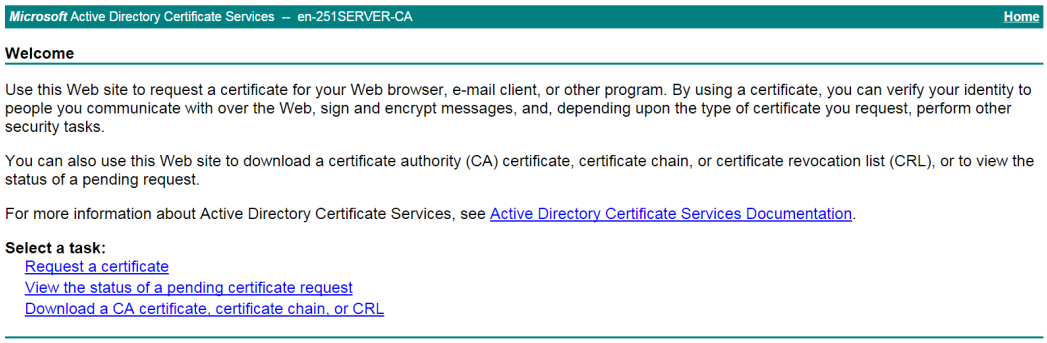
Copy the certificate request content and click **OK**.

d. Request a server certificate from the CA:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 6, click **Request a certificate**.

Figure 6 Certificate service home page

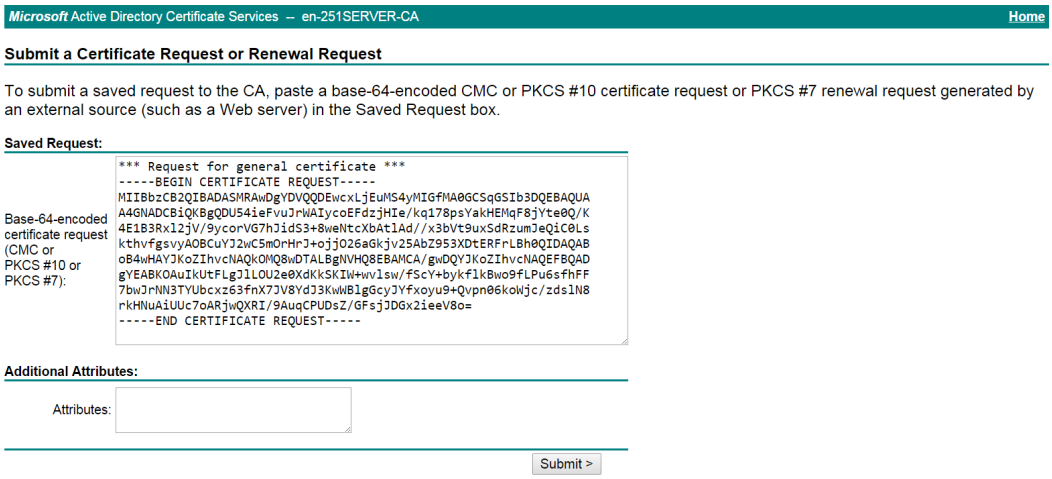


On the **Request a Certificate** page shown in Figure 7, click **advanced certificate request**.

Figure 7 Request a Certificate page

Paste the previously copied certificate request content in the **Base-64-encoded certificate request CMC or PKCS # 10 or PKCS # 7)** field, as shown in Figure 8.

Figure 8 Pasting the certificate request content

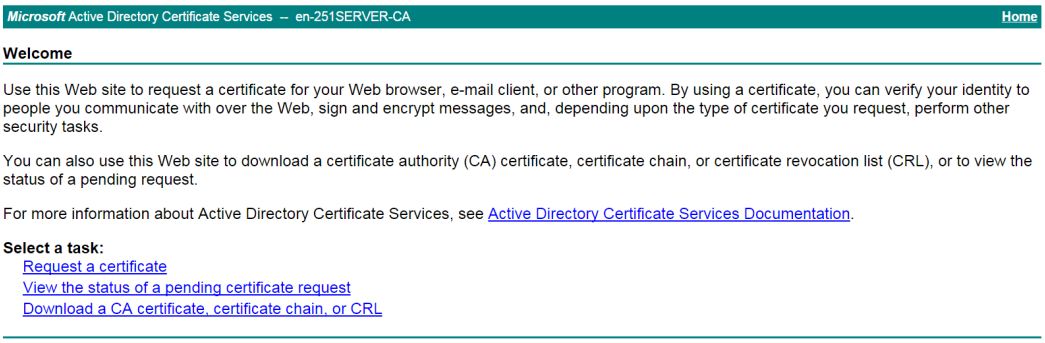


Click **Submit**.

After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

On the certificate service home page shown in Figure 9, click **View the status of a pending certificate request**.

Figure 9 Certificate service home page



Select the certificate request you want to view.

Figure 10 View the Status of a Pending Certificate Request page

The **Certificate Issued** page opens, indicating that the requested server certificate has been issued, as shown in Figure 11.

Figure 11 Certificate Issued page

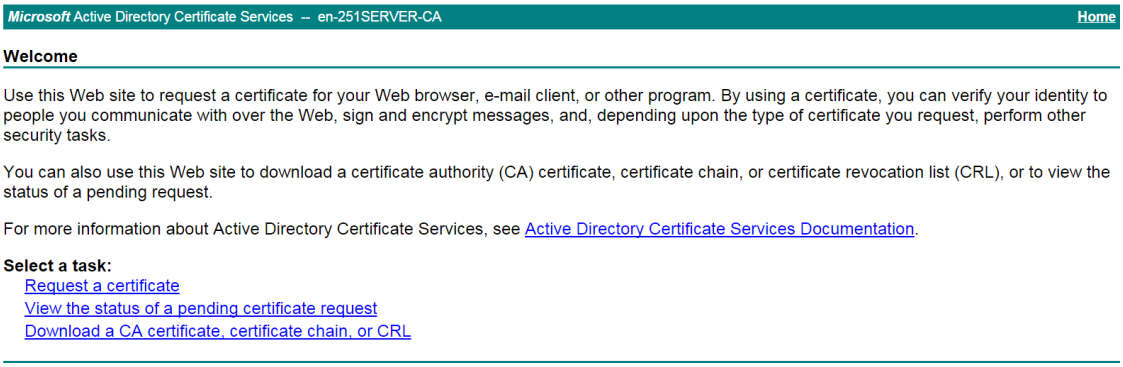
Click **Download certificate** to download the server certificate and save it locally.

5. Download the CA certificate:

Enter **http://192.168.100.247/certsrv** in the browser address bar.

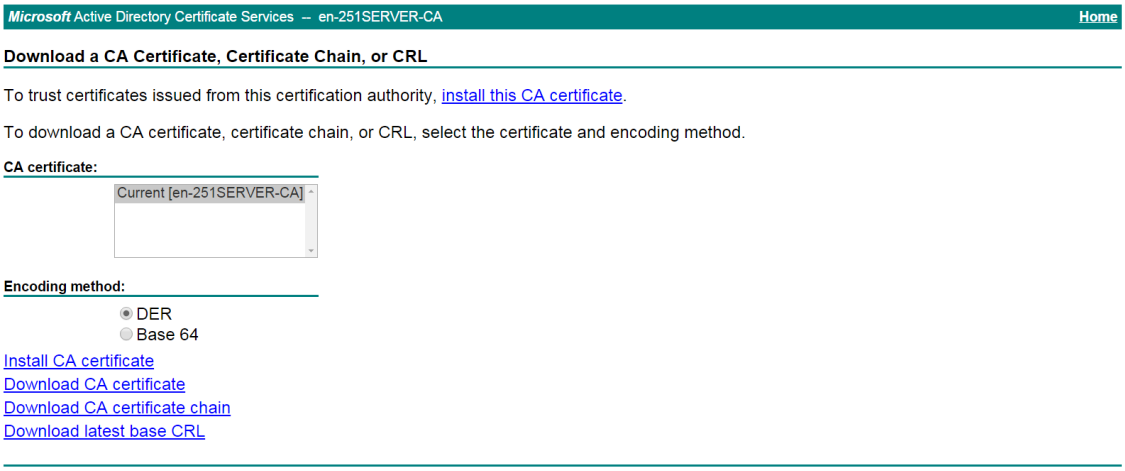
On the certificate service home page shown in Figure 12, click **Download a CA certificate, certificate chain, or CRL**.

Figure 12 Certificate service home page



On the **Download a CA certificate, certificate chain, or CRL** page shown in Figure 13, click **Download CA certificate**.

Figure 13 Download a CA certificate, certificate chain, or CRL page



Save the downloaded CA certificate locally.

6. Import the CA certificate and server certificate to the PKI domain:

a. Import the CA certificate:

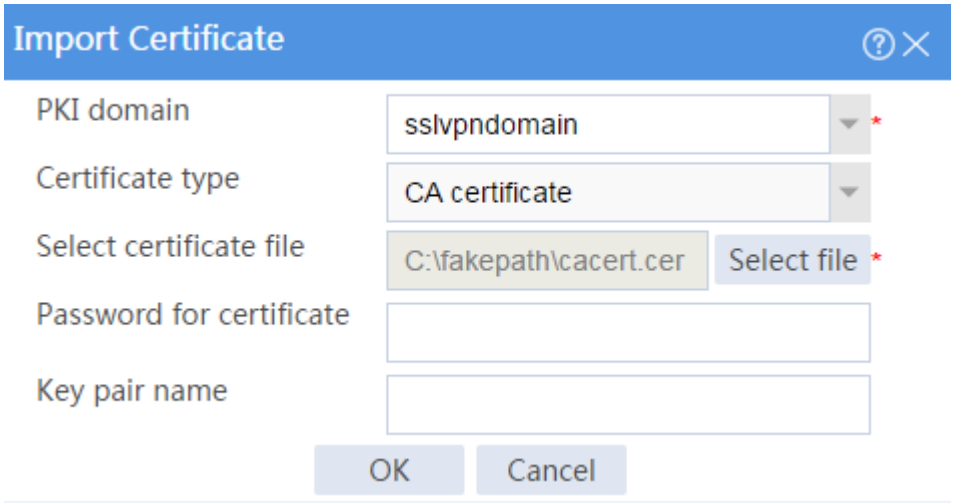
On the top navigation bar, click **Objects**.

From the navigation pane, select **PKI** > **Certificate**.

Click **Import certificate**.

Import the locally saved CA certificate, as shown in Figure 14, and then click **OK**.

Figure 14 Importing the CA certificate

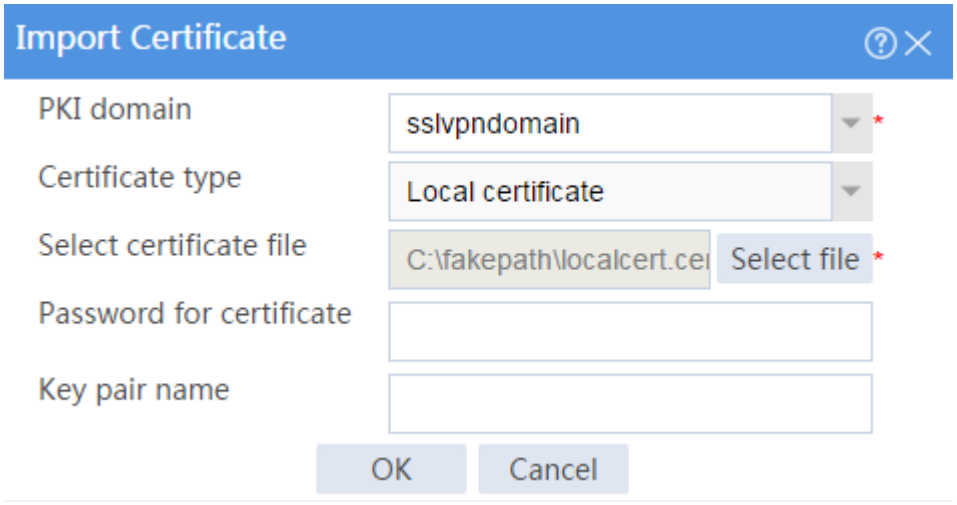


b. Import the server certificate:

On the **Certificate** page, click **Import certificate**.

Import the locally saved server certificate, as shown in Figure 15, and then click **OK**.

Figure 15 Importing the server certificate



7. Configure an SSL server policy:

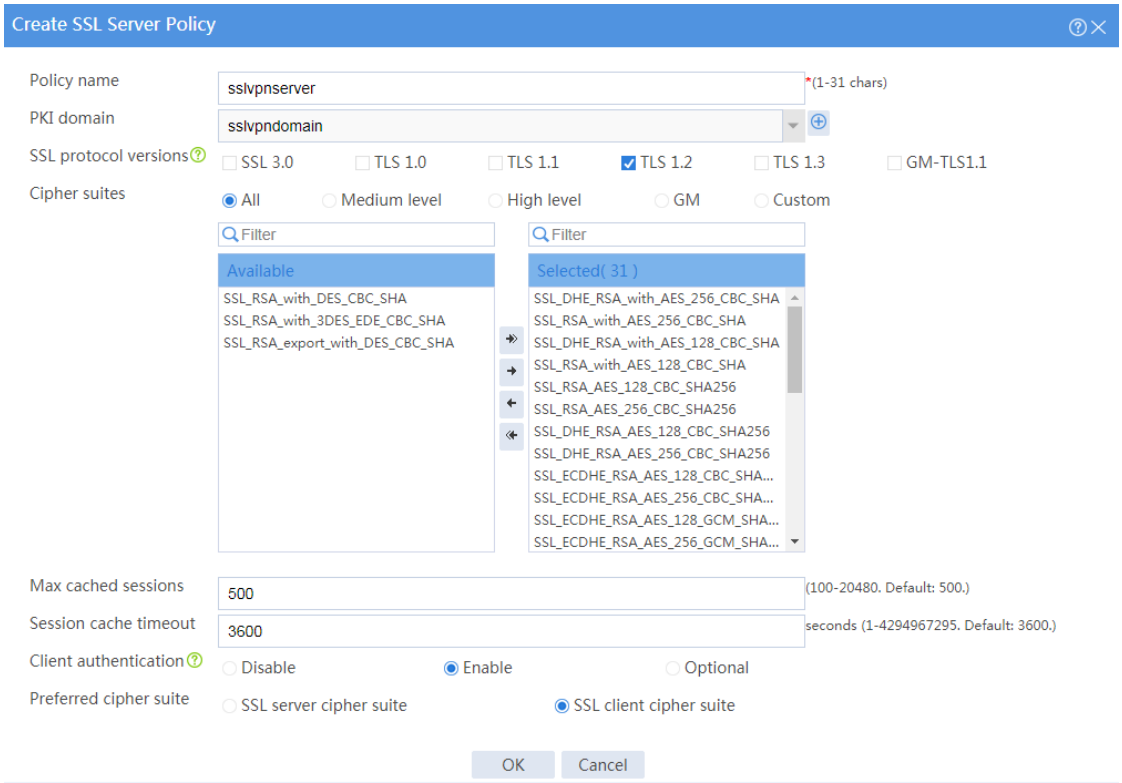
On the top navigation bar, click **Objects**.

From the navigation pane, select **SSL** > **SSL Server Policies**.

Click **Create**.

Configure an SSL server policy as shown in Figure 16, and then click **OK**.

Figure 16 Creating an SSL server policy



8. Configure an SSL client policy:

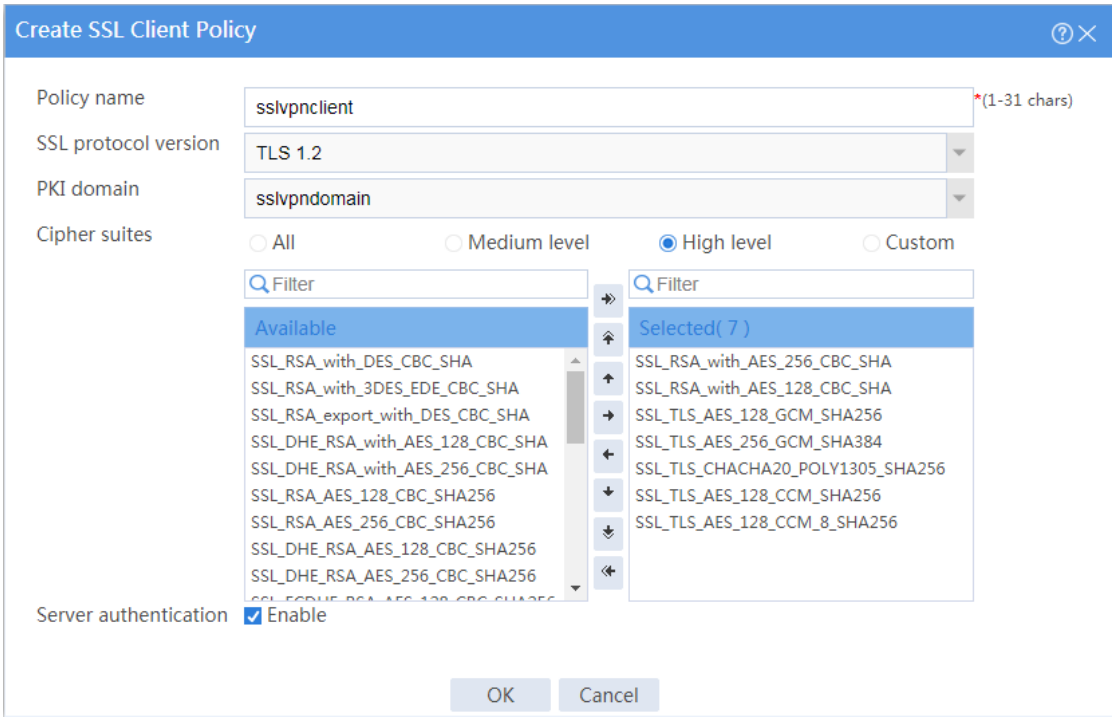
   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **SSL** > **SSL Client Policies**.

   # Click **Create**.

   # Configure an SSL client policy as shown in Figure 17, and then click **OK**.

Figure 17 Creating an SSL client policy



9. Configure the SSL VPN gateway:

On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

Click **Create**.

Create an SSL VPN gateway as shown in Figure 18, and then click **OK**.

Figure 18 Creating an SSL VPN gateway

10. Configure an SSL VPN context:

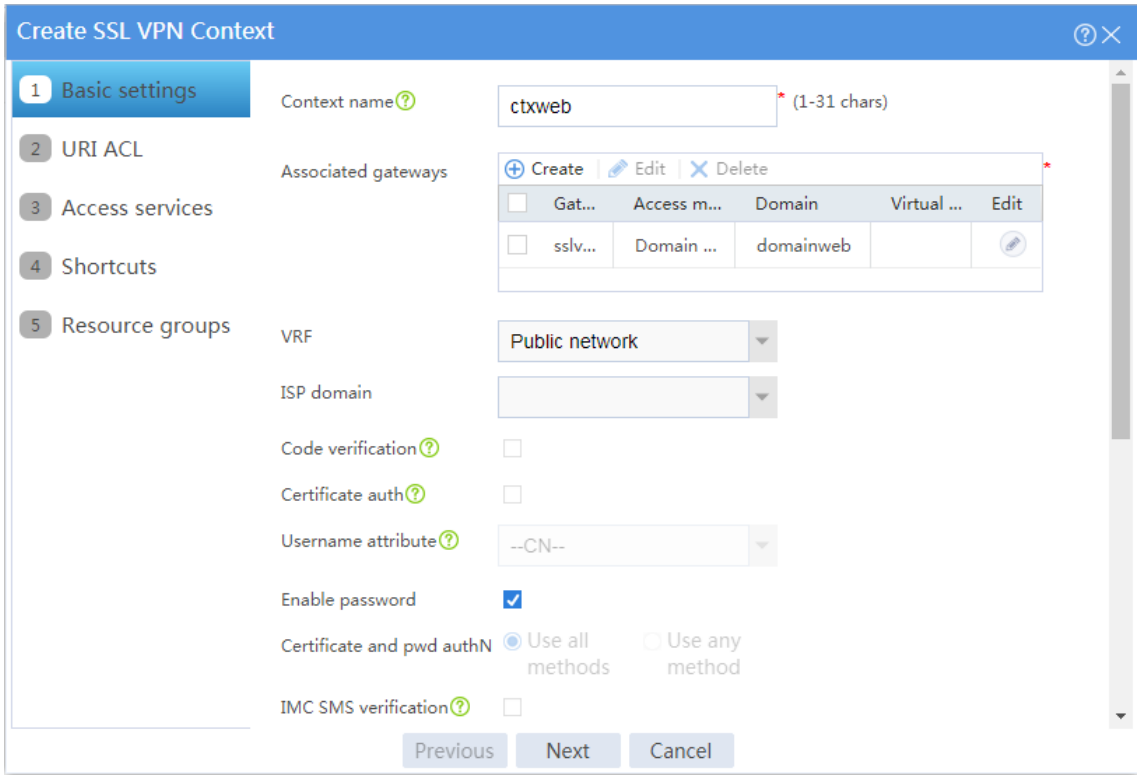
On the top navigation bar, click **Network**.

From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

Click **Create**.

Configure the basic settings for the SSL VPN context as shown in Figure 42, and then click **Next**.

Figure 19 Configuring basic settings for an SSL VPN context



On the **URI ACL** page, click **Next**.

On the **Access services** page, select **Web access** and click **Next**.

On the **Web access** page, configure the Web access service as follows:

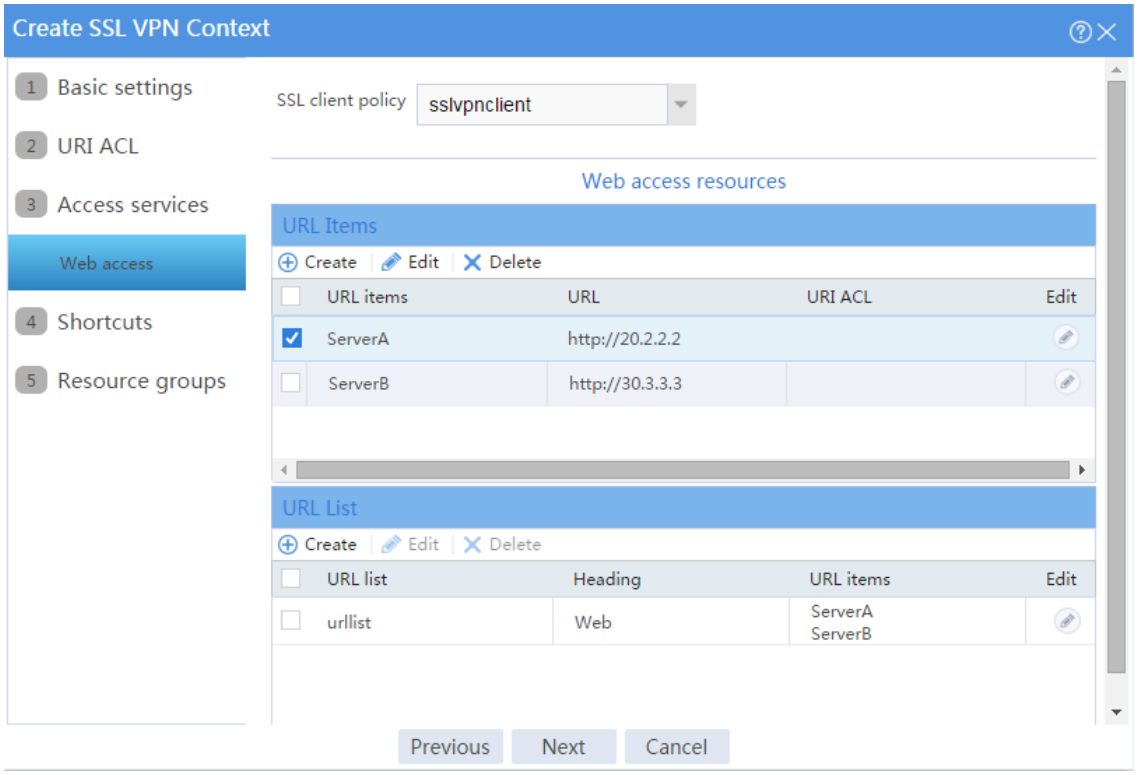
a. Select **sslvpnclient** from the **SSL client policy** list.

b. Configure two URL items pointing to Server A and Server B, respectively.

c. Add the two URL items to URL list **urllist**.

d. Click **Next**.

Figure 20 Configuring the Web access service



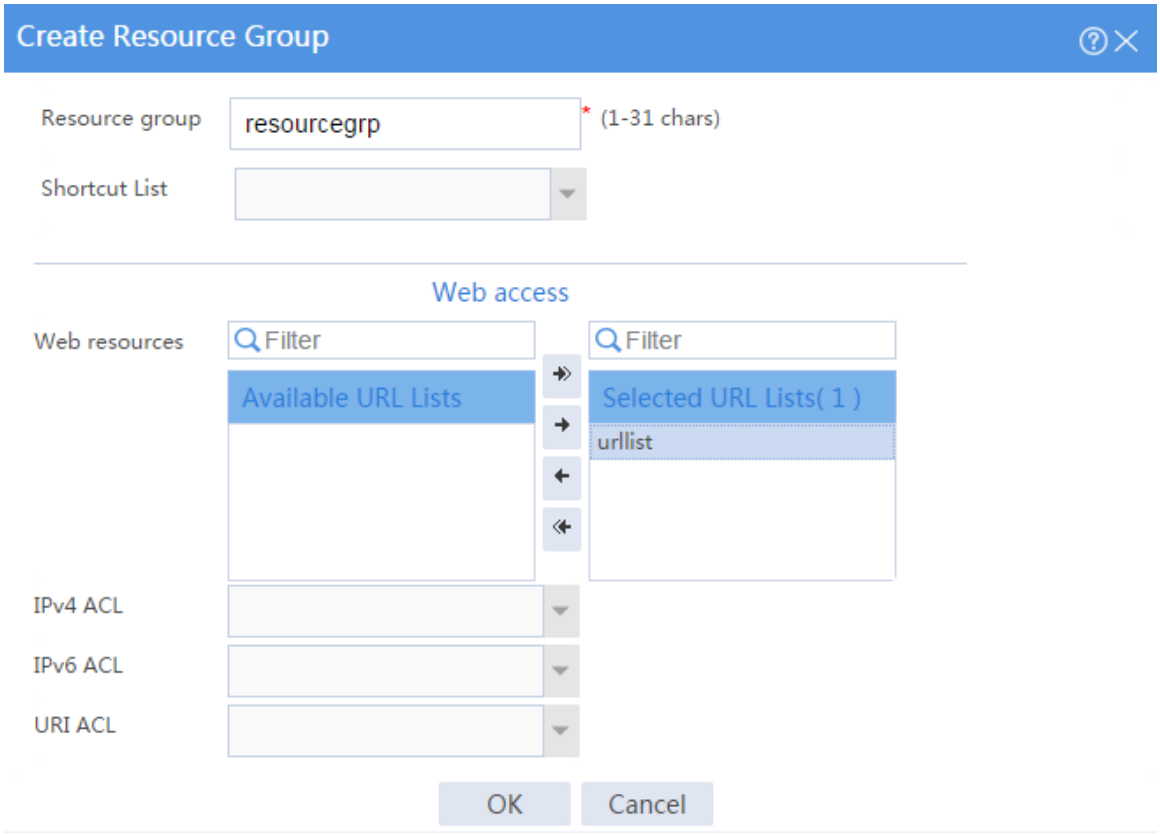
Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp** and select URL list **urllist** as the accessible Web resources, as shown in Figure 21.

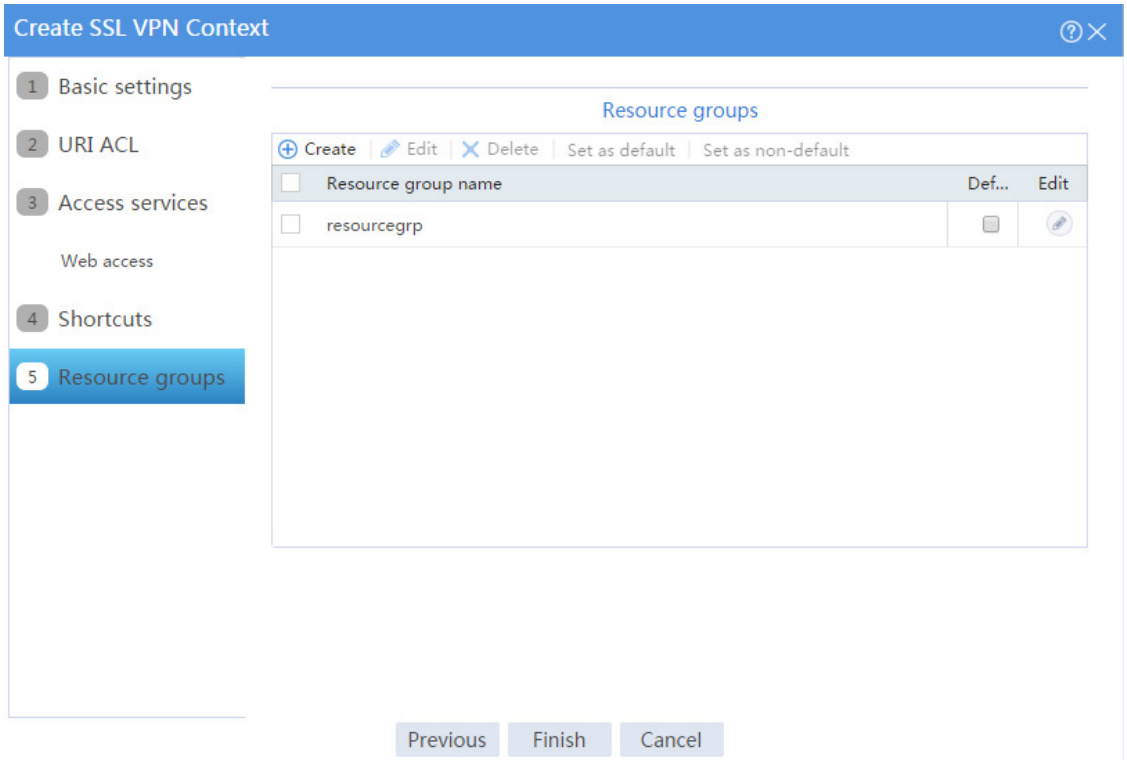
Click **OK**.

Figure 21 Creating an SSL VPN resource group



The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 22.

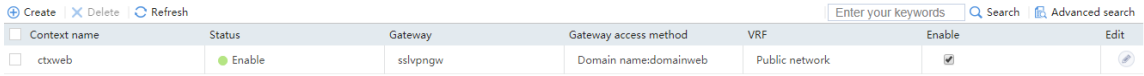
Figure 22 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 23.

Figure 23 Enabling the SSL VPN context



11. Create an SSL VPN user:

On the top navigation bar, click **Objects**.

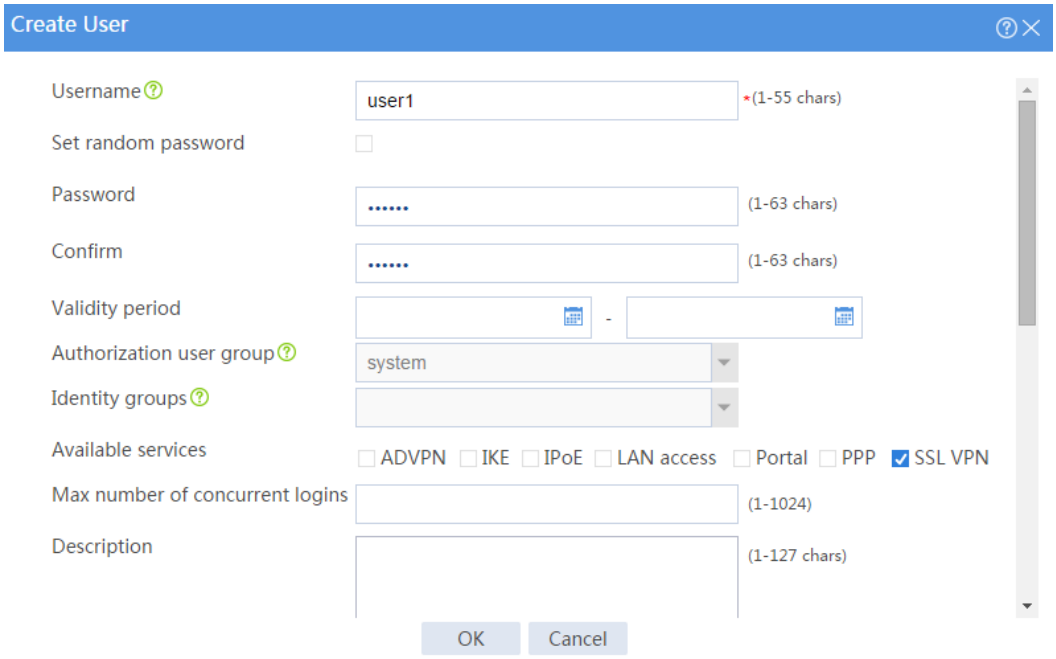
From the navigation pane, select **User** > **User Management** > **Local Users**.

Click **Create**.

Create an SSL VPN user:

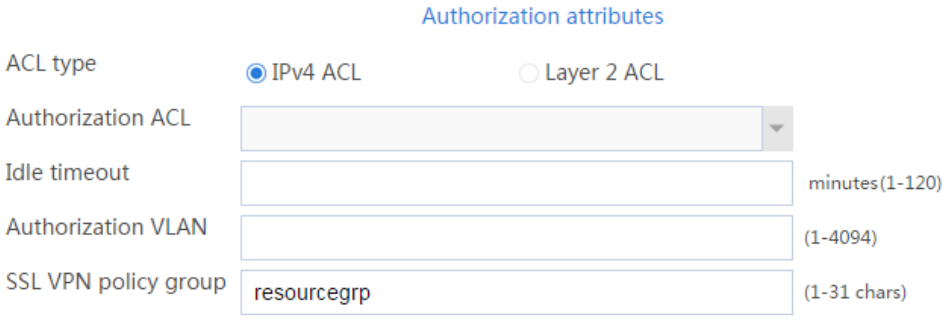
a. Set the username to **user1** and password to **123456**, and select **SSL VPN** as the available service, as shown in Figure 24.

Figure 24 Creating an SSL VPN user



b. In the **Authorization Attributes** area, authorize the user to use SSL VPN resource group **resourcegrp**, as shown in Figure 25.

Figure 25 Setting the authorization attributes for the SSL VPN user



c. Click **OK**.

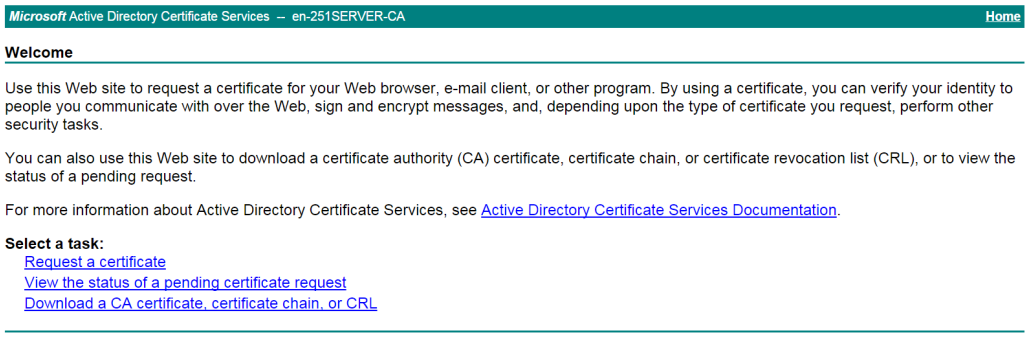
Configuring the host

1. Configure the IP address and gateway address settings for the host and make sure it can reach the SSL VPN gateway and the CA server.
2. Submit a client certificate request to the CA server:

a. Enter **http://192.168.100.247/certsrv** in the browser address bar.

b. On the certificate service home page shown in Figure 26, click **Request a certificate**.

Figure 26 Certificate service home page

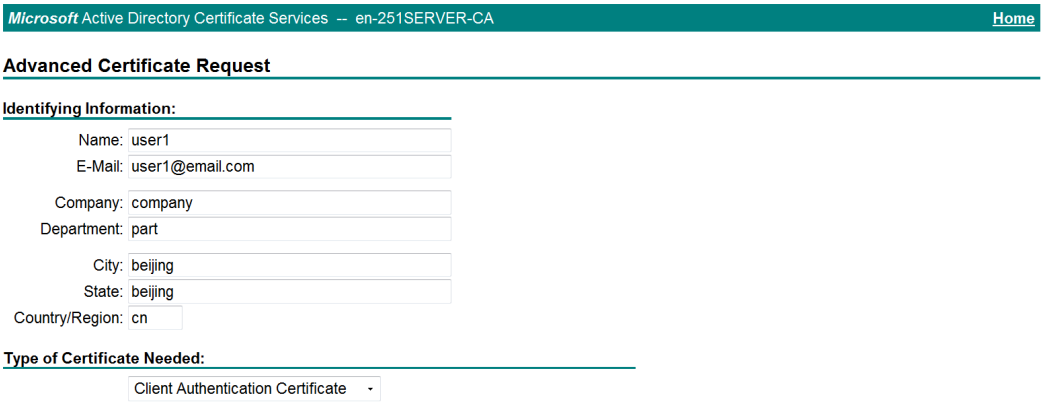


c. On the **Request a Certificate** page shown in Figure 27, click **advanced certificate request**.

Figure 27 Request a Certificate page

d. Create a client certificate request, as shown in Figure 28.

Figure 28 Creating a client certificate request



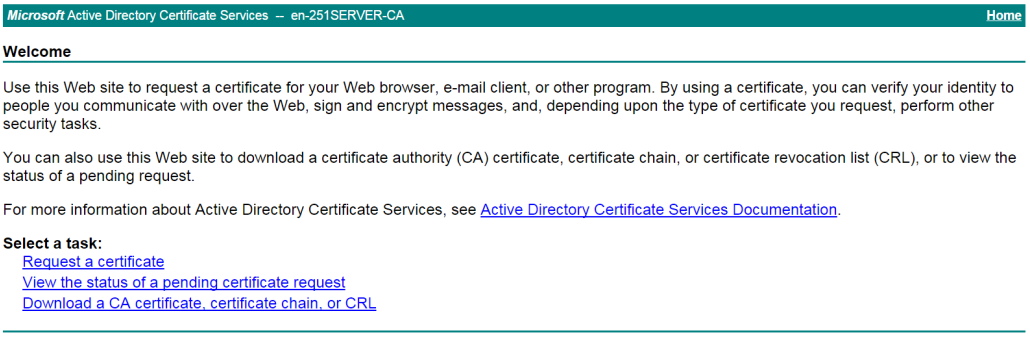
e. Click **Submit**.

3. Install the client certificate on the host:

a. After the certificate request is approved by the CA administrator, enter **http://192.168.100.247/certsrv** in the browser address bar.

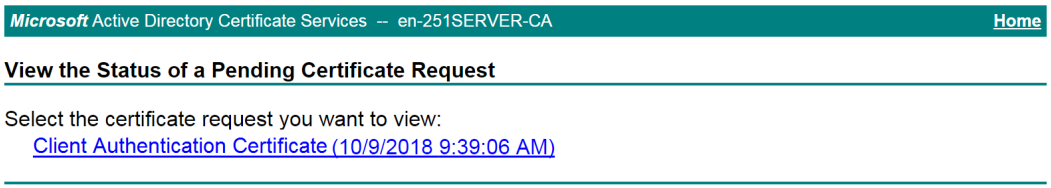
b. On the certificate service home page shown in Figure 29, click **View the status of a pending certificate request**.

Figure 29 Certificate service home page



The **View the Status of a Pending Certificate Request** page opens, as shown in Figure 30.

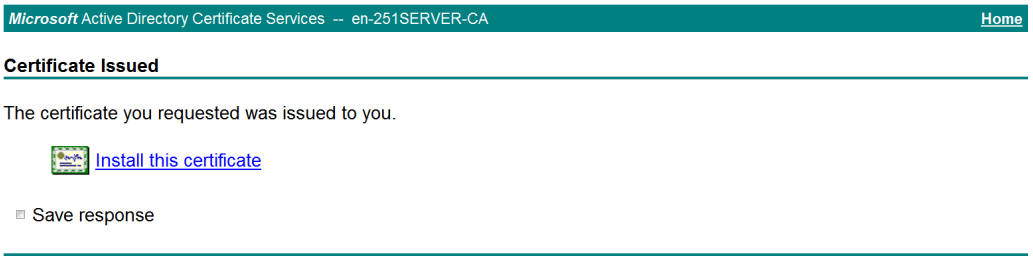
Figure 30 View the Status of a Pending Certificate Request page



c. Click the client certificate whose status you want to view.

d. On the **Certificate Issued** page shown in Figure 31, click **Install this certificate** to install the client certificate.

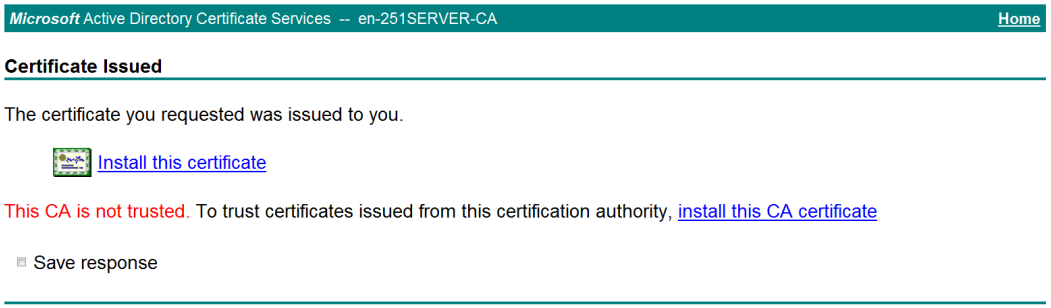
Figure 31 Installing the client certificate



If the host does not have a CA certificate, the page shown in Figure 32 opens. You must install the CA certificate first.

e. Click **install this CA certificate** to install the CA certificate. Then, click **Install this certificate** to install the client certificate.

Figure 32 Installing the CA certificate and then the client certificate



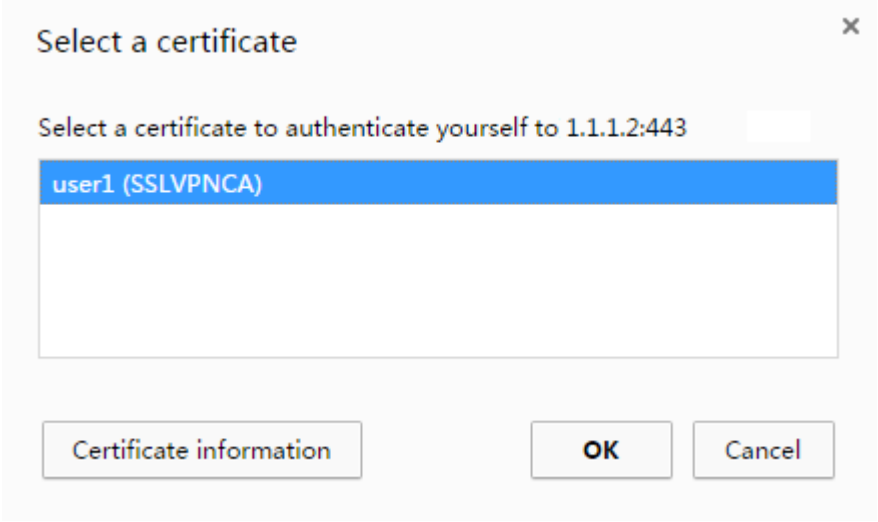
After the client certificate is installed, the **Certificate Installed** page shown in Figure 33 opens.

Figure 33 Certificate Installed page

Verifying the configuration

1. In the browser address bar of the host, enter **https://1.1.1.2** and press **Enter**.
2. On the **Select a certificate** page, select the client certificate for authentication, as shown in Figure 34.

Figure 34 Select a certificate page

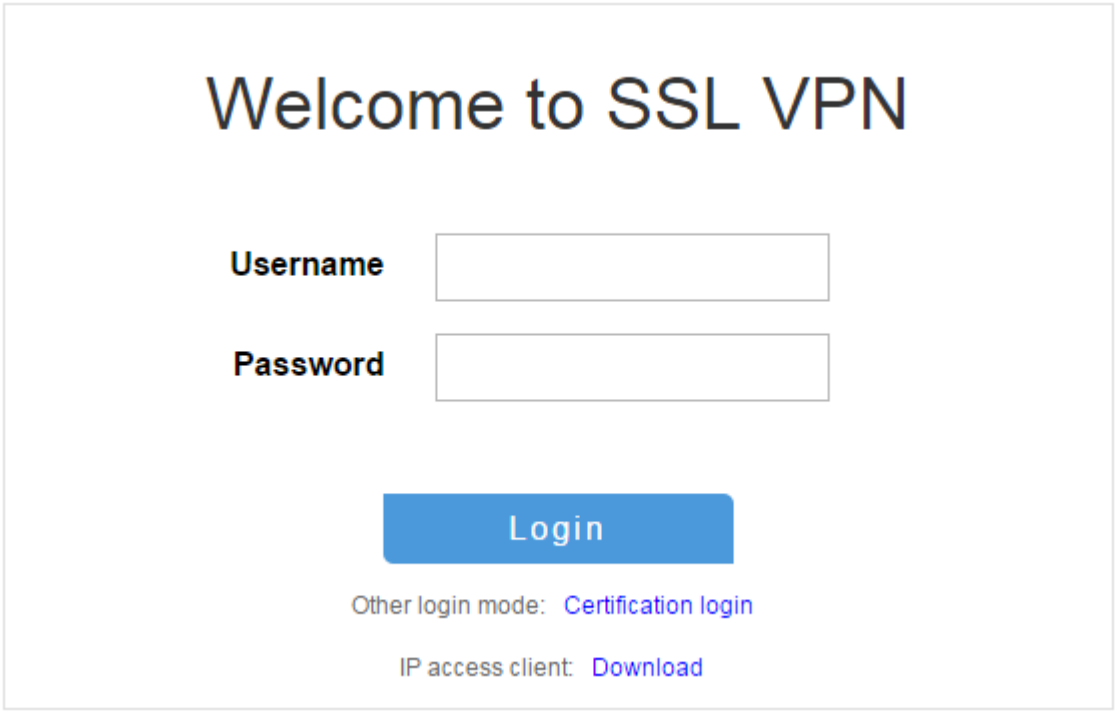


3. Click **OK**.
4. On the **Domain List** page shown in Figure 35, click **domainweb**.

Figure 35 Domain List page

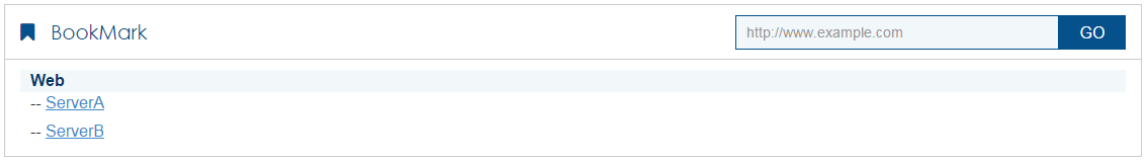
5. On the SSL VPN login page shown in Figure 36, enter username **user1** and password and **123456**, and then click **Login**

Figure 36 SSL VPN login page



The SSL VPN home page opens, displaying the Web resources the user can access in the **BookMark** area, as shown in Figure 37.

Figure 37 Accessible Web resources



6. Click **ServerA** to access Web resources on Server A.

Figure 38 Accessing Server A

7. Click **ServerB** to access Web resources on Server B.

Figure 39 Accessing Server B

Example: Configuring Web access with a self-signed server certificate

Network configuration

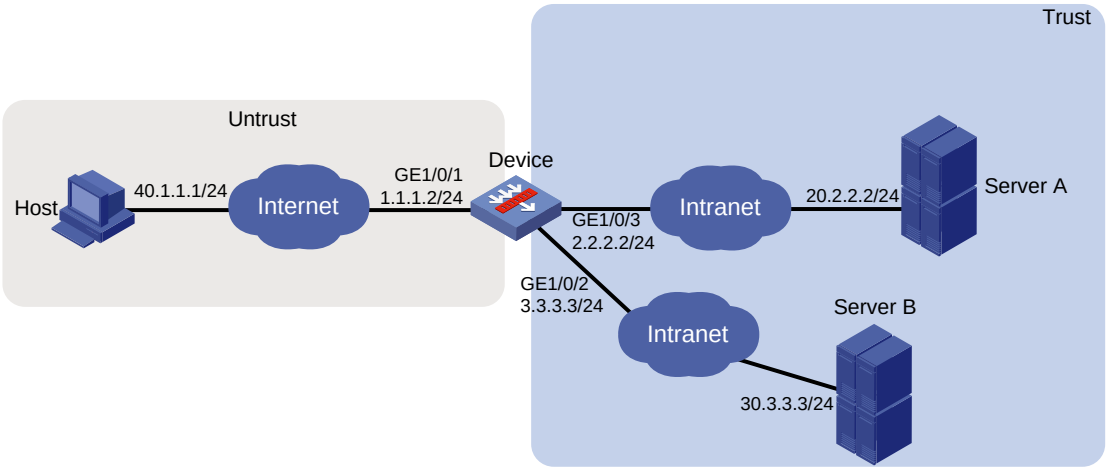
As shown in Figure 40, the device acts as the SSL VPN gateway that connects the public network and the private network. Users need to access resources on internal Web servers Server A and Server B. Both servers use HTTP over port 80.

Configure the SSL VPN Web access service on the device to allow users to access Server A and Server B in Web access mode.

Configure the device to perform local authentication and authorization for Web access users.

The device uses a self-signed SSL server certificate.

Figure 40 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.1.2/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 3.3.3.3/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 2.2.2.2/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

This example configures static routes.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static IPv4 route to reach 20.2.2.2:

a. Enter destination IP address **20.2.2.2**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 30.3.3.3:

a. Enter destination IP address **30.3.3.3**.

b. Enter mask length **24**.

c. Enter next hop address **3.3.3.4**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configure a static IPv4 route to reach 40.1.1.1:

a. Enter destination IP address **40.1.1.1**.

b. Enter mask length **24**.

c. Enter next hop address **1.1.1.3**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Create security policies:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**, and then click **Create a policy**.

In the dialog box that opens, configure a security policy named **untrust-local** to permit the specified traffic from the **Untrust** to **Local** security zones:

- Enter policy name **untrust-local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 address **40.1.1.1**.
- Select destination IPv4 address **1.1.1.2**.
- Use the default settings for other parameters.

Click **OK**.

Create security policy **local-trust** to permit the specified traffic from the **Local** to **Trust** security zones:

- Enter policy name **local-trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 addresses **2.2.2.2** and **3.3.3.3**.
- Select destination IPv4 addresses **20.2.2.2**, and **30.3.3.3**.
- Use the default settings for other parameters.

Click **OK**.

4. Configure the SSL VPN gateway:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **SSL VPN** > **SSL VPN Gateways**.

   # Click **Create**.

   # Create an SSL VPN gateway as shown in Figure 41, and then click **OK**.

Figure 41 Creating an SSL VPN gateway

5. Configure an SSL VPN context:

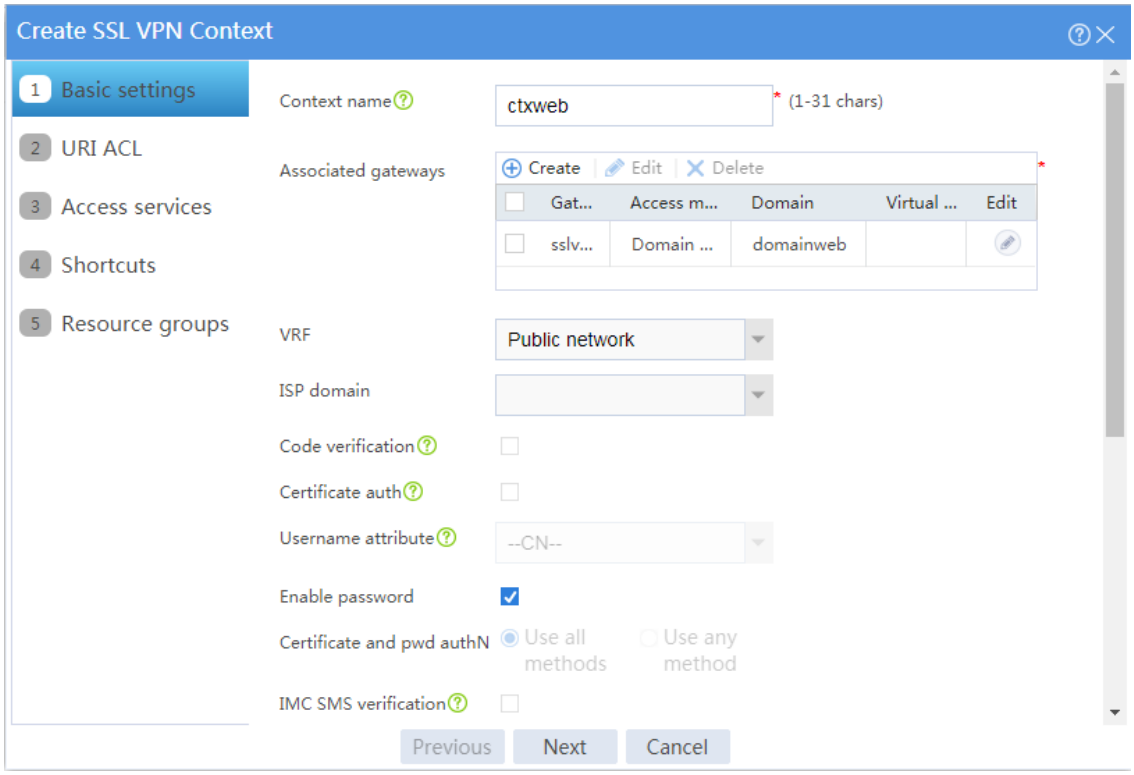
   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **SSL VPN** > **SSL VPN Contexts**.

   # Click **Create**.

   # Configure the basic settings for the SSL VPN context as shown in Figure 42, and then click **Next**.

Figure 42 Configuring basic settings for an SSL VPN context



On the **URI ACL** page, click **Next**.

On the **Access services** page, select **Web access** and click **Next**.

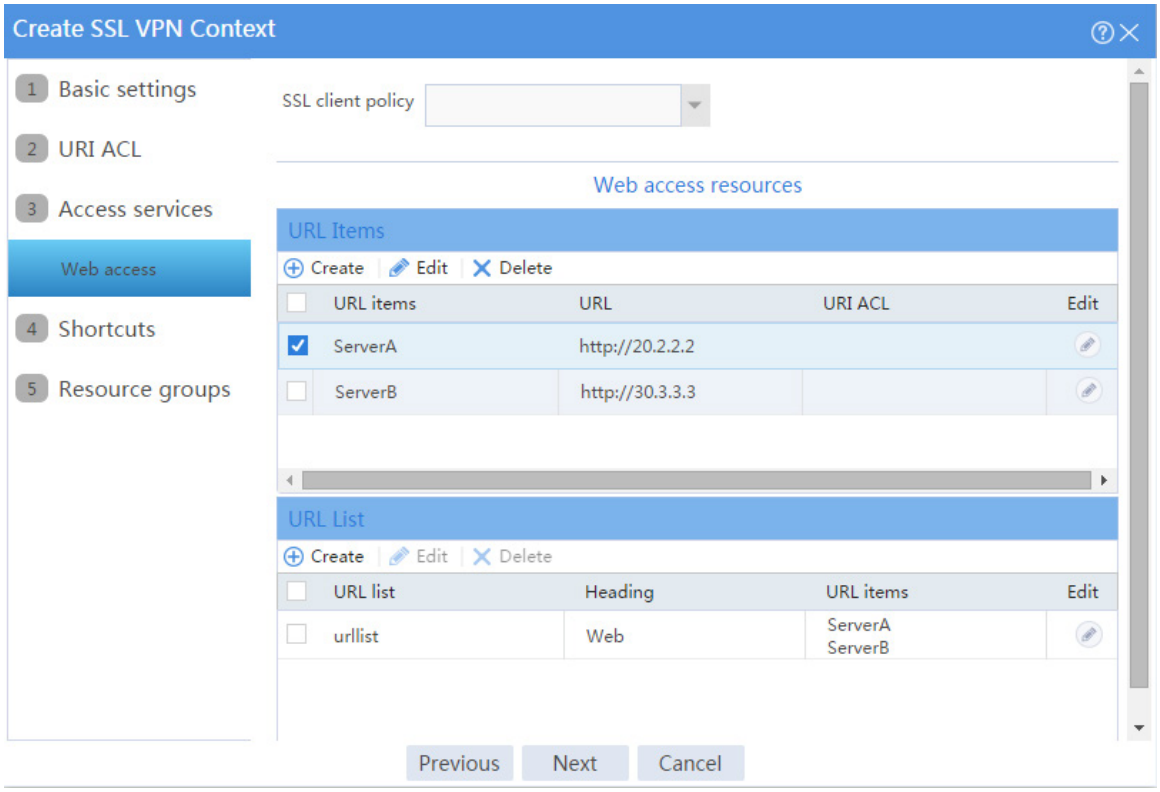
On the **Web access** page, configure the Web access service as follows:

a. Configure two URL items pointing to Server A and Server B, respectively.

b. Add the two URL items to URL list **urllist**.

c. Click **Next**.

Figure 43 Configuring Web access service

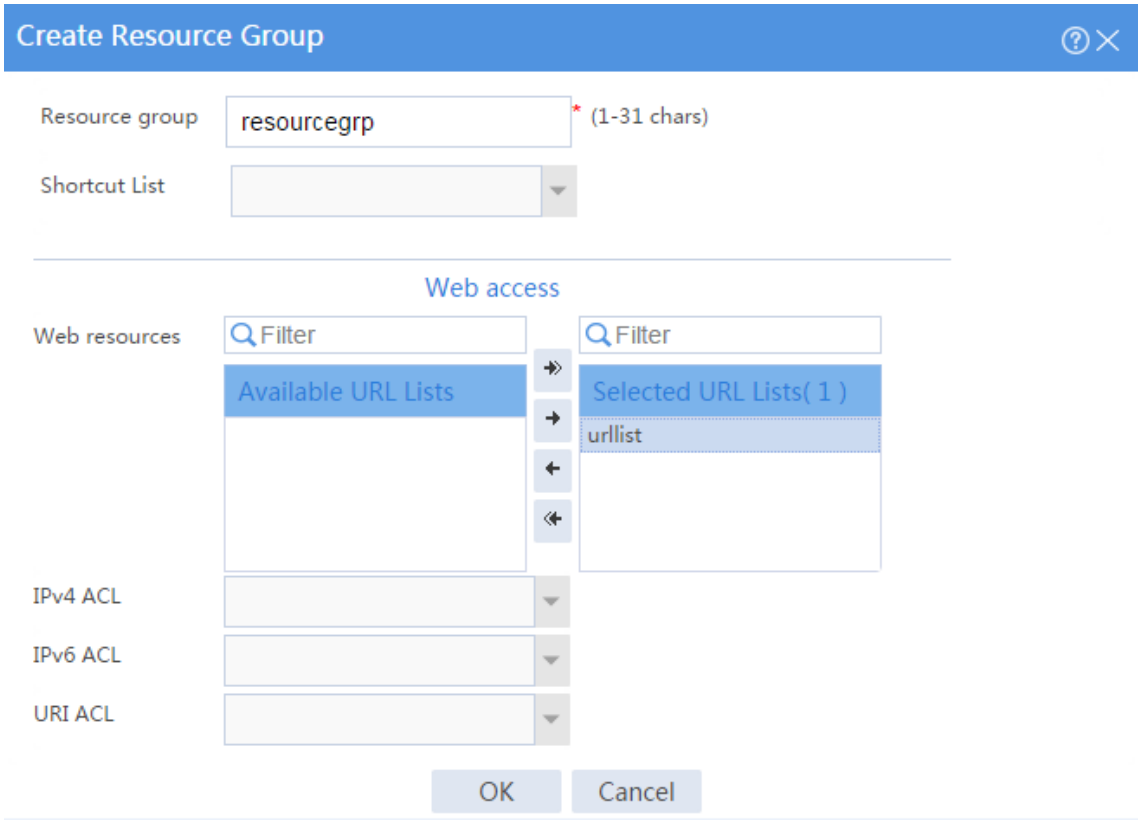


Click **Next** on the **Shortcuts** page.

On the **Resource groups** page, click **Create**.

Create a resource group named **resourcegrp** and select URL list **urllist** as the accessible Web resources, as shown in Figure 44.

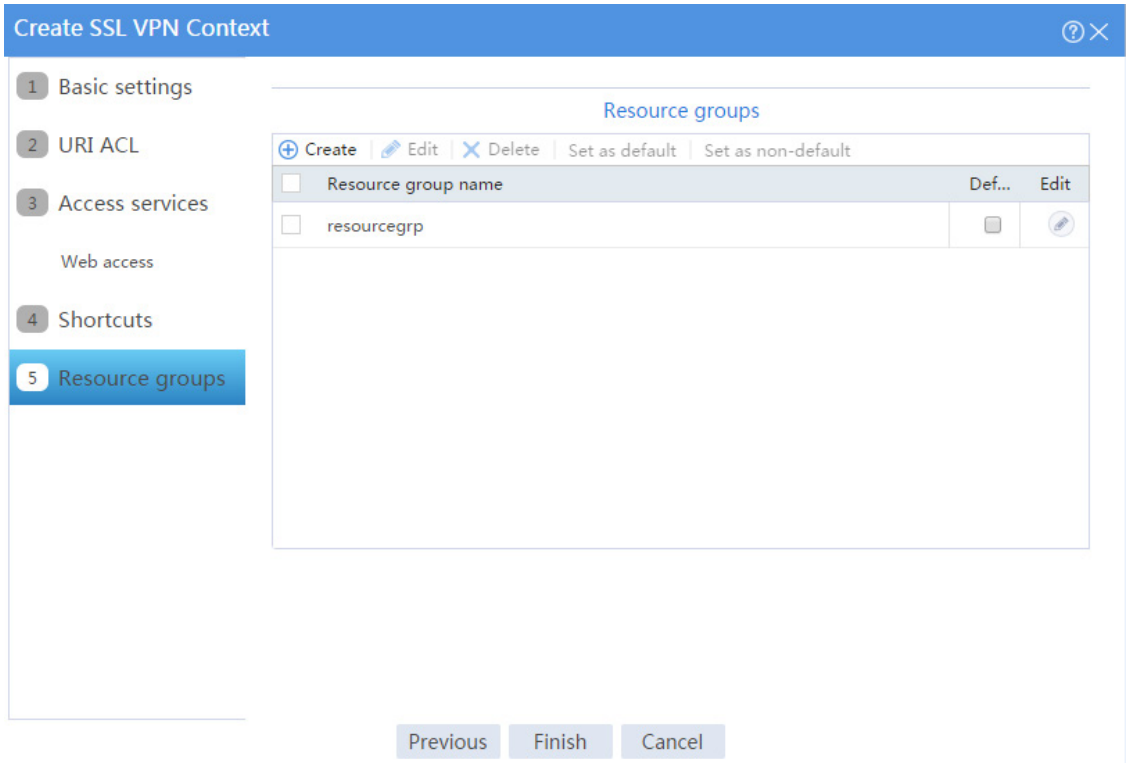
Figure 44 Creating an SSL VPN resource group



Click **OK**.

The newly created resource group is displayed on the **Resource groups** page, as shown in Figure 45.

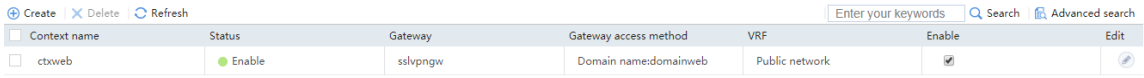
Figure 45 Resource groups configuration page



Click **Finish**.

Select the **Enable** check box to enable the SSL VPN context, as shown in Figure 46.

Figure 46 Enabling the SSL VPN context



6. Create an SSL VPN user:

On the top navigation bar, click **Objects**.

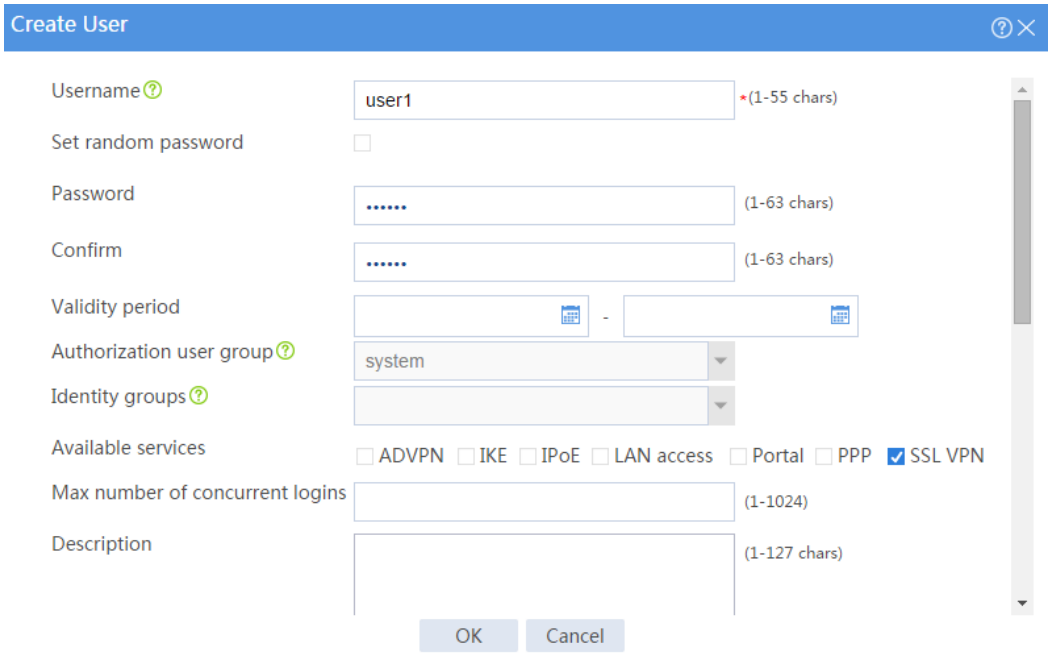
From the navigation pane, select **User** > **User Management** > **Local Users**.

Click **Create**.

Create an SSL VPN user:

a. Set the username to **user1** and password to **123456**, and select **SSL VPN** as the available service, as shown in Figure 47.

Figure 47 Creating an SSL VPN user



b. In the **Authorization Attributes** area, authorize the user to use SSL VPN resource group **resourcegrp**, as shown in Figure 48.

Figure 48 Setting the authorization attributes for the SSL VPN user

c. Click **OK**.

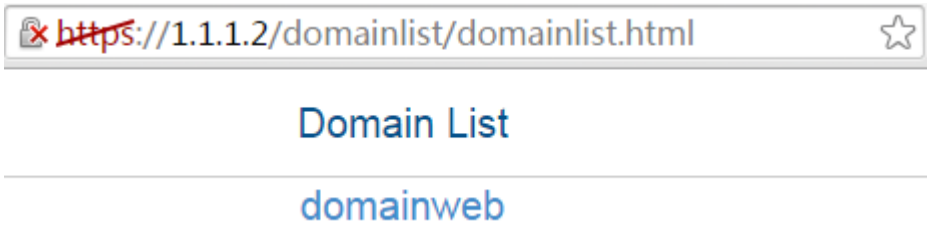
Configuring the host

Configure the IP address and gateway address settings for the host and make sure it can reach the SSL VPN gateway.

Verifying the configuration

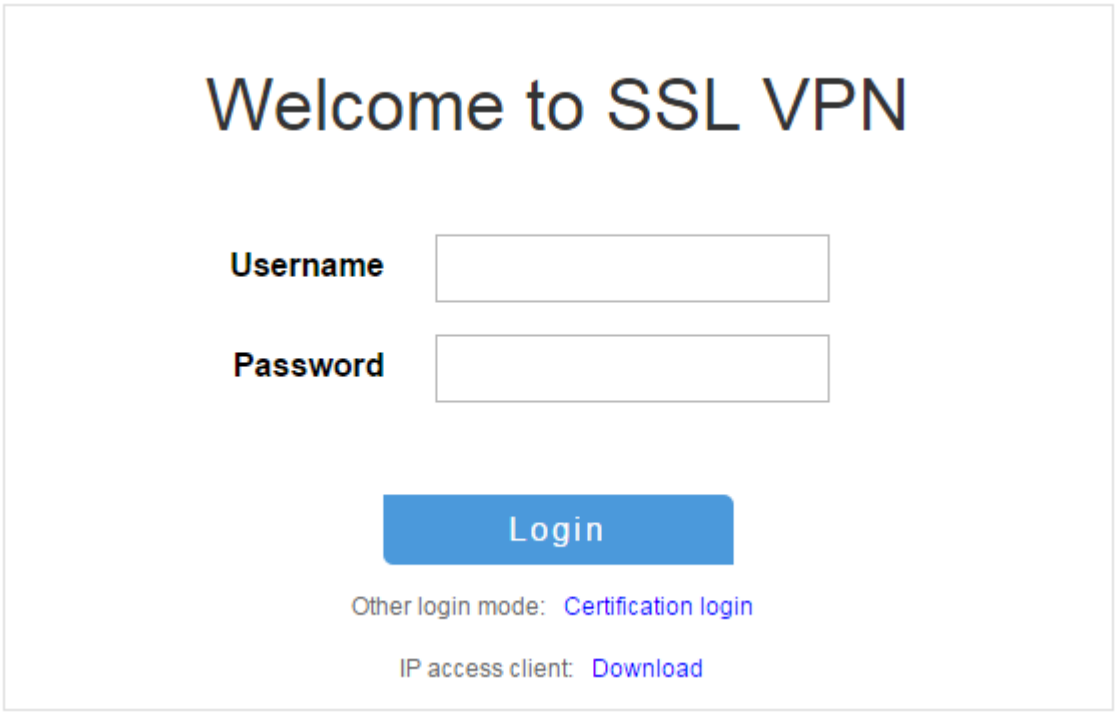
1. In the browser address bar of the host, enter **https://1.1.1.2** and press **Enter** to open the domain list page.

Figure 49 Domain list page



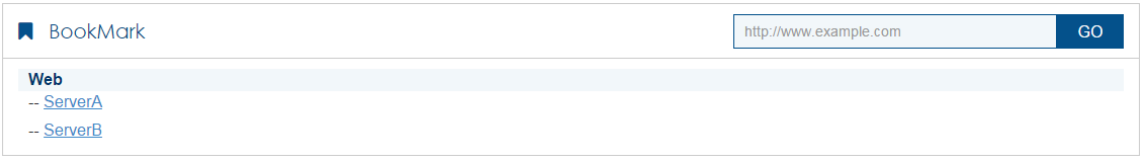
2. Select **domainweb** to access the login page.
3. On the login page, enter username **user1** and password **123456**, and then click **Login**.

Figure 50 Login page



The SSL VPN home page opens, displaying the Web resources the user can access in the **BookMark** area.

Figure 51 Accessible Web resources



4. Click **ServerA** to access Web resources on Server A.

Figure 52 Accessing Server A

5. Click **ServerB** to access Web resources on Server B.

Figure 53 Accessing Server B

L2TP configuration examples

Contents

Introduction

The following information provides L2TP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of L2TP.

Example: Configuring L2TP

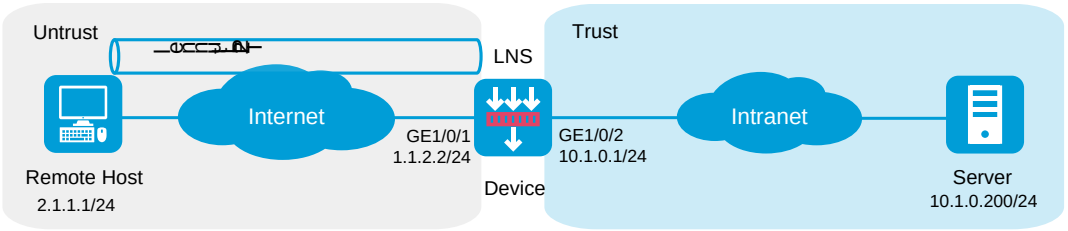
Network configuration

As shown in Figure 1, a PPP user directly establishes an L2TP tunnel to an LNS, and accesses the HQ of the company through the L2TP tunnel.

Configure the network to meet the following requirements:

- An enterprise branch can access the intranet resources of the company through an L2TP VPN.
- Traveling employees can access the intranet to work remotely through an L2TP VPN.

Figure 1 Network diagram



Software version used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1. In the dialog box that opens, configure the interface:

   - Select the **Untrust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 1.1.2.2/24.
   - Use the default settings for other parameters.

   # Click **OK**.

   # Click the **Edit** icon for GE 1/0/2. In the dialog box that opens, configure the interface:

   - Select the **Trust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.0.1/24.
   - Use the default settings for other parameters.

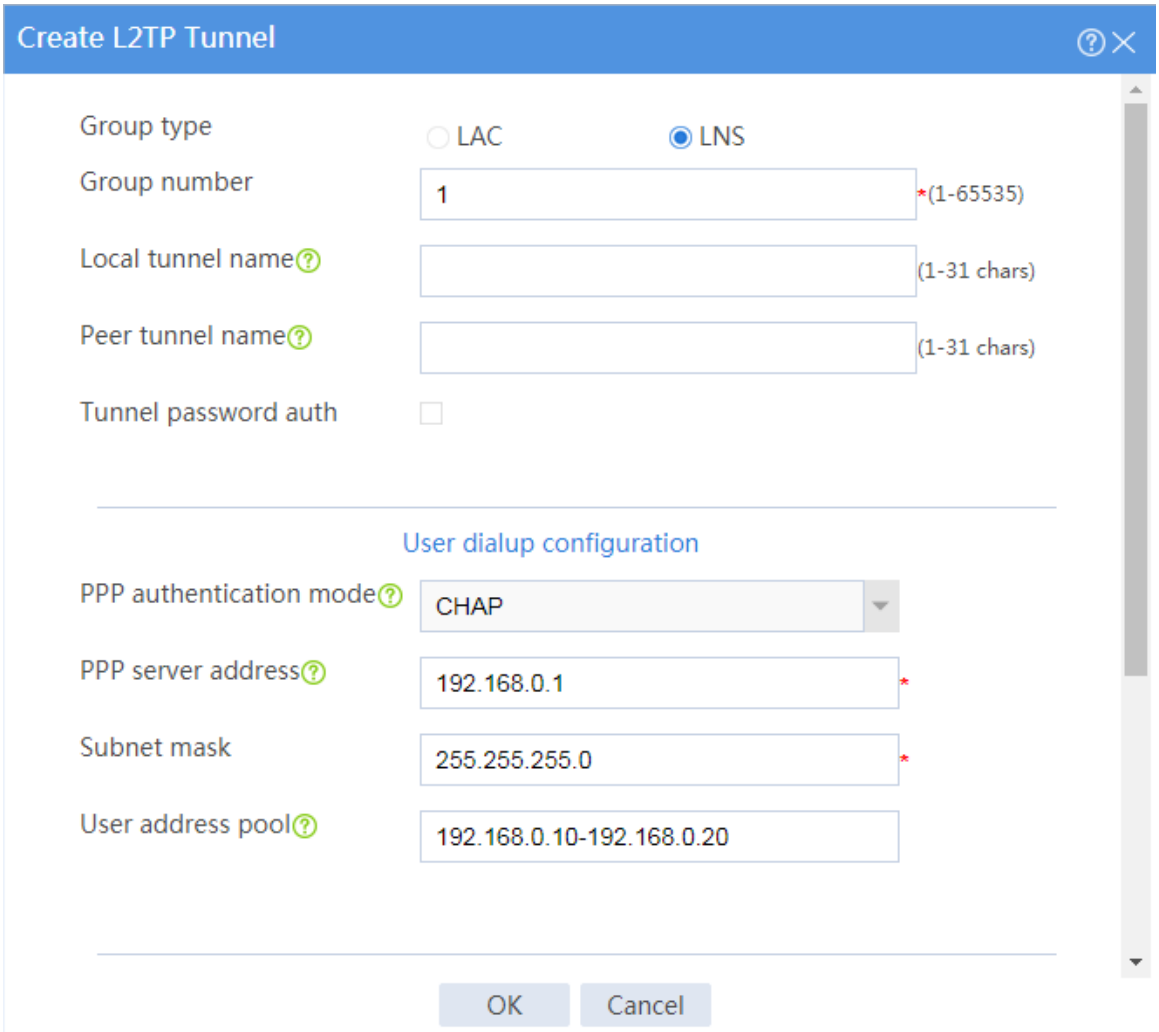
   # Click **OK**.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **VPN** > **L2TP**.

   # Click **Create**. In the dialog box that opens, configure parameters as shown in the following figure:

Figure 2 Configuring L2TP



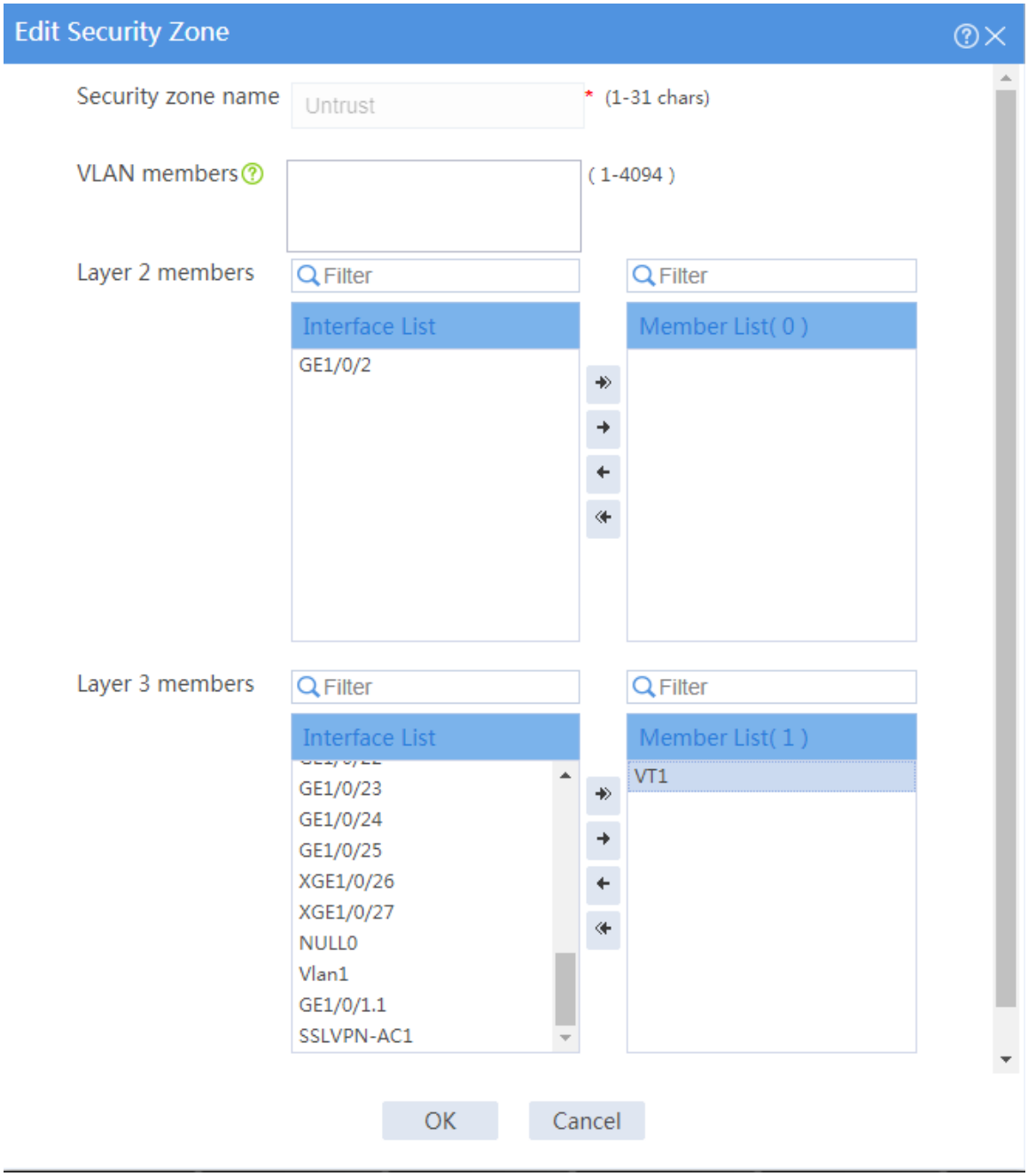
On the top navigation bar, click **Network**.

From the navigation pane, select **Security Zones**.

Click the **Edit** icon for security zone **Untrust** to enter the page for editing the security zone.

On this page, configure parameters as shown in the following figure:

Figure 3 Editing a security zone



2. Configure routing.

This section takes static routing as an example. If you need dynamic routing in your network, configure the corresponding dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv4 static route as follows:

- Enter destination address 2.1.1.1.
- Enter mask length 24.
- Enter next hop address 1.1.2.3.
- Use the default settings for other parameters.

Click **OK**.

3. Configure security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**. Click **Create**.

In the dialog box that opens, create a security policy and configure it as follows:

- Enter security policy name **untrust-local**.
- Select source security zone **Untrust**.
- Select destination security zone **Local**.
- Set the type to **IPv4**.
- Set the action to **Permit**.
- Select service **l2tp**.
- Use the default settings for other parameters.

Repeat the steps above to create a new security policy with the fowling parameter settings:

- Enter security policy name **untrust-trust**.
- Select source security zone **Untrust**.
- Select destination security zone **Trust**.

- Set the type to **IPv4**.
- Set the action to **Permit**.
- Enter source IPv4 addresses 192.168.0.10-192.168.0.20.
- Enter destination IPv4 address 10.1.0.200.
- Use the default settings for other parameters.

Click **OK**.

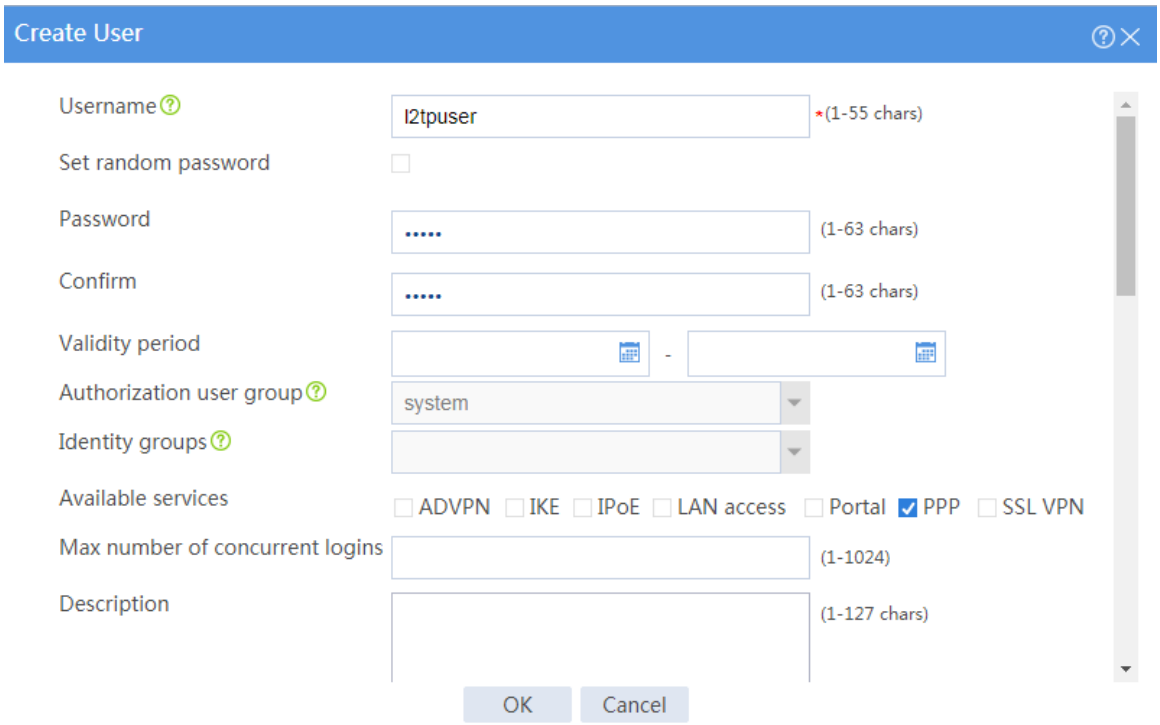
4. Create an L2TP user.

On the top navigation bar, click **Objects**.

From the navigation pane, select **User** > **User Management** > **Local Users**.

Click **Create**. Create an L2TP user. Set the username to **l2tpuser**, set the password to **hello**, and select service type **PPP**, as shown in the following figure:

Figure 4 Creating an L2TP user



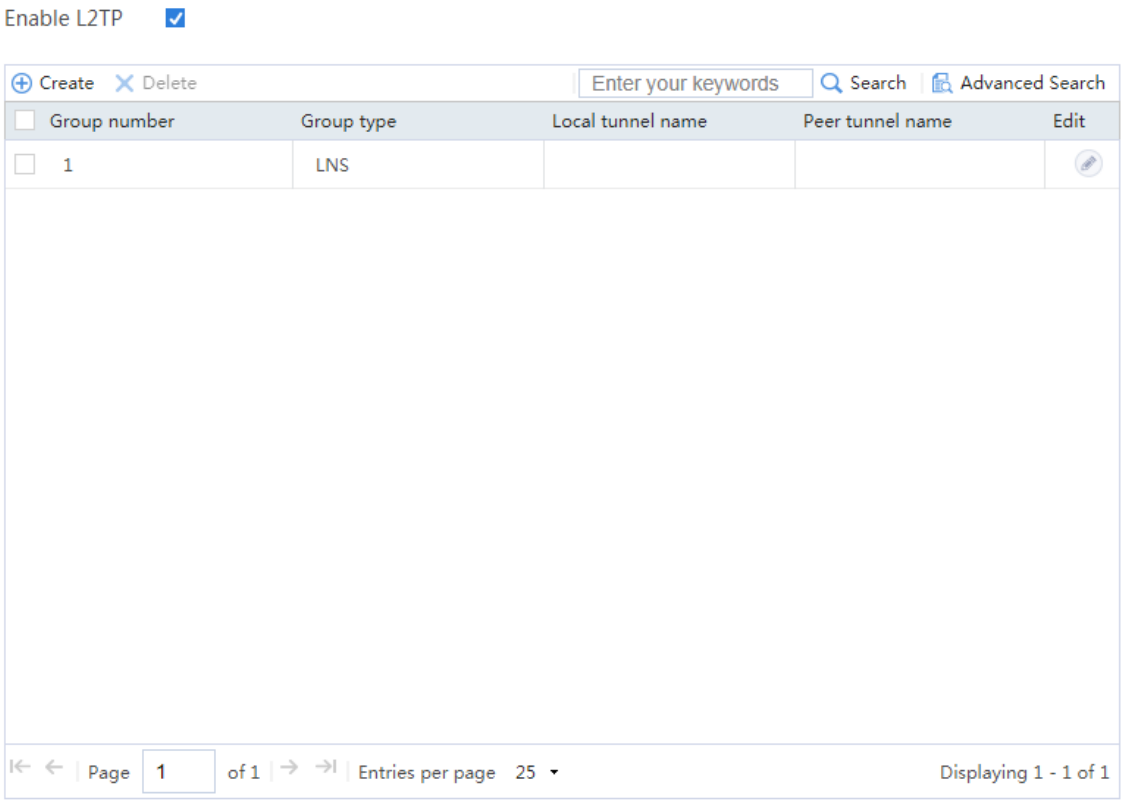
5. Enable L2TP.

On the top navigation bar, click **Network**.

From the navigation pane, select **VPN** > **L2TP**.

Click the **L2TP** tab. On this tab, enable L2TP.

Figure 5 Enabling L2TP



Configuring a VPN client

Click the **Network** icon in the lower right corner of your PC, and click **Open Network and Sharing Center** page.

Access the **Change your networking settings** area.

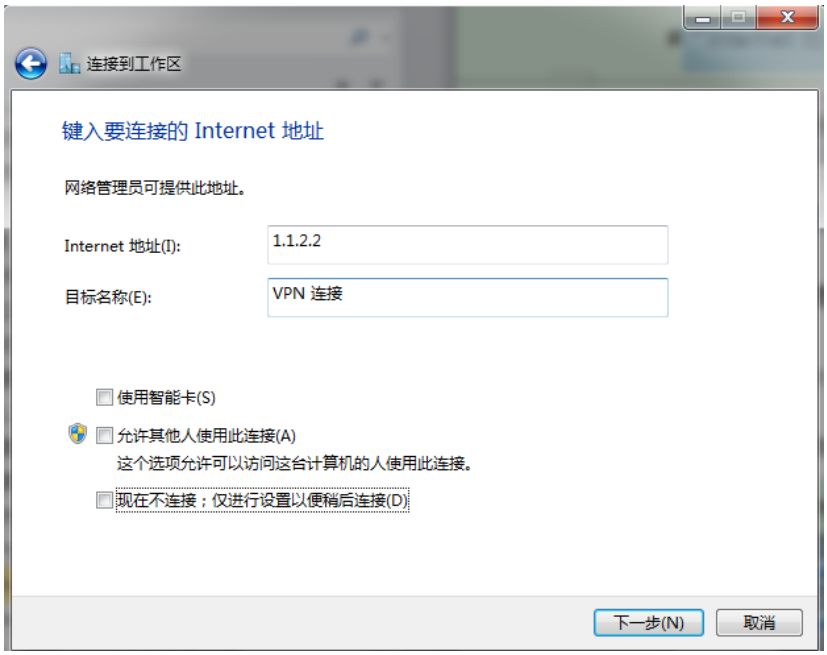
Figure 6 Changing your networking settings

Click **Connect to a workplace**, and select **Use my Internet connection (VPN)**, as shown in the following figures.

Figure 7 Setting VPN

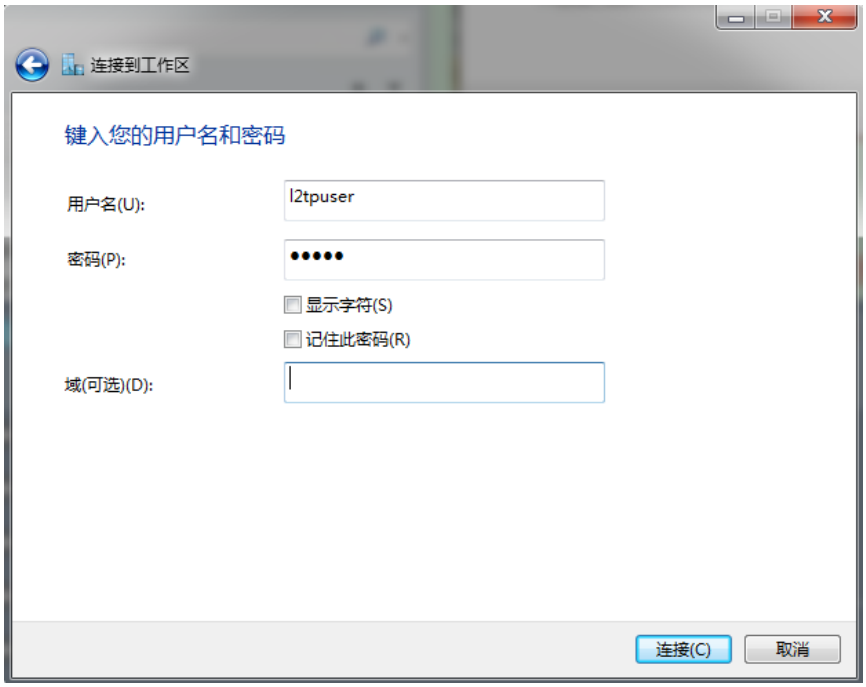
Click **Don’t connect now; just set it up so I can connect later**. In the **Internet address** field, enter the IP address of the interface connecting the device to the Internet.

Figure 8 Setting the IP address



Set the username and password for VPN dialup, as shown in the following figure:

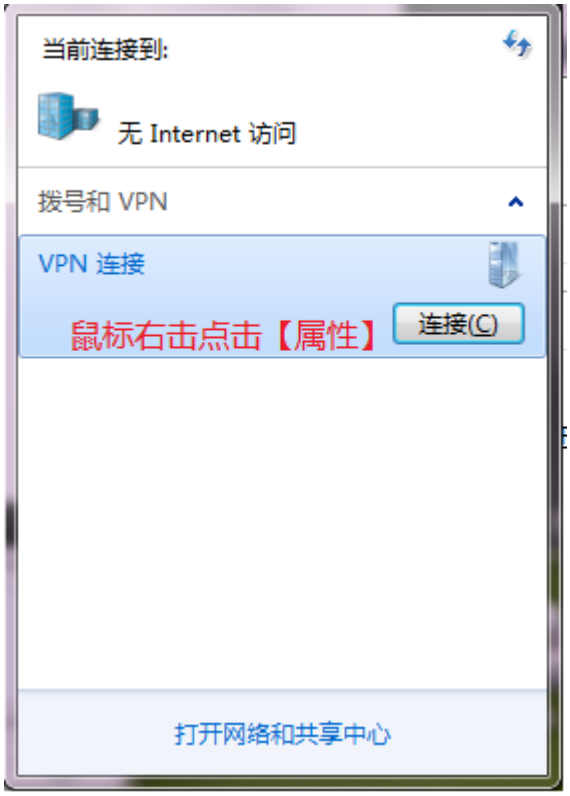
Figure 9 Setting the username and password



Set the **Network** icon in the lower right corner of your PC.

Right-click the new VPN connection, and select **Properties** from the shortcut menu.

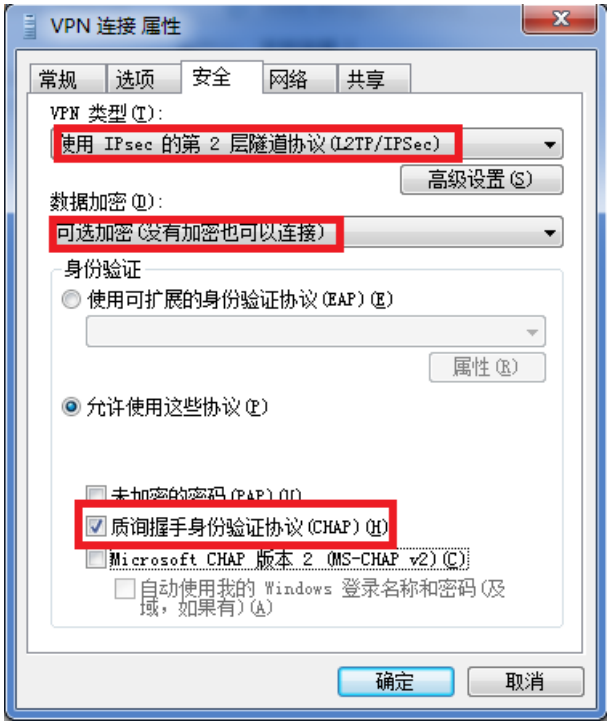
Figure 10 Setting a VPN connection



On the **Security** tab, configure the VPN connection as follows:

- Select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** from the **Type of VPN** list.
- Select **Optional encryption (connect even if no encryption)** from the **Data encryption** list.
- Select **Challenge Handshake Authentication Protocol (CHAP)** in the **Allow these protocols** area.

Figure 11 Setting the VPN properties



Verifying the configuration

After a user successfully dials up, you can see the L2TP tunnel information, as shown in the following figure:

Figure 12 L2TP tunnel information

NAT configuration examples

Contents

Introduction

The following information describes NAT configuration examples.

The following NAT translation methods are supported:

Static NAT

Static NAT creates a fixed mapping between a private address and a public address. It supports connections initiated from internal users to external network and from external users to the internal network. Static NAT applies to regular communications.

Dynamic NAT

Dynamic NAT uses an address pool to translate addresses. It applies to the scenario where a large number of internal users access the external network.

NAT Server

The NAT Server feature maps a public address and port number to the private IP address and port number of an internal server. This feature allows servers in the private network to provide services for external users.

NAT444 port block

NAT444 provides carrier-grade NAT by unifying the NAT444 gateway, AAA server, and log server. NAT444 introduces a second layer of NAT on the carrier side, with few changes on the customer side and the application server side. With port block assignment, NAT444 supports user tracking. It has become a preferred solution for carriers in transition to IPv6.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of NAT.

Restrictions and guidelines

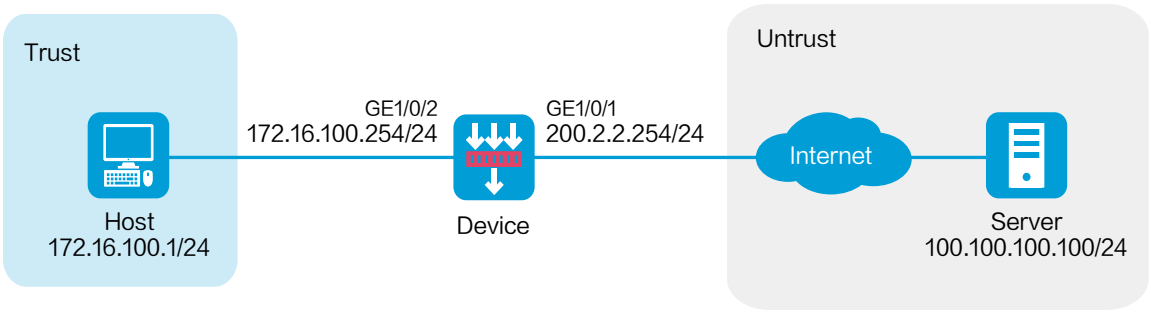
Do not configure both the NAT translation methods and a global NAT policy.

Example: Configuring static NAT

Network configuration

As shown in Figure 1, configure static NAT to allow the host at 172.16.100.1/24 to access the server at 100.100.100.100/24 on the Internet by using public IP address 200.2.2.254/24.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 200.2.2.254/24.

c. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 172.16.100.254/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing.

This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static route to permit packets from the device to the server:

a. Specify the IP address of the server as the destination IP. In this example, the address is 100.100.100.100.

b. Enter the mask length. In this example, enter 24.

c. Specify the next-hop address as 200.2.2.253.

d. Click **OK**.

3. Configure a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Trust.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP address of the host as the source IPv4 address. In this example, the address is 172.16.100.1.

g. Specify the IP address of the server as the destination IPv4 address. In this example, the address is 100.100.100.100.

h. Click **OK**.

4. Create a static NAT mapping.

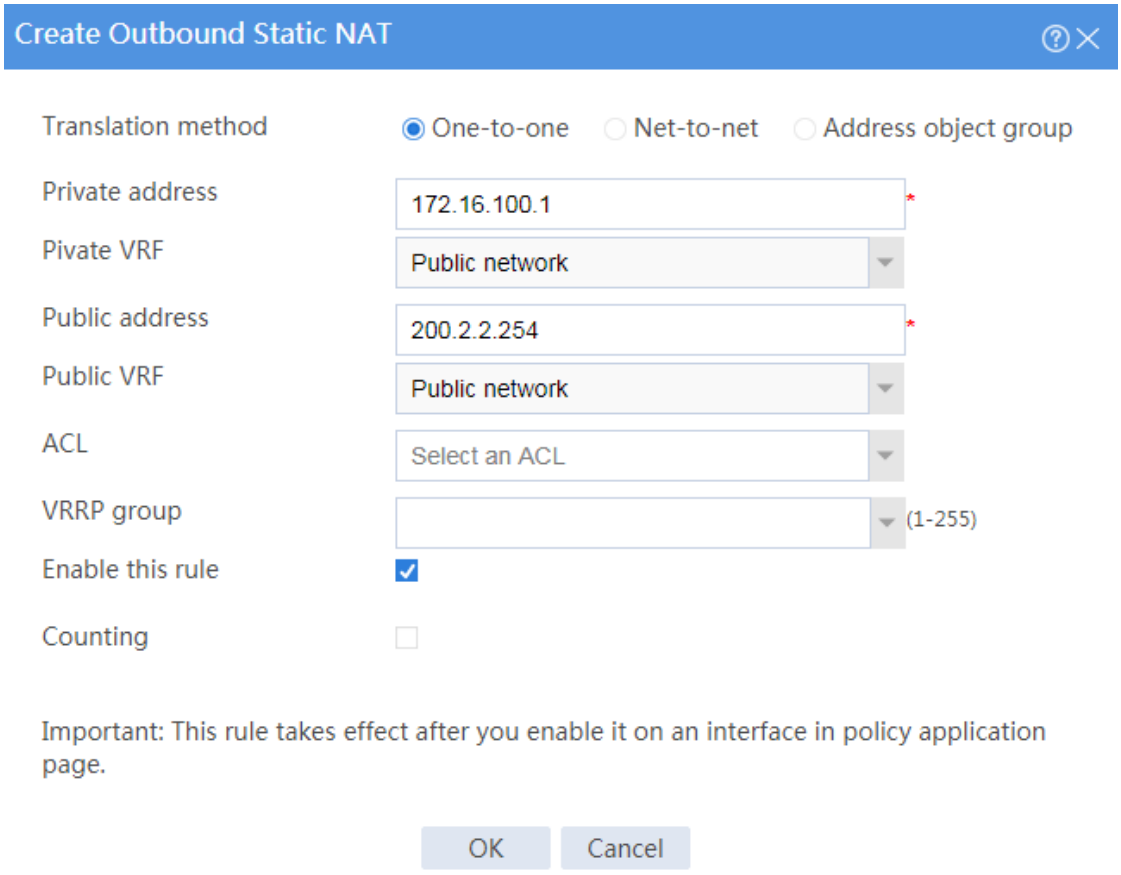
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **Static NAT** > **Policy Configuration**.

Click **Create**.

Create a static NAT mapping, as shown in Figure 2.

Figure 2 Creating a static NAT mapping



Click **OK**.

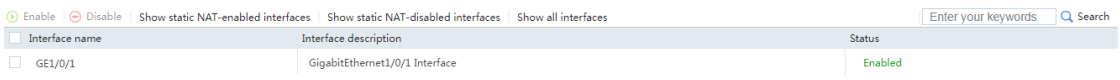
5. Apply the static NAT mapping.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **Static NAT** > **Apply Policy**.

Select GE 1/0/1 and click **Enable**. The mapping has been applied to the interface, as shown in Figure 3.

Figure 3 Applying the static NAT mapping



Verifying the configuration

1. Verify that the host can successfully ping the server on the external network.

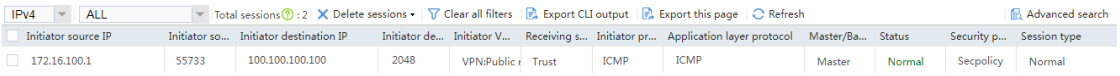
```
C:\Users\abc>ping 100.100.100.100

Pinging host.com [100.100.100.100] with 32 bytes of data:
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253

Ping statistics for 100.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a NAT session is generated when the host accesses the server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 4 Session list

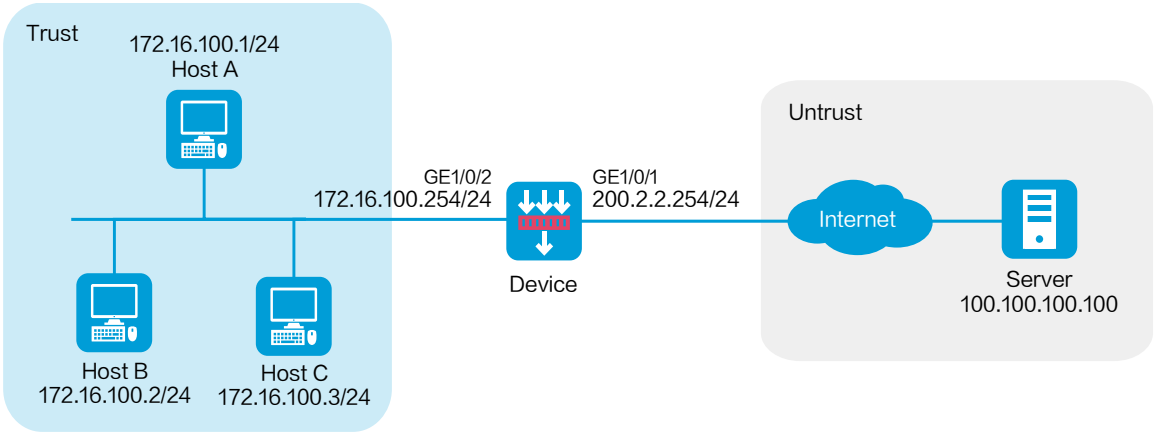


Example: Configuring NO-PAT for dynamic NAT

Network configuration

As shown in Figure 5, the company has public addresses 200.2.2.1/24 to 200.2.2.3/24. Configure NO-PAT translation to enable hosts in the internal network to access the server on the Internet.

Figure 5 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 200.2.2.254/24.

c. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 172.16.100.254/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing.

This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static route to permit packets from the internal hosts to the external server:

a. Specify the IP address of the server as the destination IP. In this example, the address is 100.100.100.100.

b. Enter the mask length. In this example, enter 24.

c. Specify the next-hop address as 200.2.2.253.

d. Click **OK**.

3. Configure a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Trust.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP addresses of the hosts as the source IPv4 addresses. In this example, the addresses are 172.16.100.1, 172.16.100.2, 172.16.100.3.

g. Specify the IP address of the server as the destination IPv4. In this example, the address is 100.100.100.100.

h. Click **OK**.

4. Configure a NAT address group.

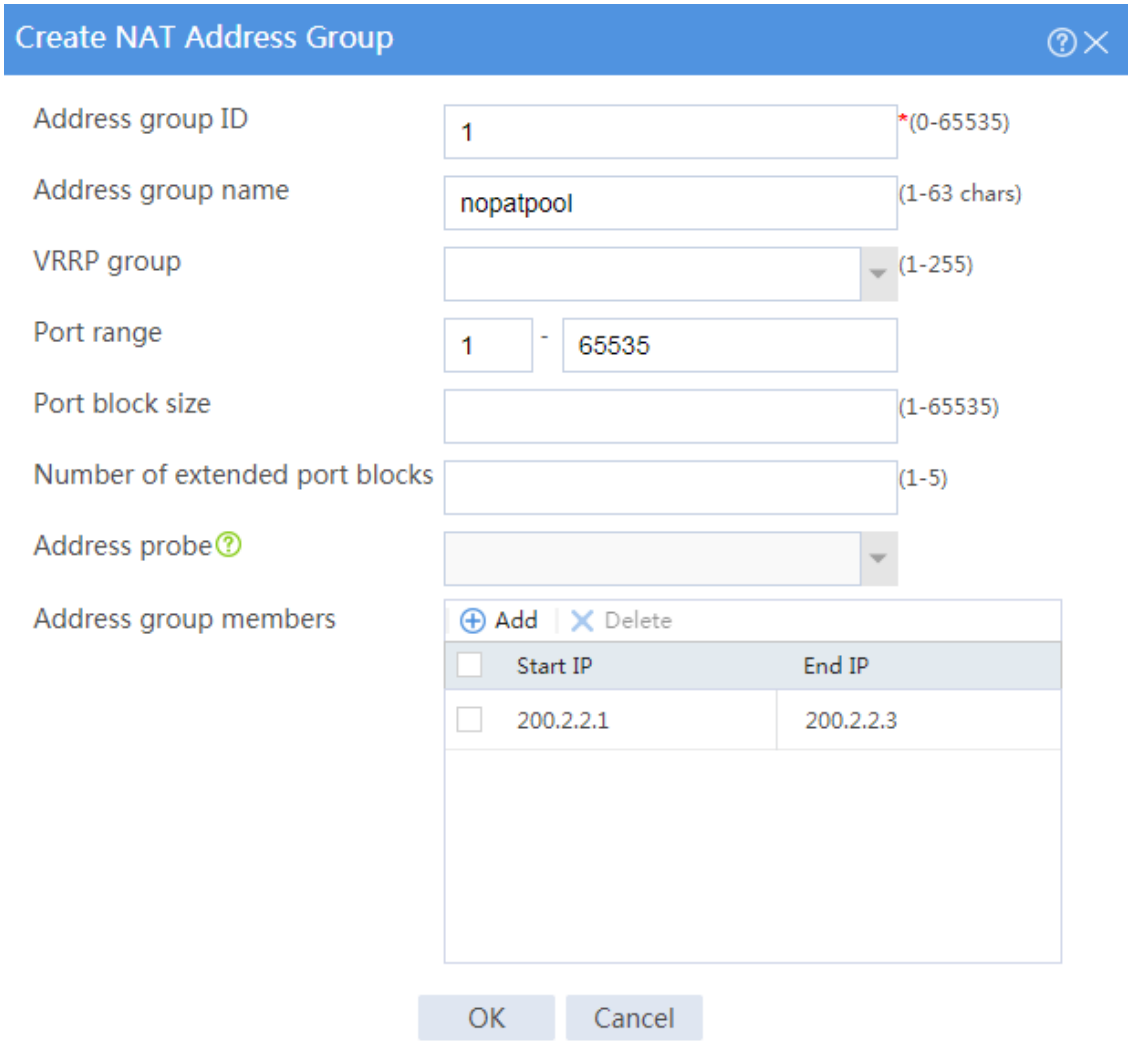
On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **NAT Address Groups**.

Click **Create**.

Create a NAT address group, as shown in Figure 6.

Figure 6 Creating a NAT address group



Click **OK**.

5. Configure an outbound dynamic NAT rule.

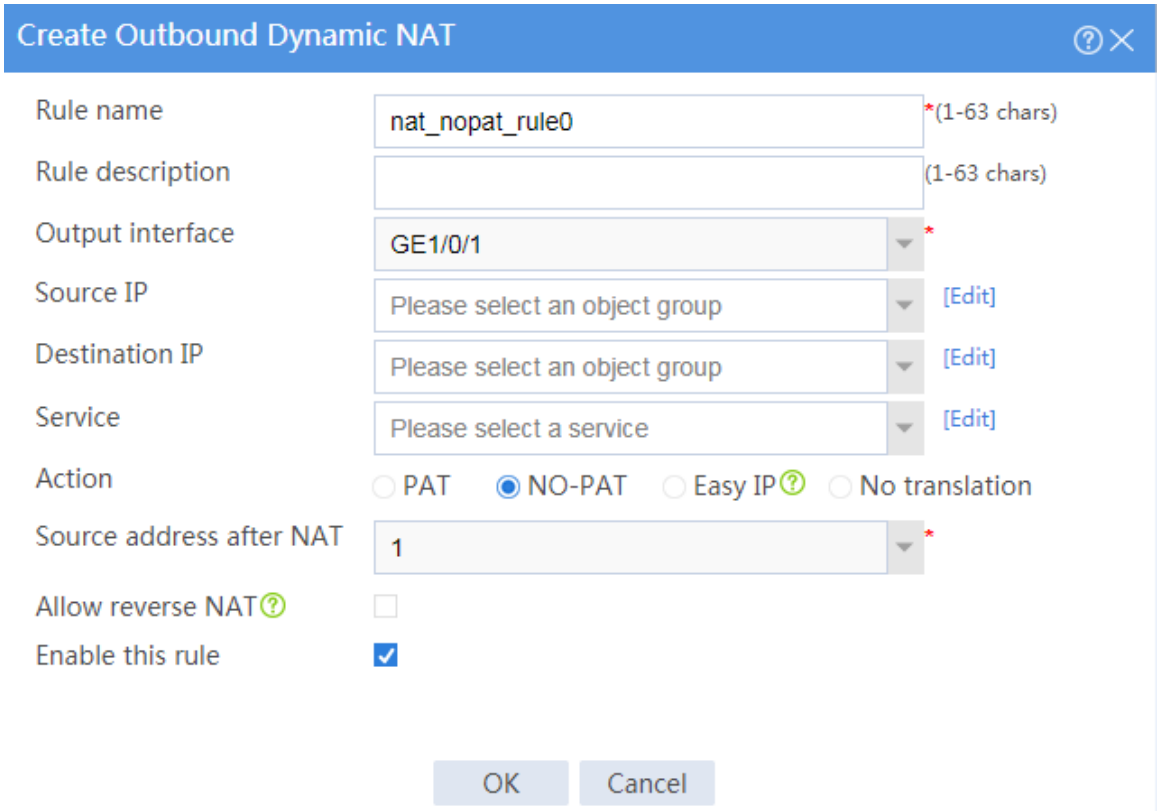
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **Dynamic NAT**.

On the **Outbound Dynamic NAT (Object Group-Based)** tab, click **Create**.

Create an outbound dynamic NAT rule, as shown in Figure 7.

Figure 7 Creating an outbound dynamic NAT rule



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the server on the external network.

```
C:\Users\abc>ping 100.100.100.100

Pinging host.com [100.100.100.100] with 32 bytes of data:
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
```

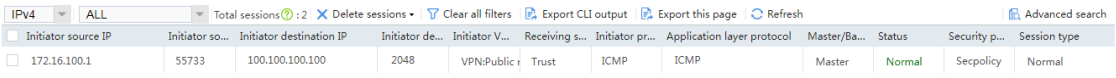
```
Ping statistics for 100.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a NAT session is generated when the host accesses the server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 8 Session list

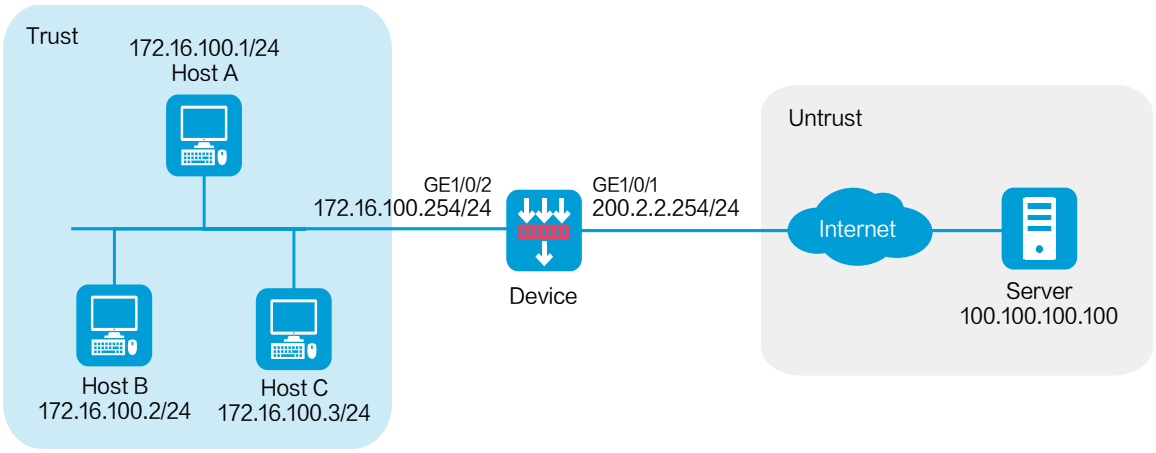


Example: Configuring PAT for dynamic NAT

Network configuration

As shown in Figure 9, a company has only one public IP addresses 200.2.2.1/24. Configure PAT for outbound dynamic NAT to allow only internal hosts to access the Internet by using this public IP address.

Figure 9 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 200.2.2.254/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and set its IP address to 172.16.100.254/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing.

   This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static route to permit packets from the hosts to the server:

   a. Specify the IP address of the server as the destination IP. In this example, the address is 100.100.100.100.

   b. Enter the mask length. In this example, enter 24.

   c. Specify the next-hop address as 200.2.2.253.

   d. Click **OK**.

3. Configure a security policy.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create** and click **Create a policy**.

   # In the dialog box that opens, configure policy parameters as follows:

   a. Enter a policy name. In this example, the name is **Secpolicy**.

   b. Select the source zone. In this example, the source zone is Trust.

   c. Select the destination zone. In this example, the destination zone is Untrust.

   d. Select **IPv4** as the type.

   e. Select **Permit** as the action.

   f. Specify the IP addresses of the hosts as the source IPv4 addresses. In this example, the addresses are 172.16.100.1, 172.16.100.2, and 172.16.100.3.

   g. Specify the IP address of the server as the destination IPv4 address. In this example, the address is 100.100.100.100.

   h. Click **OK**.

4. Configure a NAT address group.

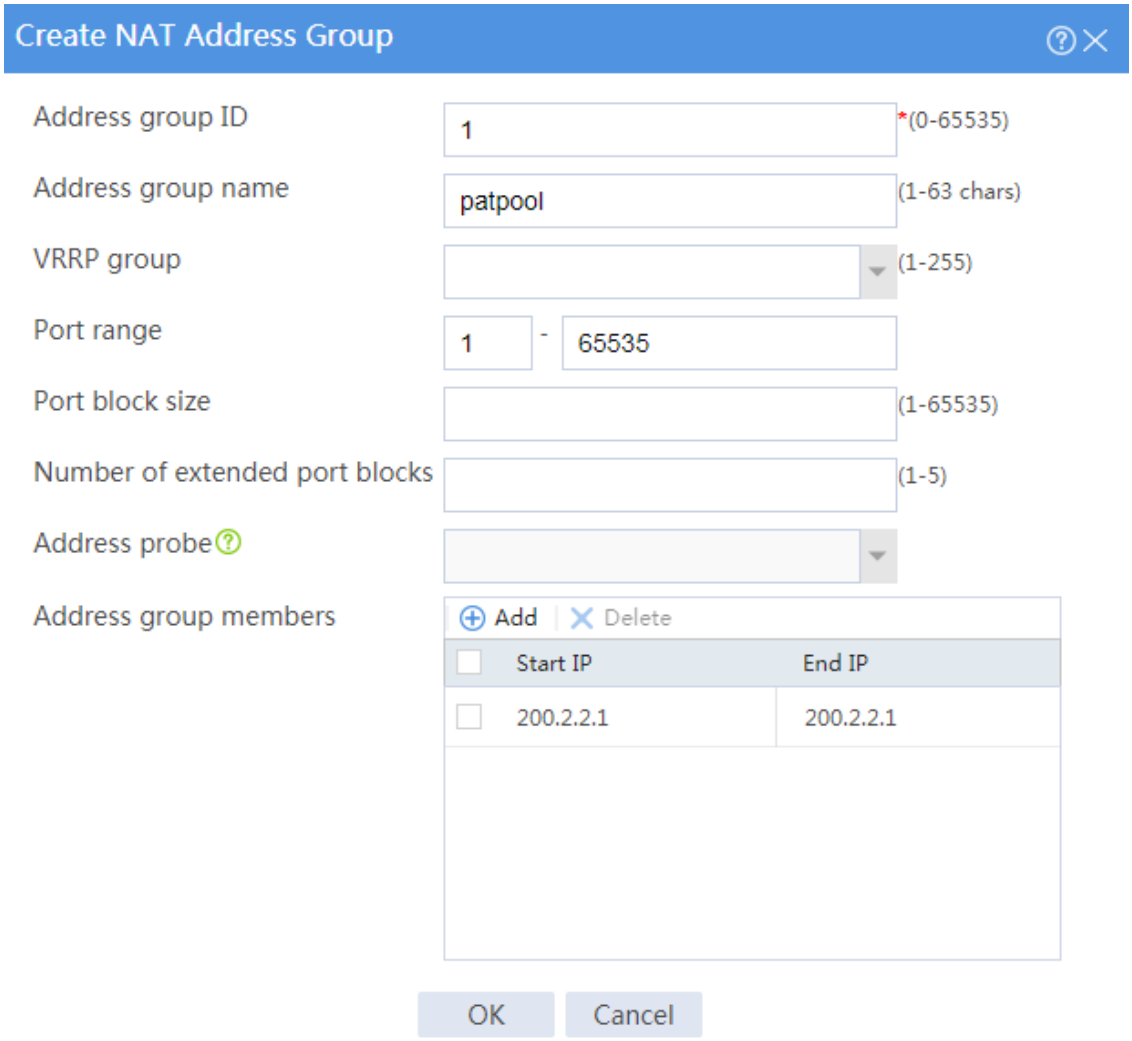
   # On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **NAT Address Groups**.

Click **Create**.

Create a NAT address group, as shown in Figure 10.

Figure 10 Creating a NAT address group



Click **OK**.

5. Configure an outbound dynamic NAT rule.

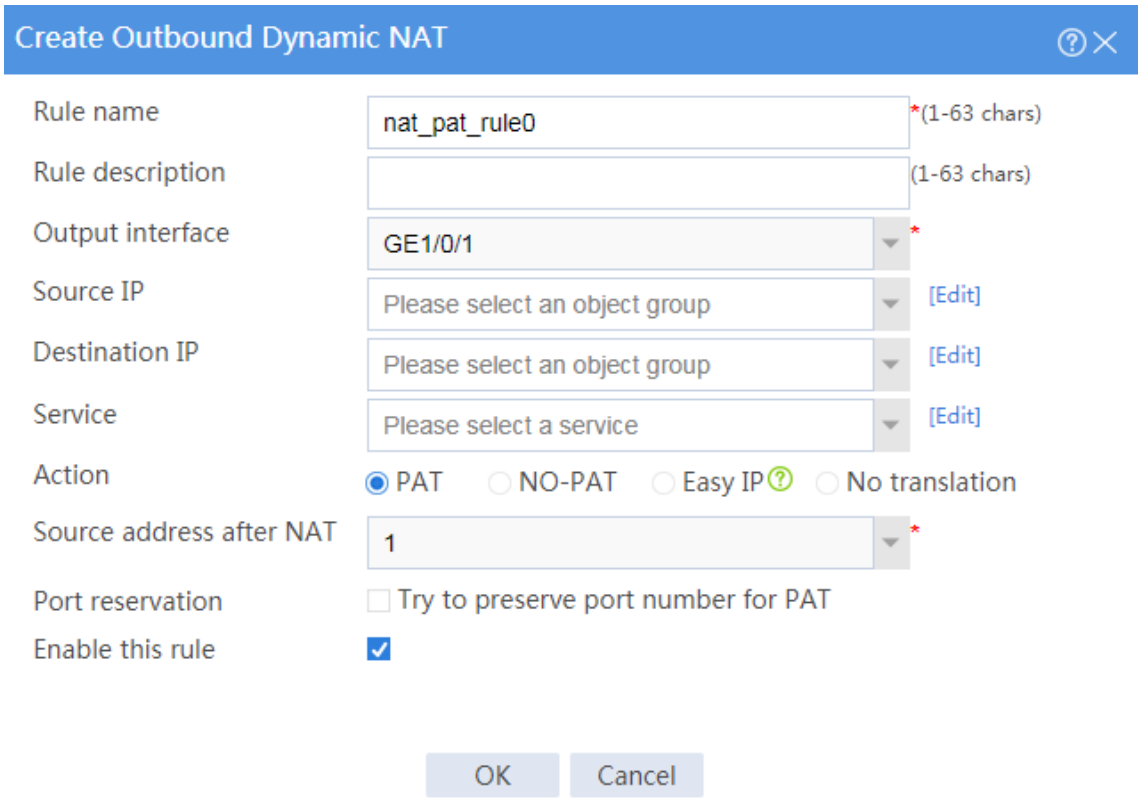
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **Dynamic NAT**.

On the **Outbound Dynamic NAT (Object Group-Based)** tab, click **Create**.

Create an outbound dynamic NAT rule, as shown in Figure 11.

Figure 11 Creating an outbound dynamic NAT rule



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the server on the external network.

```
C:\Users\abc>ping 100.100.100.100

Pinging host.com [100.100.100.100] with 32 bytes of data:
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
```

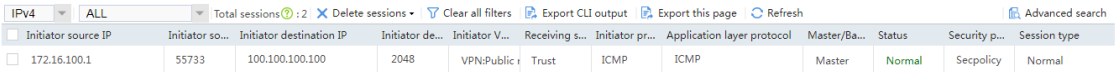
```
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253

Ping statistics for 100.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a NAT session is generated when the host accesses the server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 12 Session list



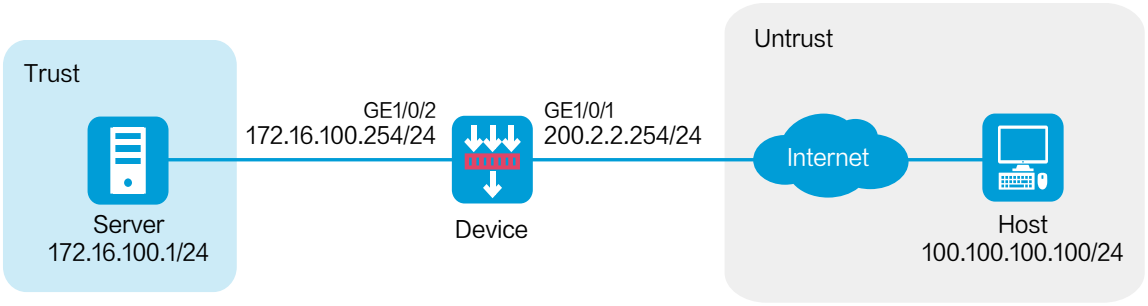
Example: Configuring the NAT Server

Network configuration

As shown in Figure 13, the server in the internal network to provide Web services for external users.

Configure the NAT Server feature to allow the external user to use public address 200.2.2.1/24 to access the internal server.

Figure 13 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 200.2.2.254/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and set its IP address to 172.16.100.254/24 in the same way you configure GE 1/0/1.

2. Configure a security policy.

   # On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Untrust.

c. Select the destination zone. In this example, the destination zone is Trust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP address of the host as the source IPv4 address. In this example, the address is 100.100.100.100.

g. Specify the IP address of the server as the destination IPv4 address. In this example, the address is 172.16.100.1.

h. Click **OK**.

3. Configure a NAT server rule.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **NAT Servers** > **Policy Configuration**.

Click **Create**.

Create a NAT server rule, as shown in Figure 14.

Figure 14 Creating a NAT server rule

Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the public address.

```
C:\Users\abc>ping 200.2.2.1

Pinging host.com [200.2.2.1] with 32 bytes of data:
Reply from 200.2.2.1: bytes=32 time<1ms TTL=253
Reply from 200.2.2.1: bytes=32 time<1ms TTL=253
Reply from 200.2.2.1: bytes=32 time<1ms TTL=253
Reply from 200.2.2.1: bytes=32 time<1ms TTL=253
```

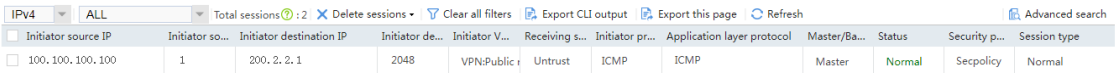
```
Ping statistics for 200.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a NAT session is generated when the host accesses the internal server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 15 Session list

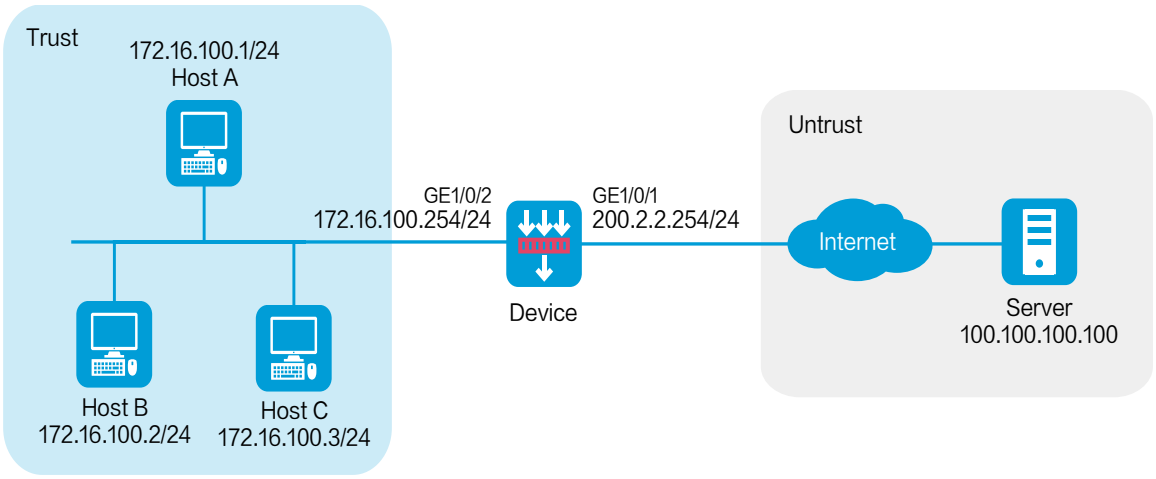


Example: Configuring static NAT444

Network configuration

As shown in Figure 16, a company has one public IP address 200.2.2.1/24. Configure static NAT444 port block mapping to allow internal network users to use this public IP address to access the Internet. Configure the port range as 10001 to 15000, and set the port block size to 500.

Figure 16 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 200.2.2.254/24.

   c. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 172.16.100.254/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing.

This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static route to permit packets from the hosts to the server:

a. Specify the IP address of the server as the destination IP address. In this example, the address is 100.100.100.100.

b. Enter the mask length. In this example, enter 24.

c. Specify the public address as the next-hop address as 200.2.2.253.

d. Click **OK**.

3. Configure a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Trust.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP addresses of the hosts as the source IPv4 addresses. In this example, the addresses are 172.16.100.1, 172.16.100.2, and 172.16.100.3.

g. Specify the IP address of the server as the destination IPv4 address. In this example, the address is 100.100.100.100.

h. Click **OK**.

4. Configure a port block group.

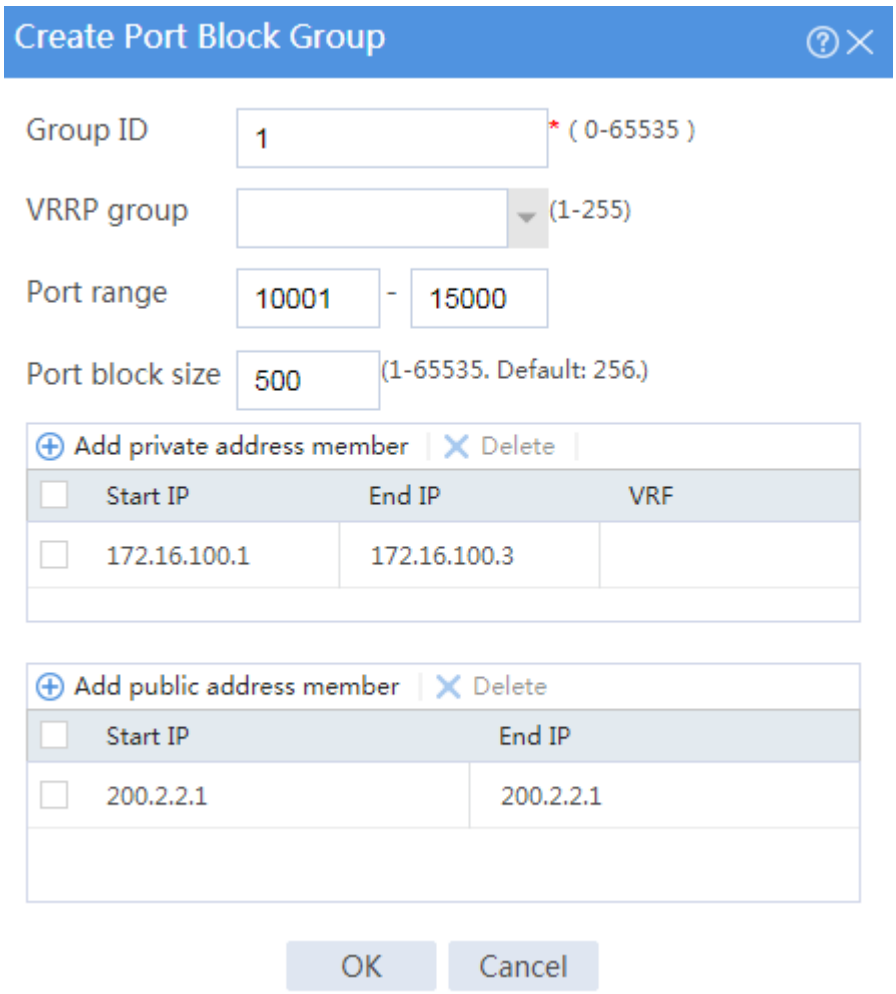
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Interface NAT** > **IPv4** > **Static NAT444** > **Port Blocks**.

   # Click **Create**.

   # Create a port block group, as shown in Figure 17.

Figure 17 Creating a port block group



   # Click **OK**.

5. Configure a static NAT444 rule.

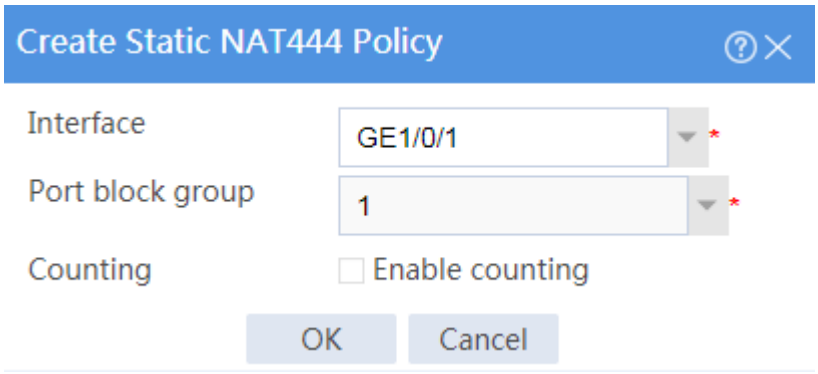
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Interface NAT** > **IPv4** > **Static NAT444** > **Policy Configuration**.

Click **Create**.

Create a static NAT444 rule, as shown in Figure 18.

Figure 18 Creating a static NAT444 rule



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the server on the external network.

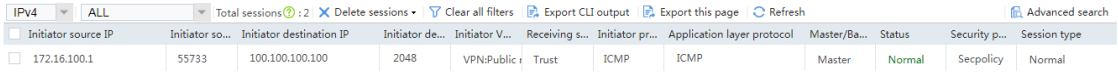
```
C:\Users\abc>ping 100.100.100.100

Pinging host.com [100.100.100.100] with 32 bytes of data:
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253

Ping statistics for 100.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a NAT session is generated when the host accesses the server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

   Figure 19 Session list



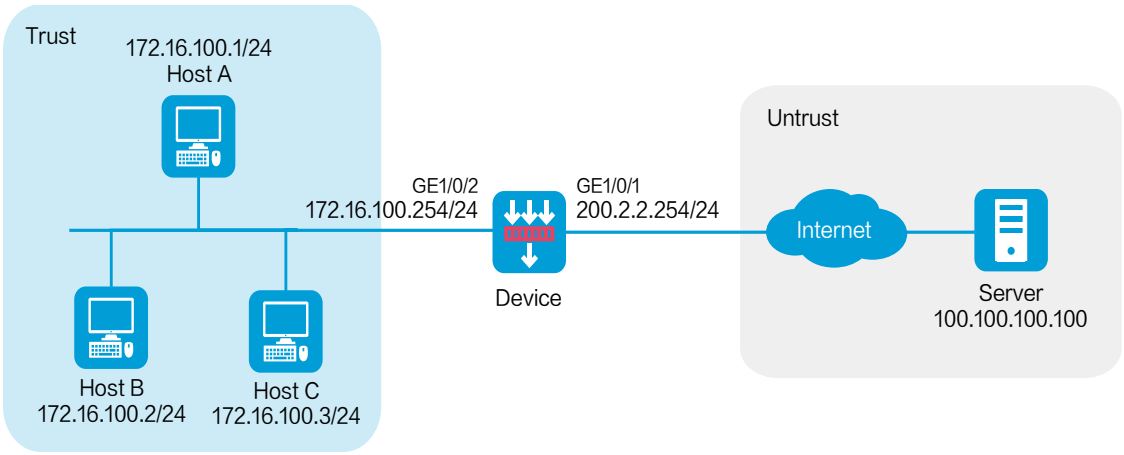
Example: Configuring dynamic NAT444

Network configuration

As shown in Figure 20, a company has public IP addresses 200.2.2.1/24 to 200.2.2.3/24. Configure NAT444 dynamic port block mapping to meet the following requirements:

- The internal network users can use public IP addresses to access the Internet.
- The port range for the public IP addresses is 1024 to 65535.
- The port block size is 500.
- If the ports in the assigned port block are all used, extend another port block for users.

Figure 20 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 200.2.2.254/24.

   c. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and set its IP address to 172.16.100.254/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing.

   This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static route to permit packets from the hosts to the server:

   a. Specify the IP address of the server as the destination IP. In this example, the address is 100.100.100.100.

   b. Enter the mask length. In this example, enter 24.

   c. Specify the public address as the next-hop address as 200.2.2.253.

   d. Click **OK**.

3. Configure a security policy.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create** and click **Create a policy**.

   # In the dialog box that opens, configure policy parameters as follows:

   a. Specify the policy name. In this example, the name is **Secpolicy**.

   b. Select the source zone. In this example, the source zone is Trust.

   c. Select the destination zone. In this example, the destination zone is Untrust.

   d. Select **IPv4** as the type.

   e. Select **Permit** as the action.

   f. Specify the IP addresses of the host as the source IPv4 addresses. In this example, the address is 172.16.100.1, 172.16.100.2, and 172.16.100.3.

   g. Specify the IP address of the server as the destination IPv4 address. In this example, the address is 100.100.100.100.

   h. Click **OK**.

4. Configure a NAT address group.

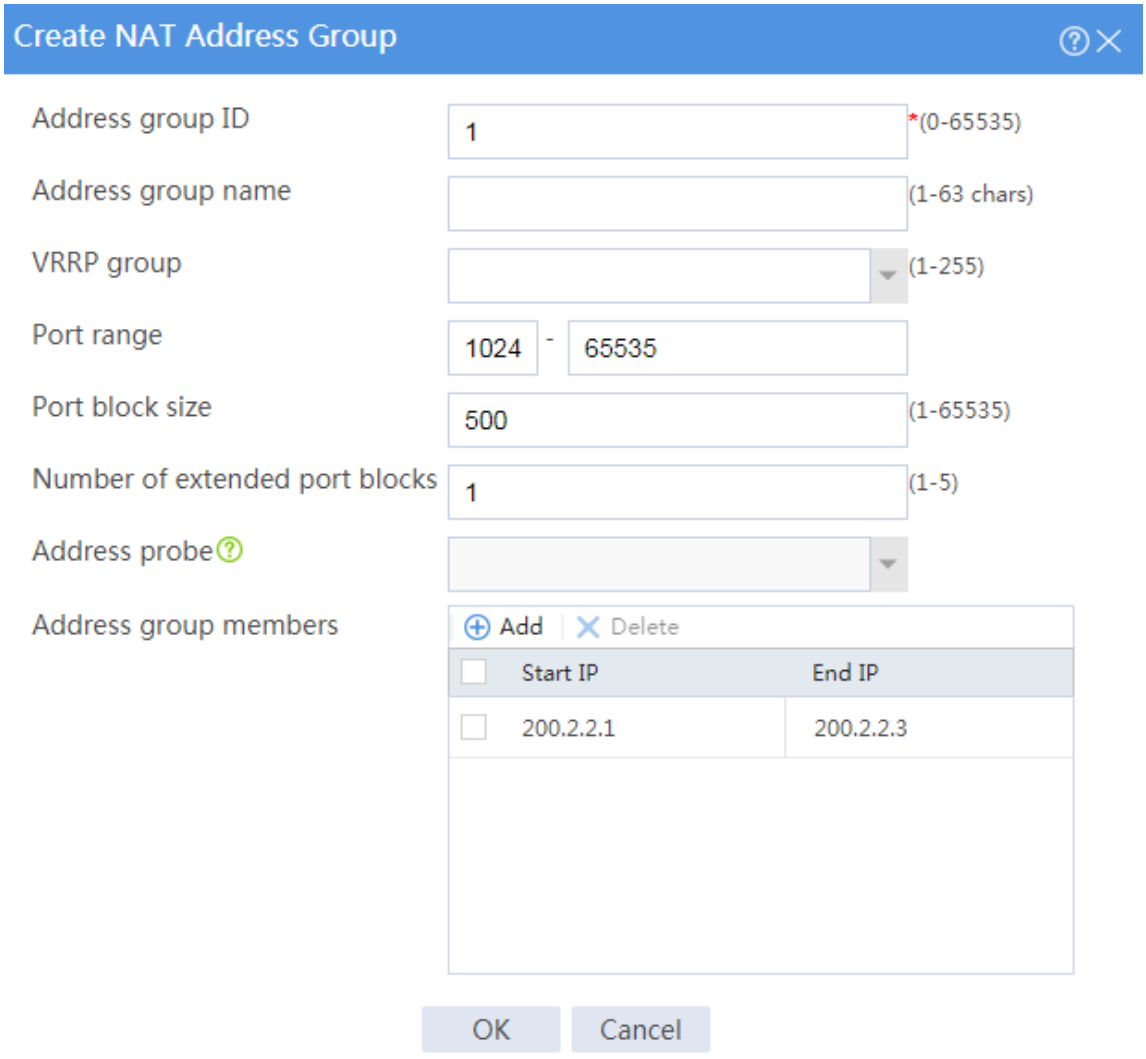
   # On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups**> **NAT Address Groups**.

Click **Create**.

Create a NAT address group, as shown in Figure 21.

Figure 21 Creating a NAT address group



Click **OK**.

5. Configure an outbound dynamic NAT444 rule.

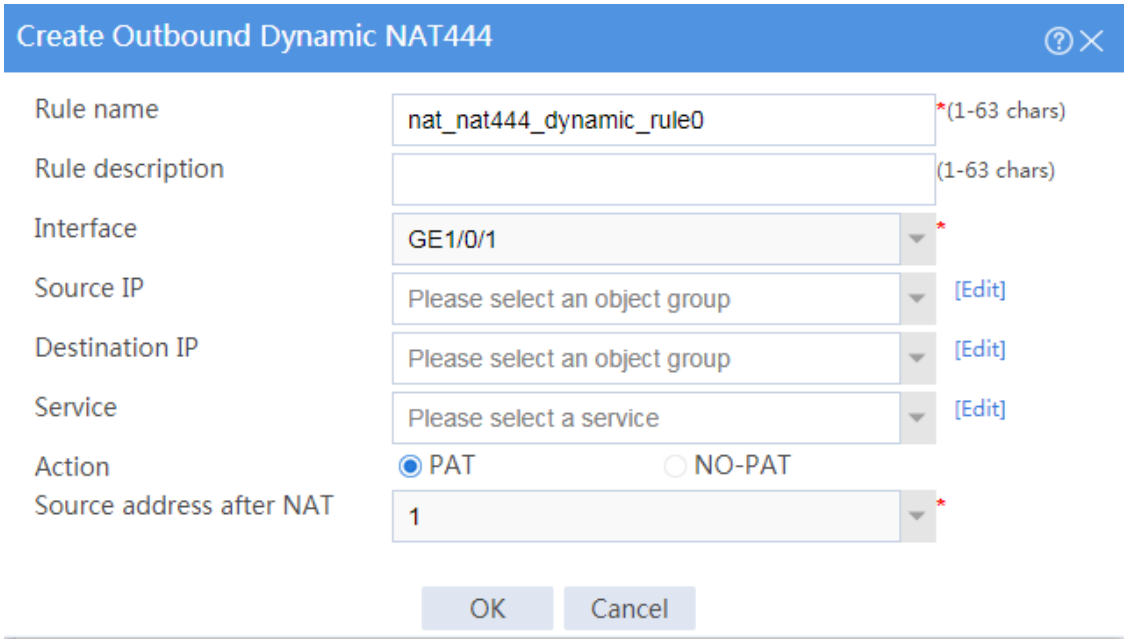
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **Dynamic NAT444**.

On the **Outbound Dynamic NAT444 (Object Group-Based)** tab, click **Create**.

Create an outbound dynamic NAT444 rule, as shown in Figure 22.

Figure 22 Configuring a dynamic NAT444 rule



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the server on the external network.

```
C:\Users\abc>ping 100.100.100.100

Pinging host.com [100.100.100.100] with 32 bytes of data:
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253

Ping statistics for 100.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

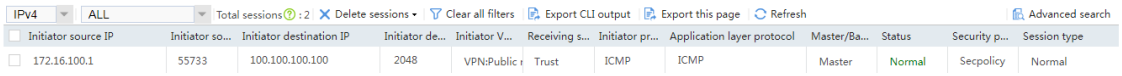
```
Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a NAT session is generated when the host accesses the server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 23 Session list



NPTv6 configuration examples

Contents

Introduction

The following information provides NPTv6 configuration examples.

IPv6-to-IPv6 Network Prefix Translation (NPTv6), also known as NAT66, translates the internal IPv6 prefix in the IPv6 packet header to an external IPv6 prefix and vice versa.

NPTv6 supports the following address translation methods:

- **Source address translation**—Translates source IPv6 addresses in packets when internal users access an external network.
- **Destination address translation**—Translates destination IPv6 addresses in packets when external hosts access servers in the internal network.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the NPTv6 feature.

Restrictions

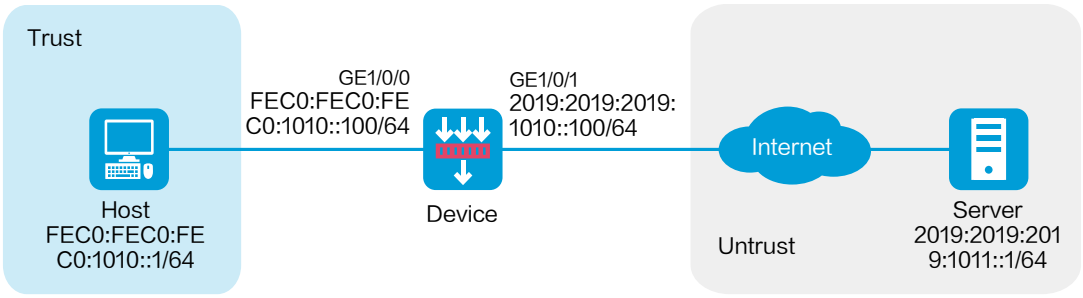
This feature is mutually exclusive with global NAT.

Example: Configuring source address translation

Network configuration

As shown in Figure 1, configure source address translation on the device to allow internal users to access the server in the external network.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv6 Address** tab, enter the IPv6 global unicast address and prefix of the interface. In this example, enter **2019:2019:2019:1010::100/64**.

c. Retain the default configuration for the rest of parameters.

d. Click **OK**.

Add GE 1/0/0 to the **Trust** security zone and set its IPv6 global unicast address to FEC0:FEC0:FEC0:1010::100/64 in the same way you configure GE 1/0/1.

2. Create a route.
   The following configuration example involves only static route for illustration. To apply a dynamic route, you can configure a dynamic routing protocol as needed.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing** > **IPv6 Static Routing**.

   # Click **Create**.

   # In the dialog box that opens, create an IPv6 static route.

   - Enter 2019:2019:2019:1011::1 as the destination address.
   - Set the prefix length to 64.
   - Enter 2019:2019:2019:1010::101 as the next hop.
   - Retain the default configuration for the rest of parameters.

   # Click **OK**.

3. Create a security policy.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that appears, configure a security policy to allow packets from the internal network to pass through.

   - Enter policy name **Secpolicy**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select type **IPv6**.
   - Select action **Permit**.

- Enter FEC0:FEC0:FEC0:1010::1 as the source address.
- Enter 2019:2019:2019:1011::1 as the destination address.
- Retain the default configuration for the rest of parameters.

Click **OK**.

4. Configure NPTv6.

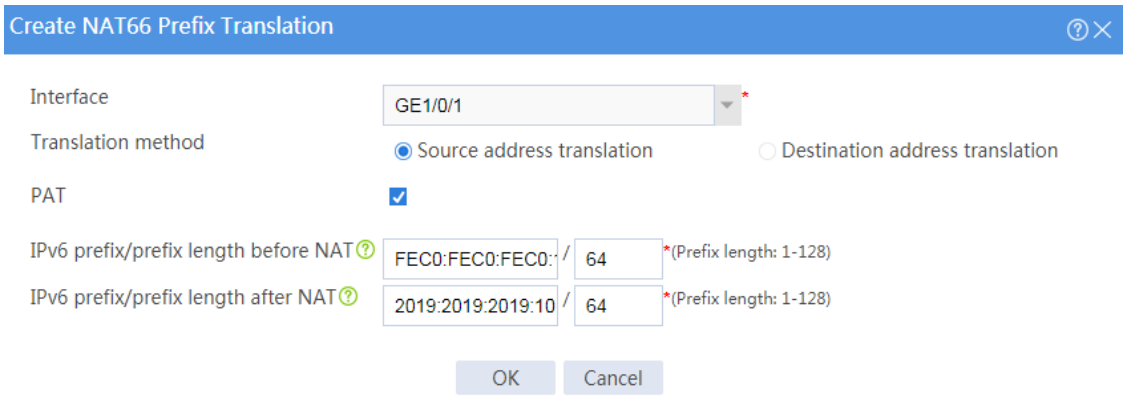
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv6** > **NAT66 Prefix Translation**.

Click **Create**.

Create a prefix translation mapping, as shown in Figure 2.

Figure 2 Creating a NAT66 prefix translation mapping



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the server in the external network.

```
C:\Users\abc>ping 2019:2019:2019:1011::1
```

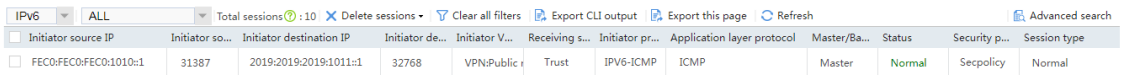
```
Pinging 2019:2019:2019:1011::1 with 32 bytes of data:

Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253

Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253

Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253

Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253


Ping statistics for 2019:2019:2019:1011::1:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a session is generated when the host accesses the server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 3 Session list

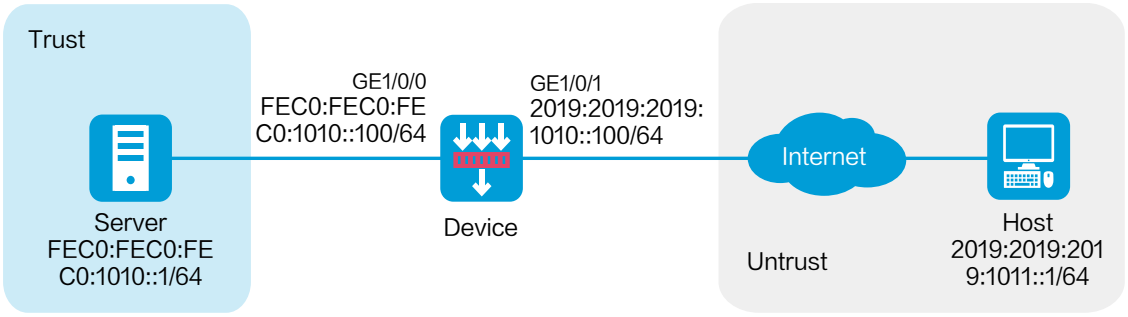


Example: Configuring destination address translation

Network configuration

As shown in Figure 4, configure destination address translation on the device to allow the external host to access the internal Web server.

Figure 4 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv6 Address** tab, enter the IPv6 global unicast address and prefix of the interface. In this example, enter **2019:2019:2019:1010::100/64**.

c. Retain the default configuration for the rest of parameters.

d. Click **OK**.

Add GE 1/0/0 to the **Trust** security zone and set its IPv6 address to FEC0:FEC0:FEC0:1010::100/64 in the same way you configure GE 1/0/1.

2. Create a route.
The following configuration example involves only static route for illustration. To apply a dynamic route, you can configure a dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing** > **IPv6 Static Routing**.

Click **Create**.

In the dialog box that opens, create an IPv6 static route.

- Enter :: as the destination address.
- Set the prefix length to 0.
- Enter 2019:2019:2019:1010::101 as the next hop.
- Retain the default configuration for the rest of parameters.

Click **OK**.

3. Create a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that appears, configure a security policy to allow packets from the external host to pass through.

- Enter policy name **Secpolicy**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv6**.
- Select action **Permit**.
- Enter 2019:2019:2019:1011::1 as the source address.
- Enter FEC0:FEC0:FEC0:1010::1 as the destination address.
- Retain the default configuration for the rest of parameters.

Click **OK**.

4. Configure NPTv6.

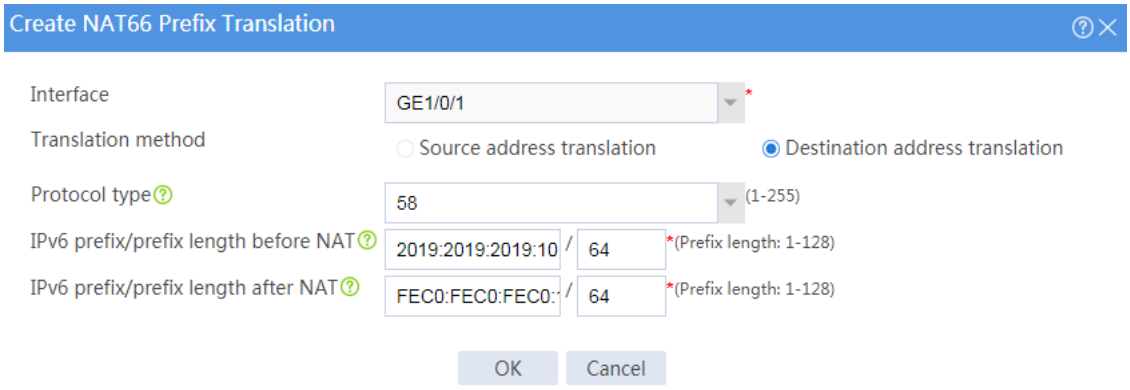
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv6** > **NAT66 Prefix Translation**.

Click **Create**.

Create a prefix translation mapping, as shown in Figure 5.

Figure 5 Creating a NAT66 prefix translation mapping



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the internal Web server.

```
C:\Users\abc>ping 2019:2019:2019:1011::1

Pinging 2019:2019:2019:1011::1 with 32 bytes of data:
Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253
Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253
Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253
Reply from 2019:2019:2019:1011::1: bytes=32 time<1ms TTL=253

Ping statistics for 2019:2019:2019:1011::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

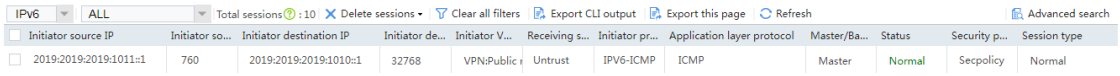
```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that a session is generated when the host accesses the internal Web server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 6 Session list



Policy-based NAT configuration examples

Contents

Introduction

The following information describes policy-based NAT configuration examples.

Policy-based NAT contains a set of NAT rules to identify and translate matching packets. The packet match criteria include source security zone, destination security zone, source IP address, destination IP address, and service.

Policy-based NAT supports the following types of rules, which are applicable to different scenarios:

- **NAT44 rule**—Used for NAT translation between IPv4 networks.

- **NAT64 rule**—Used for NAT translation between IPv4 networks and IPv6 networks.
- **NAT66 rule**—Used for NAT translation between IPv6 networks.

Policy-based NAT supports the following translation modes:

- **Source address translation**—Translates the source IP address and source port of packets.
- **Destination address translation**—Translates the destination IP address and destination port of packets.
- **Bidirectional translation**—Translates the source IP address, source port, destination IP address, and destination port of packets.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of policy-based NAT.

Restrictions and guidelines

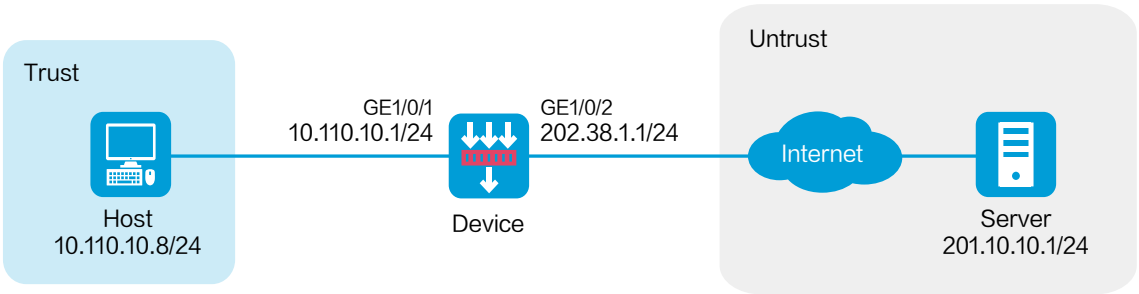
Do not configure both policy-based NAT and interface-based NAT.

Example: Configuring static NAT for internal-to-external access

Network configuration

As shown in Figure 1, configure policy-based source address translation to allow the host at 10.110.10.8/24 to access the server at 201.10.10.1/24 on the Internet by using public IP address 202.38.1.100.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

a. Select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 202.38.1.1/24.

c. Click **OK**.

Add GE 1/0/1 to the **Trust** security zone and set its IP address to 10.110.10.1/24 in the same way you configure GE 1/0/2.

2. Configure settings for routing.

This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure a static route to permit packets from the device to the server:

a. Specify the IP address of the server as the destination IP. In this example, the address is 201.10.10.1.

b. Enter the mask length. In this example, enter 24.

c. Specify the next-hop address as 202.38.1.2.

d. Click **OK**.

3. Configure a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Trust.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP address of the host as the source IPv4 address. In this example, the address is 10.110.10.8.

g. Specify the IP address of the server as the destination IPv4 address. In this example, the address is 201.10.10.1.

h. Click **OK**.

4. Create a policy-based NAT rule.

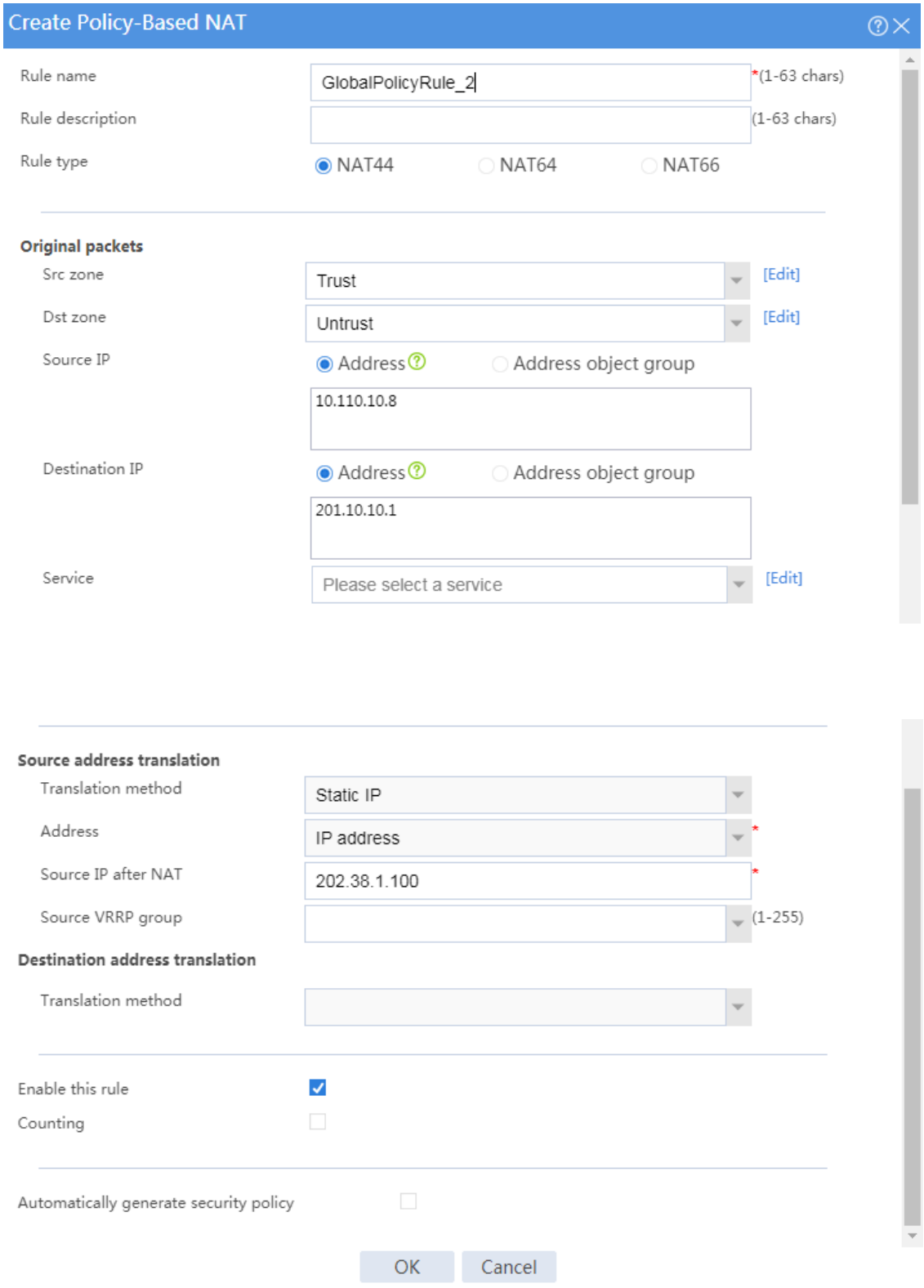
On the top navigation bar, click **Policies**.

From the navigation pane, select **Policy-based NAT**.

Click **Create**.

Create a policy-based NAT rule, as shown in Figure 2.

Figure 2 Creating a policy-based NAT rule



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the server on the external network.

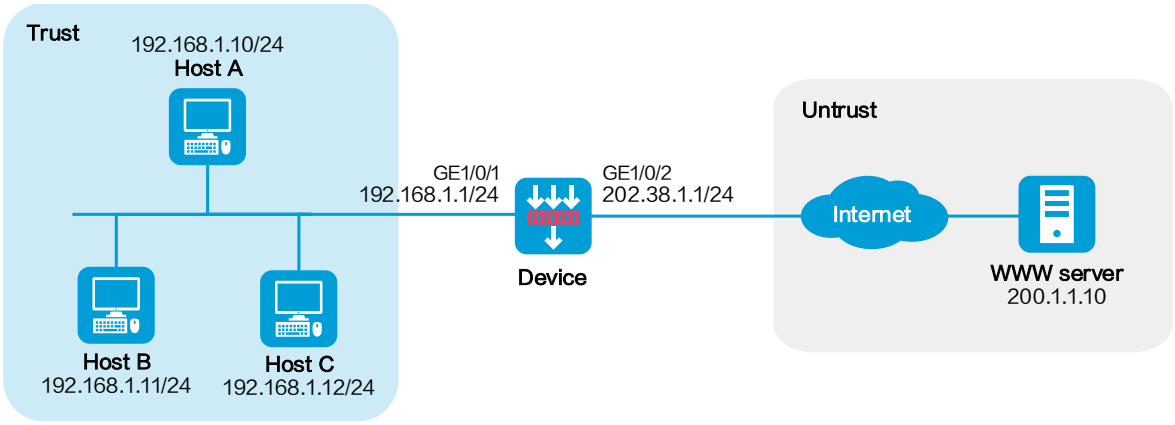
```
C:\Users\abc>ping 201.10.10.1


Pinging host.com [201.10.10.1] with 32 bytes of data:
Reply from 201.10.10.1: bytes=32 time<1ms TTL=253
Reply from 201.10.10.1: bytes=32 time<1ms TTL=253
Reply from 201.10.10.1: bytes=32 time<1ms TTL=253
Reply from 201.10.10.1: bytes=32 time<1ms TTL=253

Ping statistics for 201.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Example: Configuring dynamic NAT for internal-to-external access

Network configuration

As shown in Figure 3, the company has public addresses 202.38.1.1/24 to 202.38.1.3/24. Configure policy-based source address translation to enable internal hosts to access the server on the Internet.

Figure 3 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/2.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 202.38.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/1 to the **Trust** security zone and set its IP address to 192.168.1.1/24 in the same way you configure GE 1/0/2.

2. Configure settings for routing.

   This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static route to permit packets from the internal hosts to the external server:

   a. Specify the IP address of the server as the destination IP. In this example, the address is 200.1.1.10.

   b. Enter the mask length. In this example, enter 24.

c. Specify the next-hop address as 202.38.1.2.

d. Click **OK**.

3. Configure a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Trust.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP addresses of the hosts as the source IPv4 addresses. In this example, the addresses are 192.168.1.10, 192.168.1.11, and 192.168.1.12.

g. Specify the IP address of the server as the destination IPv4. In this example, the address is 200.1.1.10.

h. Click **OK**.

4. Configure a NAT address group.

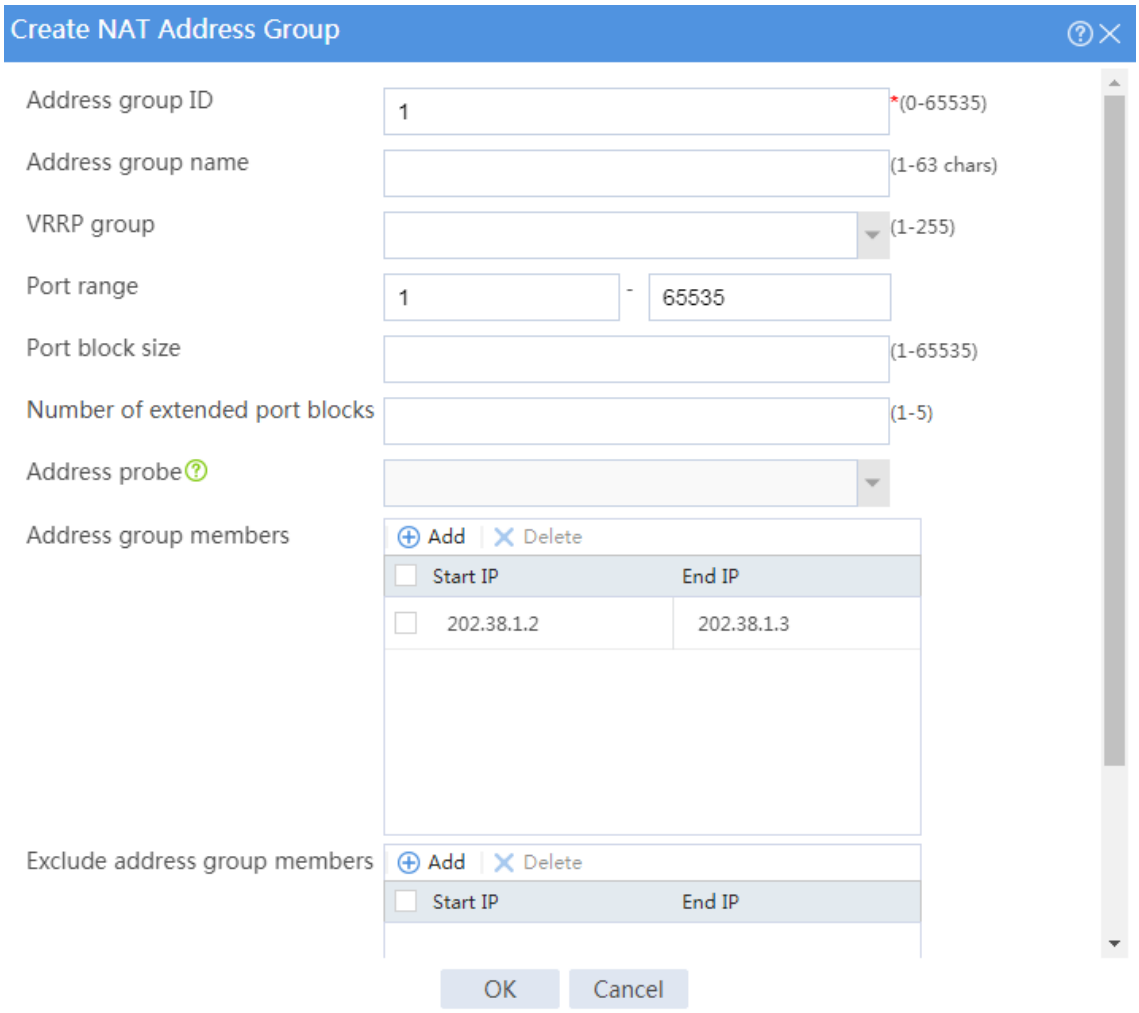
On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **NAT Address Groups**.

Click **Create**.

Create a NAT address group, as shown in Figure 4.

Figure 4 Creating a NAT address group



Click **OK**.

5. Configure a policy-based NAT rule.

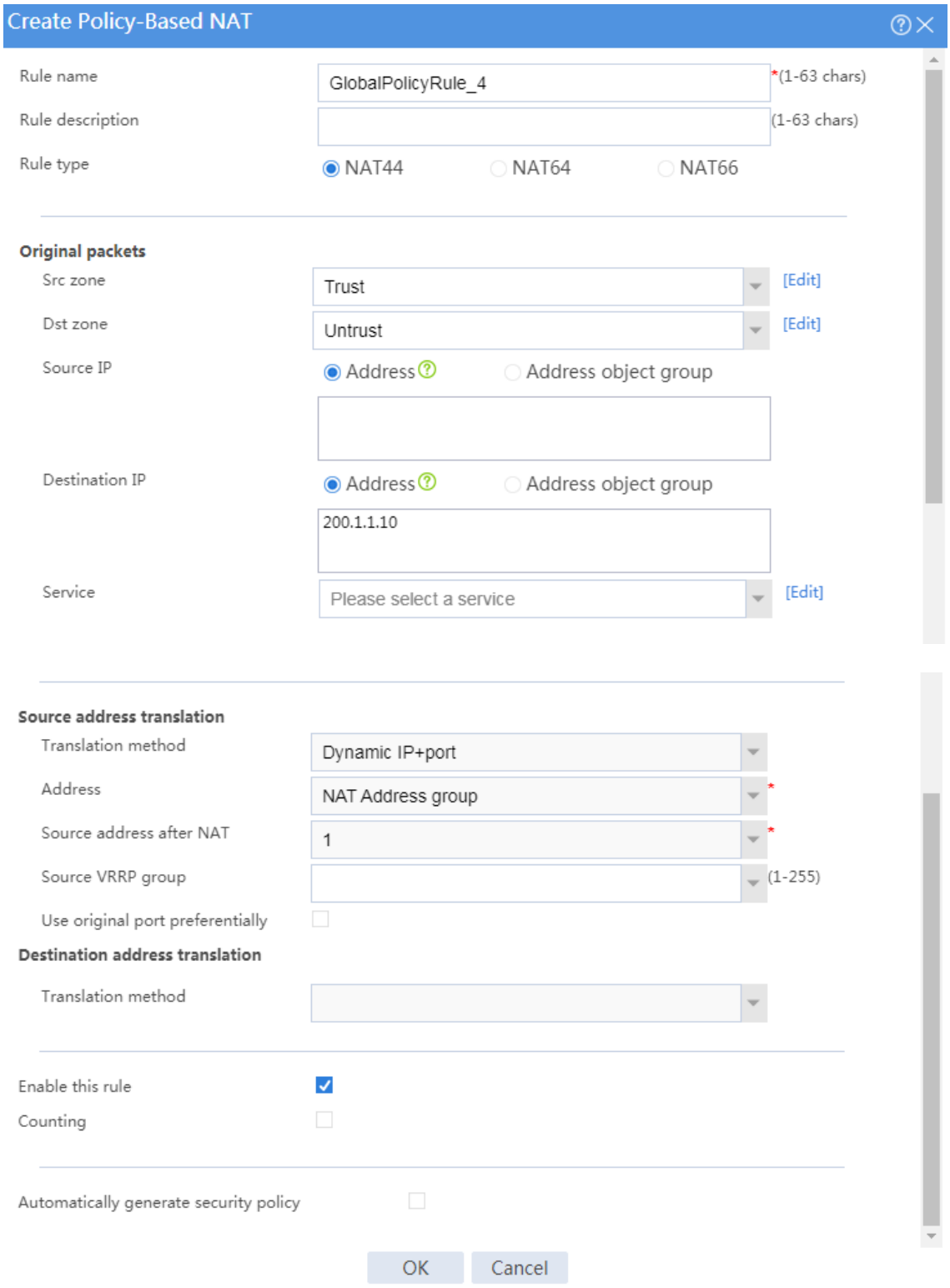
On the top navigation bar, click **Policies**.

From the navigation pane, select **NAT** > **Policy-based NAT**.

Click **Create**.

Create a policy-based NAT rule, as shown in Figure 5.

Figure 5 Creating a policy-based NAT rule



Click **OK**.

Verifying the configuration

1. Verify that the host can successfully ping the server on the external network.

```
C:\Users\abc>ping 200.1.1.10


Pinging host.com [200.1.1.10] with 32 bytes of data:

Reply from 200.1.1.10: bytes=32 time<1ms TTL=253

Reply from 200.1.1.10: bytes=32 time<1ms TTL=253

Reply from 200.1.1.10: bytes=32 time<1ms TTL=253

Reply from 200.1.1.10: bytes=32 time<1ms TTL=253


Ping statistics for 200.1.1.10:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

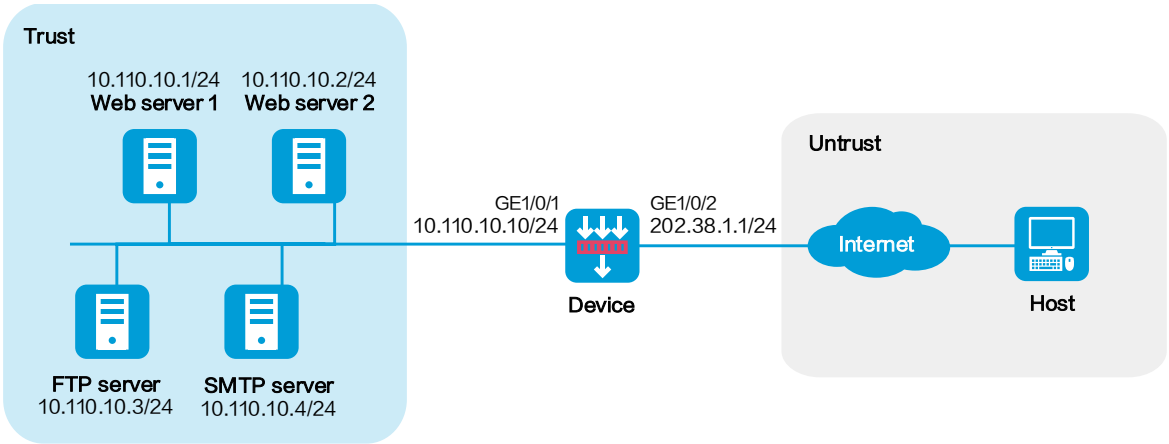
Example: Configuring destination address translation for external-to-internal access through public address

Network configuration

As shown in Figure 6, a company has four servers on the internal network at 10.110.10.0/24 and three public addresses from 202.38.1.1/24 to 202.38.1.3/24. Configure policy-based destination address translation to allow the external host to access the servers by using public address 202.38.1.1 with different ports. The external host uses the following ports to access different servers:

- Uses port 80 to access Web server 1.
- Uses port 8080 to access Web server 2.
- Uses port 21 to access FTP server.
- Uses port 25 to access SMTP server.

Figure 6 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/2.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 202.38.1.1/24.

   c. Click **OK**.

   # Add GE 1/0/1 to the **Trust** security zone and set its IP address to 10.110.10.10/24 in the same way you configure GE 1/0/2.

2. Configure a security policy.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Untrust.

c. Select the destination zone. In this example, the destination zone is Trust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP addresses of the servers as the destination IPv4 addresses. In this example, the addresses are 10.110.10.1, 10.110.10.2, 10.110.10.3, and 10.110.10.4.

g. Click **OK**.

3. Configure a policy-based NAT rule.

This example configures a policy-based NAT rule for Web server 1.

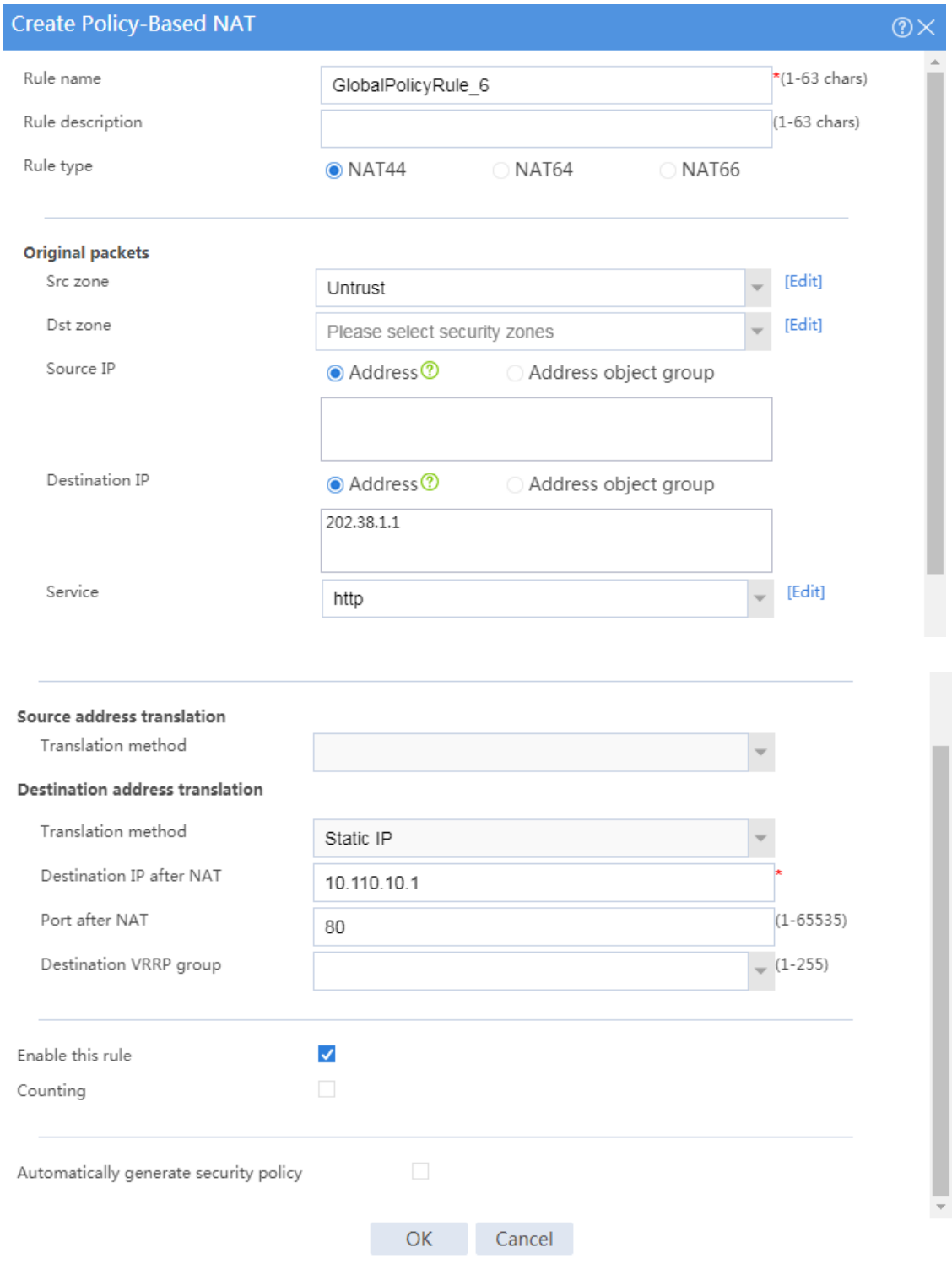
On the top navigation bar, click **Policies**.

From the navigation pane, select **Policy-based NAT**.

Click **Create**.

Create a policy-based NAT rule, as shown in Figure 7.

Figure 7 Creating a policy-based NAT rule



Click **OK**.

Verifying the configuration

Verify that the external host can successfully ping the Web server on the internal network.

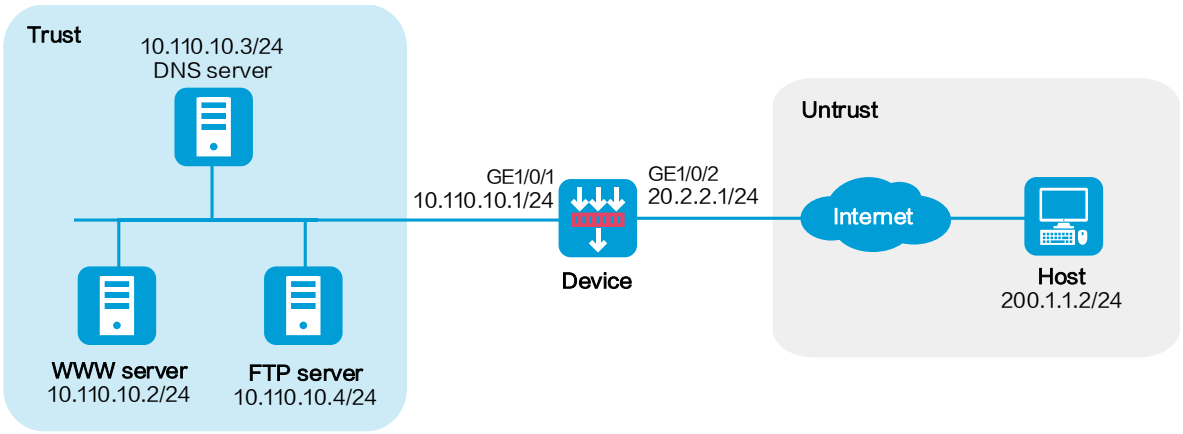
Example: Configuring bidirectional translation for external-to-internal access through domain name

Network configuration

As shown in Figure 8, Web server at 10.110.10.2/24 in the internal network to provide services for external users. A DNS server at 10.110.10.3/24 is used to resolve the domain name of the Web server. The company has public addresses 202.38.1.2 and 202.38.1.3.

Configure bidirectional translation to allow the external user to access the internal Web server by using the domain name.

Figure 8 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/2.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 20.2.2.1/24.

c. Click **OK**.

Add GE 1/0/1 to the **Trust** security zone and set its IP address to 10.110.10.1/24 in the same way you configure GE 1/0/2.

2. Configure a security policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Enter a policy name. In this example, the name is **Secpolicy**.

b. Select the source zone. In this example, the source zone is Untrust.

c. Select the destination zone. In this example, the destination zone is Trust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP addresses of the servers as the destination IPv4 addresses. In this example, the addresses are 10.110.10.2, 10.110.10.3, and 10.110.10.4.

g. Click **OK**.

3. Configure a NAT address group.

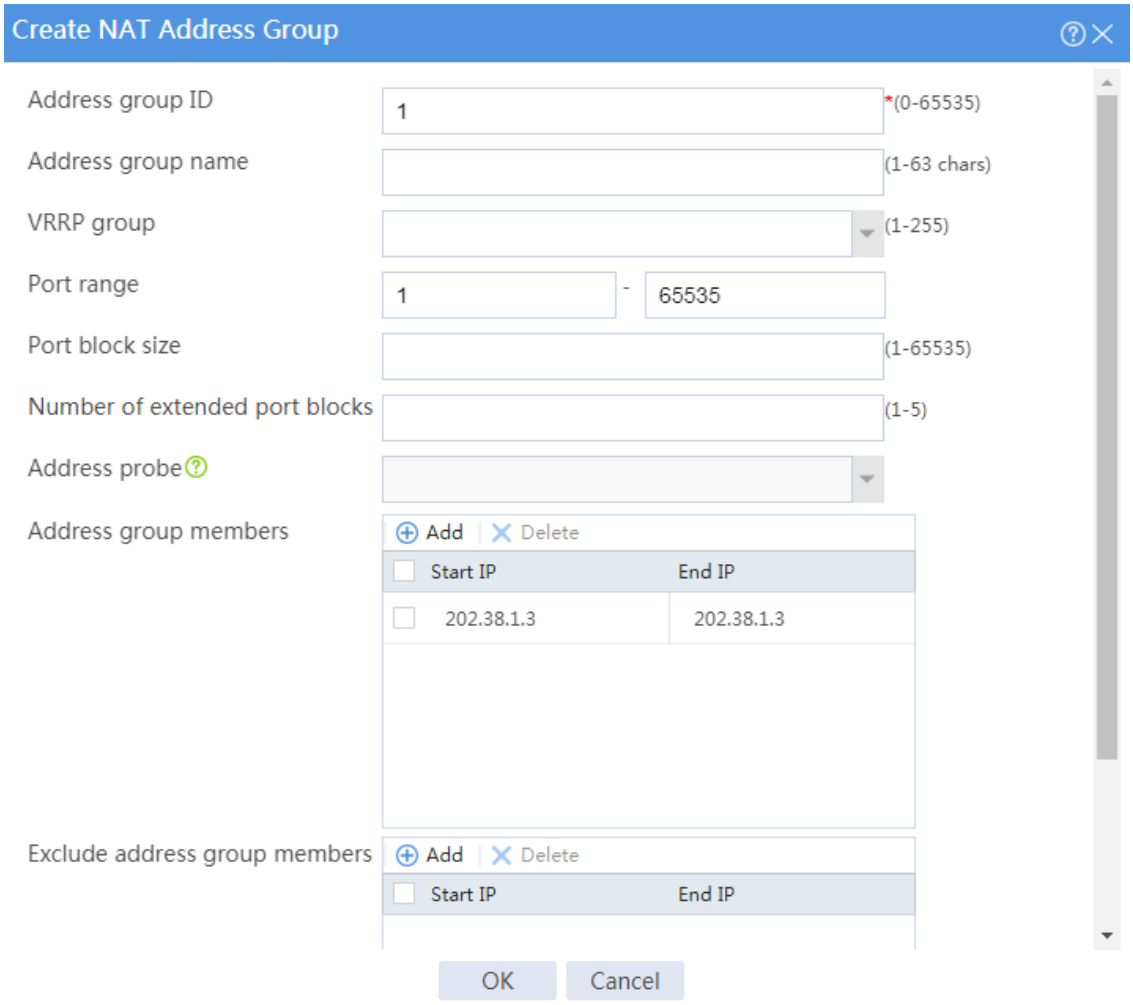
On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **NAT Address Groups**.

Click **Create**.

Create a NAT address group, as shown in Figure 9.

Figure 9 Creating a NAT address group



Click **OK**.

4. Configure policy-based NAT rule 1.

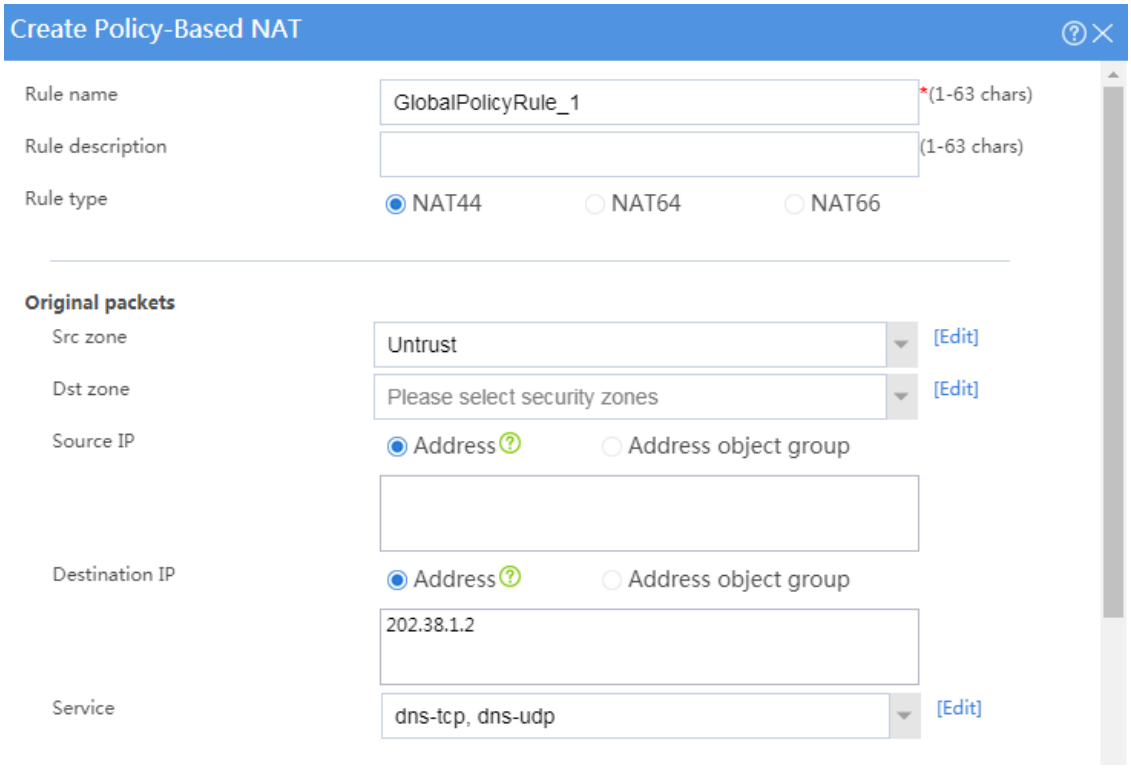
On the top navigation bar, click **Policies**.

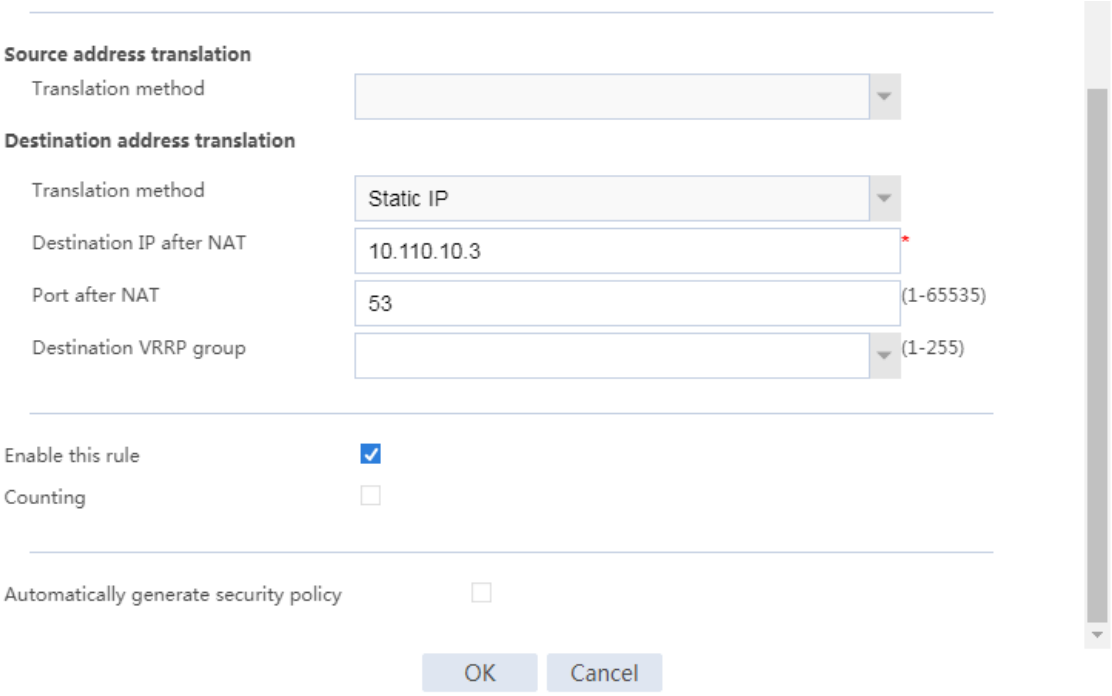
From the navigation pane, select **Policy-based NAT**.

Click **Create**.

Create policy-NAT rule 1 to allow the external user to use public address 202.38.1.2 to access the internal DNS server, as shown in Figure 7.

Figure 10 Creating policy-based NAT rule 1





Click **OK**.

5. Configure policy-based NAT rule 2.

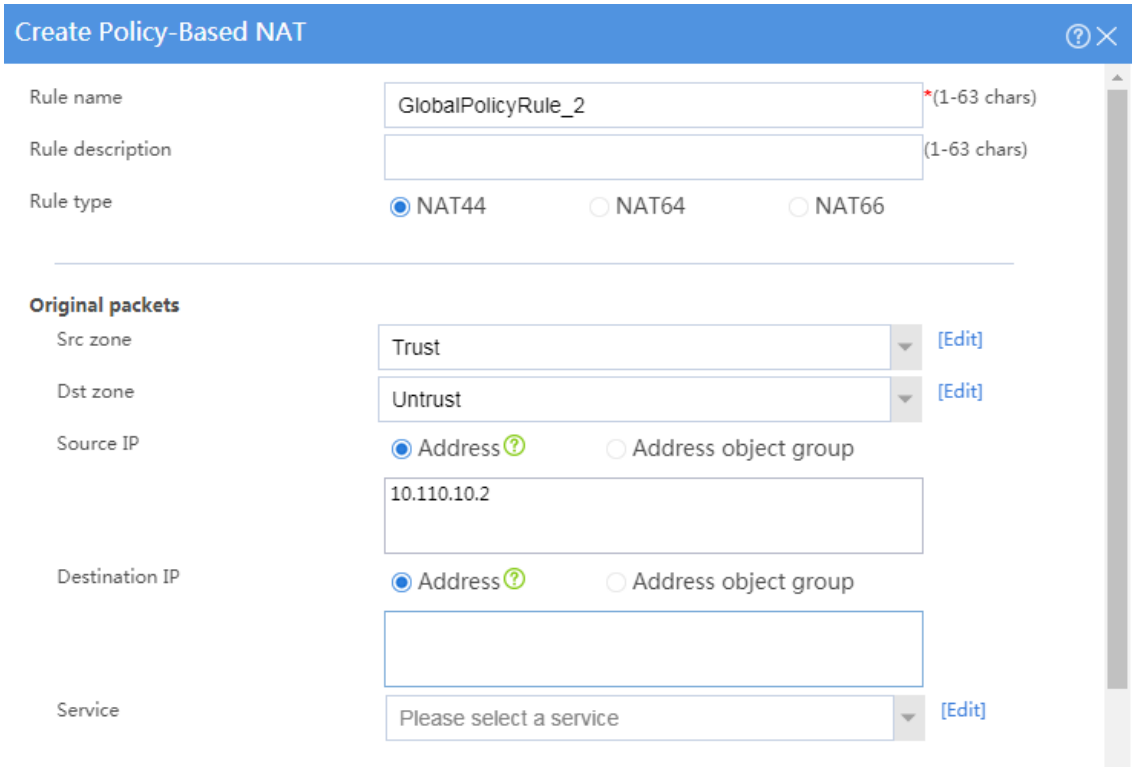
On the top navigation bar, click **Policies**.

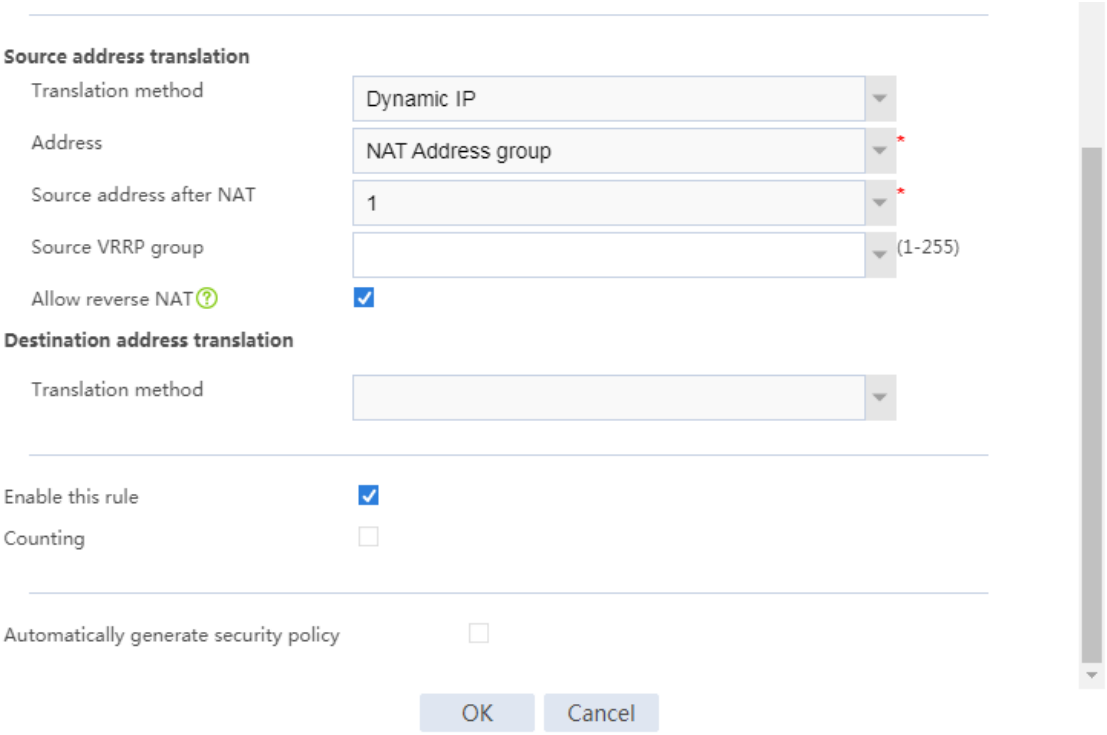
From the navigation pane, select **Policy-based NAT**.

Click **Create**.

Create policy-NAT rule 2 to translate the source address in a DNS response packet to one address in NAT address group 1, as shown in Figure 7.

Figure 11 Creating policy-based NAT rule 2





Click **OK**.

Verifying the configuration

Verify that the external user can successfully ping the Web server on the internal network by using the domain name.

NAT hairpin configuration examples

Contents

Introduction

The following information describes NAT hairpin configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of NAT.

Restrictions and guidelines

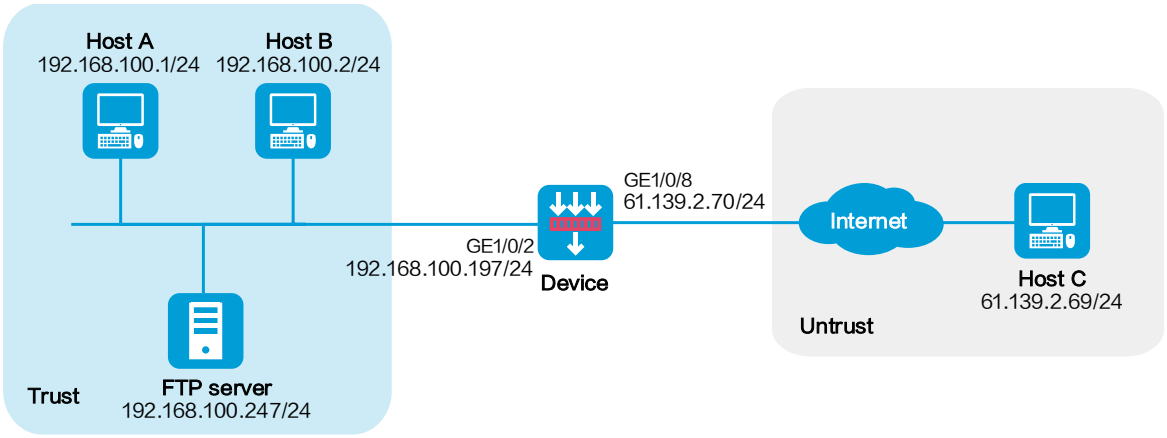
Do not configure both the NAT hairpin feature and a global NAT policy.

Example: Configuring NAT hairpin

Network configuration

As shown in Figure 1, the internal FTP server at 192.168.100.247/24 provides services for internal and external users. Configure NAT hairpin in C/S mode to allow external and internal users to access the internal FTP server by using public IP address 61.139.2.70/24.

Figure 1 Network diagram



Analysis

This example is a typical use of NAT hairpin in C/S mode. To meet the network requirements, perform the following tasks:

- To allow internal hosts to access the internal FTP server by using a public IP address, enable NAT hairpin on the interface connected to the internal network. Configure outbound NAT on

the interface where the NAT server mapping is configured. The destination address is translated by matching the NAT server mapping. The source address is translated by matching the outbound NAT.

- To allow external hosts to access the internal FTP server by using a public IP address, configure NAT Server on the interface connected to the external network.

Software versions used

This configuration example was created and verified on R8560 of the NFNX5-HD6480 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/2.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 192.168.100.197/24.

   c. Click **OK**.

   # Add GE 1/0/8 to the **Untrust** security zone and set its IP address to 61.139.2.70/24 in the same way you configure GE 1/0/1.

2. Configure security policy **Secpolicy1**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create** and click **Create a policy**.

   # In the dialog box that opens, configure policy parameters as follows:

a. Specify the policy name. In this example, the name is **Secpolicy1**.

b. Select the **Trust** security zone as the source zone.

c. Select the **Trust** security zone as the destination zone.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP address of GE 1/0/8 as the source IPv4 address. In this example, the address is 61.139.2.70/24.

g. Specify the IP address of FTP server as the destination IPv4 address. In this example, the address is 192.168.100.247/24.

h. Click **OK**. The configuration is shown in Figure 2.

3. Configure security policy **Secpolicy2**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Specify the policy name. In this example, the name is **Secpolicy2**.

b. Select the **Untrust** security zone as the source zone.

c. Select the **Trust** security zone as the source zone.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP address of Host C as the source IPv4 address. In this example, the address is 61.139.2.69/24.

g. Specify the IP address of FTP server as the destination IPv4 address. In this example, the address is 192.168.100.247/24.

h. Click **OK**.

4. Configure NAT.

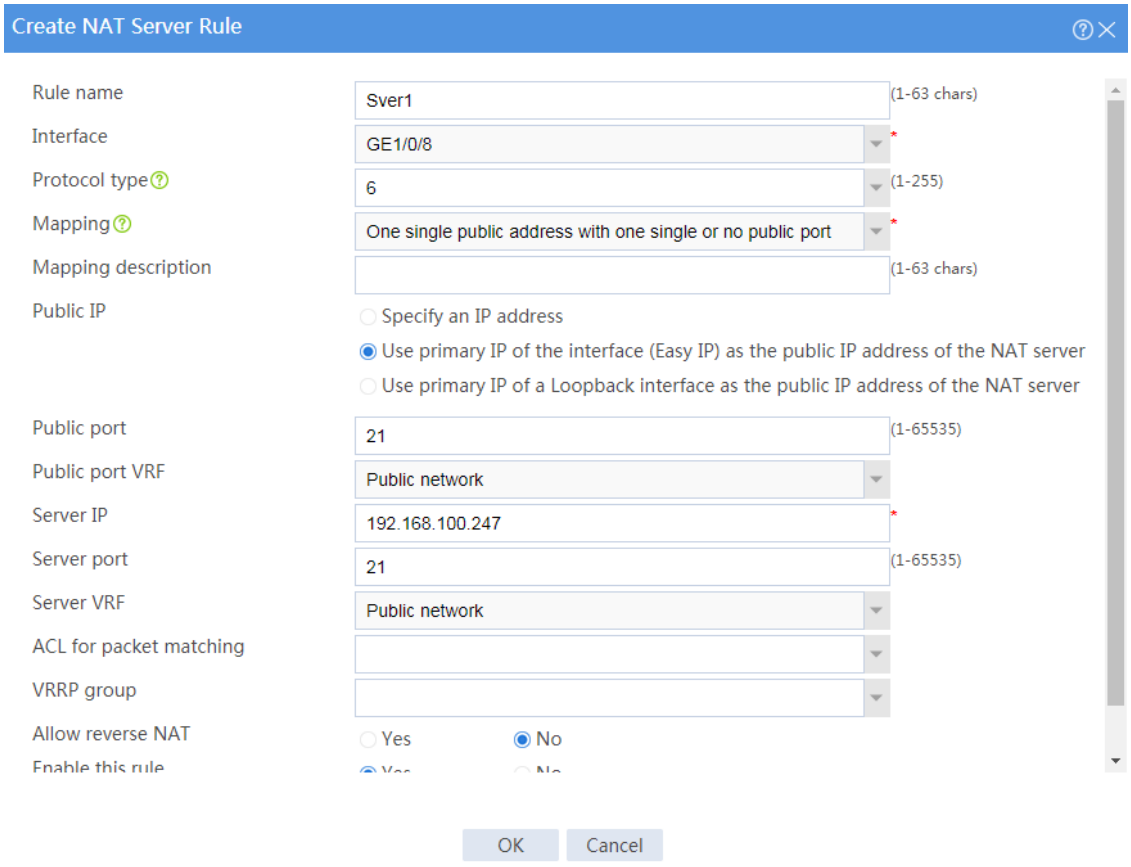
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **NAT Servers** > **Policy Configuration**.

Click **Create**.

In the dialog box that opens, create a NAT server rule, as shown in Figure 2.

Figure 2 Creating a NAT server rule



Click **OK**.

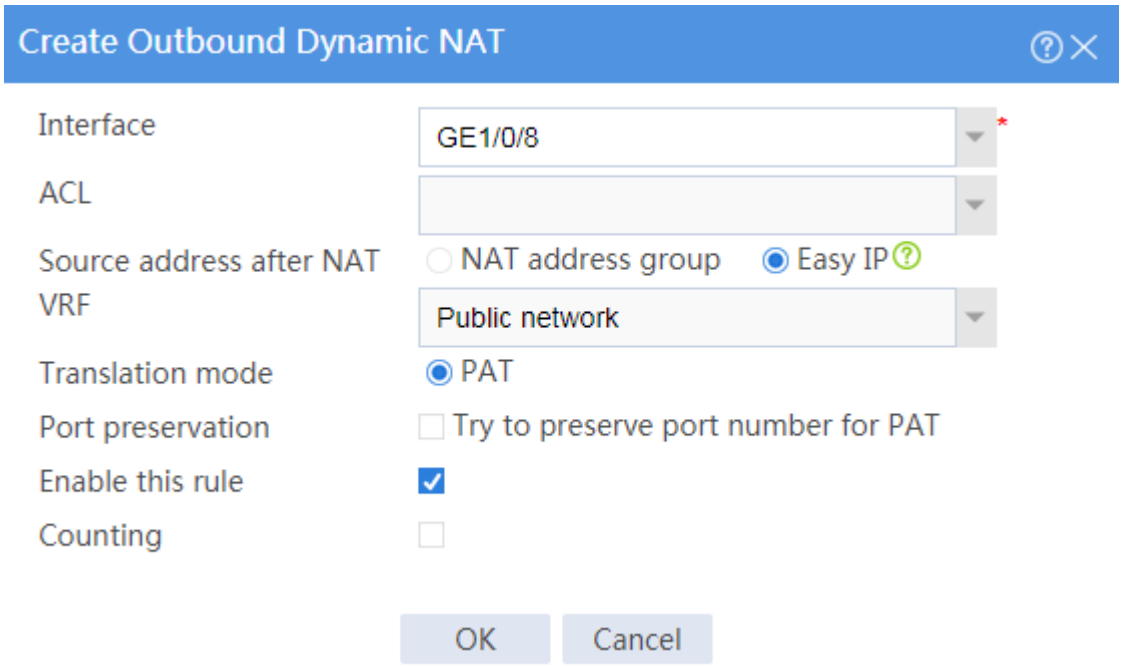
On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **Dynamic NAT**.

On the **Outbound Dynamic NAT (ACL-Based)** tab, click **Create**.

Create an outbound dynamic NAT rule, as shown in Figure 3.

Figure 3 Creating an outbound dynamic NAT rule



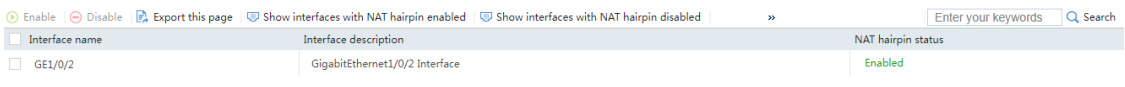
Click **OK**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Interface NAT** > **IPv4** > **NAT Advanced Settings** > **NAT Hairpin**.

Select GE 1/0/2, and click **Enable**. GE 1/0/2 is enabled with NAT hairpin, as shown in Figure 4.

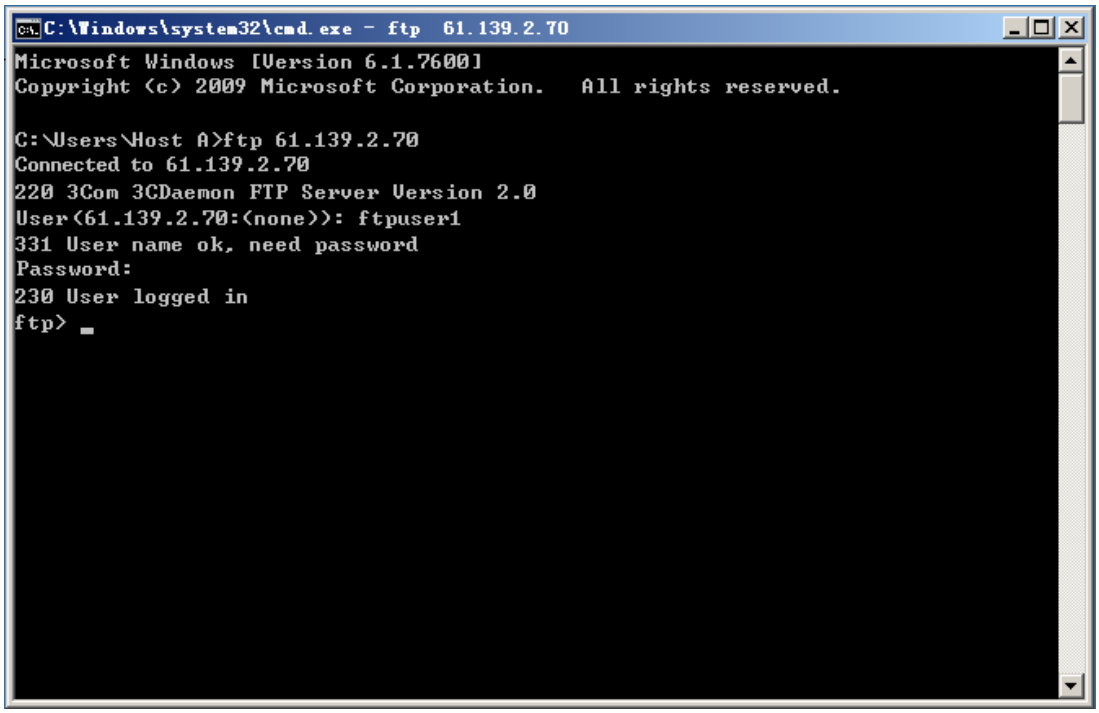
Figure 4 Enabling NAT hairpin



Verifying the configuration

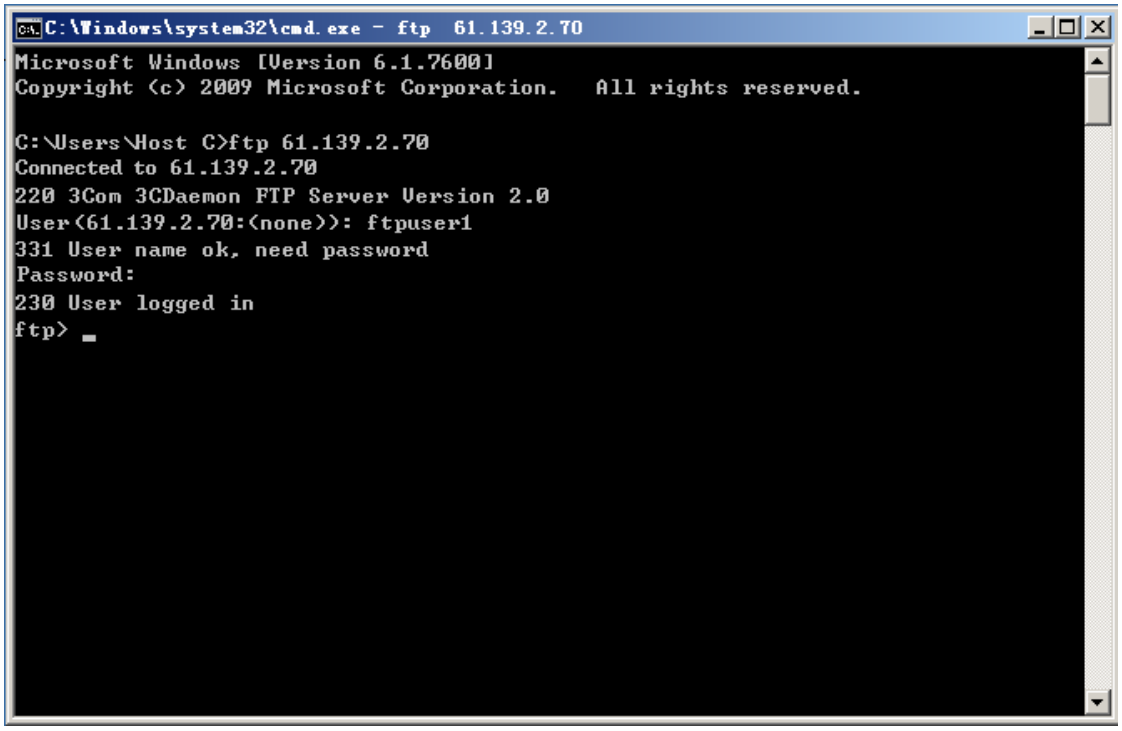
1. Verify that the internal host can access the FTP server by using the public address, as shown in Figure 5.

Figure 5 Connecting to the FTP server from the internal host



2. Verify that the external host can access the FTP server by using the public address, as shown in Figure 6.

Figure 6 Connecting to the FTP server from the external host

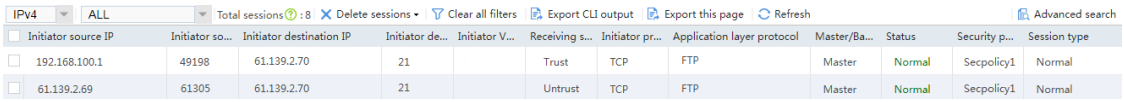


3. Verify that sessions have been created for the internal host and the external host when they access the FTP server.

   # On the top navigation bar, click **Monitor**.

   # From the navigation pane, select **Sessions**.

Figure 7 Session list



NAT flow logging configuration examples

Contents

Introduction

The following information provides NAT flow logging configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

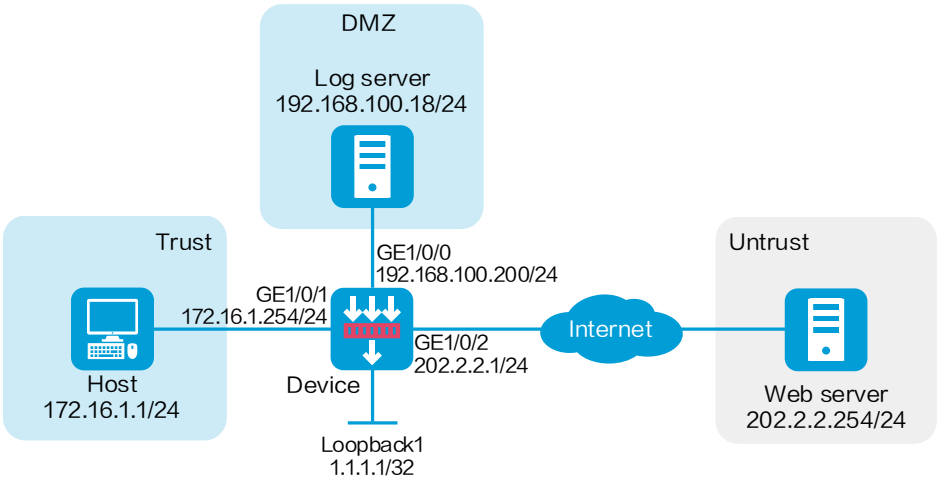
The following information is provided based on the assumption that you have basic knowledge of flow logging, NAT logging, and NAT.

Example: Configuring NAT flow logging

Network configuration

As shown in Figure 1, configure NAT flow logging on the device to enable it to send NAT session information to the log server for user tracing and analysis. The following log information is recorded when the internal host accesses the server on the public network: Source IP address, source port number, destination IP address, and destination port number before and after NAT translation.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

- To record IP address and port number after translation, use log version 3.0.
- For the NAT flow logging to take effect, you must enable NAT logging.
- Logs cannot be sent to the log host and the information center at the same time. By default, logs are sent to the log host. If the information center is specified as the log output destination, logs will not be sent to the log host.

Procedure

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/0.

In the dialog box that opens, configure the interface:

a. Select the **DMZ** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 192.168.100.200/24.

c. Click **OK**.

Add GE 1/0/1 to the **Trust** security zone and set its IP address to 172.16.1.254/24 in the same way you configure GE 1/0/0.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 202.2.2.1/24 in the same way you configure GE 1/0/0.

2. Create security policy **SecPolicy1**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create** and click **Create a policy**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **SecPolicy1**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select **IPv4** as the type.
   - Select action **Permit**.
   - Specify 172.16.1.0/24 as the source address.
   - Specify 202.2.2.0/24 as the destination address.

   # Click **OK**.

3. Create security policy **SecPolicy2**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **SecPolicy2**.
   - Select source zone **Local**.
   - Select **IPv4** as the type.

- Select destination zone **DMZ**.
- Select action **Permit**.
- Specify 192.168.100.0/24 as the destination address.

Click **OK**.

4. Configure a policy-based NAT rule.

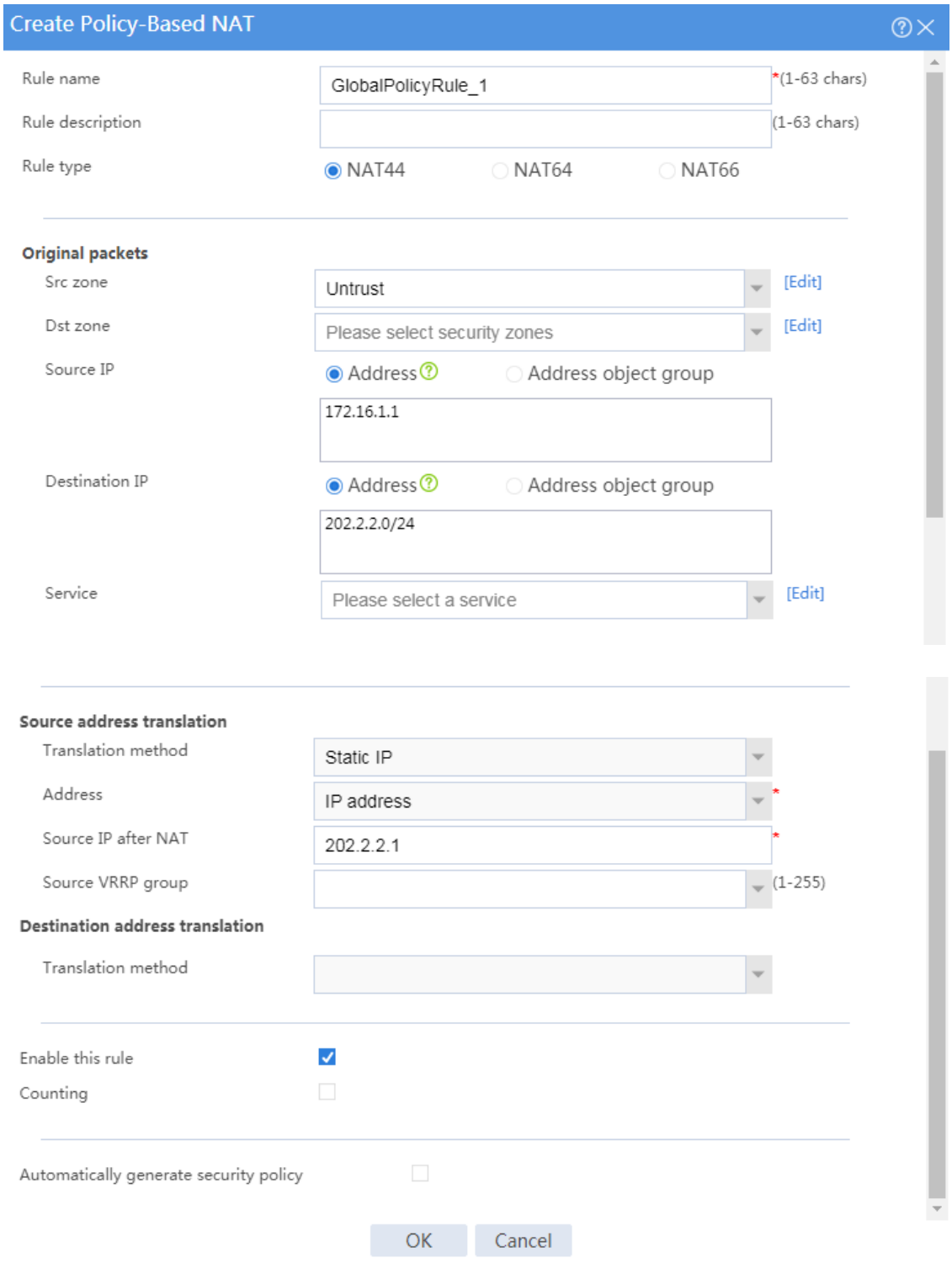
On the top navigation bar, click **Policies**.

From the navigation pane, select **Policy-based NAT**.

Click **Create**.

Create a policy-based NAT rule, as shown in Figure 2.

Figure 2 Creating a policy-based NAT rule



Click **OK**.

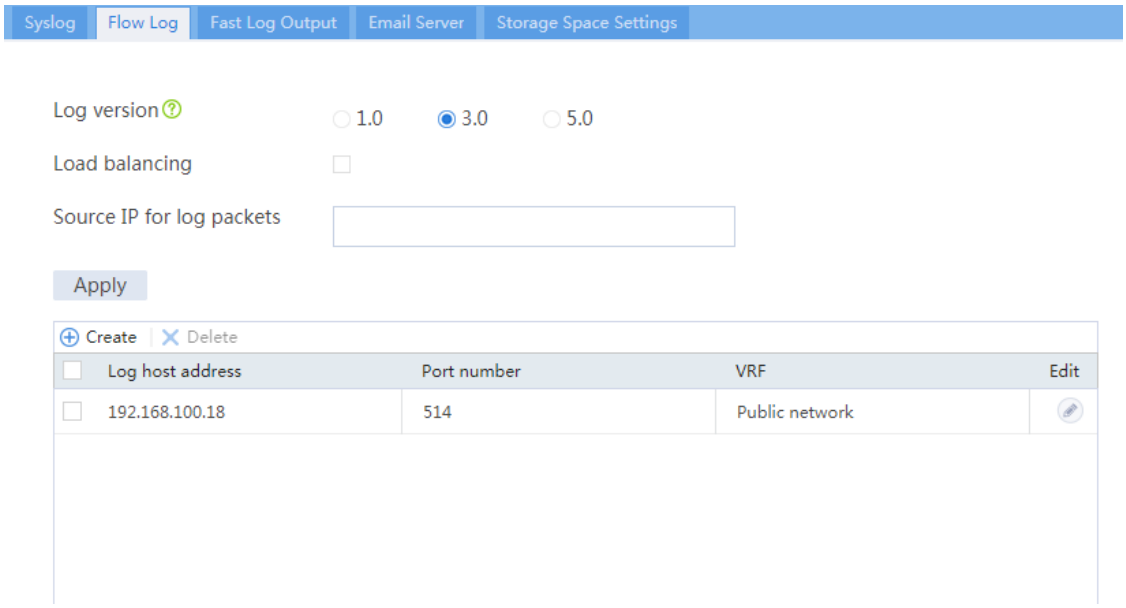
5. Configure flow logging.

On the top navigation bar, click **System**.

From the navigation pane, select **Log Settings** > **Basic Settings**.

On the **Flow Log** tab, configure flow logging, as shown in Figure 3.

Figure 3 Configure flow logging



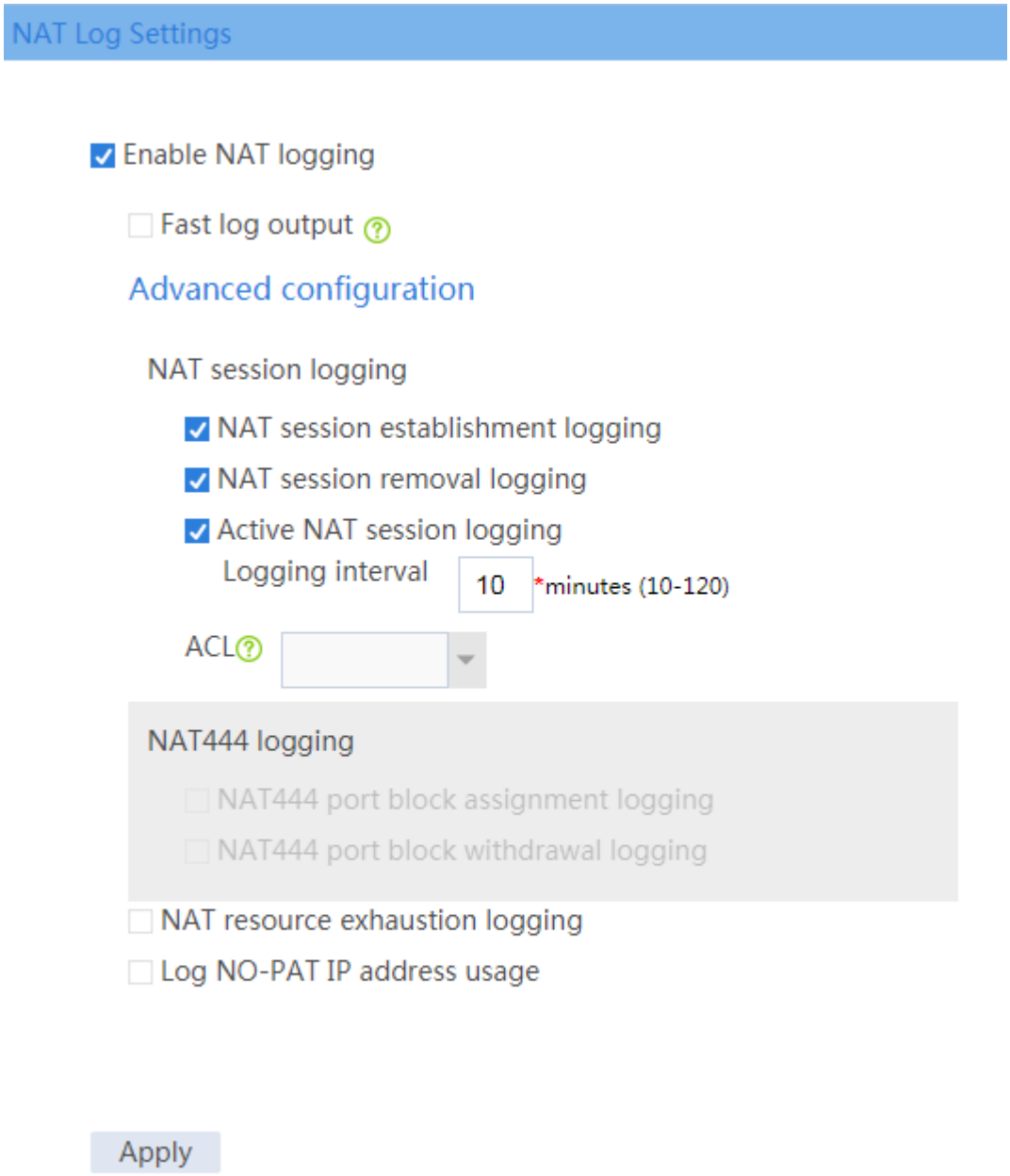
6. Configure NAT logging.

On the top navigation bar, click **System**.

From the navigation pane, select **Log Settings** > **NAT Log Settings**.

Configure NAT logging, as shown in Figure 4.

Figure 4 Configure NAT logging



Click **Apply**.

Configuring the log server

Configure the log server. (Details not shown.)

Verifying the configuration

Verify that a NAT session log is generated on the log server when the host accesses the server on the public network. The log information includes source IP address, source port number, destination IP address, and destination port number before and after translation.

Inbound link load balancing configuration examples

Contents

Introduction

The following information provides inbound link load balancing configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the inbound link load balancing feature.

Restrictions and guidelines

When you configure inbound link load balancing, follow these restrictions and guidelines:

- To ensure correct operation of inbound link load balancing when server load balancing is also enabled, do not specify the virtual server's IP address as the DNS listener's IP address.
- The virtual server's IPv4 address for inbound link load balancing must be a unicast address with a 32-bit mask length. The IPv4 address cannot be an all-zero address.
- You must contact the ISP to configure a delegating domain on the local DNS server to specify the LB device as the authoritative DNS server.

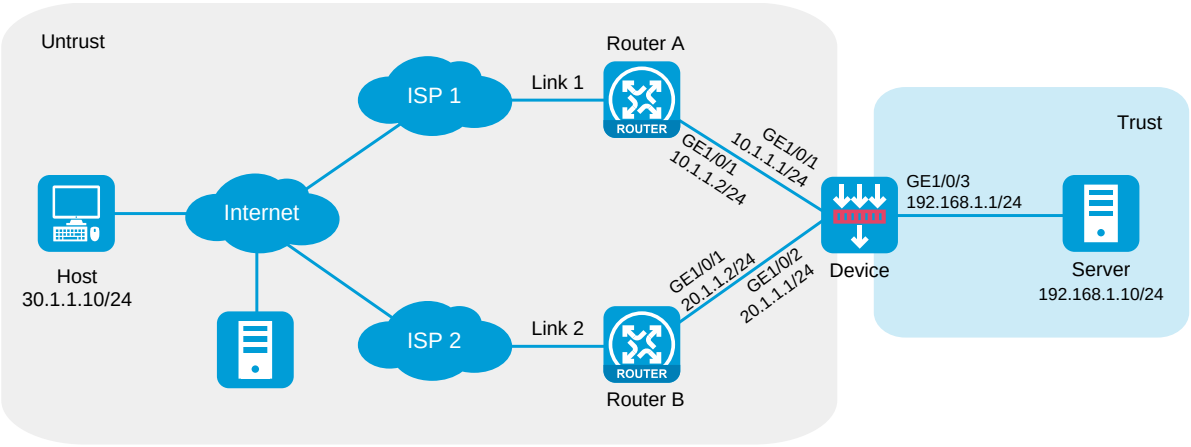
Example: Configuring inbound link load balancing

Network configuration

As shown in Figure 1, ISP 1 and ISP 2 provide an enterprise with two links, Link 1 and Link 2. Both links have the same router hop count, bandwidth, and cost.

Configure inbound link load balancing for the device to select an optimal link for traffic from the client host to the server.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedures

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click the **Network** tab.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Untrust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask length of the interface. In this example, enter 10.1.1.1/24.
   - Use the default settings for other parameters.
   - Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Trust** security zone and set its IP address to 192.168.1.1/24 in the same way you configure GE 1/0/1.

2. Configure security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy named **Untrust-to-Trust**:

- Enter policy name **Untrust-to-Trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 address **192.168.1.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

Configure a security policy named **Local-to-Untrust**:

- Enter policy name **Local-to-Untrust**.
- Select source zone **Local**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 addresses **10.1.1.0/24** and **20.1.1.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

3. Configure an ICMP probe template.

On the top navigation bar, click **Objects**.

From the navigation pane, click **Health Monitoring**.

Click **Create**.

In the dialog box that opens, configure an ICMP probe template:

a. Enter template name **t1**.

b. Select type **ICMP**.

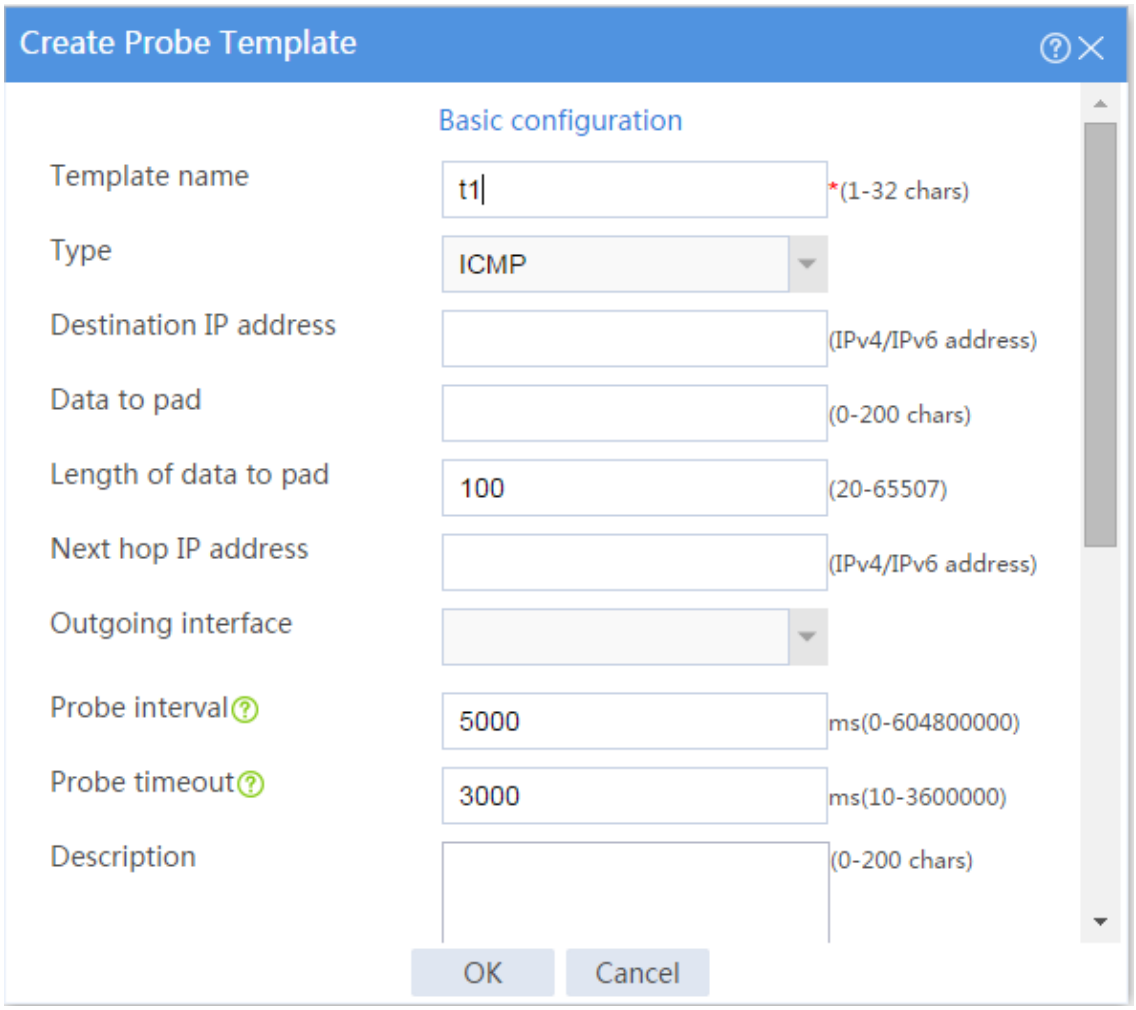
c. Enter 100 for the **Length of data to pad** field.

d. Enter 5000 for the **Probe interval** field.

e. Enter 3000 for the **Probe timeout** field.

f. Click **OK**.

Figure 2 Creating an ICMP probe template



4. Configure links.

On the top navigation bar, click **Polices**.

From the navigation pane, select **Load Balancing** > **Common Configuration** > **Links**.

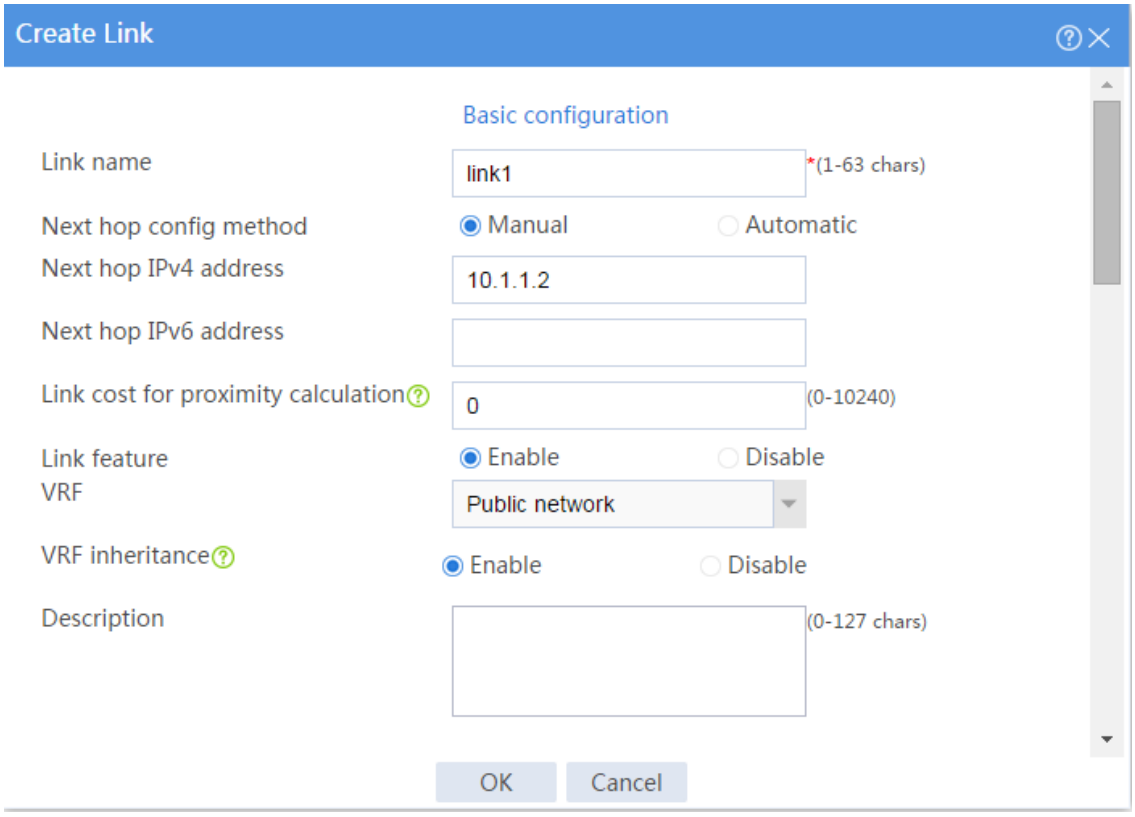
Click **Create**.

In the dialog box that opens, configure a link named **link1**:

Basic configuration:

- Enter link name **link1**.
- Select **Manual** for the **Next hop config method** field.
- Enter next hop IPv4 address 10.1.1.2.
- Enable the link feature.
- Enable VRF inheritance.

Figure 3 Creating link link1 (basic configuration)

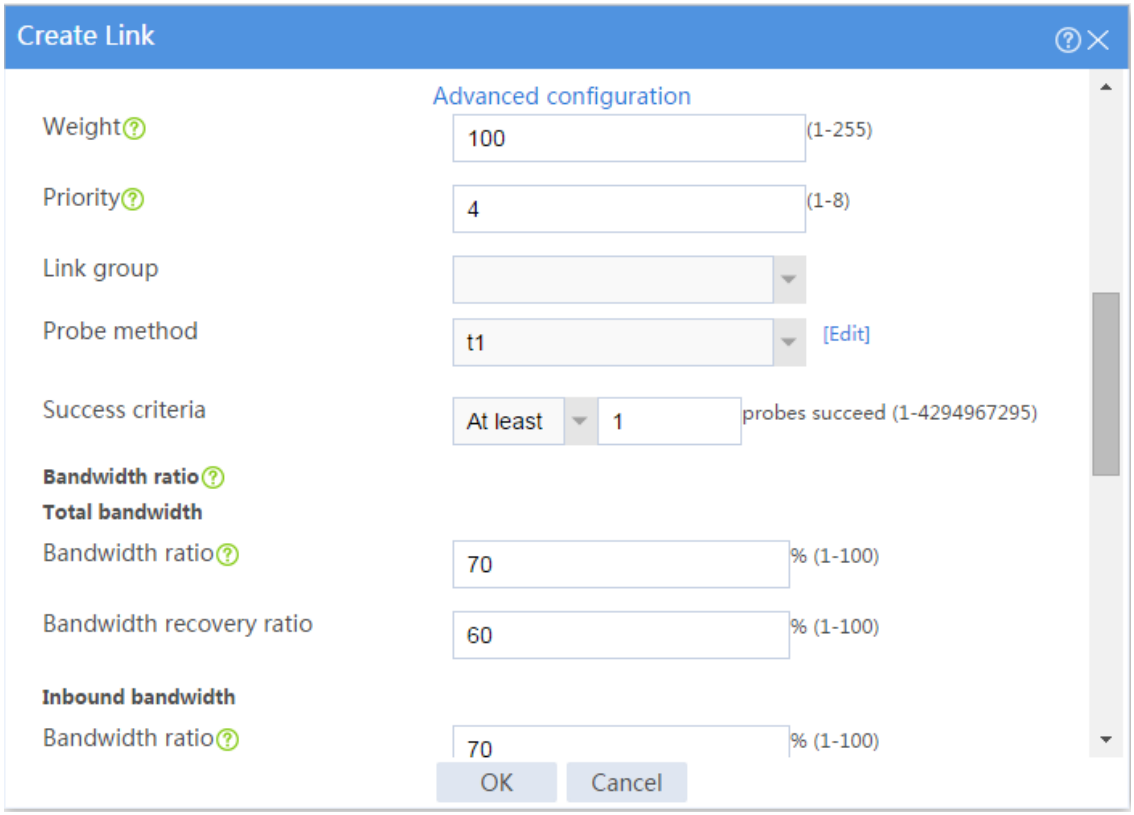


Advanced configuration:

- Enter weight 100.

- Enter priority 4.
- Select probe method **t1**.
- Set the success criteria to **At least 1**.
- Enter total bandwidth ratio 70%.
- Enter bandwidth recovery ratio 60%.
- Enter inbound bandwidth ratio 70%.
- Click **OK**.

Figure 4 Creating link link1 (advanced configuration)



Configure link **link2** in the same way you configure link **link1**.

Figure 5 Creating link link2 (basic configuration)

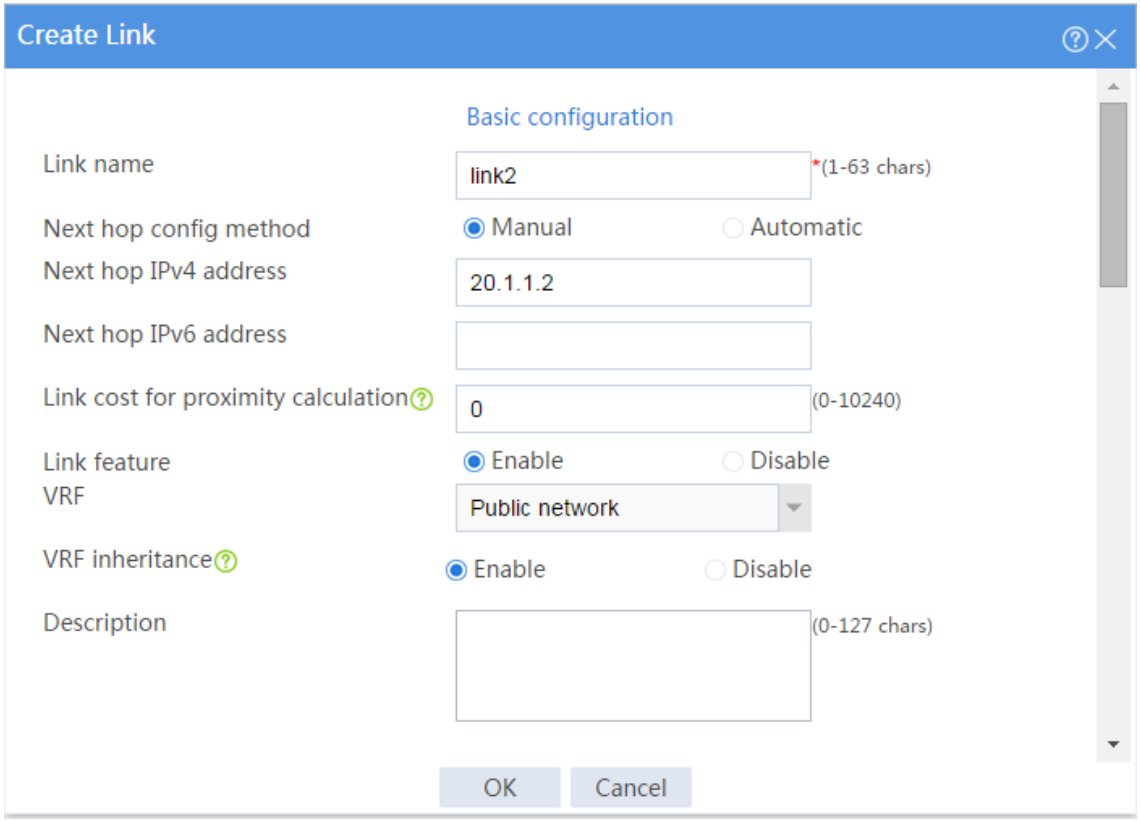
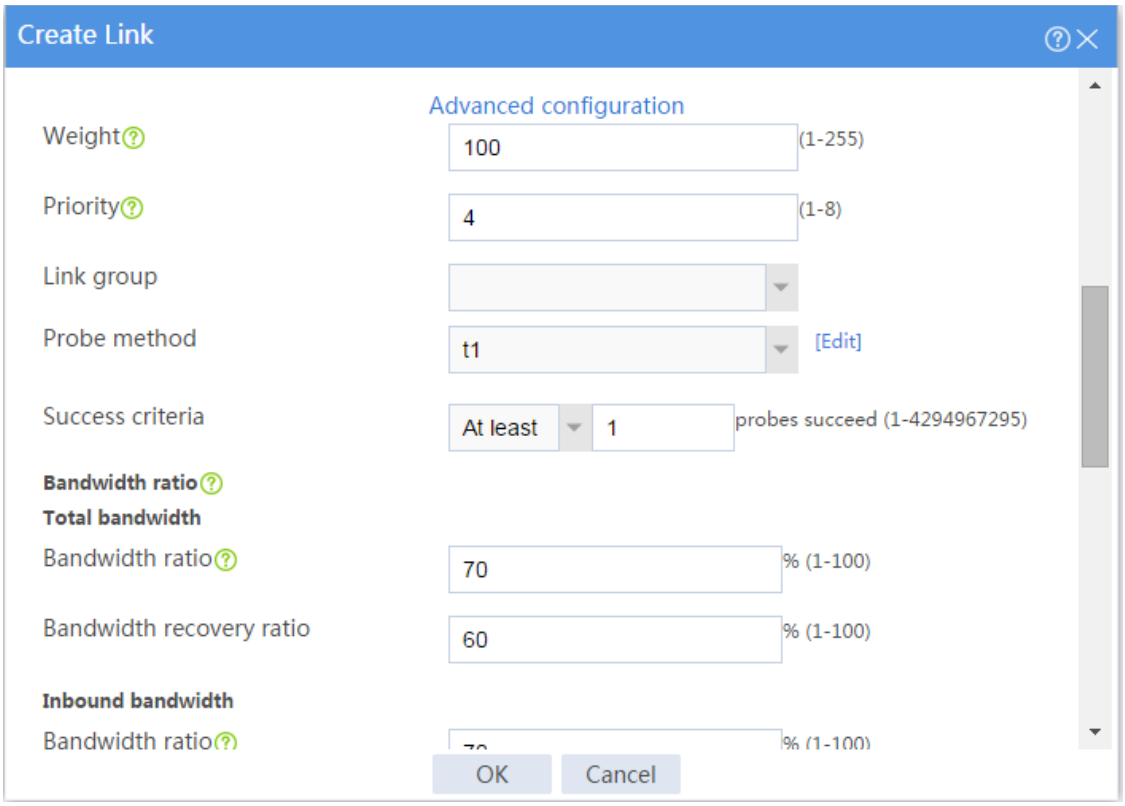


Figure 6 Creating link link2 (advanced configuration)



5. Configure a real server.

   # On the top navigation bar, click **Polices**.

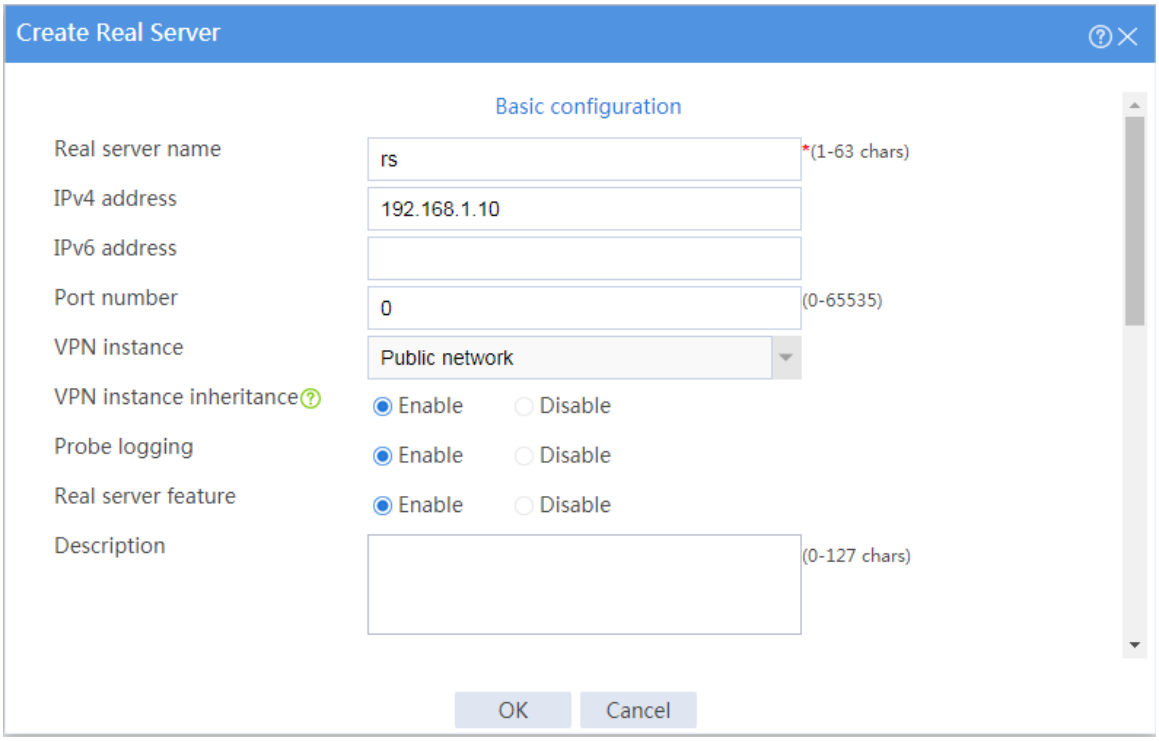
   # From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Real Servers**.

   # Click **Create**.

   # In the dialog box that opens, configure a real server named **rs**:

   - Enter server name **rs**.
   - Enter IPv4 address 192.168.1.10.
   - Enter port number 0.
   - Enable VRF inheritance.
   - Enable the real server.
   - Click **OK**.

Figure 7 Creating real server rs



6. Configure a server farm.

   # On the top navigation bar, click **Polices**.

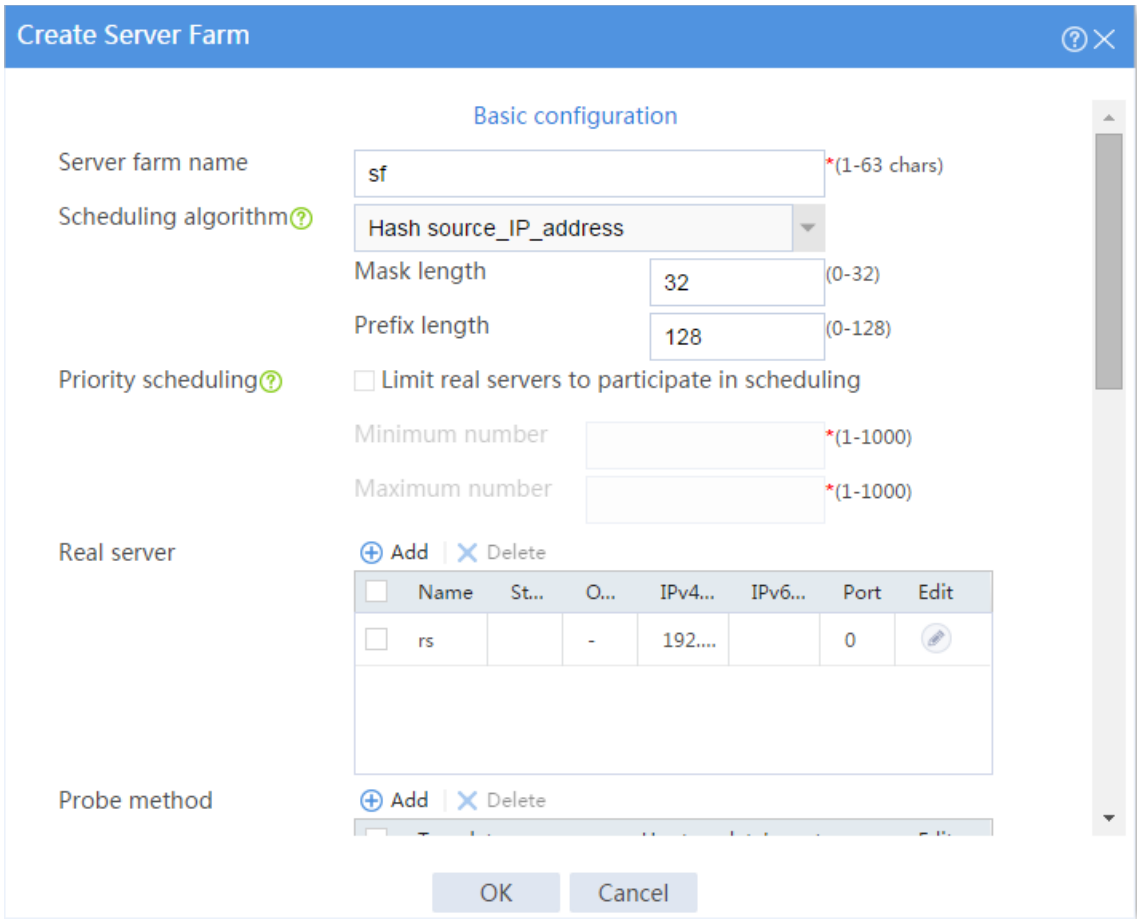
   # From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Server Farms**.

   # Click **Create**.

   # In the dialog box that opens, configure a server farm named **sf**:

   - Enter server farm name **sf**.
   - Select scheduling algorithm **Hash source_IP_address**.
   - Enter mask length 32 and prefix length 128.
   - Add real server **rs** to the server farm.
   - Select probe method **t1**.
   - Click **OK**.

Figure 8 Creating server farm sf



7. Configure virtual servers.

   # On the top navigation bar, click **Polices**.

   # From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Virtual Servers**.

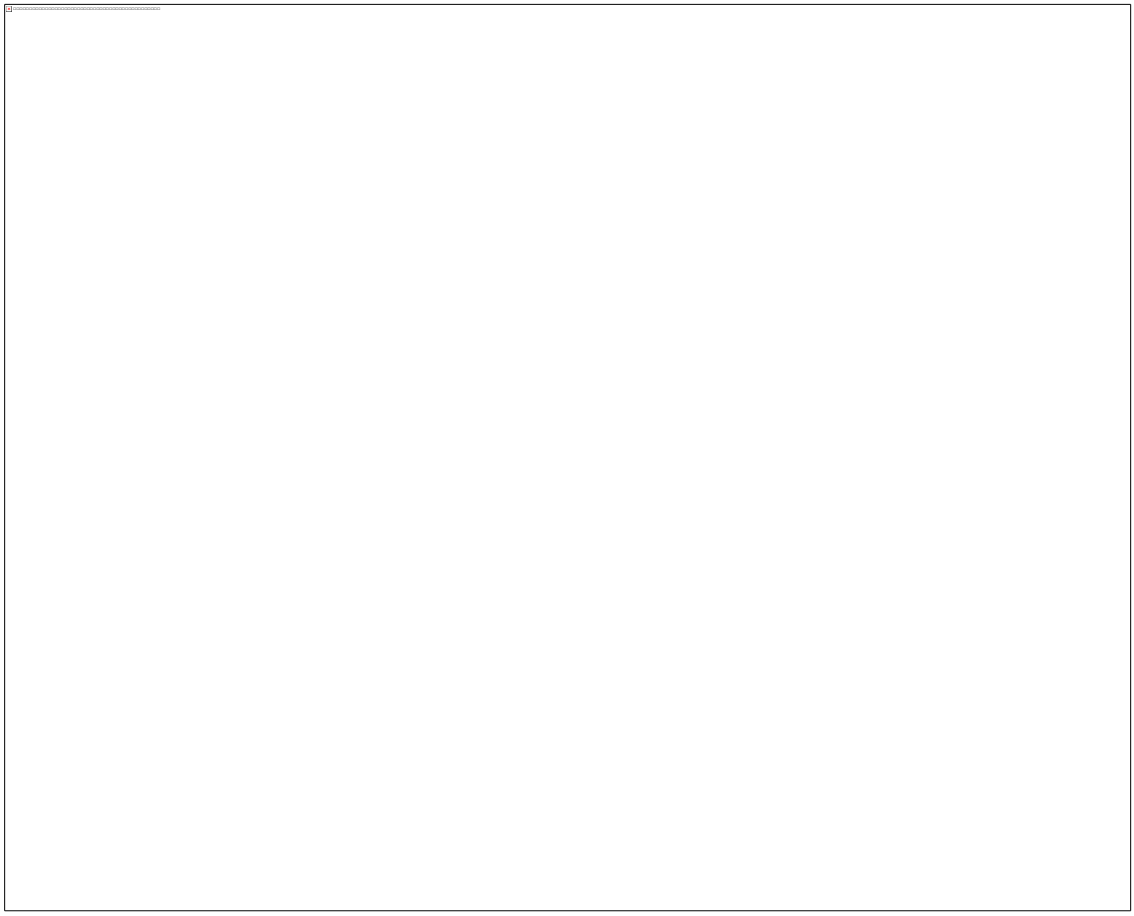
   # Click **Create**.

   # In the dialog box that opens, configure a virtual server named **vs1**:

   - Enter server name **vs1**.
   - Select type **HTTP**.
   - Enter IPv4 address 10.1.1.3.
   - Enter port number 80.
   - Select server farm **sf**.
   - Disable IP address advertisement.

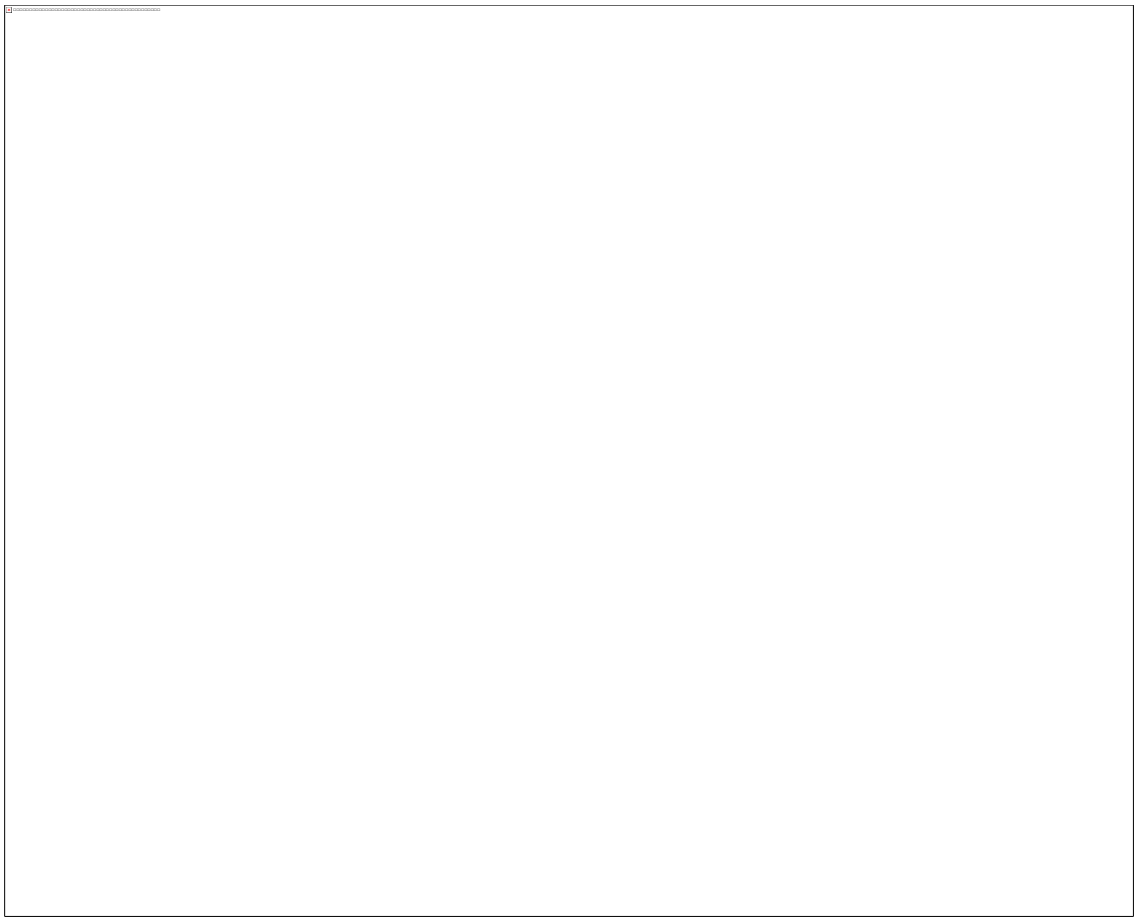
- Enable sticky entry synchronization.
- Enable the virtual server.
- Click **OK**.

Figure 9 Creating virtual server vs1



Configure virtual server **vs2** in the same way you configure virtual server **vs1**.

Figure 10 Creating virtual server vs2



8. Configure a DNS mapping.

On the top navigation bar, click **Polices**.

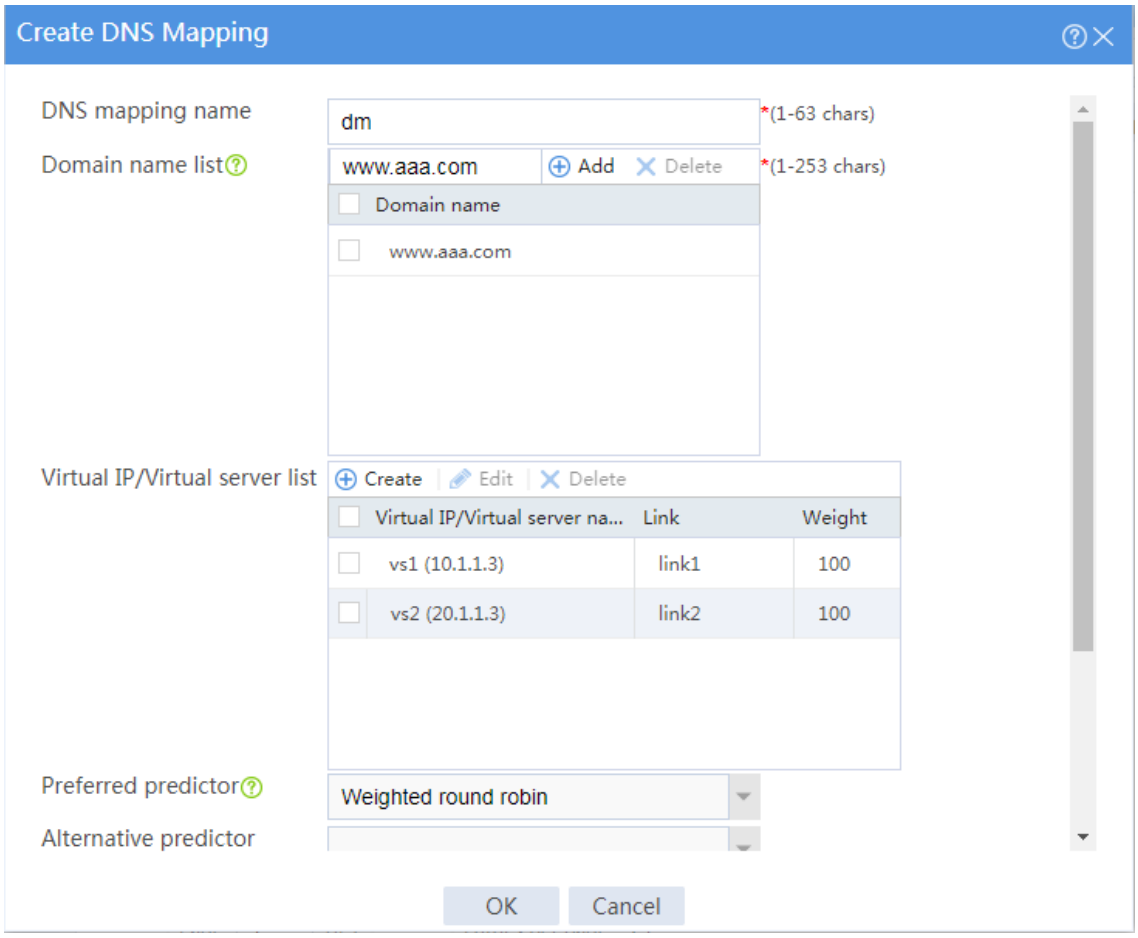
From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Inbound Link LB**.

On the **DNS Mapping** tab, click **Create**.

In the dialog box that opens, configure a DNS mapping named **dm**:

- Enter DNS mapping name **dm**.
- Select virtual IP pool **vsp**.
- Add domain name **www.aaa.com** to the domain name list.
- Set the TTL to 3600 seconds.
- Enable DNS mapping.
- Click **OK**.

Figure 11 Creating DNS mapping dm



9. Configure DNS listeners.

On the top navigation bar, click **Polices**.

From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Inbound Link LB**.

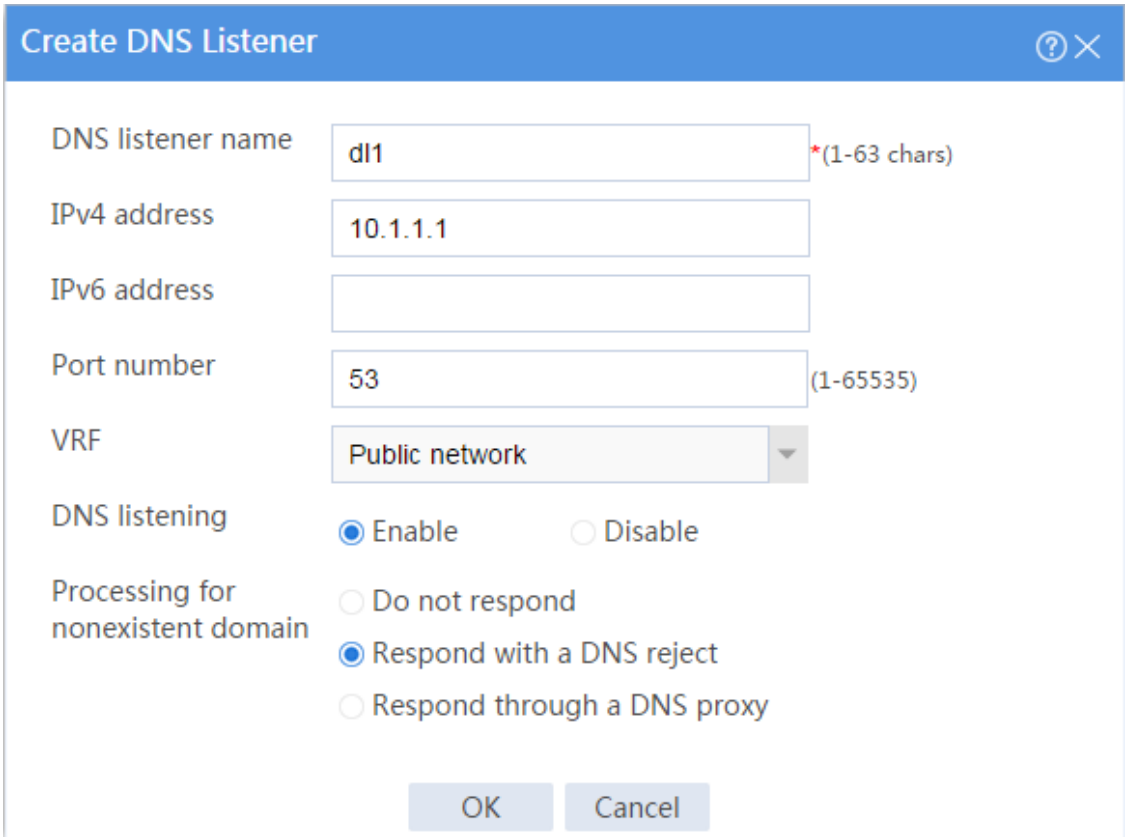
On the **DNS Listener** tab, click **Create**.

In the dialog box that opens, configure a DNS listener named **dl1**:

- Enter DNS listener name **dl1**.
- Enter IPv4 address 10.1.1.1.
- Enter port number 53.
- Enable DNS listening.

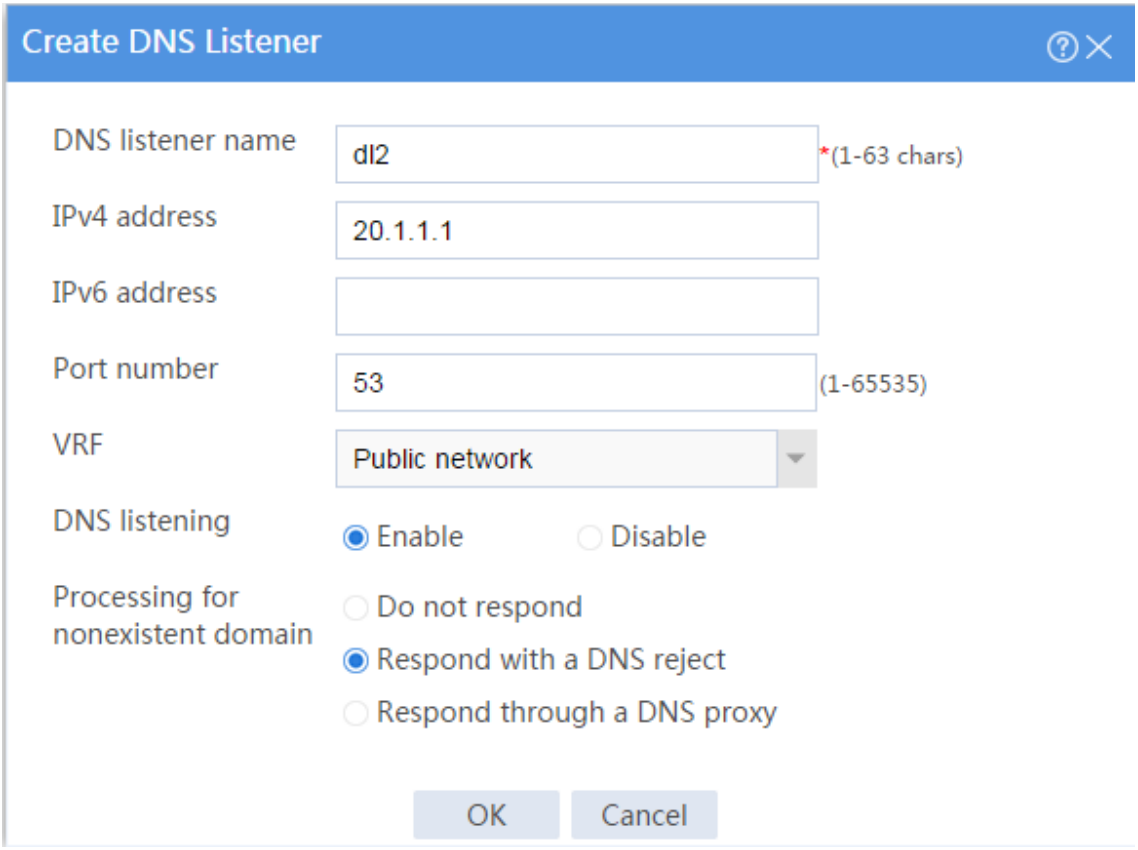
- Select **Respond with a DNS reject** for the **Processing for nonexistent domain** field.
- Click **OK**.

Figure 12 Creating DNS listener d1



Configure DNS listener **dl2** in the same way you configure DNS listener **dl1**.

Figure 13 Creating DNS listener dl2



Verifying the configuration

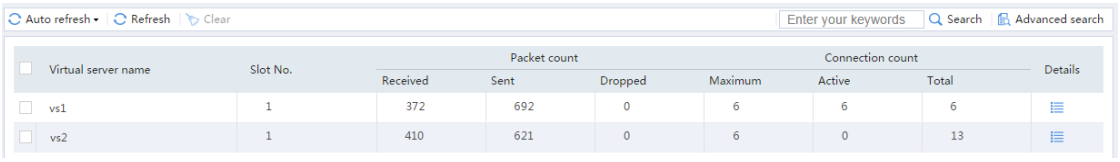
1. Access http://www.aaa.com through the browser on the host, and verify that the device distributes the HTTP requests to the links **link1** and **link2**.

   # On the top navigation bar, click the **Monitor** tab.

   # From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

   The **Virtual Server Statistics** page is as follows:

Figure 14 Virtual Server statistics



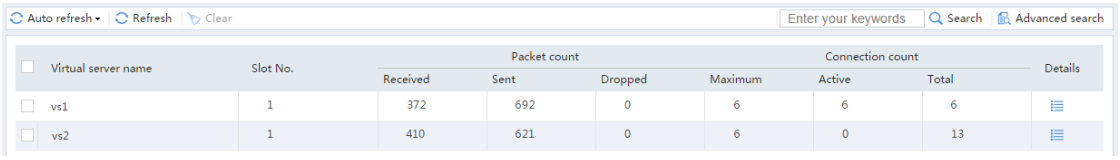
2. Disable virtual server **vs1**, access http://www.aaa.com through the browser on the host, and verify that the device distributes the HTTP requests to only link **link2**.

   # On the top navigation bar, click the **Monitor** tab.

   # From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

   The **Virtual Server Statistics** page is as follows:

Figure 15 Virtual Server statistics



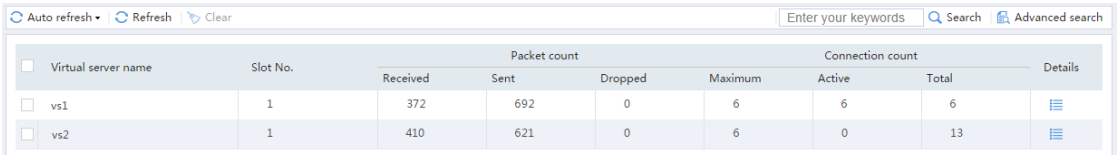
3. Disable virtual server **vs2**, access http://www.aaa.com through the browser on the host, and verify that the device distributes the HTTP requests to only link **link1**.

   # On the top navigation bar, click the **Monitor** tab.

   # From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

   The **Virtual Server Statistics** page is as follows:

Figure 16 Virtual Server statistics



Outbound link load balancing configuration examples

Contents

Introduction

The following information provides outbound link load balancing configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the outbound link load balancing feature.

Example: Configuring application-based outbound link load balancing

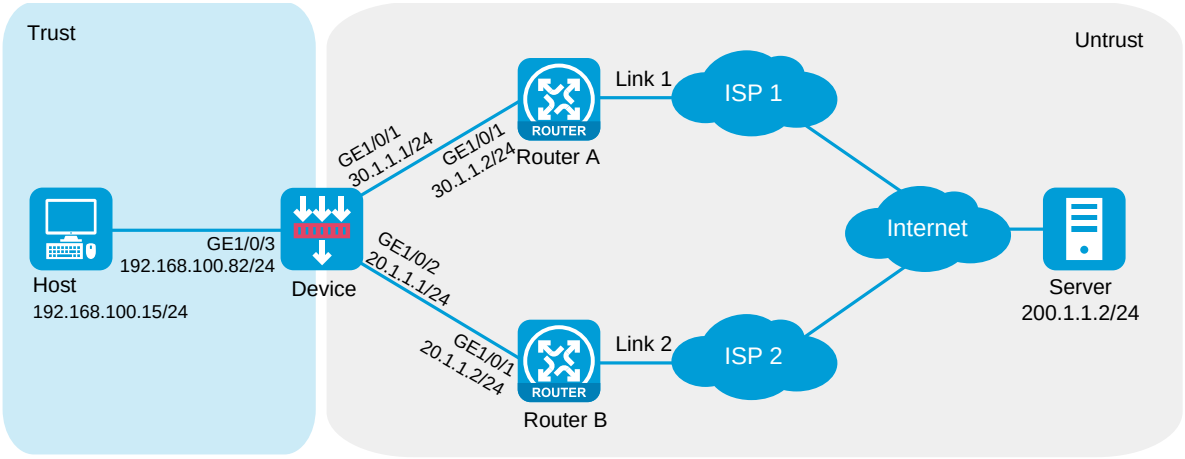
Network configuration

ISP 1 and ISP 2 provide an enterprise with two links, Link 1 and Link 2. Both links have the same router hop count, bandwidth, and cost.

Configure outbound link load balancing to meet the following requirements:

- The traffic for SoHu video application is distributed to link **Link1**.
- The traffic for all other application is distributed to link **Link2**.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedures

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click the **Network** tab.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Untrust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask length of the interface. In this example, enter 30.1.1.1/24.
   - Use the default settings for other parameters.
   - Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

   # Add GE 1/0/3 to the **Trust** security zone and set its IP address to 192.168.100.82/24 in the same way you configure GE 1/0/1.

2. Configure security policies.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy named **Trust-to-Untrust**:

   - Enter policy name **Trust-to-Untrust**.
   - Select source zone **Trust**.

- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter source IPv4 address **192.168.100.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

Configure a security policy named **Local-to-Untrust**:

- Enter policy name **Local-to-Untrust**.
- Select source zone **Local**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 addresses **20.1.1.0/24** and **30.1.1.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

3. Configure an ICMP probe template.

On the top navigation bar, click **Objects**.

From the navigation pane, click **Health Monitoring**.

Click **Create**.

In the dialog box that opens, configure an ICMP probe template:

a. Enter template name **t1**.

b. Select type **ICMP**.

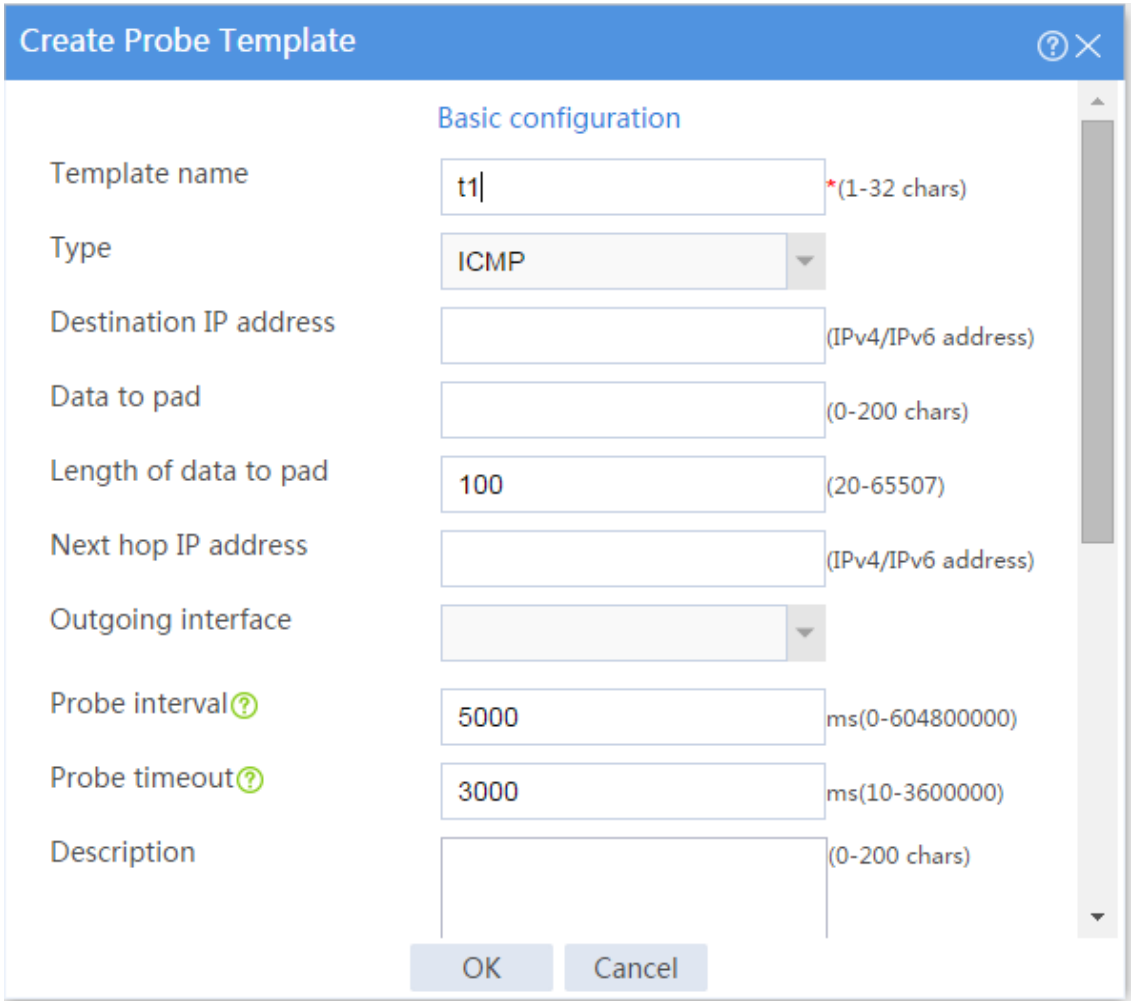
c. Enter 100 for the **Length of data to pad** field.

d. Enter 5000 for the **Probe interval** field.

e. Enter 3000 for the **Probe timeout** field.

f. Click **OK**.

Figure 2 Creating probe template t1



4. Configure an application group.

   # On the top navigation bar, click **Objects**.

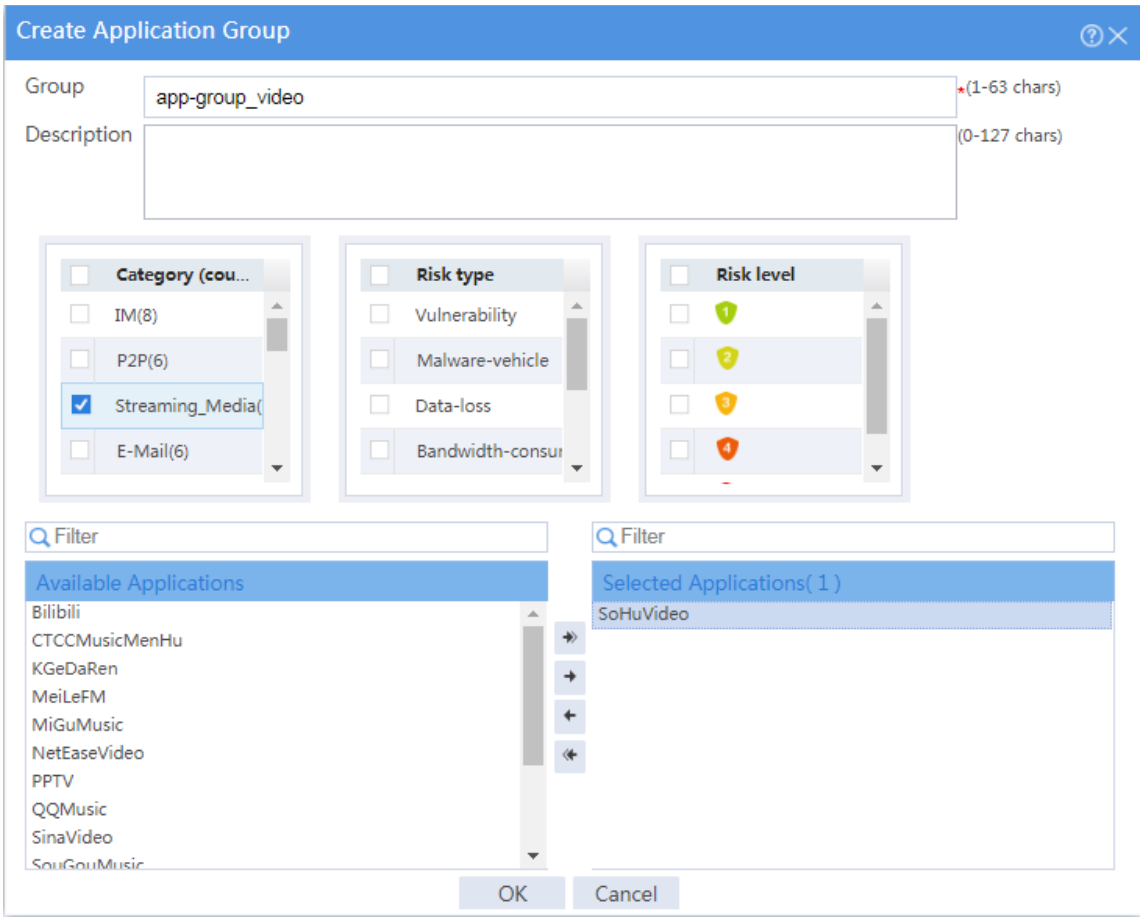
   # From the navigation pane, select **APPSecurity** > **APP Recognition** > **Application Groups**.

   # Click **Create**.

   # In the dialog box that opens, configure an application group named **app-group_video**:

   - Enter group name **app-group_video**.
   - Add application **SoHuVideo** in the **Streaming_Media** category to the **Selected Applications** pane.
   - Click **OK**.

Figure 3 Creating an application group



5. Configure links.

On the top navigation bar, click **Polices**.

From the navigation pane, select **Load Balancing** > **Common Configuration** > **Links**.

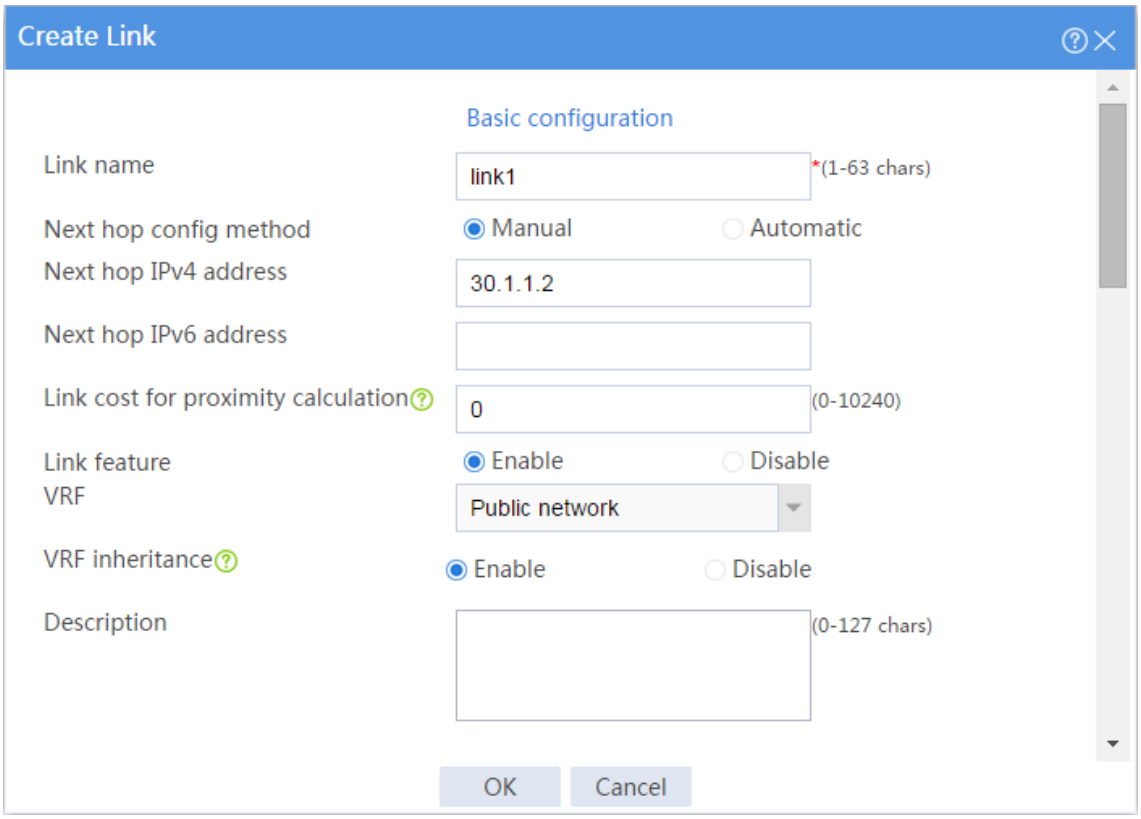
Click **Create**.

In the dialog box that opens, configure a link named **link1**:

- Enter link name **link1**.
- Select **Manual** for the **Next hop config method** field.
- Enter next hop IPv4 address 30.1.1.2.
- Set the link cost for proximity calculation to 0.
- Enable the link feature.
- Enable VRF inheritance.

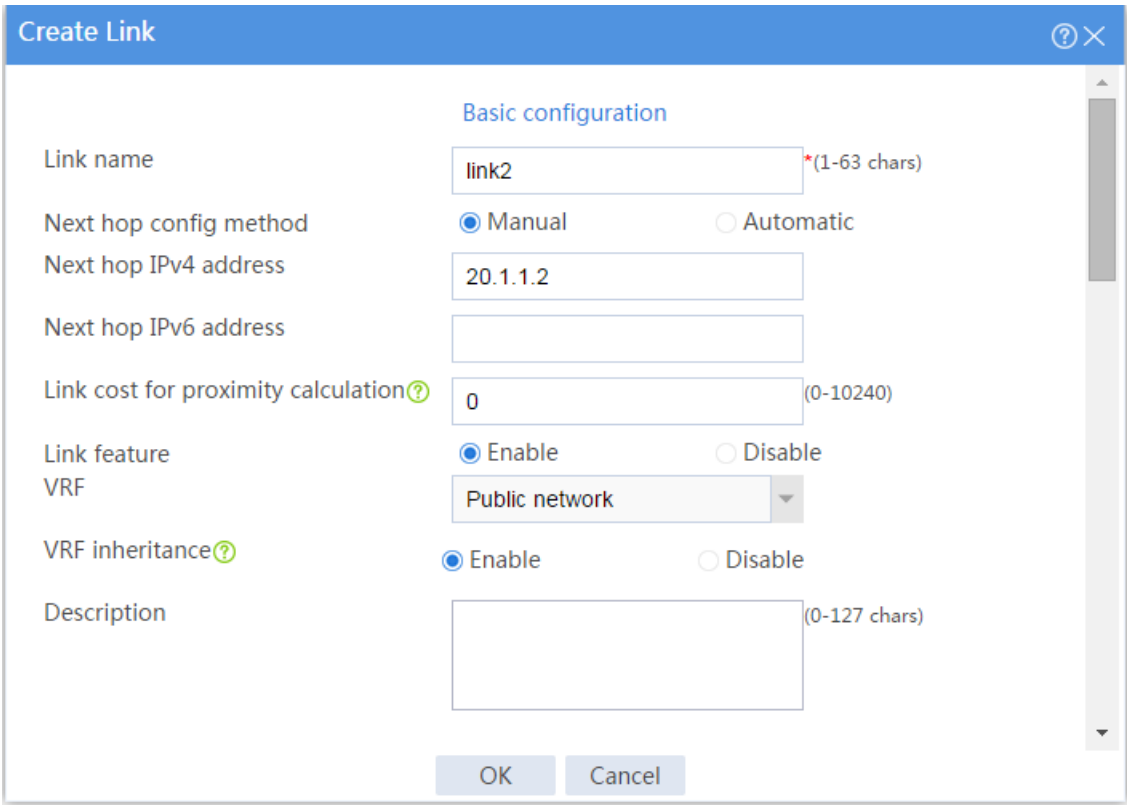
- Click **OK**.

Figure 4 Creating link link1



Configure link **link2** in the same way you configure link **link1**.

Figure 5 Creating link link2



6. Configure link groups.

   # On the top navigation bar, click **Polices**.

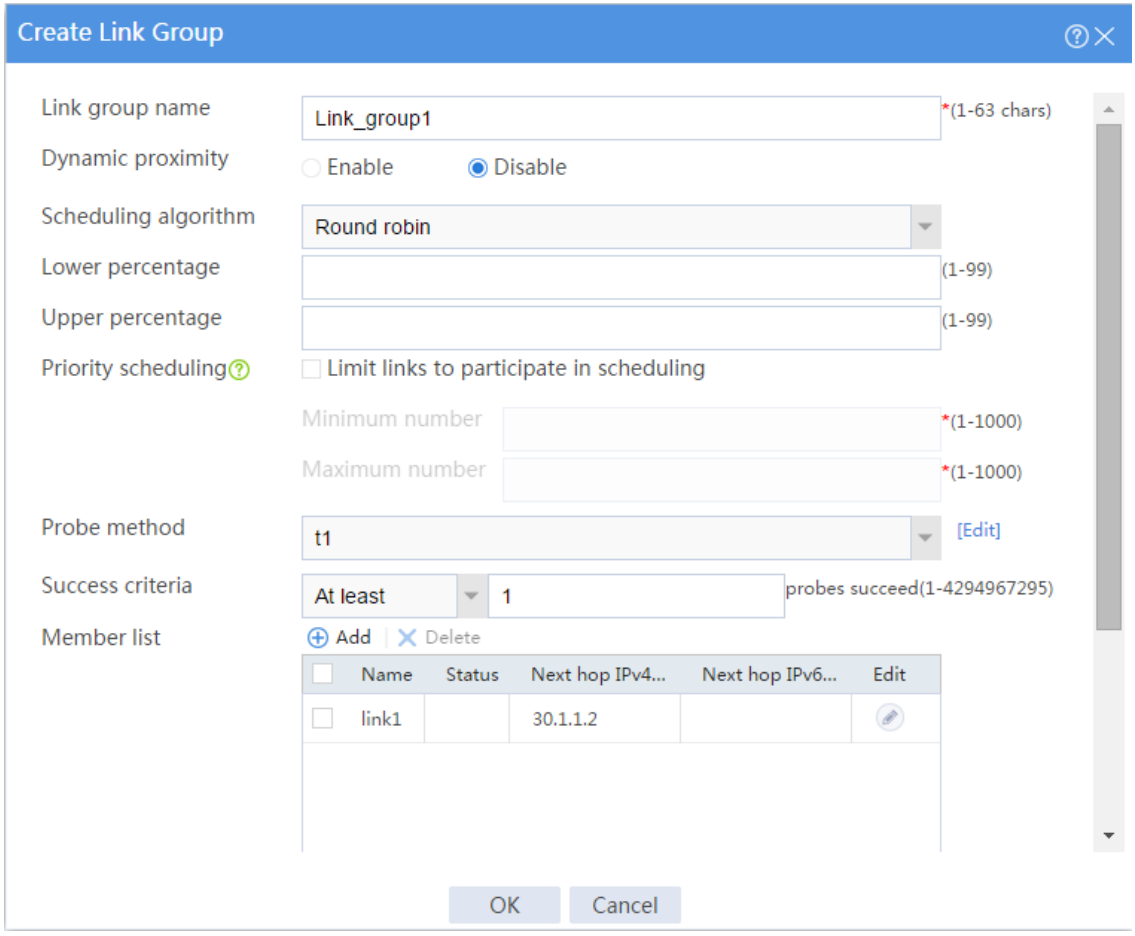
   # From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Outbound Link LB**.

   # On the **Link Group** tab, click **Create**.

   # In the dialog box that opens, configure a link group named **Link_group1**:

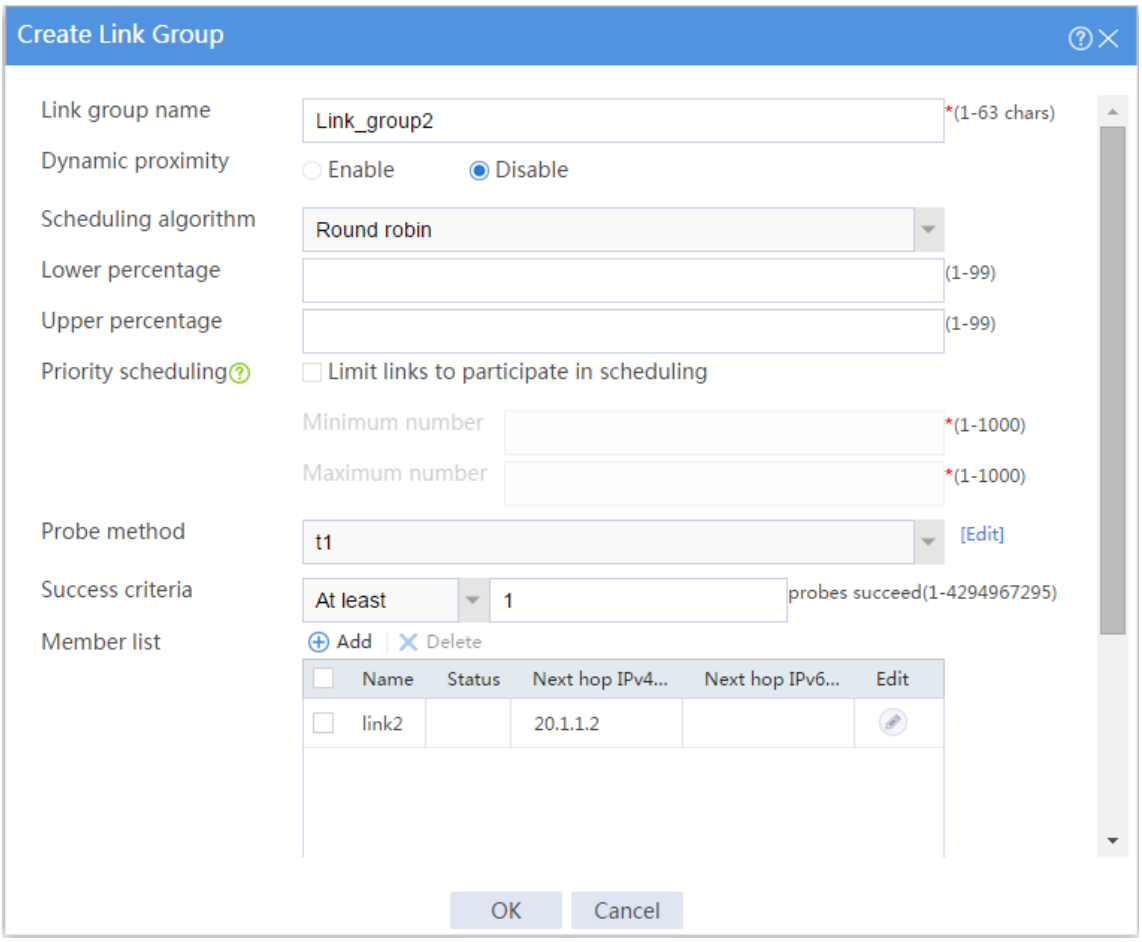
   - Enter link group name **Link_group1**.
   - Disable dynamic proximity.
   - Select scheduling algorithm **Round robin**.
   - Select probe method **t1**.
   - Set the success criteria to **At least 1**.
   - Add link **link1** to the link group.
   - Click **OK**.

Figure 6 Creating link group Link_group1



Configure link group **Link_group2** in the same way you configure link group **Link_group1**.

Figure 7 Creating link group Link_group2



7. Configure a class.

On the top navigation bar, click **Polices**.

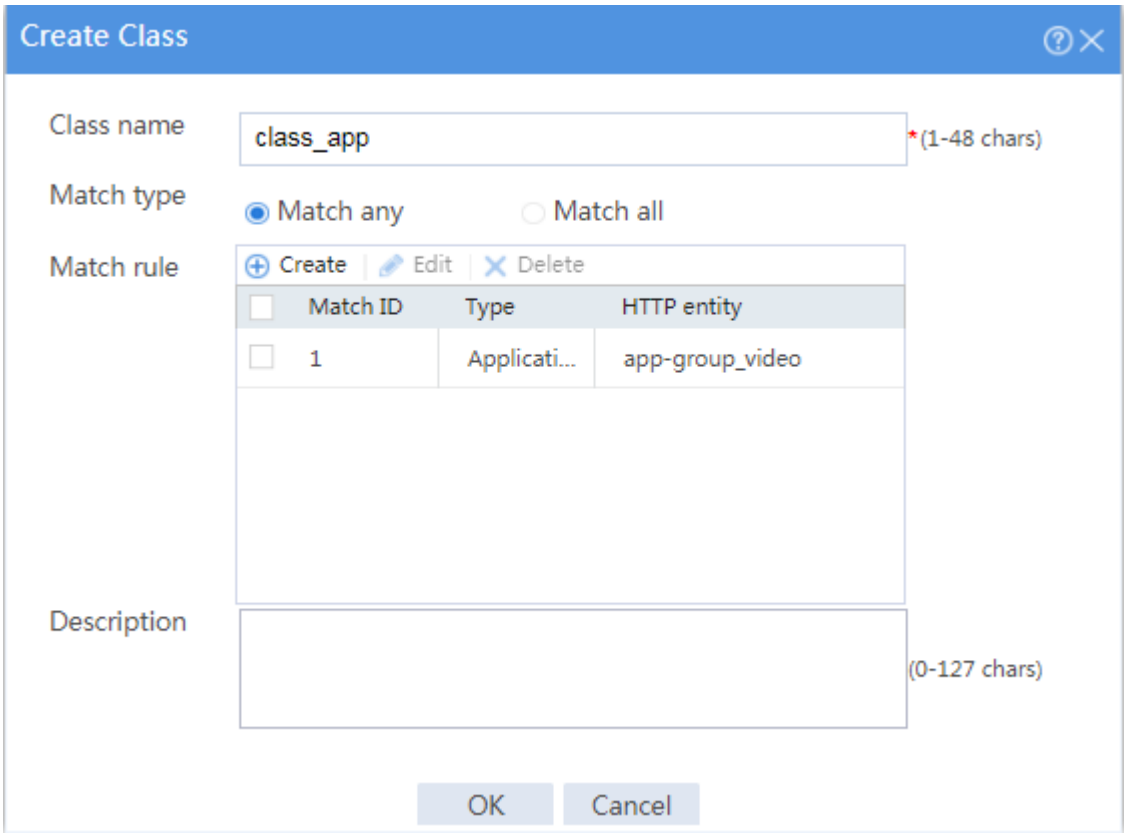
From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Outbound Link LB**.

On the **Class** tab, click **Create**.

In the dialog box that opens, configure a class named **class_app**:

- Enter class name **class_app**.
- Select **Match any** for the **Match type** field.
- Add application group **app-group_video** as a match rule.
- Click **OK**.

Figure 8 Creating class class_app



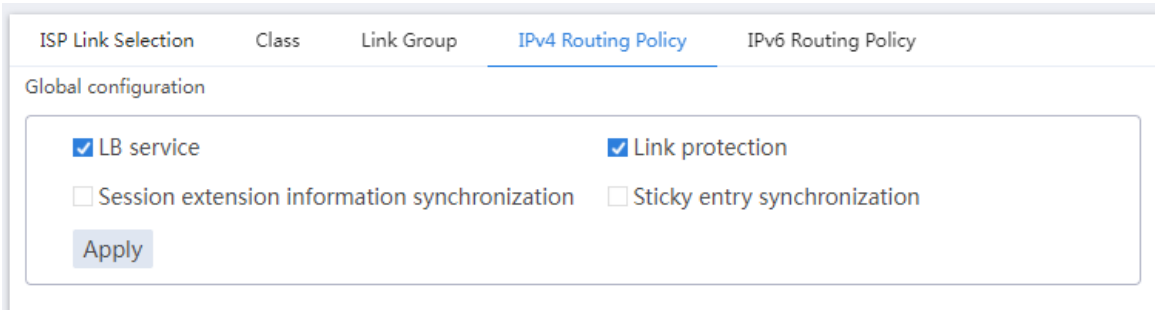
8. Configure IPv4 routing policies.

   # On the top navigation bar, click **Polices**.

   # From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Outbound Link LB**.

   # In the **Global configuration** area on the **IPv4 Routing Policy** tab, enable **LB service** and **Link protection**.

Figure 9 Global configuration

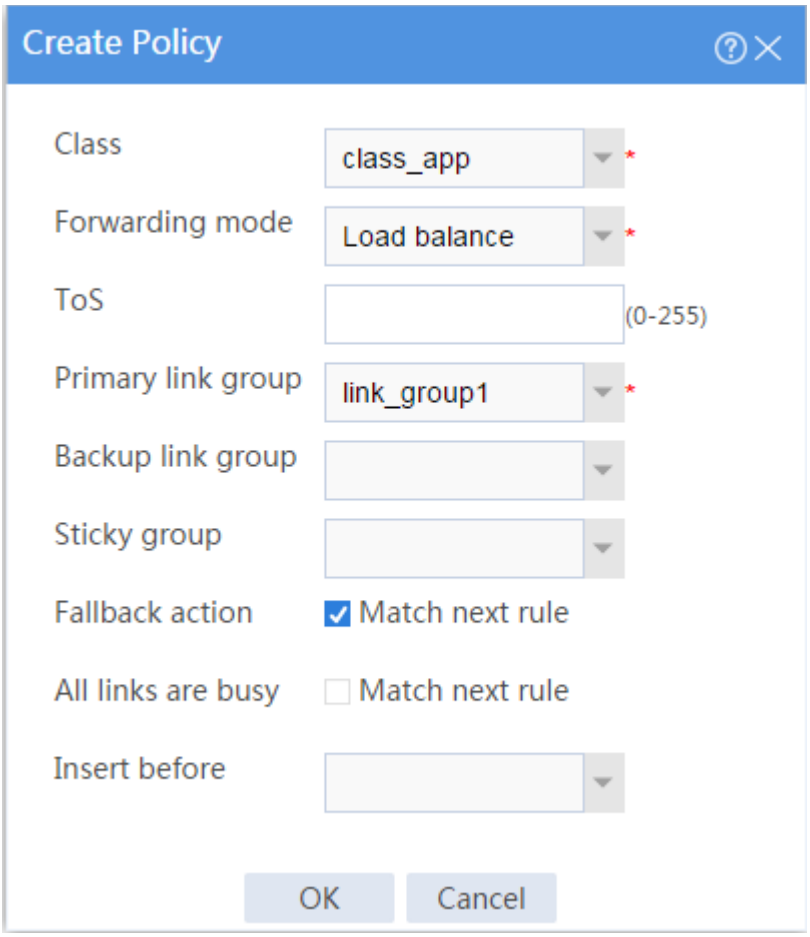


In the **Policy** area on the **IPv4 Routing Policy** tab, click **Create**.

In the dialog box that opens, configure an IPv4 routing policy:

- Select name **class-app**.
- Select forwarding mode **Load balance**.
- Select primary link group **link_group1**.
- Select **Match next rule** for the **Fallback action** field.
- Click **OK**.

Figure 10 Creating class class-app

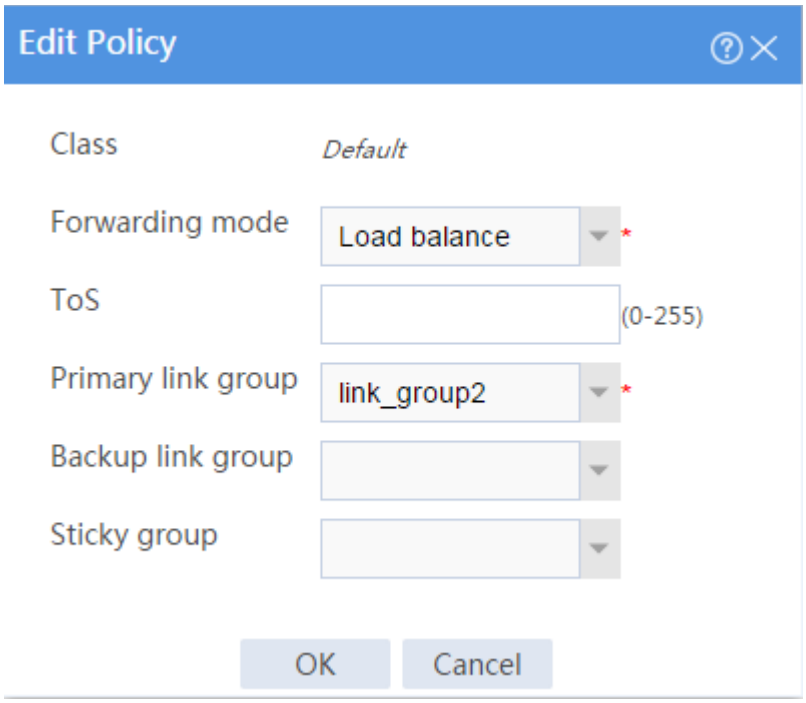


In the **Policy** area on the **IPv4 Routing Policy** tab, click the **Edit** icon for the default IPv4 routing policy named ***Default***.

In the dialog box that opens, configure the default IPv4 routing policy:

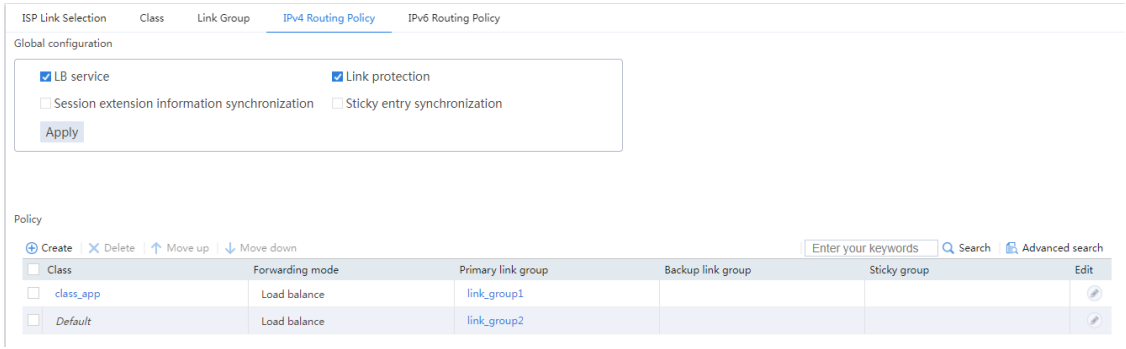
- Select forwarding mode **Load balance**.
- Select primary link group **link_group2**.
- Click **OK**.

Figure 11 Editing the default IPv4 routing policy



The IPv4 routing policy configuration is as follows:

Figure 12 IPv4 routing policy configuration



Verifying the configuration

1. Open the Sohu video client, and select a movie to play.

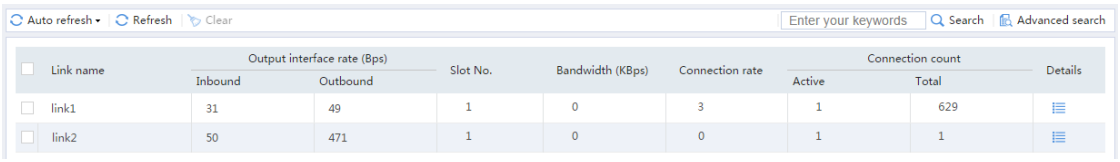
2. Verify that the traffic for the Sohu video client is transmitted over link **link1**:

   # On the top navigation bar, click the **Monitor** tab.

   # From the navigation pane, select **Statistics** > **Outbound Link LB Statistics** > **Links**.

   The **Link Statistics** page is as follows:

Figure 13 Link statistics



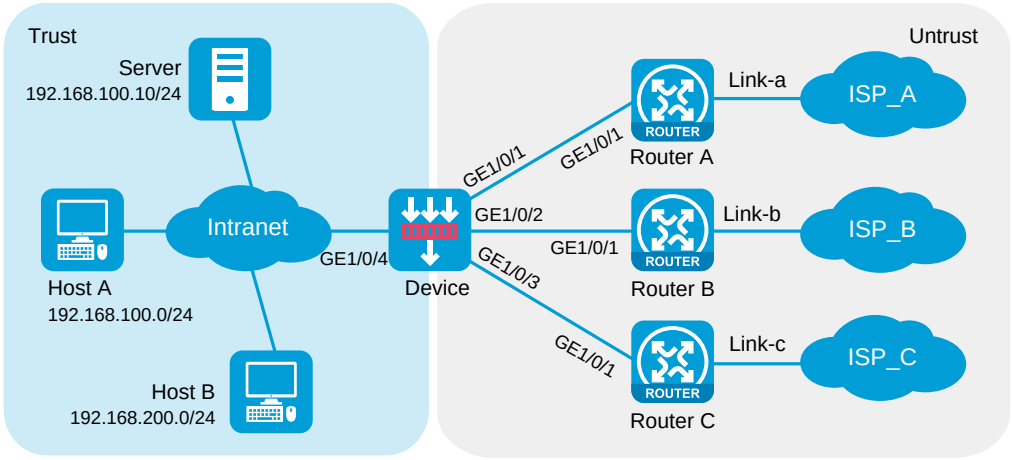
Example: Configuring ISP-based outbound link load balancing

Network configuration

As shown in Figure 14, an enterprise accesses the external servers through ISP links **Link_a**, **Link_b**, and **Link_c** provided by ISP_A, ISP_B, and ISP_C, respectively. Configure outbound link load balancing to meet the following requirements:

- The LB device distributes outbound traffic to external servers matching ISP_A, ISP_B, and ISP_C through **Link_a**, **Link_b**, and **Link_c**, respectively.
- Host B (with IP address 192.168.200.0/24 in the finance department) needs to access online payment services. To avoid frequent egress IP address changes, the LB device distributes finance data traffic through **Link_a**. When the bandwidth usage on **Link_a** exceeds, the LB device distributes consequent traffic to **Link_b**.

Figure 14 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device	GE1/0/1	30.1.1.1/24	Router A	GE1/0/1	30.1.1.2/24
Device	GE1/0/2	20.1.1.1/24	Router B	GE1/0/1	20.1.1.2/24
Device	GE1/0/3	10.1.1.124	Router C	GE1/0/1	10.1.1.2/24
Device	GE1/0/4	192.168.100.82/24			

Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedures

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click the **Network** tab.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

- Select the **Untrust** security zone.
- On the **IPv4 Address** tab, enter the IP address and mask length of the interface. In this example, enter 30.1.1.1/24.
- Use the default settings for other parameters.
- Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1./24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Untrust** security zone and set its IP address to 10.1.1.1/24 in the same way you configure GE 1/0/1.

Add GE 1/0/4 to the **Trust** security zone and set its IP address to 192.168.100.82/24 in the same way you configure GE 1/0/1.

2. Configure routes:

This section uses static routes as an example. You can also configure a dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv4 static route with next hop IP address **30.1.1.2**:

- Enter destination IP address **0.0.0.0**.
- Enter mask length **0**.
- Enter next hop IP address **30.1.1.2**.
- Use the default settings for other parameters.
- Click **OK**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv4 static route with next hop IP address **20.1.1.2**:

- Enter destination IP address **0.0.0.0**.
- Enter mask length **0**.
- Enter next hop IP address **20.1.1.2**.
- Use the default settings for other parameters.
- Click **OK**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv4 static route with next hop IP address **10.1.1.2**:

- Enter destination IP address **0.0.0.0**.
- Enter mask length **0**.
- Enter next hop IP address **10.1.1.2**.
- Use the default settings for other parameters.
- Click **OK**.

3. Configure security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy named **Trust-to-Untrust**:

- Enter policy name **Trust-to-Untrust**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter source IPv4 addresses **192.168.100.0/24** and **192.168.200.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

Configure a security policy named **Local-to-Untrust**:

- Enter policy name **Local-to-Untrust**.
- Select source zone **Local**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 addresses **10.1.1.0/24**, **20.1.1.0/24**, and **30.1.1.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

4. Configure ICMP probe templates.

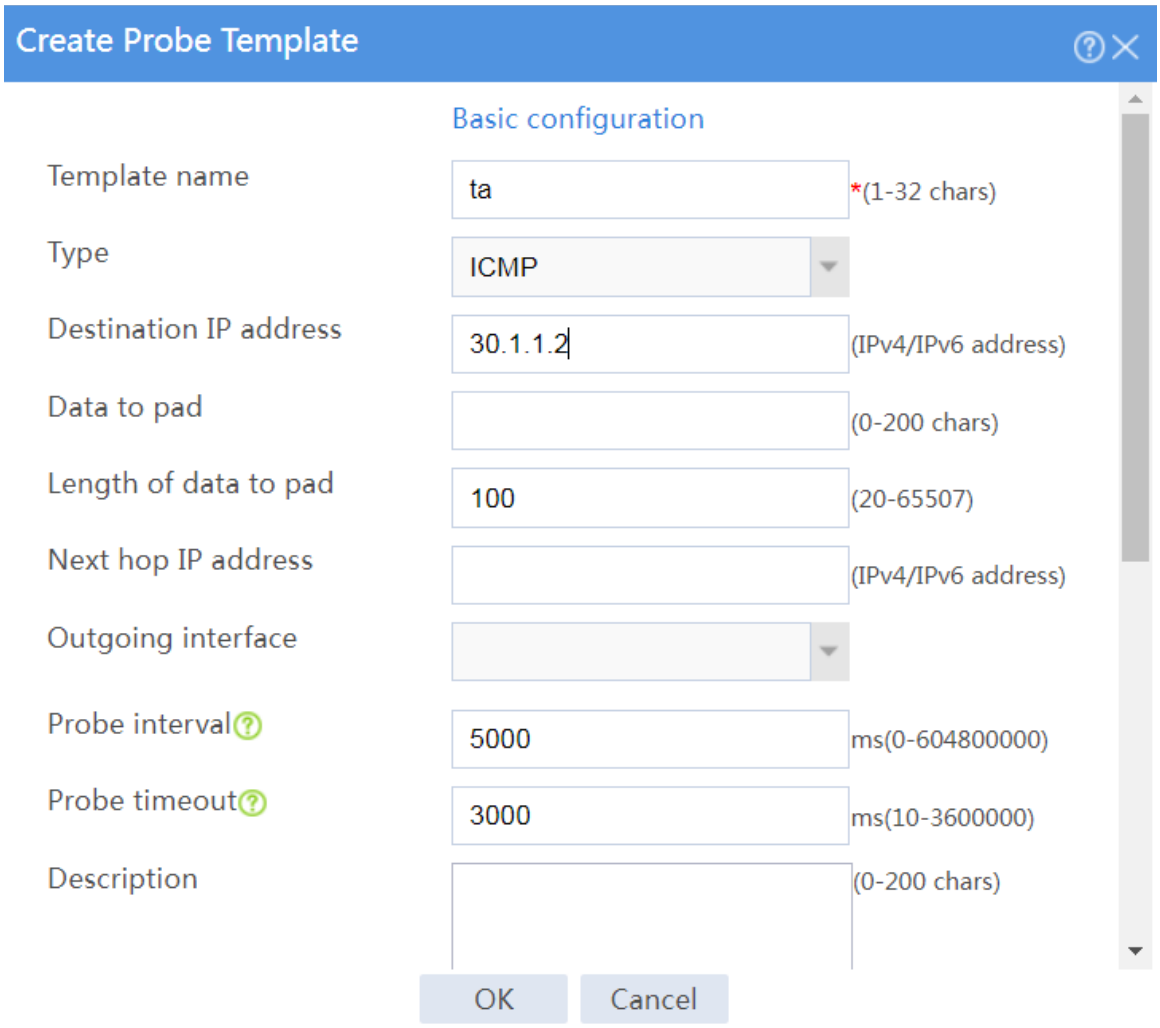
On the top navigation bar, click **Objects**.

From the navigation pane, click **Health Monitoring**.

Click **Create**.

In the dialog box that opens, configure an ICMP probe template named **ta**, as shown in Figure 15.

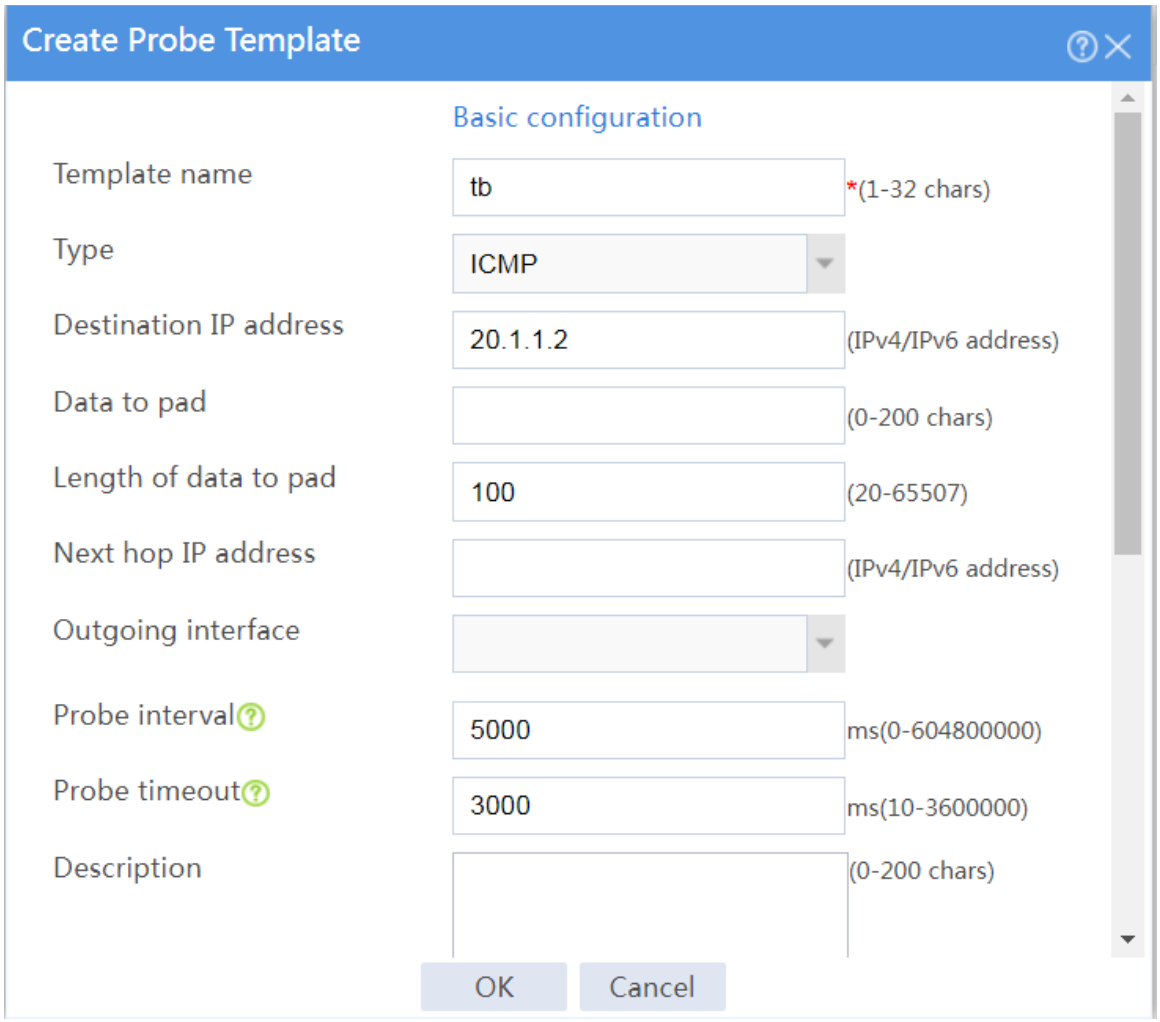
Figure 15 Creating probe template ta



Click **OK**.

Configure an ICMP probe template named **tb**, as shown in Figure 16.

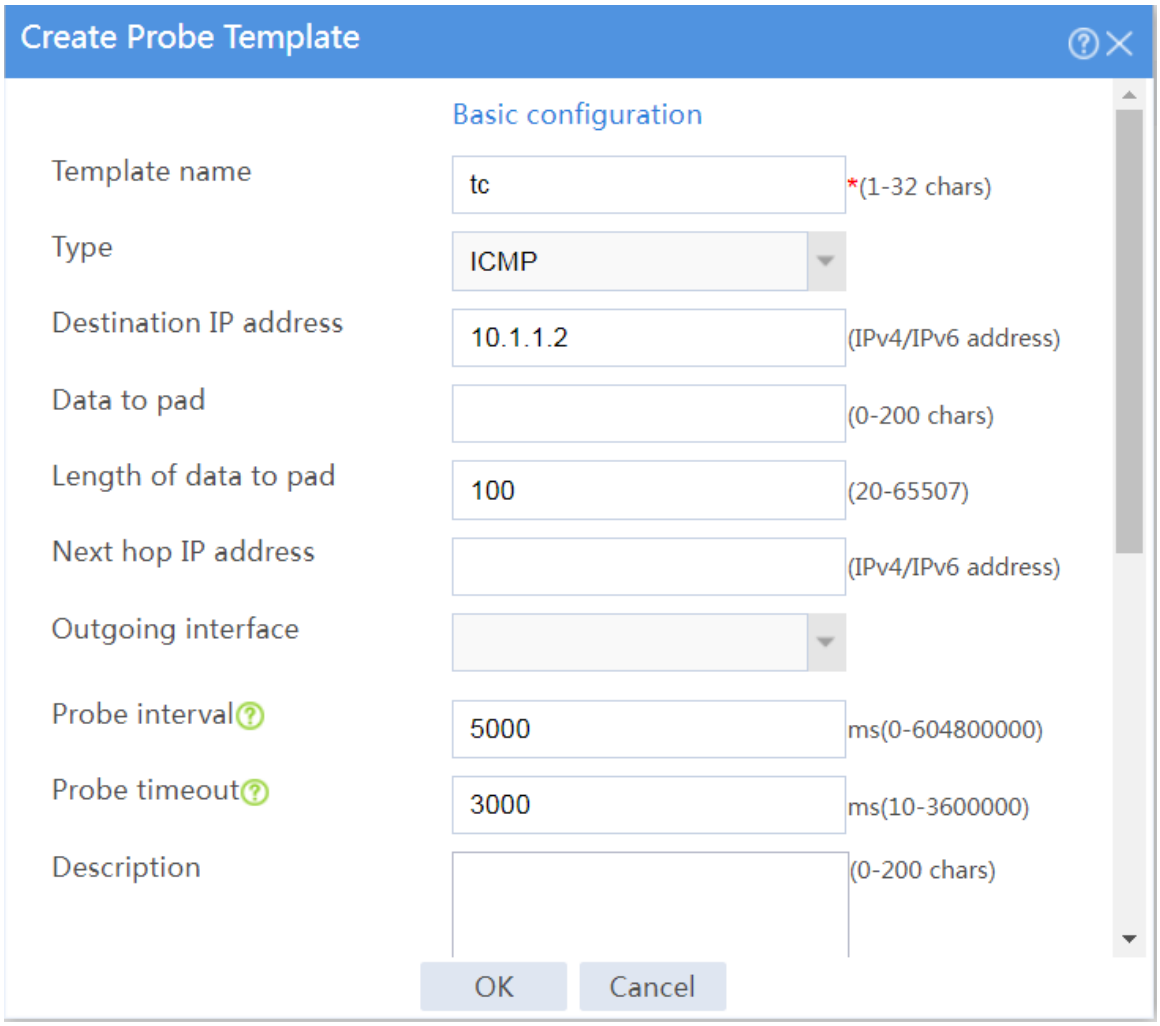
Figure 16 Creating probe template tb



Click **OK**.

Configure an ICMP probe template named **tc**, as shown in Figure 17.

Figure 17 Creating probe template tc



Click **OK**.

5. Configure outbound dynamic NAT rules.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Interface NAT** > **IPv4** > **Dynamic NAT**.

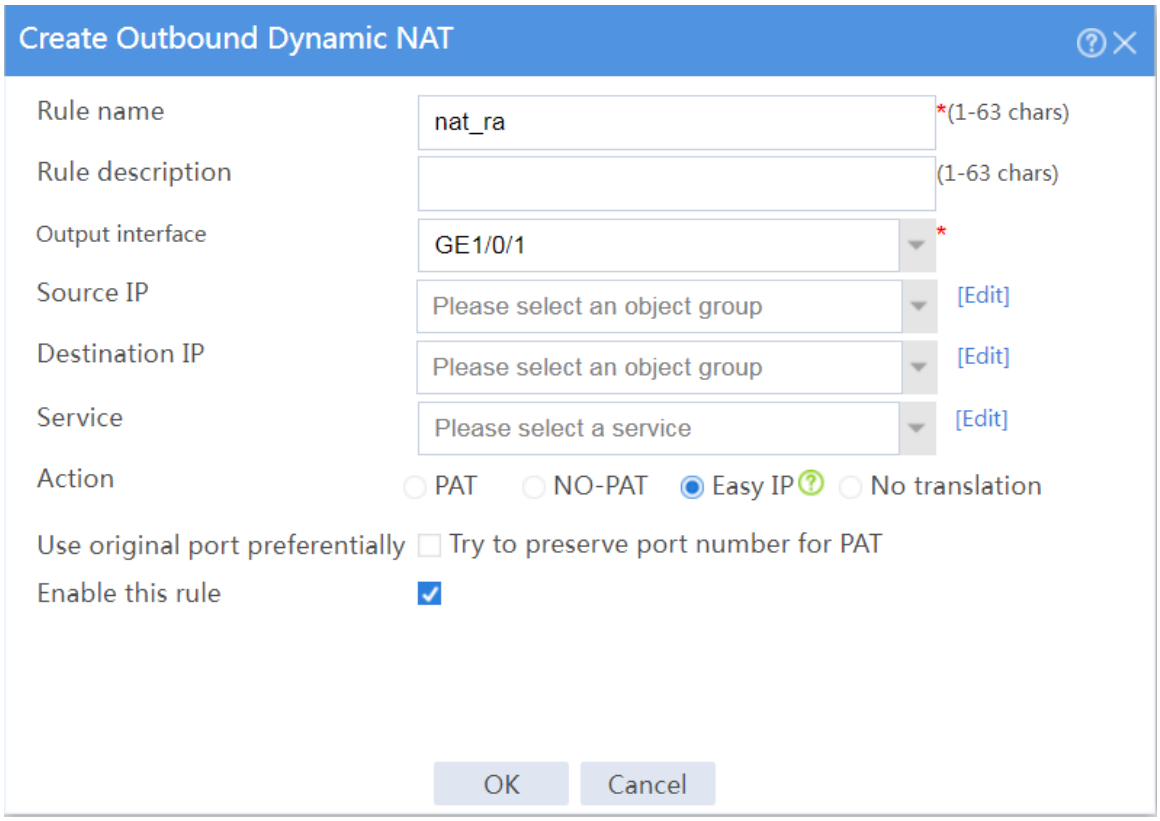
   # On the **Outbound Dynamic NAT (Object Group-Based)** tab, click **Create**.

   # Create an outbound dynamic NAT rule named **nat_ra**, as shown in Figure 18:

   - Enter rule name **nat_ra**.
   - Select output interface **GE1/0/1**.
   - Select action **Easy IP.**
   - Select **Enable this rule**.

- Click **OK**.

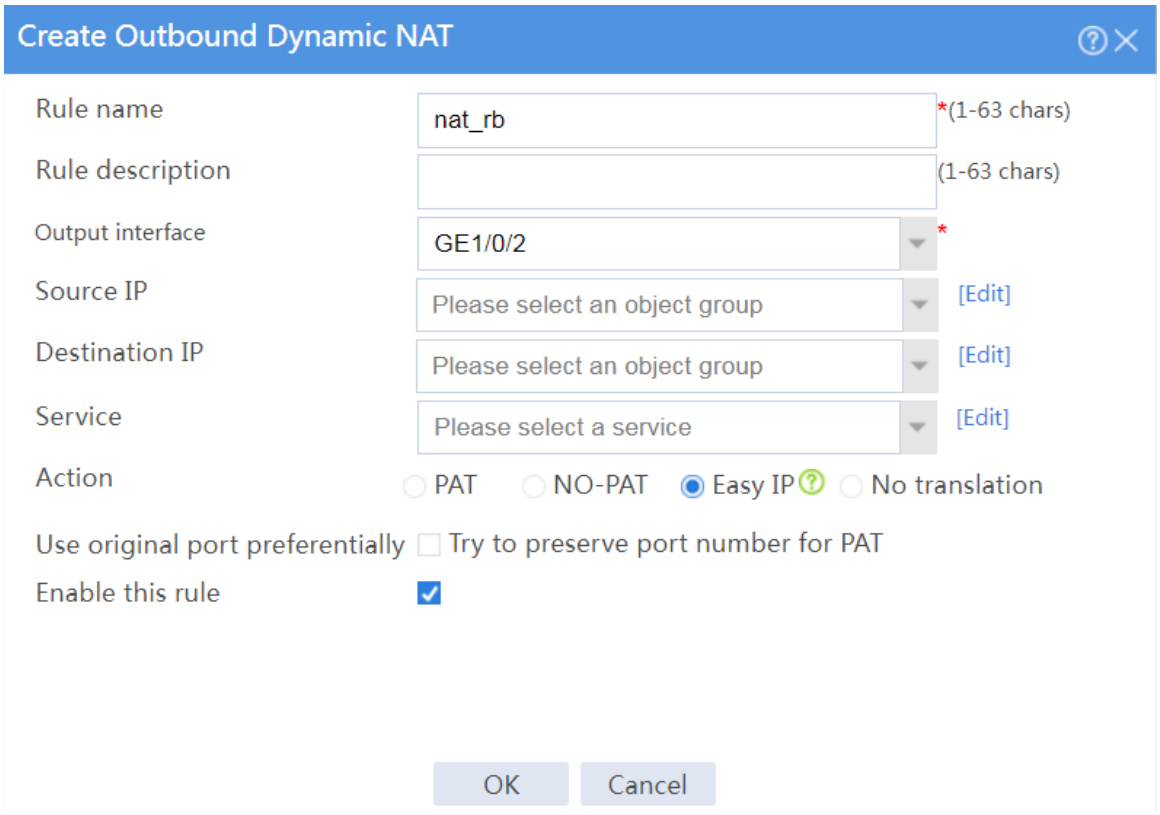
Figure 18 Configuring an outbound dynamic NAT rule named nat_ra



Create an outbound dynamic NAT rule named **nat_rb**, as shown in Figure 19:

- Enter rule name **nat_rb**.
- Select output interface **GE1/0/2**.
- Select action **Easy IP.**
- Select **Enable this rule**.
- Click **OK**.

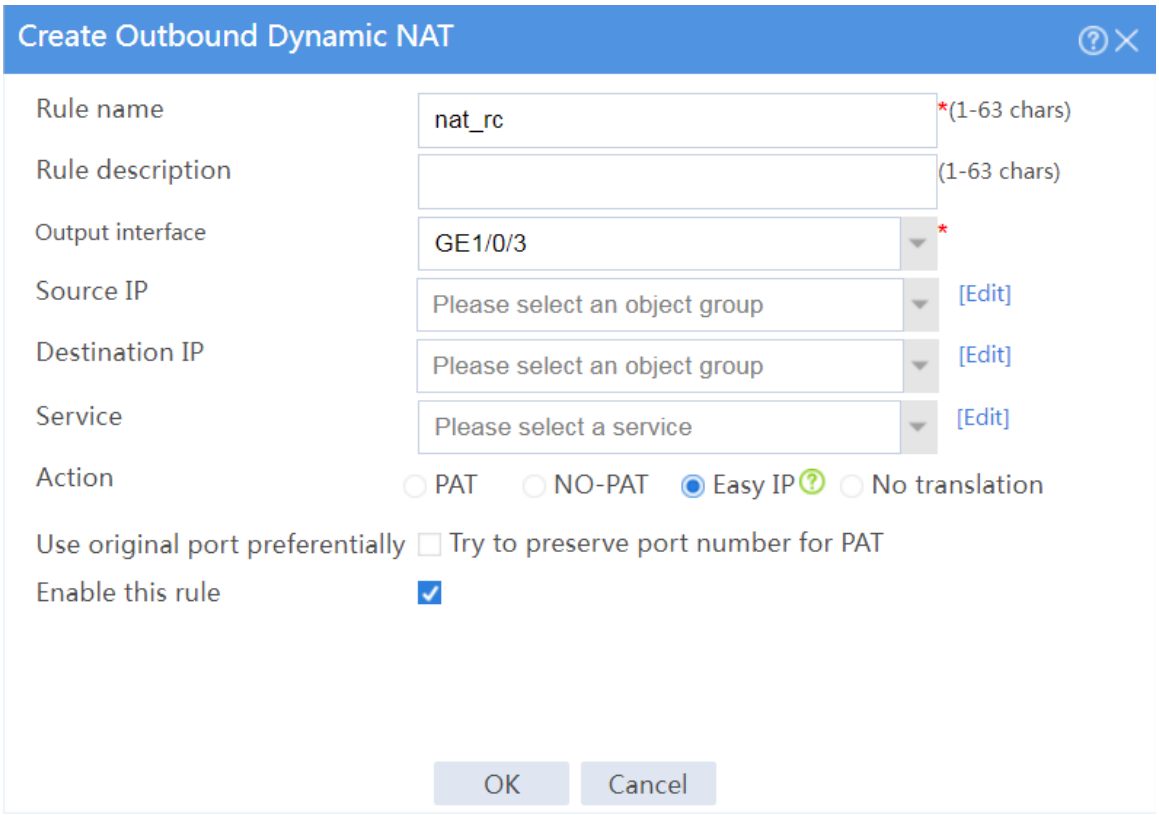
Figure 19 Configuring an outbound dynamic NAT rule named nat_rb



Create an outbound dynamic NAT rule named **nat_rc**, as shown in Figure 20:

- Enter rule name **nat_rc**.
- Select output interface **GE1/0/3**.
- Select action **Easy IP.**
- Select **Enable this rule**.
- Click **OK**.

Figure 20 Configuring an outbound dynamic NAT rule named nat_rc



6. Configure links.

   # On the top navigation bar, click **Polices**.

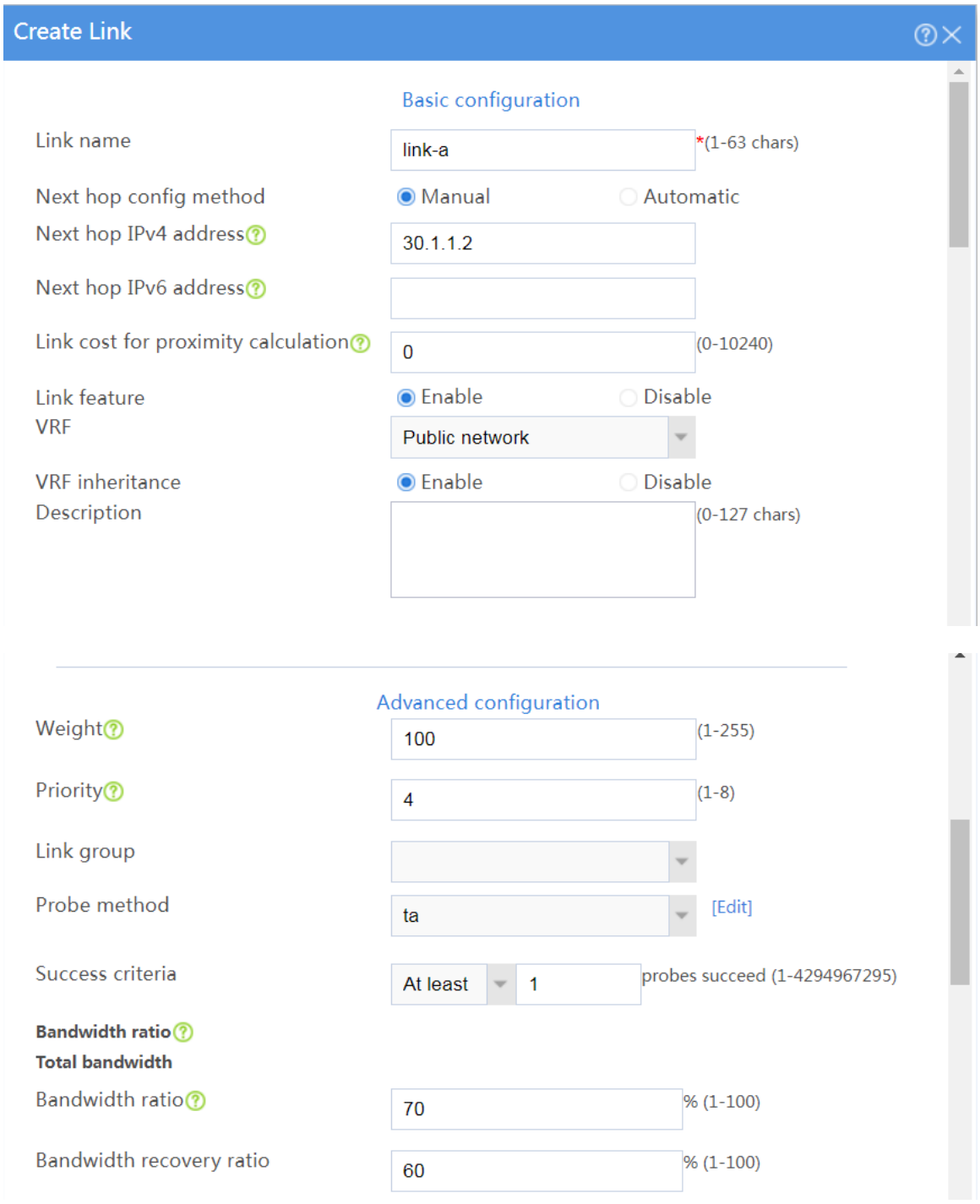
   # From the navigation pane, select **Load Balancing** > **Common Configuration** > **Links**.

   # Click **Create**.

   # In the dialog box that opens, configure a link named **link-a** as shown in Figure 21.

   # Click **OK**.

Figure 21 Creating link link-a

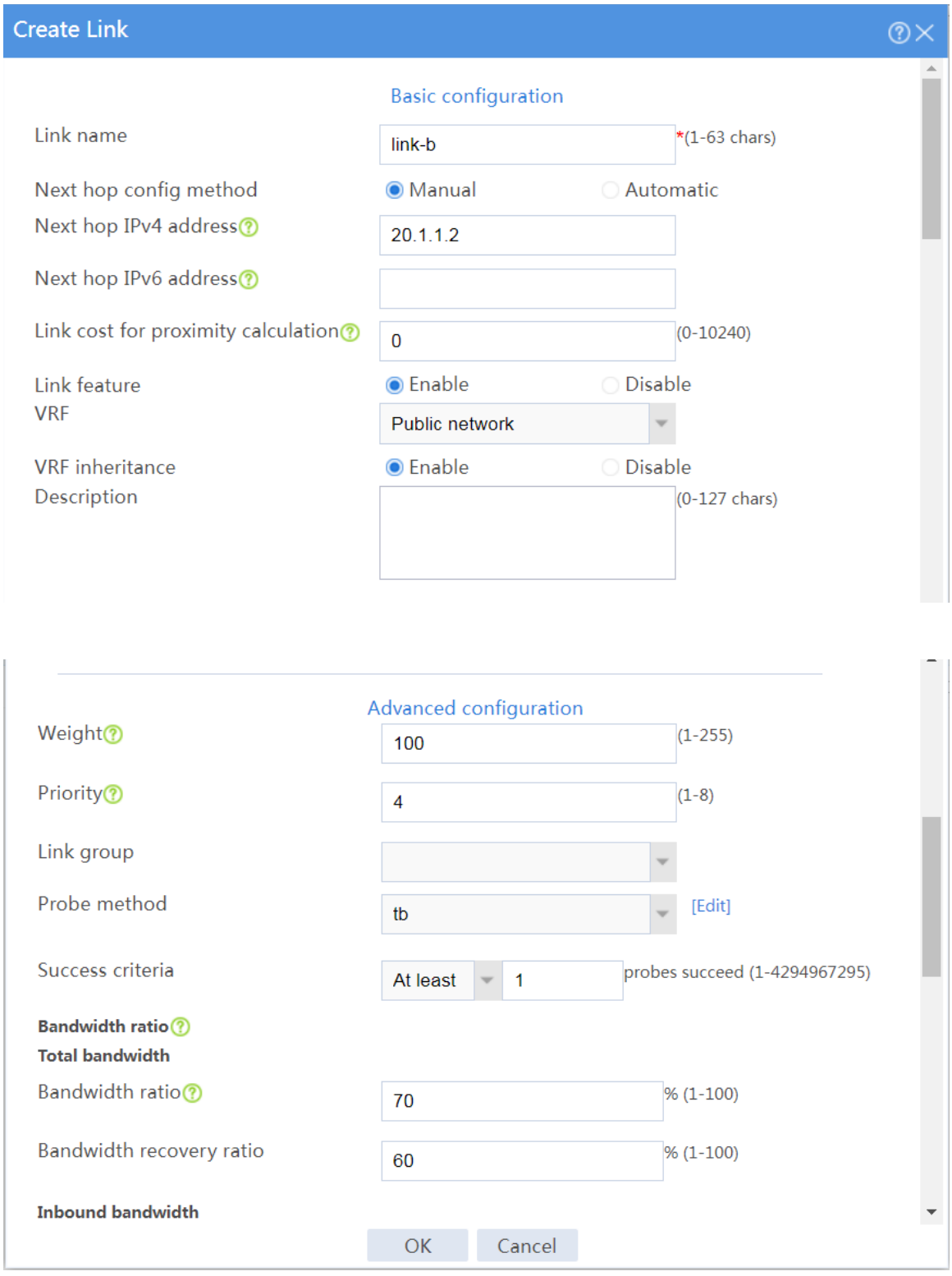


Click **Create**.

In the dialog box that opens, configure a link named **link-b** as shown in Figure 22.

Click **OK**.

Figure 22 Creating link link-b

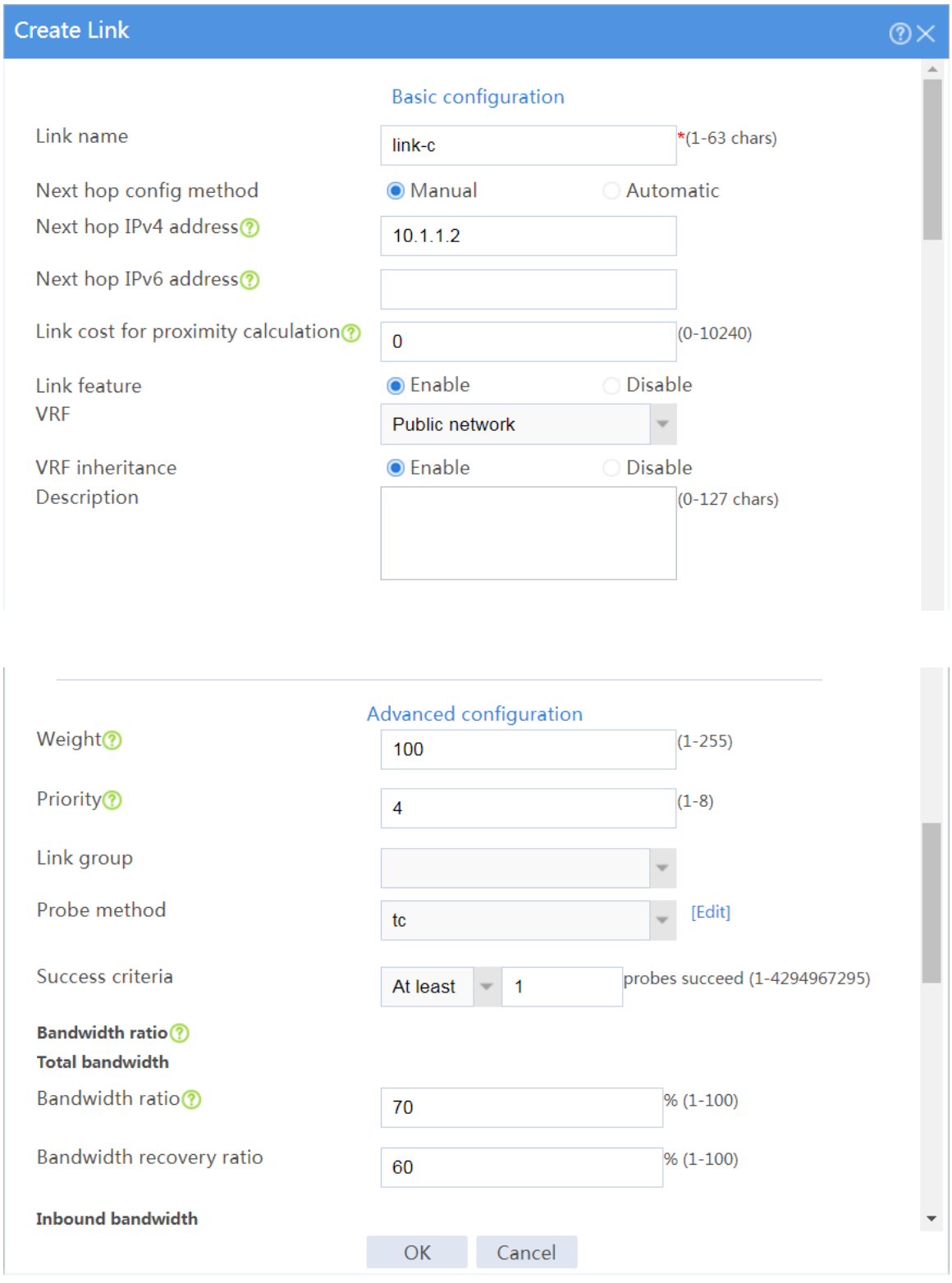


Click **Create**.

In the dialog box that opens, configure a link named **link-c** as shown in Figure 23.

Click **OK**.

Figure 23 Creating link link-c



7. Configure link groups.

   # On the top navigation bar, click **Polices**.

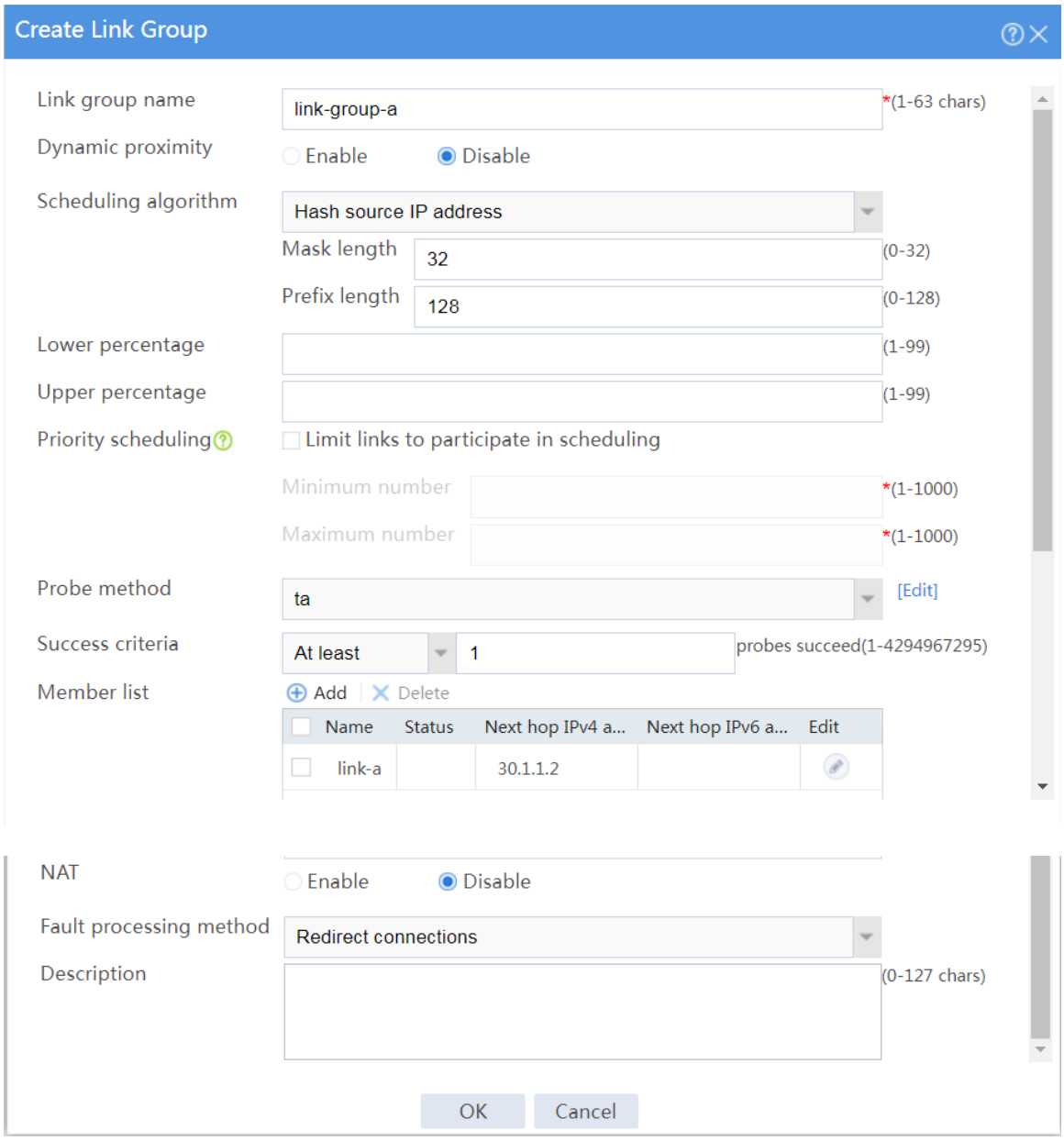
   # From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Outbound Link LB**.

   # On the **Link Group** tab, click **Create**.

   # In the dialog box that opens, configure a link group named **link-group-a** as shown in Figure 24.

   # Click **OK**.

Figure 24 Creating link group link-group-a

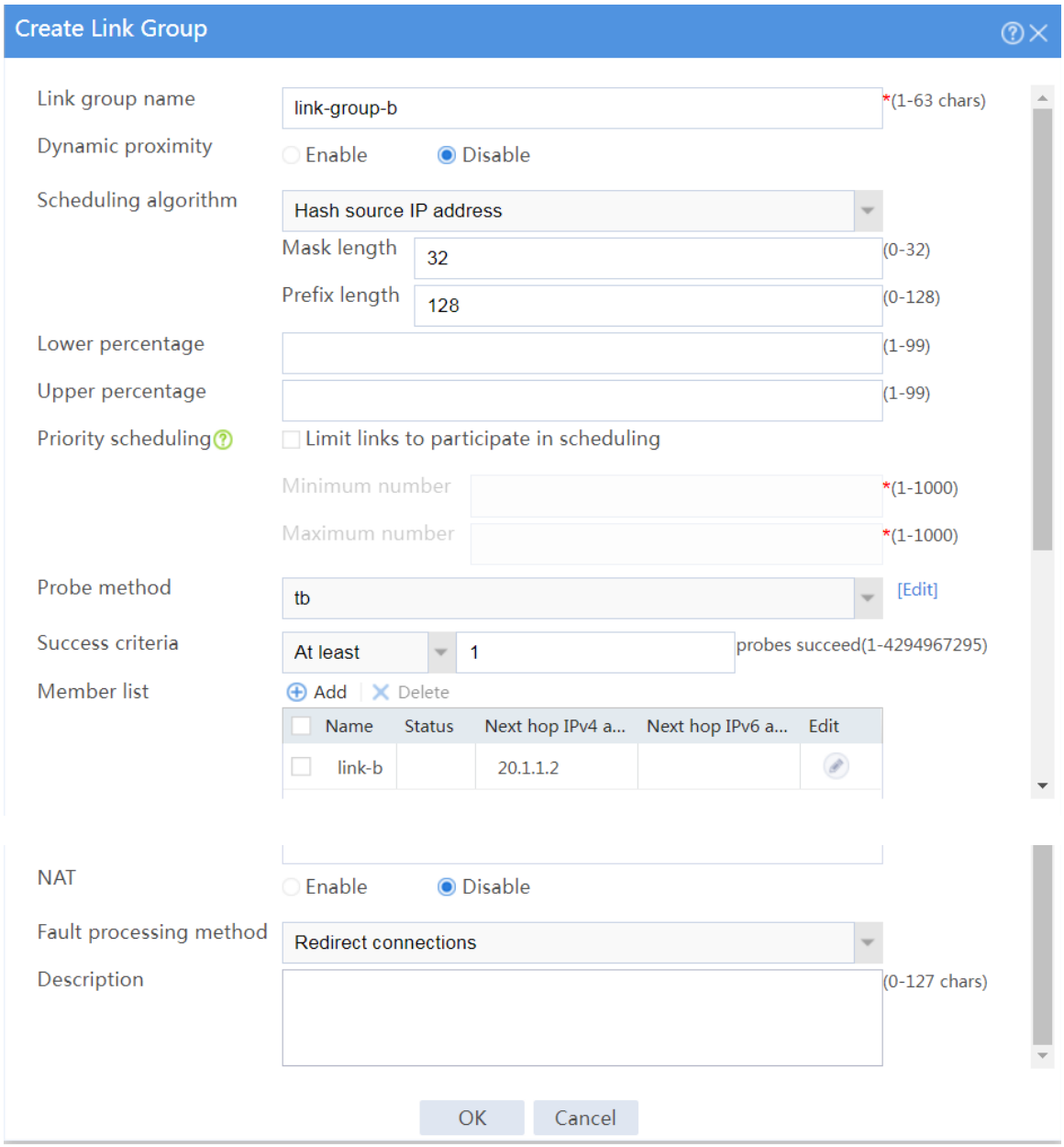


On the **Link Group** tab, click **Create**.

In the dialog box that opens, configure a link group named **link-group-b** as shown in Figure 25.

Click **OK**.

Figure 25 Creating link group link-group-b

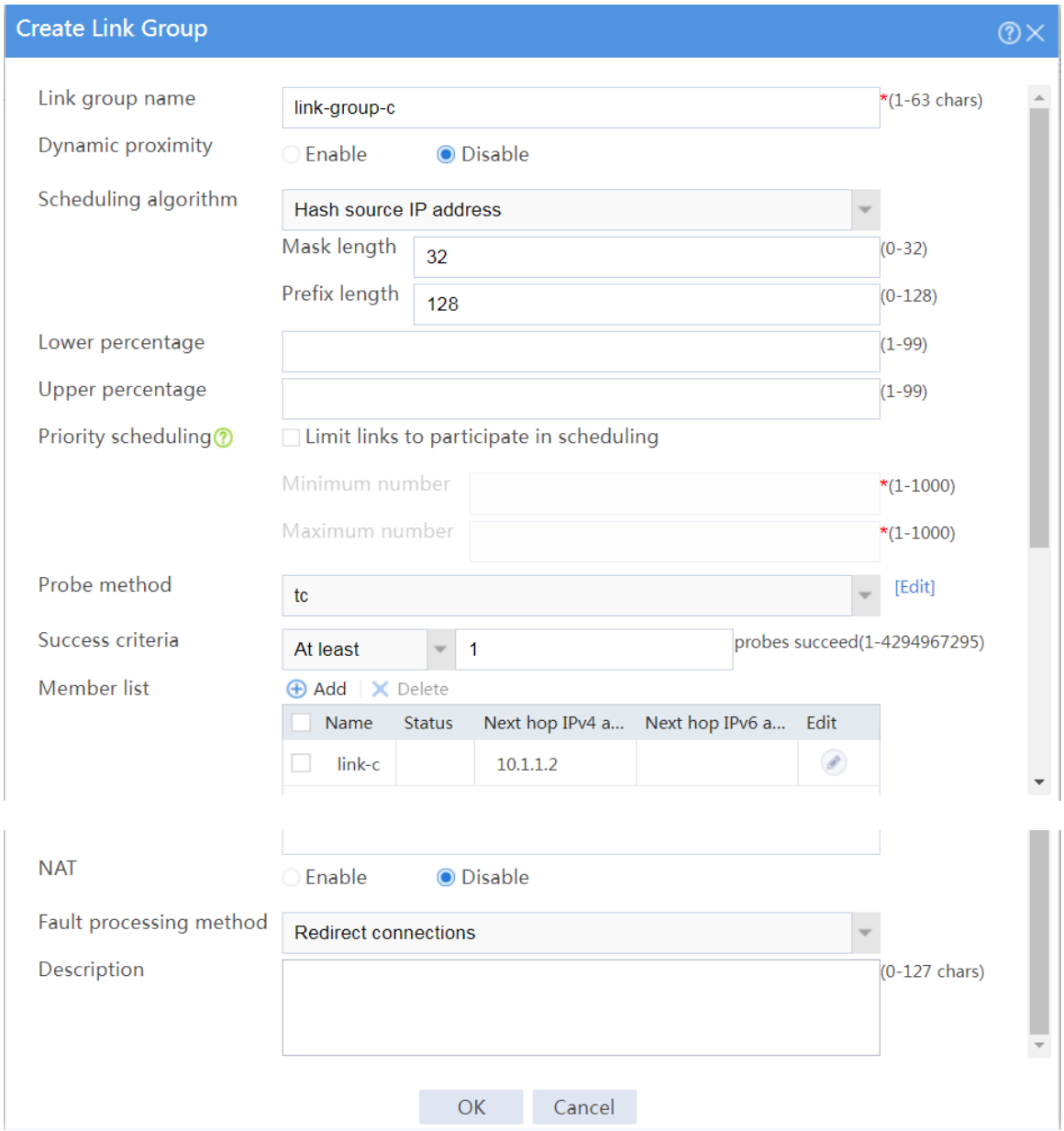


On the **Link Group** tab, click **Create**.

In the dialog box that opens, configure a link group named **link-group-c** as shown in Figure 26

Click **OK**.

Figure 26 Creating link group link-group-c



8. Import ISP information.

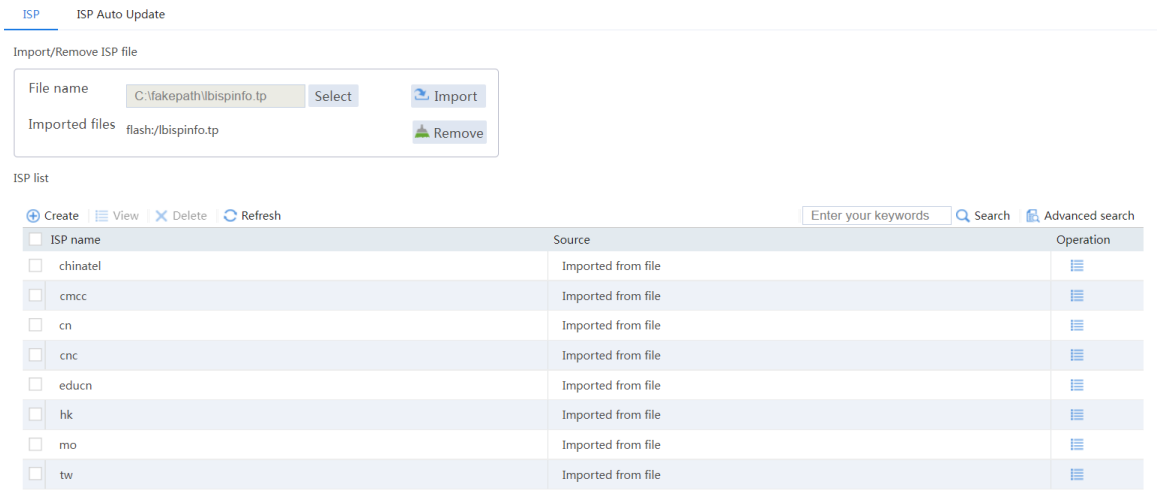
   # On the top navigation bar, click **Polices**.

   # From the navigation pane, select **Load Balancing** > **Common Configuration** > **ISP**.

   # Select file **lbispinfo.tp**.

   # Click **Import**.

Figure 27 Importing ISP information



9. Configure classes.

On the top navigation bar, click **Polices**.

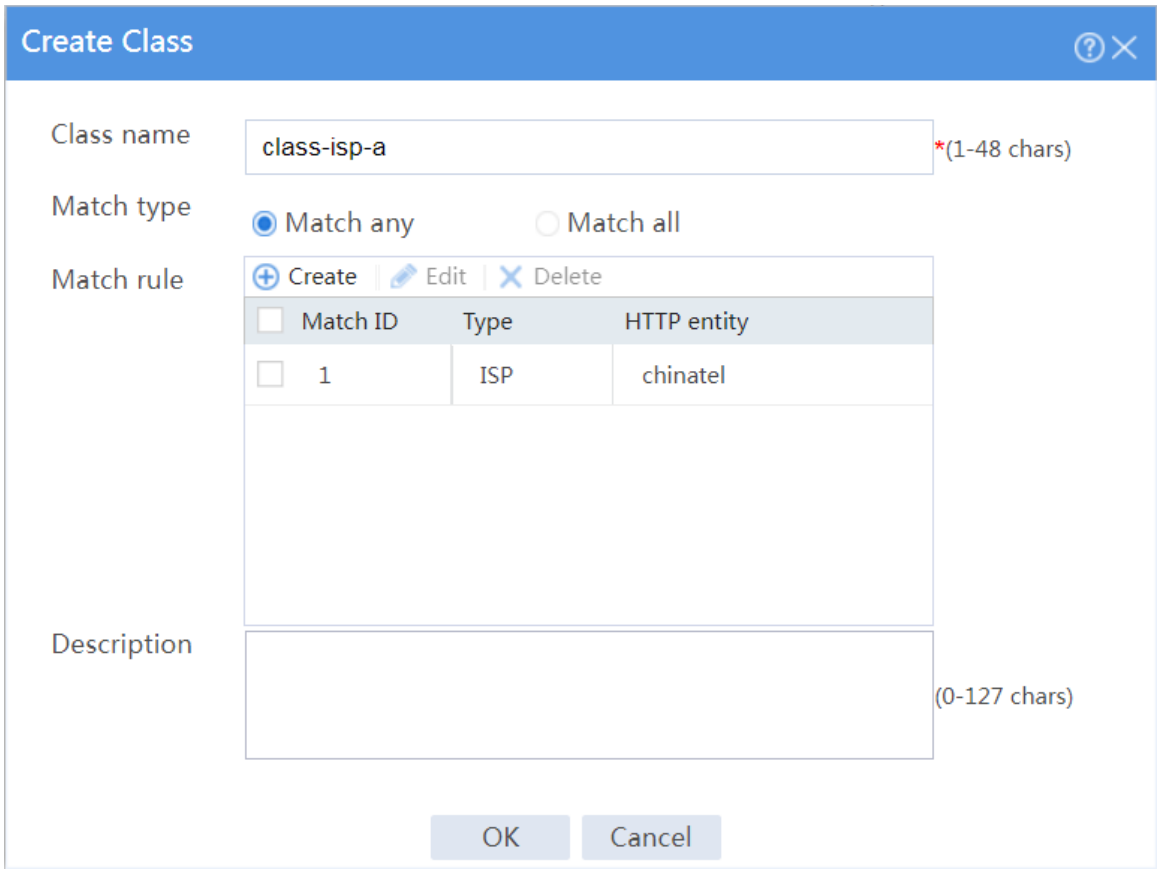
From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Outbound Link LB**.

On the **Class** tab, click **Create**.

In the dialog box that opens, configure a class named **class-isp-a** as shown in Figure 28.

Click **OK**.

Figure 28 Creating class class-isp-a

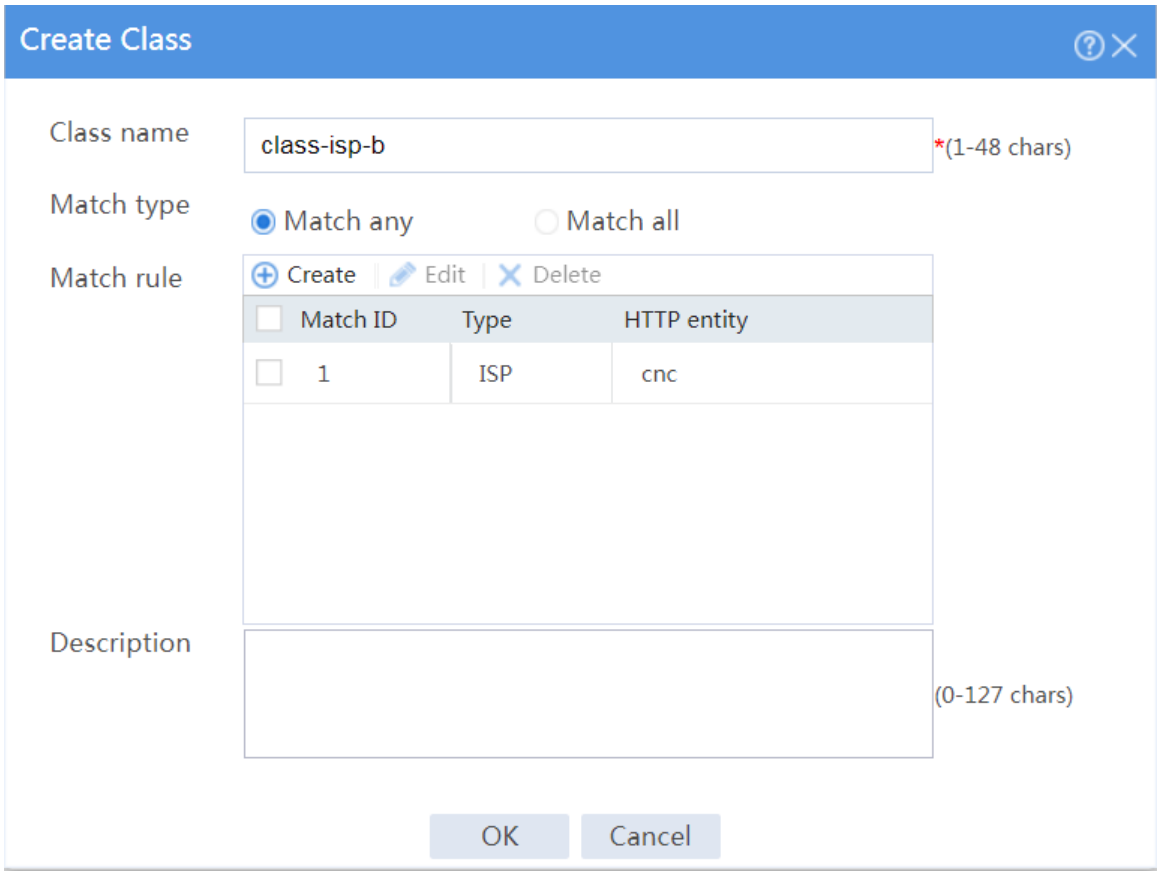


On the **Class** tab, click **Create**.

In the dialog box that opens, configure a class named **class-isp-b** as shown in Figure 29.

Click **OK**.

Figure 29 Creating class class-isp-b

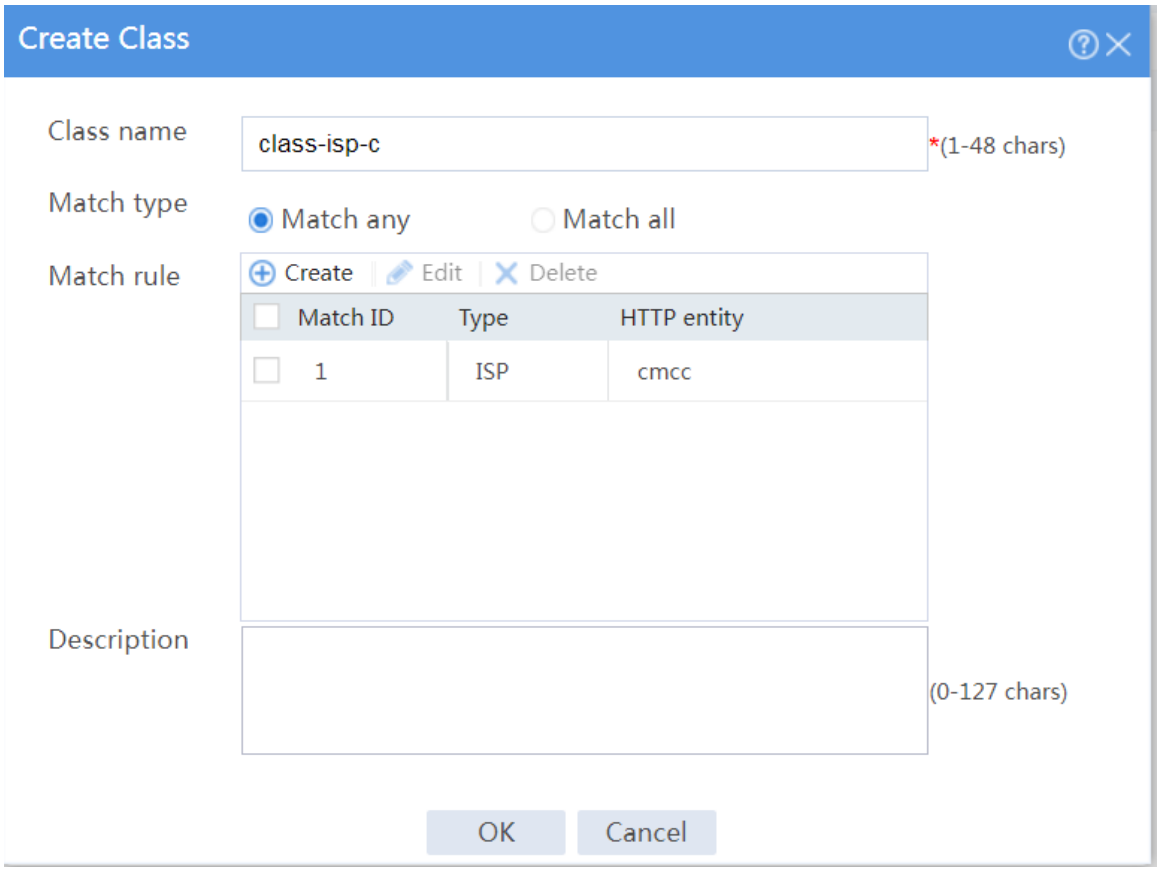


On the **Class** tab, click **Create**.

In the dialog box that opens, configure a class named **class-isp-c** as shown in Figure 30.

Click **OK**.

Figure 30 Creating class class-isp-c

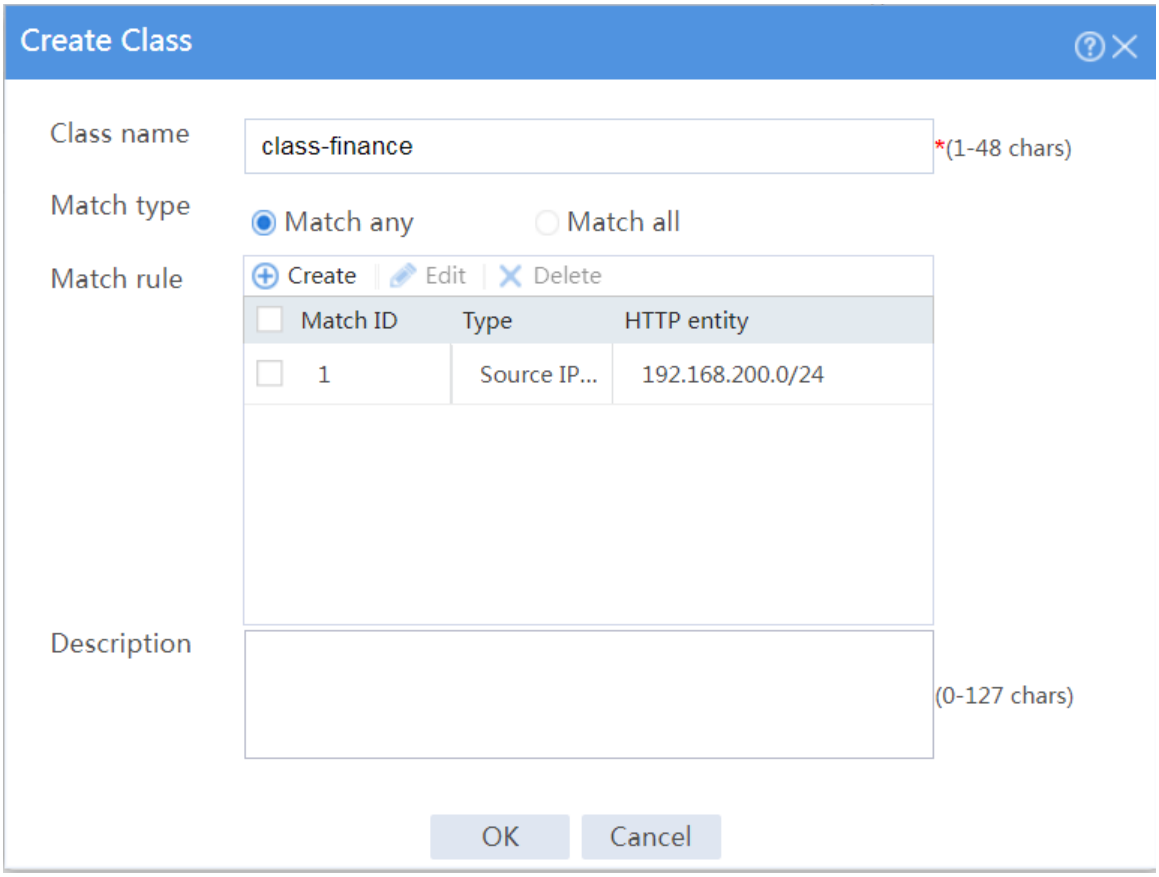


On the **Class** tab, click **Create**.

In the dialog box that opens, configure a class named **class-finance** as shown in Figure 31.

Click **OK**.

Figure 31 Creating class class-finance



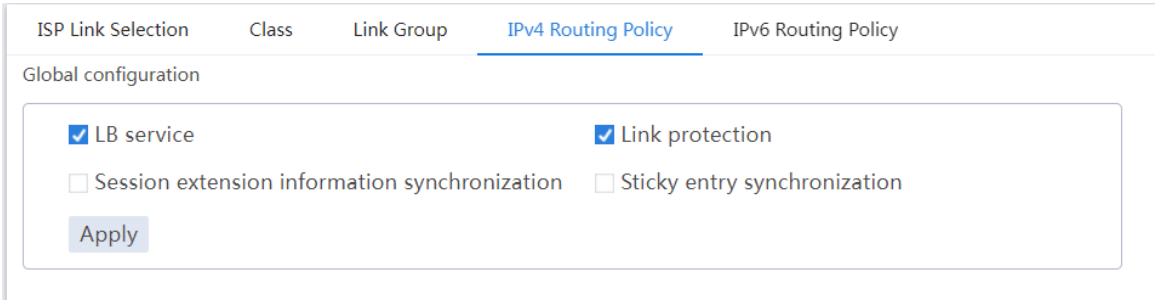
10. Configure IPv4 routing policies.

On the top navigation bar, click **Polices**.

From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **Outbound Link LB**.

In the **Global configuration** area on the **IPv4 Routing Policy** tab, select **LB service** and **Link protection**.

Figure 32 Global configuration

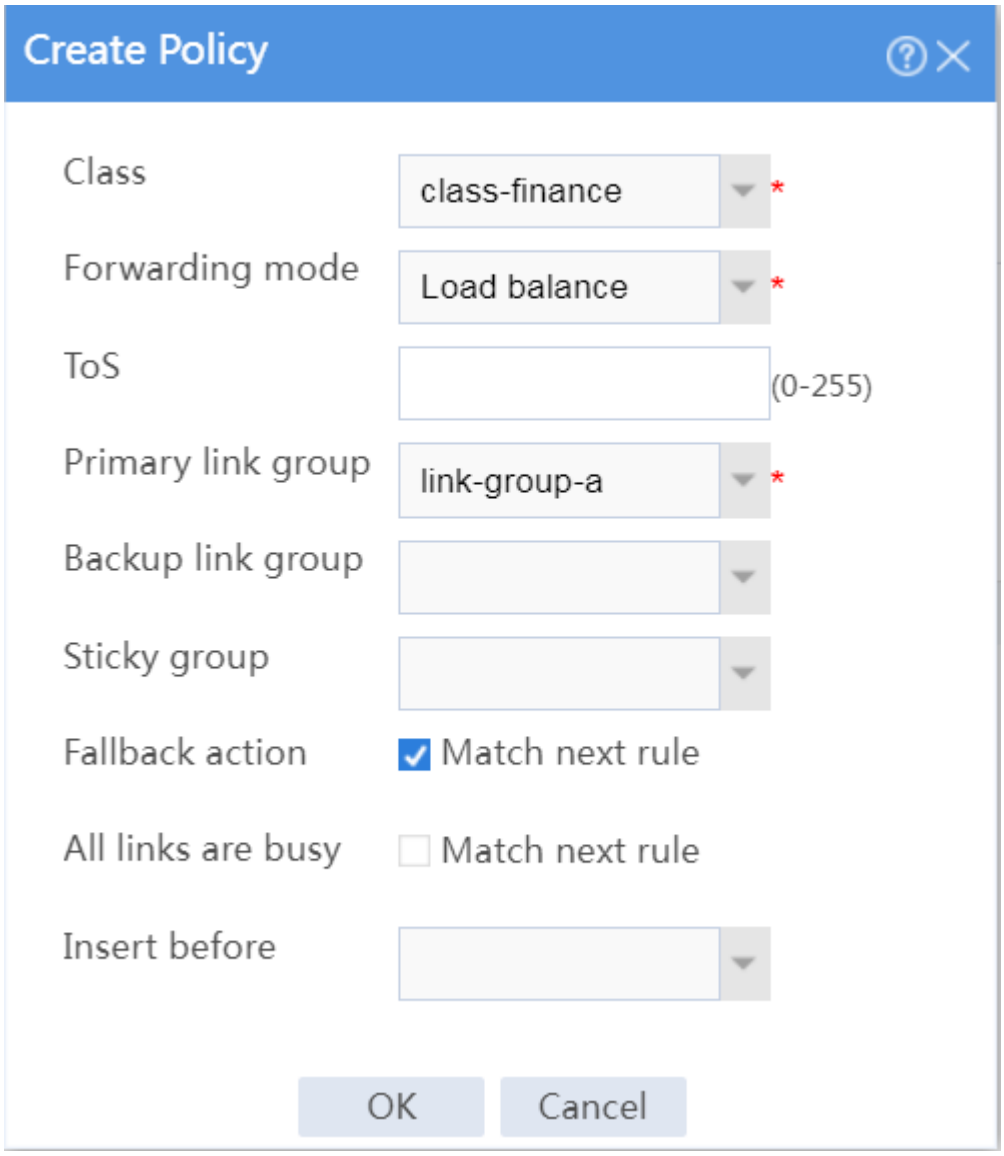


In the **Policy** area on the **IPv4 Routing Policy** tab, click **Create**.

In the dialog box that opens, configure an IPv4 routing policy for class **class-finance**:

- Select class **class-finance**.
- Select forwarding mode **Load balance**.
- Select primary link group **link-group-a**.
- Select **Match next rule** for the **Fallback action** field.
- Click **OK**.

Figure 33 Creating a policy for class class-finance

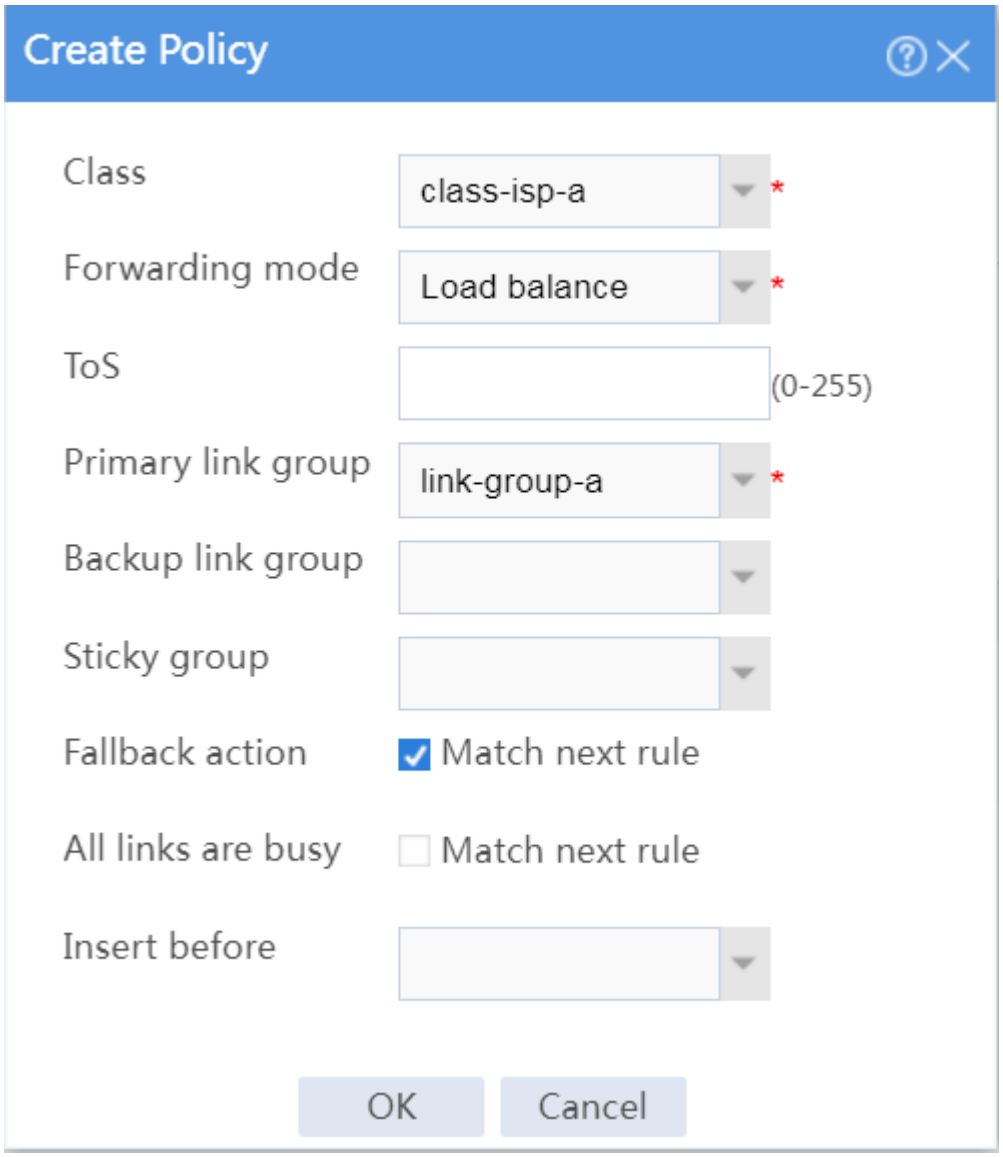


In the **Policy** area on the **IPv4 Routing Policy** tab, click **Create**.

In the dialog box that opens, configure an IPv4 routing policy for class **class-isp-a**:

- Select class **class-isp-a**.
- Select forwarding mode **Load balance**.
- Select primary link group **link-group-a**.
- Select **Match next rule** for the **Fallback action** field.
- Click **OK**.

Figure 34 Creating a policy for class class-isp-a

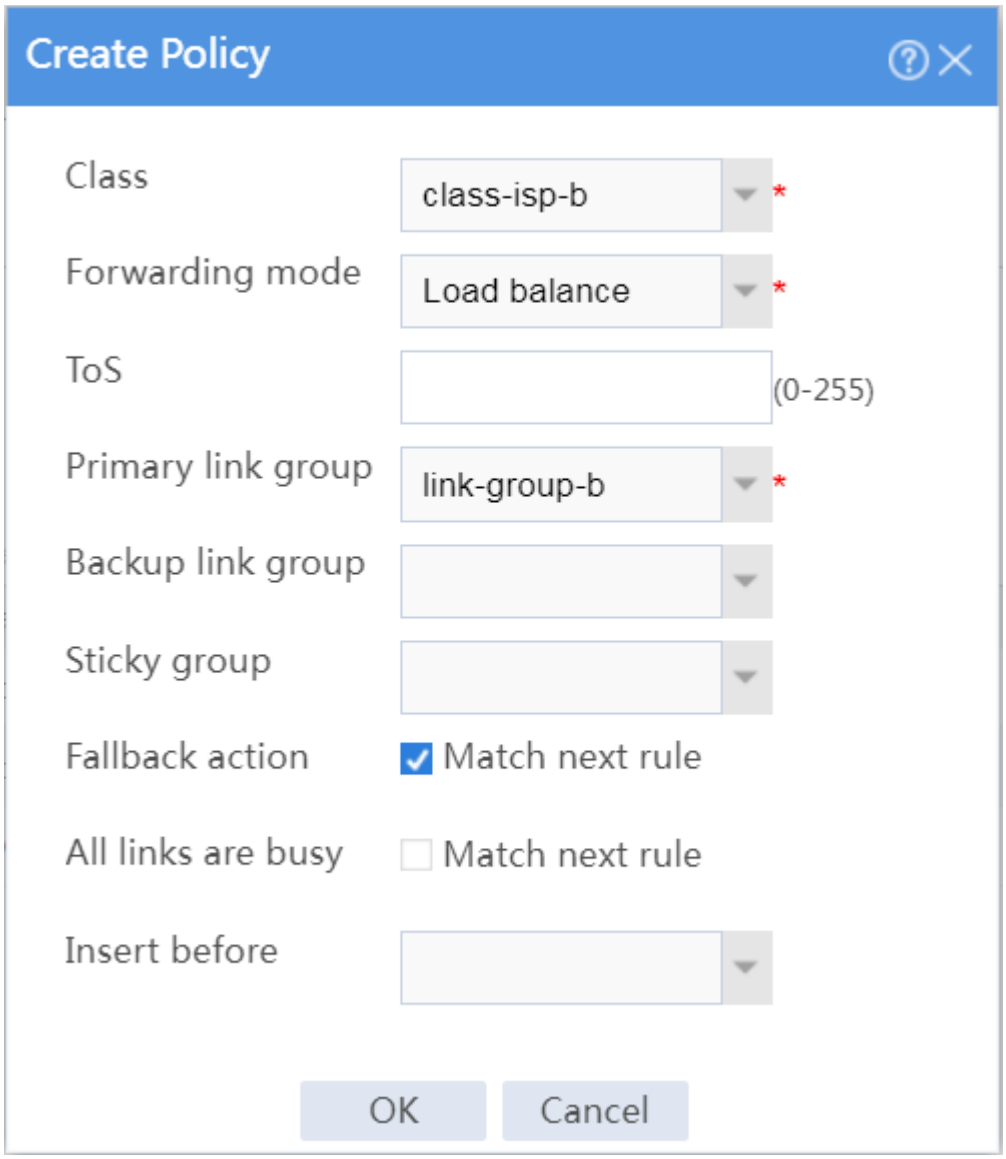


In the **Policy** area on the **IPv4 Routing Policy** tab, click **Create**.

In the dialog box that opens, configure an IPv4 routing policy for class **class-isp-b**:

- Select class **class-isp-b**.
- Select forwarding mode **Load balance**.
- Select primary link group **link-group-b**.
- Select **Match next rule** for the **Fallback action** field.
- Click **OK**.

Figure 35 Creating a policy for class class-isp-b

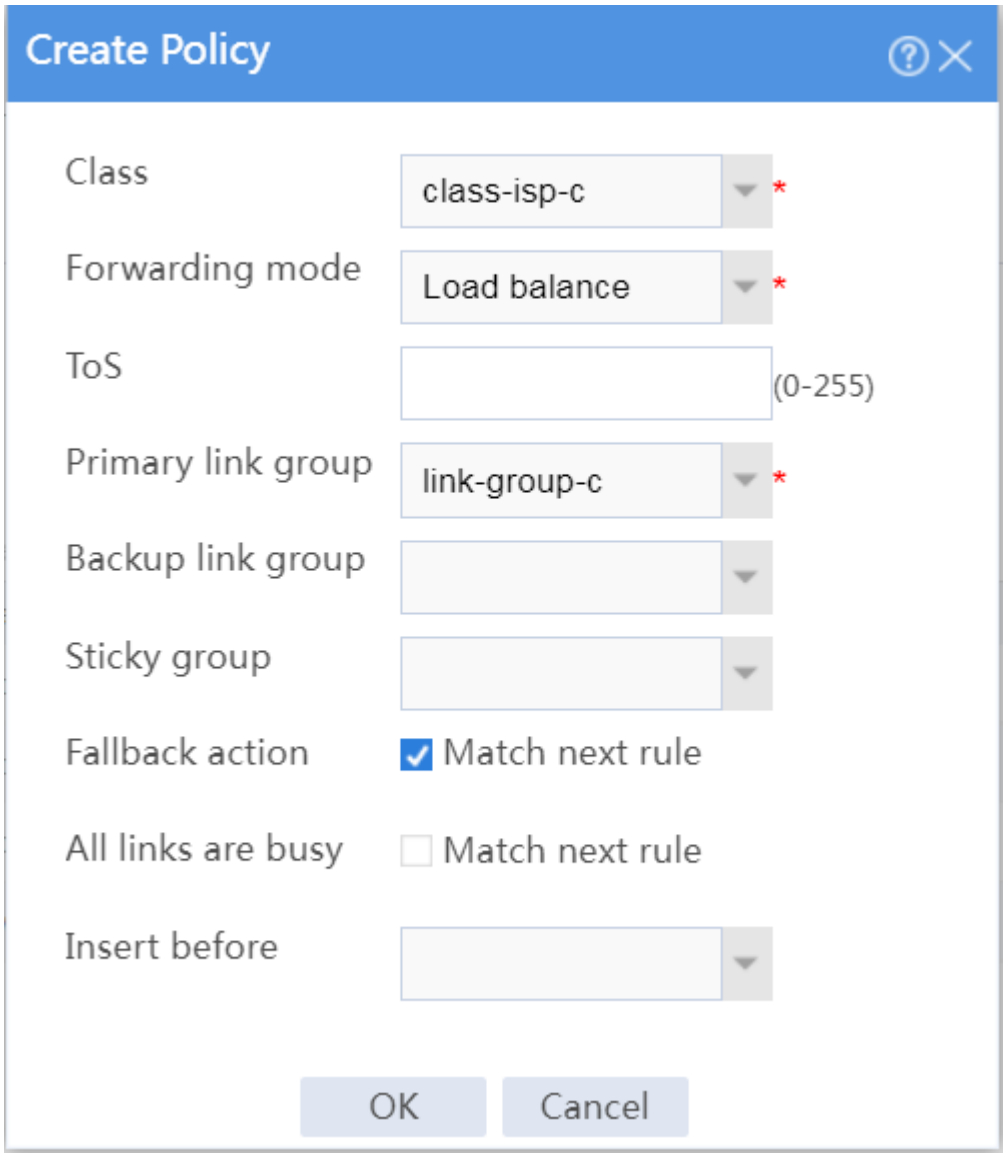


In the **Policy** area on the **IPv4 Routing Policy** tab, click **Create**.

In the dialog box that opens, configure an IPv4 routing policy for class **class-isp-c**:

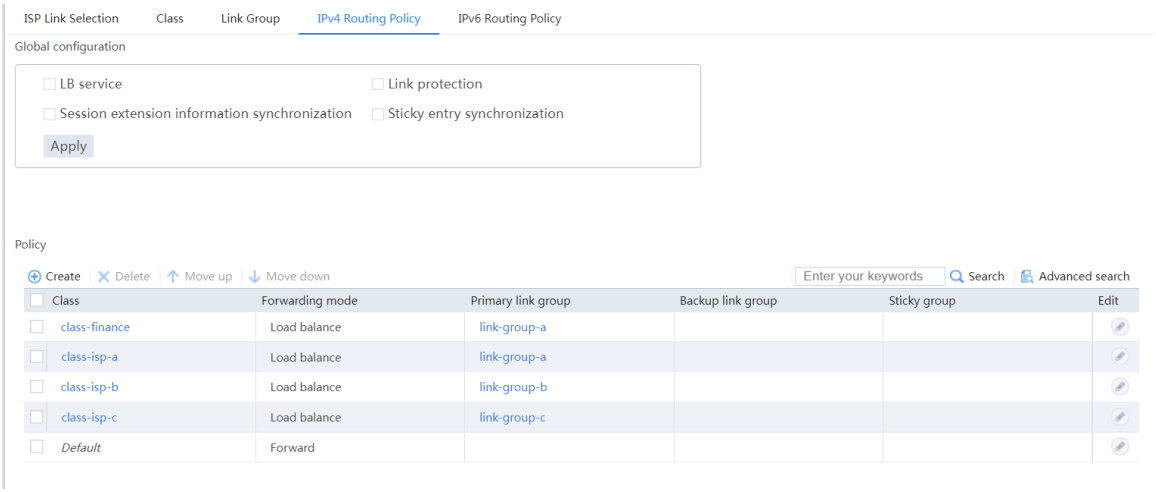
- Select class **class-isp-c**.
- Select forwarding mode **Load balance**.
- Select primary link group **link-group-c**.
- Select **Match next rule** for the **Fallback action** field.
- Click **OK**.

Figure 36 Creating a policy for class class-isp-c



View the configured IPv4 routing policies as shown in Figure 37.

Figure 37 IPv4 routing policies



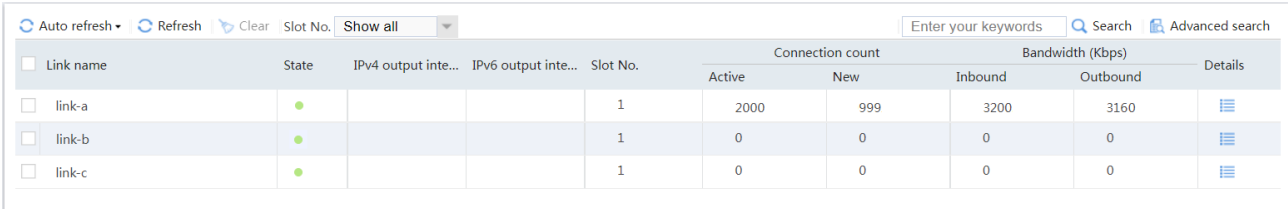
Verifying the configuration

On the top navigation bar, click the **Monitor** tab.

From the navigation pane, select **Statistics** > **Outbound Link LB Statistics** > **Links**.

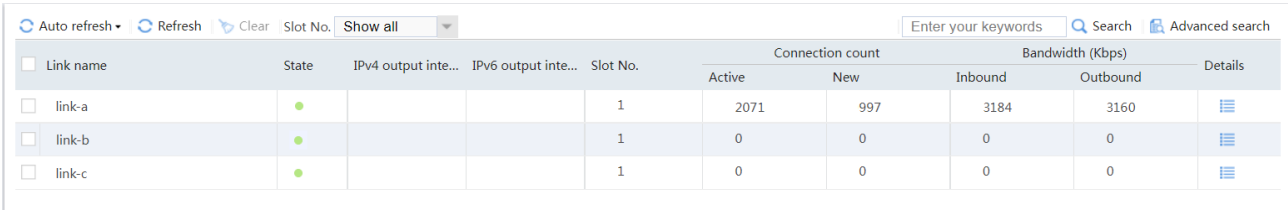
View the statistics of link **link-a** as shown in Figure 38. Traffic from subnet **192.168.200.0/24** in the finance department matches class **class-finance**, and is distributed to link group **link-group-a**.

Figure 38 Statistics of traffic from the finance department



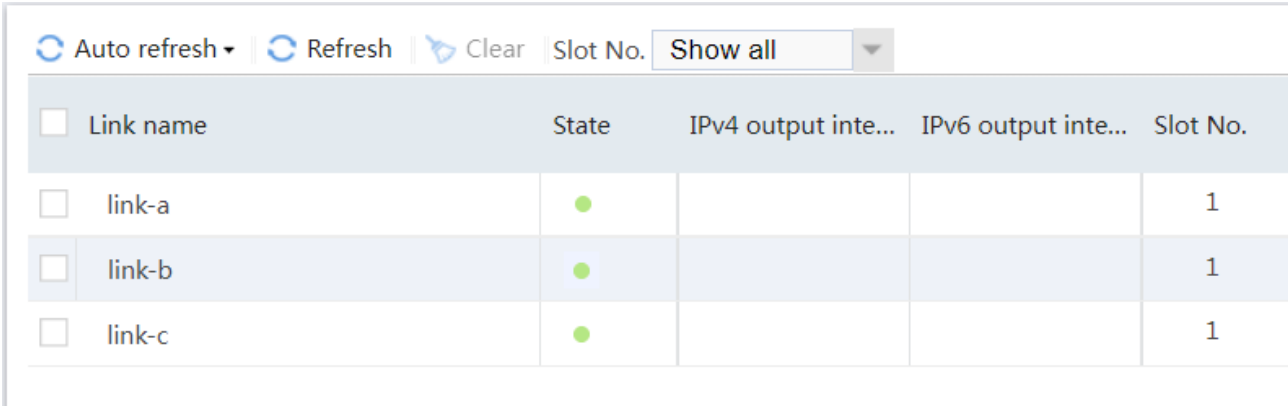
View the statistics of link **link-a** as shown in Figure 39. Traffic destined for ISP-A matches class **class-isp-a**, and is distributed to link group **link-group-a**.

Figure 39 Statistics of traffic destined for ISP_A



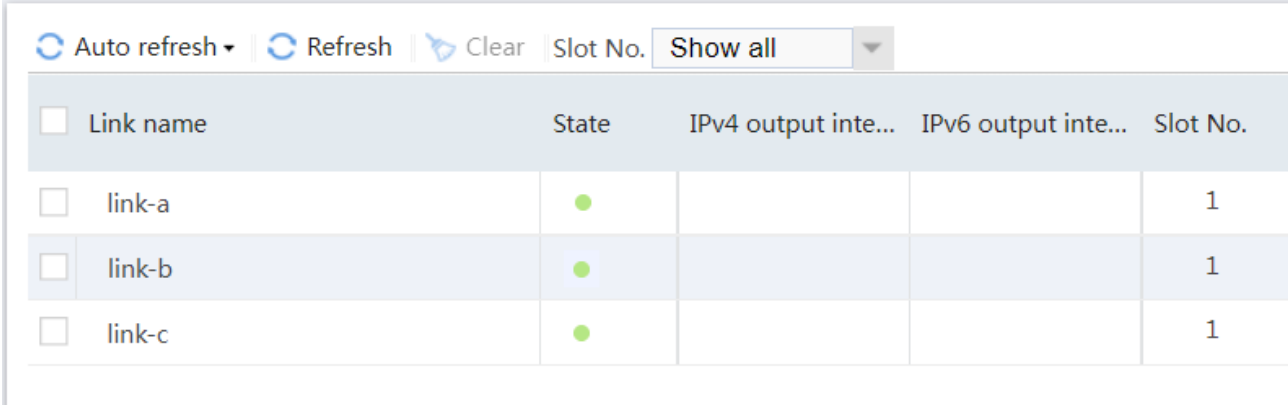
View the statistics of link **link-b** as shown in Figure 40. Traffic destined for ISP-B belongs to class **class-isp-b**, and is distributed to link group **link-group-b**.

Figure 40 Statistics of traffic destined for ISP_B



View the statistics of link **link-c** as shown in Figure 41. Traffic destined for ISP_C belongs to class **class-isp-c**, and is distributed to link group **link-group-c**.

Figure 41 Statistics of traffic destined for ISP_C



Server load balancing configuration examples

Contents

Introduction

The following information provides server load balancing configuration examples.

Server load balancing is classified into Layer 4 server load balancing and Layer 7 server load balancing.

- **Layer 4 server load balancing**—Implemented based on streams. It distributes packets in the same stream to the same server. Layer 4 server load balancing cannot distribute Layer 7 services based on contents.
- **Layer 7 server load balancing**—Implemented based on contents. It analyzes packet contents, distributes packets one by one based on the contents, and distributes connections to the specified server according to the predefined policies. Layer 7 server load balancing applies load balancing services to a large scope.

Server load balancing supports IPv4 and IPv6, but does not support IPv4-to-IPv6 or IPv6-to-IPv4 translation.

The virtual server types supported by server load balancing include IP, TCP, UDP, HTTP, Performance (HTTP), HTTPS, and HTTP redirection. IP, TCP, and UDP, are called Layer 4 server load balancing. HTTP, Performance (HTTP), HTTPS, and HTTP redirection are called Layer 7 server load balancing.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

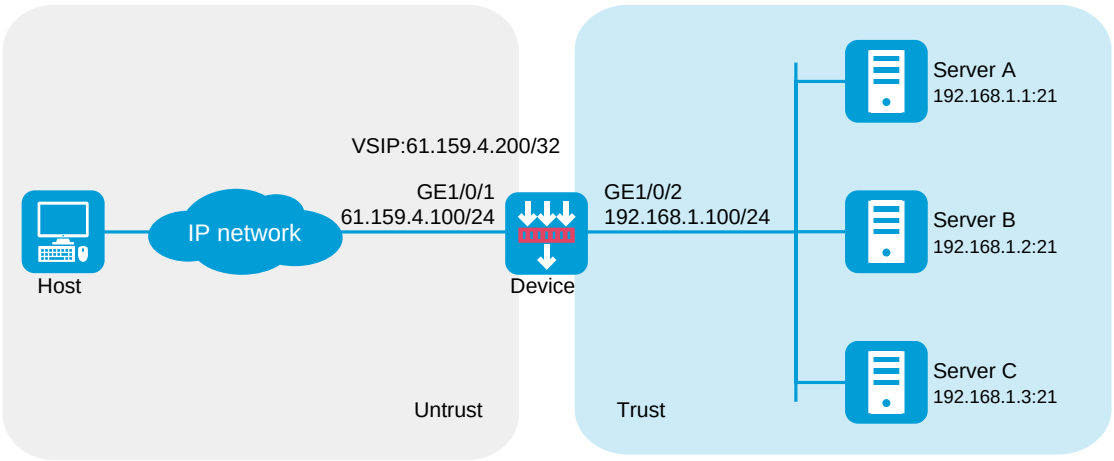
The following information is provided based on the assumption that you have basic knowledge of the server load balancing feature.

Example: Configuring Layer 4 server load balancing

Network configuration

As shown in Figure 1, an enterprise uses Server A, Server B, and Server C to provide FTP services. Configure server load balancing to load balance FTP requests from Host among the servers based on source address. For example, enable the device to assign FTP requests sourced from 62.159.4.0/24 and 63.159.4.0/24 to Server A and Server B, respectively; enable the device to assign FTP requests with other source addresses to Server C.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Untrust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask length of the interface. In this example, enter 61.159.4.100/24.
   - Use the default settings for other parameters.
   - Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and set its IP address to 192.168.1.100/24 in the same way you configure GE 1/0/1.

2. Configure security policies.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy named **Untrust-to-Trust**:

- Enter policy name **Untrust-to-Trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 address **61.159.4.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

Configure a security policy named **Local-to-Trust**:

- Enter policy name **Local-to-Trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 address **192.168.1.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

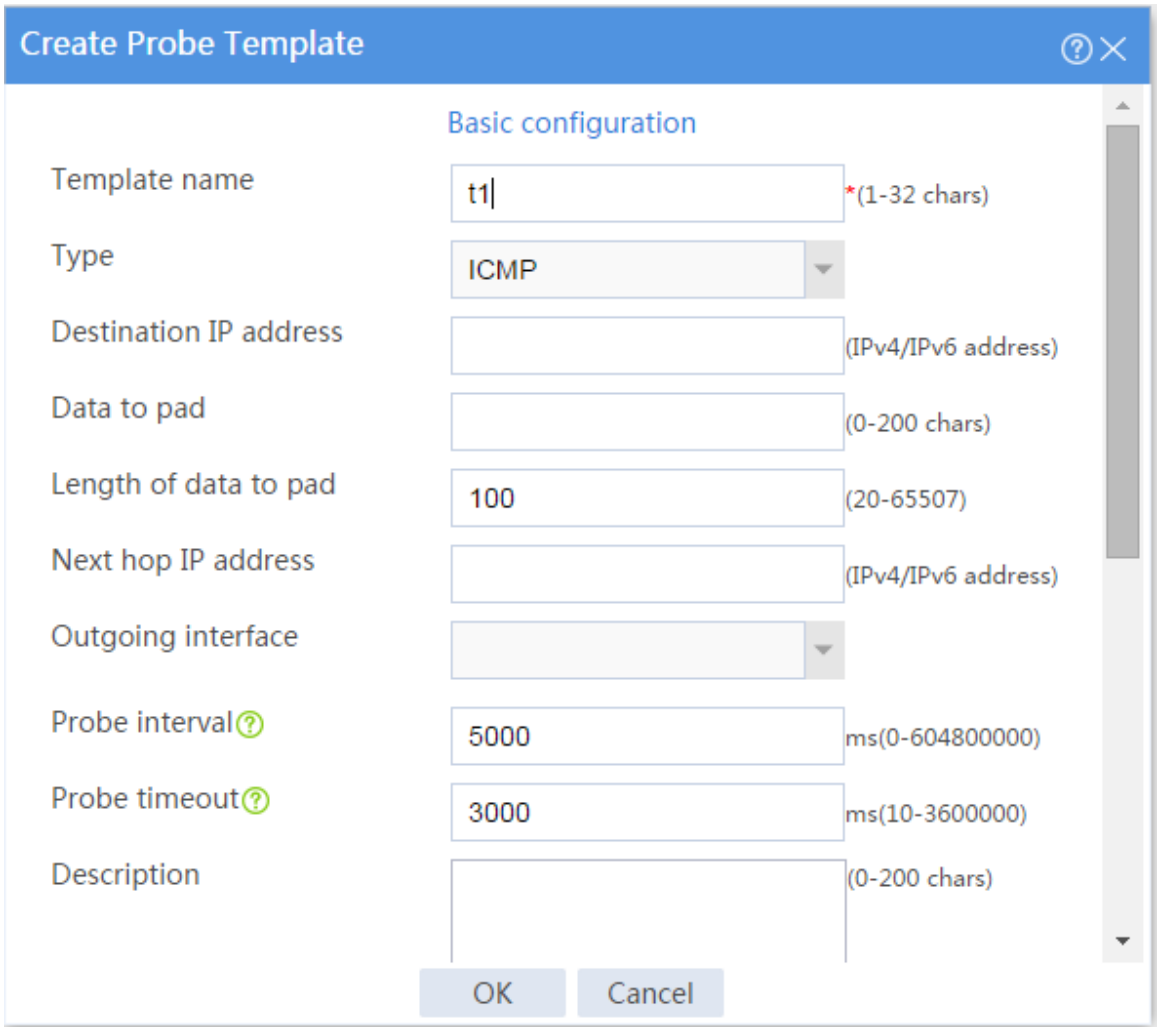
3. Create an ICMP-type probe template.

On the top navigation bar, click **Objects**.

From the navigation pane, select **Health Monitoring**.

Click **Create** to configure the probe template **t1** as shown in Figure 2.

Figure 2 Creating probe template t1



Click **OK**.

4. Create an address- and port-type sticky group.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Common Configuration** > **Sticky Groups**.

Click **Create** to configure the sticky group **sticky_group** as shown in Figure 3.

Figure 3 Creating sticky group sticky_group (part 1)

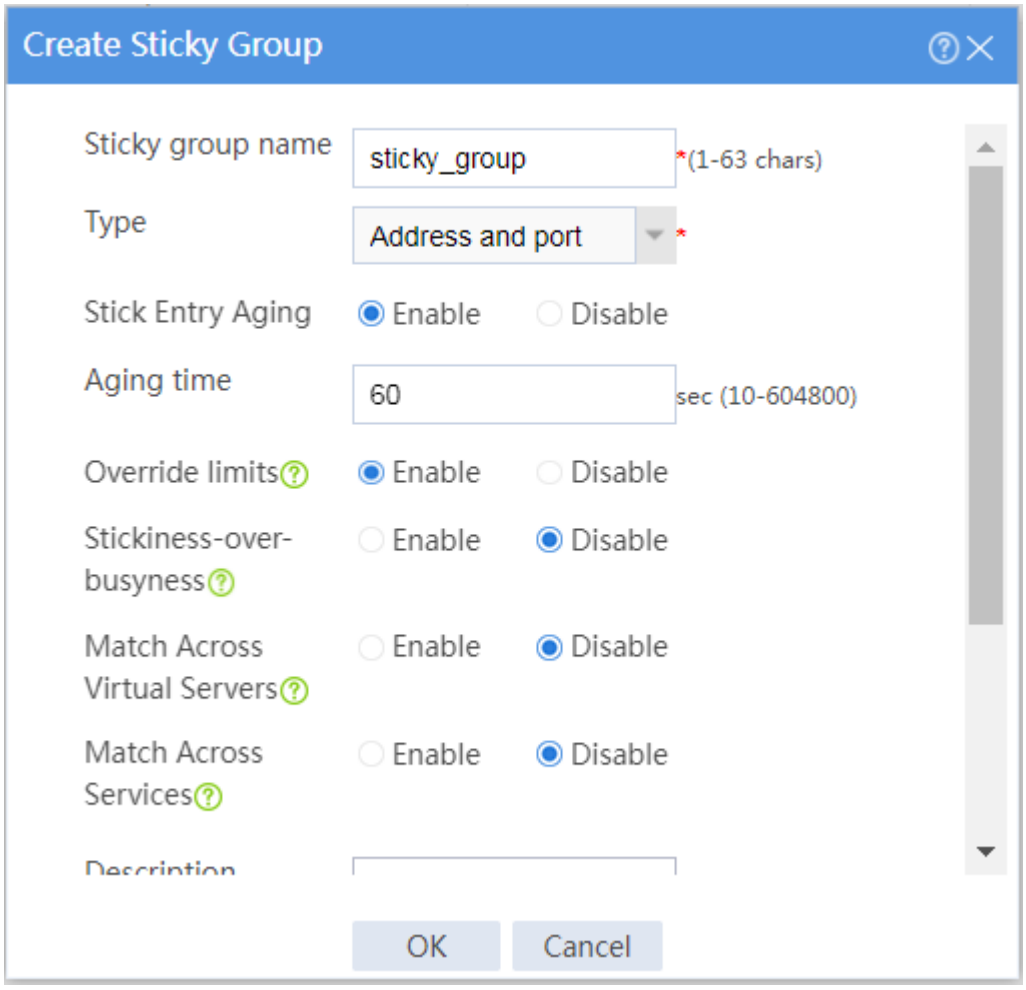
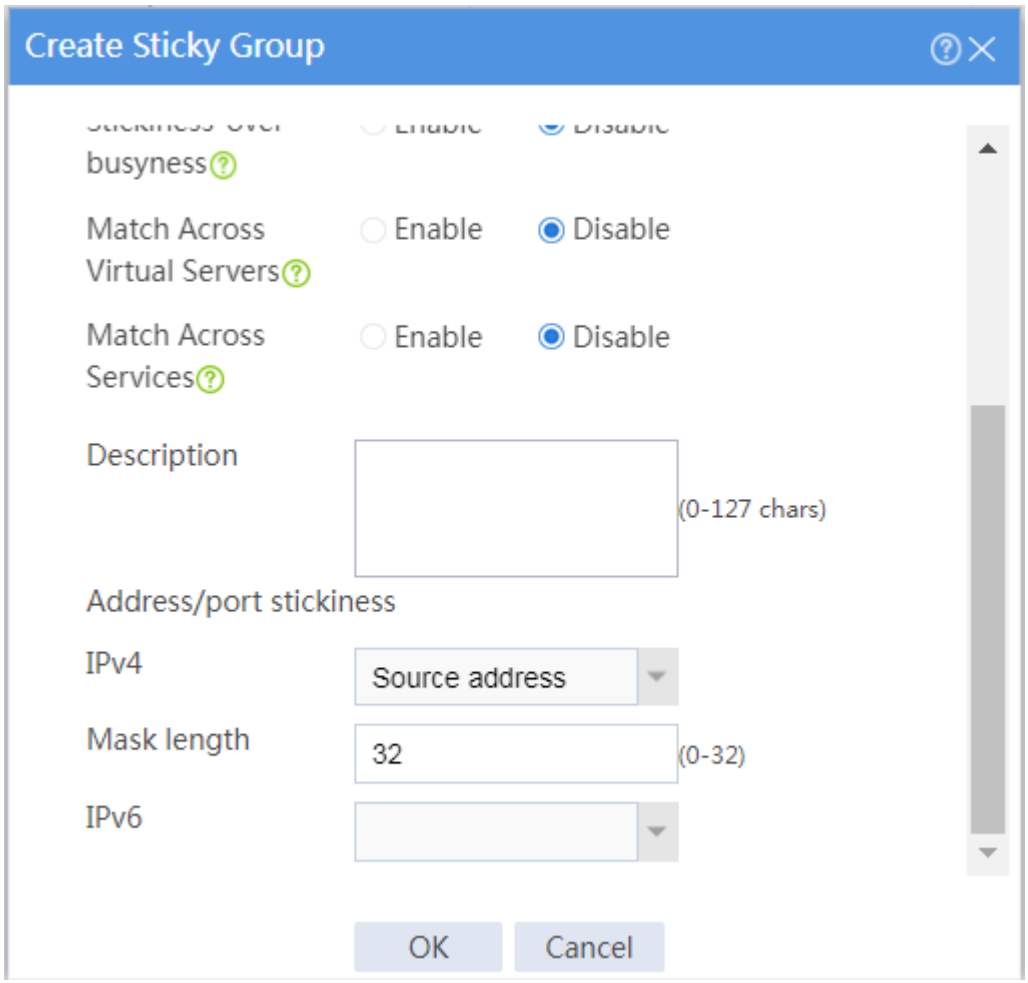


Figure 4 Creating sticky group sticky_group (part 2)



Click **OK**.

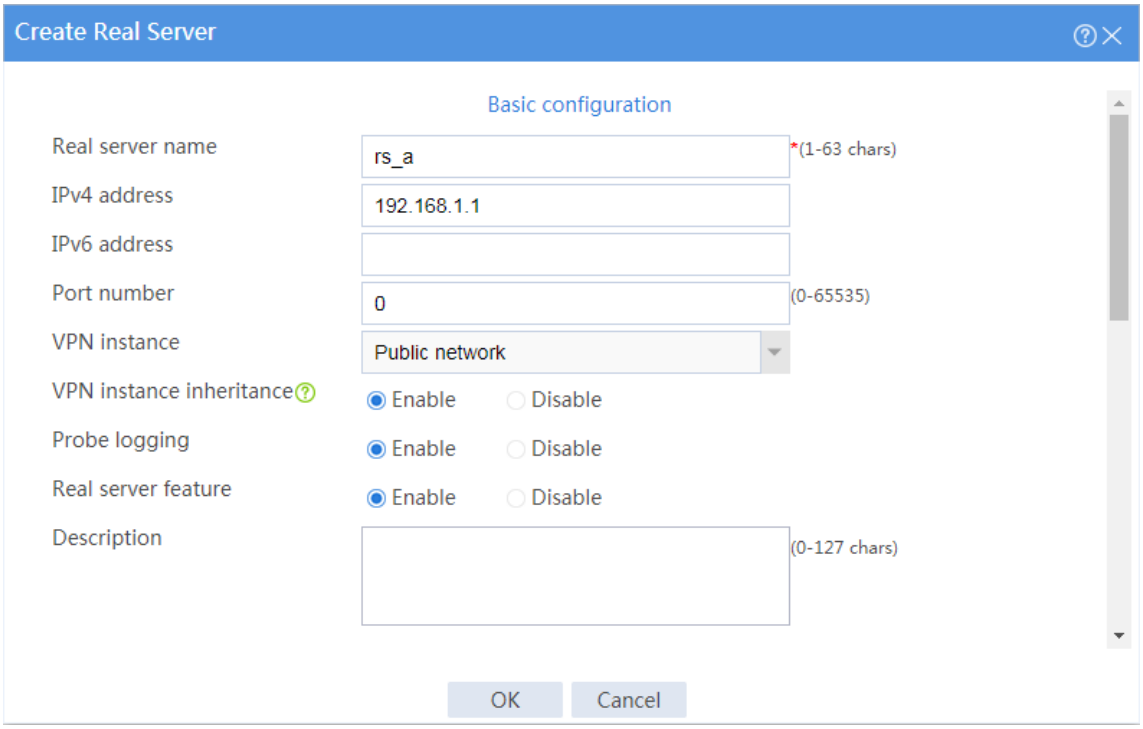
5. Create real servers.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Real Servers**.

Click **Create** to configure the real server **rs_a** as shown in Figure 5.

Figure 5 Creating real server rs_a



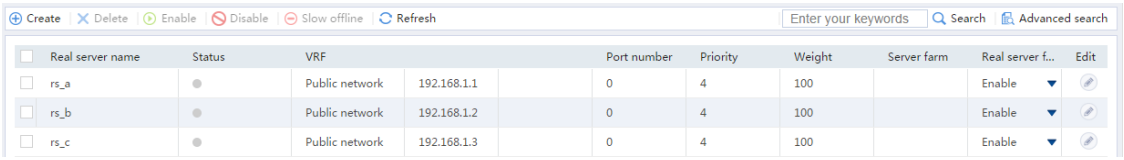
Click **OK**.

Configure real server **rs_b** and set its IP address to 192.168.1.2 in the same way you configure real server **rs_a**.

Configure real server **rs_c** and set its IP address to 192.168.1.3 in the same way you configure real server **rs_a**.

Display the configured real servers as shown in Figure 6.

Figure 6 Displaying the configured real servers



6. Create server farms.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Server Farms**.

Click **Create** to configure the server farm **sf1** as shown in Figure 7 and Figure 8.

Figure 7 Creating server farm sf1 (I)

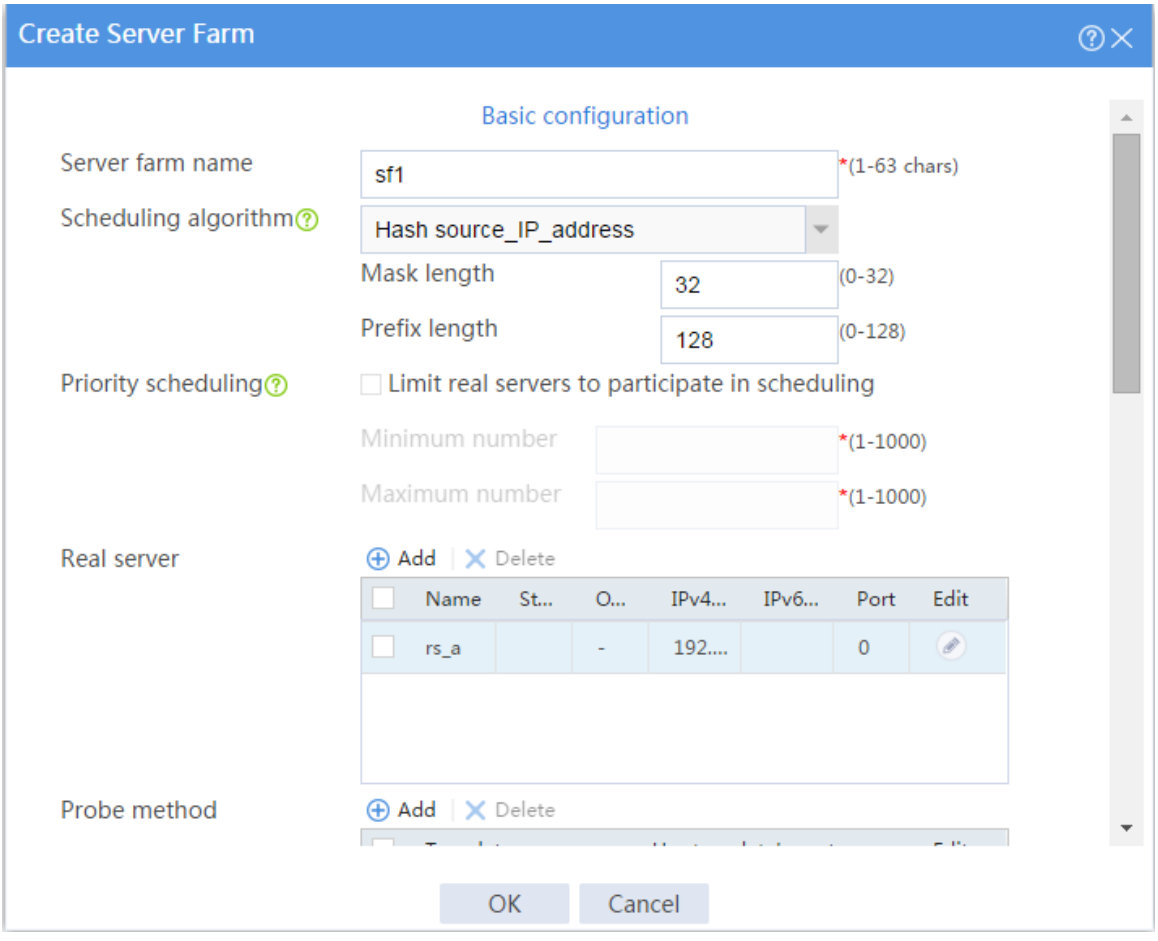
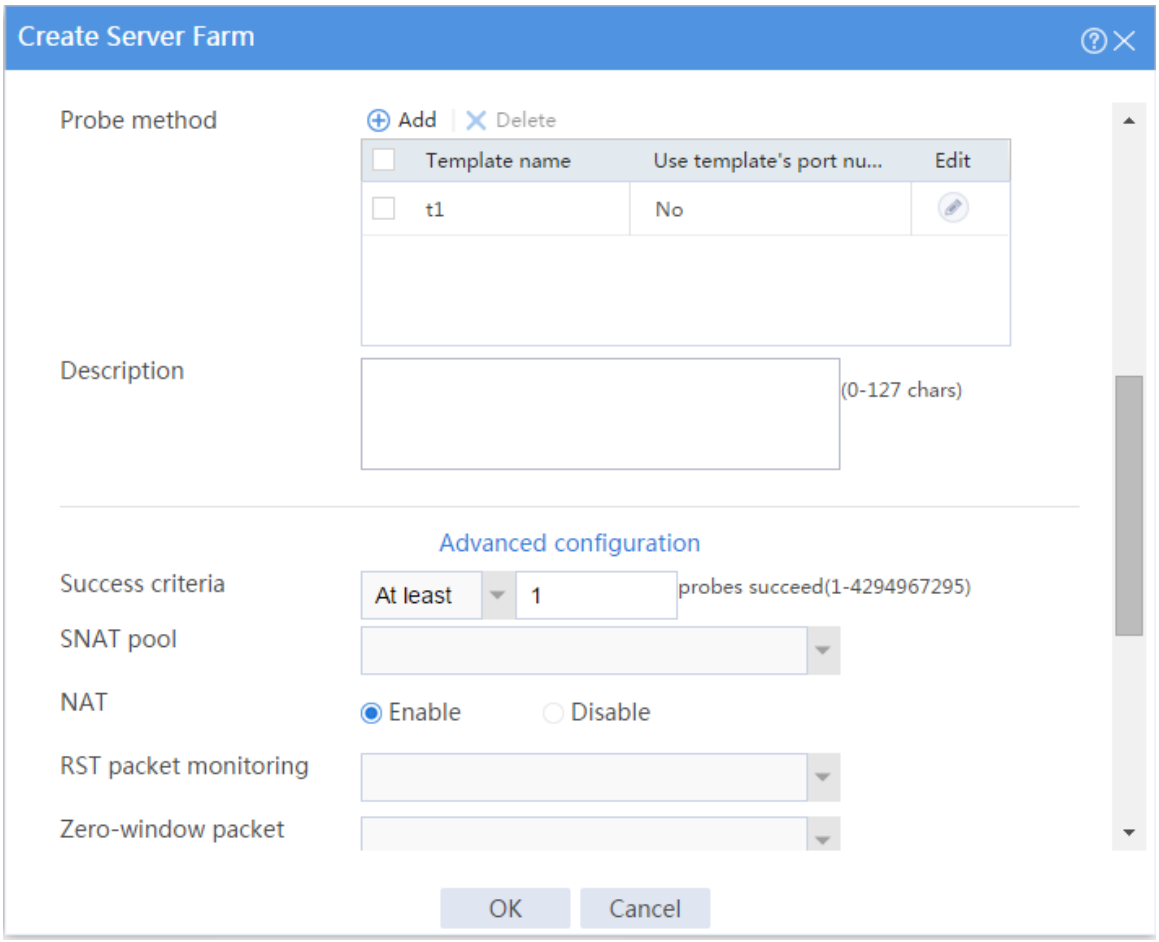


Figure 8 Creating server farm sf1 (II)



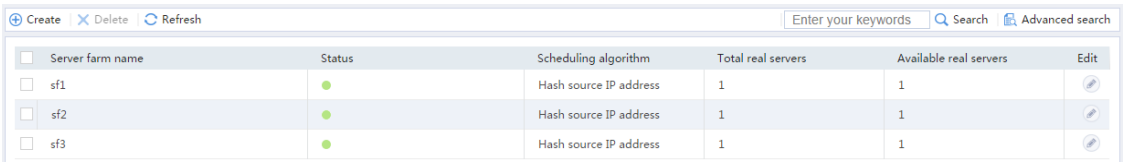
Click **OK**.

Configure server farm **sf2** and specify real server **rs_b** in the same way you configure server farm **sf1**.

Configure server farm **sf3** and specify real server **rs_c** in the same way you configure server farm **sf1**.

Display the configured server farms as shown in Figure 9.

Figure 9 Displaying the configured server farms



7. Create classes.

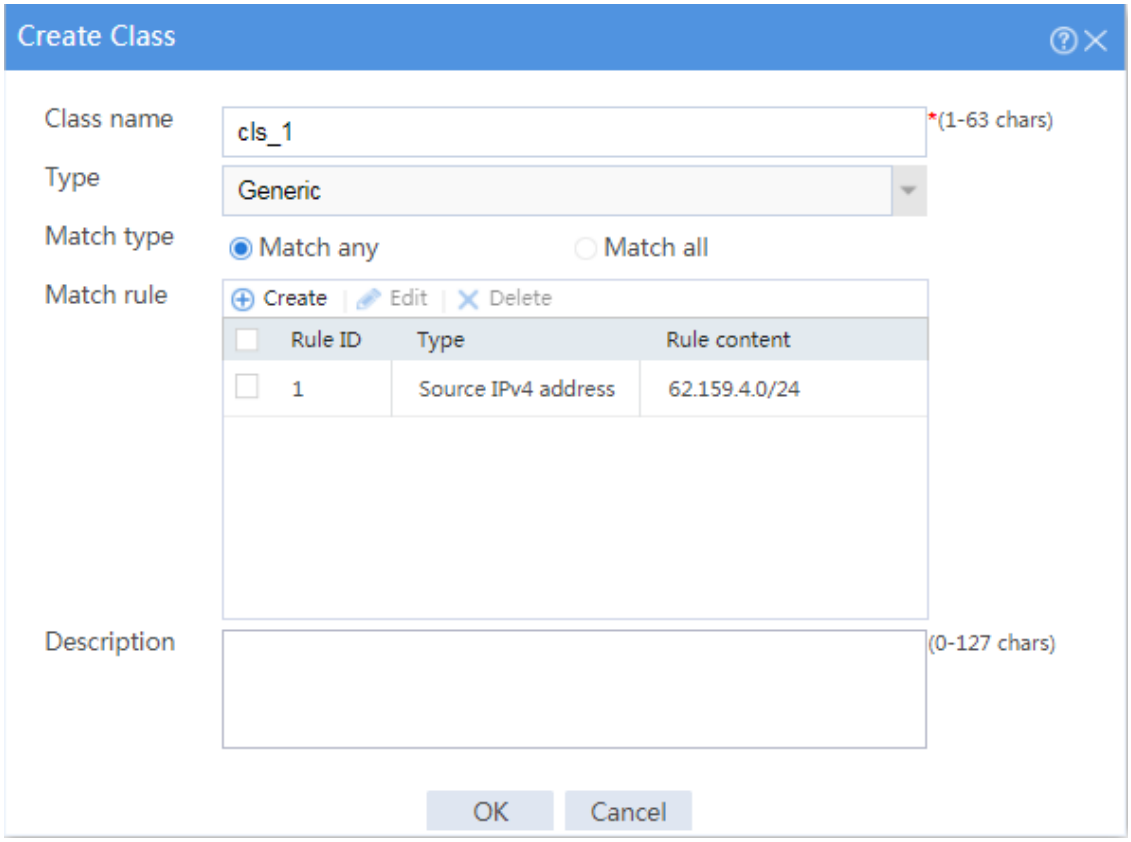
On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Advanced Policies**.

Click the **Class** tab.

Click **Create** to configure the class **cls_1** as shown in Figure 10.

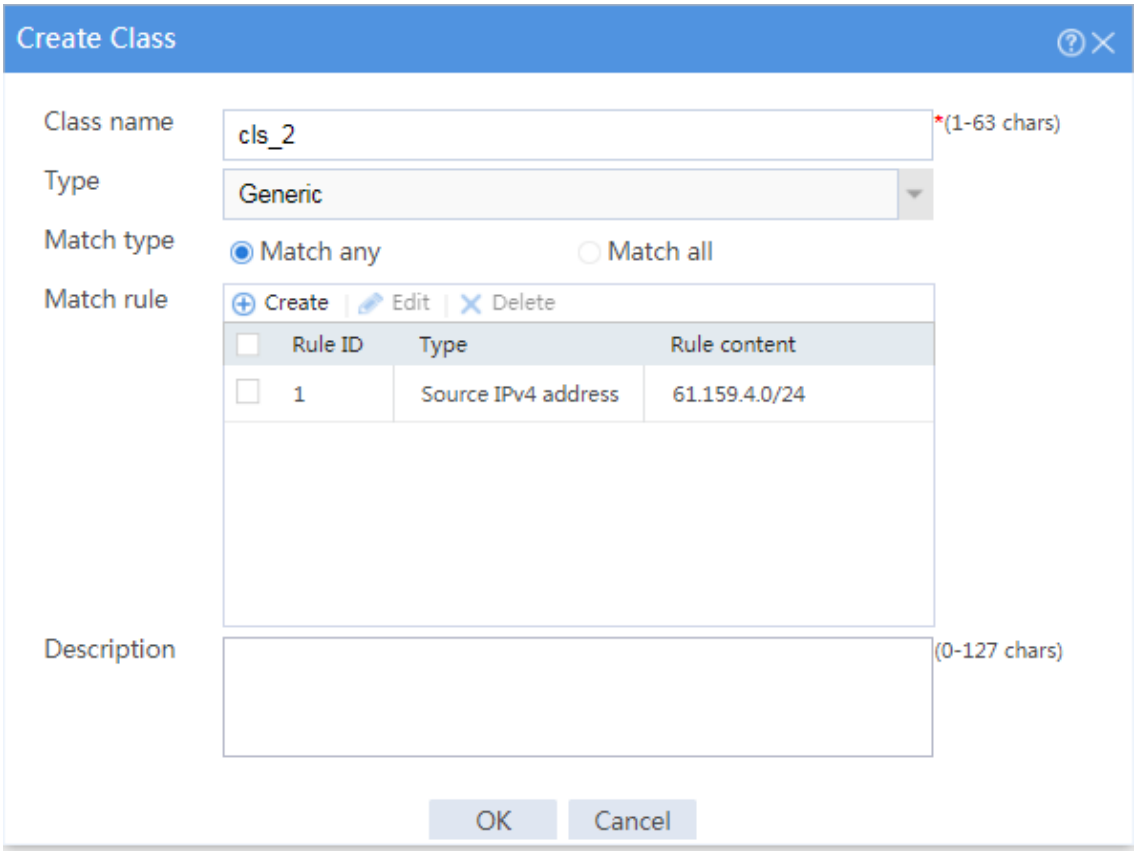
Figure 10 Creating class cls_1



Click **OK**.

Click **Create** to configure the class **cls_2** as shown in Figure 11.

Figure 11 Creating class cls_2



Click **OK**.

8. Create actions.

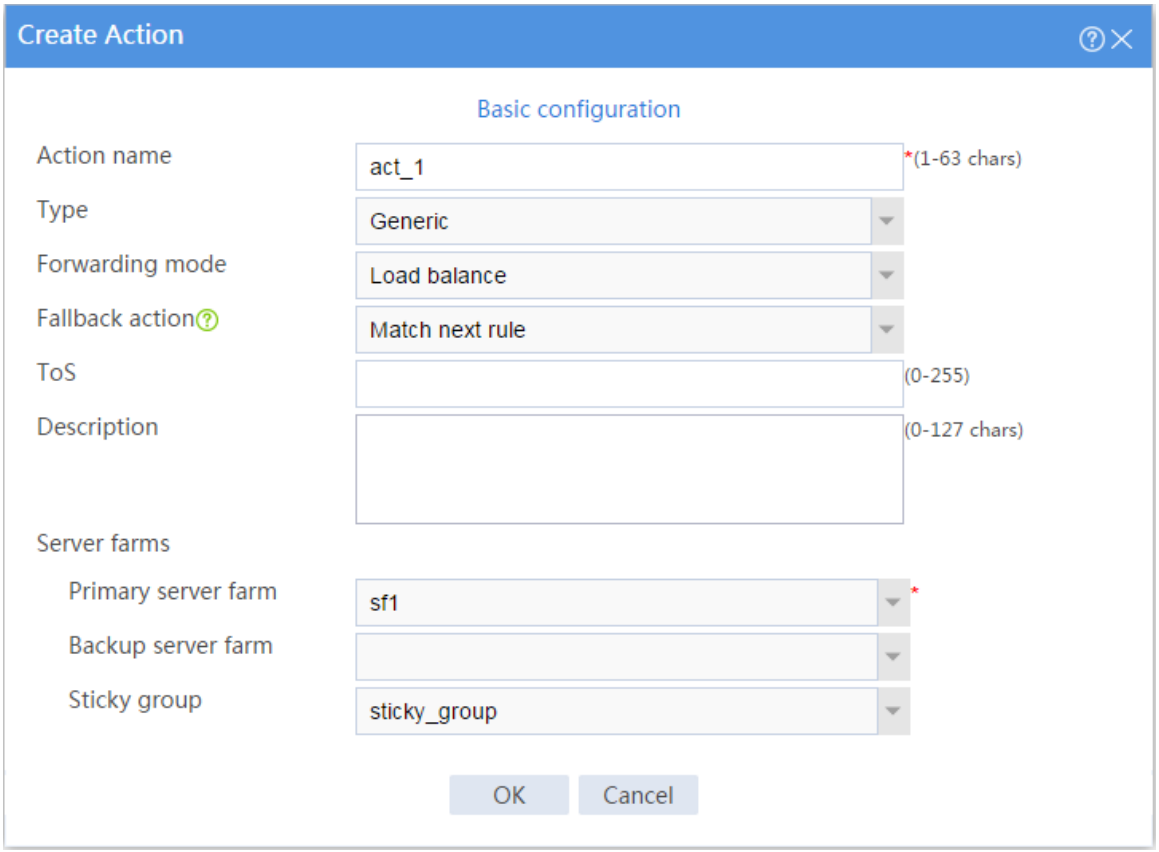
On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Advanced Policies**.

Click the **Action** tab.

Click **Create** to configure the action **act_1** as shown in Figure 12.

Figure 12 Creating action act_1



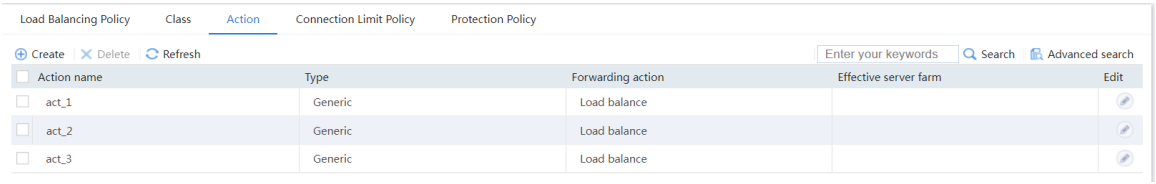
Click **OK**.

Configure action **act_2** and specify primary server farm **sf2** in the same way you configure action **act_1**.

Configure action **act_3** and specify primary server farm **sf3** in the same way you configure action **act_1**.

Display the configured actions as shown in Figure 13.

Figure 13 Displaying the configured actions



9. Create a load balancing policy.

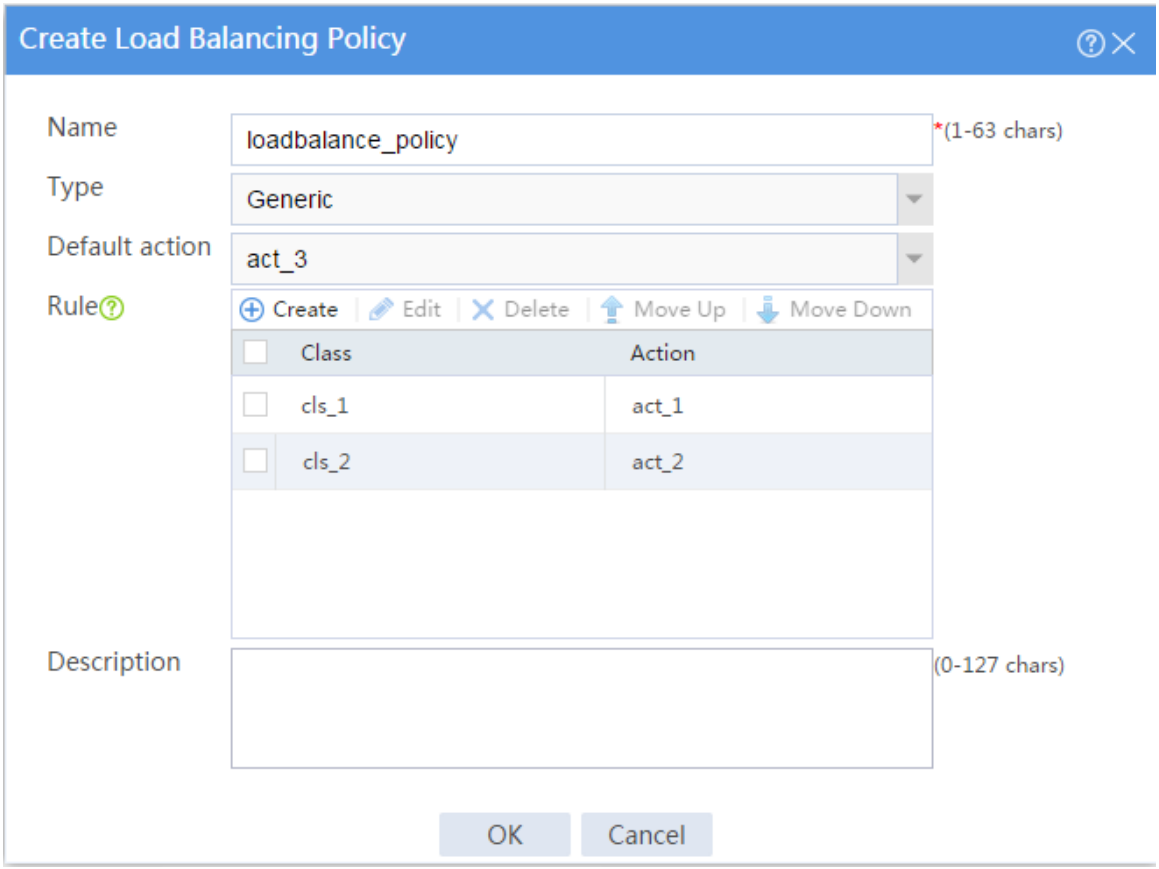
On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Advanced Policies**.

Click the **Load Balancing Policy** tab.

Click **Create** to configure the load balancing policy **loadbalance_policy** as shown in Figure 14.

Figure 14 Creating load balancing policy loadbalance_policy



Click **OK**.

10. Create a virtual server.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Virtual Servers**.

Click **Create** to configure the virtual server **vs** as shown in Figure 15 and Figure 17.

Figure 15 Creating virtual server vs (basic configuration, part 1)

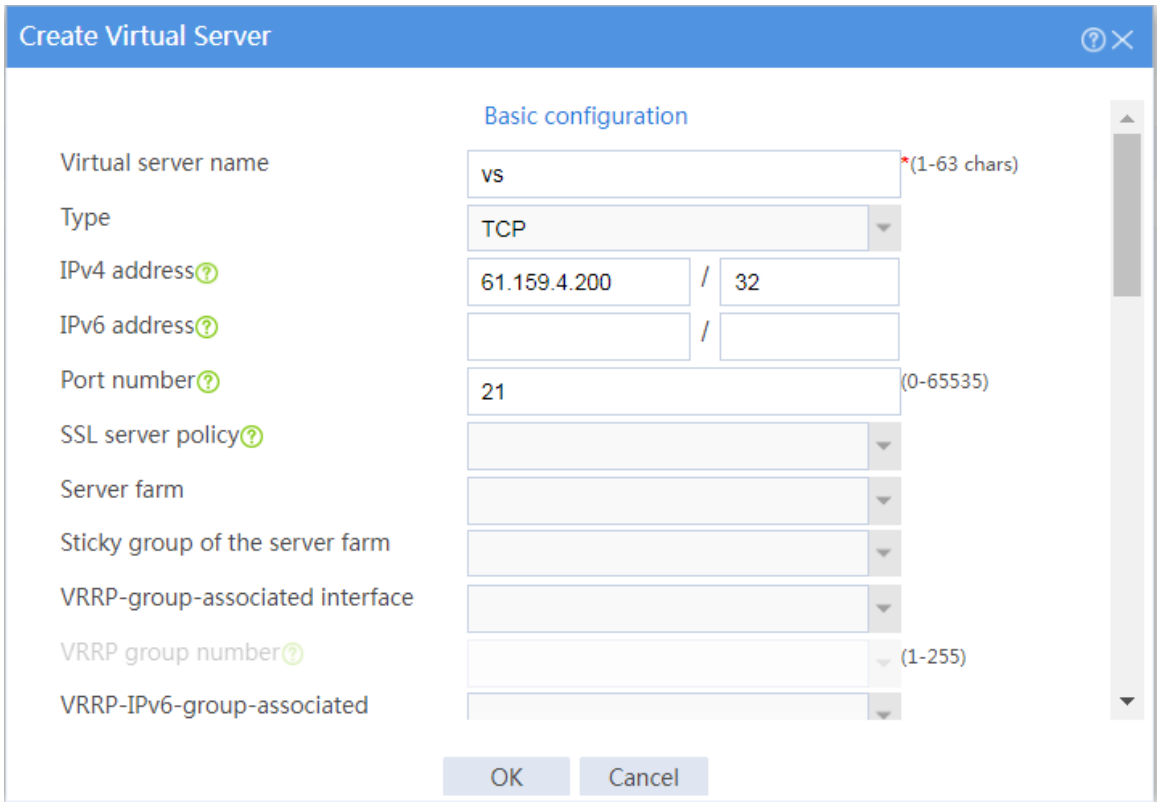


Figure 16 Creating virtual server vs (basic configuration, part 2)

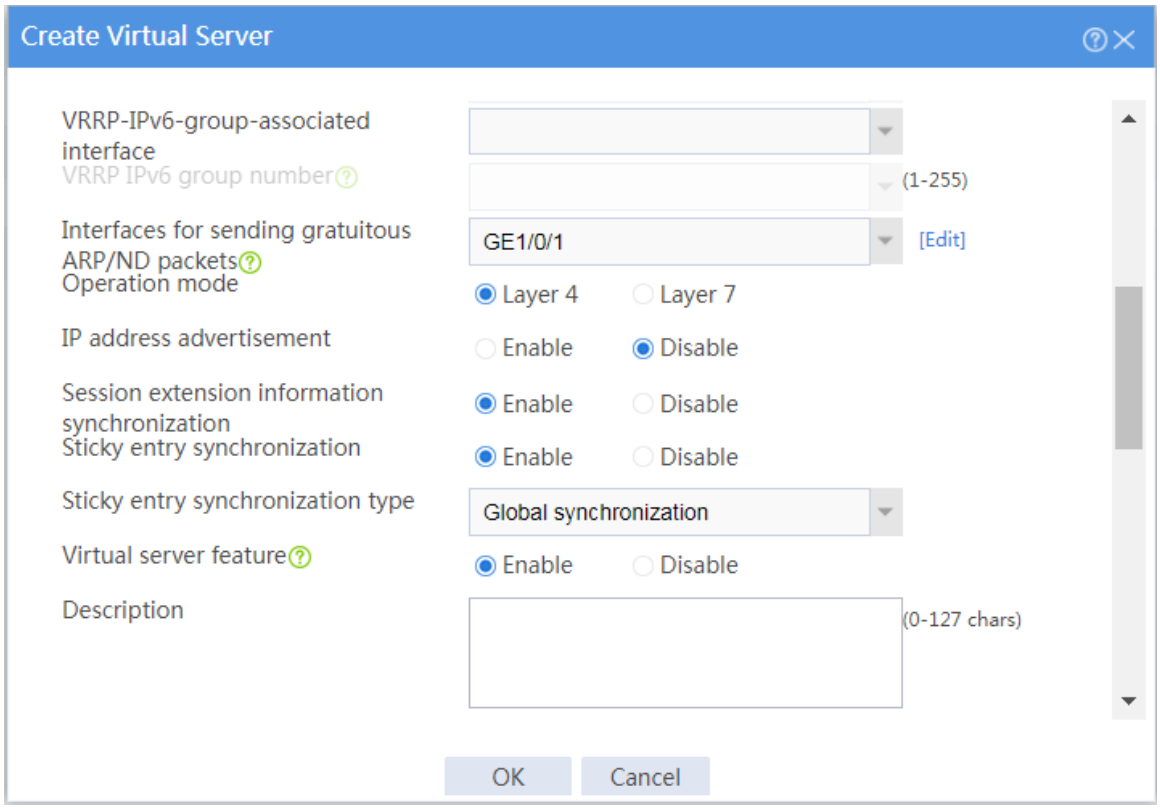
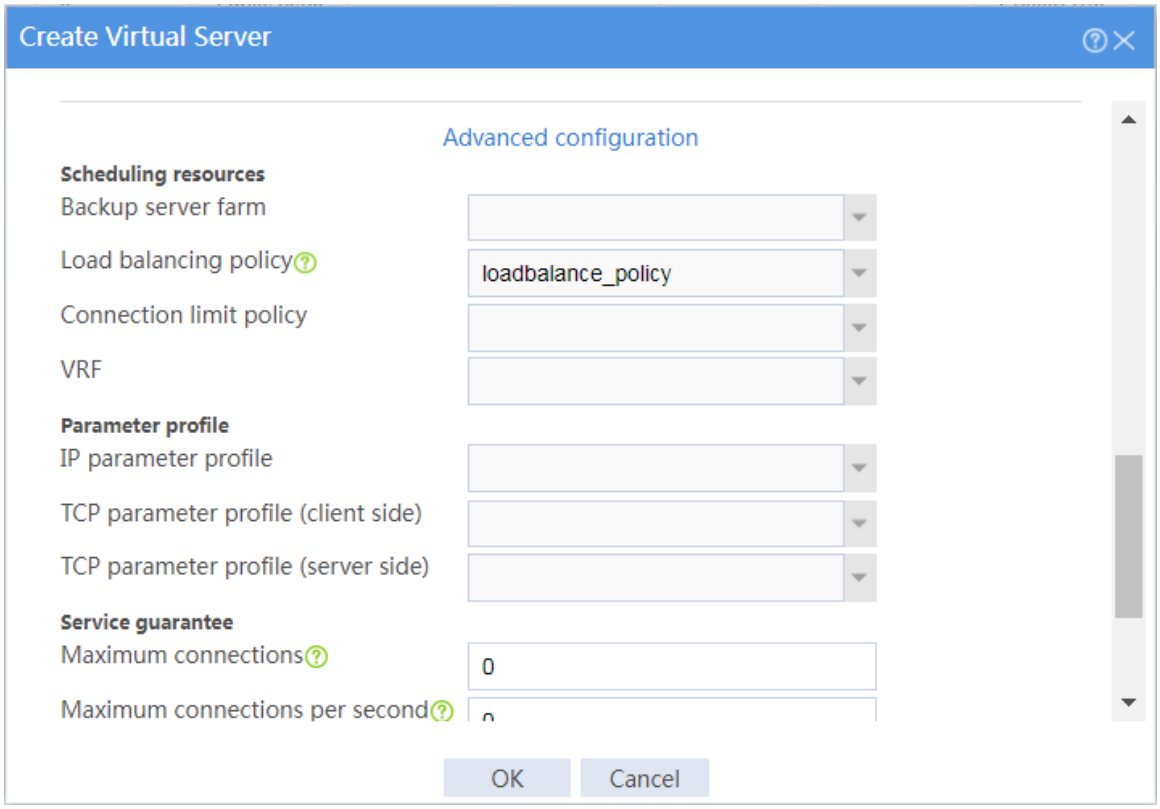


Figure 17 Creating virtual server vs (advanced configuration)



Click **OK**.

Verifying the configuration

1. Verify that Device assigns Sever A the FTP requests sourced from host IP address 62.159.4.1 and destined to virtual server IP address 61.159.4.100.

   # Access virtual server IP address 61.159.4.100 on the host with IP address 62.159.4.1.

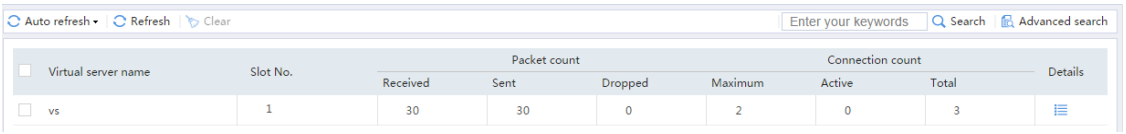
   ```
   C:\Users\system>ftp 61.159.4.200
   Connected to 61.159.4.200.
   220 FTP service ready.
   User (61.159.4.200:(none)): admin
   ```

```
331 Password required for admin.
Password:
230 User logged in.
ftp>
```

On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

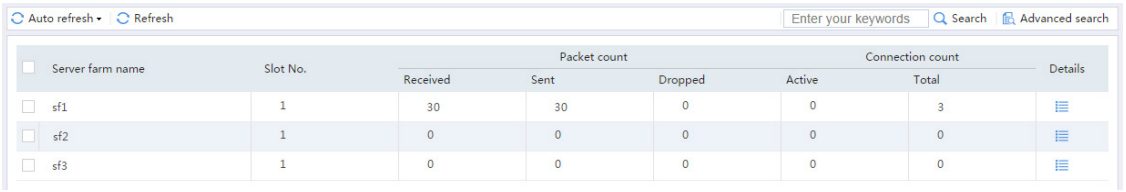
Figure 18 Displaying virtual server statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Servers Farms**. You can see that Device assigns FTP requests sourced from 62.159.4.1 to server farm **sf1**.

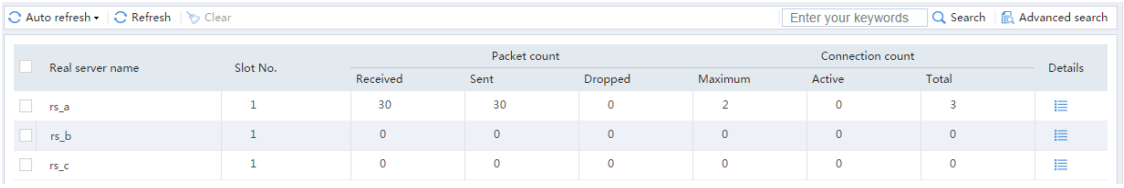
Figure 19 Displaying server farm statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Real Servers**. You can see that Device assigns FTP requests sourced from 62.159.4.1 to real server **rs_a**.

Figure 20 Displaying real server statistics



2. Verify that Device assigns Sever B the FTP requests sourced from host IP address 63.159.4.1 and destined to virtual server IP address 61.159.4.200.

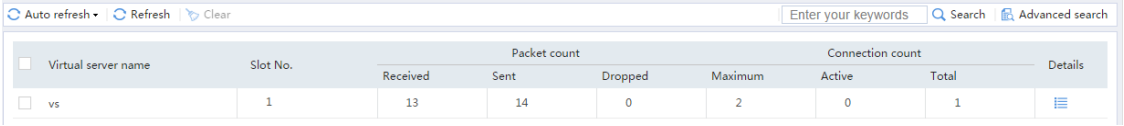
Access virtual server IP address 61.159.4.200 on the host with IP address 63.159.4.1.

```
C:\Users\system>ftp 61.159.4.200

Connected to 61.159.4.200.

220 FTP service ready.

User (61.159.4.200:(none)): admin

331 Password required for admin.

Password:

230 User logged in.

ftp>
```

On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

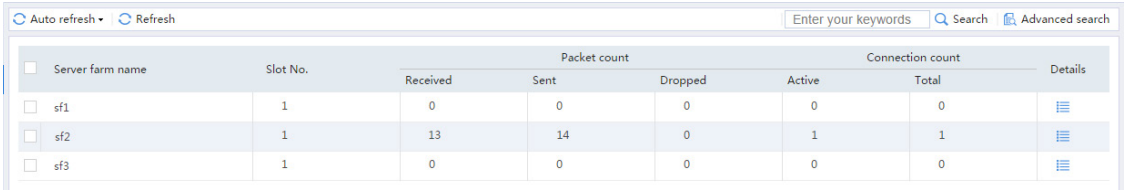
Figure 21 Displaying virtual server statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Servers Farms**. You can see that Device assigns FTP requests sourced from 63.159.4.1 to server farm **sf2**.

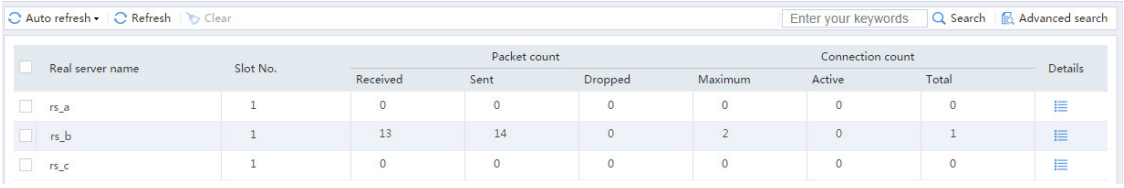
Figure 22 Displaying server farm statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Real Servers**. You can see that Device assigns FTP requests sourced from 63.159.4.1 to real server **rs_b**.

Figure 23 Displaying real server statistics



3. Verify that Device assigns Sever C the FTP requests sourced from host IP address 64.159.4.1 and destined to virtual server IP address 61.159.4.200.

Access virtual server IP address 61.159.4.200 on the host with IP address 64.159.4.1.

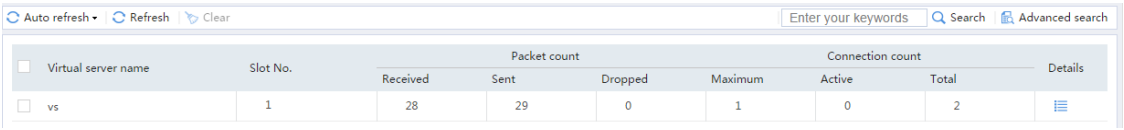
```
C:\Users\system>ftp 61.159.4.200
Connected to 61.159.4.200.
220 FTP service ready.
User (61.159.4.200:(none)): admin
331 Password required for admin.
```

```
Password:

230 User logged in.

ftp>
```

On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

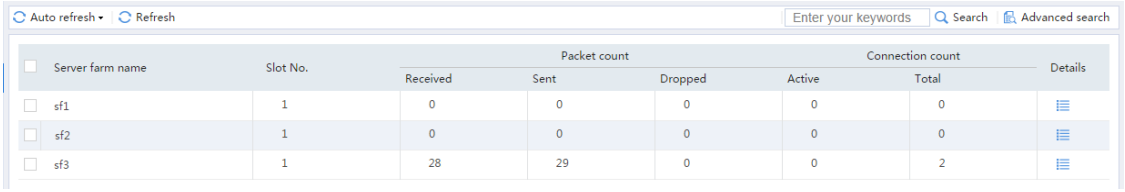
Figure 24 Displaying virtual server statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Servers Farms**. You can see that Device assigns FTP requests sourced from 64.159.4.1 to server farm **sf3**.

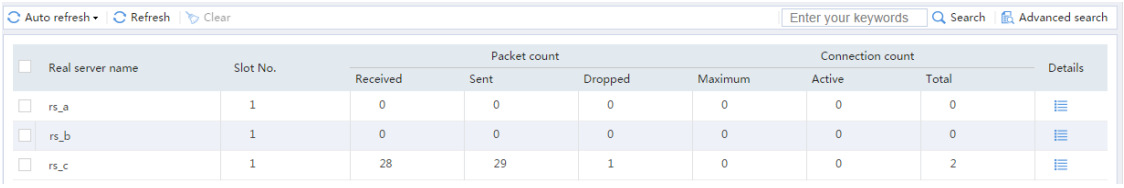
Figure 25 Displaying server farm statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Real Servers**. You can see that Device assigns FTP requests sourced from 64.159.4.1 to real server **rs_c**.

Figure 26 Displaying real server statistics

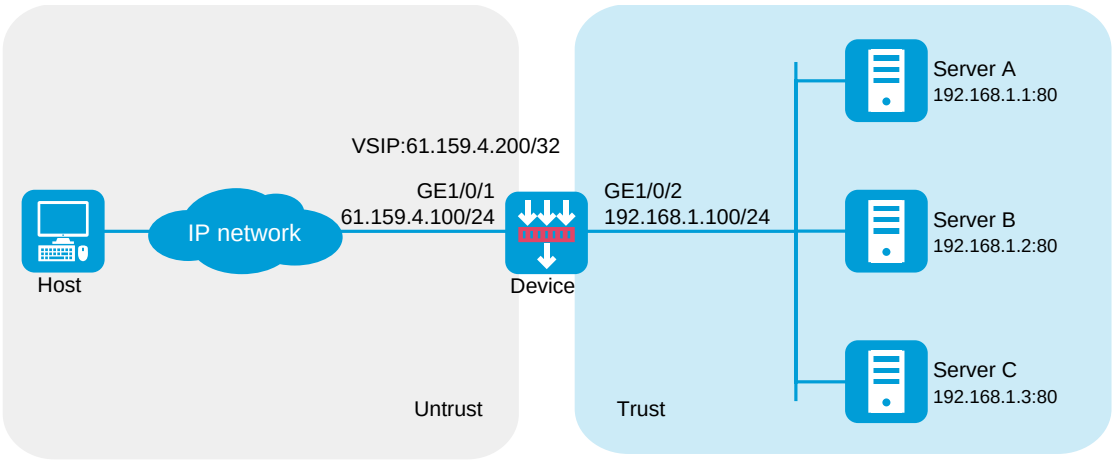


Example: Configuring Layer 7 server load balancing

Network configuration

As shown in Figure 27, an enterprise uses Server A, Server B, and Server C to provide HTTP services. Configure server load balancing to load balance HTTP requests from Host. The device assigns requests whose URLs contain sports, government, and news to Server A; assigns requests whose URLs contain finance, technology, and shopping to Server B; and assigns other requests to Server C.

Figure 27 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Untrust** security zone.

- On the **IPv4 Address** tab, enter the IP address and mask length of the interface. In this example, enter 61.159.4.100/24.
- Use the default settings for other parameters.
- Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 192.168.1.100/24 in the same way you configure GE 1/0/1.

2. Configure security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy named **Untrust-to-Local**:

- Enter policy name **Untrust-to-Local**.
- Select source zone **Untrust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 address **61.159.4.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

Configure a security policy named **Local-to-Trust**:

- Enter policy name **Local-to-Trust**.
- Select source zone **Local**.
- Select destination zone **Trust**.

- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 address **192.168.1.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

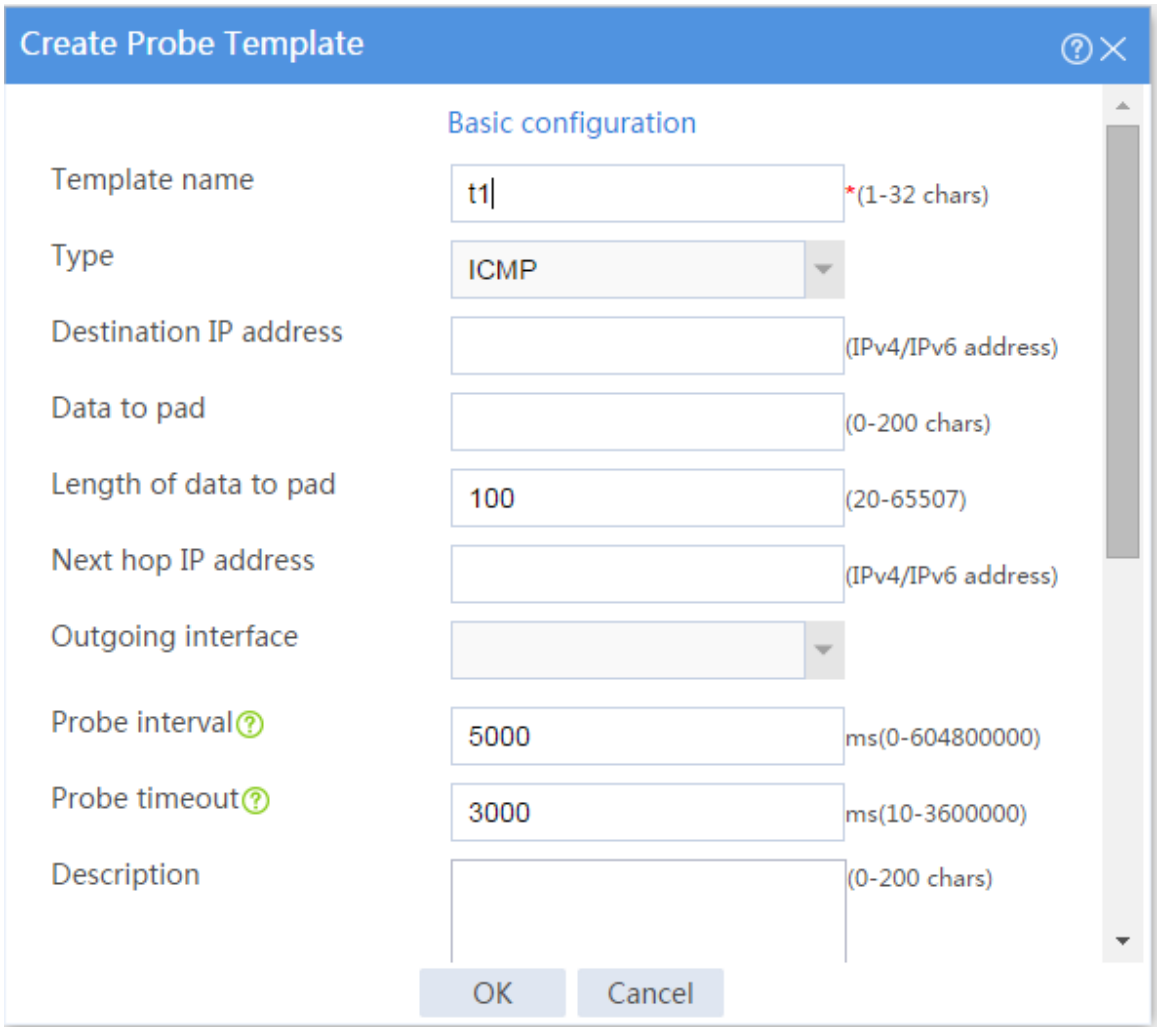
3. Create an ICMP-type probe template.

On the top navigation bar, click **Objects**.

From the navigation pane, select **Health Monitoring**.

Click **Create** to configure the probe template **t1** as shown in Figure 28.

Figure 28 Creating probe template t1



Click **OK**.

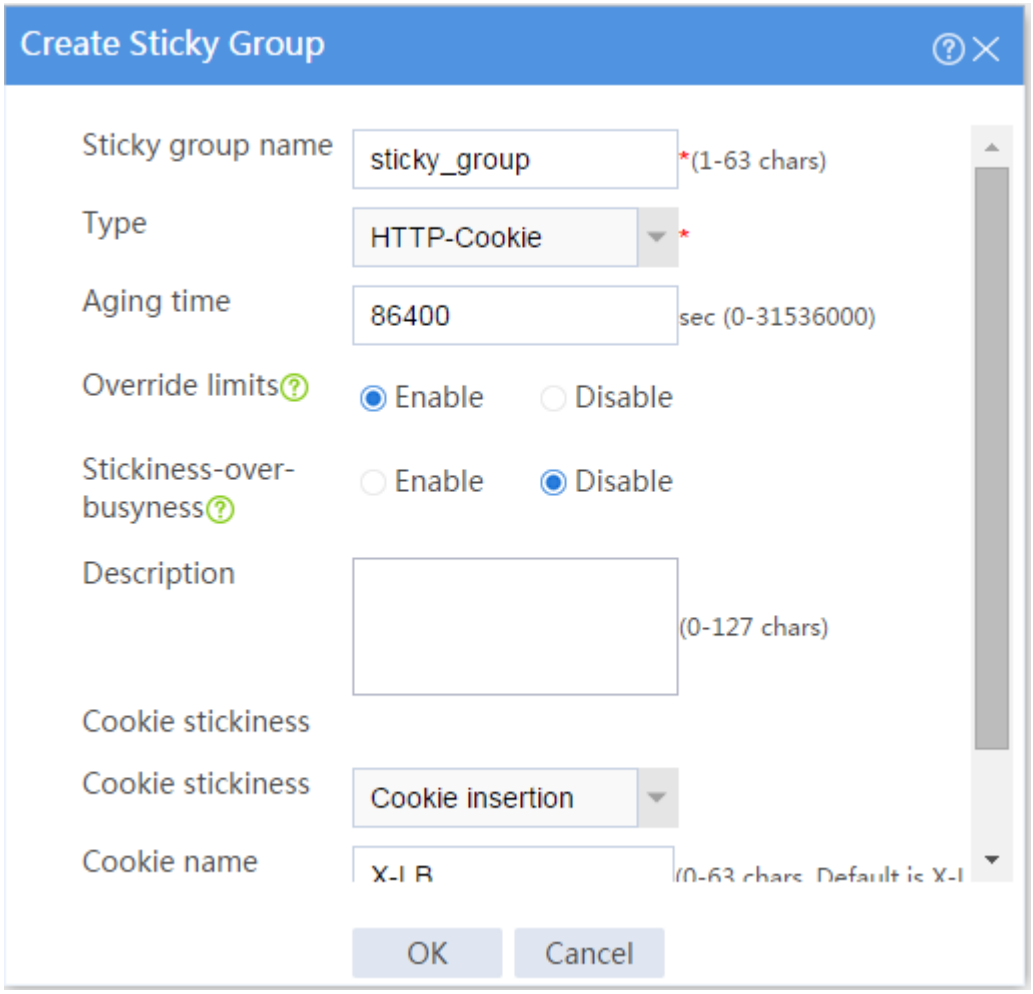
4. Create an HTTP cookie sticky group.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Common Configuration** > **Sticky Groups**.

Click **Create** to configure the sticky group **sticky_group** as shown in Figure 29.

Figure 29 Creating sticky group sticky_group



Click **OK**.

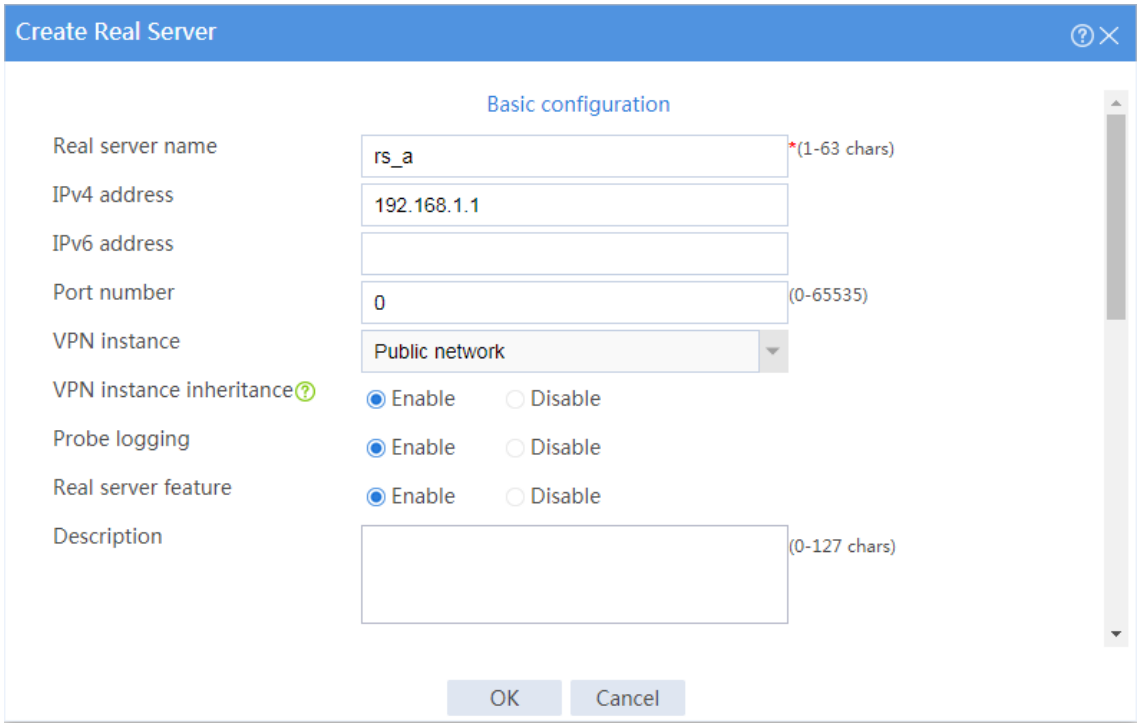
5. Create real servers.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Real Servers**.

Click **Create** to configure the real server **rs_a** as shown in Figure 30.

Figure 30 Creating real server rs_a



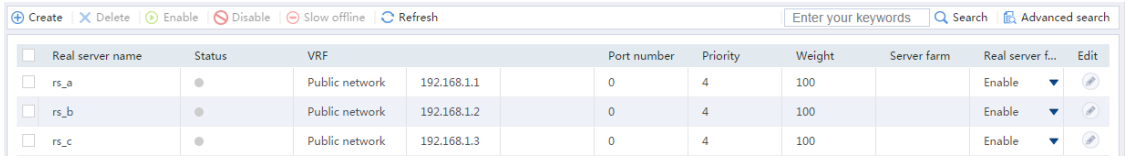
Click **OK**.

Configure real server **rs_b** and set its IP address to 192.168.1.2 in the same way you configure real server **rs_a**.

Configure real server **rs_c** and set its IP address to 192.168.1.3 in the same way you configure real server **rs_a**.

Display the configured real servers as shown in Figure 31.

Figure 31 Displaying the configured real servers



6. Create server farms.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Server Farms**.

Click **Create** to configure the server farm **sf1** as shown in Figure 32 and Figure 33.

Figure 32 Creating server farm sf1 (I)

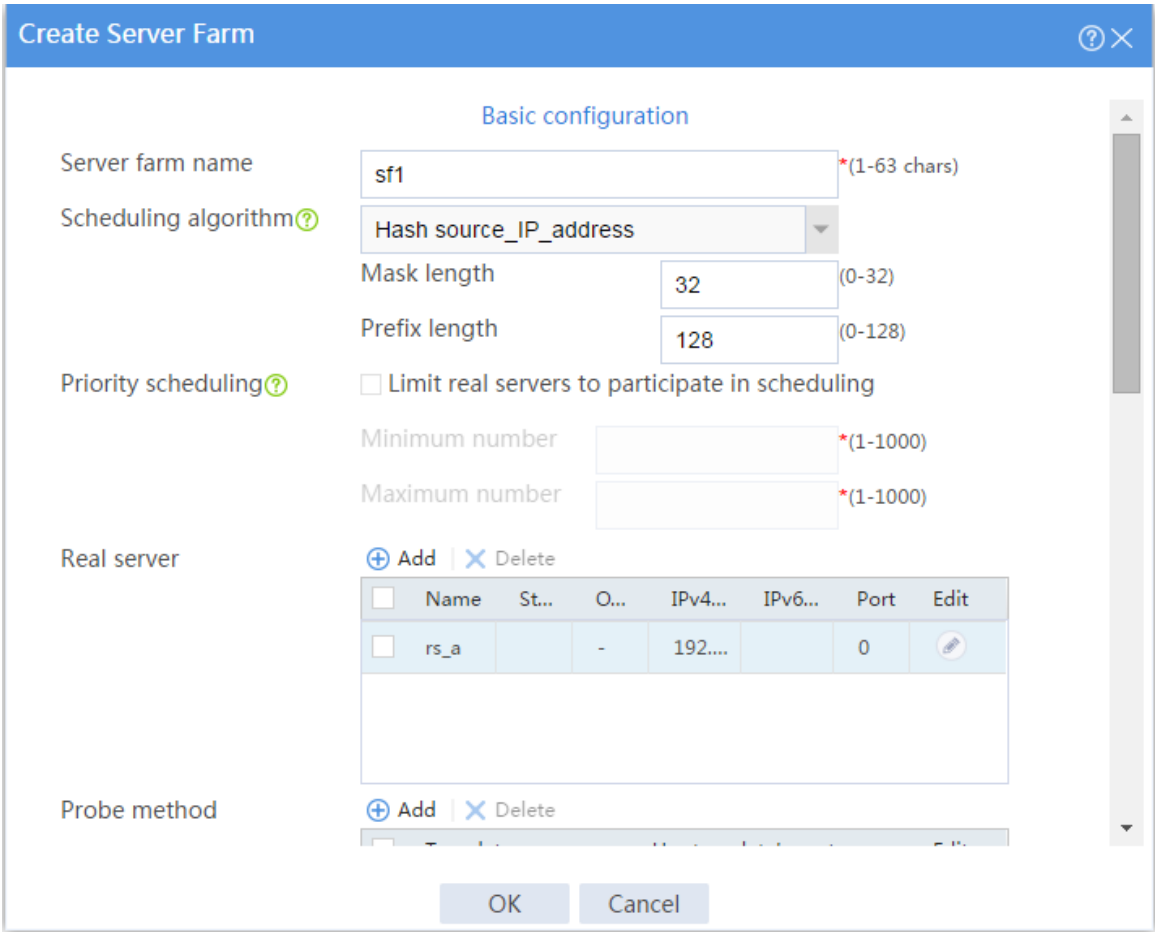
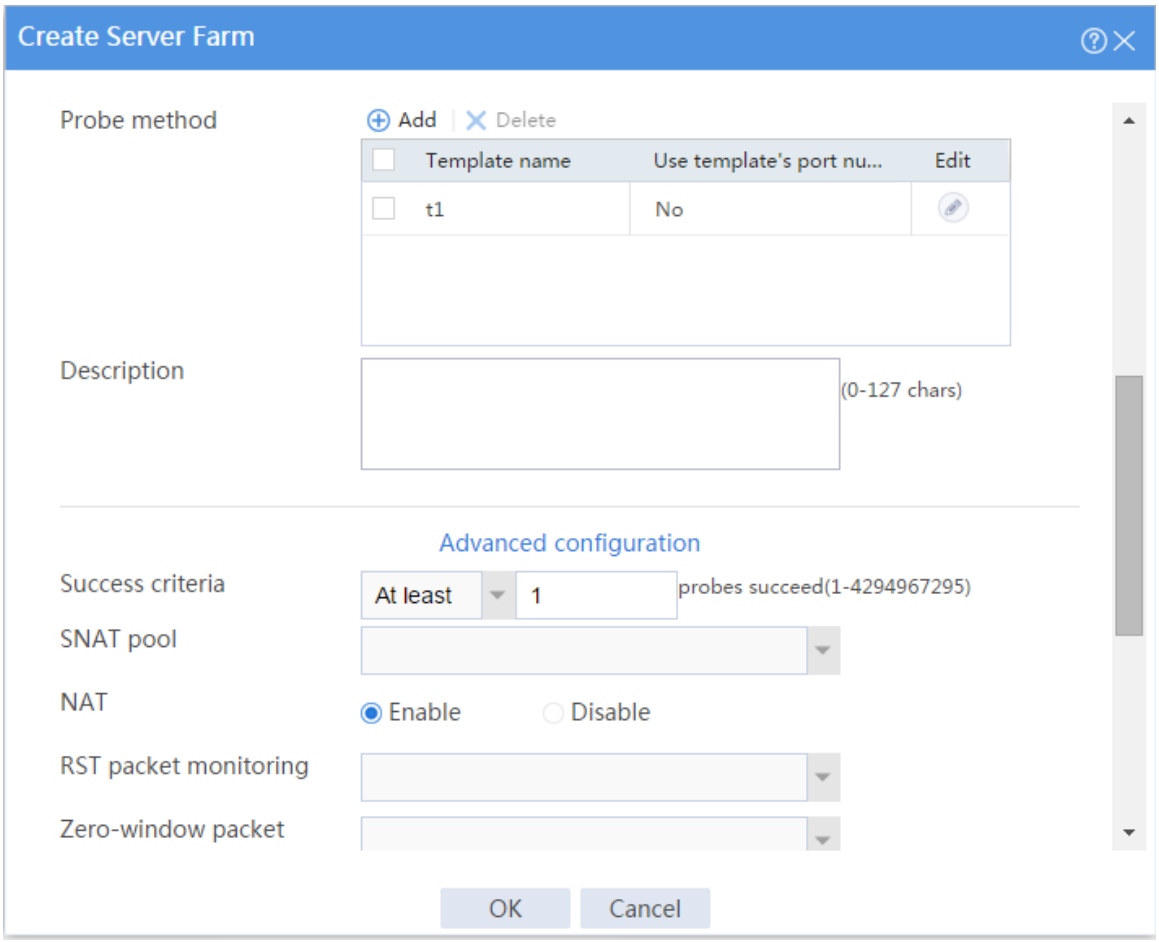


Figure 33 Creating server farm sf1 (II)



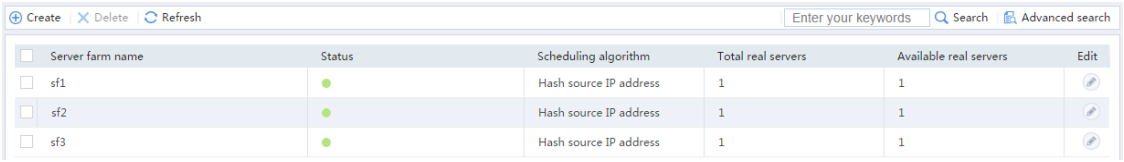
Click **OK**.

Configure server farm **sf2** and specify real server **rs_b** in the same way you configure server farm **sf1**.

Configure server farm **sf3** and specify real server **rs_c** in the same way you configure server farm **sf1**.

Display the configured server farms as shown in Figure 34.

Figure 34 Displaying the configured server farms



7. Create classes.

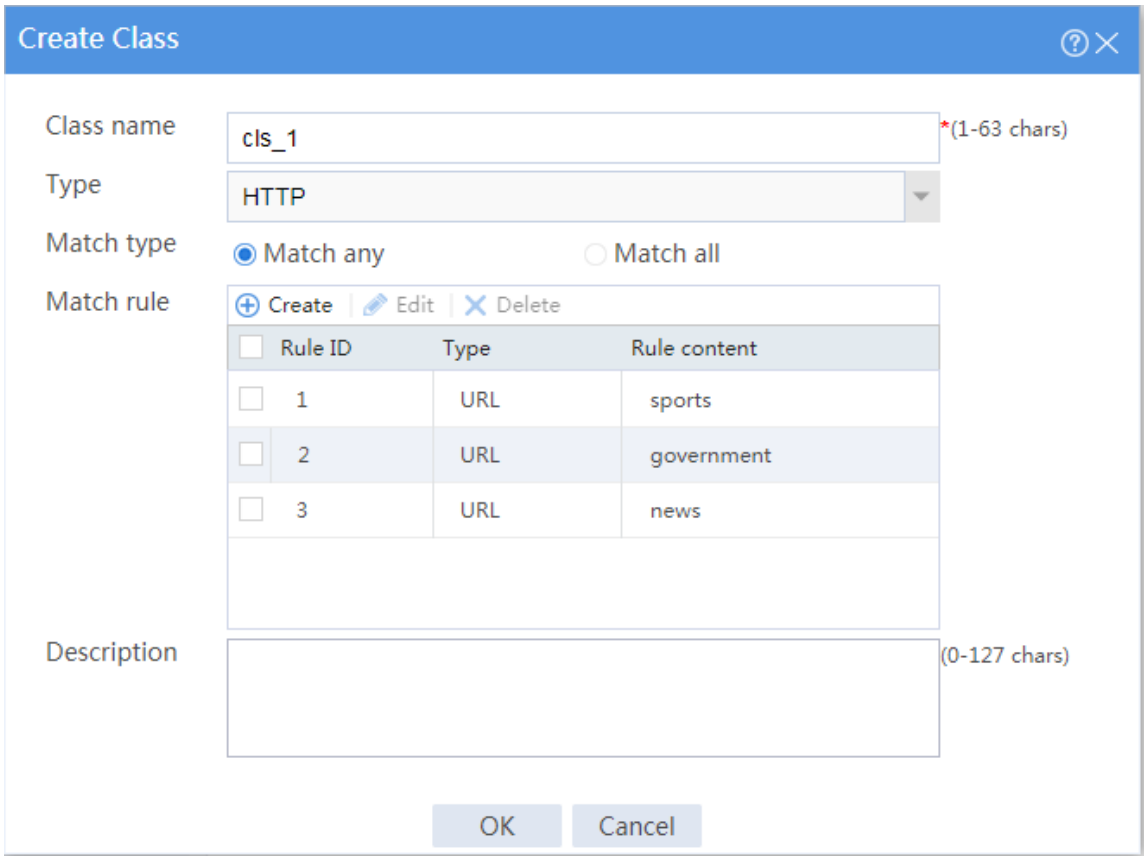
   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Advanced Policies**.

   # Click the **Class** tab.

   # Click **Create** to configure the class **cls_1** as shown in Figure 35.

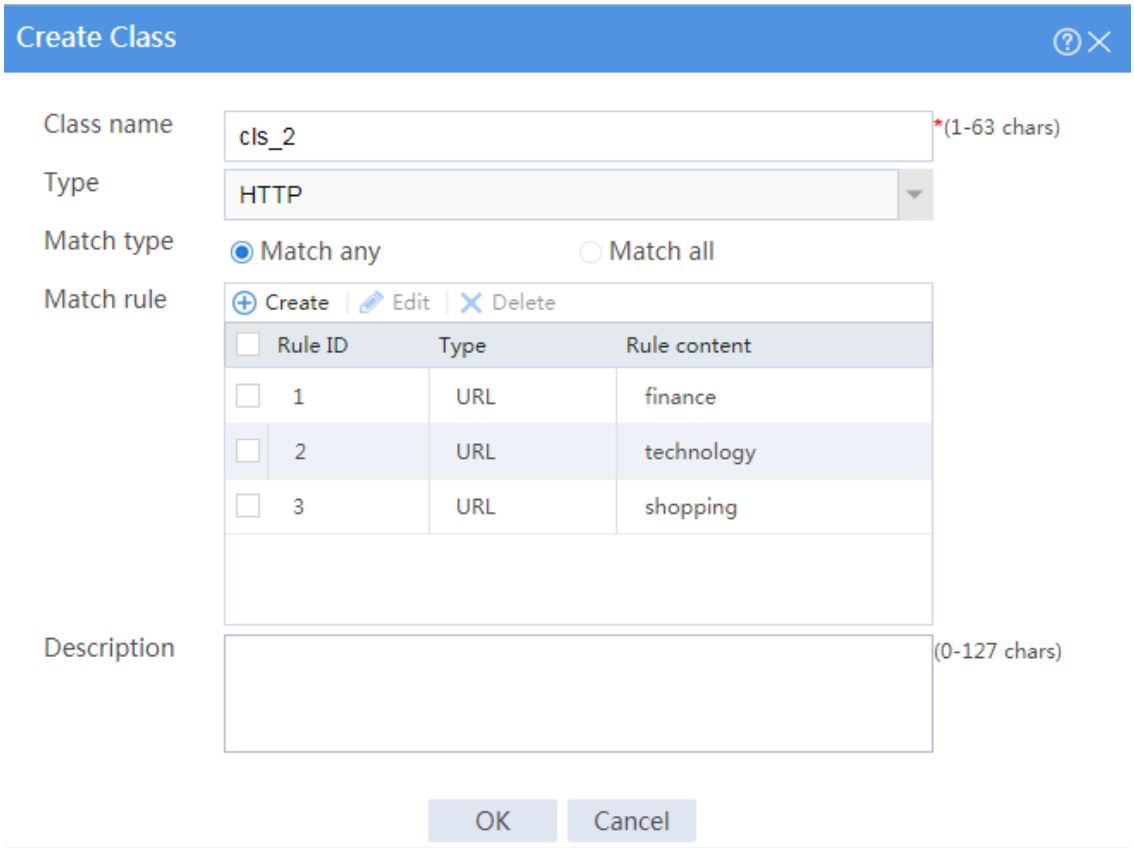
Figure 35 Creating class cls_1



Click **OK**.

Click **Create** to configure the class **cls_2** as shown in Figure 36.

Figure 36 Creating class cls_2



Click **OK**.

8. Create actions.

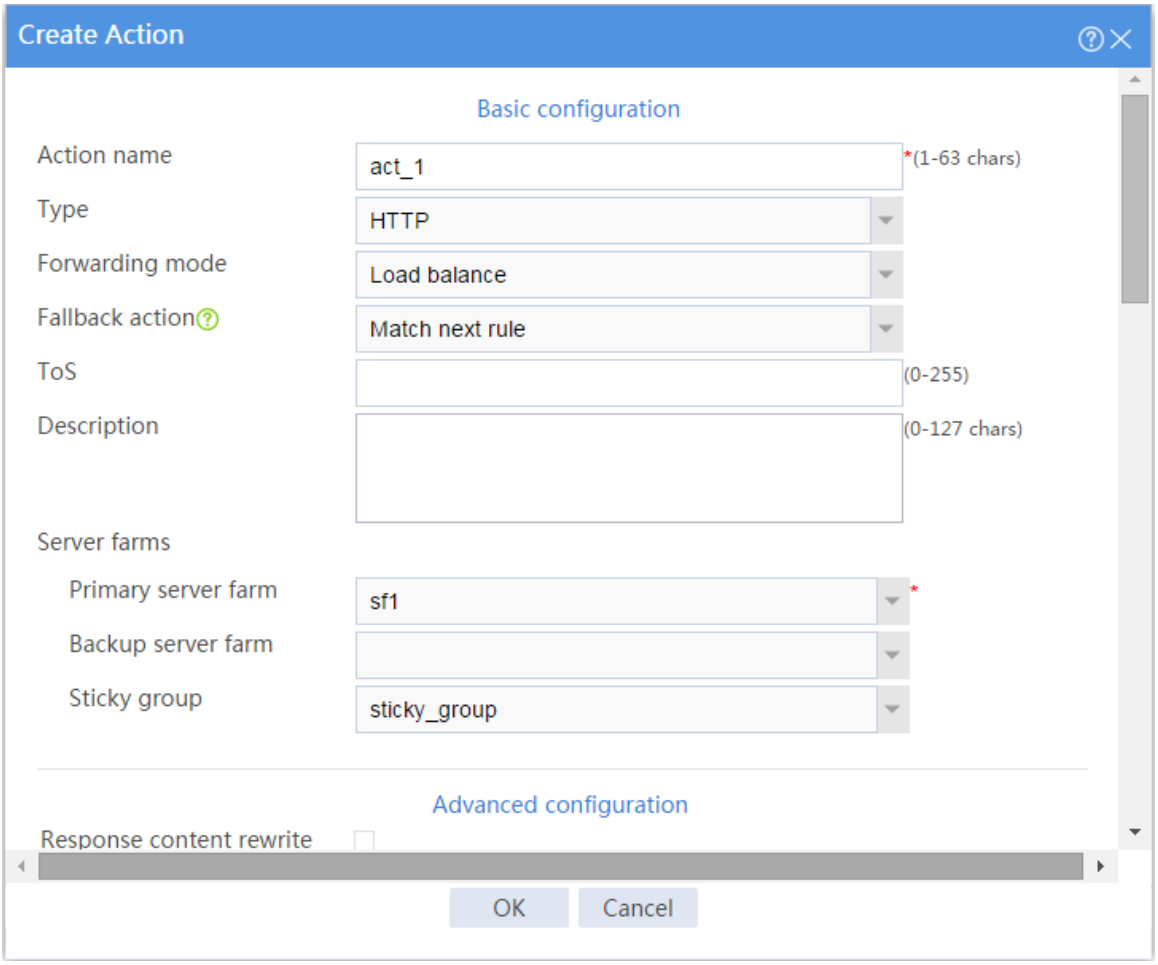
On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Advanced Policies**.

Click the **Action** tab.

Click **Create** to configure the action **act_1** as shown in Figure 37.

Figure 37 Creating action act_1



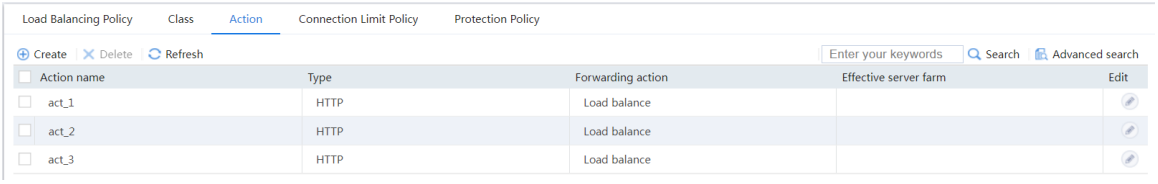
Click **OK**.

Configure action **act_2** and specify primary server farm **sf2** in the same way you configure action **act_1**.

Configure action **act_3** and specify primary server farm **sf3** in the same way you configure action **act_1**.

Display the configured actions as shown in Figure 38.

Figure 38 Displaying the configured actions



9. Create a load balancing policy.

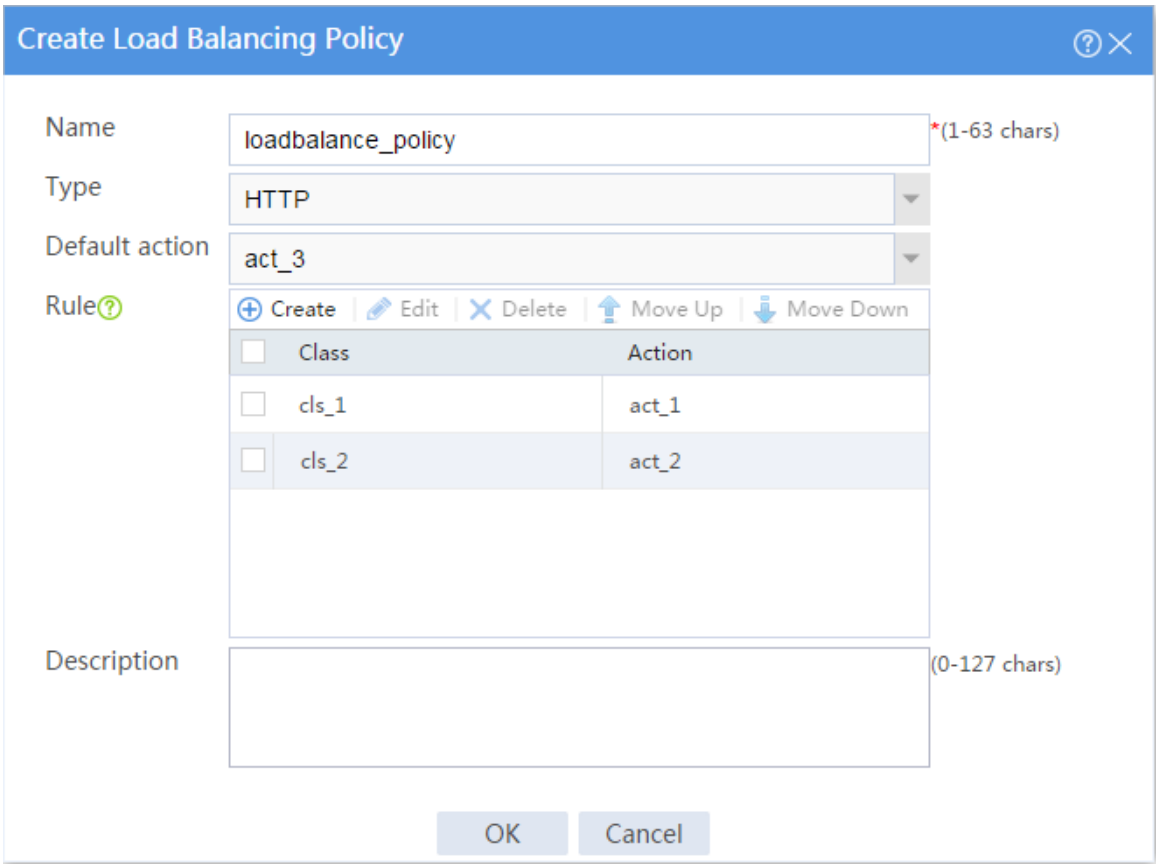
On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Advanced Policies**.

Click the **Load Balancing Policy** tab.

Click **Create** to configure the load balancing policy **loadbalance_policy** as shown in Figure 39.

Figure 39 Creating load balancing policy loadbalance_policy



Click **OK**.

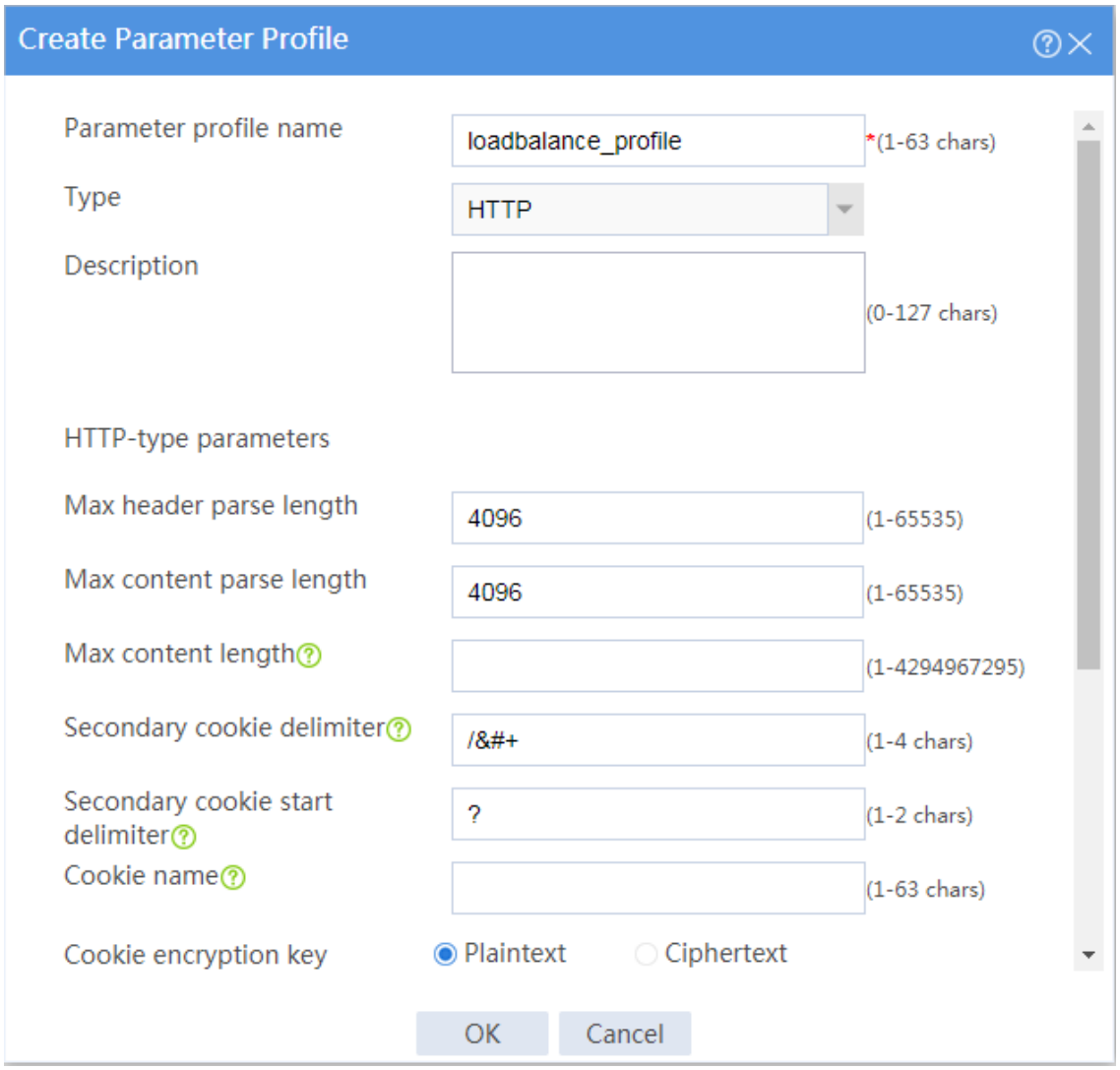
10. Create an HTTP-type parameter profile.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Parameter Profiles**.

Click **Create** to configure the parameter profile **loadbalance_profile** as shown in Figure 40.

Figure 40 Creating parameter profile loadbalance_profile



Click **OK**.

11. Create a virtual server.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Load Balancing** > **Server Load Balancing** > **Virtual Servers**.

Click **Create** to configure the virtual server **vs** as shown in Figure 41 and Figure 43.

Figure 41 Creating virtual server vs (basic configuration, part 1)

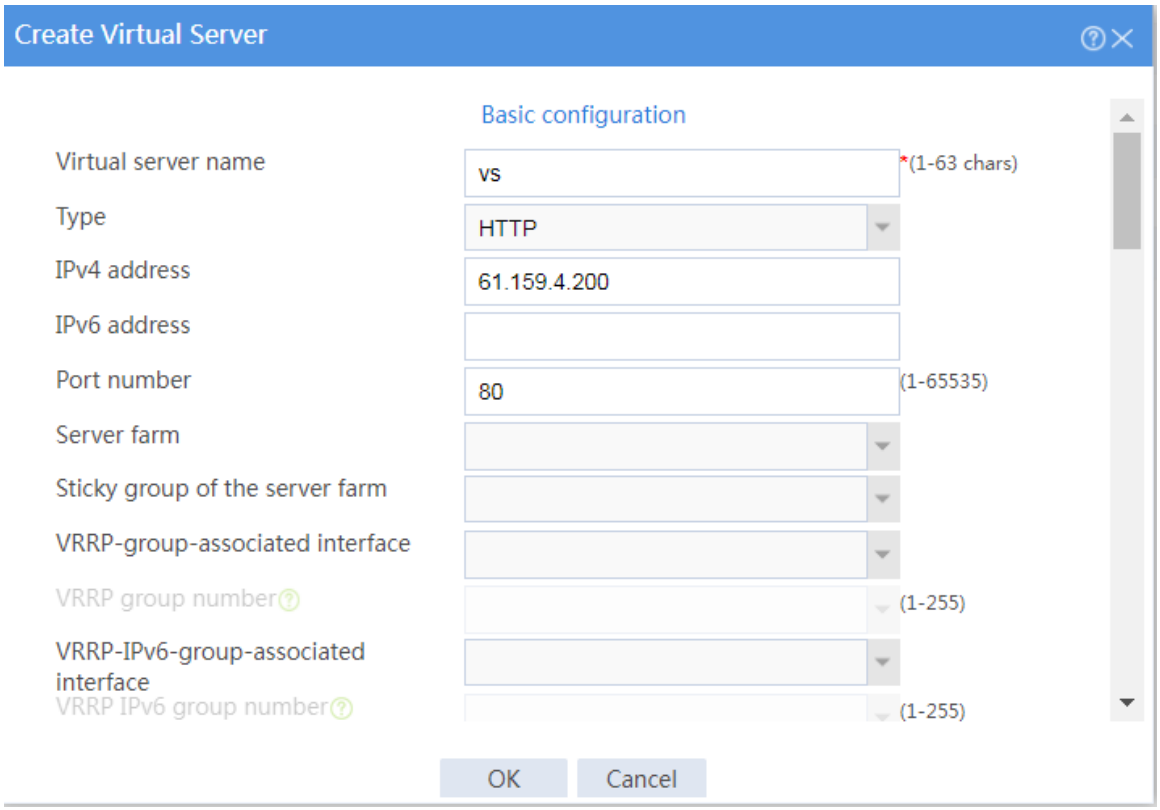


Figure 42 Creating virtual server vs (basic configuration, part 2)

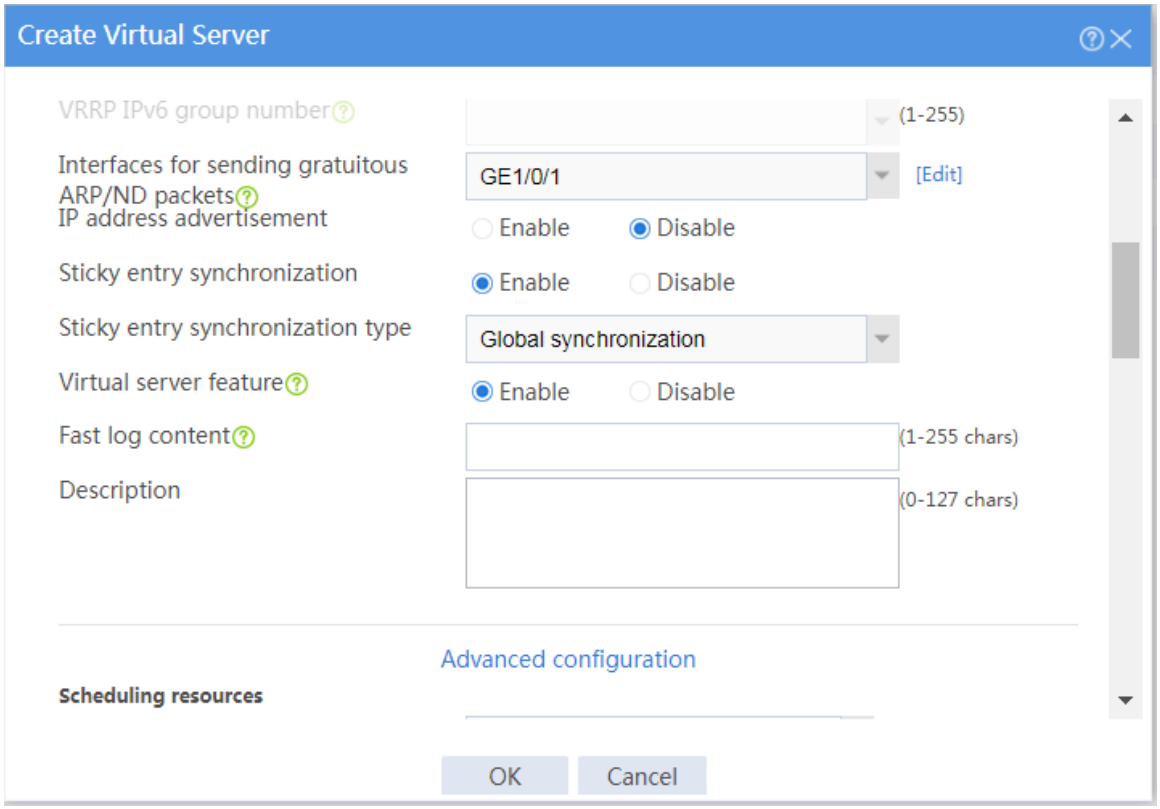
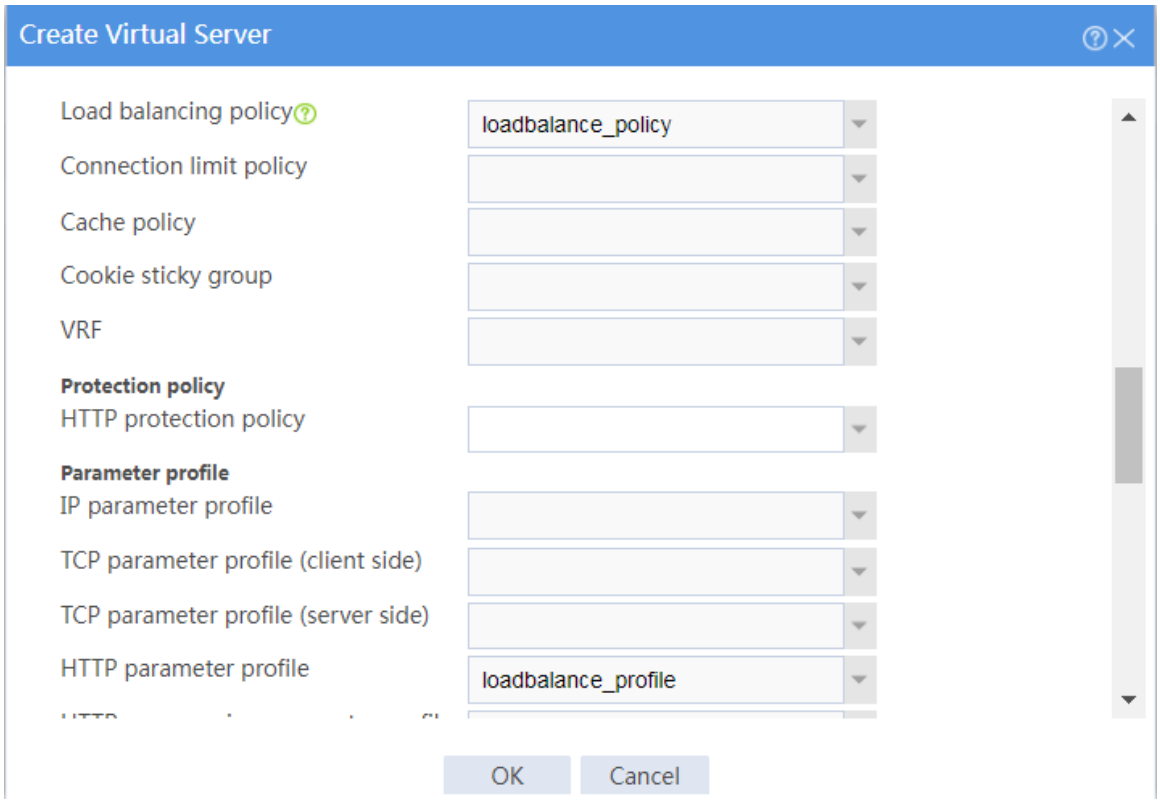


Figure 43 Creating virtual server vs (advanced configuration)



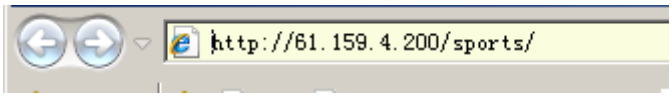
Click **OK**.

Verifying the configuration

1. Verify that the device assigns Sever A the HTTP request with URL **http://61.159.4.200/sports/**.

   # Access **http://61.159.4.200/sports/** on Host.

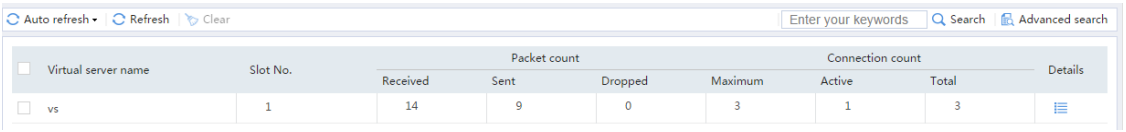
Figure 44 Accessing the HTTP service



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

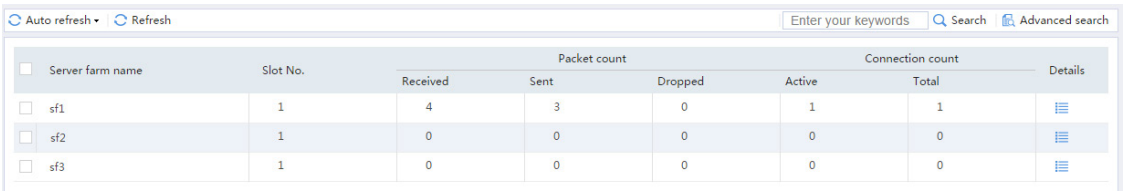
Figure 45 Displaying virtual server statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Servers Farms**. You can see that the device assigns the HTTP request containing URL **http://61.159.4.200/sports/** to server farm **sf1**.

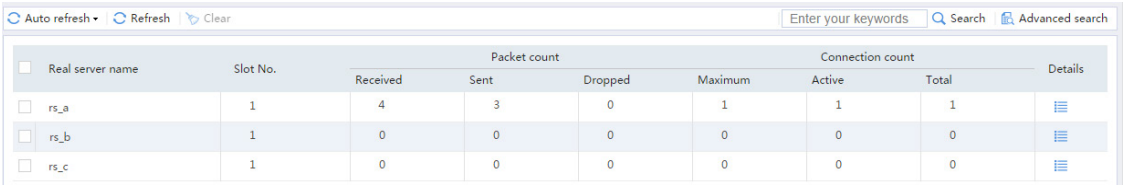
Figure 46 Displaying server farm statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Real Servers**. You can see that the device assigns the HTTP request containing URL **http://61.159.4.200/sports/** to real server **rs_a**.

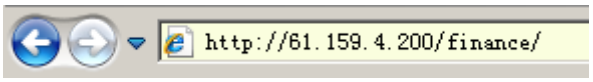
Figure 47 Displaying real server statistics



2. Verify that the device assigns Sever B the HTTP request with URL **http://61.159.4.200/finance/**.

Access **http://61.159.4.200/finance/** on Host.

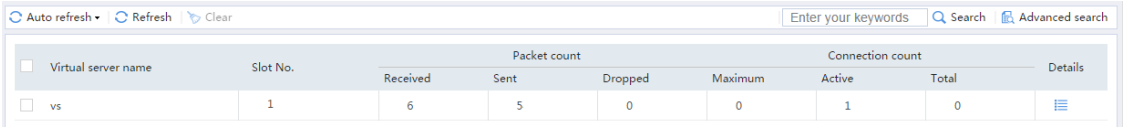
Figure 48 Accessing the HTTP service



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

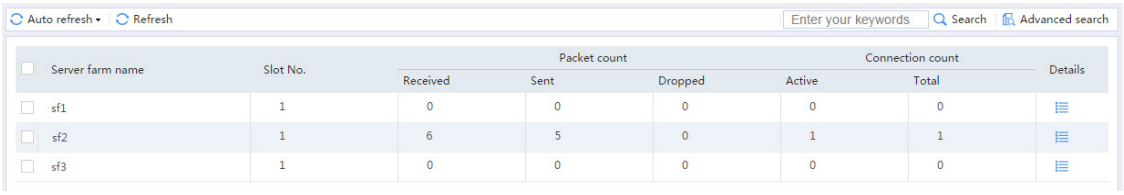
Figure 49 Displaying virtual server statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Servers Farms**. You can see that the device assigns the HTTP request containing URL **http://61.159.4.200/finance/** to server farm **sf2**.

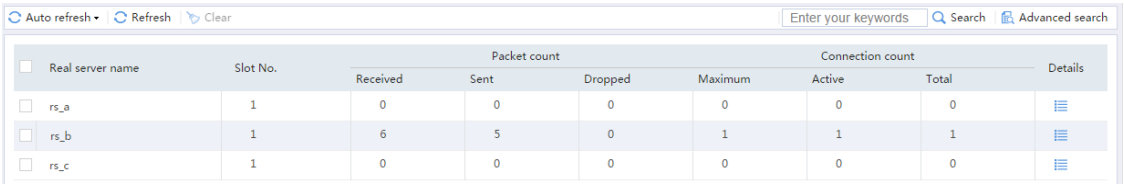
Figure 50 Displaying server farm statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Real Servers**. You can see that the device assigns the HTTP request containing URL **http://61.159.4.200/finance/** to real server **rs_b**.

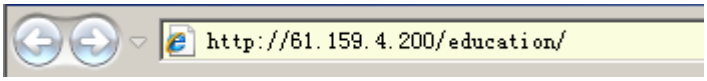
Figure 51 Displaying real server statistics



3. Verify that the device assigns Sever C the HTTP request with URL **http://61.159.4.200/education/**.

Access **http://61.159.4.200/education/** on Host.

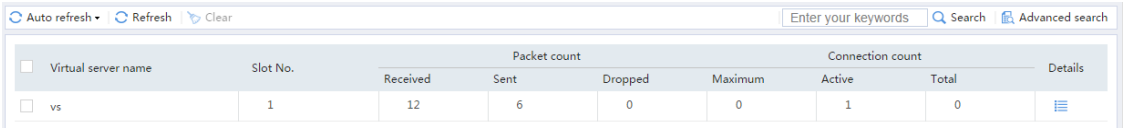
Figure 52 Accessing the HTTP service



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Virtual Servers**.

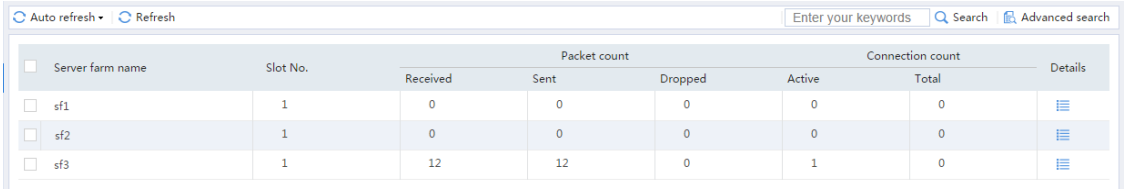
Figure 53 Displaying virtual server statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Servers Farms**. You can see that the device assigns the HTTP request containing URL **http://61.159.4.200/education/** to server farm **sf3**.

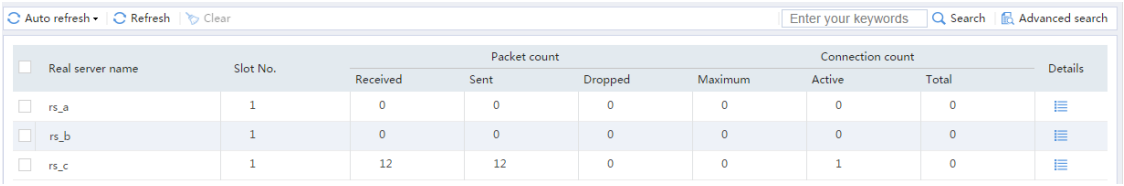
Figure 54 Displaying server farm statistics



On the top navigation bar, click **Monitor**.

From the navigation pane, select **Statistics** > **Server LB Statistics** > **Real Servers**. You can see that the device assigns the HTTP request containing URL **http://61.159.4.200/education/** to real server **rs_c**.

Figure 55 Displaying real server statistics



Real server name	Slot No.	Packet count			Connection count			Details
		Received	Sent	Dropped	Maximum	Active	Total	
rs_a	1	0	0	0	0	0	0	
rs_b	1	0	0	0	0	0	0	
rs_c	1	12	12	0	0	1	0	

Transparent DNS proxy configuration examples

Contents

Introduction

The following information provides transparent DNS proxy configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the transparent DNS proxy feature.

Restrictions and guidelines

To use this feature, do not deploy DNS servers in the internal network of the enterprise. If you deploy a DNS server in the internal network, DNS requests will be forwarded to the DNS server instead of being processed by this feature.

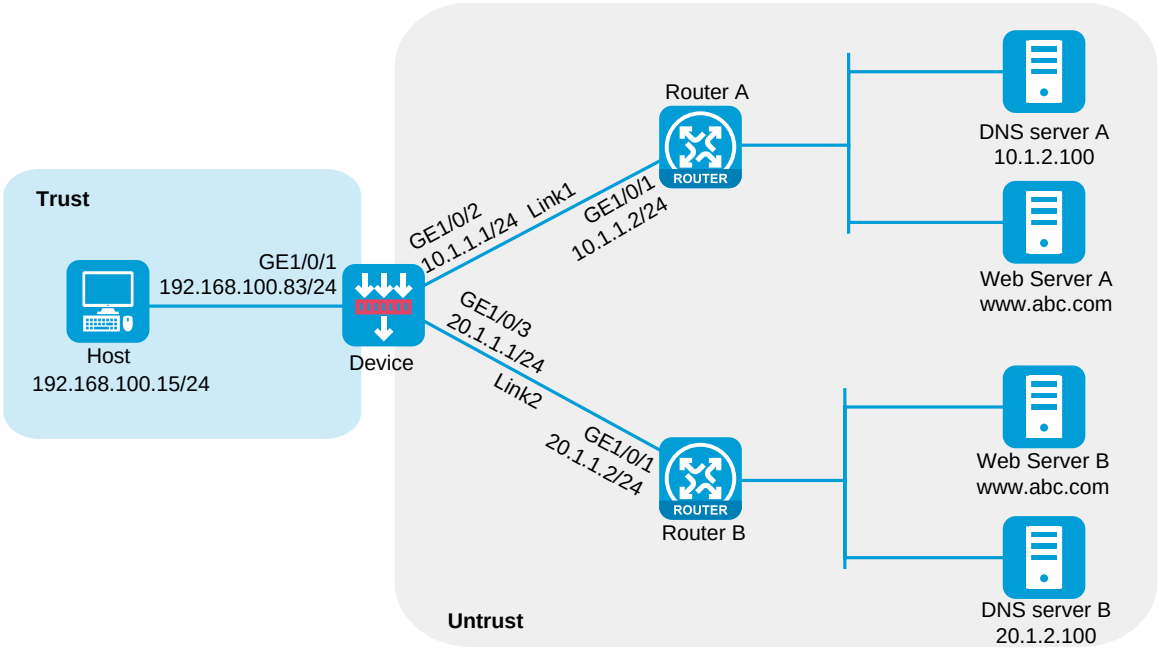
Example: Configuring the transparent DNS proxy

Network configuration

As shown in Figure 1, ISP 1 and ISP 2 provide two links with the same bandwidth to an enterprise: Link 1 and Link 2. The DNS server IP address of ISP 1 is 10.1.2.100. The DNS server IP address of ISP 2 is 20.1.2.100. Intranet users use domain name **www.abc.com** to access Web server A and Web server B.

Configure a transparent DNS proxy on the device to evenly distribute user traffic to Link 1 and Link 2.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedures

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click the **Network** tab.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Trust** security zone.

- On the **IPv4 Address** tab, enter the IP address and mask length of the interface. In this example, enter 192.168.100.83/24.
- Use the default settings for other parameters.
- Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 10.1.1.1/24 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Untrust** security zone and set its IP address to 20.1.1.1/24 in the same way you configure GE 1/0/1.

2. Configure security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy named **Trust-to-Untrust**:

- Enter policy name **Trust-to-Untrust**.
- Select source zone **Trust**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter source IPv4 address **192.168.100.0/24**.
- Use the default settings for other parameters.
- Click **OK**.

Configure a security policy named **Local-to-Untrust**:

- Enter policy name **Local-to-Untrust**.
- Select source zone **Local**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.
- Enter destination IPv4 addresses **10.1.1.0/24** and **20.1.1.0/24**.
- Use the default settings for other parameters.

- Click **OK**.

3. Configure an ICMP probe template.

   # On the top navigation bar, click **Objects**.

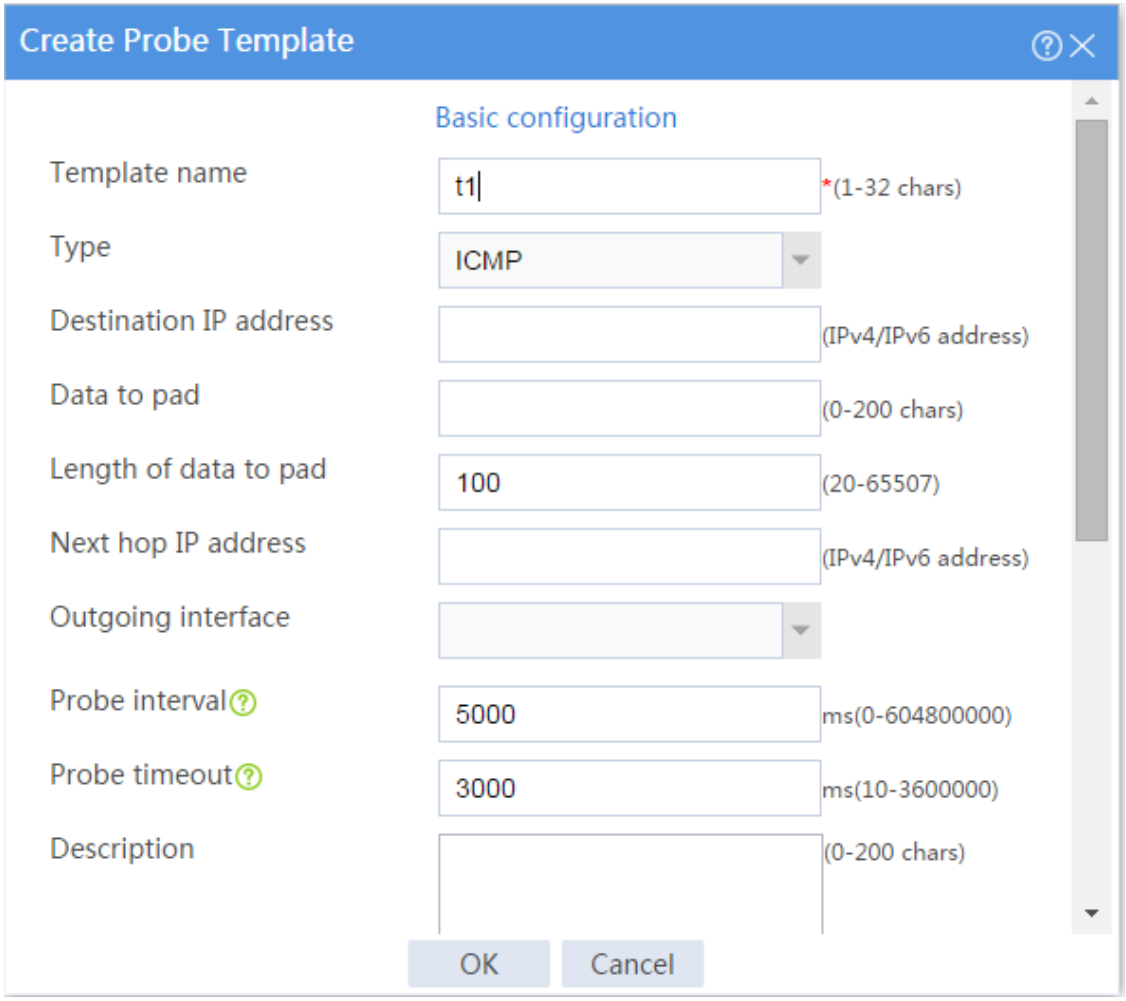
   # From the navigation pane, click **Health Monitoring**.

   # Click **Create**.

   # In the dialog box that opens, configure an ICMP probe template:

   - Enter template name **t1**.
   - Select type **ICMP**.
   - Enter 100 for the **Length of data to pad** field.
   - Enter 5000 for the **Probe interval** field.
   - Enter 3000 for the **Probe timeout** field.
   - Use the default settings for other parameters.
   - Click **OK**.

Figure 2 Creating an ICMP probe template



4. Configure links.

   # On the top navigation bar, click **Polices**.

   # From the navigation pane, select **Load Balancing** > **Common Configuration** > **Links**.

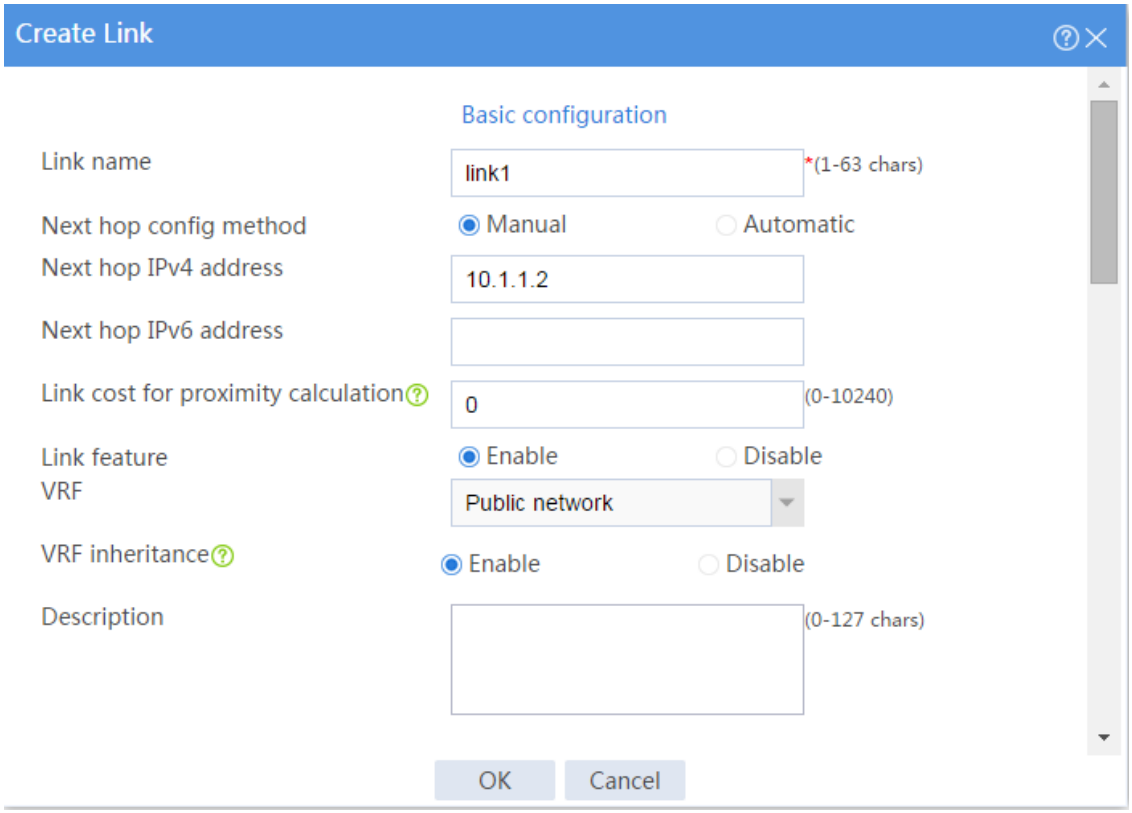
   # Click **Create**.

   # In the dialog box that opens, configure a link named **link1**:

   - Enter link name **link1**.
   - Select **Manual** for the **Next hop config method** field.
   - Enter next hop IPv4 address 10.1.1.2.
   - Set the link cost for proximity calculation to 0.
   - Enable the link feature.

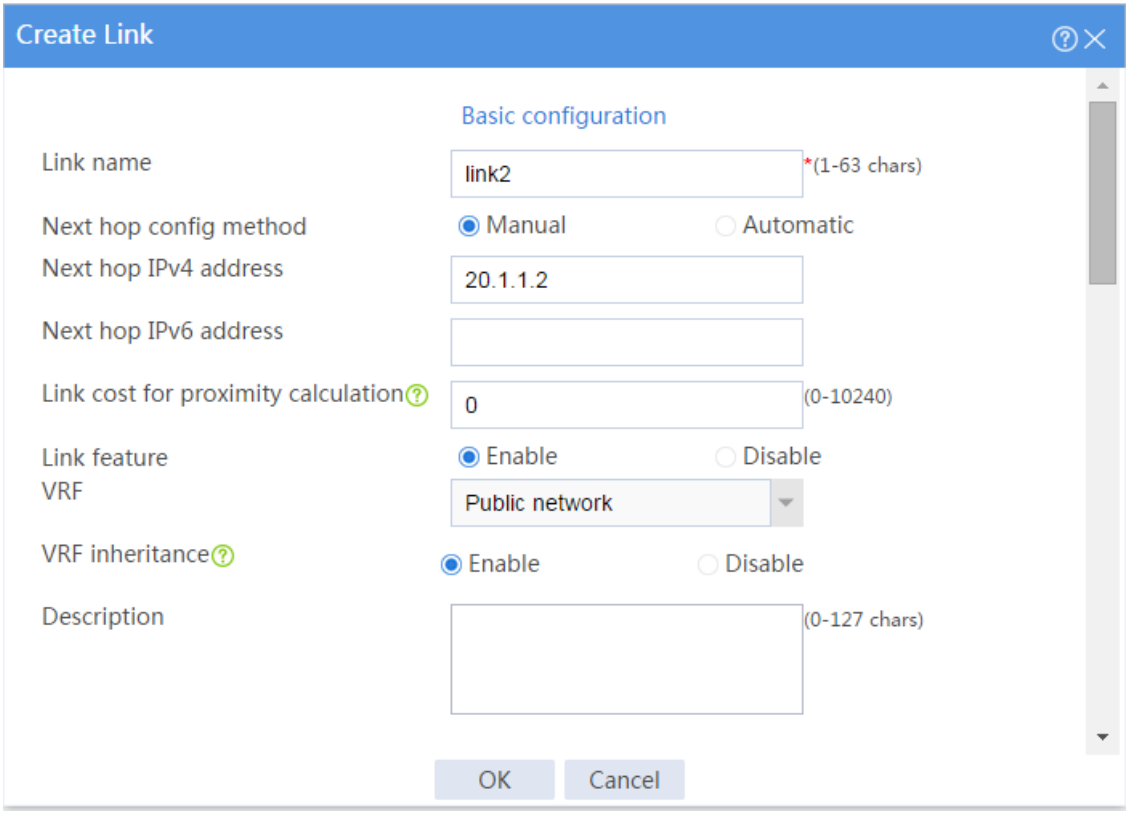
- Enable VRF inheritance.
- Click **OK**.

Figure 3 Creating link link1



Configure link **link2** in the same way you configure link **link1**.

Figure 4 Creating link link2



5. Configure DNS servers.

   # On the top navigation bar, click **Polices**.

   # From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **DNS Proxy**.

   # On the **DNS Server** tab, click **Create**.

   # In the dialog box that opens, configure a DNS server named **dns_a**:

   - Enter DNS server name **dns_a**.
   - Select **Manual** for the **IP address config method** field.
   - Enter IPv4 address 10.1.2.100.
   - Enter port number 0.
   - Enter weight 100.
   - Enter priority 4.
   - Select probe method **t1**.
   - Set the success criteria to **At least 1**.

- Select link **link1**.
- Click **OK**.

Figure 5 Creating DNS server dns_a

Configure DNS server **dns_b** in the same way you configure DNS server **dns_a**.

Figure 6 Creating DNS server dns_b

6. Configure a DNS server pool.

   # On the top navigation bar, click **Polices**.

   # From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **DNS Proxy**.

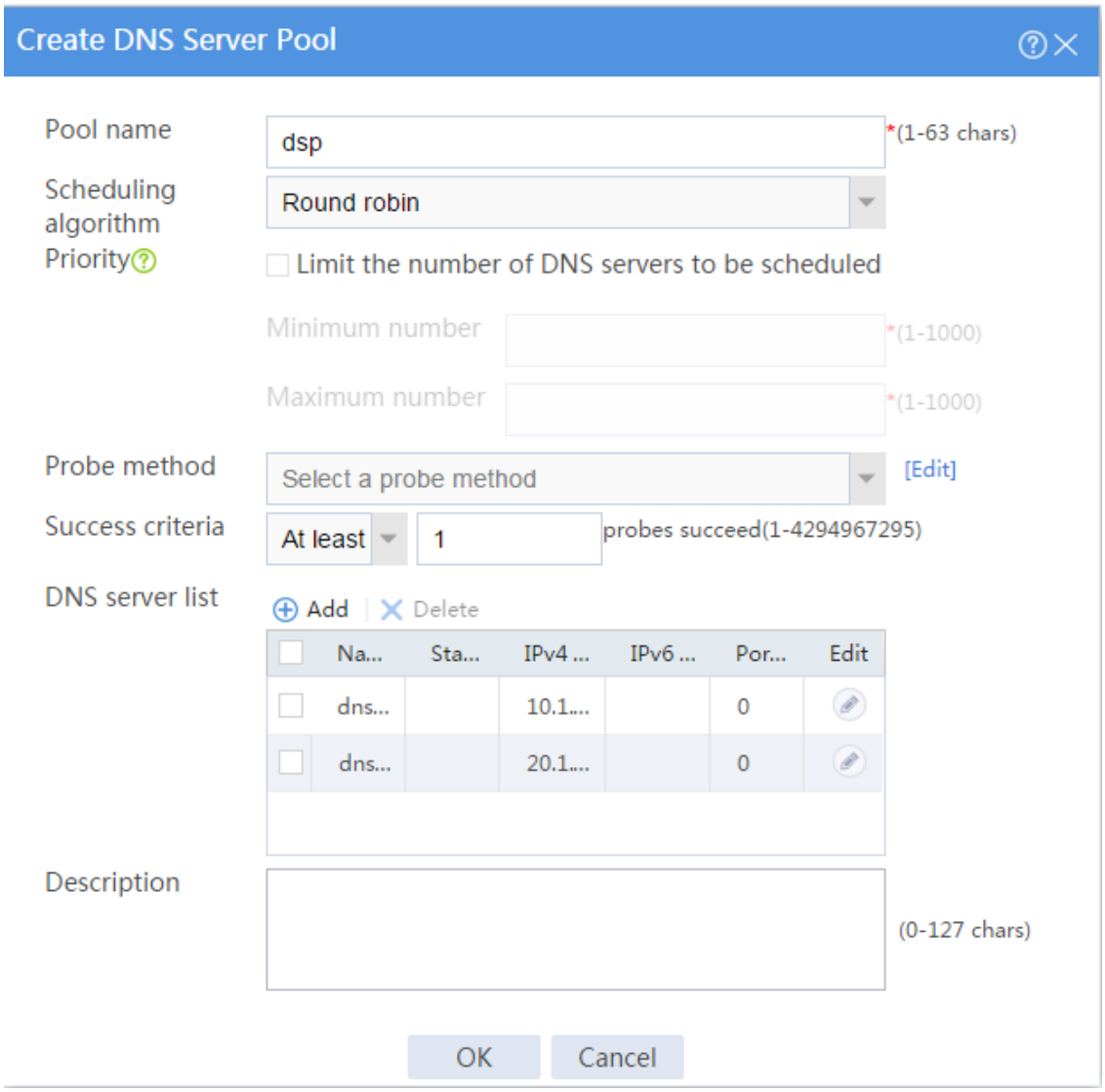
   # On the **DNS Server Pool** tab, click **Create**.

   # In the dialog box that opens, configure a DNS server pool named **dsp**:

   - Enter DNS server pool name **dsp**.
   - Select scheduling algorithm **Round robin**.
   - Set the success criteria to **At least 1**.

- Add DNS servers **dns_a** and **dns_b** to the DNS server pool.
- Click **OK**.

Figure 7 Creating DNS server pool dsp



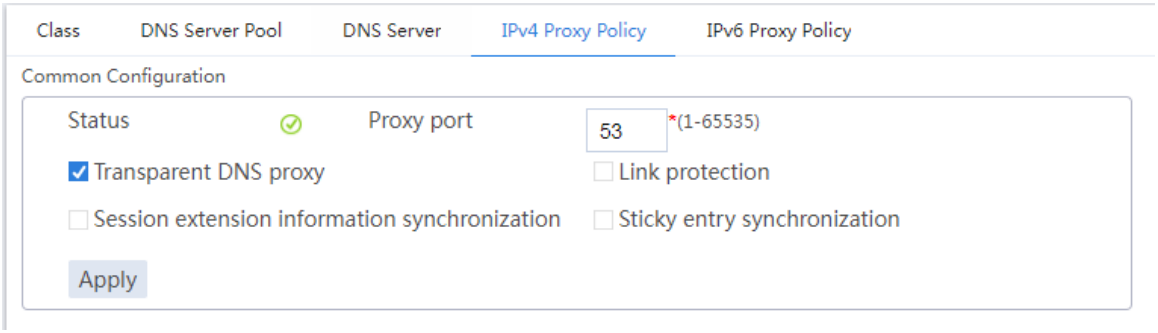
7. Configure IPv4 routing policies.

On the top navigation bar, click **Polices**.

From the navigation pane, select **Load Balancing** > **Link Load Balancing** > **DNS Proxy**.

In the **Common configuration** area on the **IPv4 Routing Policy** tab, select the **Transparent DNS proxy** option and click **Apply**.

Figure 8 Common configuration

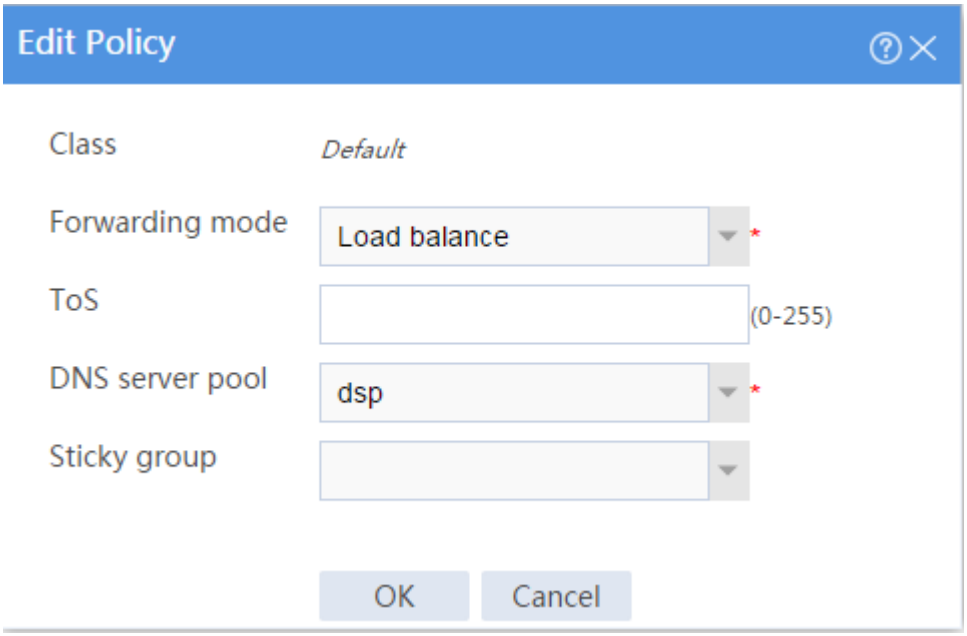


In the **Policy** area on the **IPv4 Routing Policy** tab, click the **Edit** icon for the default IPv4 routing policy named ***Default***.

In the dialog box that opens, configure the default IPv4 routing policy:

- Select forwarding mode **Load balance**.
- Select DNS server pool **dsp**.
- Click **OK**.

Figure 9 Editing the default IPv4 routing policy



Verifying the configuration

Access http://www.abc.com through the browser on the host, and verify that the device distributes the DNS requests to DNS servers **dns_a** and **dns_b**.

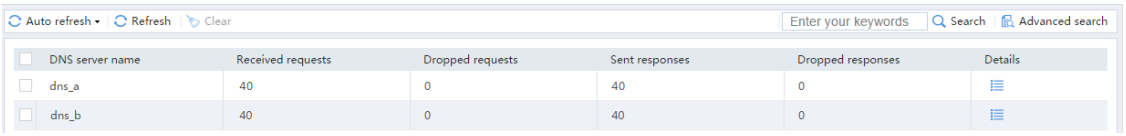
1. View the **DNS Server Statistics** page.

   # On the top navigation bar, click the **Monitor** tab.

   # From the navigation pane, select **Statistics** > **DNS Proxy Statistics** > **DNS Servers**.

   The **DNS Server Statistics** page is as follows:

   Figure 10 DNS server statistics

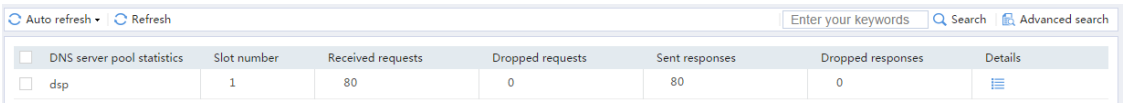


2. View the **DNS Server Pool Statistics** page.

   # From the navigation pane, select **Statistics** > **DNS Proxy Statistics** > **DNS Server Pools**.

   The **DNS Server Pool Statistics** page is as follows:

   Figure 11 DNS server pool statistics



High availability group configuration examples

Contents

Introduction

The following information provides high availability (HA) group configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the HA group, VRRP, and Track features.

Restrictions and guidelines

Verify that the devices to be assigned to the HA group meet the hardware and software environment consistency requirements in this section.

Hardware environment consistency

Before you configure the HA group, verify that the following hardware settings are the same on the devices to be assigned to the HA group:

- Device model.
- Location, number, and type of MPUs.
- Location, number, and type of service modules.
- Location, number, and type of switching fabric modules.
- Location, number, and type of interface modules.

- Number and type of management interfaces, service interfaces, interfaces for setting up the control channel, and interfaces for setting up the data channel. Do not use one interface for multiple purposes.
- Location, number, and type of disks. A device without disks installed has small log storage and does not support some types of logs or reports.

Software environment consistency

Before you configure the HA group, verify that the following software settings are the same on the devices to be assigned to the HA group:

- Software environment and version, including boot packages, system packages, feature packages, and patches.
- Licensed signature libraries and features, such as signature library types, signature library version, validation time, and number of licensed resources.
- Interface numbers.
- Type, speed, and number of the interfaces for setting up the control channel. As a best practice, use aggregate interfaces.
- Type, speed, and number of the interfaces for setting up the data channel. As a best practice, use aggregate interfaces.
- Aggregate interface numbers and aggregation member port numbers.
- Security zone configuration on the interfaces at the same location.

Feature compatibility restrictions

Compatibility with NAT

If you configure both VRRP and NAT on the HA group, you must associate NAT configuration with VRRP groups, such as NAT rules, source translation methods, and NAT server mappings. If you fail to do so, NAT cannot operate correctly.

Compatibility with SSL VPN

For SSL VPN to operate correctly on the HA group, you must configure the port used for transmitting user data for the HA group on the global setting configuration page of SSL VPN.

You can use SSL VPN only when the HA group is operating in active/standby mode and collaborating with VRRP. You cannot use SSL VPN in any other scenario.

Compatibility with application security

If asymmetric-path traffic exists on the transparent in-path HA group operating in dual-active mode, enable DPI services to support the HA group feature on the advanced setting configuration page of application security. If you fail to do so, application security services cannot identify or process traffic correctly.

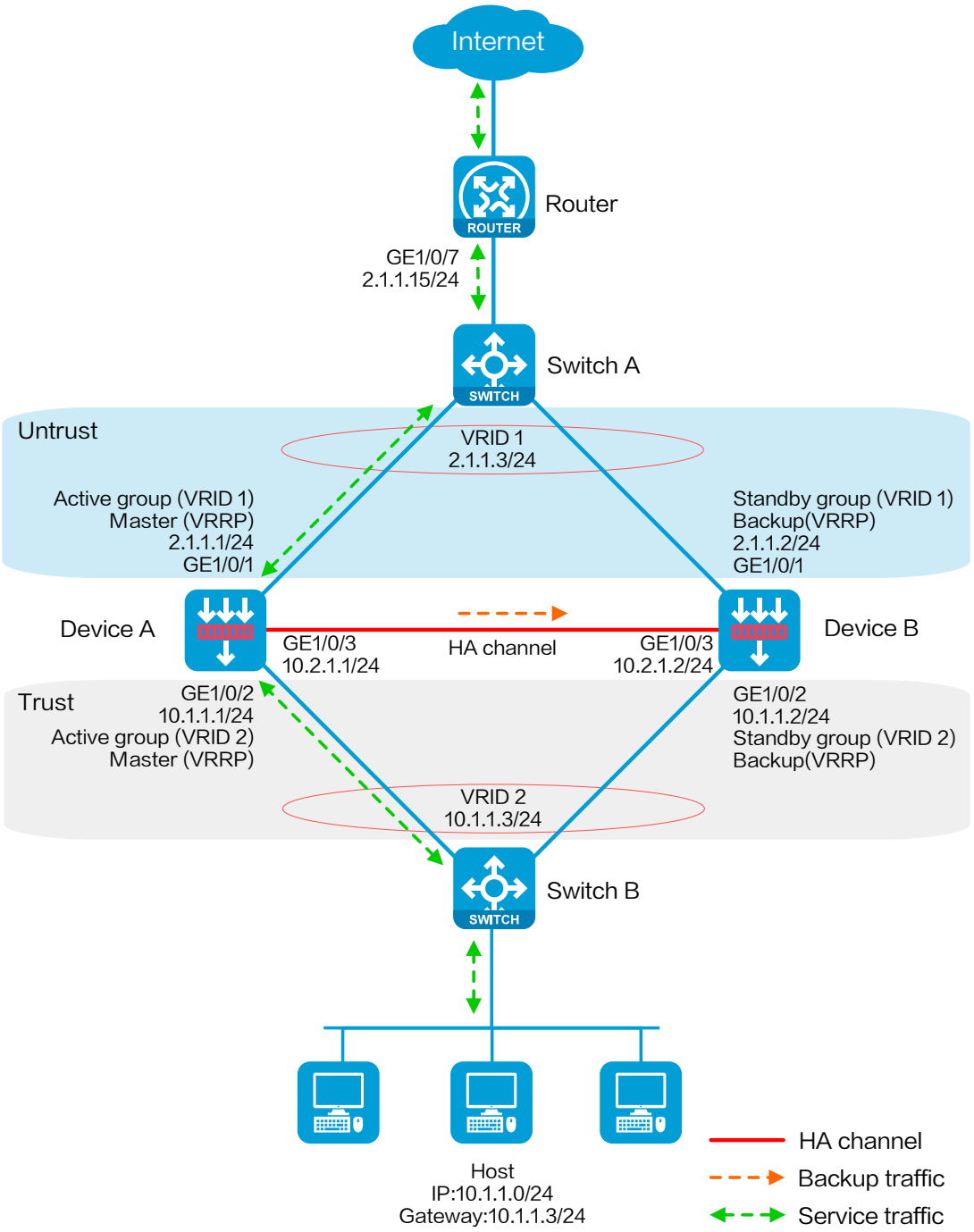
Example: Configuring the HA group in active/standby mode in collaboration with VRRP (IPv4)

Network configuration

As shown in Figure 1, set up the HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to collaborate with VRRP.
- Configure the HA group to operate in active/standby mode.
- Configure Device A and Device B as the primary device and the secondary device, respectively.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Switch A

Create VLAN 10.

Configure the interfaces attached to the HA group and the router to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring Switch B

Create VLAN 10.

Configure the interfaces attached to the HA group and the host to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring the router

Assign 2.1.1.15/24 to GigabitEthernet 1/0/7.

Configure routes as follows:

- Specify 2.1.1.3 (virtual IP address of VRRP group 1) as the next hop of the routes to the internal network.
- Specify the IP address of the peer interface attached to the traffic outgoing interface as the next hop of the route to the Internet.

Configuring Device A

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. On the **Basic Configuration** tab, select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.1.1/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and assign 10.1.1.1/24 to it in the same way you configure GE 1/0/1.

   # Assign 10.2.1.1/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

   This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure an IPv4 static route:

   a. Enter destination IP address **0.0.0.0**.

   b. Enter mask length **0**.

   c. Enter next hop address **2.1.1.15**.

   d. Use the default settings for other parameters.

   e. Click **OK**.

3. Configure a security policy to permit service traffic:

   Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Select **Create** > **Create a policy**.

   # In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

   a. Enter security policy name **Trust-Untrust**.

   b. Select source zone **Trust**.

   c. Select destination zone **Untrust**.

   d. Select IP version **IPv4**.

   e. Set the action to **Permit**.

   f. Enter source IP address **10.1.1.0/24**.

   g. Use the default settings for other parameters.

   h. Click **OK**.

4. Configure security policies to permit VRRP protocol packets:

   This task allows Device A and Device B to exchange VRRP packets and elect a VRRP master when the HA channels are disconnected.

   Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Select **Create** > **Create a policy**.

   # In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Local**:

   a. Enter security policy name **vrrp1**.

   b. Select source zone **Trust**.

   c. Select destination zone **Local**.

   d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Select policy group **vrrp**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Trust**:

i. Enter security policy name **vrrp2**.

j. Select source zone **Local**.

k. Select destination zone **Trust**.

l. Select IP version **IPv4**.

m. Set the action to **Permit**.

n. Select policy group **vrrp**.

o. Use the default settings for other parameters.

p. Click **OK**.

Configure a security policy to permit traffic from zone **Untrust** to zone **Local**:

q. Enter security policy name **vrrp3**.

r. Select source zone **Untrust**.

s. Select destination zone **Local**.

t. Select IP version **IPv4**.

u. Set the action to **Permit**.

v. Select policy group **vrrp**.

w. Use the default settings for other parameters.

x. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Untrust**:

y. Enter security policy name **vrrp4**.

z. Select source zone **Local**.

aa. Select destination zone **Untrust**.

bb. Select IP version **IPv4**.

cc. Set the action to **Permit**.

dd. Select policy group **vrrp**.

ee. Use the default settings for other parameters.

ff. Click **OK**.

Configuring HA group settings

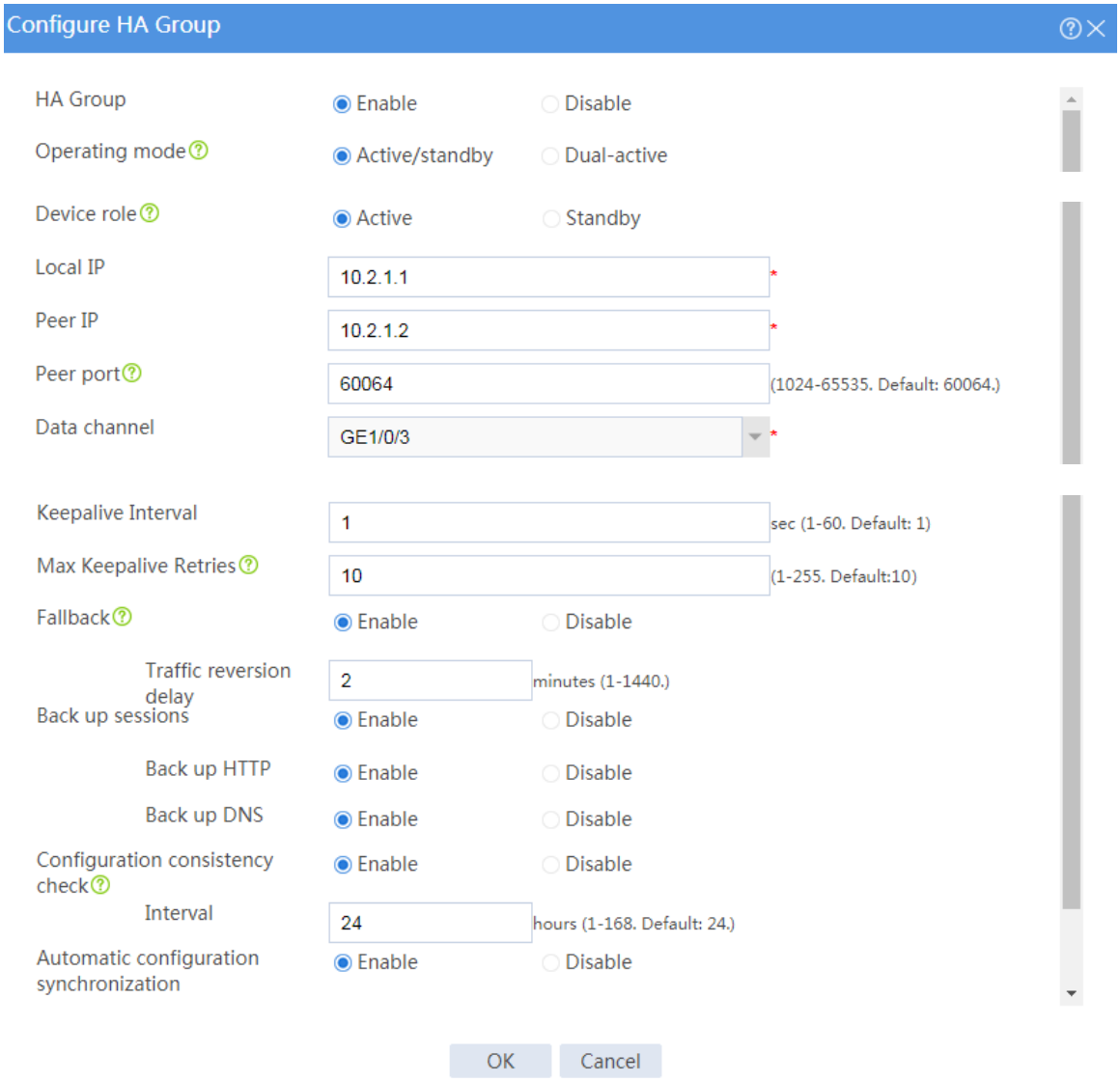
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 2.

Figure 2 Configuring HA group parameters



Click **OK**.

Associating the HA group with VRRP

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **VRRP**.

Click **Create**.

Configure VRRP groups as shown in the follow figures.

Figure 3 Creating VRRP group 1

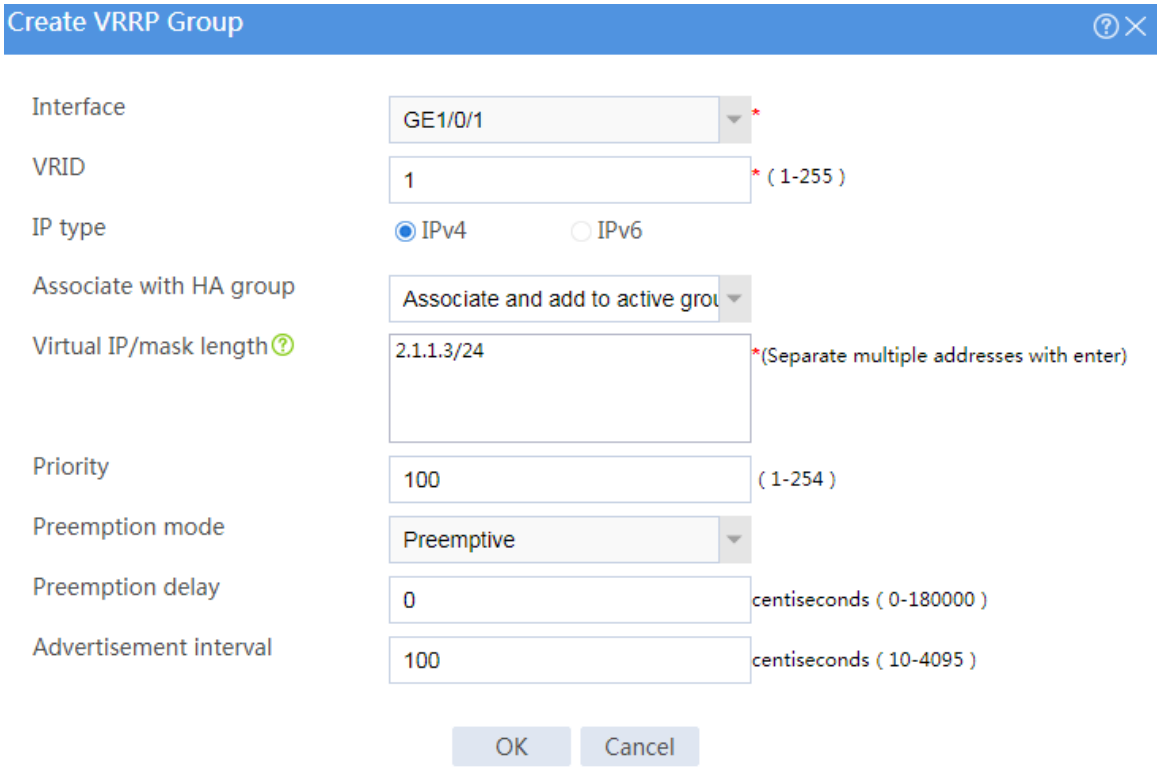
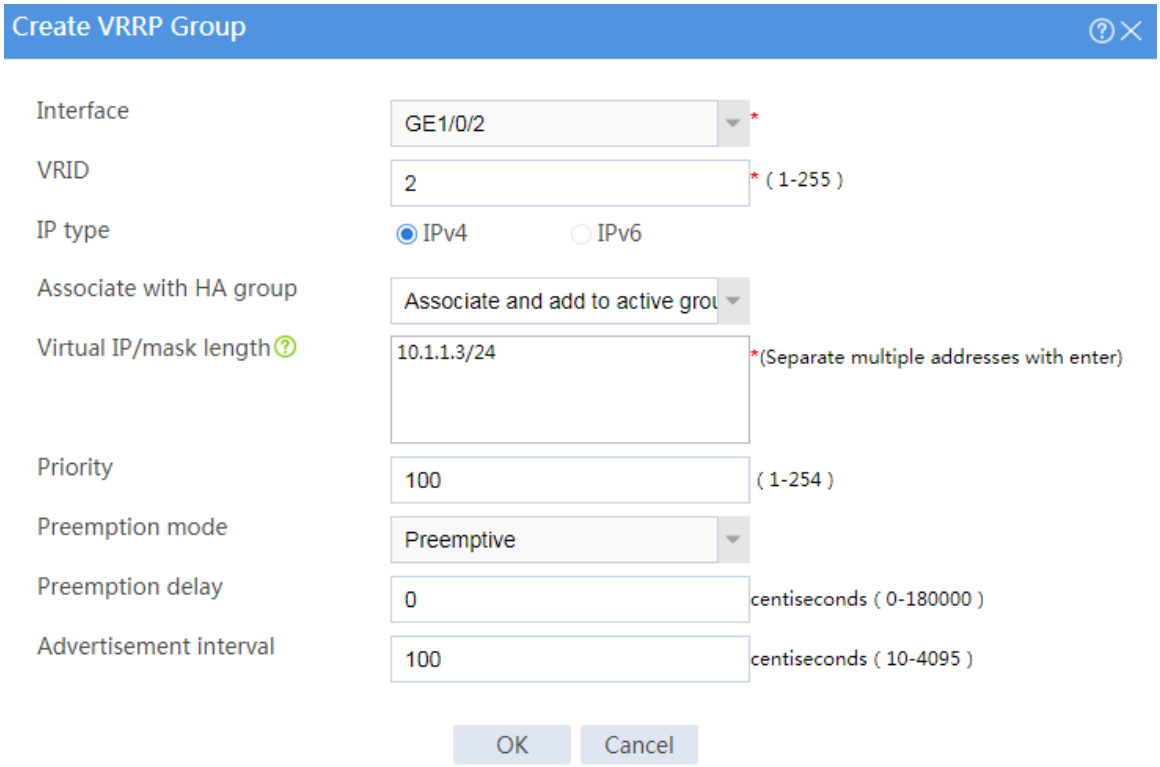


Figure 4 Creating VRRP group 2



Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.1.2/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and assign 10.1.1.2/24 to it in the same way you configure GE 1/0/1.

Assign 10.2.1.2/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv4 static route:

a. Enter destination IP address **0.0.0.0**.

b. Enter mask length **0**.

c. Enter next hop address **2.1.1.15**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configuring HA group settings

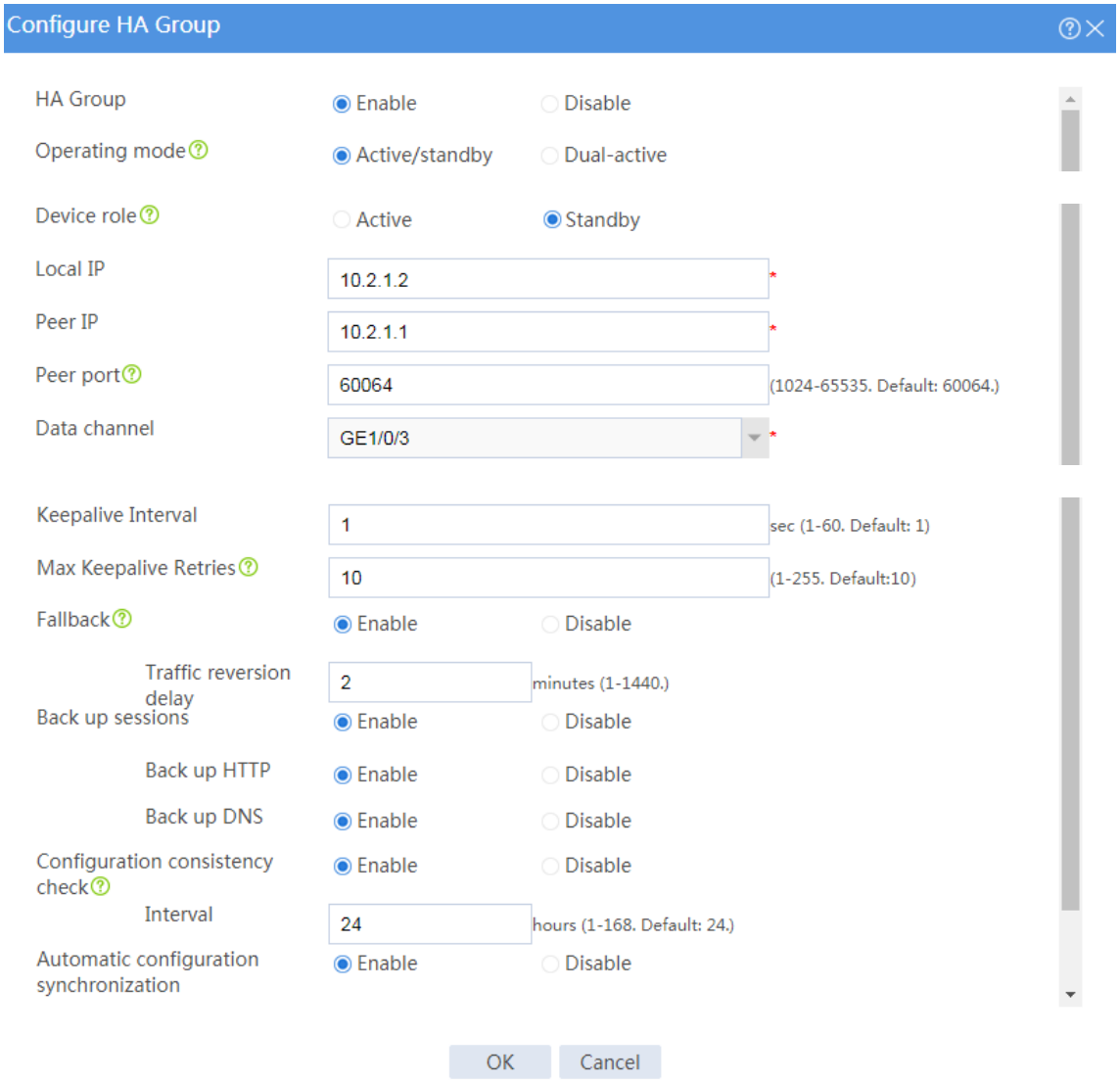
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 5.

Figure 5 Configuring HA group parameters



Click **OK**.

Associating the HA group with VRRP

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **VRRP**.

Click **Create**.

Configure VRRP groups as shown in the follow figures.

Figure 6 Creating VRRP group 1

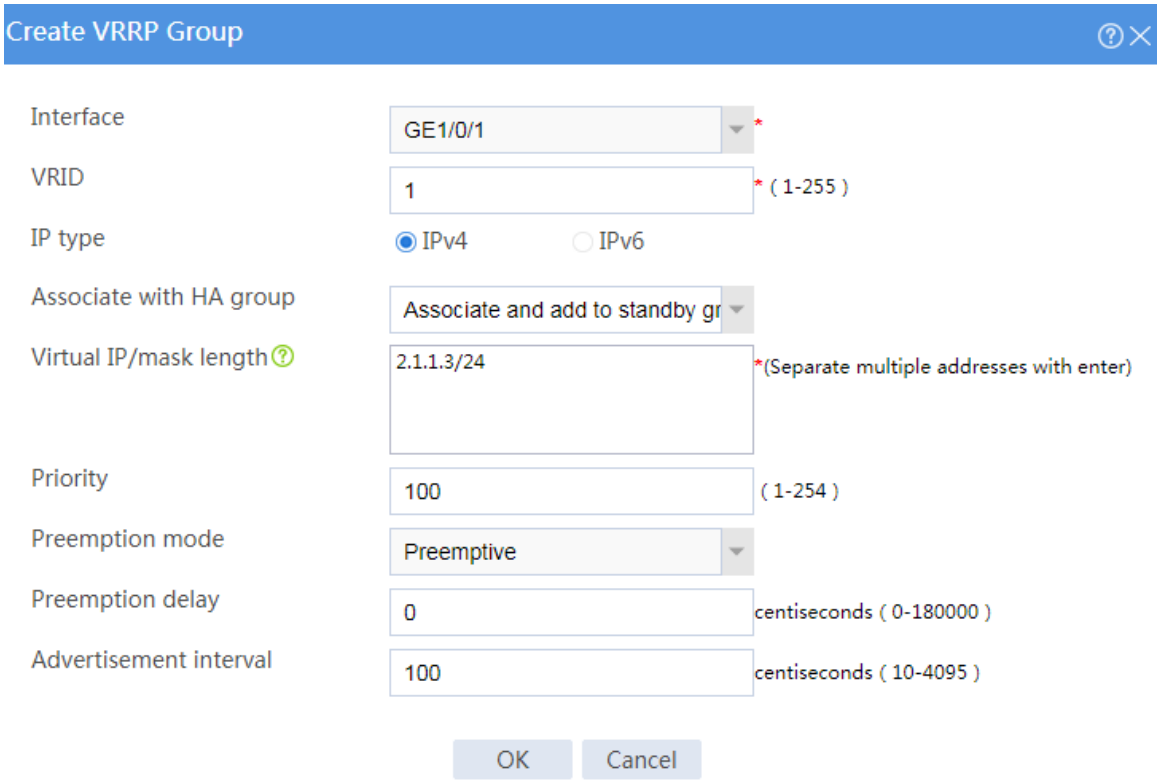
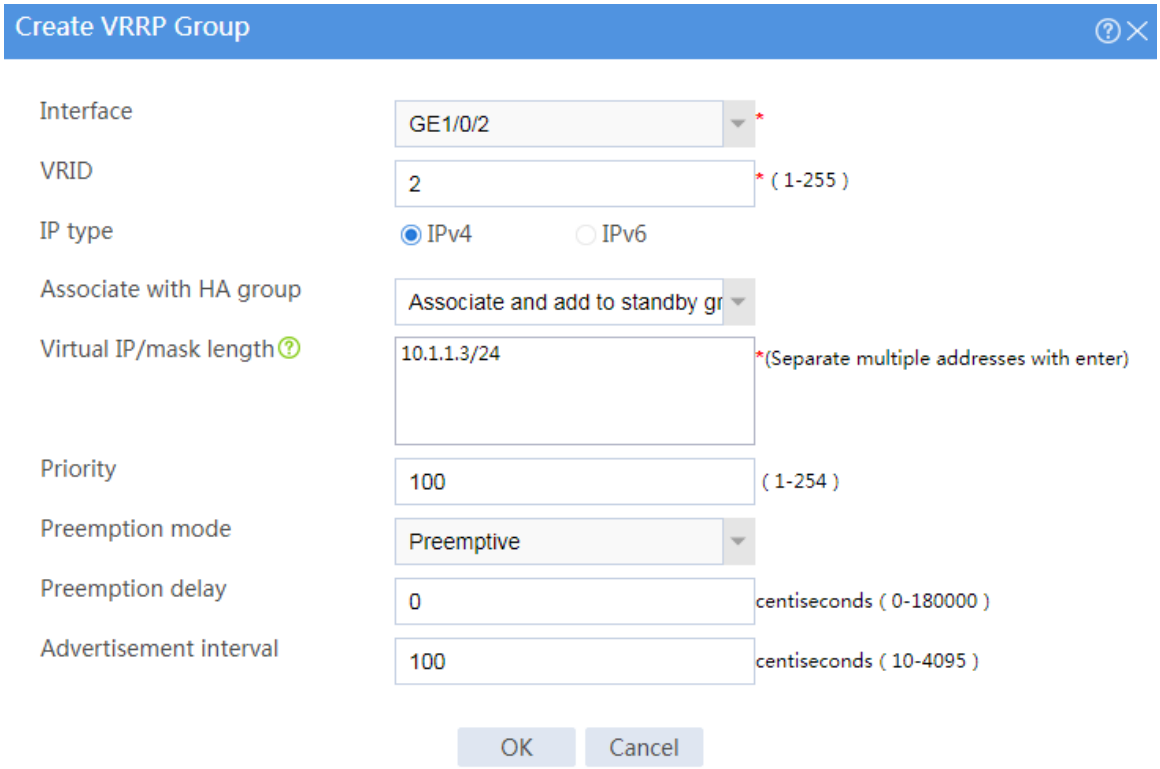


Figure 7 Creating VRRP group 2



Click **OK**.

Configuring the host

On the host, specify 10.1.1.3 (virtual IP address of VRRP group 2) as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that only Device A generates log messages when the host communicates with the Internet.

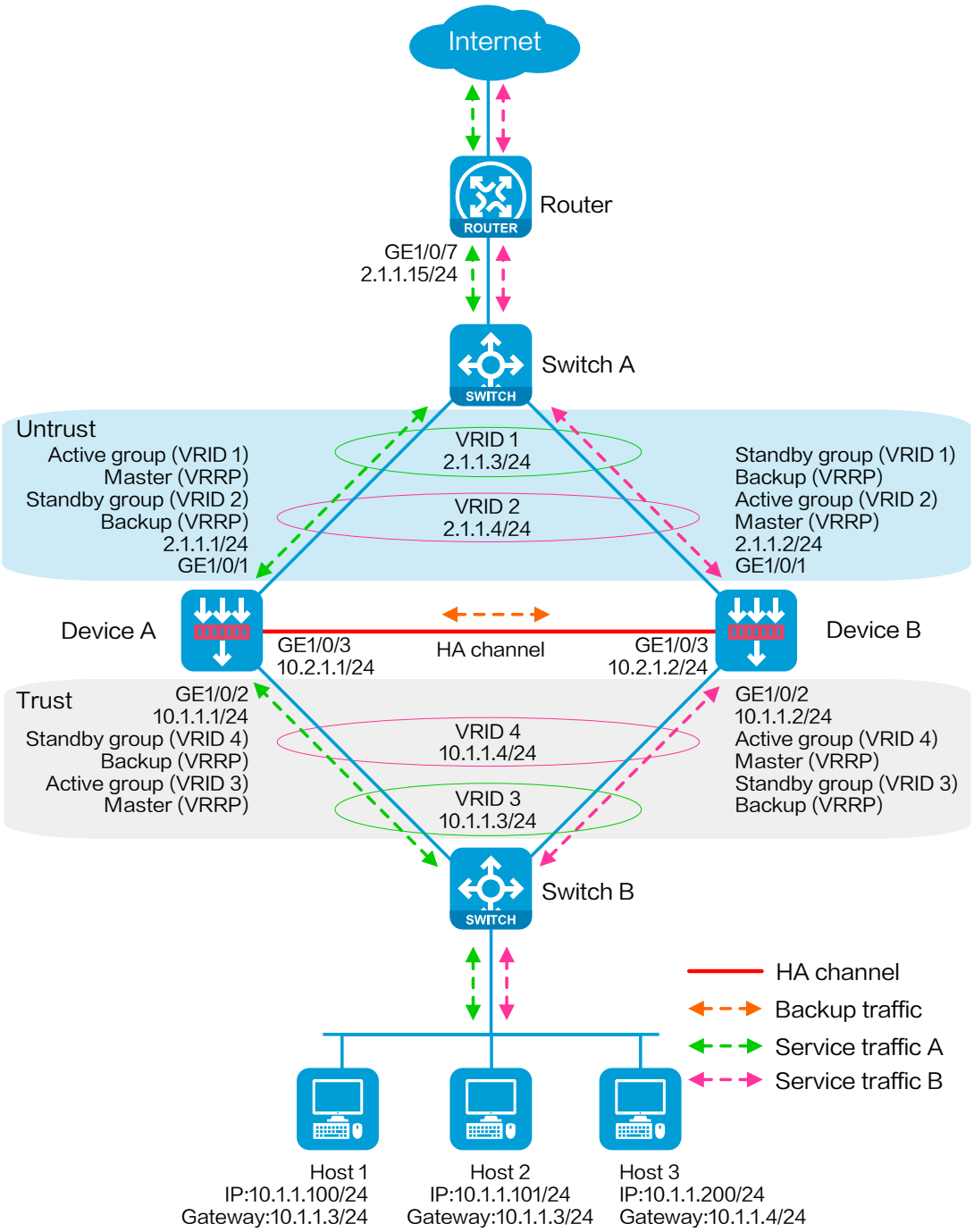
Example: Configuring the HA group in dual-active mode in collaboration with VRRP (IPv4)

Network configuration

As shown in Figure 8, set up the HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to collaborate with VRRP.
- Configure the HA group to operate in dual-active mode.
- Configure Device A and Device B to load share traffic.

Figure 8 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Switch A

Create VLAN 10.

Configure the interfaces attached to the HA group and the router to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring Switch B

Create VLAN 10.

Configure the interfaces attached to the HA group and the host to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring the router

Assign 2.1.1.15/24 to GigabitEthernet 1/0/7.

Specify 2.1.1.3 (virtual IP address of VRRP group 1) as the next hop of the routes to some subnets of the internal network. Specify 2.1.1.4 (virtual IP address of VRRP group 2) as the next hop of the routes to the other subnets of the internal network.

Specify the IP address of the peer interface attached to the traffic outgoing interface as the next hop of the route to the Internet.

Configuring Device A

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. On the **Basic Configuration** tab, select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.1.1/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Trust** security zone and assign 10.1.1.1/24 to it in the same way you configure GE 1/0/1.

   # Assign 10.2.1.1/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

   This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure an IPv4 static route:

   a. Enter destination IP address **0.0.0.0**.

   b. Enter mask length **0**.

   c. Enter next hop address **2.1.1.15**.

   d. Use the default settings for other parameters.

   e. Click **OK**.

3. Configure a security policy to permit service traffic:

   Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Select **Create** > **Create a policy**.

   # In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

   a. Enter security policy name **Trust-Untrust**.

   b. Select source zone **Trust**.

   c. Select destination zone **Untrust**.

   d. Select IP version **IPv4**.

   e. Set the action to **Permit**.

   f. Enter source IP address **10.1.1.0/24**.

   g. Use the default settings for other parameters.

   h. Click **OK**.

4. Configure security policies to permit VRRP protocol packets:

   This task allows Device A and Device B to exchange VRRP packets and elect a VRRP master when the HA channels are disconnected.

   Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Select **Create** > **Create a policy**.

   # In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Local**:

   a. Enter security policy name **vrrp1**.

   b. Select source zone **Trust**.

   c. Select destination zone **Local**.

   d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Select policy group **vrrp**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Trust**:

i. Enter security policy name **vrrp2**.

j. Select source zone **Local**.

k. Select destination zone **Trust**.

l. Select IP version **IPv4**.

m. Set the action to **Permit**.

n. Select policy group **vrrp**.

o. Use the default settings for other parameters.

p. Click **OK**.

Configure a security policy to permit traffic from zone **Untrust** to zone **Local**:

q. Enter security policy name **vrrp3**.

r. Select source zone **Untrust**.

s. Select destination zone **Local**.

t. Select IP version **IPv4**.

u. Set the action to **Permit**.

v. Select policy group **vrrp**.

w. Use the default settings for other parameters.

x. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Untrust**:

y. Enter security policy name **vrrp4**.

z. Select source zone **Local**.

aa. Select destination zone **Untrust**.

bb. Select IP version **IPv4**.

cc. Set the action to **Permit**.

dd. Select policy group **vrrp**.

ee. Use the default settings for other parameters.

ff. Click **OK**.

Configuring HA group settings

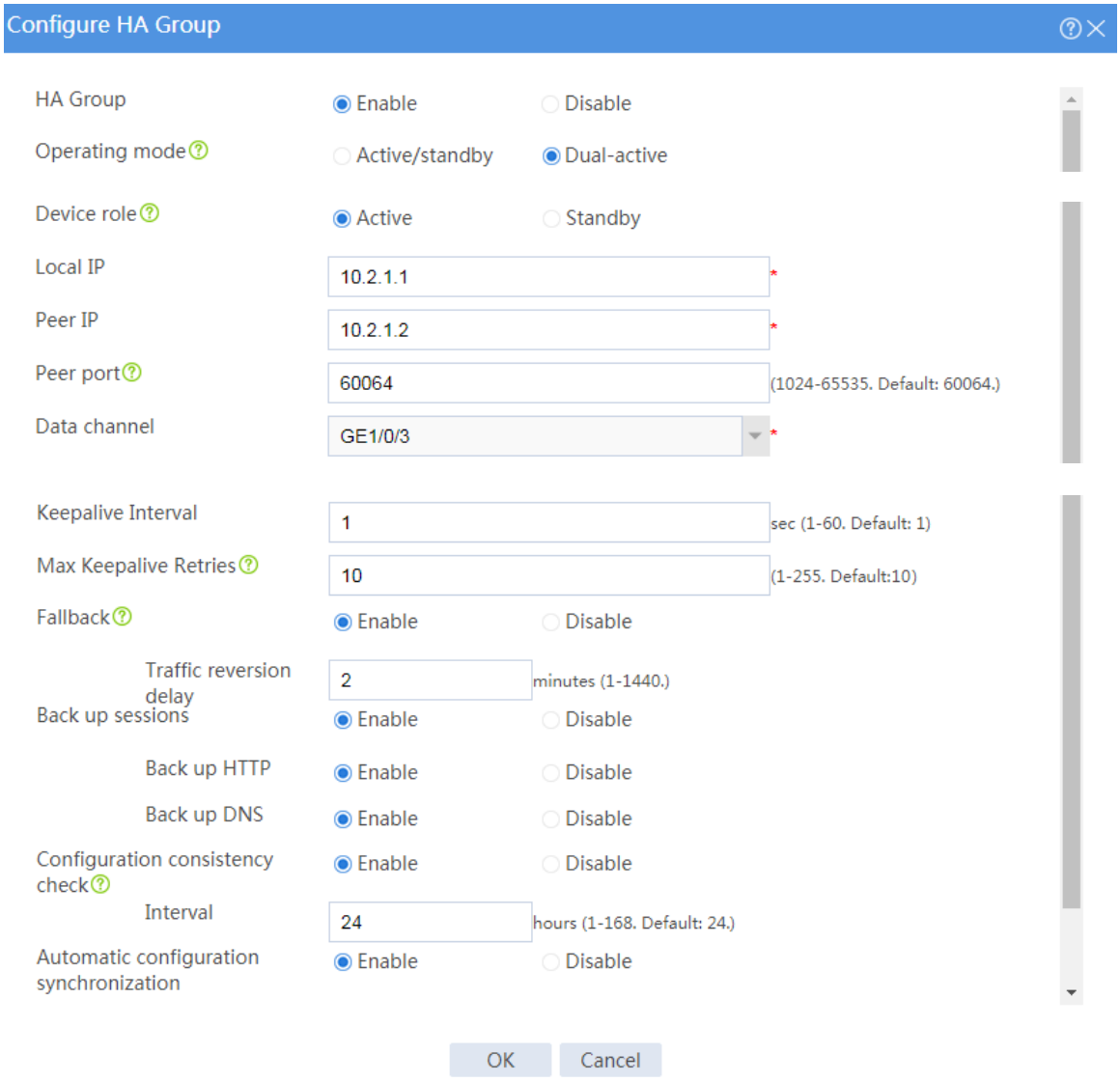
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 9.

Figure 9 Configuring HA group parameters



Click **OK**.

Associating the HA group with VRRP

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **VRRP**.

Click **Create**.

Configure VRRP groups as shown in the follow figures.

Figure 10 Creating VRRP group 1

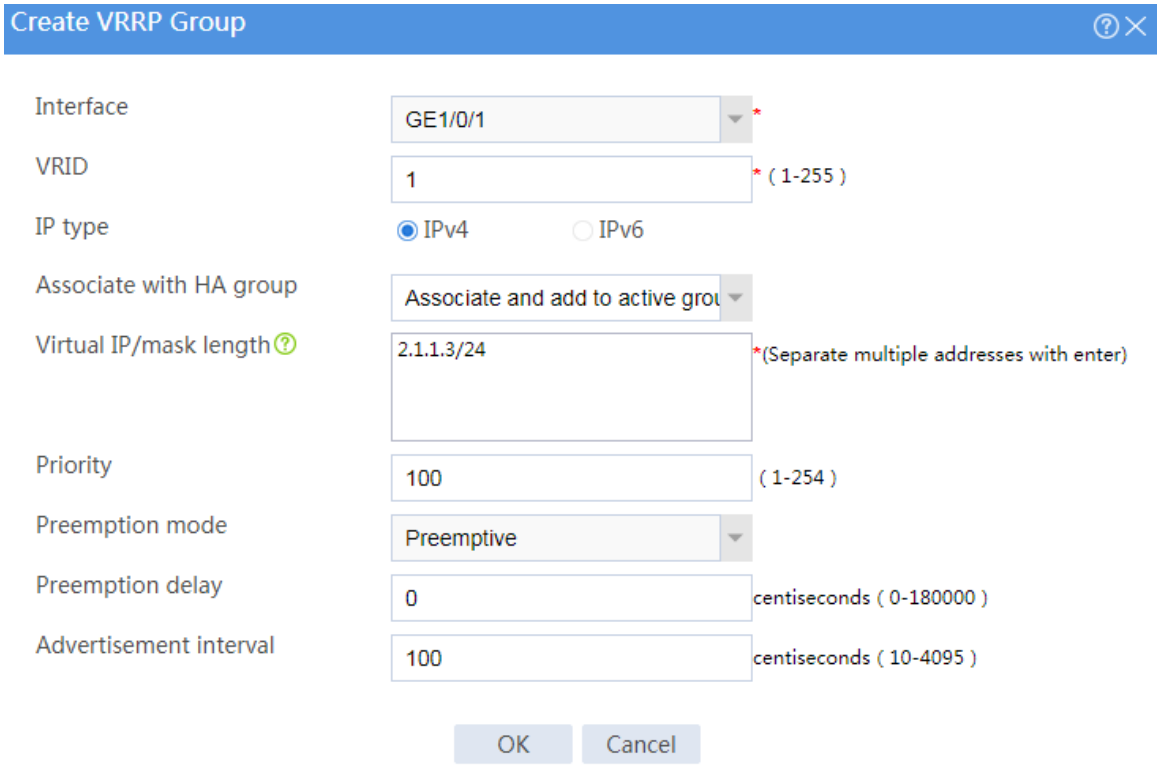


Figure 11 Creating VRRP group 2

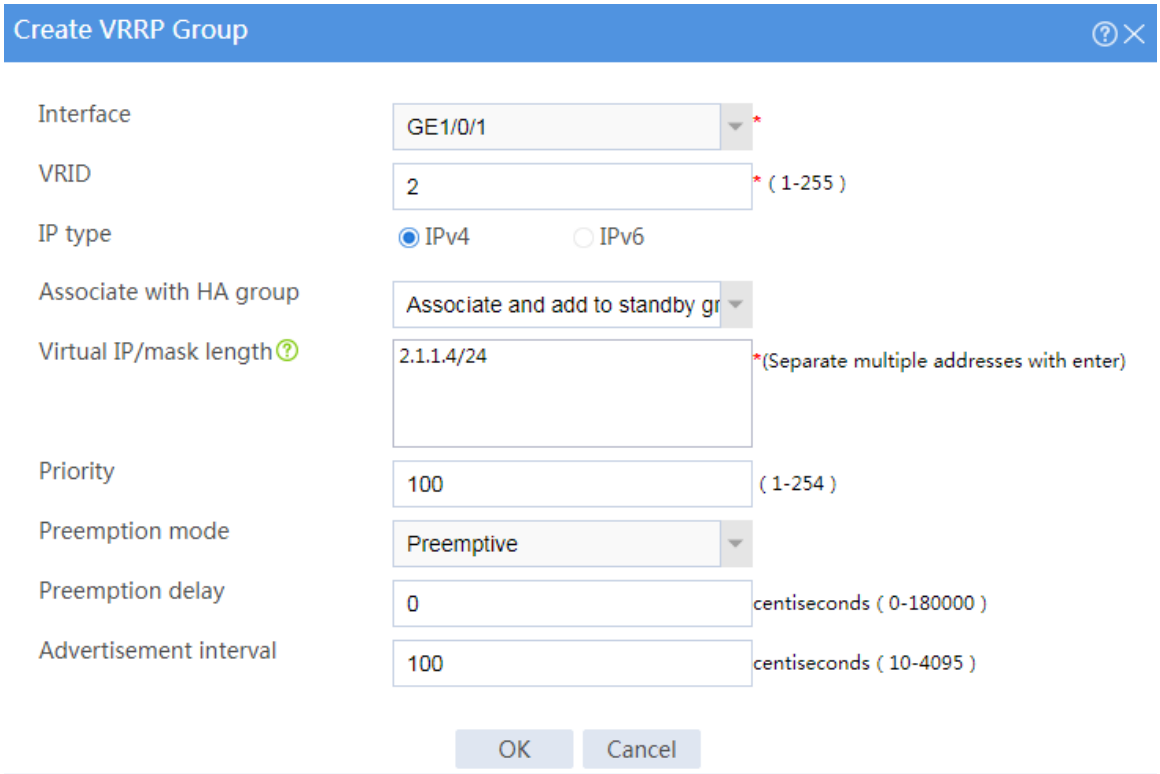


Figure 12 Creating VRRP group 3

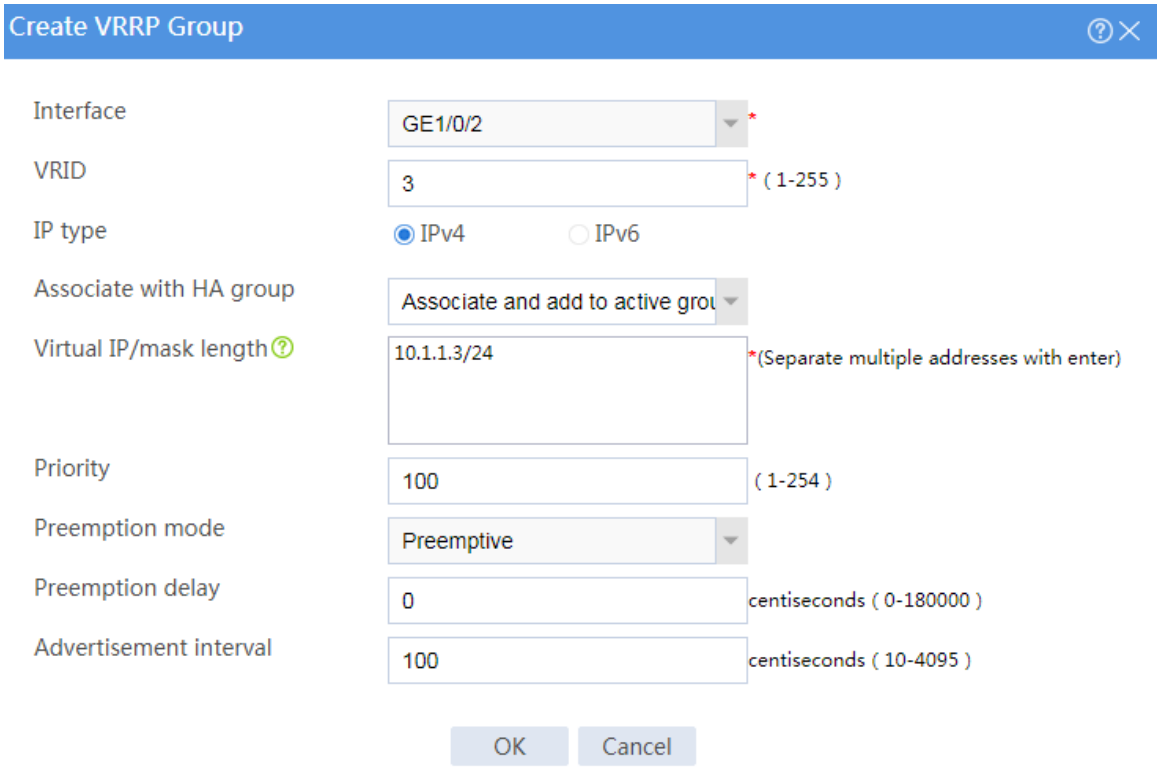
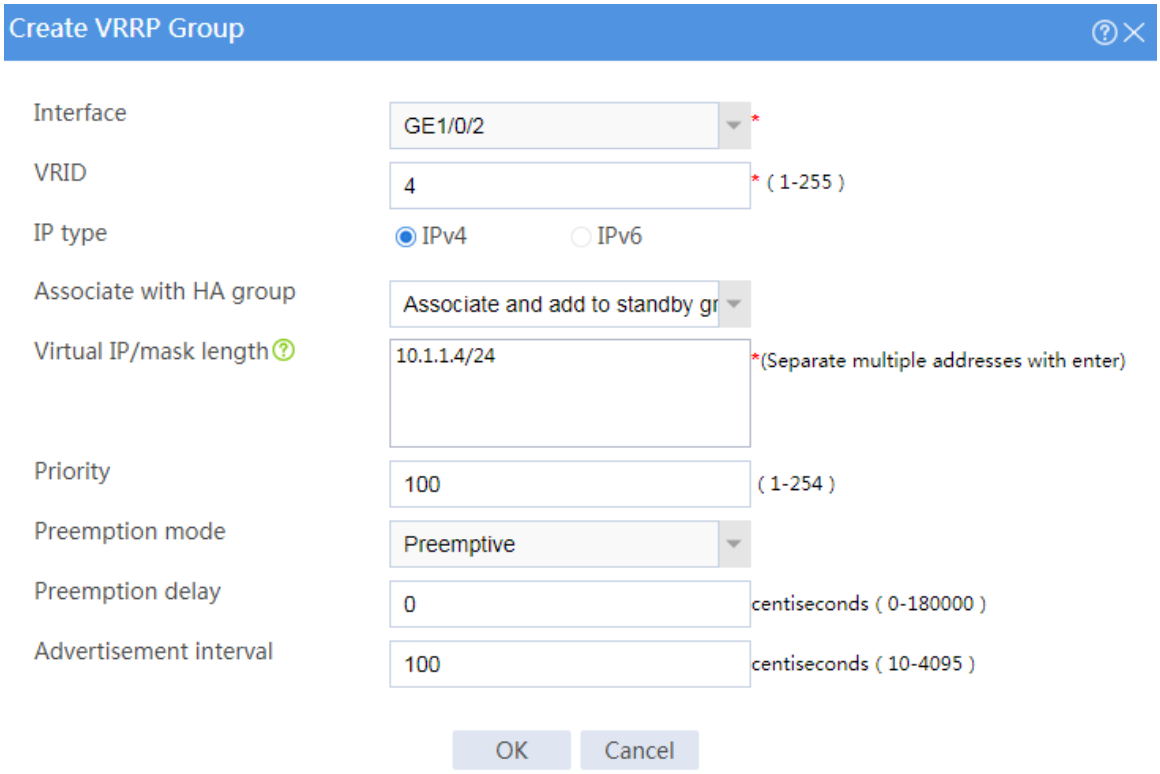


Figure 13 Creating VRRP group 4



Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.1.2/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and assign 10.1.1.2/24 to it in the same way you configure GE 1/0/1.

Assign 10.2.1.2/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv4 static route:

a. Enter destination IP address **0.0.0.0**.

b. Enter mask length **0**.

c. Enter next hop address **2.1.1.15**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configuring HA group settings

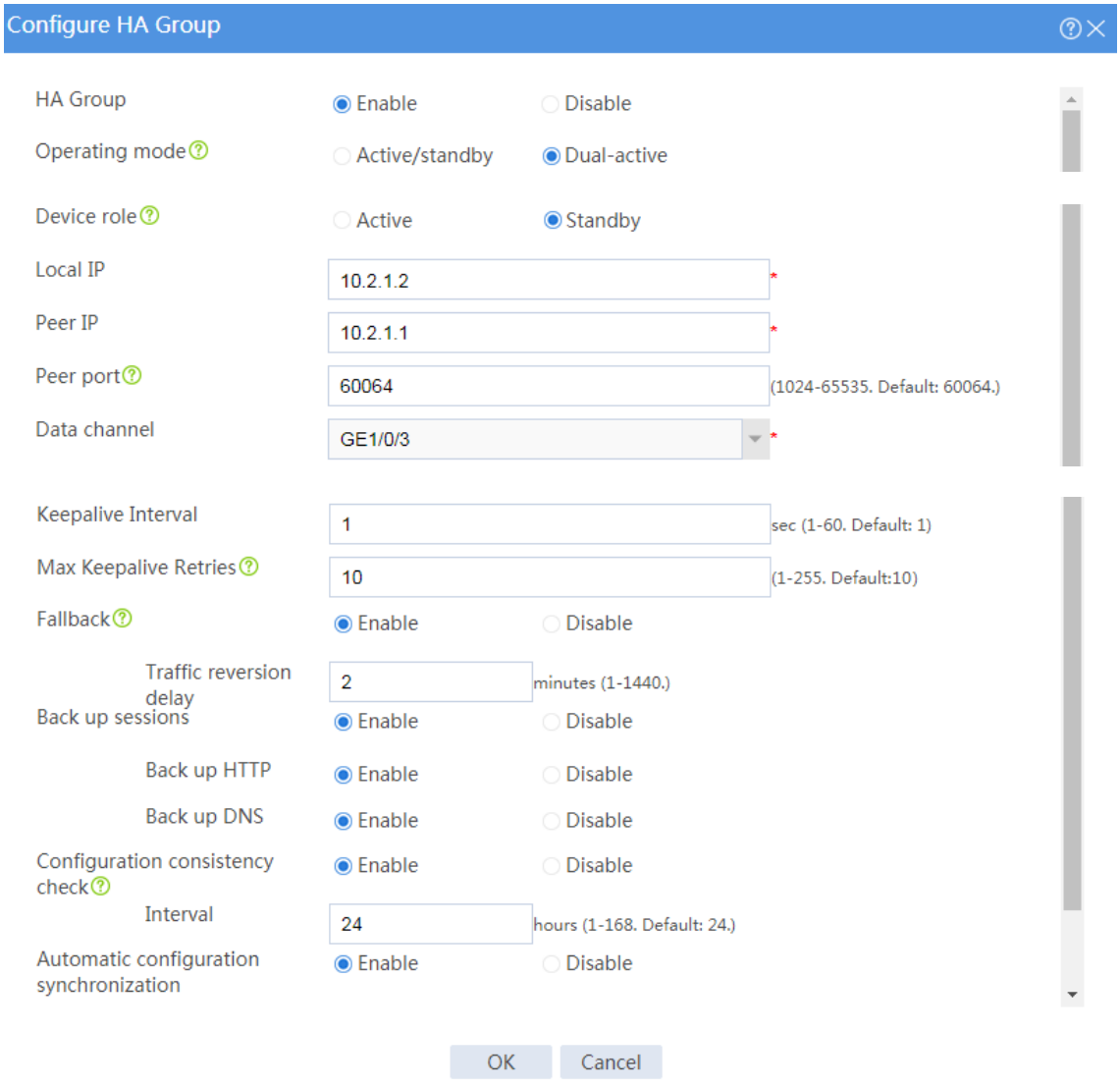
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 14.

Figure 14 Configuring HA group parameters



Click **OK**.

Associating the HA group with VRRP

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **VRRP**.

Click **Create**.

Configure VRRP groups as shown in the follow figures.

Figure 15 Creating VRRP group 1

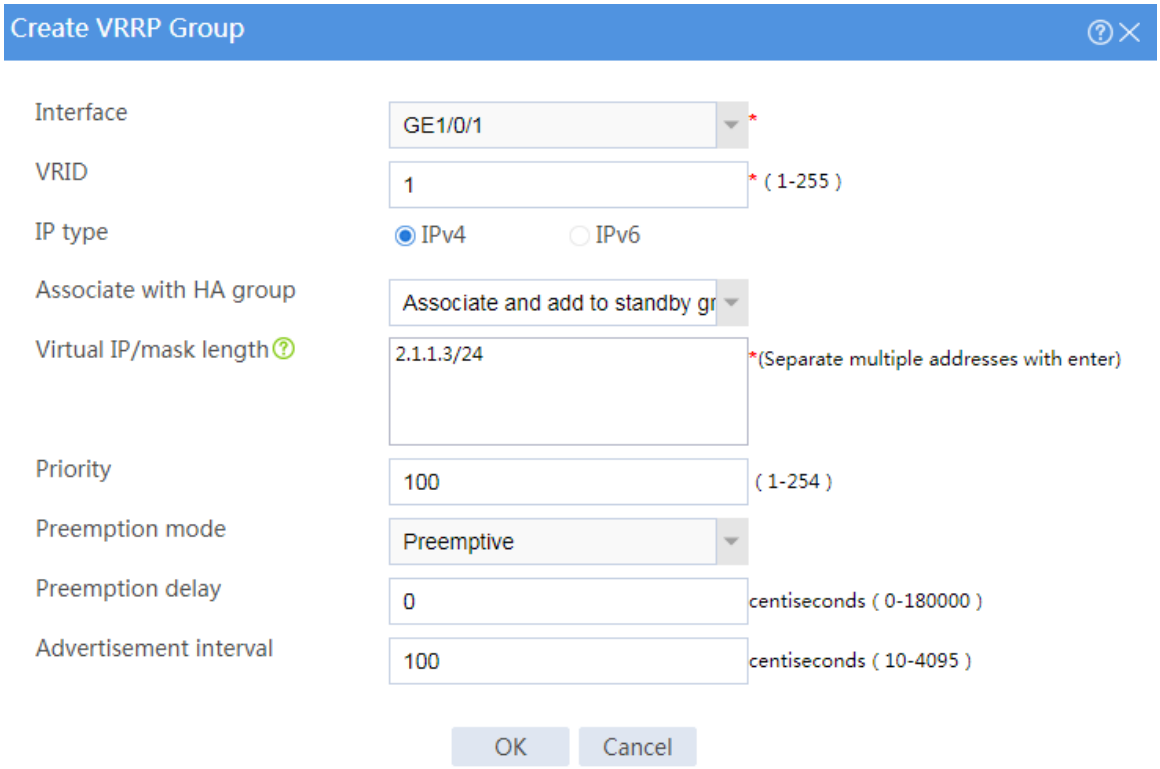


Figure 16 Creating VRRP group 2

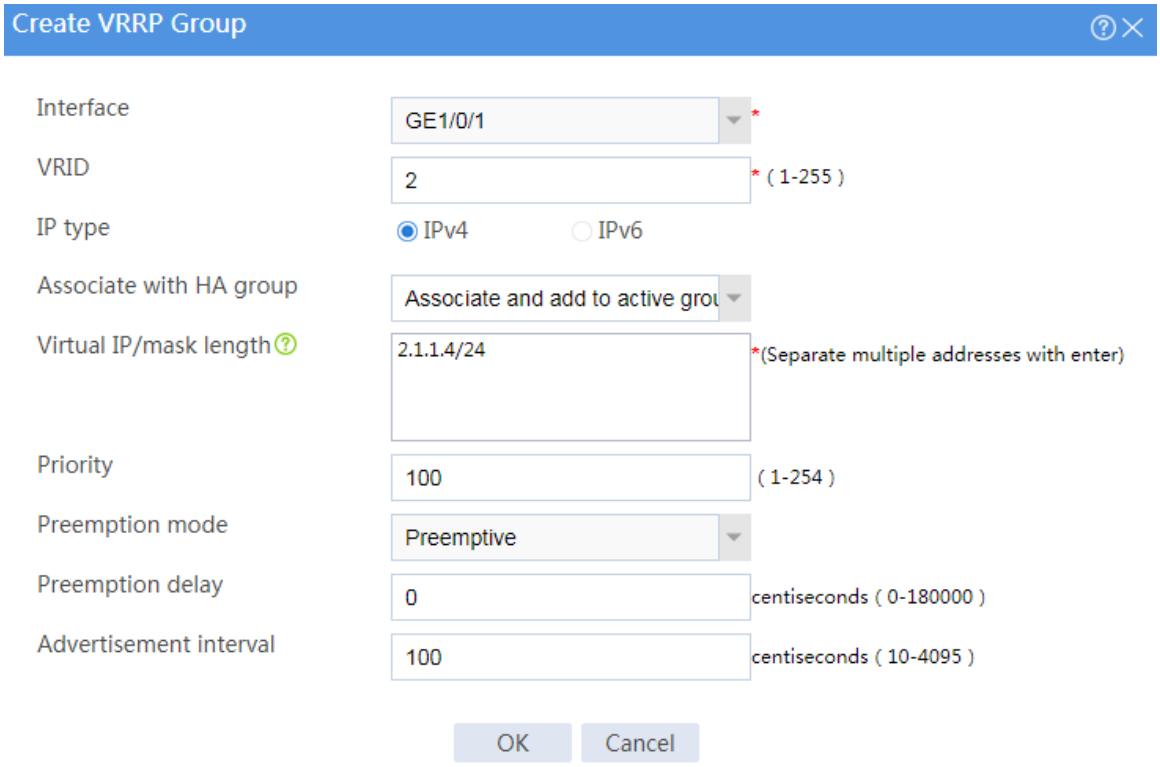


Figure 17 Creating VRRP group 3

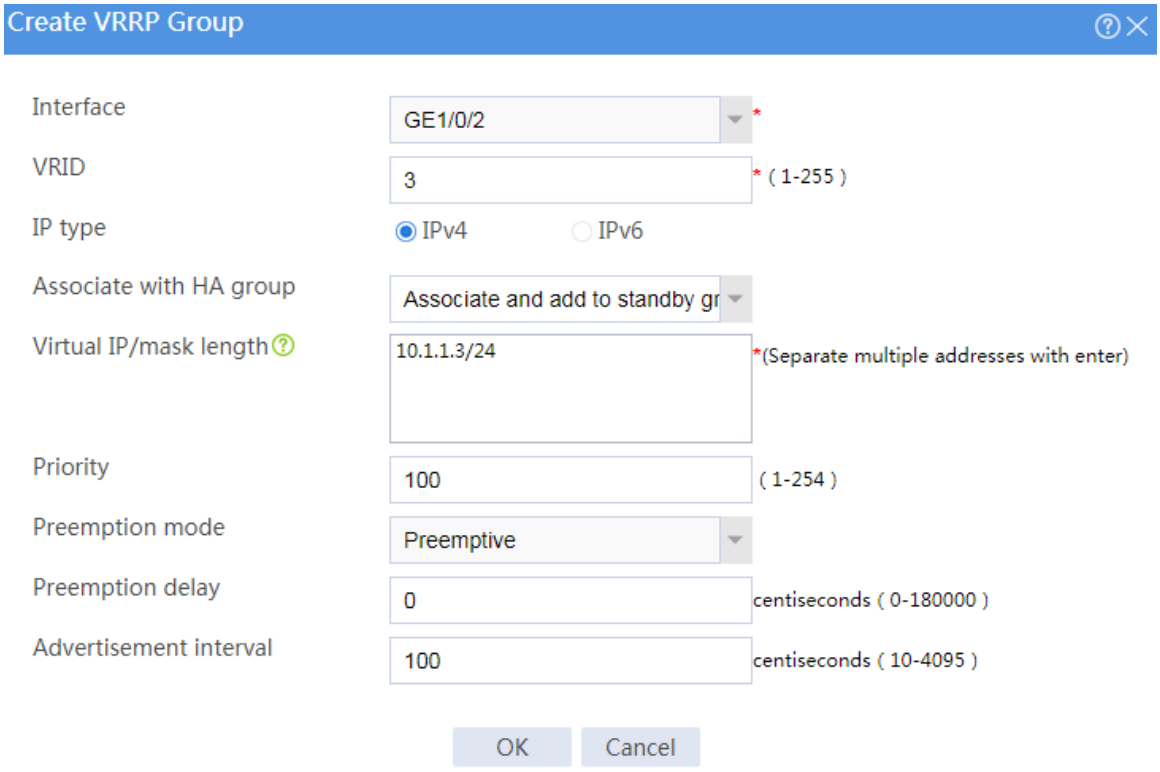
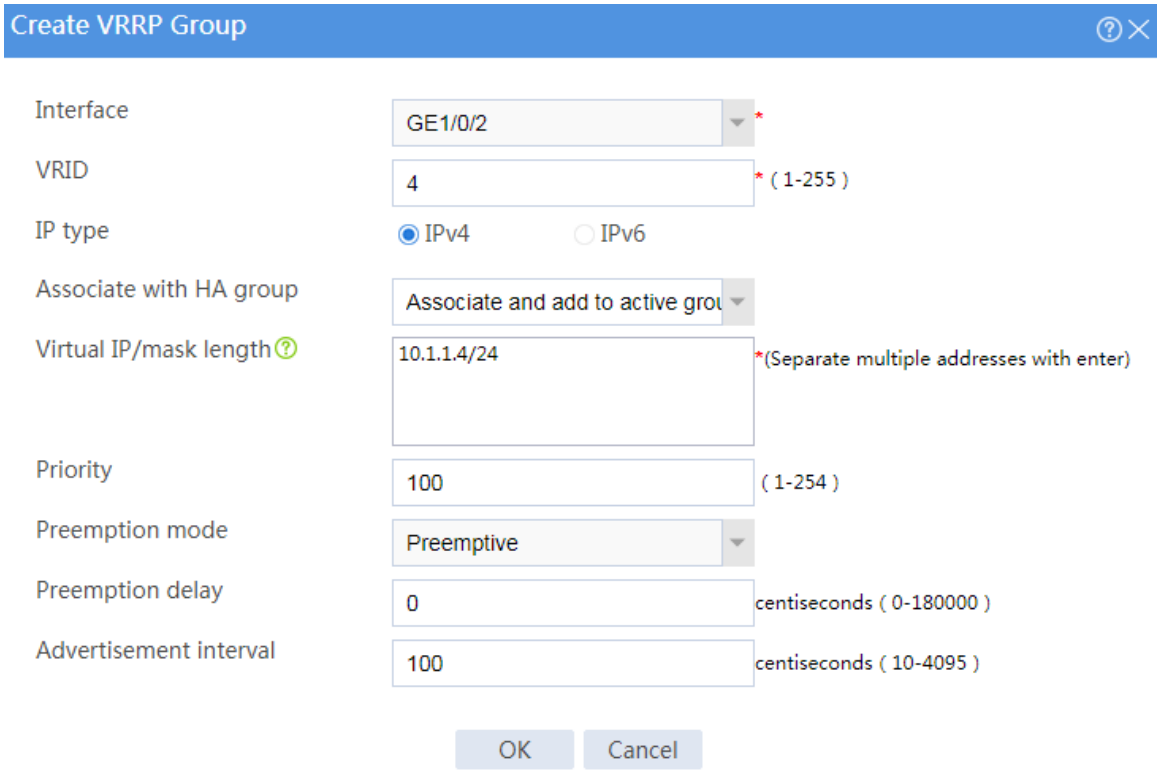


Figure 18 Creating VRRP group 4



Click **OK**.

Configuring the hosts

On some hosts, specify 10.1.1.3 (virtual IP address of VRRP group 3) as the default gateway. On the other hosts, specify 10.1.1.4 (virtual IP address of VRRP group 4) as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that only Device A generates log messages when a host for which Device A forwards traffic communicates with the Internet. Verity that only Device B generates log messages when a host for which Device B forwards traffic communicates with the Internet.

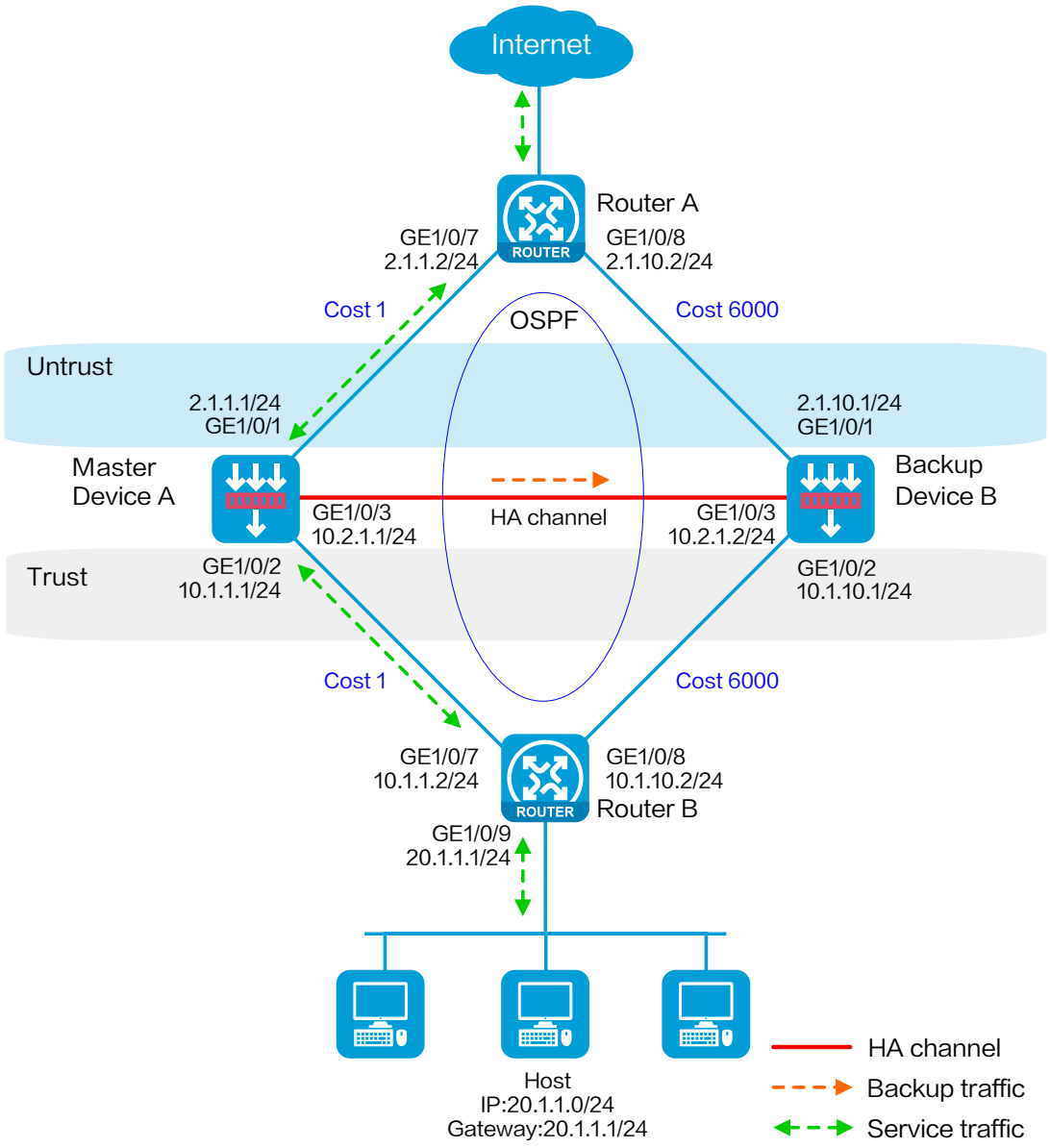
Example: Configuring the HA group in active/standby mode in collaboration with a routing protocol (IPv4)

Network configuration

As shown in Figure 19, set up the HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to collaborate with OSPF.
- Configure the HA group to operate in active/standby mode.
- Configure Device A and Device B as the primary device and the secondary device, respectively.

Figure 19 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Router A

Assign 2.1.1.2/24 to GigabitEthernet 1/0/7.

Assign 2.1.10.2/24 to GigabitEthernet 1/0/8.

Configure OSPF for Router A to have Layer 3 reachability to other devices.

Configuring Router B

Assign 10.1.1.2/24 to GigabitEthernet 1/0/7.

Assign 10.1.10.2/24 to GigabitEthernet 1/0/8.

Configure OSPF for Router B to have Layer 3 reachability to other devices.

Configuring Device A

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. On the **Basic Configuration** tab, select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.1.1/24.

   c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and assign 10.1.1.1/24 to it in the same way you configure GE 1/0/1.

Assign 10.2.1.1/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

This step uses OSPF as an example. You can configure another dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

Click **Create**.

In the dialog box that opens, configure an OSPF instance:

a. Select version **OSPFv2**.

b. Enter instance name **1**.

c. Enter router ID **2.1.1.1**.

d. Use the default settings for other parameters.

e. Click **OK**.

Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

f. Enter area ID **0.0.0.0**.

g. Add subnets **2.1.1.0/24** and **10.1.1.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

3. Configure a security policy to permit service traffic:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

a. Enter security policy name **Trust-Untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Enter source IP address **20.1.1.0/24**.

g. Use the default settings for other parameters.

h. Click **OK**.

4. Configure security policies to permit OSPF protocol packets:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Local**:

a. Enter security policy name **ospf1**.

b. Select source zone **Trust**.

c. Select destination zone **Local**.

d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Select policy group **ospf**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Trust**:

i. Enter security policy name **ospf2**.

j. Select source zone **Local**.

k. Select destination zone **Trust**.

l. Select IP version **IPv4**.

m. Set the action to **Permit**.

n. Select policy group **ospf**.

o. Use the default settings for other parameters.

p. Click **OK**.

Configure a security policy to permit traffic from zone **Untrust** to zone **Local**:

q. Enter security policy name **ospf3**.

r. Select source zone **Untrust**.

s. Select destination zone **Local**.

t. Select IP version **IPv4**.

u. Set the action to **Permit**.

v. Select policy group **ospf**.

w. Use the default settings for other parameters.

x. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Untrust**:

y. Enter security policy name **ospf4**.

z. Select source zone **Local**.

aa. Select destination zone **Untrust**.

bb. Select IP version **IPv4**.

cc. Set the action to **Permit**.

dd. Select policy group **ospf**.

ee. Use the default settings for other parameters.

ff. Click **OK**.

Configuring HA group settings

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **Track**.

Click **Add**.

Configure a track entry:

1. Enter track entry ID **1**.
2. Select the interface module.
3. Select GE 1/0/1 as the monitored interface.
4. Use the default settings for other parameters.

Configure track entry 2 to monitor the state of GE 1/0/2. (Details not shown.)

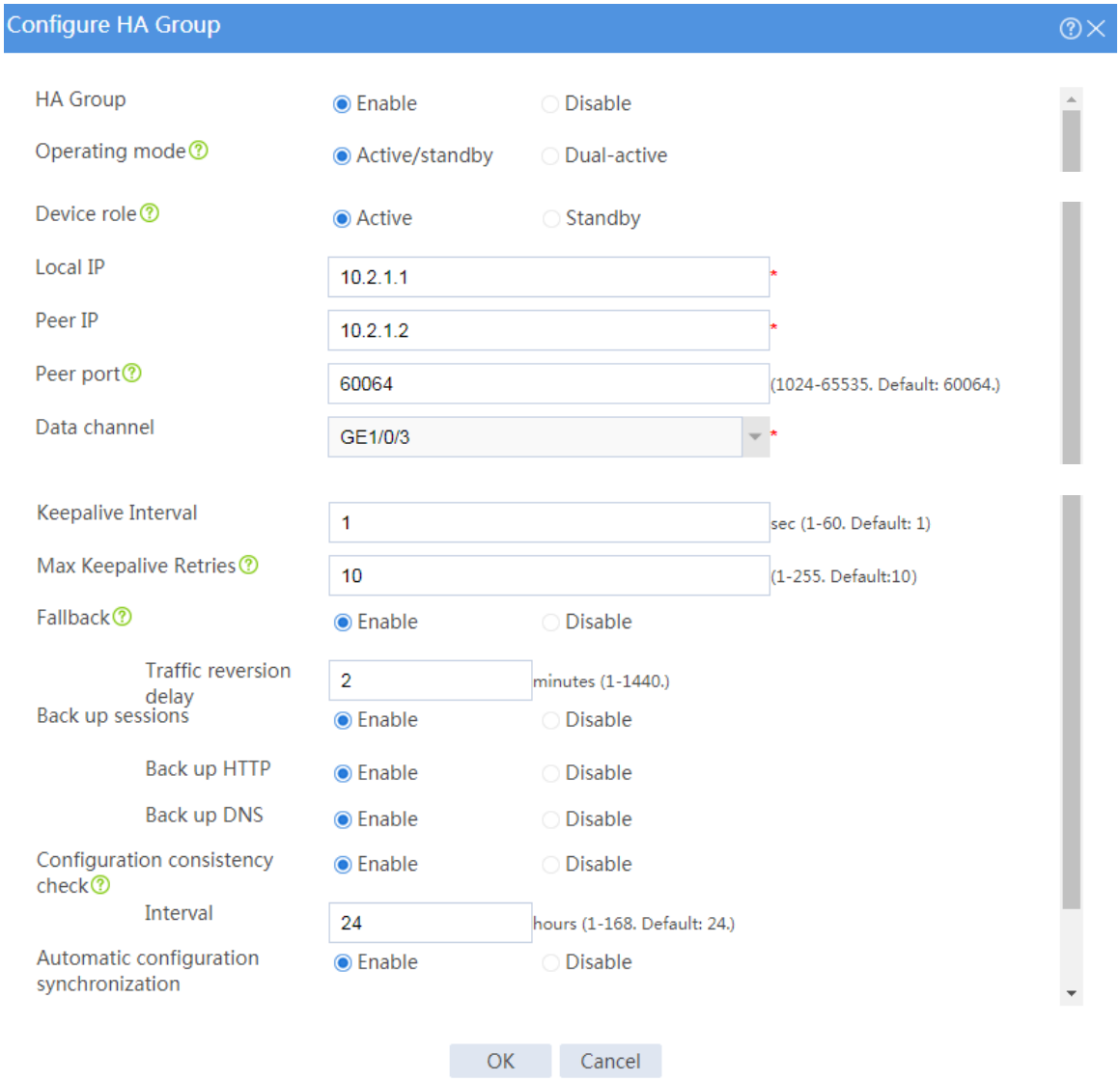
On the top navigation bar, click **System**.

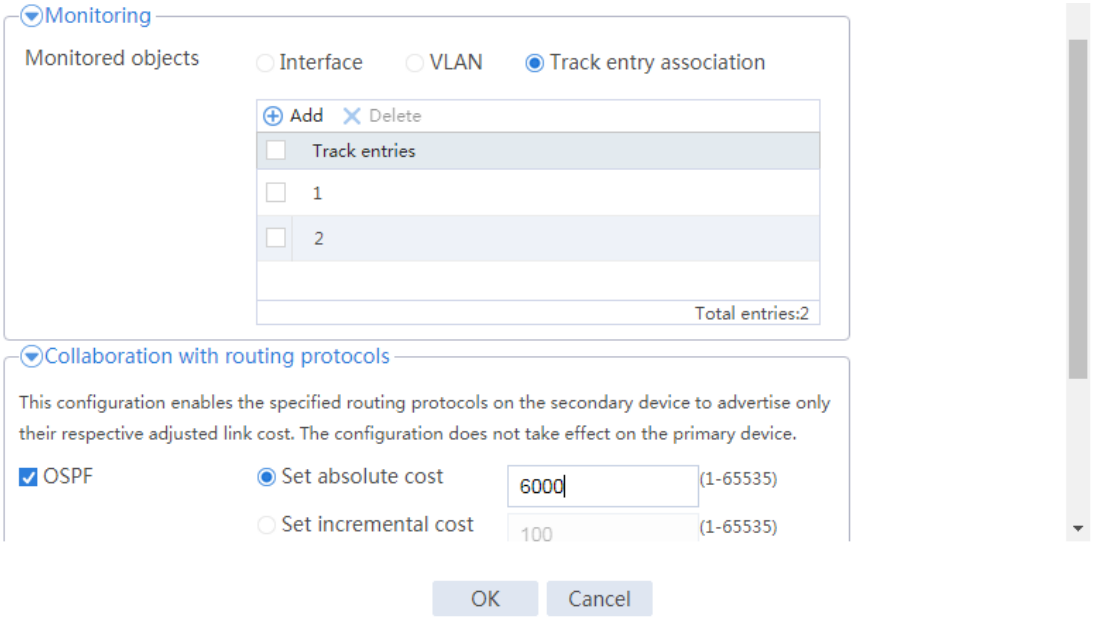
From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 20.

Figure 20 Configuring HA group parameters





Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Assign IP addresses to interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.10.1/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and assign 10.1.10.1/24 to it in the same way you configure GE 1/0/1.

Assign 10.2.1.2/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

This step uses OSPF as an example. You can configure another dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

Click **Create**.

In the dialog box that opens, configure an OSPF instance:

a. Select version **OSPFv2**.

b. Enter instance name **1**.

c. Enter router ID **2.1.10.1**.

d. Use the default settings for other parameters.

e. Click **OK**.

Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

f. Enter area ID **0.0.0.0**.

g. Add subnets **2.1.10.0/24** and **10.1.10.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

Configuring HA group settings

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **Track**.

Click **Add**.

Configure a track entry:

1. Enter track entry ID **1**.
2. Select the interface module.
3. Select GE 1/0/1 as the monitored interface.
4. Use the default settings for other parameters.

Configure track entry 2 to monitor the state of GE 1/0/2. (Details not shown.)

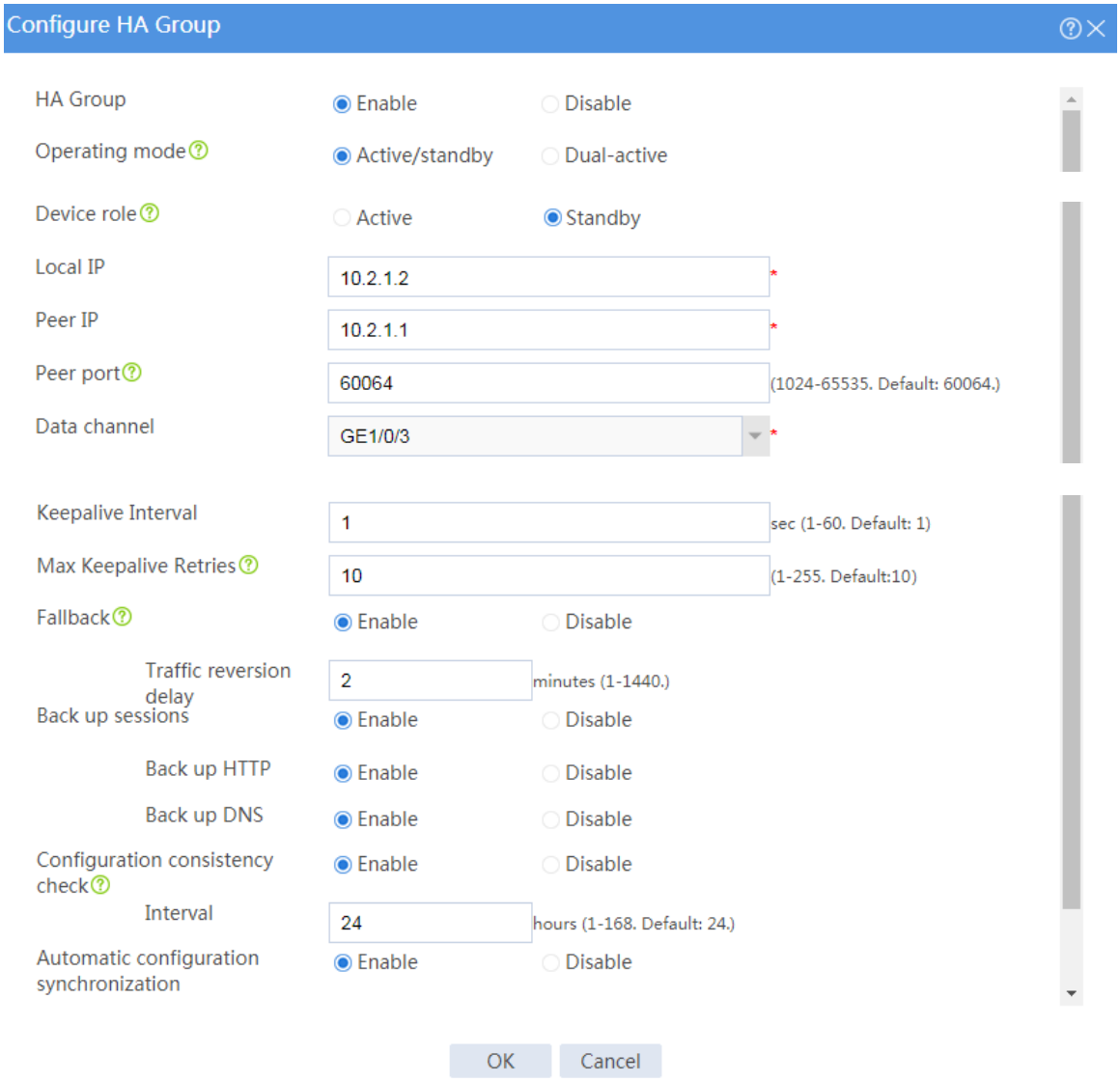
On the top navigation bar, click **System**.

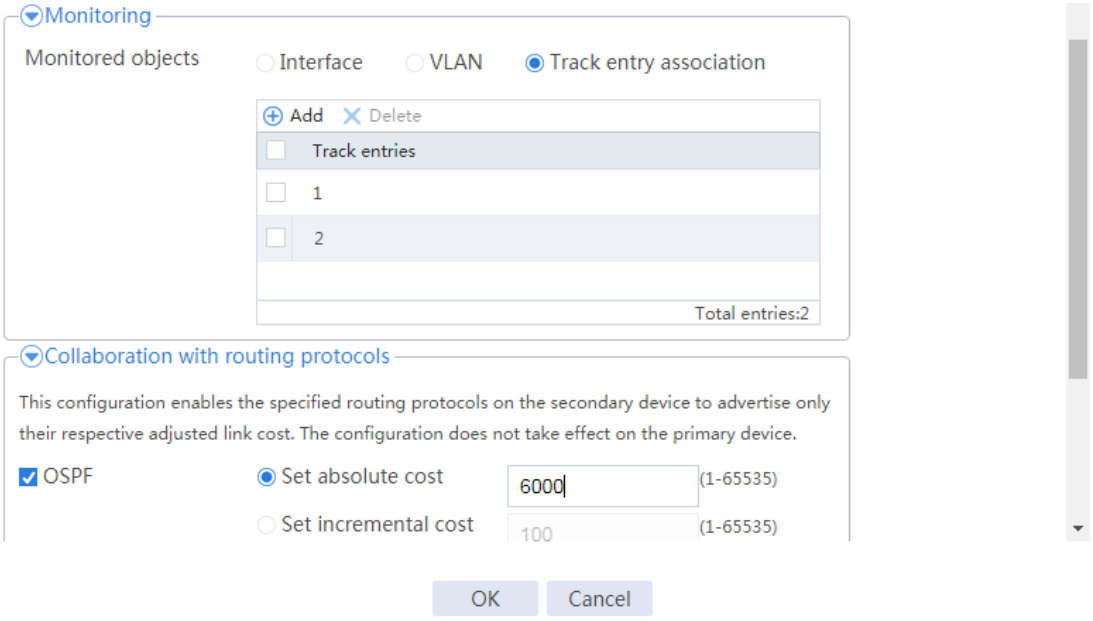
From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 21.

Figure 21 Configuring HA group parameters





Click **OK**.

Configuring the host

On the host, specify 20.1.1.1 as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that only Device A generates log messages when the host communicates with the Internet.

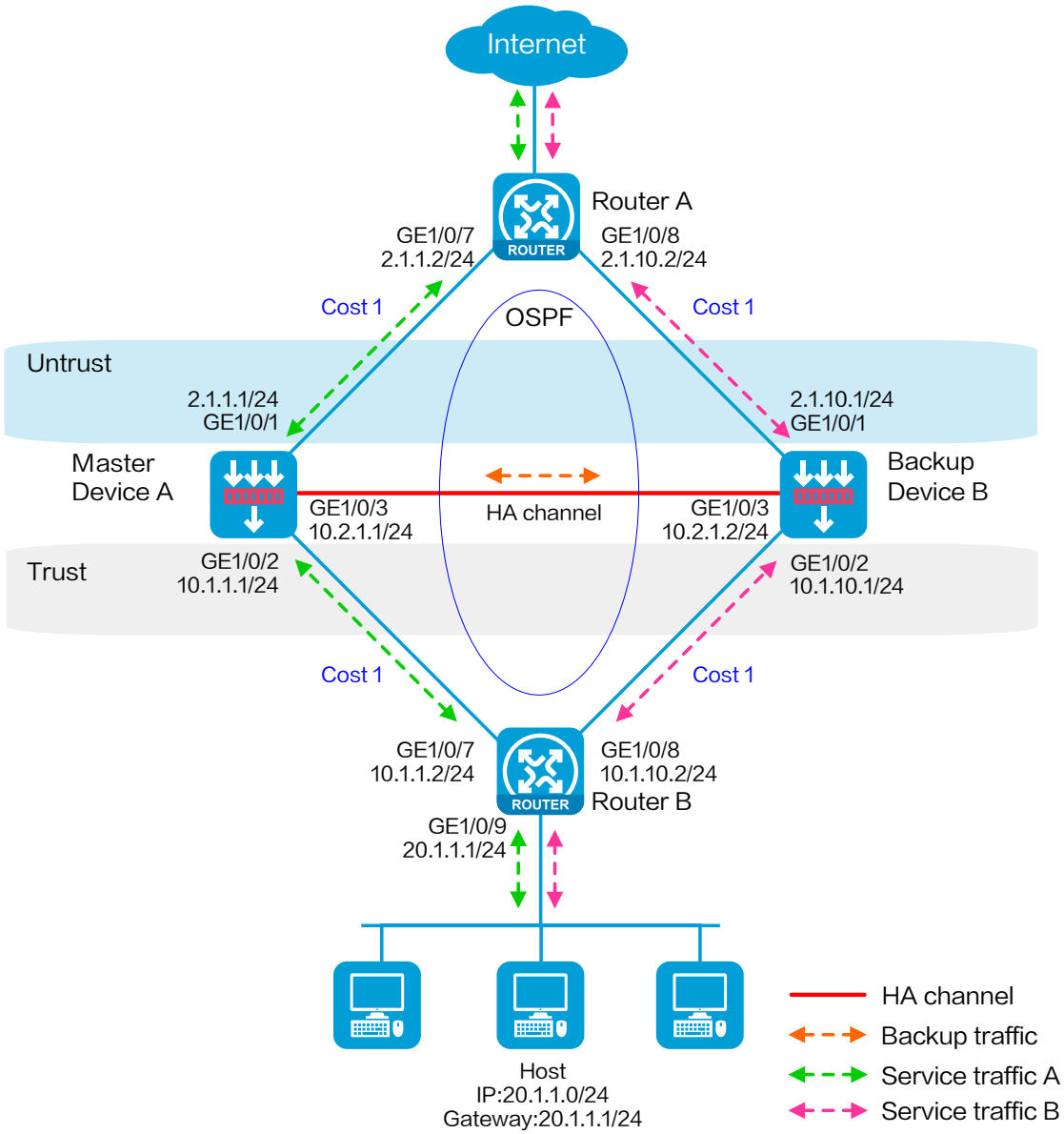
Example: Configuring the HA group in dual-active mode in collaboration with a routing protocol (IPv4)

Network configuration

As shown in Figure 22, set up the HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to collaborate with OSPF.
- Configure the HA group to operate in dual-active mode.
- Configure Device A and Device B to load share traffic.

Figure 22 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Router A

Assign 2.1.1.2/24 to GigabitEthernet 1/0/7.

Assign 2.1.10.2/24 to GigabitEthernet 1/0/8.

Configure OSPF for Router A to have Layer 3 reachability to other devices.

Configure per-flow load sharing for IP forwarding.

Configuring Router B

Assign 10.1.1.2/24 to GigabitEthernet 1/0/7.

Assign 10.1.10.2/24 to GigabitEthernet 1/0/8.

Configure OSPF for Router B to have Layer 3 reachability to other devices.

Configure per-flow load sharing for IP forwarding.

Configuring Device A

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.1.1/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and assign 10.1.1.1/24 to it in the same way you configure GE 1/0/1.

Assign 10.2.1.1/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

This step uses OSPF as an example. You can configure another dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

Click **Create**.

In the dialog box that opens, configure an OSPF instance:

a. Select version **OSPFv2**.

b. Enter instance name **1**.

c. Enter router ID **2.1.1.1**.

d. Use the default settings for other parameters.

e. Click **OK**.

Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

f. Enter area ID **0.0.0.0**.

g. Add subnets **2.1.1.0/24** and **10.1.1.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

3. Configure a security policy to permit service traffic:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

a. Enter security policy name **Trust-Untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Enter source IP address **20.1.1.0/24**.

g. Use the default settings for other parameters.

h. Click **OK**.

4. Configure security policies to permit OSPF protocol packets:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Local**:

a. Enter security policy name **ospf1**.

b. Select source zone **Trust**.

c. Select destination zone **Local**.

d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Select policy group **ospf**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Trust**:

i. Enter security policy name **ospf2**.

j. Select source zone **Local**.

k. Select destination zone **Trust**.

l. Select IP version **IPv4**.

m. Set the action to **Permit**.

n. Select policy group **ospf**.

o. Use the default settings for other parameters.

p. Click **OK**.

Configure a security policy to permit traffic from zone **Untrust** to zone **Local**:

q. Enter security policy name **ospf3**.

r. Select source zone **Untrust**.

s. Select destination zone **Local**.

t. Select IP version **IPv4**.

u. Set the action to **Permit**.

v. Select policy group **ospf**.

w. Use the default settings for other parameters.

x. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Untrust**:

y. Enter security policy name **ospf4**.

z. Select source zone **Local**.

aa. Select destination zone **Untrust**.

bb. Select IP version **IPv4**.

cc. Set the action to **Permit**.

dd. Select policy group **ospf**.

ee. Use the default settings for other parameters.

ff. Click **OK**.

Configuring HA group settings

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **Track**.

Click **Add**.

Configure a track entry:

1. Enter track entry ID **1**.
2. Select the interface module.
3. Select GE 1/0/1 as the monitored interface.
4. Use the default settings for other parameters.

Configure track entry 2 to monitor the state of GE 1/0/2. (Details not shown.)

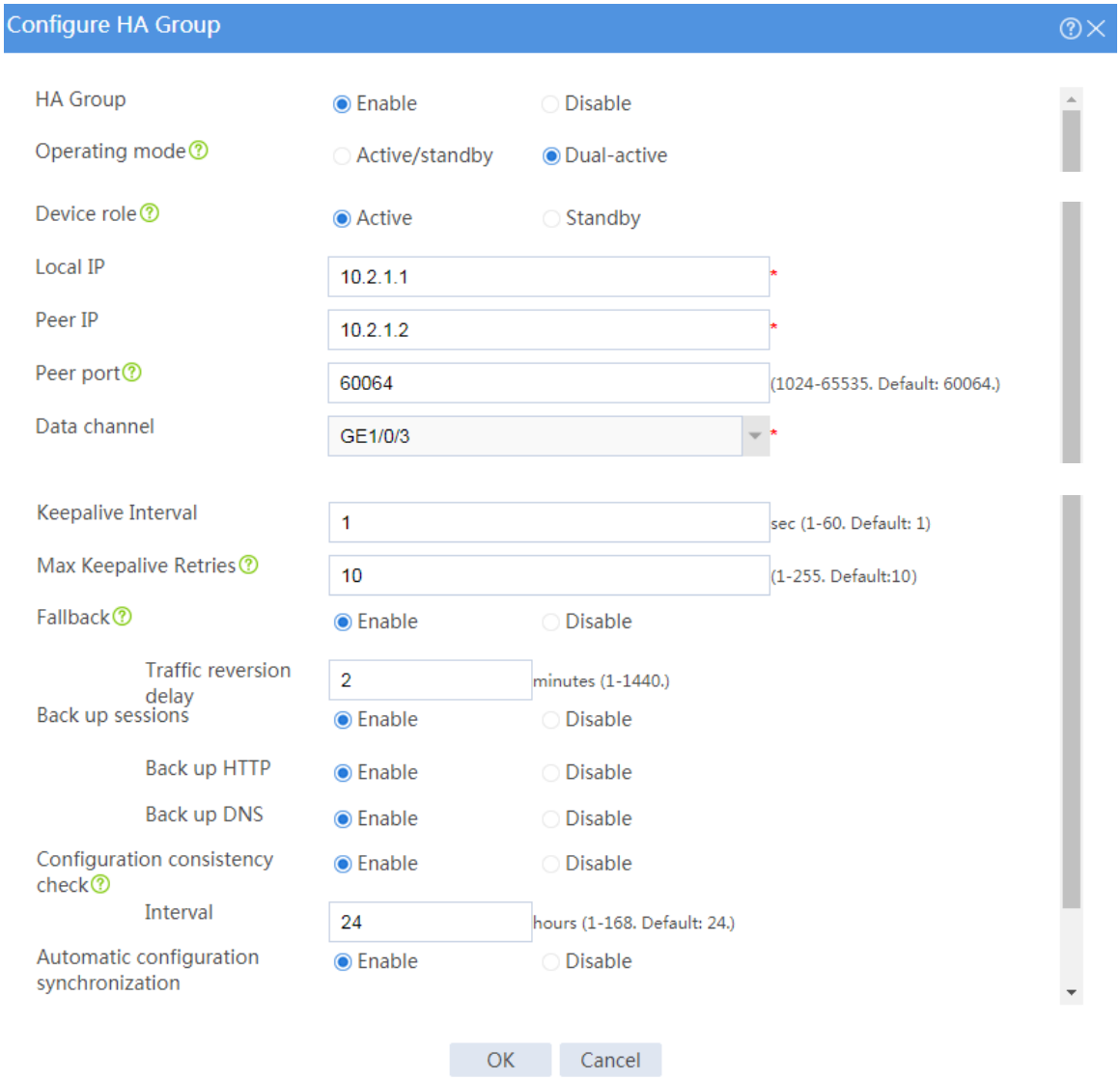
On the top navigation bar, click **System**.

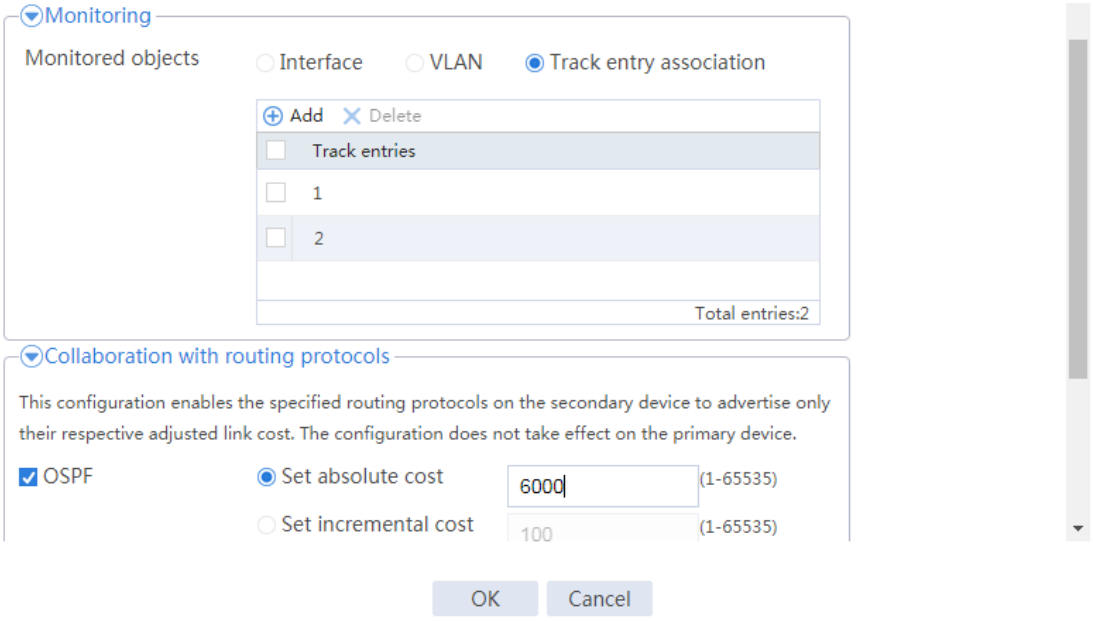
From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 23.

Figure 23 Configuring HA group parameters





Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Assign IP addresses to interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.1.10.1/24.

c. Use the default settings for other parameters.

d. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and assign 10.1.10.1/24 to it in the same way you configure GE 1/0/1.

Assign 10.2.1.2/24 to GE 1/0/3 in the same way you configure GE 1/0/1.

2. Configure routing:

This step uses OSPF as an example. You can configure another dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

Click **Create**.

In the dialog box that opens, configure an OSPF instance:

a. Select version **OSPFv2**.

b. Enter instance name **1**.

c. Enter router ID **2.1.10.1**.

d. Use the default settings for other parameters.

e. Click **OK**.

Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

f. Enter area ID **0.0.0.0**.

g. Add subnets **2.1.10.0/24** and **10.1.10.0/24**.

h. Use the default settings for other parameters.

i. Click **OK**.

Configuring HA group settings

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **Track**.

Click **Add**.

Configure a track entry:

1. Enter track entry ID **1**.
2. Select the interface module.
3. Select GE 1/0/1 as the monitored interface.
4. Use the default settings for other parameters.

Configure track entry 2 to monitor the state of GE 1/0/2. (Details not shown.)

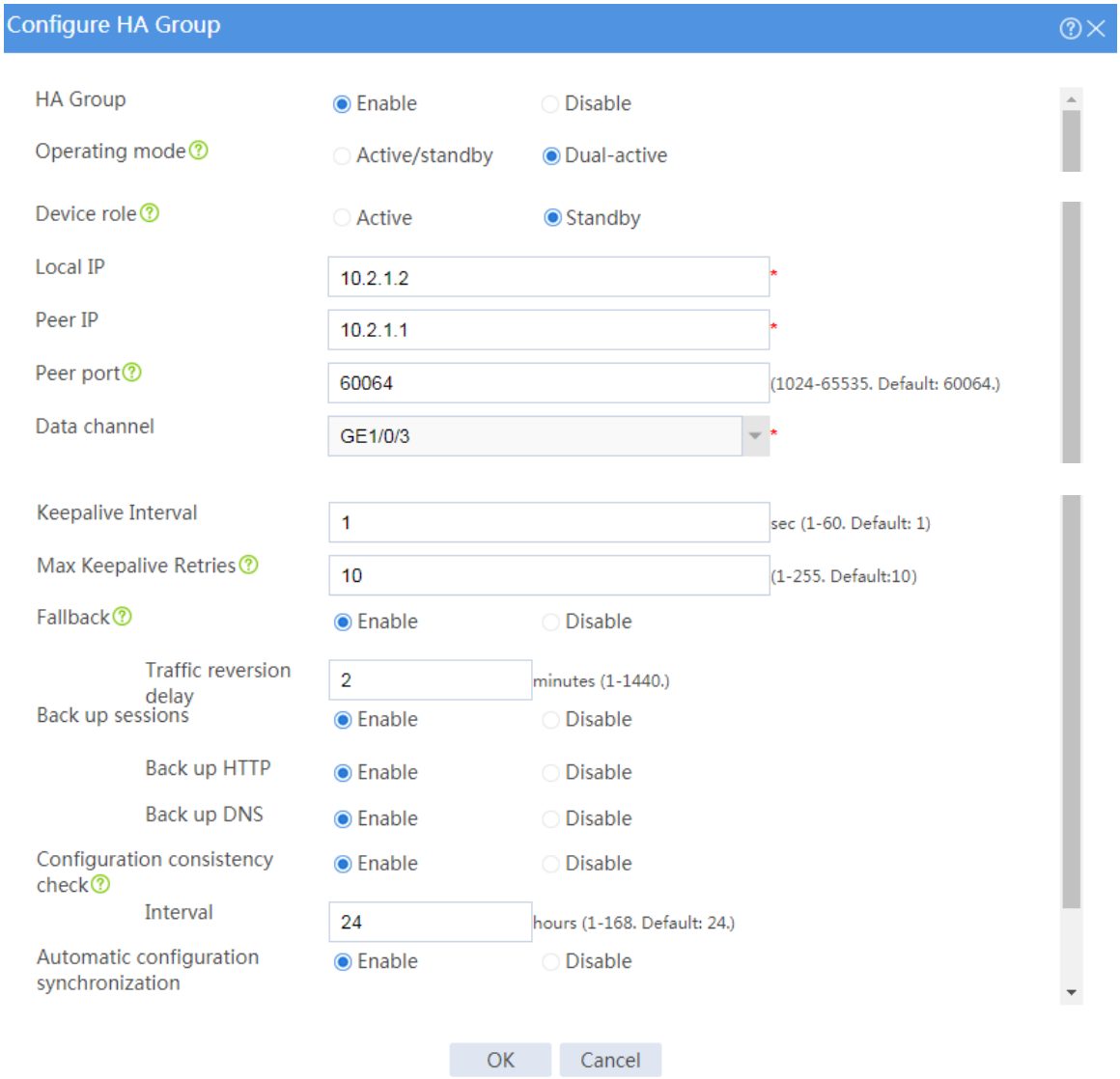
On the top navigation bar, click **System**.

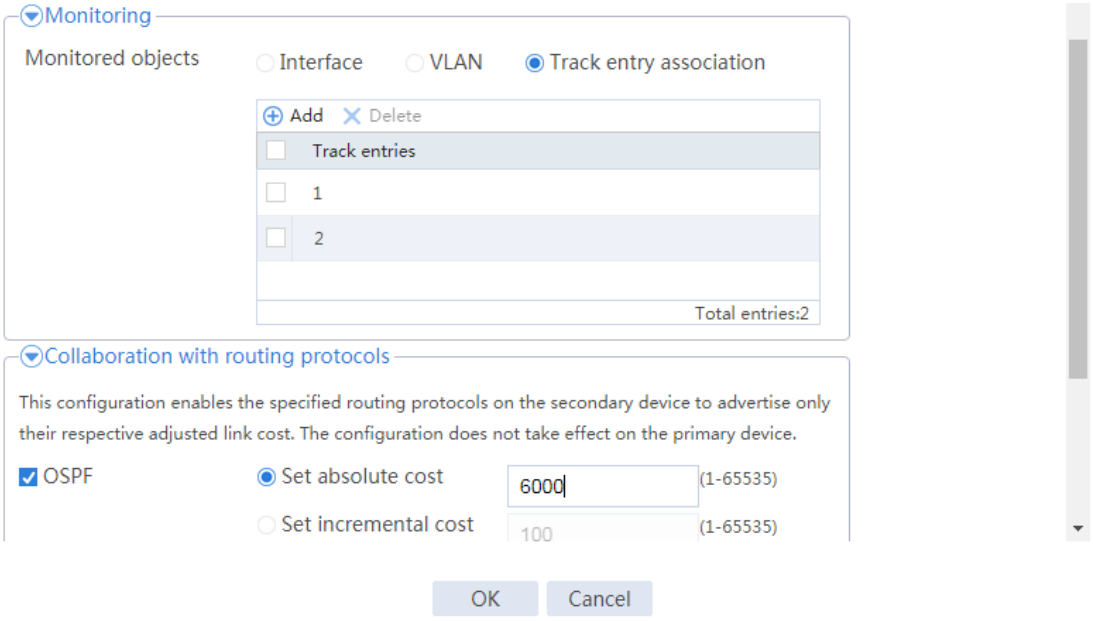
From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 24.

Figure 24 Configuring HA group parameters





Click **OK**.

Configuring the hosts

On the hosts, specify 20.1.1.1 as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that both Device A and Device B generate log messages when the hosts communicate with the Internet.

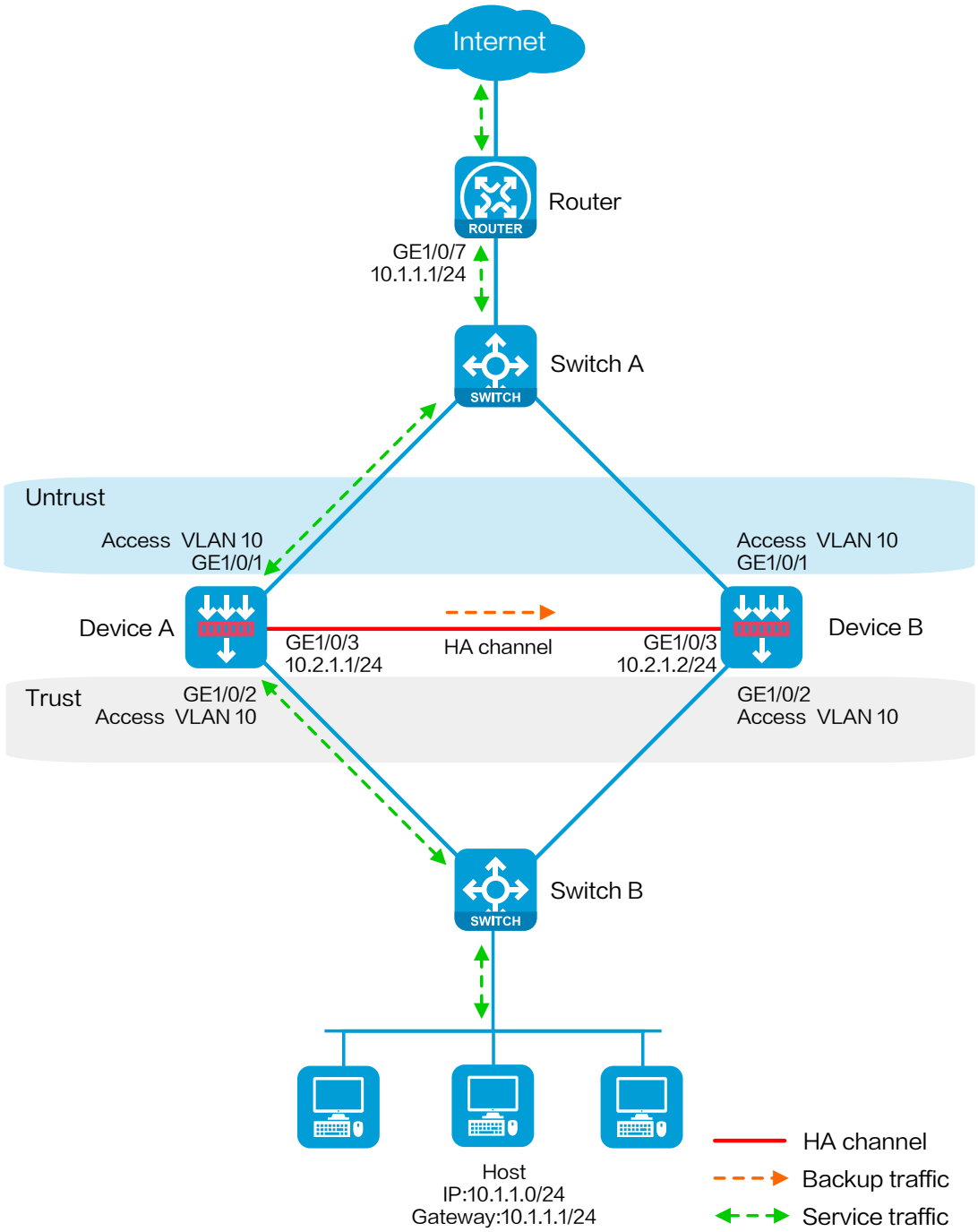
Example: Configuring a transparent in-path HA group in active/standby mode (IPv4)

Network configuration

As shown in Figure 25, set up a transparent in-path HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to operate in active/standby mode.
- Connect Switch A and Switch B to Layer 2 interfaces of the HA group.
- Configure Device A and Device B as the primary device and the secondary device, respectively.

Figure 25 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Switch A

Create VLAN 10.

Configure the interfaces attached to the HA group and the router to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring Switch B

Create VLAN 10.

Configure the interfaces attached to the HA group and the host to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring Device A

Configuring basic network settings

1. Configure Layer 2 service interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Link** > **VLANs**.

   # Click **Create**.

   a. Enter VLAN ID **10**.

   b. Click **OK**.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

c. Select the Layer 2 link mode.

d. Select security zone **Untrust**.

e. Select VLAN 10.

f. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

g. Use the default settings for other parameters.

h. Click **OK**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

i. Select the Layer 2 link mode.

j. Select security zone **Trust**.

k. Select VLAN 10.

l. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

m. Use the default settings for other parameters.

n. Click **OK**.

2. Assign IP addresses to interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/3.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.2.1.1/24.

b. Use the default settings for other parameters.

c. Click **OK**.

3. Configure a security policy to permit service traffic:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

a. Enter security policy name **Trust-Untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Enter source IP address **10.1.1.0/24**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configuring HA group settings

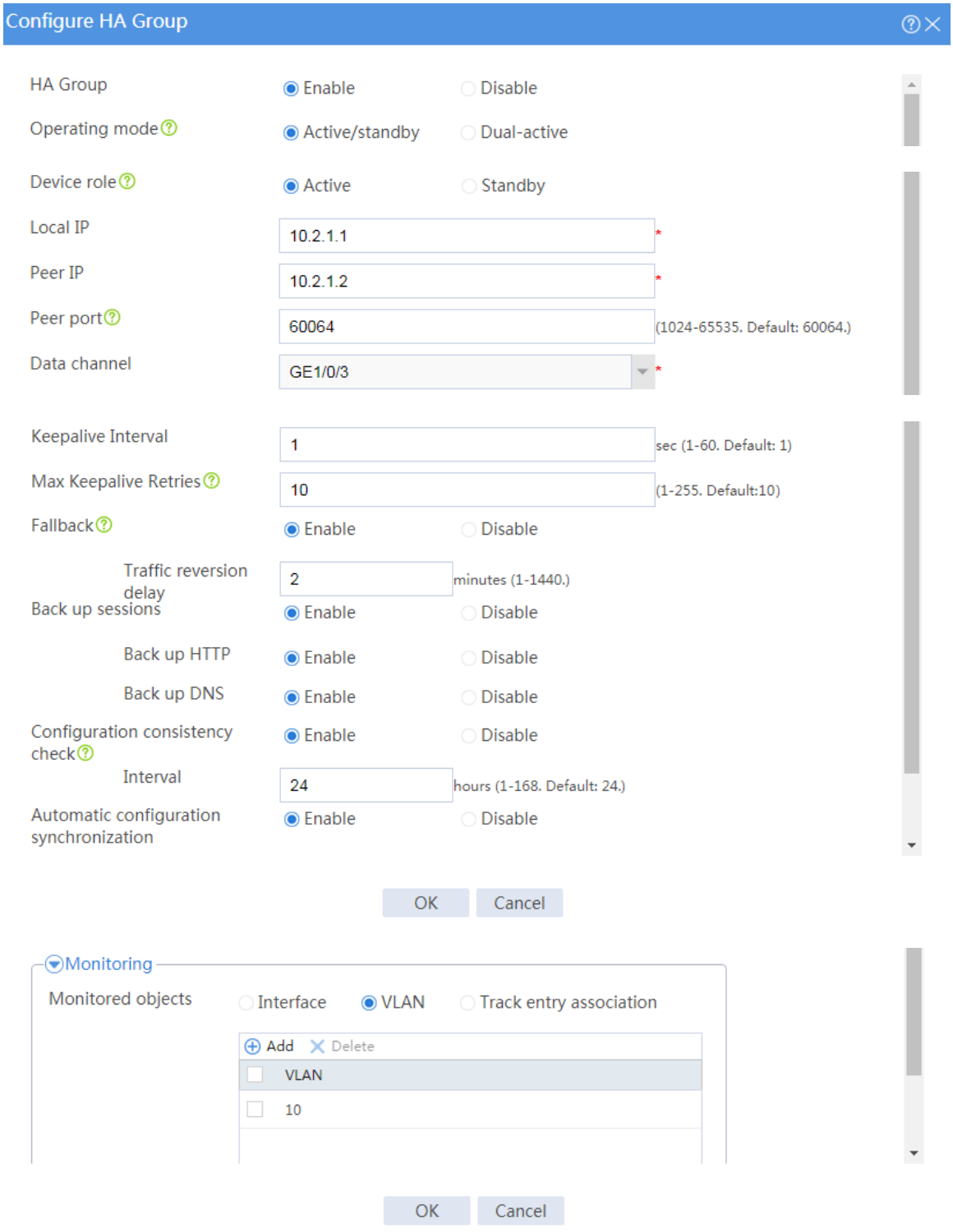
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 26.

Figure 26 Configuring HA group parameters



Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Configure Layer 2 service interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Link** > **VLANs**.

Click **Create**.

a. Enter VLAN ID **10**.

b. Click **OK**.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

c. Select the Layer 2 link mode.

d. Select security zone **Untrust**.

e. Select VLAN 10.

f. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

g. Use the default settings for other parameters.

h. Click **OK**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

i. Select the Layer 2 link mode.

j. Select security zone **Trust**.

k. Select VLAN 10.

l. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

m. Use the default settings for other parameters.

n. Click **OK**.

2. Assign IP addresses to interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/3.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.2.1.2/24.

b. Use the default settings for other parameters.

c. Click **OK**.

Configuring HA group settings

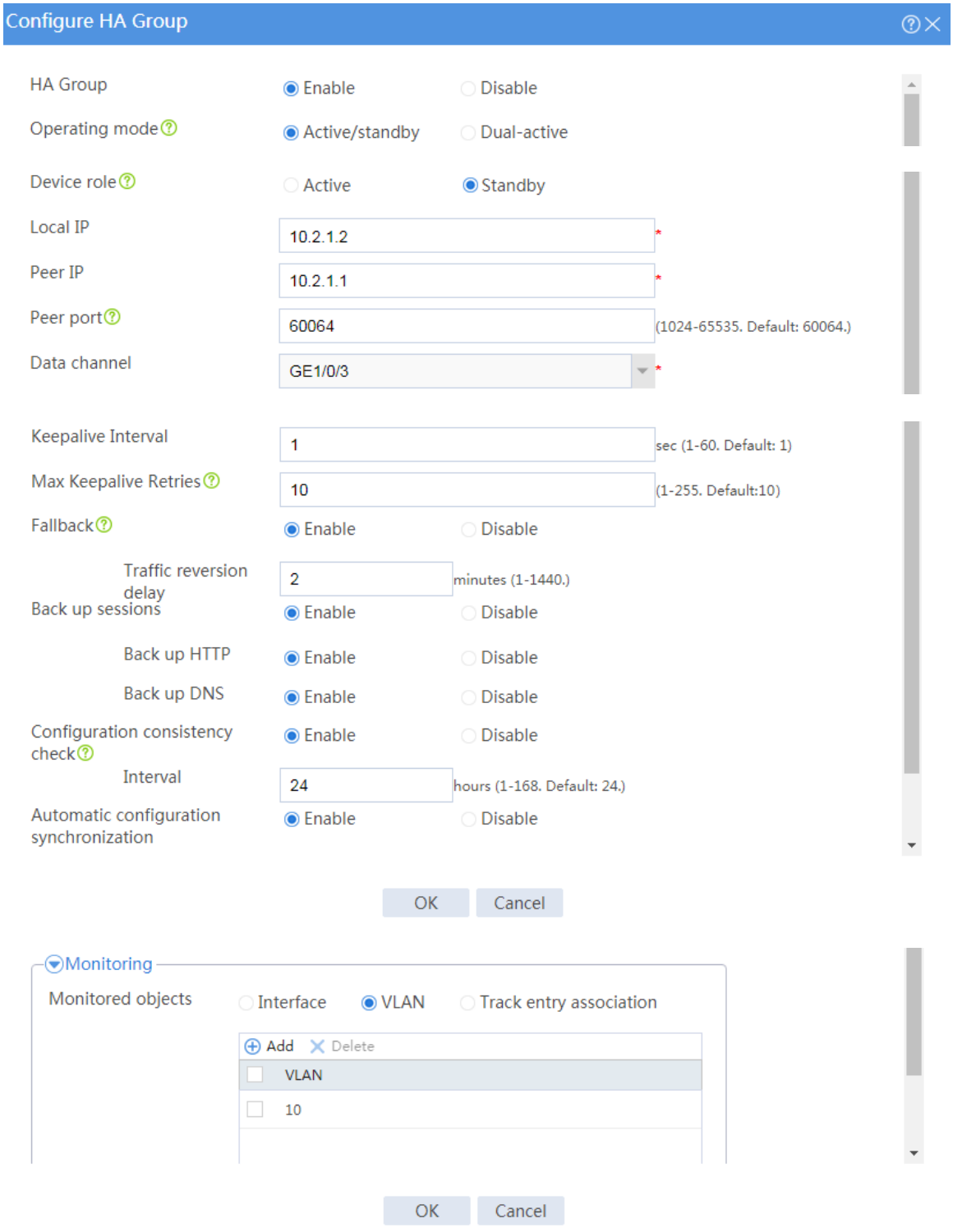
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 27.

Figure 27 Configuring HA group parameters



Click **OK**.

Configuring the host

On the host, specify 10.1.1.1 as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that only Device A generates log messages when the host communicates with the Internet.

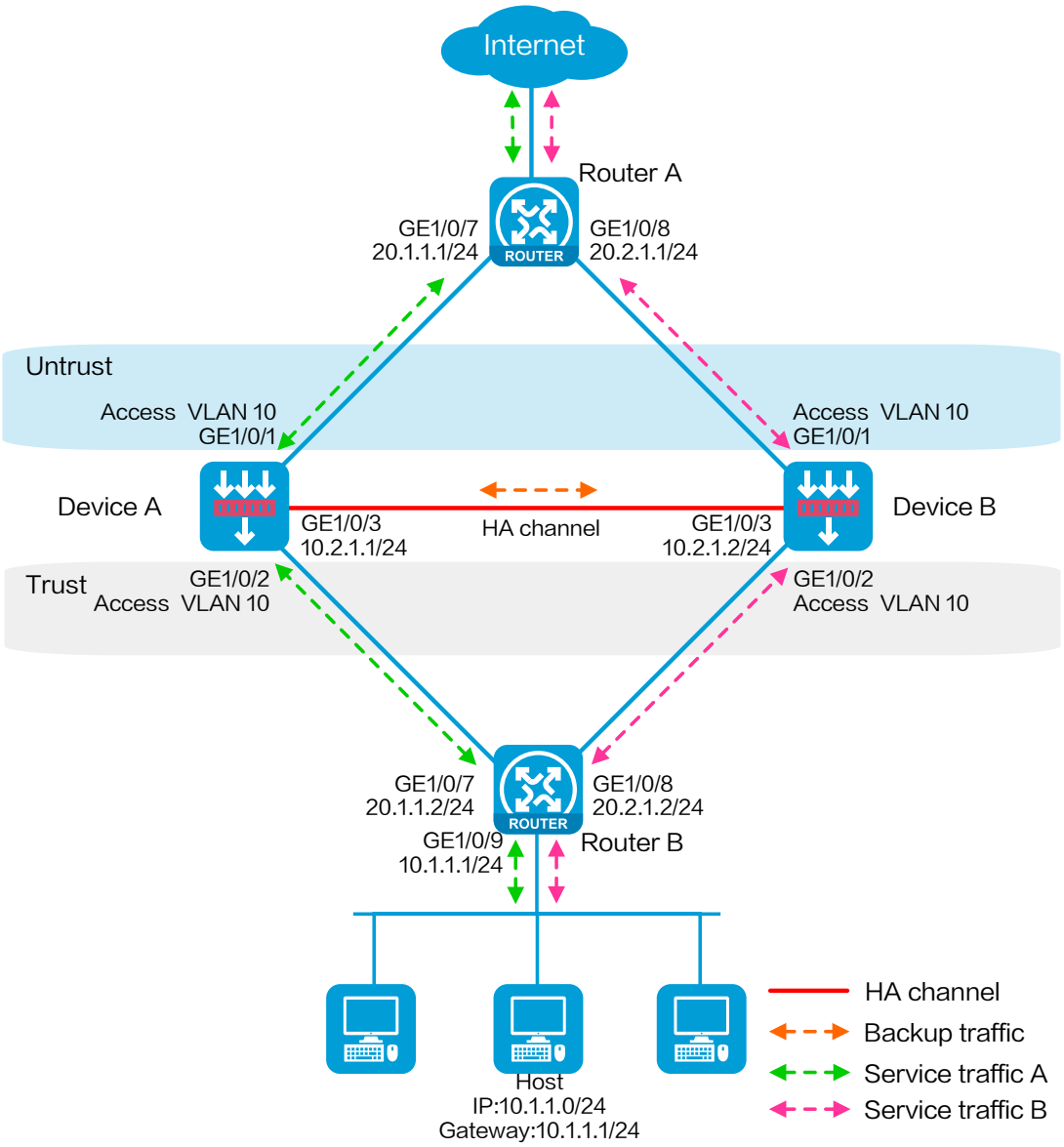
Example: Configuring a transparent in-path HA group in dual-active mode (IPv4)

Network configuration

As shown in Figure 28, set up a transparent in-path HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to operate in dual-active mode.
- Connect Router A and Router B to Layer 2 interfaces of the HA group.
- Configure Device A and Device B to load share traffic.

Figure 28 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Router A

Configure OSPF for the hosts to access the Internet and for Device A and Device B to load share the traffic sent to the hosts.

Configuring Router B

Configure OSPF for the hosts to access the Internet and for Device A and Device B to load share the traffic sent to the hosts.

Configuring Device A

Configuring basic network settings

1. Configure Layer 2 service interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Link** > **VLANs**.

   # Click **Create**.

   a. Enter VLAN ID **10**.

   b. Click **OK**.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   c. Select the Layer 2 link mode.

d. Select security zone **Untrust**.

e. Select VLAN 10.

f. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

g. Use the default settings for other parameters.

h. Click **OK**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

i. Select the Layer 2 link mode.

j. Select security zone **Trust**.

k. Select VLAN 10.

l. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

m. Use the default settings for other parameters.

n. Click **OK**.

2. Assign IP addresses to interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/3.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.2.1.1/24.

b. Use the default settings for other parameters.

c. Click **OK**.

3. Configure a security policy to permit service traffic:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

a. Enter security policy name **Trust-Untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Enter source IP address **10.1.1.0/24**.

g. Use the default settings for other parameters.

h. Click **OK**.

4. Configure security policies to permit OSPF protocol packets:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

a. Enter security policy name **ospf1**.

b. Select source zone **Untrust**.

c. Select destination zone **Local**.

d. Select IP version **IPv4**.

e. Set the action to **Permit**.

f. Select policy group **ospf**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configure a security policy to permit traffic from zone **Untrust** to zone **Trust**:

i. Enter security policy name **ospf2**.

j. Select source zone **Untrust**.

k. Select destination zone **Trust**.

l. Select IP version **IPv4**.

m. Set the action to **Permit**.

n. Select policy group **ospf**.

o. Use the default settings for other parameters.

p. Click **OK**.

Configuring HA group settings

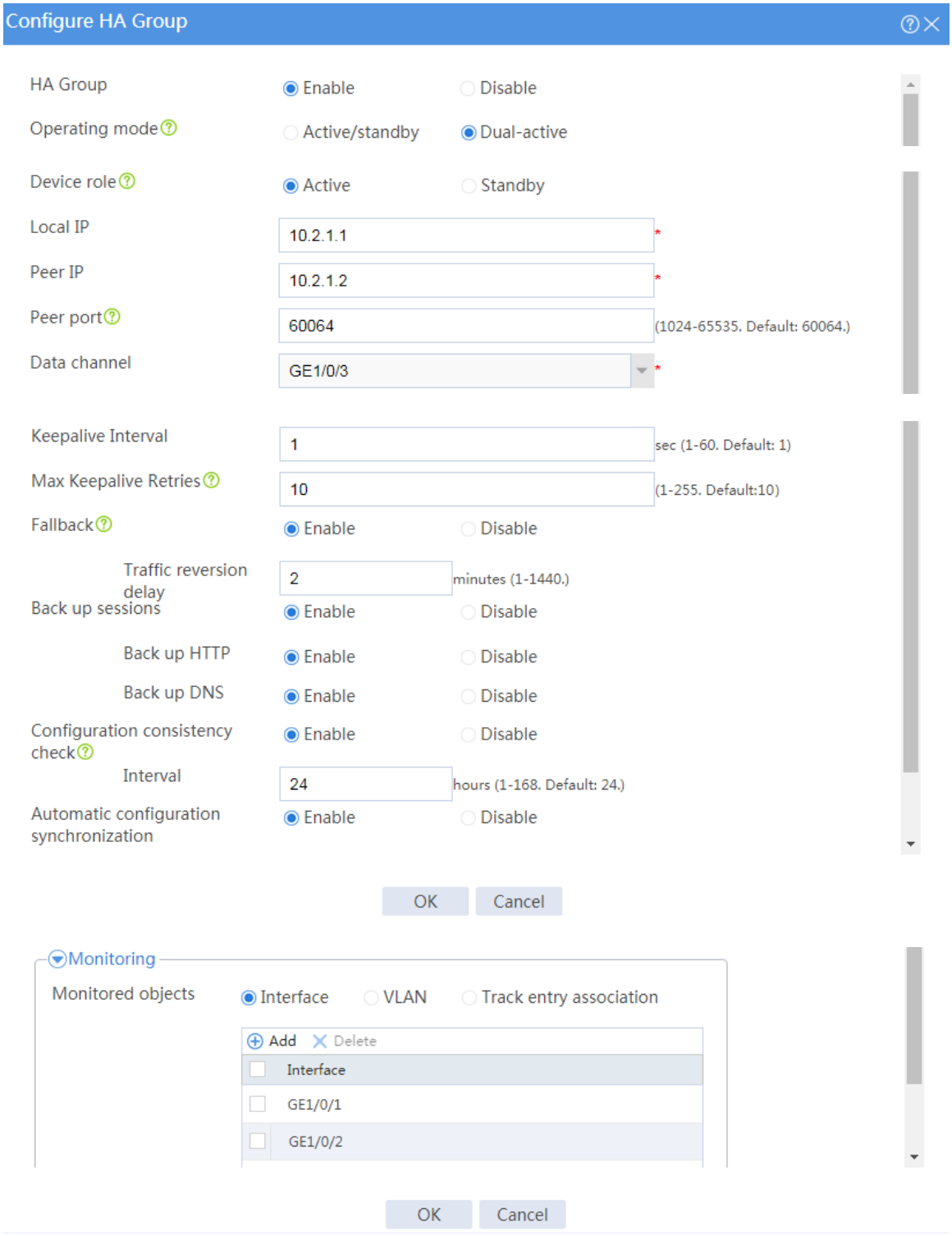
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 29.

Figure 29 Configuring HA group parameters



Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Configure Layer 2 service interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Link** > **VLANs**.

Click **Create**.

a. Enter VLAN ID **10**.

b. Click **OK**.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

c. Select the Layer 2 link mode.

d. Select security zone **Untrust**.

e. Select VLAN 10.

f. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

g. Use the default settings for other parameters.

h. Click **OK**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

i. Select the Layer 2 link mode.

j. Select security zone **Trust**.

k. Select VLAN 10.

l. On the VLAN tab, set the link type to **Access** and enter PVID **10**.

m. Use the default settings for other parameters.

n. Click **OK**.

2. Assign IP addresses to interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/3.

In the dialog box that opens, configure the interface:

a. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.2.1.2/24.

b. Use the default settings for other parameters.

c. Click **OK**.

Configuring HA group settings

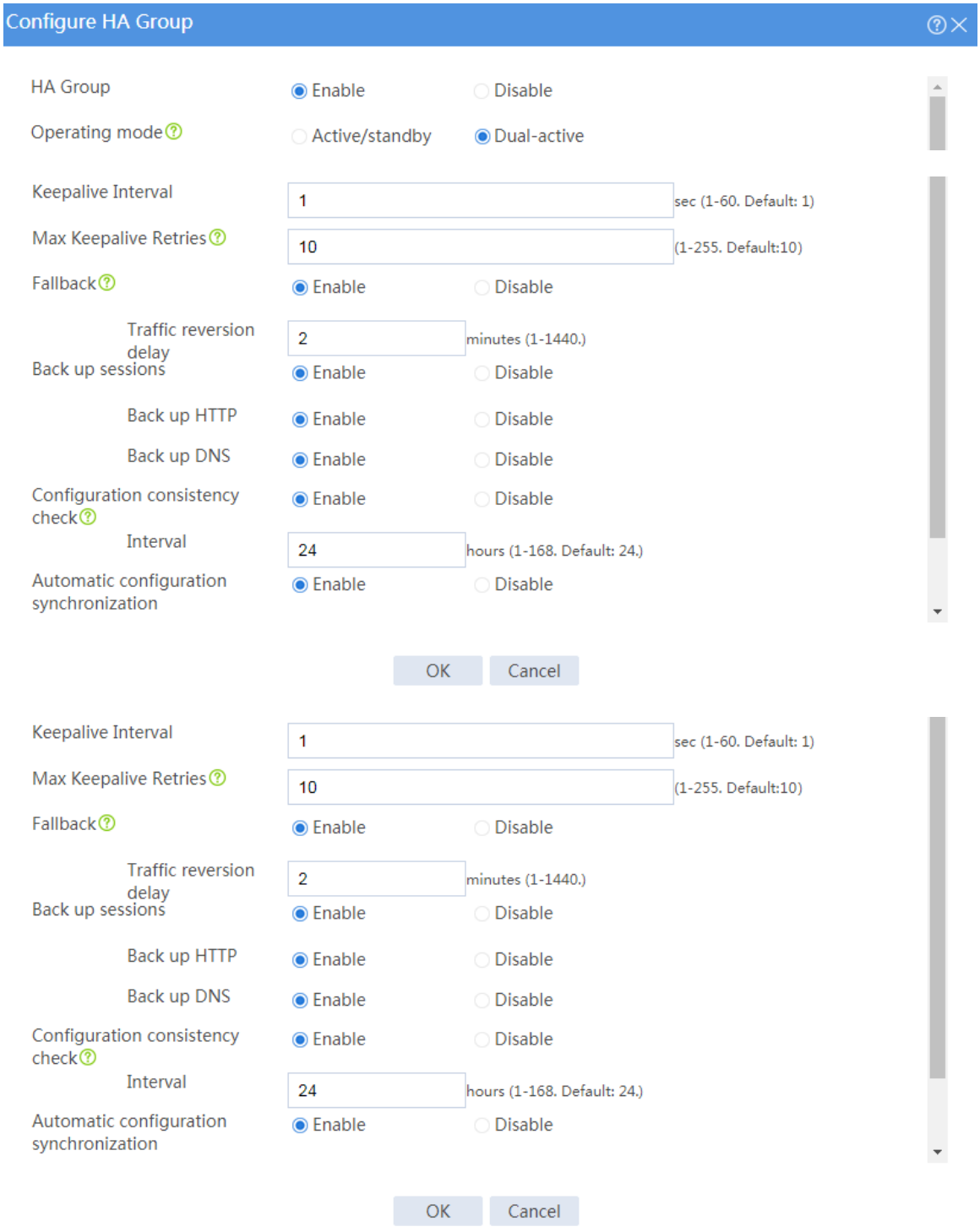
On the top navigation bar, click **System**.

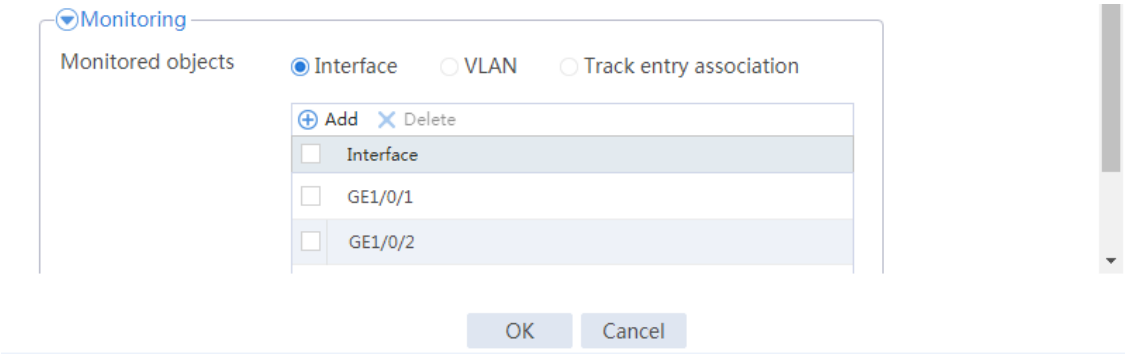
From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 30.

Figure 30 Configuring HA group parameters





Click **OK**.

Configuring the hosts

On the hosts, specify 10.1.1.1 as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that both Device A and Device B generate log messages when the hosts communicate with the Internet.

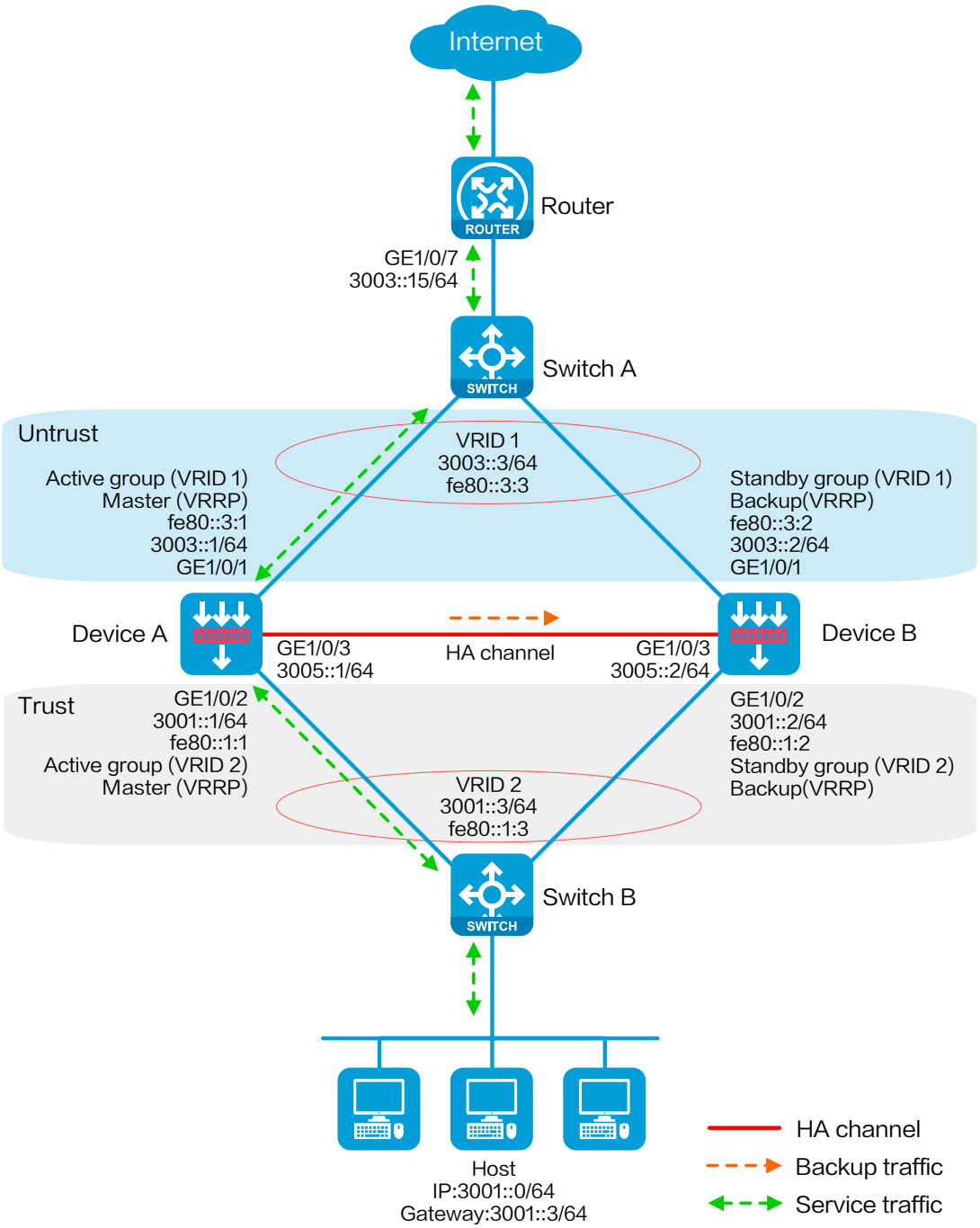
Example: Configuring the HA group in active/standby mode in collaboration with VRRP (IPv6)

Network configuration

As shown in Figure 31, set up the HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to collaborate with VRRP.
- Configure the HA group to operate in active/standby mode.
- Configure Device A and Device B as the primary device and the secondary device, respectively.

Figure 31 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Switch A

Create VLAN 10.

Configure the interfaces attached to the HA group and the router to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring Switch B

Create VLAN 10.

Configure the interfaces attached to the HA group and the host to operate at Layer 2. Assign them to VLAN 10 as access interfaces.

Configuring the router

Assign 3003::15/64 to GigabitEthernet 1/0/7.

Configure routes as follows:

- Specify 3003::3/64 (virtual IP address of VRRP group 1) as the next hop of the routes to the internal network.
- Specify the IP address of the peer interface attached to the traffic outgoing interface as the next hop of the route to the Internet.

Configuring Device A

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. On the **Basic Configuration** tab, select the **Untrust** security zone.

   b. On the **IPv6 Address** tab, enter global unicast address **3003::1/64** and link local address **fe80::3:1**.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Click the **Edit** icon for GE 1/0/2.

   # In the dialog box that opens, configure the interface:

   e. On the **Basic Configuration** tab, select the **Trust** security zone.

   f. On the **IPv6 Address** tab, enter global unicast address **3001::1/64** and link local address **fe80::1:1**.

   g. Use the default settings for other parameters.

   h. Click **OK**.

   # Click the **Edit** icon for GE 1/0/3.

   # In the dialog box that opens, configure the interface:

   i. On the **IPv6 Address** tab, enter global unicast address **3005::1/64** and configure the interface to use a link local address generated automatically.

   j. Use the default settings for other parameters.

   k. Click **OK**.

2. Configure routing:

This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv6 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv6 static route:

a. Enter destination IP address **0::0**.

b. Enter mask length **0**.

c. Enter next hop address **3003::15**.

d. Use the default settings for other parameters.

e. Click **OK**.

3. Configure a security policy to permit service traffic:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

a. Enter security policy name **Trust-Untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select IP version **IPv6**.

e. Set the action to **Permit**.

f. Enter source IP address **3001::0/64**.

g. Use the default settings for other parameters.

h. Click **OK**.

4. Configure security policies to permit VRRP protocol packets:

This task allows Device A and Device B to exchange VRRP packets and elect a VRRP master when the HA channels are disconnected.

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Local**:

a. Enter security policy name **vrrp1**.

b. Select source zone **Trust**.

c. Select destination zone **Local**.

d. Select IP version **IPv6**.

e. Set the action to **Permit**.

f. Select policy group **vrrp**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Trust**:

i. Enter security policy name **vrrp2**.

j. Select source zone **Local**.

k. Select destination zone **Trust**.

l. Select IP version **IPv6**.

m. Set the action to **Permit**.

n. Select policy group **vrrp**.

o. Use the default settings for other parameters.

p. Click **OK**.

Configure a security policy to permit traffic from zone **Untrust** to zone **Local**:

q. Enter security policy name **vrrp3**.

r. Select source zone **Untrust**.

s. Select destination zone **Local**.

t. Select IP version **IPv6**.

u. Set the action to **Permit**.

v. Select policy group **vrrp**.

w. Use the default settings for other parameters.

x. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Untrust**:

y. Enter security policy name **vrrp4**.

z. Select source zone **Local**.

aa. Select destination zone **Untrust**.

bb. Select IP version **IPv6**.

cc. Set the action to **Permit**.

dd. Select policy group **vrrp**.

ee. Use the default settings for other parameters.

ff. Click **OK**.

Configuring HA group settings

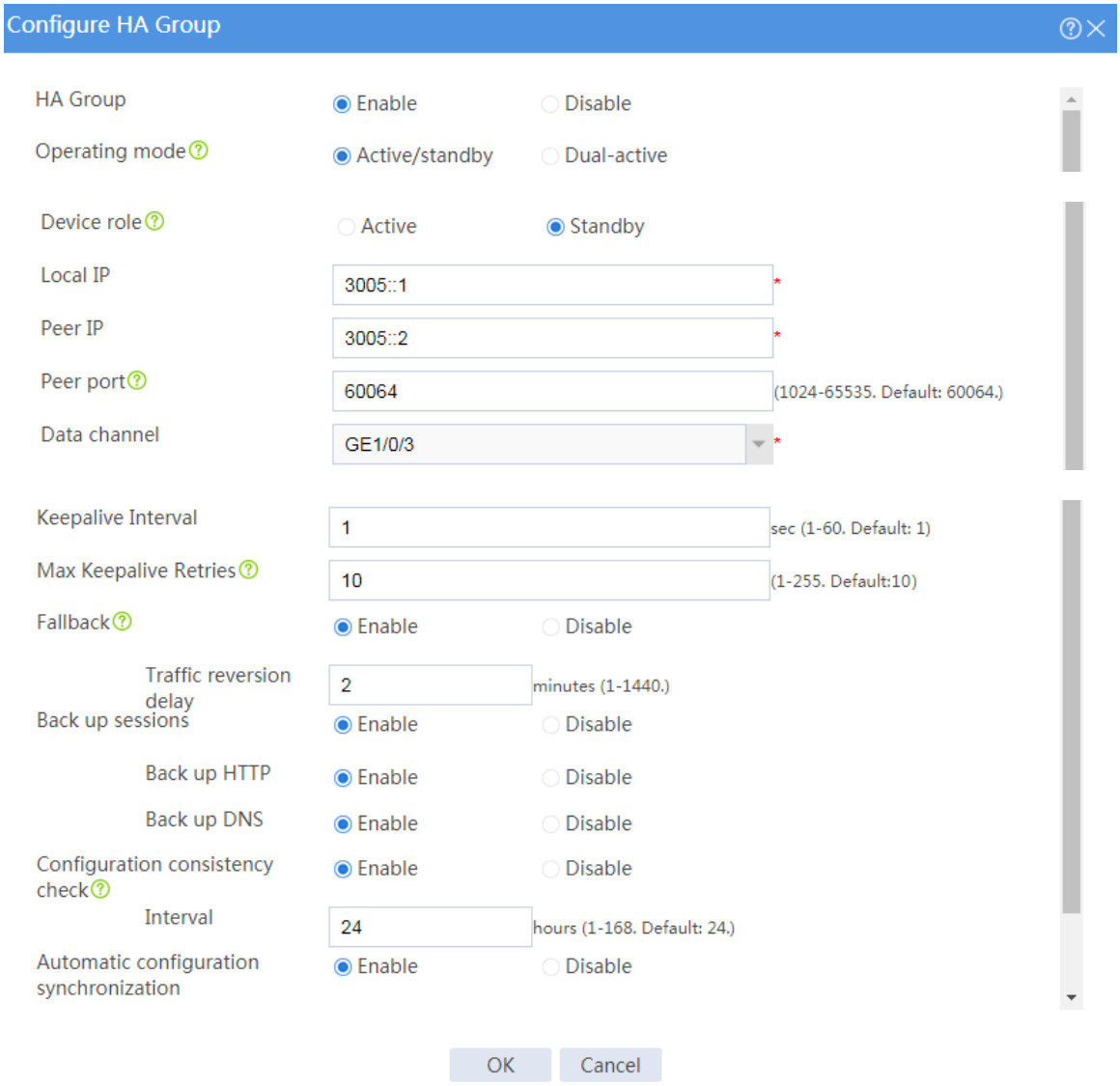
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 32.

Figure 32 Configuring HA group parameters



Click **OK**.

Associating the HA group with VRRP

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **VRRP**.

Click **Create**.

Configure VRRP groups as shown in the follow figures.

Figure 33 Creating VRRP group 1

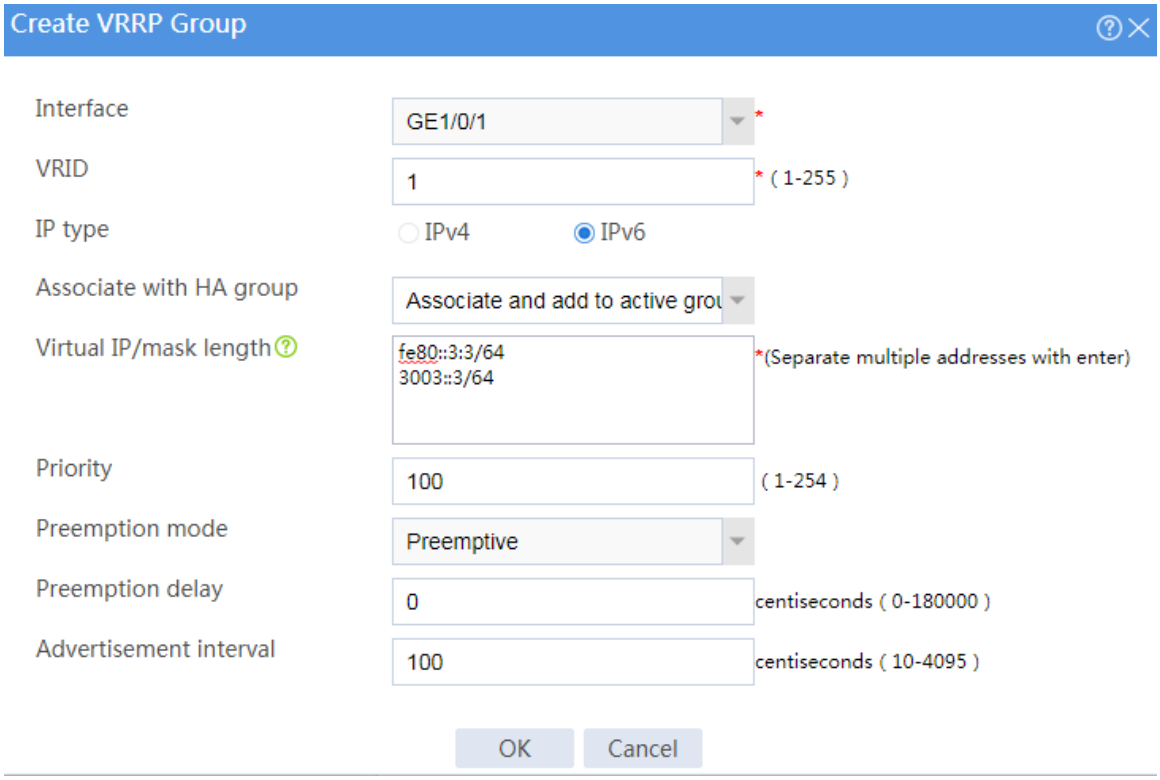
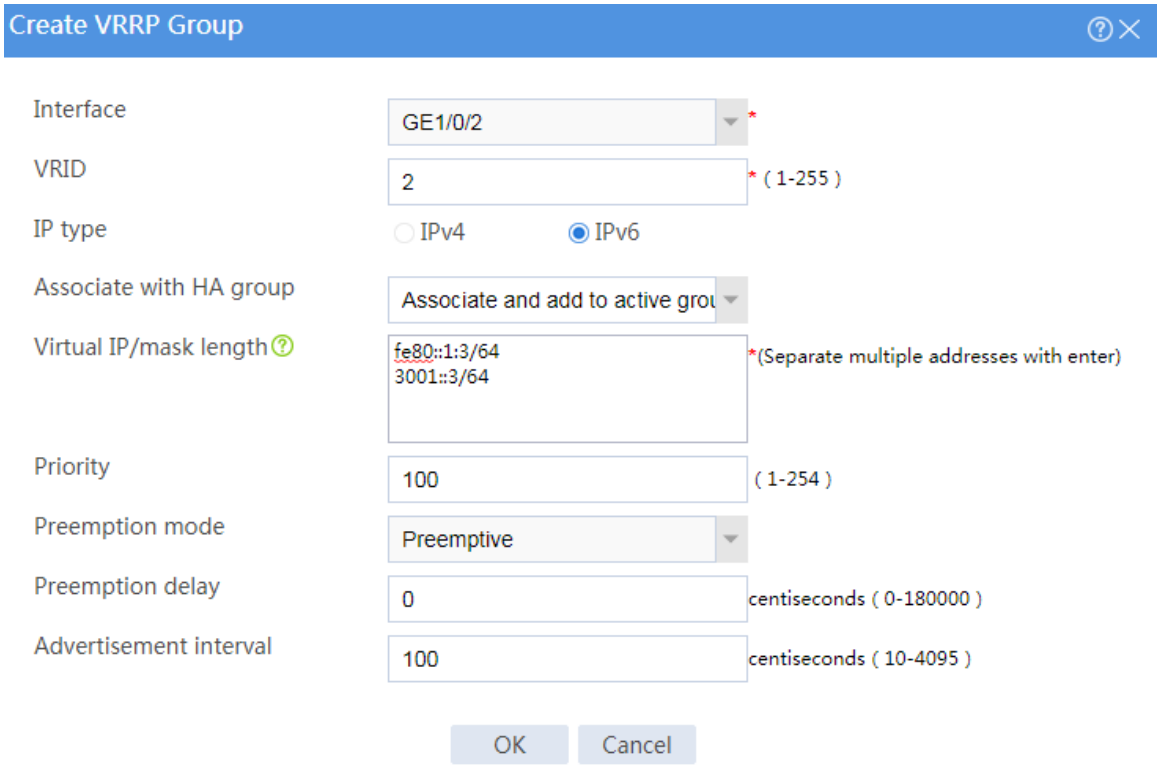


Figure 34 Creating VRRP group 2



Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv6 Address** tab, enter global unicast address **3003::2/64** and link local address **fe80::3:2**.

c. Use the default settings for other parameters.

d. Click **OK**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

e. On the **Basic Configuration** tab, select the **Trust** security zone.

f. On the **IPv6 Address** tab, enter global unicast address **3001::2/64** and link local address **fe80::1:2**.

g. Use the default settings for other parameters.

h. Click **OK**.

Click the **Edit** icon for GE 1/0/3.

In the dialog box that opens, configure the interface:

i. On the **IPv6 Address** tab, enter global unicast address **3005::2/64** and configure the interface to use a link local address generated automatically.

j. Use the default settings for other parameters.

k. Click **OK**.

2. Configure routing:

This step uses static routing as an example. To use dynamic routing, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv6 Static Routing** tab, click **Create**.

In the dialog box that opens, configure an IPv6 static route:

a. Enter destination IP address **0::0**.

b. Enter mask length **0**.

c. Enter next hop address **3003::15**.

d. Use the default settings for other parameters.

e. Click **OK**.

Configuring HA group settings

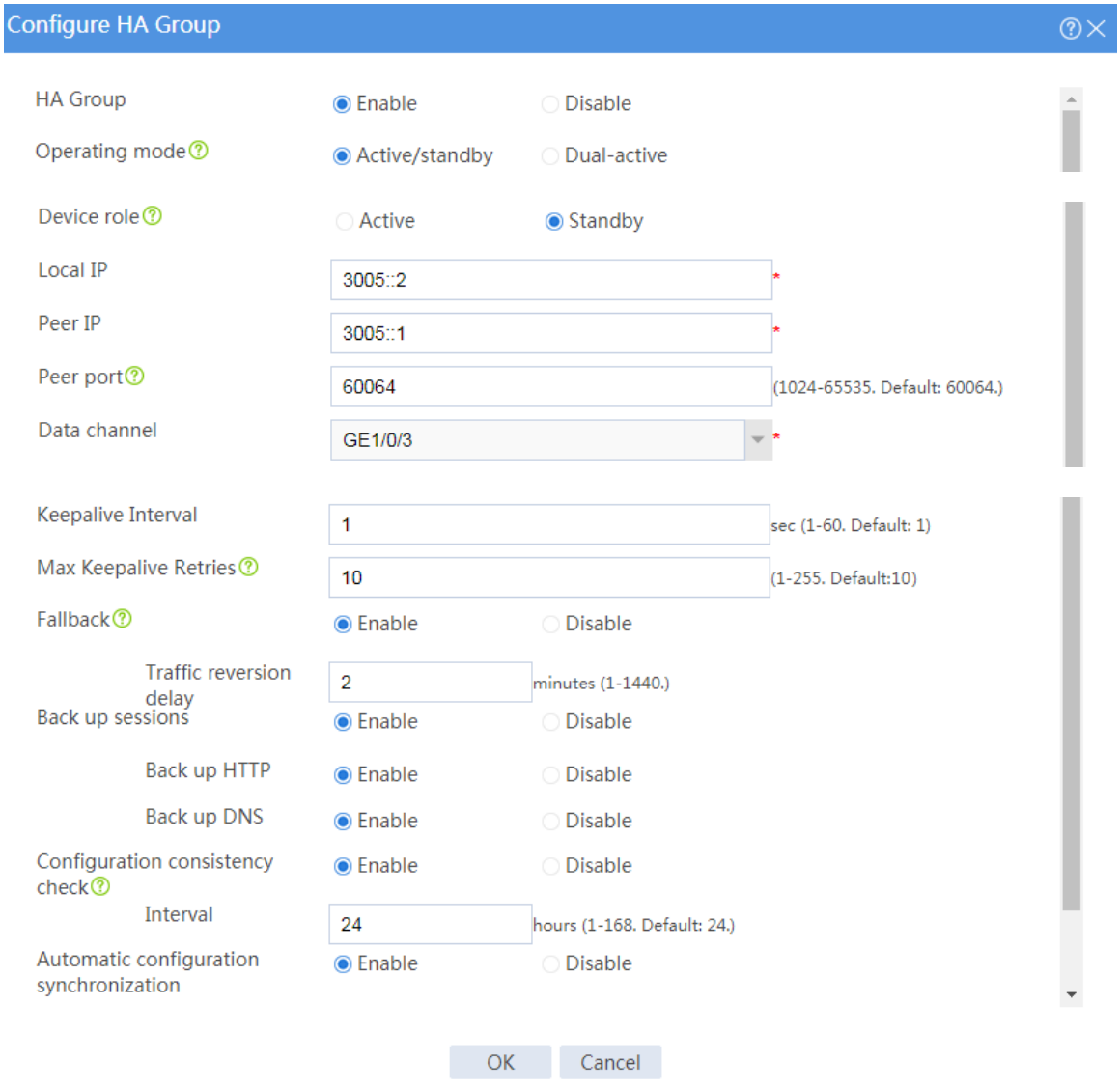
On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 35.

Figure 35 Configuring HA group parameters



Click **OK**.

Associating the HA group with VRRP

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **VRRP**.

Click **Create**.

Configure VRRP groups as shown in the follow figures.

Figure 36 Creating VRRP group 1

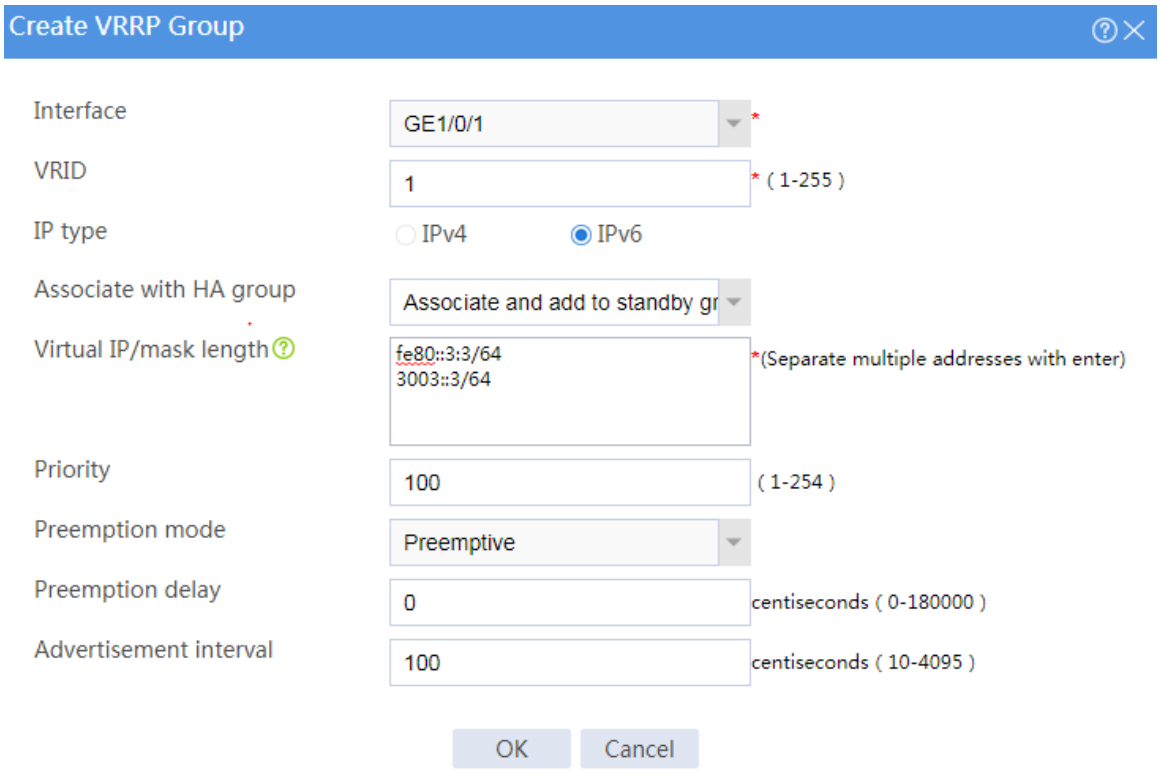
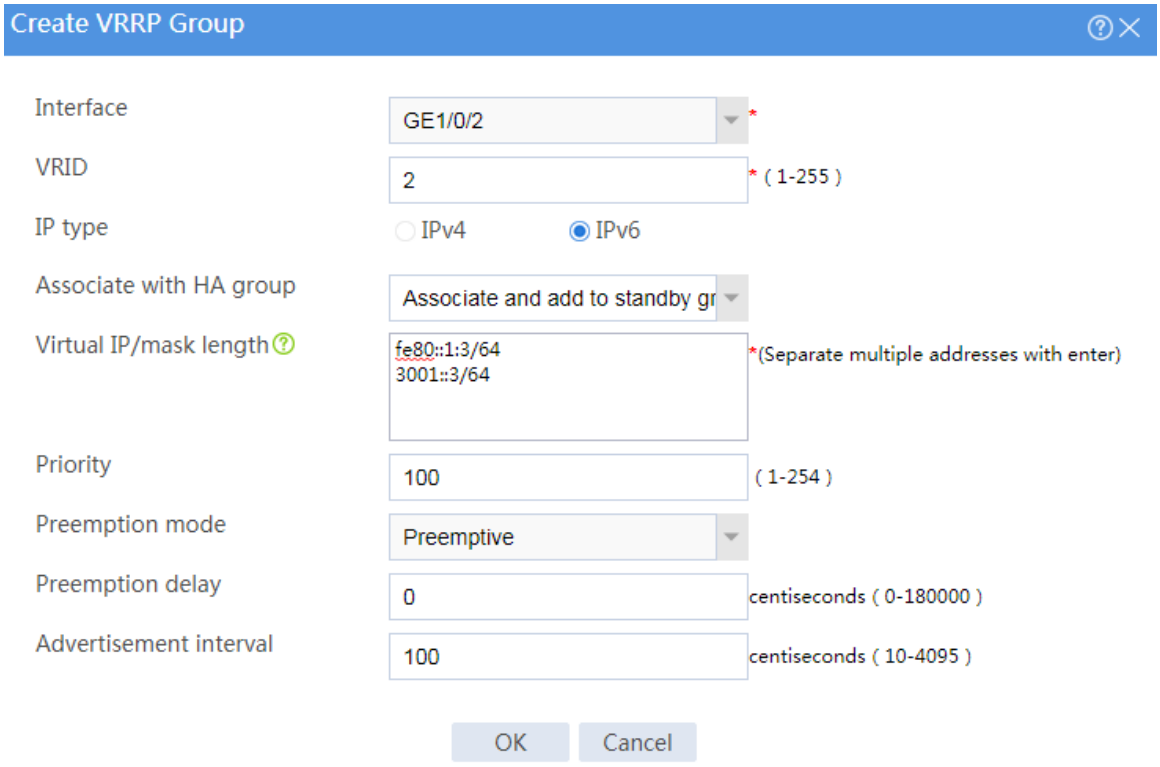


Figure 37 Creating VRRP group 2



Click **OK**.

Configuring the host

On the host, specify 3001::3 (virtual IP address of VRRP group 2) as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that only Device A generates log messages when the host communicates with the Internet.

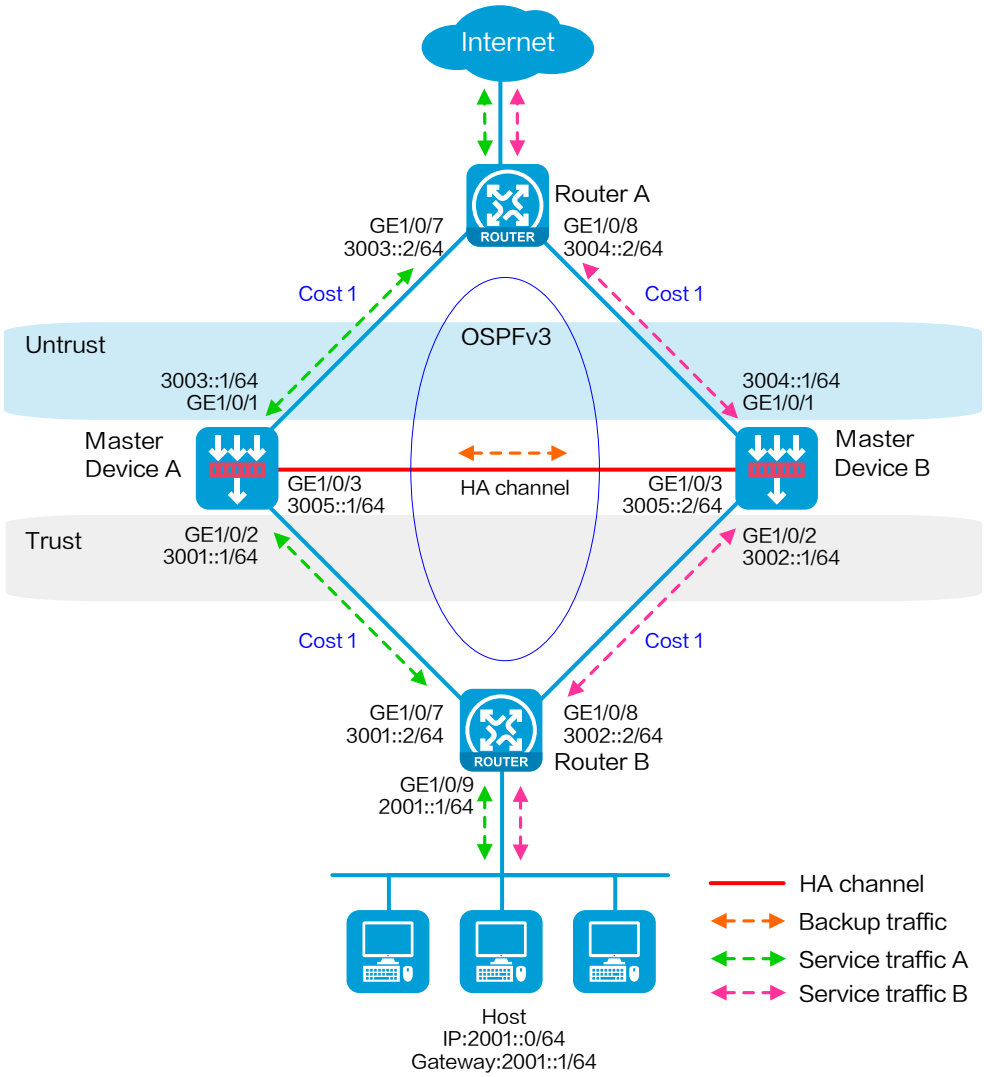
Example: Configuring the HA group in dual-active mode in collaboration with a routing protocol (IPv6)

Network configuration

As shown in Figure 38, set up the HA group at the border between the Internet and the internal network of an enterprise to ensure service continuity.

- Configure the HA group to collaborate with OSPFv3.
- Configure the HA group to operate in dual-active mode.
- Configure Device A and Device B to load share traffic.

Figure 38 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Router A

Assign 3003::2/64 to GigabitEthernet 1/0/7.

Assign 3004::2/64 to GigabitEthernet 1/0/8.

Configure OSPFv3 for Router A to have Layer 3 reachability to other devices.

Configure per-flow load sharing for IP forwarding.

Configuring Router B

Assign 3001::2/64 to GigabitEthernet 1/0/7.

Assign 3002::2/64 to GigabitEthernet 1/0/8.

Configure OSPFv3 for Router B to have Layer 3 reachability to other devices.

Configure per-flow load sharing for IP forwarding.

Configuring Device A

Configuring basic network settings

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv6 Address** tab, enter global unicast address **3003::1/64** and configure the interface to use a link local address generated automatically.

c. Use the default settings for other parameters.

d. Click **OK**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

e. On the **Basic Configuration** tab, select the **Trust** security zone.

f. On the **IPv6 Address** tab, enter global unicast address **3001::1/64** and configure the interface to use a link local address generated automatically.

g. Use the default settings for other parameters.

h. Click **OK**.

Click the **Edit** icon for GE 1/0/3.

In the dialog box that opens, configure the interface:

i. On the **IPv6 Address** tab, enter global unicast address **3005::1/64** and configure the interface to use a link local address generated automatically.

j. Use the default settings for other parameters.

k. Click **OK**.

2. Configure routing:

This step uses OSPF as an example. You can configure another dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

Click **Create**.

In the dialog box that opens, configure an OSPF instance:

a. Select version **OSPFv3**.

b. Enter instance name **1**.

c. Enter router ID **2.1.1.1**.

d. Use the default settings for other parameters.

e. Click **OK**.

Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

f. Enter area ID **0.0.0.0**.

g. Click **OK**.

Click **0** in the **Number of OSPF interfaces** column for the created OSPF instance.

On the OSPF interface configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

h. Enter area ID **0.0.0.0**.

i. Select interface **GE 1/0/1**.

j. Enter interface instance ID **1**.

k. Click **OK**.

Click **1** in the **Number of OSPF interfaces** column for the created OSPF instance.

On the OSPF interface configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

l. Enter area ID **0.0.0.0**.

m. Select interface **GE 1/0/2**.

n. Enter interface instance ID **1**.

o. Click **OK**.

3. Configure a security policy to permit service traffic:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Untrust**:

a. Enter security policy name **Trust-Untrust**.

b. Select source zone **Trust**.

c. Select destination zone **Untrust**.

d. Select IP version **IPv6**.

e. Set the action to **Permit**.

f. Enter source IP address **2001::0/64**.

g. Use the default settings for other parameters.

h. Click **OK**.

4. Configure security policies to permit OSPF protocol packets:

Perform this task only on the primary device. The secondary device will synchronize security policy configuration with the primary device after the HA group is set up.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

In the dialog box that opens, configure a security policy to permit traffic from zone **Trust** to zone **Local**:

a. Enter security policy name **ospf1**.

b. Select source zone **Trust**.

c. Select destination zone **Local**.

d. Select IP version **IPv6**.

e. Set the action to **Permit**.

f. Select policy group **ospf**.

g. Use the default settings for other parameters.

h. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Trust**:

i. Enter security policy name **ospf2**.

j. Select source zone **Local**.

k. Select destination zone **Trust**.

l. Select IP version **IPv6**.

m. Set the action to **Permit**.

n. Select policy group **ospf**.

o. Use the default settings for other parameters.

p. Click **OK**.

Configure a security policy to permit traffic from zone **Untrust** to zone **Local**:

q. Enter security policy name **ospf3**.

r. Select source zone **Untrust**.

s. Select destination zone **Local**.

t. Select IP version **IPv6**.

u. Set the action to **Permit**.

v. Select policy group **ospf**.

w. Use the default settings for other parameters.

x. Click **OK**.

Configure a security policy to permit traffic from zone **Local** to zone **Untrust**:

y. Enter security policy name **ospf4**.

z. Select source zone **Local**.

aa. Select destination zone **Untrust**.

bb. Select IP version **IPv6**.

cc. Set the action to **Permit**.

dd. Select policy group **ospf**.

ee. Use the default settings for other parameters.

ff. Click **OK**.

Configuring HA group settings

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **Track**.

Click **Add**.

Configure a track entry:

1. Enter track entry ID **1**.

2. Select the interface module.

3. Select GE 1/0/1 as the monitored interface.

4. Use the default settings for other parameters.

Configure track entry 2 to monitor the state of GE 1/0/2. (Details not shown.)

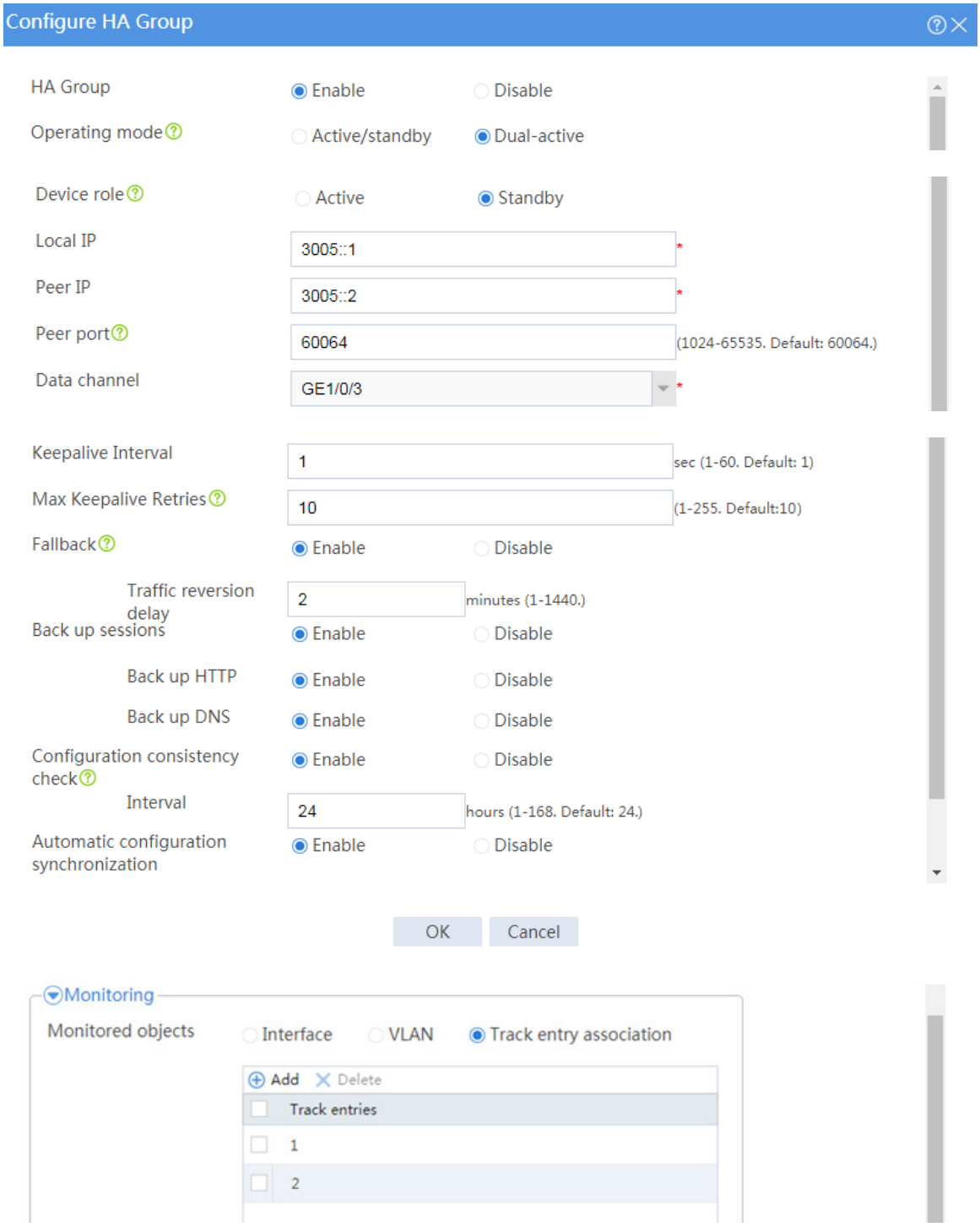
On the top navigation bar, click **System**.

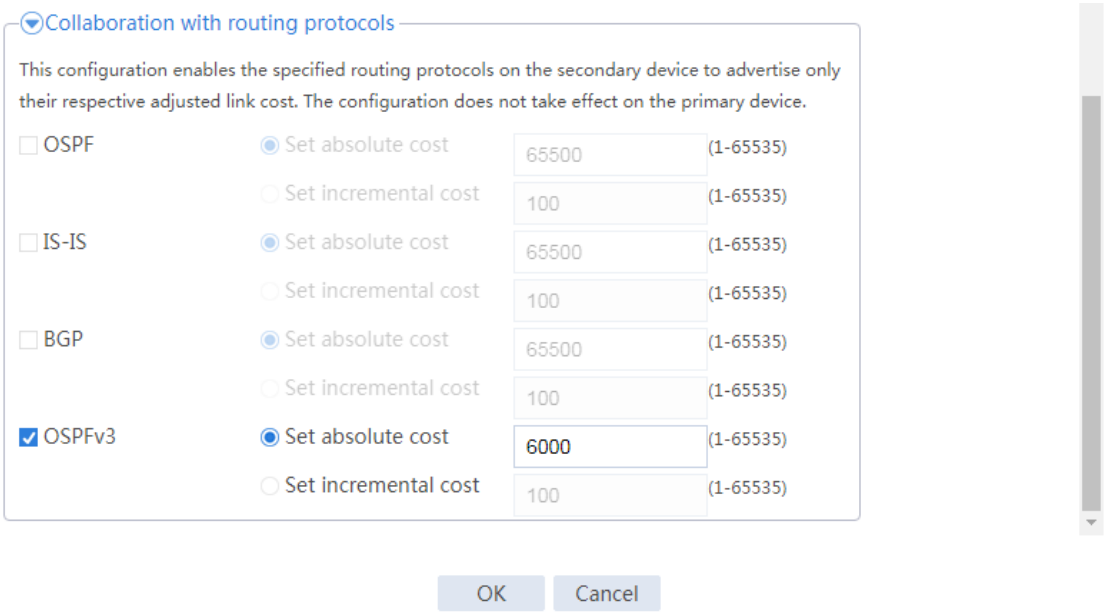
From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 39.

Figure 39 Configuring HA group parameters





Click **OK**.

Configuring security services

Configure security devices on the HA group member devices. If the HA group can back up configuration for a module, configure the module only on the primary device (Device A).

Configuring Device B

Configuring basic network settings

1. Assign IP addresses to interfaces:

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the **Basic Configuration** tab, select the **Untrust** security zone.

b. On the **IPv6 Address** tab, enter global unicast address **3004::1/64** and configure the interface to use a link local address generated automatically.

c. Use the default settings for other parameters.

d. Click **OK**.

Click the **Edit** icon for GE 1/0/2.

In the dialog box that opens, configure the interface:

e. On the **Basic Configuration** tab, select the **Trust** security zone.

f. On the **IPv6 Address** tab, enter global unicast address **3002::1/64** and configure the interface to use a link local address generated automatically.

g. Use the default settings for other parameters.

h. Click **OK**.

Click the **Edit** icon for GE 1/0/3.

In the dialog box that opens, configure the interface:

i. On the **IPv6 Address** tab, enter global unicast address **3005::2/64** and configure the interface to use a link local address generated automatically.

j. Use the default settings for other parameters.

k. Click **OK**.

2. Configure routing:

This step uses OSPF as an example. You can configure another dynamic routing protocol as needed.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **OSPF**.

Click **Create**.

In the dialog box that opens, configure an OSPF instance:

a. Select version **OSPFv3**.

b. Enter instance name **1**.

c. Enter router ID **2.1.10.1**.

d. Use the default settings for other parameters.

e. Click **OK**.

Click **0** in the **Number of OSPF areas** column for the created OSPF instance.

On the OSPF area configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

f. Enter area ID **0.0.0.0**.

g. Click **OK**.

Click **0** in the **Number of OSPF interfaces** column for the created OSPF instance.

On the OSPF interface configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

h. Enter area ID **0.0.0.0**.

i. Select interface **GE 1/0/1**.

j. Enter interface instance ID **1**.

k. Click **OK**.

Click **1** in the **Number of OSPF interfaces** column for the created OSPF instance.

On the OSPF interface configuration page that opens, click **Create**.

In the dialog box that opens, configure an area:

l. Enter area ID **0.0.0.0**.

m. Select interface **GE 1/0/2**.

n. Enter interface instance ID **1**.

o. Click **OK**.

Configuring HA group settings

On the top navigation bar, click **System**.

From the navigation pane, select **High Availability** > **Track**.

Click **Add**.

Configure a track entry:

1. Enter track entry ID **1**.

2. Select the interface module.

3. Select GE 1/0/1 as the monitored interface.

4. Use the default settings for other parameters.

Configure track entry 2 to monitor the state of GE 1/0/2. (Details not shown.)

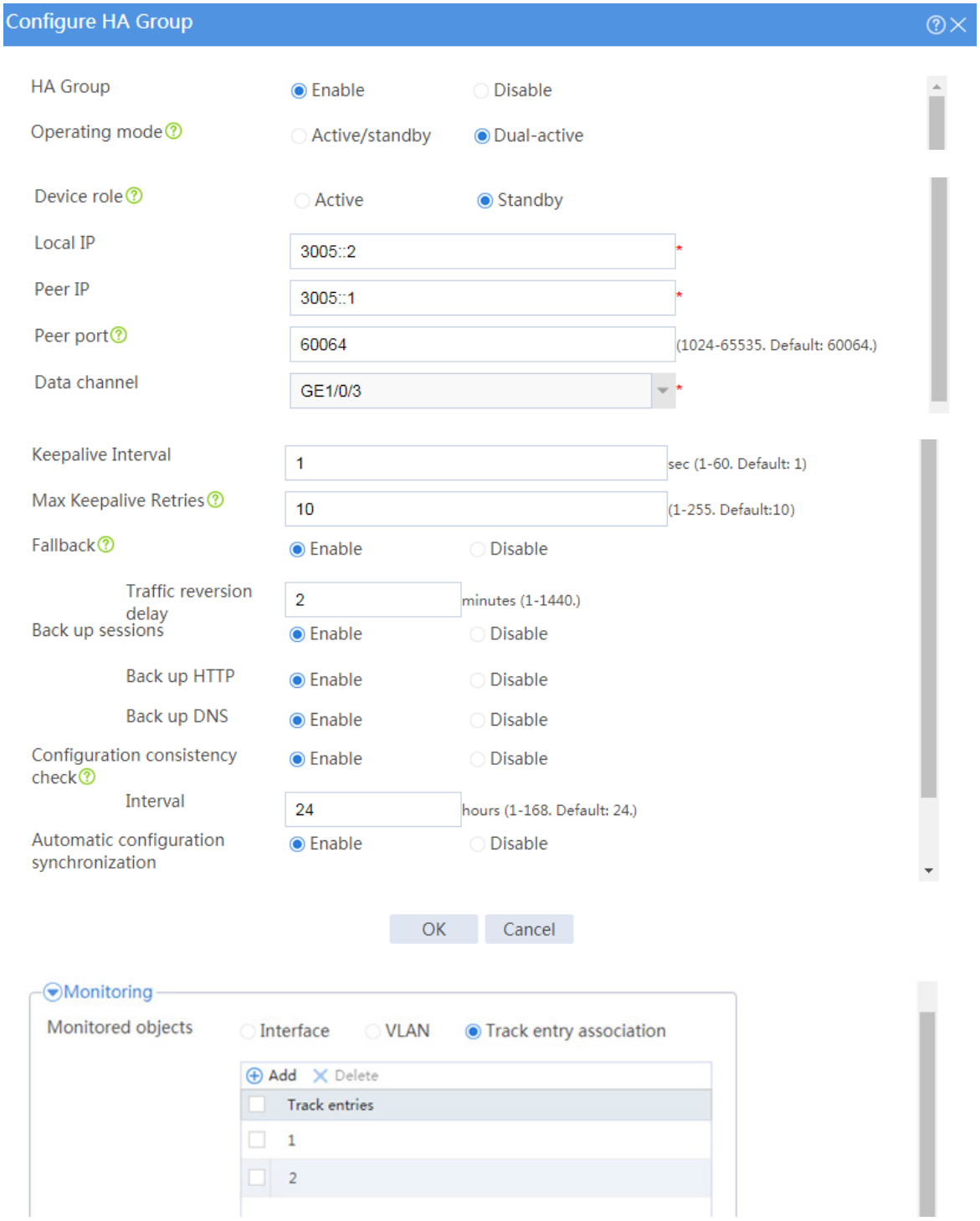
On the top navigation bar, click **System**.

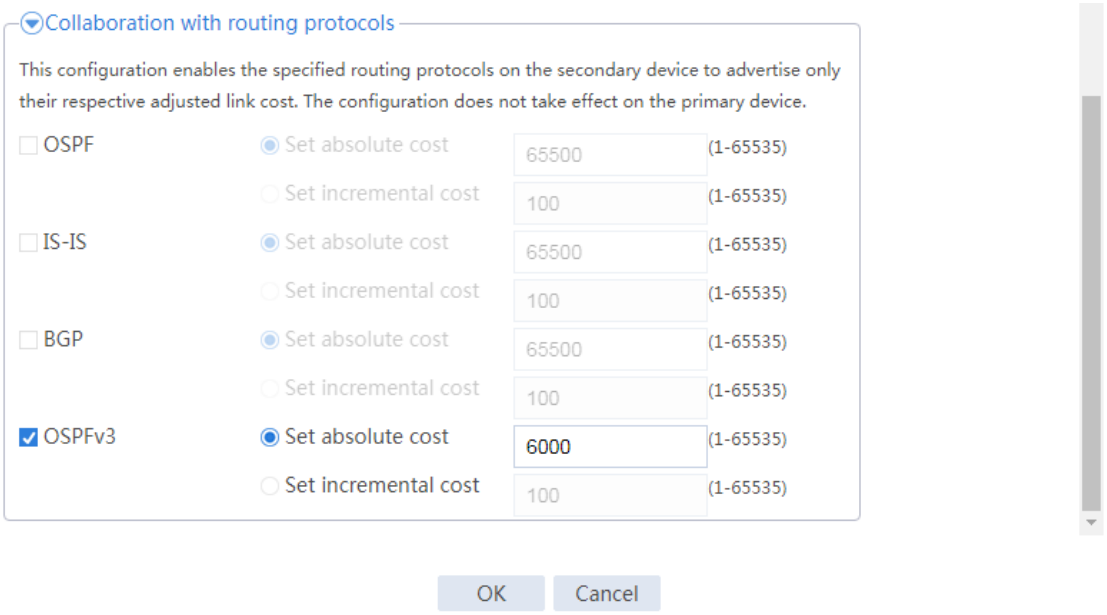
From the navigation pane, select **High Availability** > **HA Group**.

Click **Configure**.

Configure the HA group parameters as shown in Figure 40.

Figure 40 Configuring HA group parameters





Click **OK**.

Configuring the hosts

On the hosts, specify 2002::1 as the default gateway.

Verifying the configuration

Enable logging for the interzone policy that permits communication between security zones **Trust** and **Untrust**. Verity that both Device A and Device B generate log messages when the hosts communicate with the Internet.

Context configuration examples

Contents

Introduction

The following information provides context configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the context feature.

Restrictions and guidelines

When you assign VLANs to contexts, follow these restrictions and guidelines:

- For contexts without the VLAN-unshared attribute, you can only assign VLANs to them and cannot use the **vlan** command to create VLANs for them. Before the assignment, you must create the VLANs on the default context.
- You cannot assign the following VLANs to a context without the VLAN-unshared attribute:
    - VLAN 1.
    - Default VLANs of interfaces.
    - VLANs for which you have created VLAN interfaces.

When you assign interfaces to contexts, follow these restrictions and guidelines:

- Subinterfaces, VLAN interfaces, and aggregate interfaces can be assigned to a context only in shared mode.
- After assigning a subinterface to a context, you cannot assign its primary interface to a context. After assigning a primary interface to a context, you cannot assign its subinterfaces to a context.
- Do not assign member interfaces of an aggregate interface to a context in shared mode.
- After assigning an interface to contexts in shared mode, you cannot assign the interface to contexts in exclusive mode before reclaiming the interface.
- Do not assign IRF physical interfaces to a non-default context.
- If a subinterface of a Layer 3 interface is a member interface of a Reth interface, do not assign the Layer 3 interface to a non-default context.

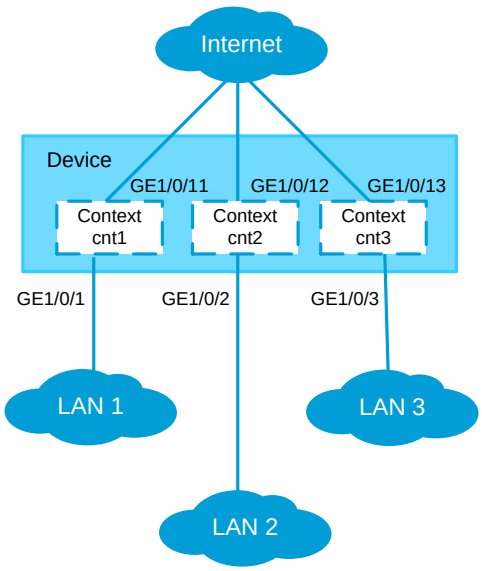
Example: Configuring contexts

Network configuration

As shown in Figure 1, configure contexts for the LANs as follows:

- LAN 1 has a large number of users and complicated services. Configure context **cnt1** for LAN 1. Assign 60% disk space and 60% memory space to the context and set the CPU weight to 8. Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/11 to the context.
- LAN 2 has a normal scale of users. Configure context **cnt2** for LAN 2. Leave the context to use the default amount of disk space and the default amount of memory space. Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/12 to the context.
- LAN 3 has a small number of users. Configure context **cnt3** for LAN 3. Assign 30% disk space and 30% memory space to the context and set the CPU weight to 3. Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/13 to the context.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Configure context **cnt1**:

   # On the top navigation bar, click **System**.

   # From the navigation pane, select **Virtualization Advanced Settings** > **Contexts** > **Contexts**.

   # Click **Create**.

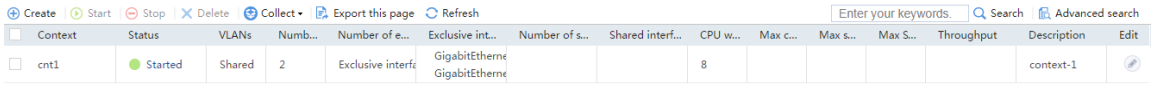
   # Configure context **cnt1** as shown in Figure 2.

   # Click **OK**.

Figure 2 Creating a context

Select context **cnt1** from the context list and click **Start**.

Figure 3 Starting context cnt1

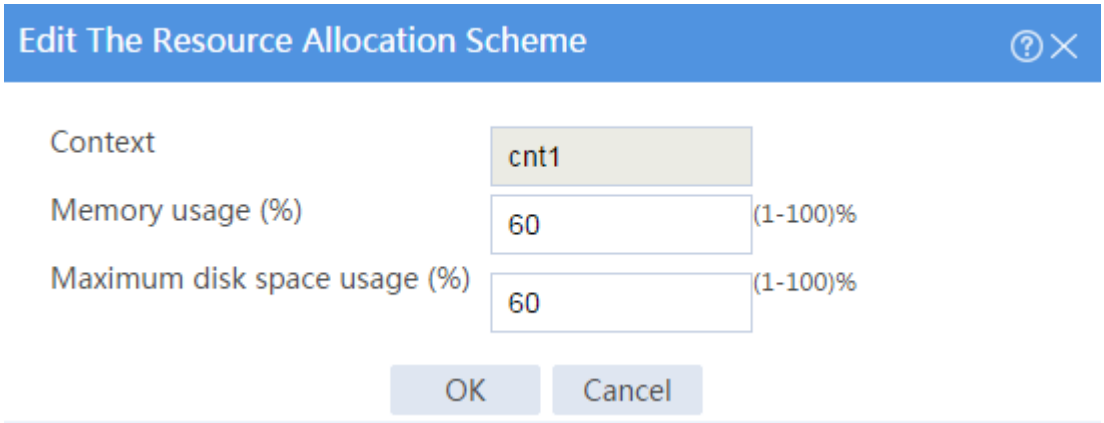


From the navigation pane, select **Virtualization Advanced Settings** > **Contexts** > **Resource Allocation**.

Click context **cnt1** and edit the resource allocation scheme for the context as shown in Figure 4.

Click **OK**.

Figure 4 Editing the resource allocation scheme

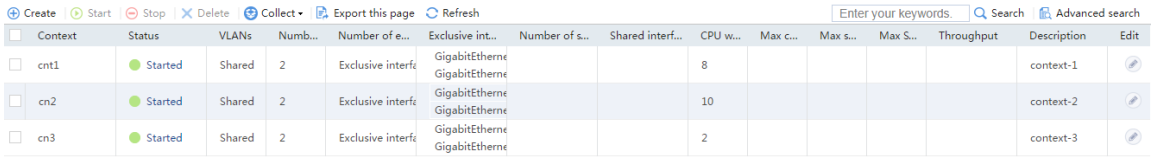


2. Configure context **cnt2** and **cnt3** in the same way you configure context **cnt1**.

Verifying the configuration

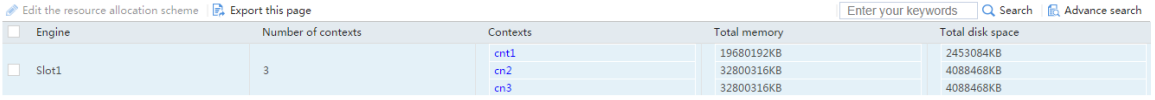
1. On the top navigation bar, click **System**.
2. From the navigation pane, select **Virtualization Advanced Settings** > **Contexts** > **Contexts**.
3. Verify that the contexts are listed and their settings are as configured.

Figure 5 Viewing contexts



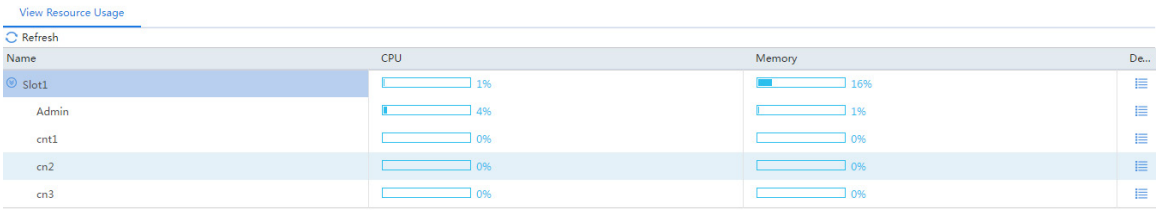
4. From the navigation pane, select **Virtualization Advanced Settings** > **Contexts** > **Resource Allocation** to view the amounts of memory and disk resources allocated to contexts.

Figure 6 Viewing context resource allocation



5. From the navigation pane, select **Virtualization Advanced Settings** > **Contexts** > **Resource Usage** to view the resource usage of contexts

Figure 7 Viewing resource usage of contexts



IRF configuration examples

Contents

Introduction

The following information provides IRF configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

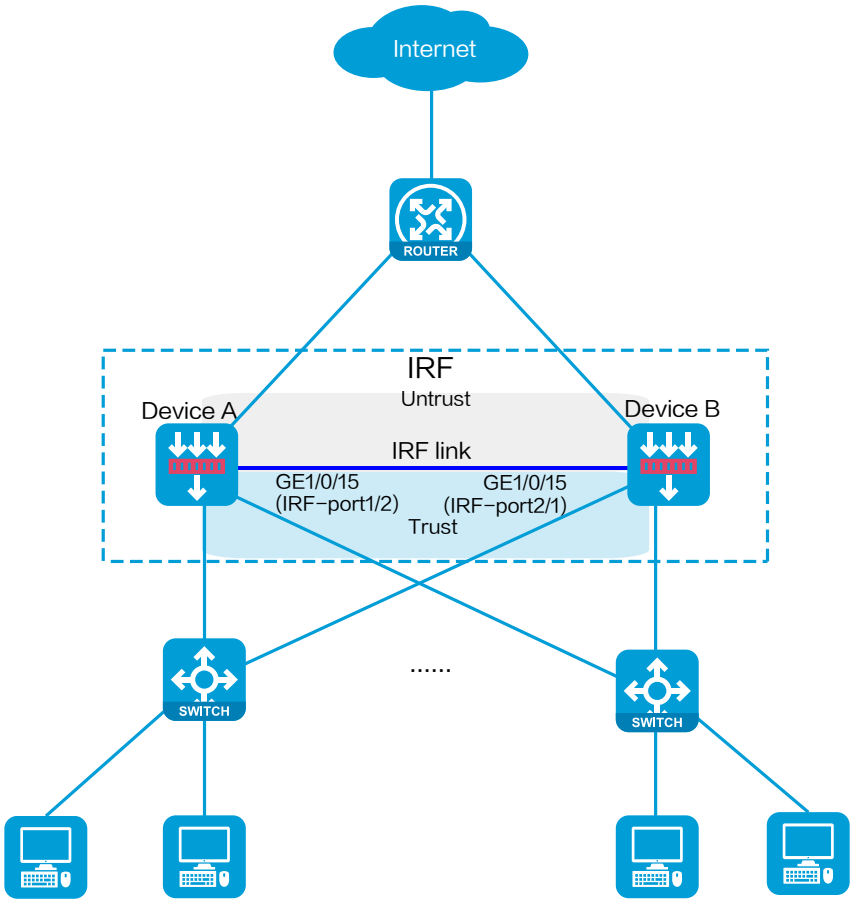
The following information is provided based on the assumption that you have basic knowledge of the IRF feature.

Example: Setting up an IRF fabric

Network configuration

As shown in Figure 1, use Device A and Device B to set up an IRF fabric. Assign Device A a higher priority than Device B so Device A can be the master device.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring Device A

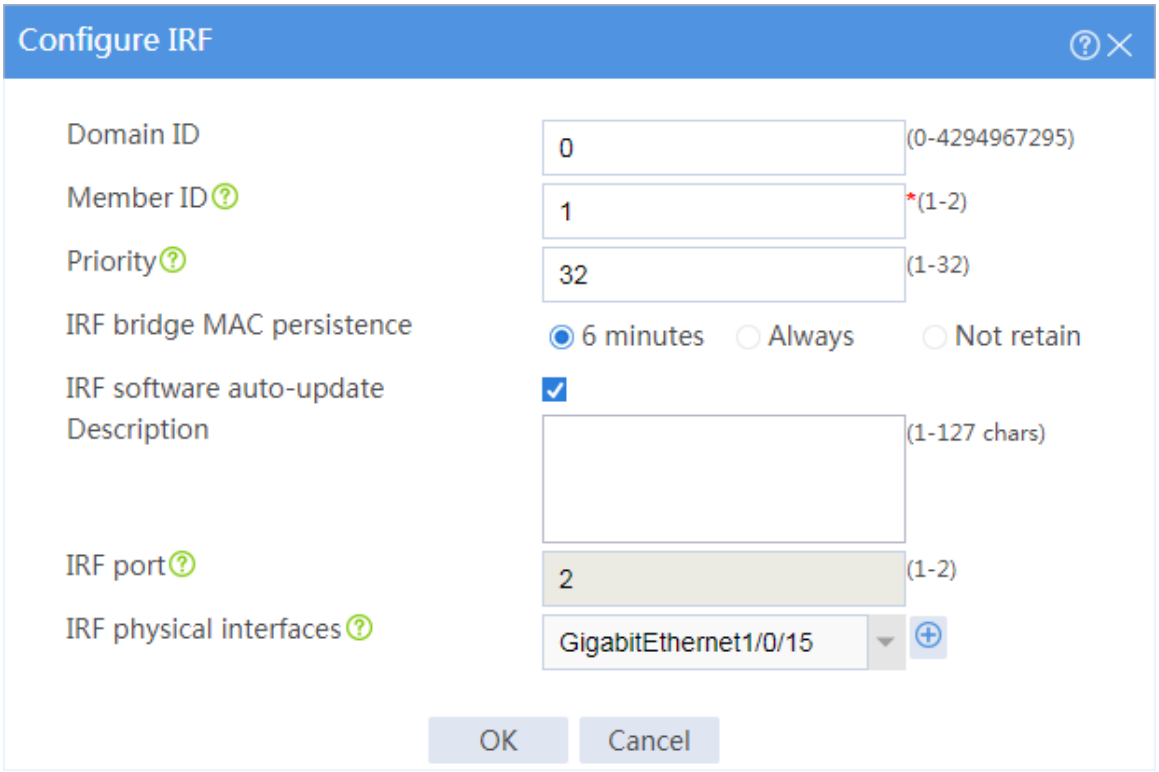
On the top navigation bar, click **System**.

From the navigation pane, select **Virtualization Advanced Settings** > **IRF**.

Click the **Settings** icon for IRF-port 2.

In the dialog box that opens, configure IRF parameters as shown in Figure 2.

Figure 2 Configuring IRF on Device A



Click **OK**.

Configuring Device B

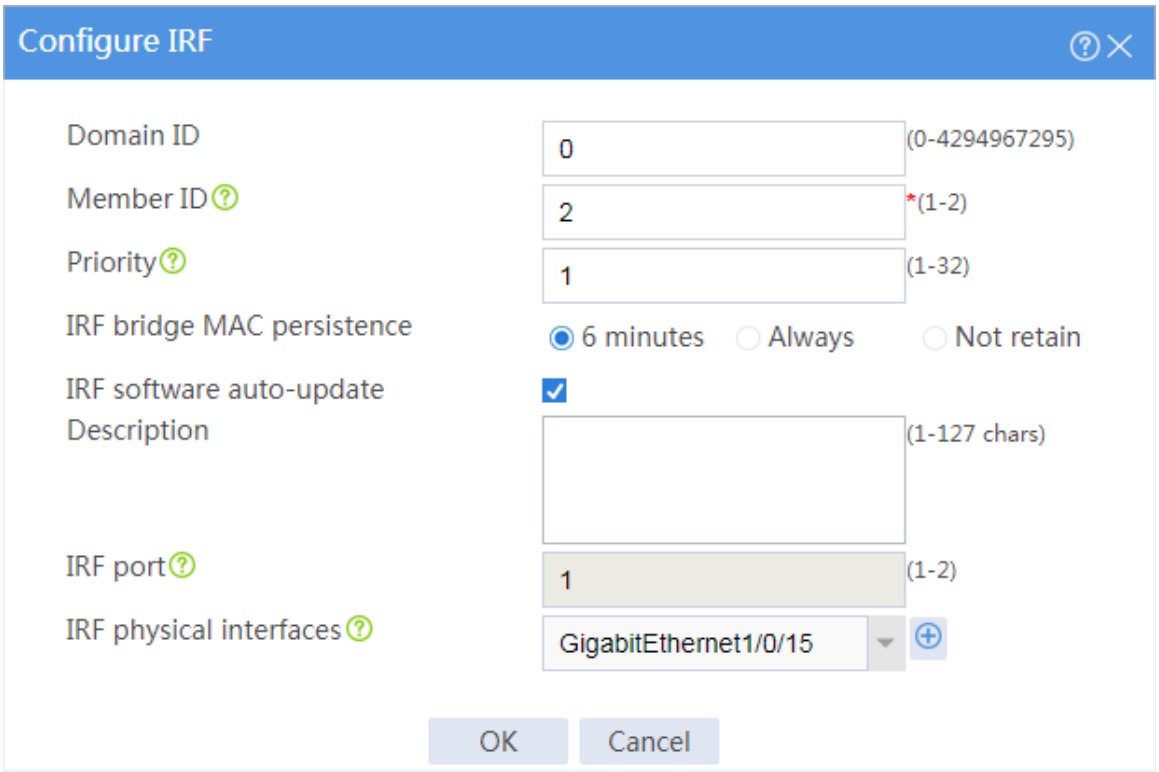
On the top navigation bar, click **System**.

From the navigation pane, select **Virtualization Advanced Settings** > **IRF**.

Click the **Settings** icon for IRF-port 1.

In the dialog box that opens, configure IRF parameters as shown in Figure 3.

Figure 3 Configuring IRF on Device B



Click **OK**.

Device B automatically reboots. The member ID and physical interface numbers of Device B change after the reboot. The device forms an IRF fabric with Device A.

Verifying the configuration

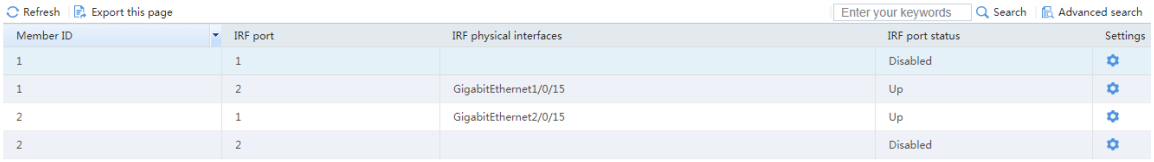
Use the management address of the master (Device A) to log in to the Web interface of the IRF fabric.

On the top navigation bar, click **System**.

From the navigation pane, select **Virtualization Advanced Settings** > **IRF**.

Verify that Device A and Device B are IRF member devices and their IRF ports are up.

Figure 4 IRF information



DHCP configuration examples

Contents

Introduction

The following information describes DHCP configuration examples.

The Dynamic Host Configuration Protocol (DHCP) provides a framework to assign configuration information to network devices.

DHCP uses the client-server model for network configuration parameter assignment. DHCP clients request network configuration parameters from a DHCP server and the DHCP server assigns network configuration parameters to DHCP clients. This document provides configuration of the DHCP server.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of DHCP.

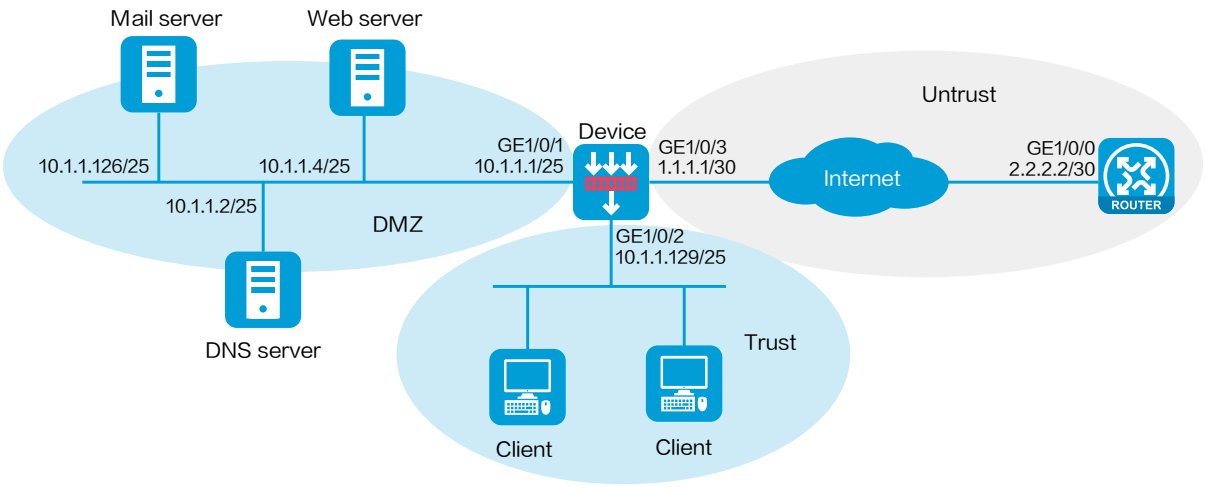
Example: Configuring DHCP

Network configuration

As shown in Figure 1, clients and internal servers are on different subnets. Create DHCP address pools on the device to meet the following requirements:

- The internal servers obtain static IP addresses, the DNS server address, and the gateway from the device.
- Clients dynamically obtain IP addresses from the device.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

- Make sure the network segment for dynamic allocation is on the same subnet as the DHCP server-enabled interface. Otherwise, clients cannot obtain IP addresses from the DHCP server.
- To ensure the communication between the local security zone and the security zone of the DHCP server-enabled interface, configure a security policy between the local security zone and the DHCP server-enabled interface.

Procedure

1. Assign IP addresses to interfaces.

On the top navigation bar, click **Network**.

From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **DMZ** security zone.

b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.1.1/25.

Retain the default configuration for the remaining parameters.

c. Click **OK**.

Add GE 1/0/2 to the **Trust** security zone and set its IP address to 10.1.1.129/25 in the same way you configure GE 1/0/1.

Add GE 1/0/3 to the **Untrust** security zone and set its IP address to 1.1.1.1/30 in the same way you configure GE 1/0/1.

2. Create security policies.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Select **Create** > **Create a policy**.

Create security policy **dhcp-a**:

- Enter policy name **dhcp-a**.
- Select source zone **Trust**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.

Click **OK**.

Create security policy **dhcp-b**:

- Enter policy name **dhcp-b**.
- Select source zone **Local**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.

Click **OK**.

Create security policy **dhcp-c**:

- Enter policy name **dhcp-c**.
- Select source zone **DMZ**.
- Select destination zone **Local**.
- Select type **IPv4**.
- Select action **Permit**.

Click **OK**.

Create security policy **dhcp-d**:

- Enter policy name **dhcp-d**.
- Select source zone **Local**.
- Select destination zone **DMZ**.
- Select type **IPv4**.
- Select action **Permit**.

Click **OK**.

3. Configure statically assigned IP addresses.

On the top navigation bar, click **Network**.

From the navigation pane, select **DHCP** > **DHCP service**.

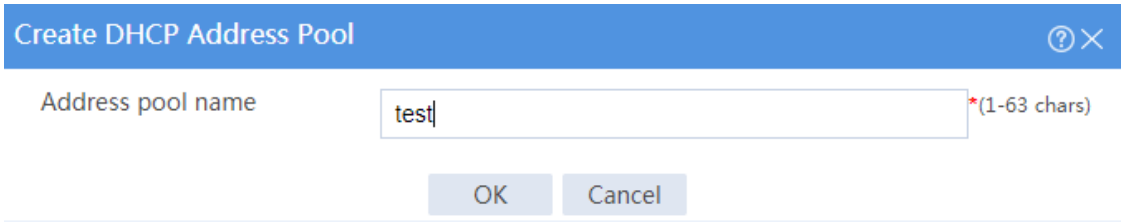
Select **Enable** for **DHCP service**.

From the navigation pane, select **DHCP** > **DHCP Address Pools**.

Click **Create address pool**.

Enter the address pool name, and click **OK**, as shown in Figure 2.

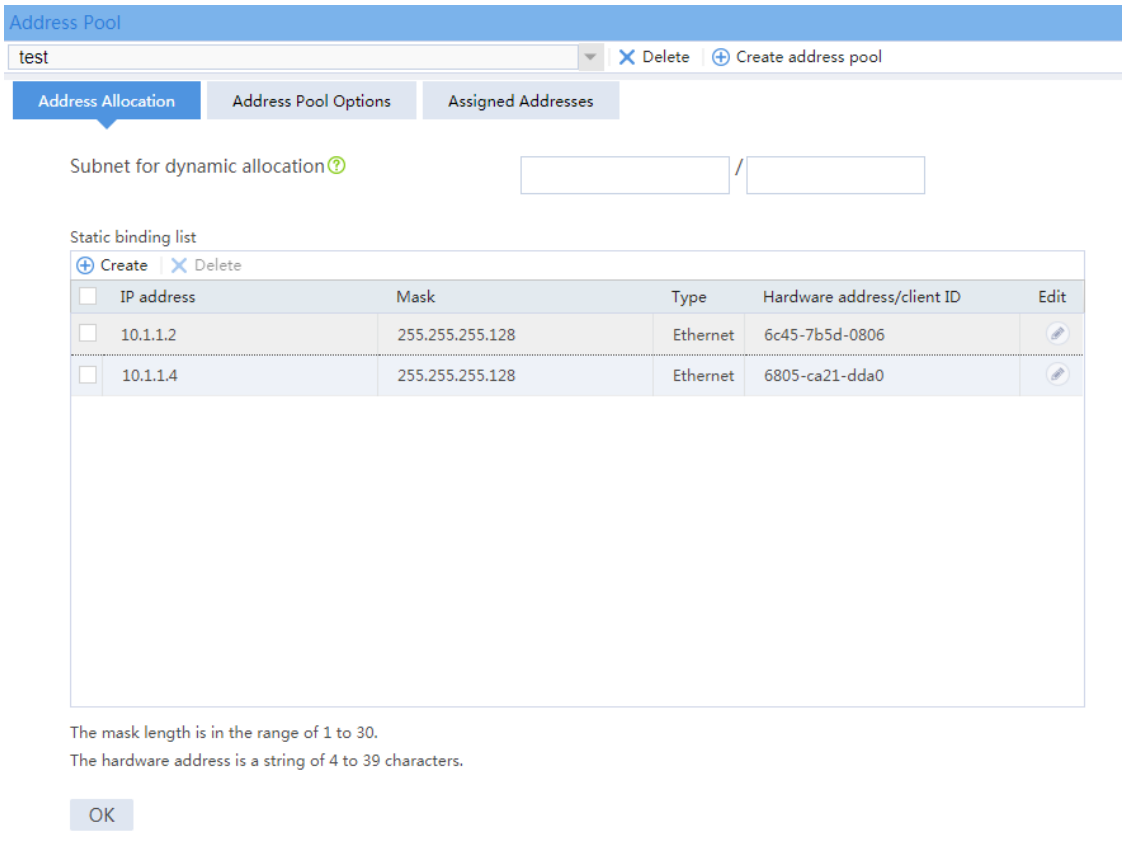
Figure 2 Creating a DHCP address pool



Click the **Address Allocation** tab.

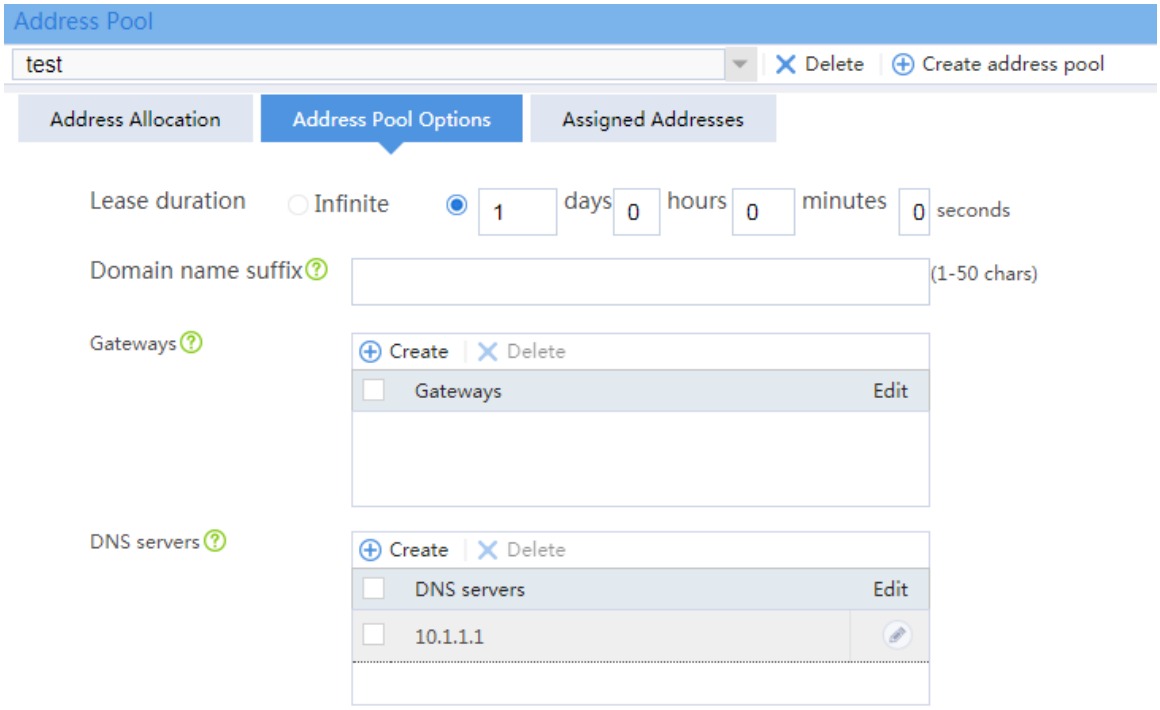
Add statically assigned IP addresses, as shown in Figure 3.

Figure 3 Configuring address allocation



Click the **Address Pool Options** tab, and configure address pool options as shown in Figure 4.

Figure 4 Configuring address pool options



Click **OK**.

4. Configure dynamic address allocation.

On the top navigation bar, click **Network**.

From the navigation pane, select **DHCP** > **DHCP service**.

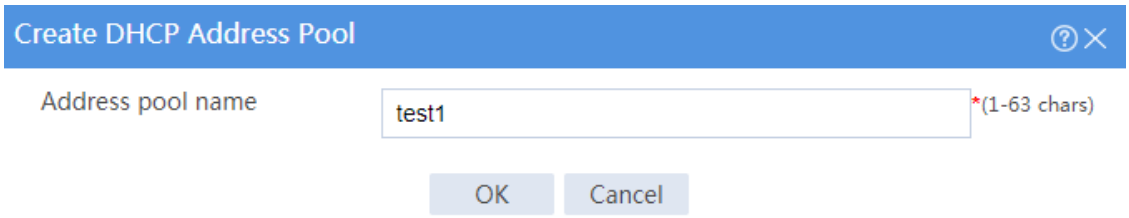
Select **Enable** for **DHCP service**.

From the navigation pane, select **DHCP** > **DHCP Address Pools**.

Click **Create address pool**.

Enter the address pool name, and click **OK**, as shown in Figure 5.

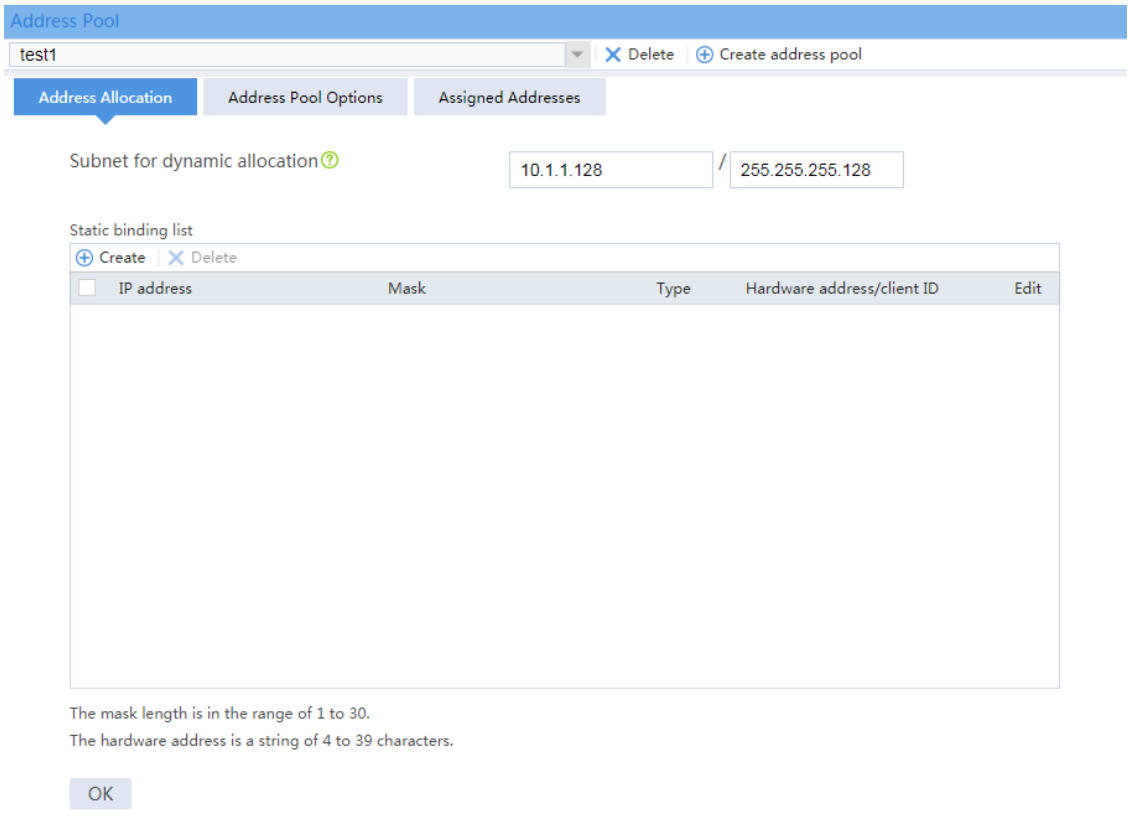
Figure 5 Creating a DHCP address pool



Click the **Address Allocation** tab.

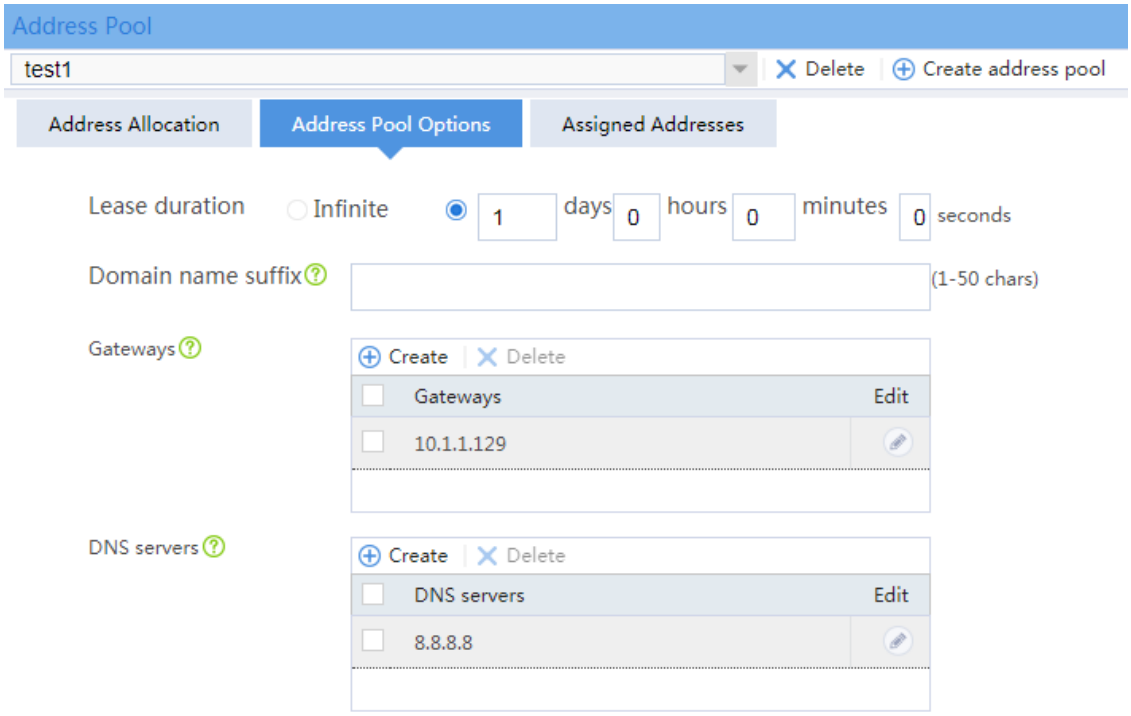
Enter a subnet address for dynamic allocation. The configuration is shown in Figure 6.

Figure 6 Configuring address allocation



Click the **Address Pool Options** tab, add the gateway address and the DNS server address as shown in Figure 7.

Figure 7 Configuring address pool options



Click **OK**.

Verifying the configuration

Verifying statically-bound IP address allocation

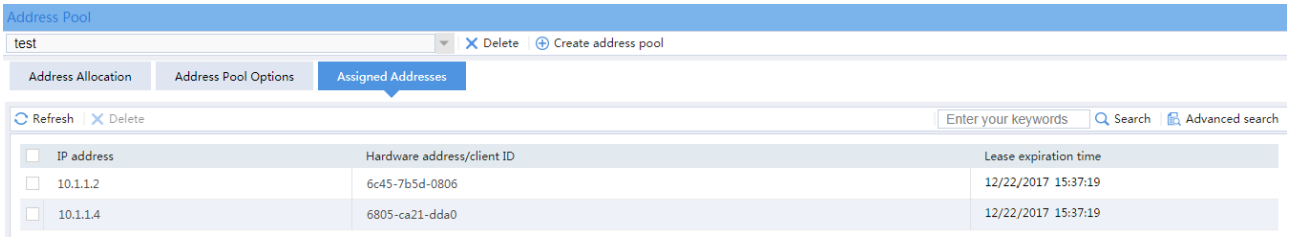
On the top navigation bar, click **Network**.

From the navigation pane, select **DHCP** > **DHCP Address Pools**.

Select the DHCP address pool for the static allocation, and click the **Assigned Addresses** tab.

Verify that the device has assigned static addresses to internal servers.

Figure 8 Verifying statically assigned IP addresses



Verifying dynamic IP address allocation

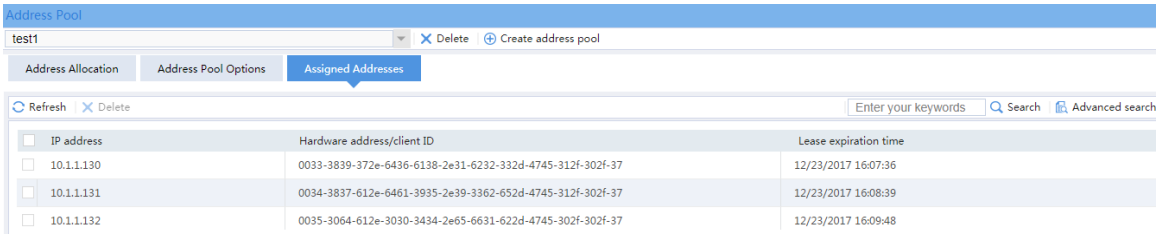
On the top navigation bar, click **Network**.

From the navigation pane, select **DHCP** > **DHCP Address Pools**.

Select the DHCP address pool for dynamic allocation, and click the **Assigned Addresses** tab.

Verify that the device has dynamically assigned addresses to clients.

Figure 9 Verifying dynamically assigned IP addresses



DNS configuration examples

Contents

Introduction

The following information describes DNS configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

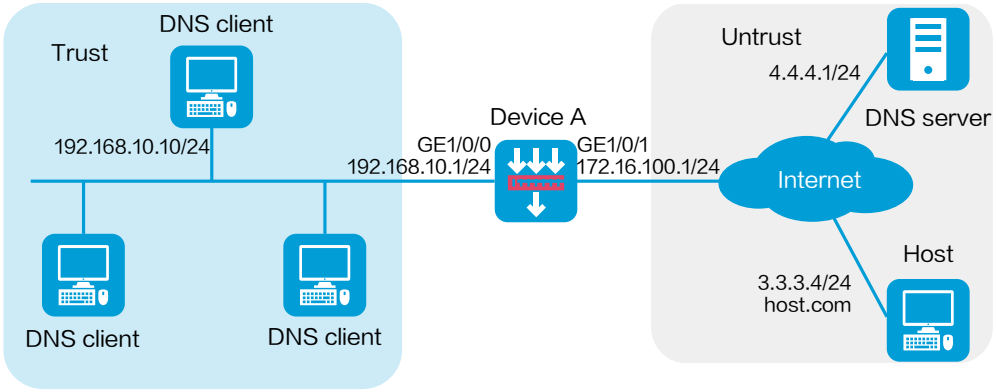
The following information is provided based on the assumption that you have basic knowledge of DNS.

Example: Configuring DNS proxy

Network configuration

As shown in Figure 1, Device A acts as the DNS proxy to relay DNS packets between DNS clients and the DNS server. DNS clients access the host with domain name **host.com** through the DNS proxy.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Restrictions and guidelines

Clear the DNS cache on the DNS proxy and DNS clients if the IP address of the DNS server changes or a domain name-to-IP address mapping changes.

Procedure

Configuring Device A

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Untrust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 172.16.100.1/24.

   c. Click **OK**.

   # Add GE 1/0/0 to the **Trust** security zone and set its IP address to 192.168.10.1/24 in the same way you configure GE 1/0/1.

2. Configure security policy **dns-a**.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Specify the policy name. In this example, the name is **dns-a**.

b. Select the source zone. In this example, the source zone is Trust.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Specify the IP address of the DNS client as the source IPv4 address. In this example, the address is 192.168.10.10/24.

g. Specify the IP address of the external host as the destination IPv4 address. In this example, the address is 3.3.3.4/24.

h. Click **OK**.

3. Configure security policy **dns-b**.

a. Specify the policy name. In this example, the name is **dns-b**.

b. Select the source zone. In this example, the source zone is Local.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Click **OK**.

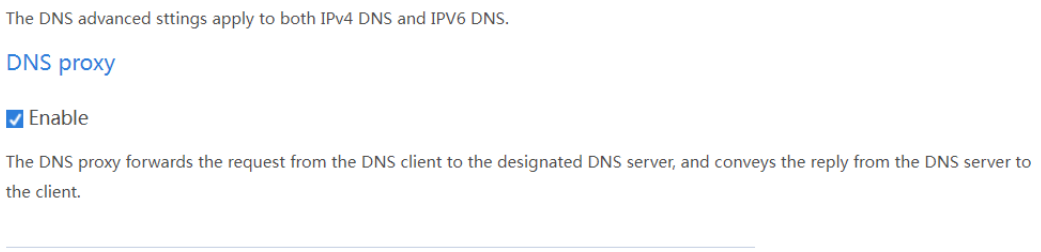
4. Configure DNS proxy.

On the top navigation bar, click **Network**.

From the navigation pane, select **DNS** > **Advanced Settings**.

Select **Enable**.

Figure 2 Enabling DNS proxy



5. Specify the IP address of the DNS server.

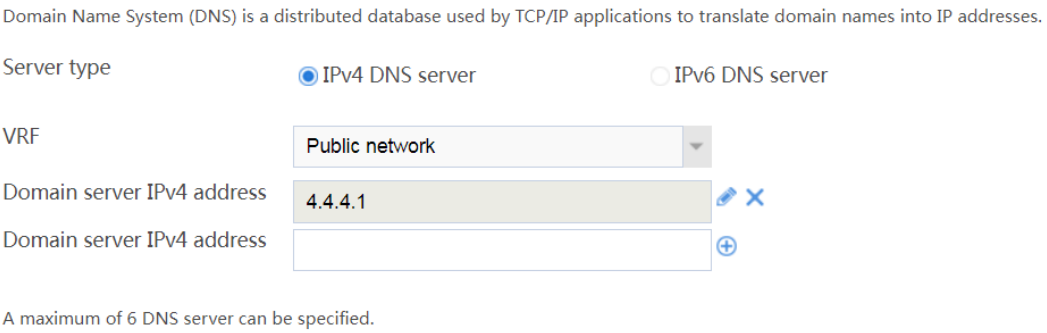
   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **DNS** > **DNS Client**.

   # Enter the IP address of the DNS server.

   # Click the **Add** icon.

Figure 3 Specifying the DNS server



Configuring DNS clients

Assign IP addresses to DNS clients and specify the IP address of the DNS server on DNS clients.

Verifying the configuration

1. Verify that each DNS client can successfully ping the host with domain name **host.com**.

```
C:\Users\abc>ping host.com


Pinging host.com [3.3.3.4] with 32 bytes of data:
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253

Ping statistics for 3.3.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

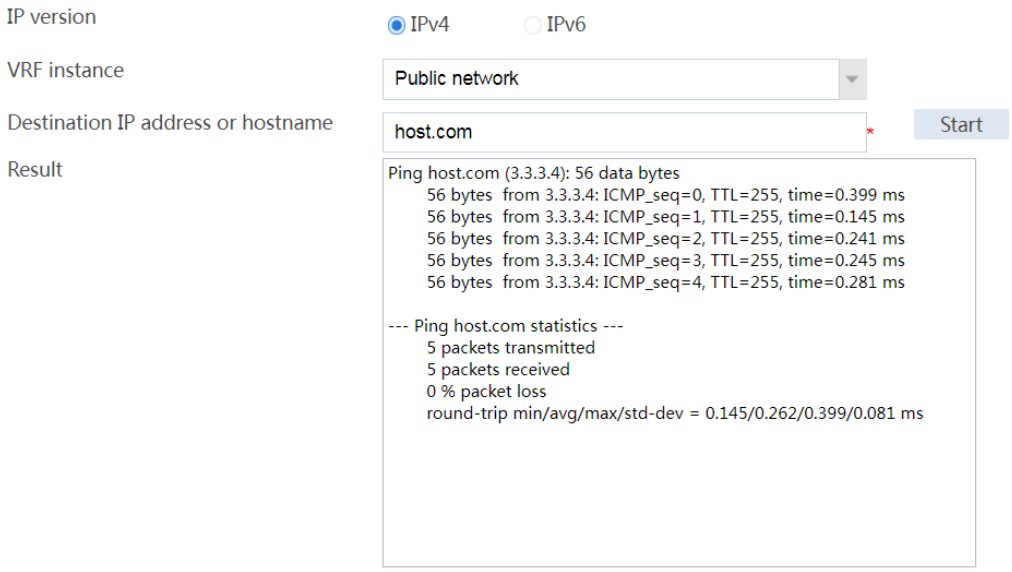
2. Verify that Device A can successfully ping the host with domain name **host.com**.

   # On the top navigation bar, click **System**.

   # From the navigation pane, select **Diagnosis Center** > **Ping**.

   # In the **Destination IP address or hostname** field, enter **host. com**, and click **Start**.

Figure 4 Ping operation



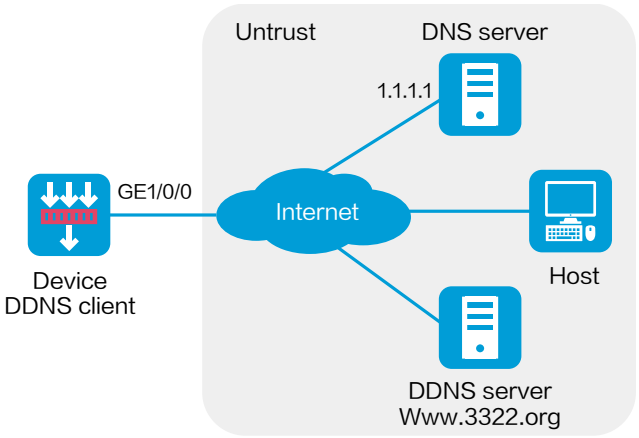
Example: Configuring DDNS

Network configuration

As shown in Figure 5, the device is a Web server with domain name **whatever.3322.org** and uses an IP address dynamically obtained through DHCP. To make sure the device can always provide Web services at **whatever.3322.org** when its IP address changes, perform the following tasks on the device:

- Configure a DDNS policy to update the device's domain name-to-IP address mapping on the DDNS server. The DDNS server then updates the mapping on the DNS server.
- Specify the IP address of the DNS server so that the device can access the DDNS server through domain name.

Figure 5 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Prerequisites

Before configuring DDNS on the device, perform the following tasks:

- Register with username **hell** and password **neve** at http://www.3322.org/.
- Create a mapping between the device's FQDN and IP address on the DNS server.

Procedure

1. Configure security policy **ddns-a**.

   # On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Specify the policy name. In this example, the name is **ddns-a**.

b. Select the source zone. In this example, the source zone is Local.

c. Select the destination zone. In this example, the destination zone is Untrust.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Click **OK**.

2. Configure security policy **ddns-b**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create** and click **Create a policy**.

In the dialog box that opens, configure policy parameters as follows:

a. Specify the policy name. In this example, the name is **ddns-b**.

b. Select the source zone. In this example, the source zone is Untrust.

c. Select the destination zone. In this example, the destination zone is Local.

d. Select **IPv4** as the type.

e. Select **Permit** as the action.

f. Click **OK**.

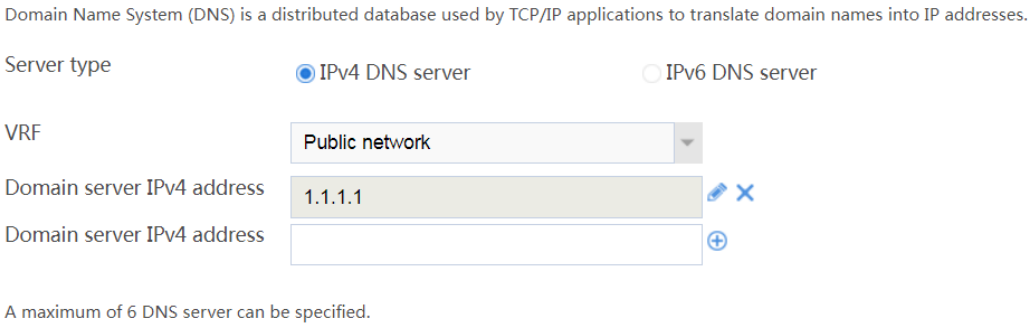
3. Specify the IP address of the DNS server.

On the top navigation bar, click **Network**.

From the navigation pane, select **DNS** > **DNS Client**.

Add the IP address of the DNS server, as shown in Figure 6.

Figure 6 Specifying the DNS server



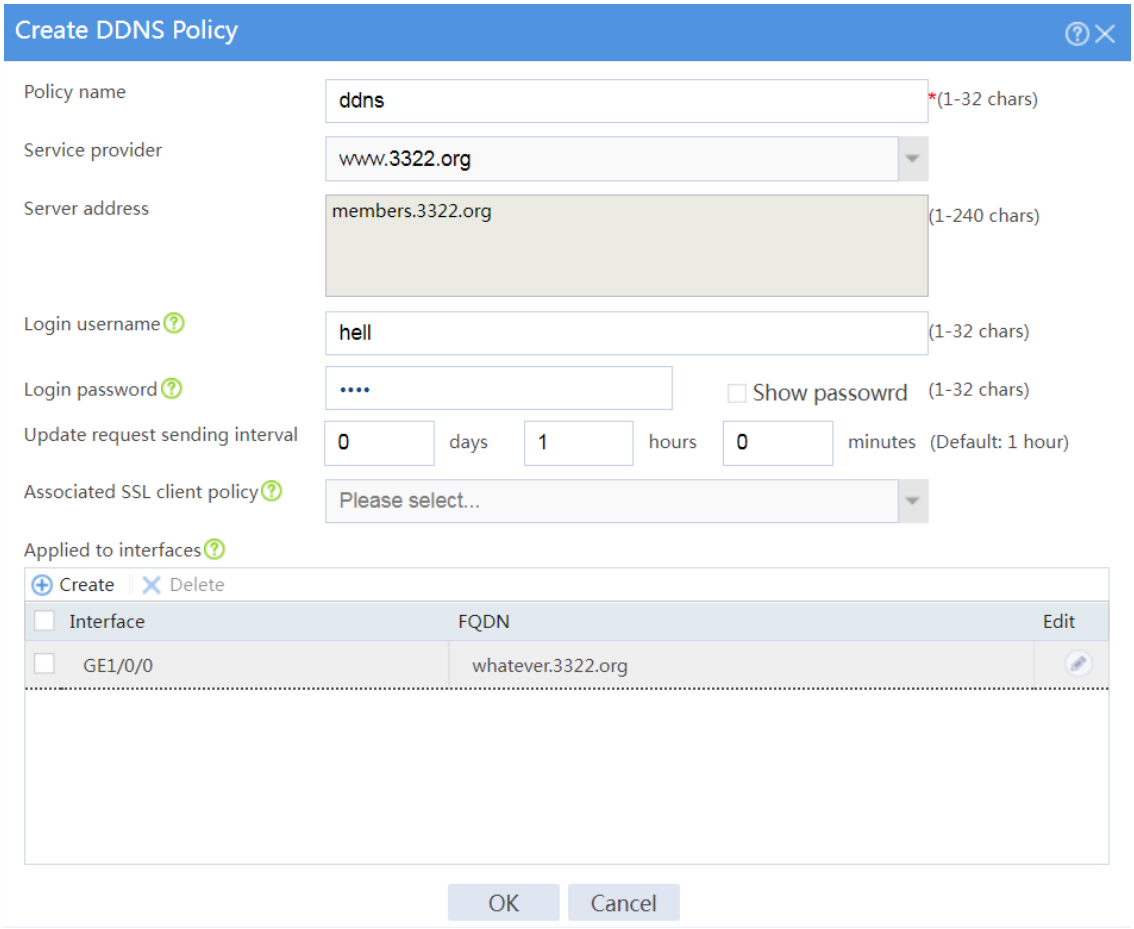
4. Configure a DDNS policy.

   # From the navigation pane, select **DNS** > **DDNS Policies**.

   # Click **Create**.

   # In the dialog box that opens, create a DDNS policy, as shown in Figure 7.

Figure 7 Creating a DDNS policy



Click **OK**.

Verifying the configuration

Verify that the device can update its domain name-IP mapping through the DDNS provider www.3322.org when its IP address changes. The Internet users can resolve the correct IP address through the domain name **whatever.3322.org** to access the Web service.

Server connection detection configuration examples

Contents

Introduction

The following information provides server connection detection (SCD) configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the SCD feature.

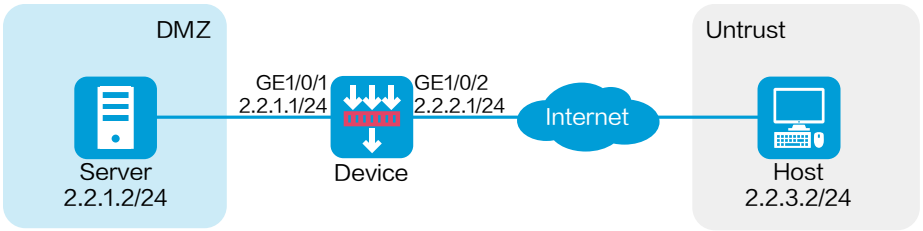
Example: Configuring SCD

Network configuration

As shown in Figure 1, configure SCD on the device to perform the following tasks:

- Monitor connections initiated by servers in subnet 2.2.1.0/24 for one day.
- Logs all connections initiated by the server except for TCP connections destined for TCP ports 80 and 443 on host 2.2.3.2/24.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

Click the **Edit** icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. Select the **DMZ** security zone.

b. Click the **IPv4 Address** tab, and then enter the IP address and mask of the interface. In this example, enter 2.2.1.1/24.

c. Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 2.2.2.1./24 in the same way you configure GE 1/0/1.

2. Configure a route:

This example configures a static route. If dynamic routes are required, configure a dynamic routing protocol.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

On the **IPv4 Static Routing** tab, click **Create**.

In the dialog box that opens, create an IPv4 static route:

- Enter destination address **2.2.3.0**.
- Enter mask length **24**.
- Enter next hop address **2.2.2.2**.

Click **OK**.

3. Create a security policy:

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that opens, configure a security policy:

- Enter policy name **test-a**.
- Select source zone **DMZ**.
- Select destination zone **Untrust**.
- Select type **IPv4**.
- Select action **Permit**.

- Select source IP address **2.2.1.0/24**.

Cilck **OK**.

4. Create an internal IP address object group.

On the top navigation bar, click **Objects**.

From the navigation pane, select **Object Groups** > **IPv4 Address Object Groups**.

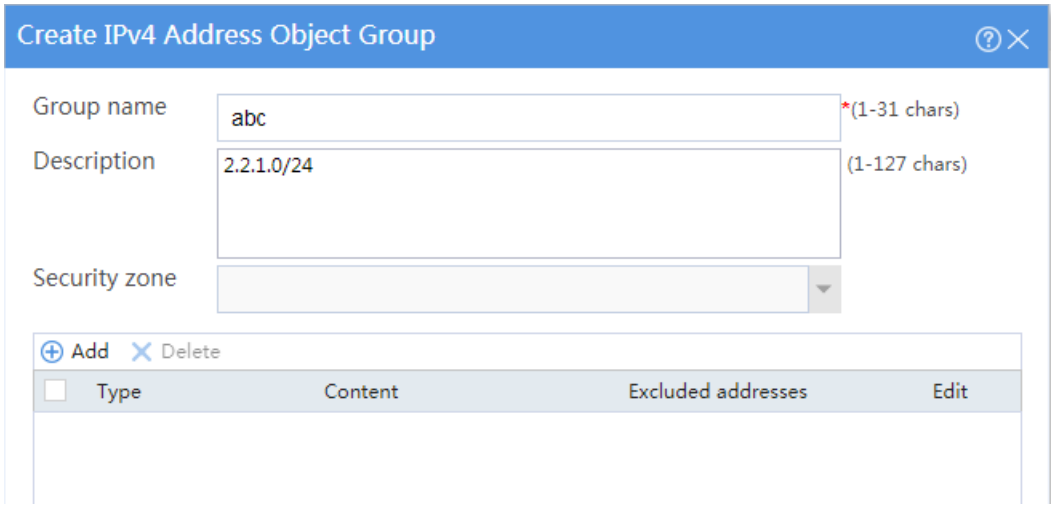
Click **Create**.

In the dialog box that opens, configure the IPv4 address object group:

a. Enter a group name. In this example, enter **abc**.

b. Enter a description. In this example, enter **2.2.1.0/24**.

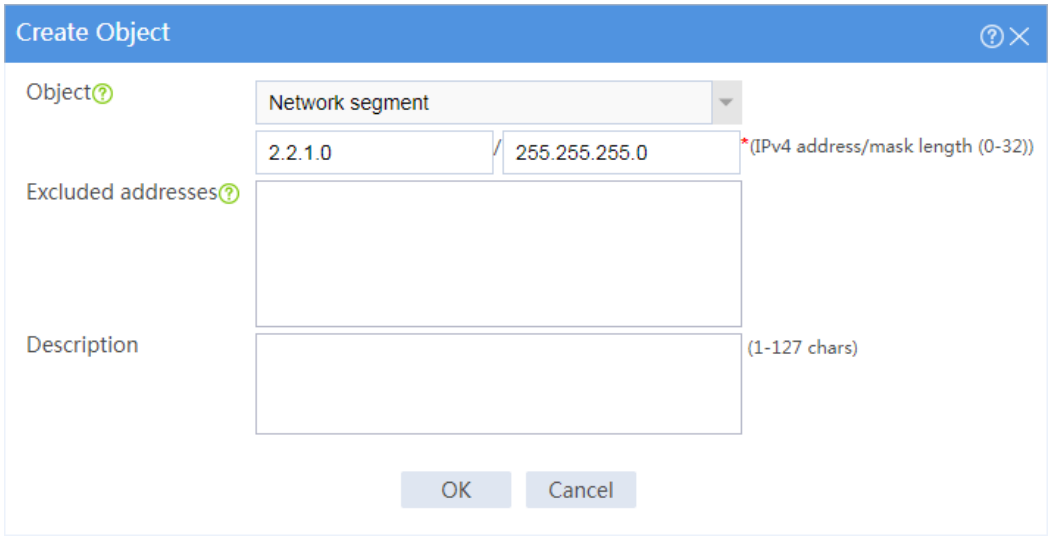
Figure 2 Creating IPv4 address object group



c. Click **Add**.

d. In the dialog box that opens, select the **Network segment** object, and enter the IPv4 address and mask **2.2.1.0/24**.

Figure 3 Creating object



e. Click **OK**.

5. Configure server connection learning.

On the top navigation bar, click **Policies**.

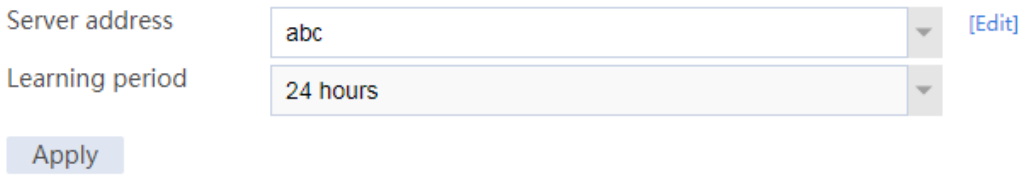
From the navigation pane, select **Server Connection Detect** > **SCD learning**.

Enter a server address. In this example, enter **abc**.

Select a learning period. In this example, select **24 hours**.

Click **Apply**.

Figure 4 Configuring server connection learning



6. Configure an SCD policy.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Server Connection Detect** > **SCD Policy**.

Click **Create**.

In the dialog box that opens, create an SCD policy:

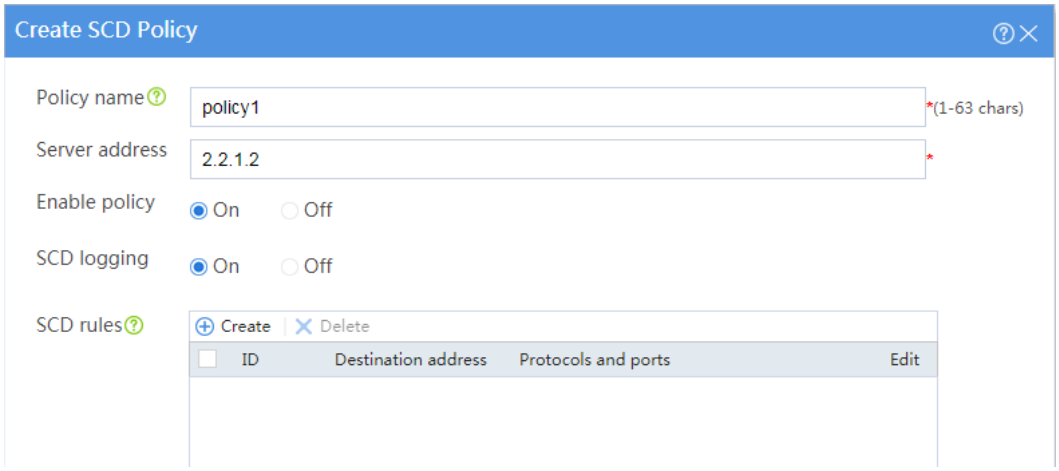
a. Enter a policy name. In this example, enter **policy1**.

b. Enter a server address. In this example, enter **2.2.1.2**.

c. Enable policy.

d. Enable SCD logging.

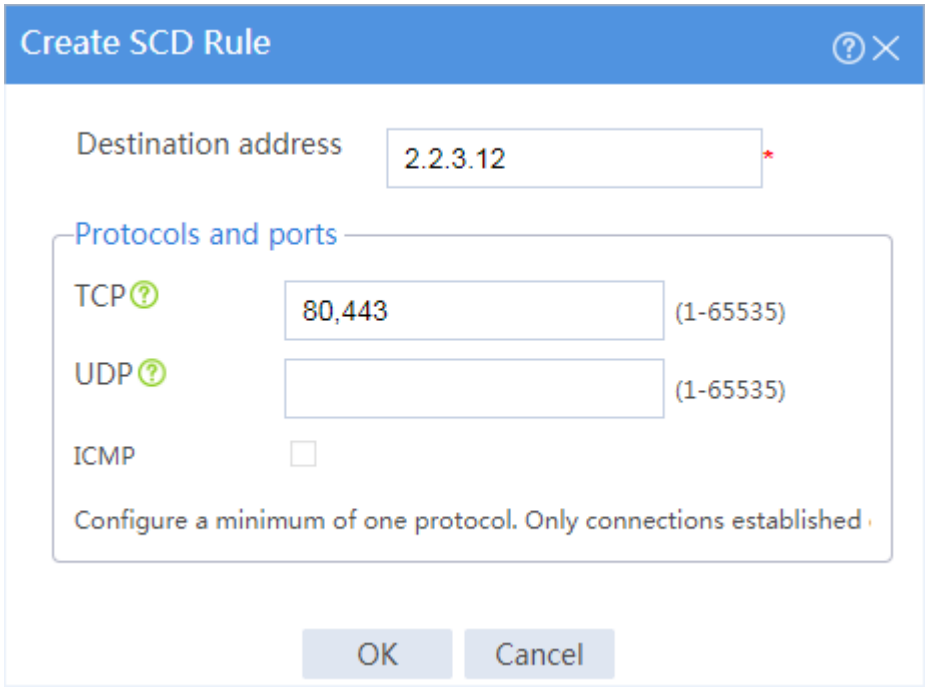
Figure 5 Creating an SCD policy



e. Click **Create**.

f. In the dialog box that opens, enter the destination address **2.2.3.12** and TCP ports **80** and **443**.

Figure 6 Creating an SCD rule



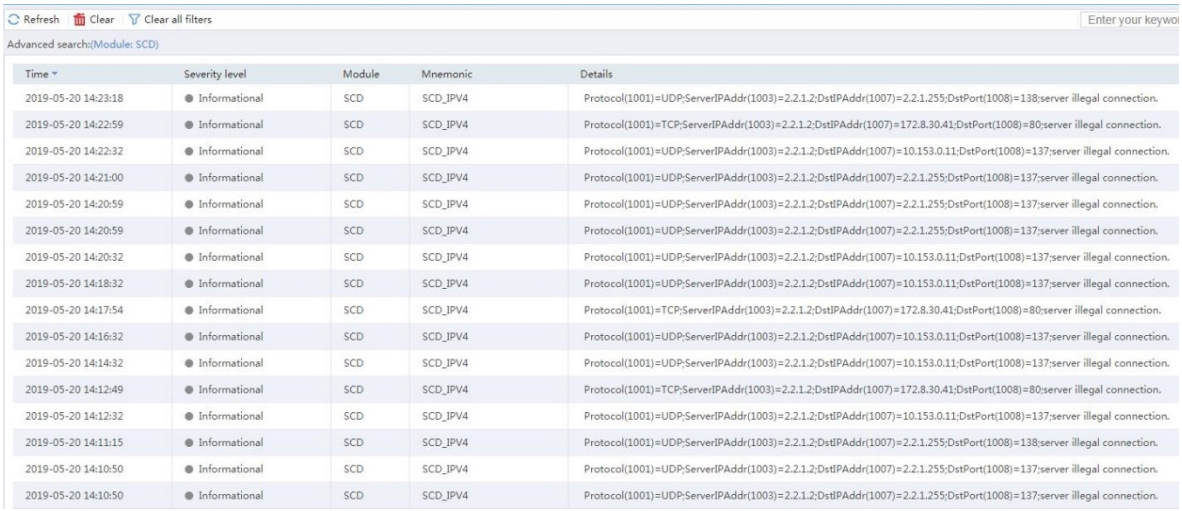
g. Click **OK** to create the SCD rule.

h. Click **OK** to create the SCD policy.

Verifying the configuration

To view the logs generated for server connection events, click **Monitor** on the top navigation bar, and then select **Device Logs** > **System Logs** from the navigation pane.

Figure 7 Viewing the device logs



Time	Severity level	Module	Mnemonic	Details
2019-05-20 14:23:18	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=138;server illegal connection.
2019-05-20 14:22:59	Informational	SCD	SCD_IPV4	Protocol(1001)=TCP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=172.8.30.41;DstPort(1008)=80;server illegal connection.
2019-05-20 14:22:32	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:21:00	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:20:59	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:20:59	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:20:32	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:18:32	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:17:54	Informational	SCD	SCD_IPV4	Protocol(1001)=TCP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=172.8.30.41;DstPort(1008)=80;server illegal connection.
2019-05-20 14:16:32	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:14:32	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:12:49	Informational	SCD	SCD_IPV4	Protocol(1001)=TCP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=172.8.30.41;DstPort(1008)=80;server illegal connection.
2019-05-20 14:12:32	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:11:15	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=138;server illegal connection.
2019-05-20 14:10:50	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:10:50	Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.

Connection limit configuration examples

Contents

Introduction

The following information provides connection limit configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of the connection limit feature.

Example: Configuring connection limits

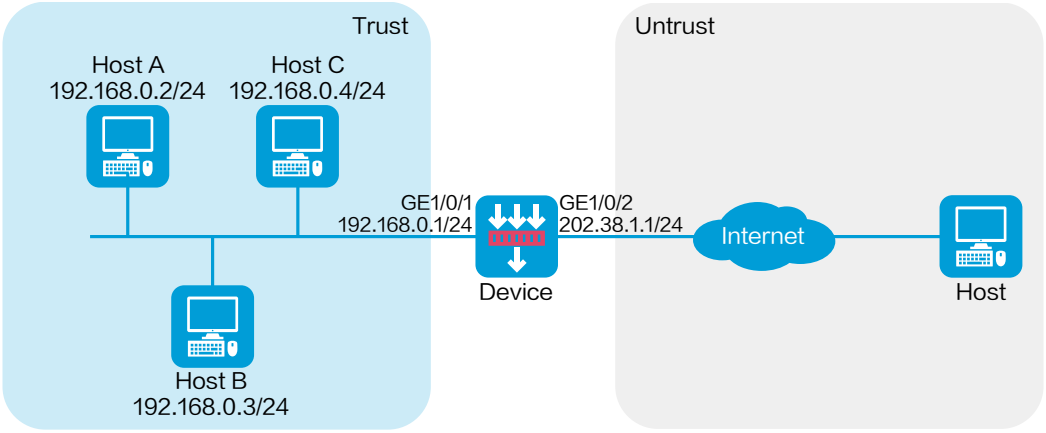
Network configuration

As shown in Figure 1, a firewall is deployed as the egress device that connects the internal network to the Internet.

Configure connection limits to meet the following requirements:

- All hosts on 192.168.0.0/24 can establish a total of up to 100000 connections with the Internet.
- Each host on 192.168.0.0/24 can establish a maximum of 100 connections with the Internet.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedures

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   - Select the **Trust** security zone.
   - On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 192.168.0.1/24.
   - Use the default settings for other parameters.
   - Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 202.38.1.1/24 in the same way you configure GE 1/0/1.

2. Configure security policies.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **test-a**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select type **IPv4**.
   - Select action **Permit**.
   - Enter source IPv4 address **192.168.0.0/24**.
   - Enter destination IPv4 address **202.38.1.0/24**.

- Use the default settings for other parameters.
- Click **OK**.

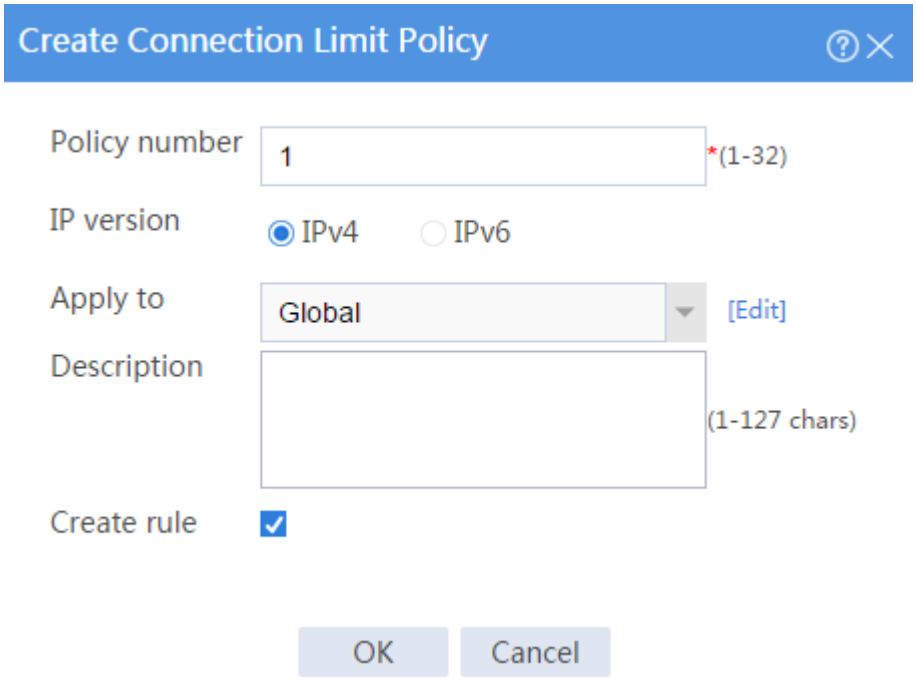
3. Configure connection limit policies.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Attack Defense** > **Connection Limit**.

   # Click **Create**.

Figure 2 Creating connection limit policy 1



   # In the dialog box that opens, configure connection limit policy **1**:

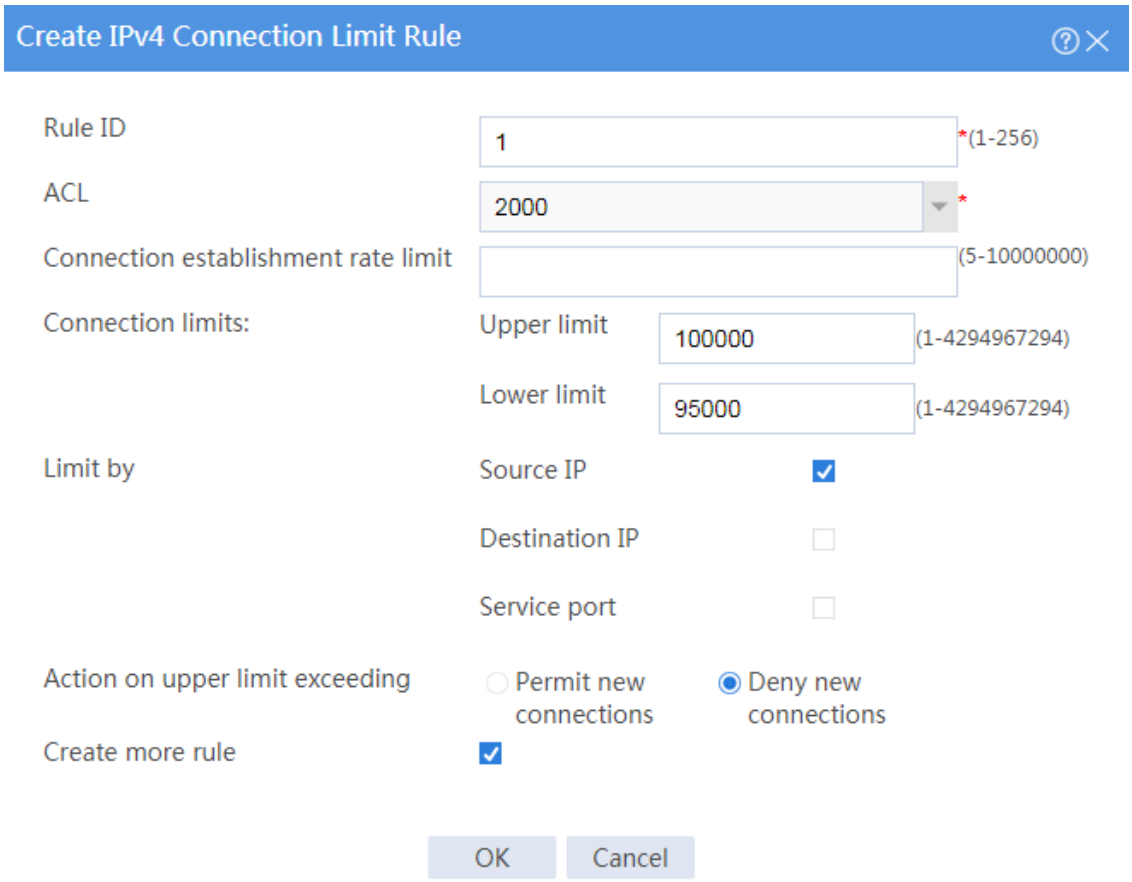
   - Enter policy number 1.
   - Select IP version **IPv4**.
   - Select **Global** for the **Apply to** field.
   - Select **Create rule**.
   - Click **OK** to create a connection limit rule.

   # In the dialog box that opens, configure connection limit rule **1**:

   - Enter rule ID 1.

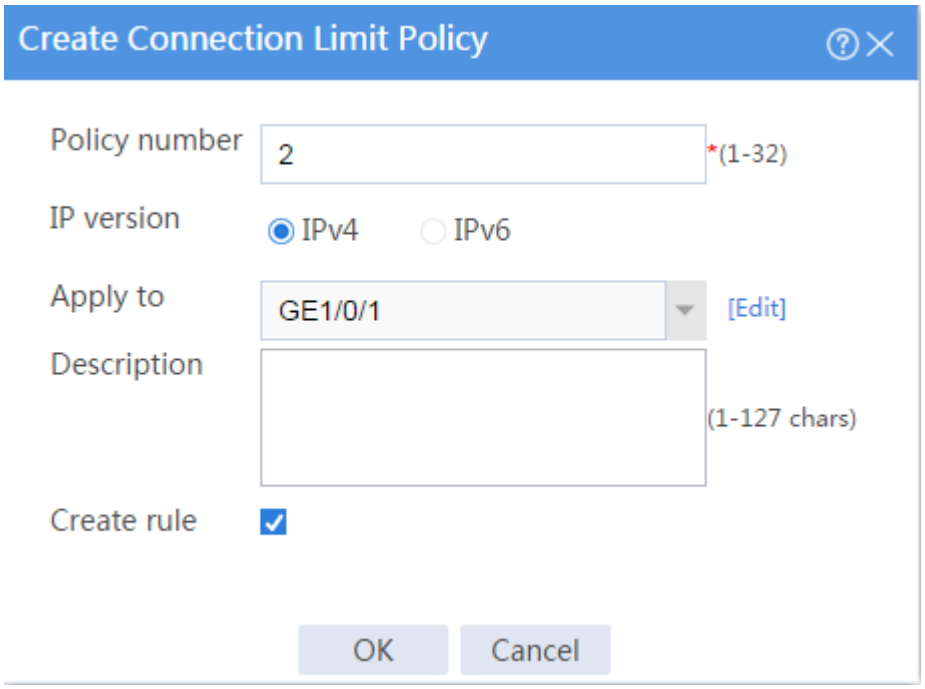
- Select ACL 2000. This ACL matches the source IP addresses on the network segment 192.168.0.0/24..
- Set the upper limit to 100000 and lower limit to 95000.
- Select **Source IP** for the **Limit by** field.
- Deselect **Create more rule**.
- Click **OK**.

Figure 3 Creating connection limit rule 1



Click **Create** to create another connection limit policy.

Figure 4 Creating connection limit policy 2



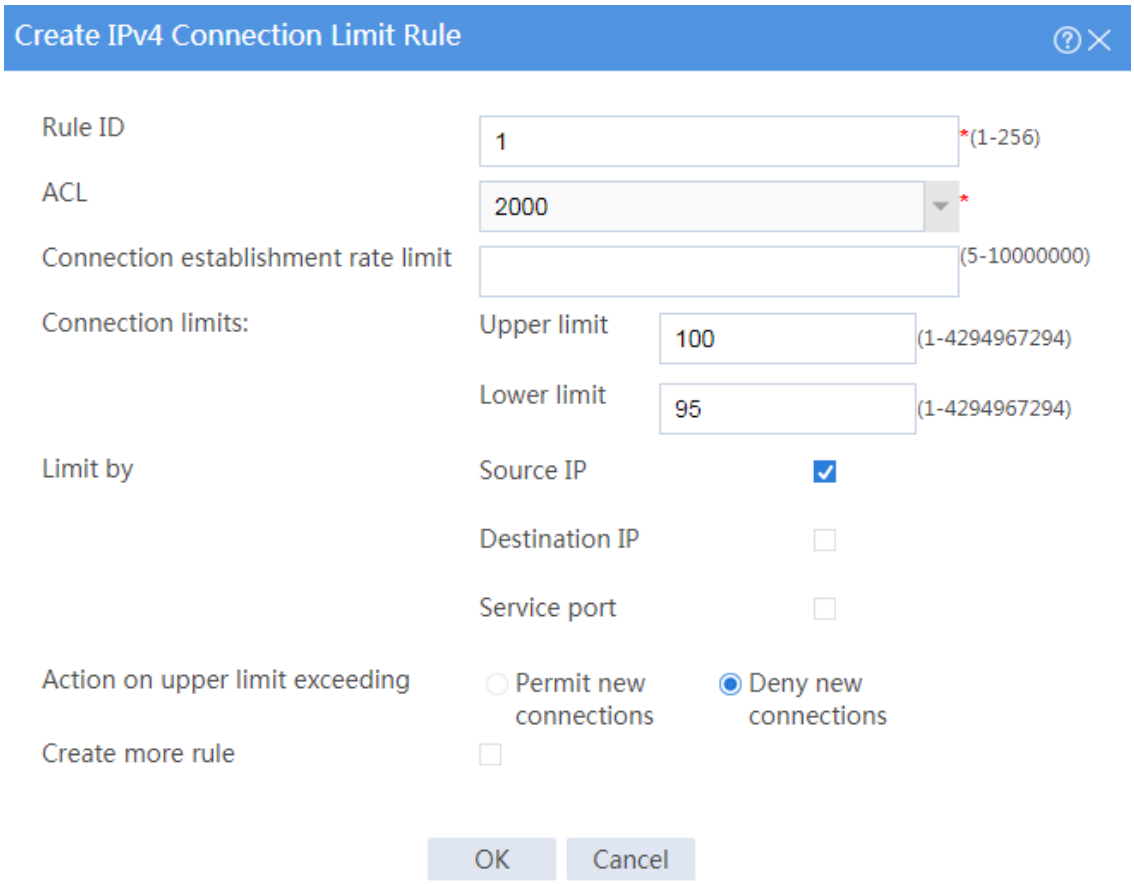
In the dialog box that opens, configure connection limit policy **2**:

- Enter policy number 2.
- Select IP version **IPv4**.
- Select **GE1/0/1** for the **Apply to** field.
- Select **Create rule**.
- Click **OK** to create a connection limit rule.

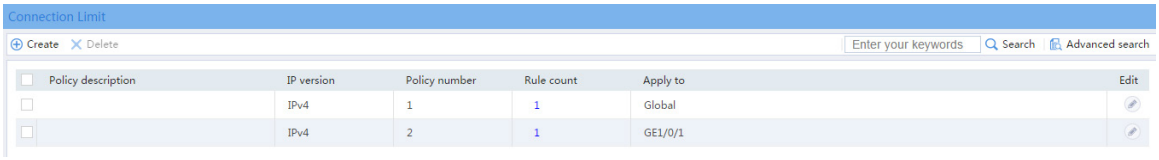
In the dialog box that opens, configure connection limit rule **1**:

- Enter rule ID 1.
- Select ACL 2000. This ACL matches the source IP addresses on the network segment 192.168.0.0/24.
- Set the upper limit to 100 and lower limit to 95.
- Select **Source IP** for the **Limit by** field.
- Deselect **Create more rule**.
- Click **OK**.

Figure 5 Creating connection limit rule 1



After the configuration, the connection limit policies appear as follows:



Verifying the configuration

Verify that all hosts on 192.168.0.0/24 can establish a total of up to 100000 connections with the Internet and that each host on 192.168.0.0/24 can establish a maximum of 100 connections with the Internet.

Public key management configuration examples

Contents

Introduction

The following information provides configuration examples for public key management.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of public key management.

Restrictions and guidelines

When you manually enter the peer host public key, make sure the entered key is in the correct format. To obtain the peer host public key in the correct format, display the public key on the peer device and record the key. The format of the public key displayed in any other way might be incorrect. If the key is not in the correct format, the system discards the key and displays an error message.

As a best practice, import rather than enter the peer host public key if you are not sure whether the device supports the format of the recorded peer host public key.

Example: Entering a peer host public key

Network configuration

As shown in Figure 1, to prevent illegal access from Device A to Device B, Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, use the following procedure to configure the public key of Device A on Device B:

- Create RSA key pairs on Device A and display the public keys of the RSA key pairs.

- Manually specify the RSA host public key of Device A on Device B.

Figure 1 Network diagram

Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedures

Configuring Device A

On the top navigation bar, click **Objects**.

From the navigation pane, select **Public Key Management** > **Local Key Pairs**.

Click **Create**. The **Create Local Key Pair** page opens.

Create an RSA local key pair as follows:

- Enter key pair name **devicea-rsa**.
- Select the **RSA** algorithm.
- Enter key length **1800**.

Click **OK**.

Click key pair name **devicea-rsa** to open the **Key Pair Details** page.

Record the data displayed in the **Public key** field.

Figure 2 Creating a local key pair

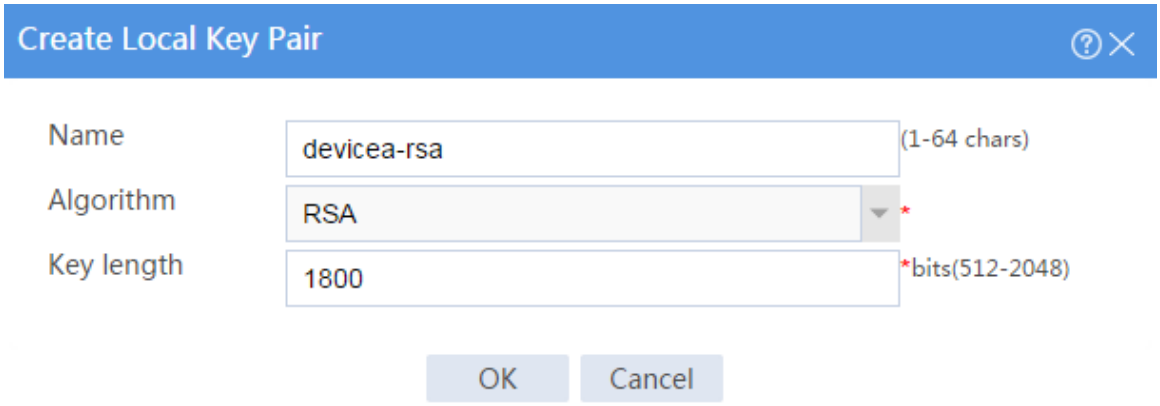
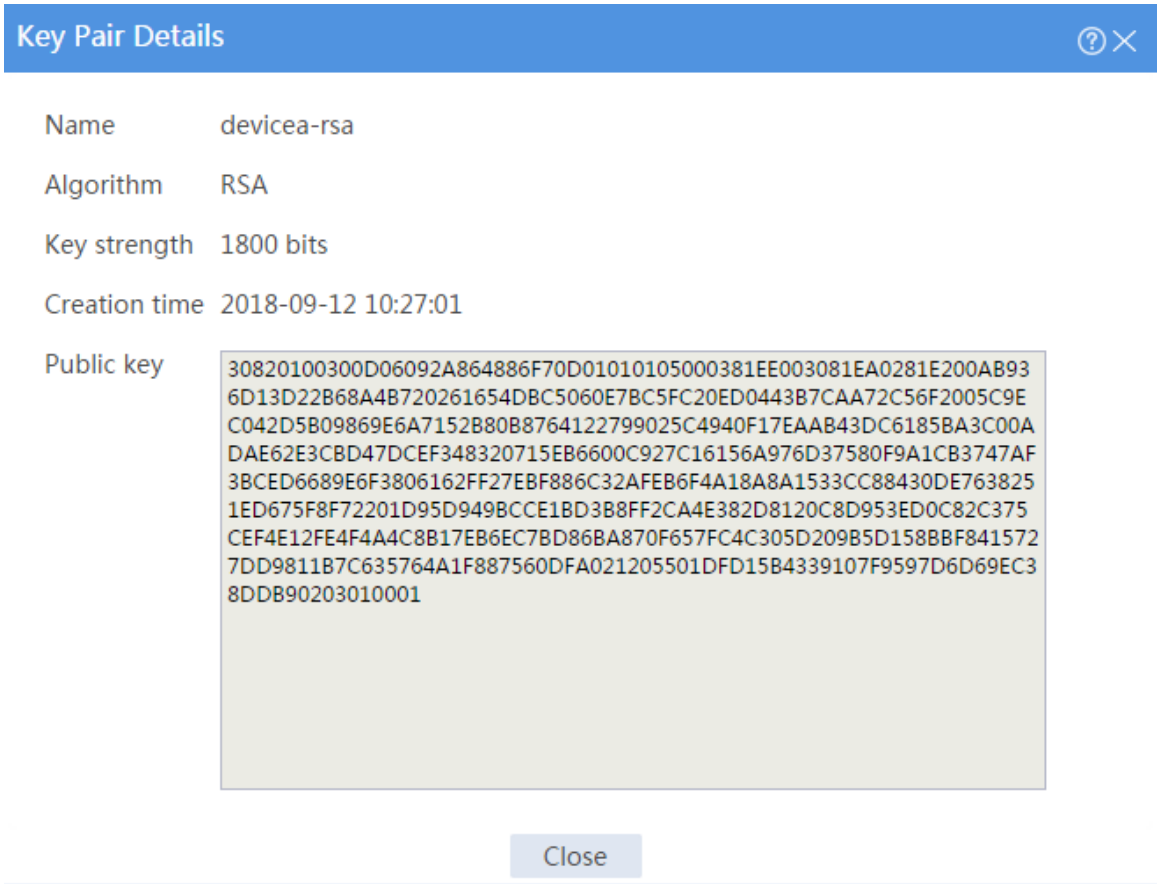


Figure 3 Key details



Configuring Device B

On the top navigation bar, click **Objects**.

From the navigation pane, select **Public Key Management** > **Local Key Pairs**.

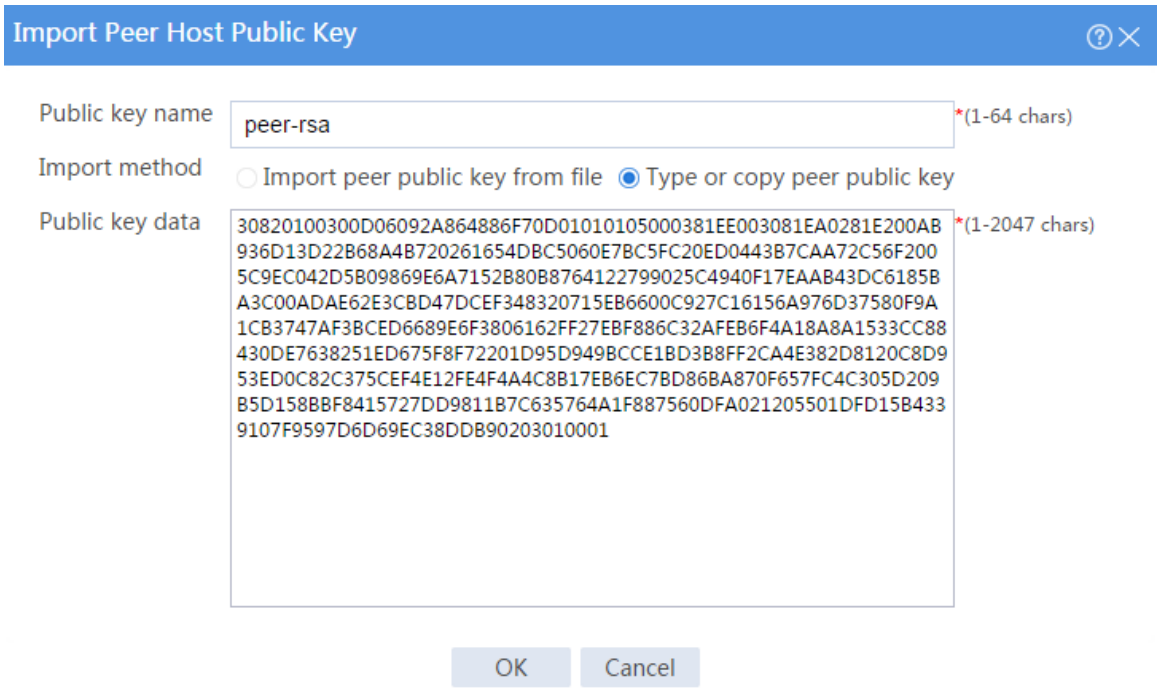
Click **Import**. The **Import Peer Host Public Key** page opens.

Configure the peer host public key as follows:

- Enter public key name **peer-rsa**.
- Select the **Type or copy peer public key** import method.
- In the **Public key data** field, type the public key data of Device A, or copy and then paste the public key data of Device A.

Click **OK**.

Figure 4 Entering the peer host public key



Verifying the configuration

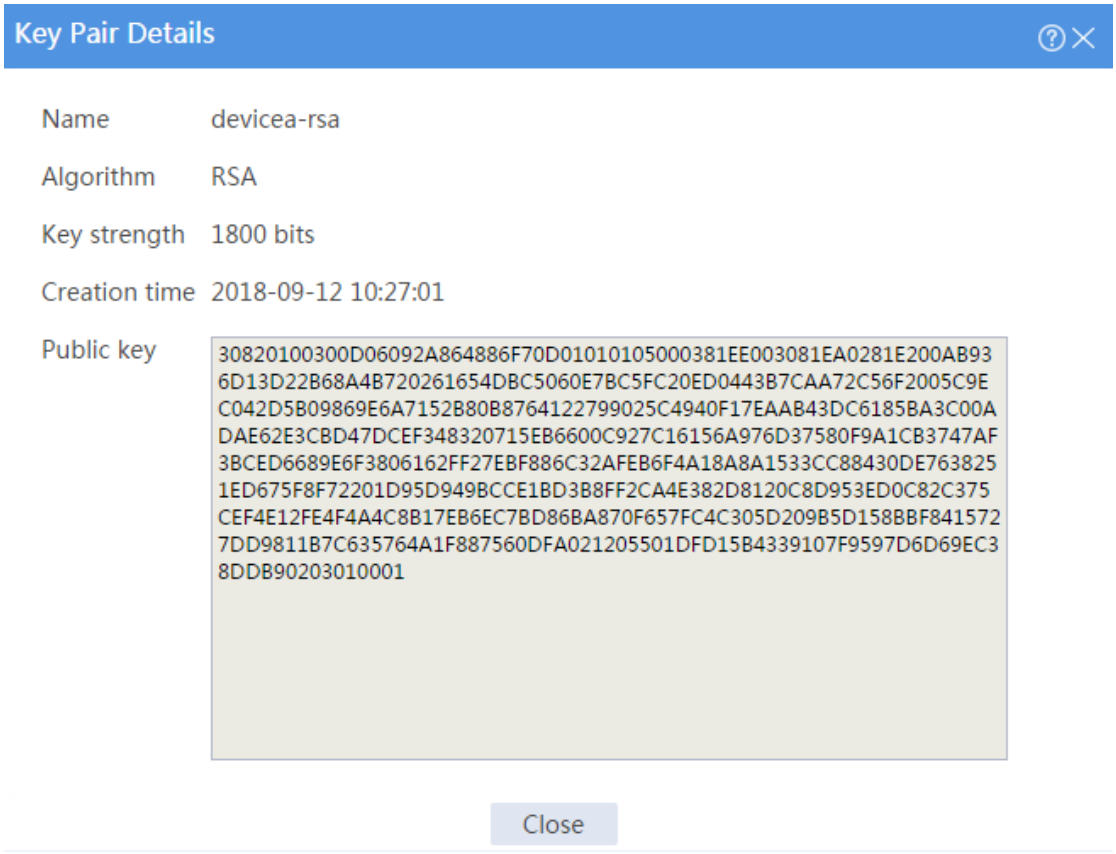
1. Display information about the local public key on Device A.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, **Public Key Management** > **Local Key Pairs**.

   # Click the **Details** icon for key pair **devicea-rsa** to open the **Key Pair Details** page. The **Public key** field displays the content of the public key.

   Figure 5 Local host public key information



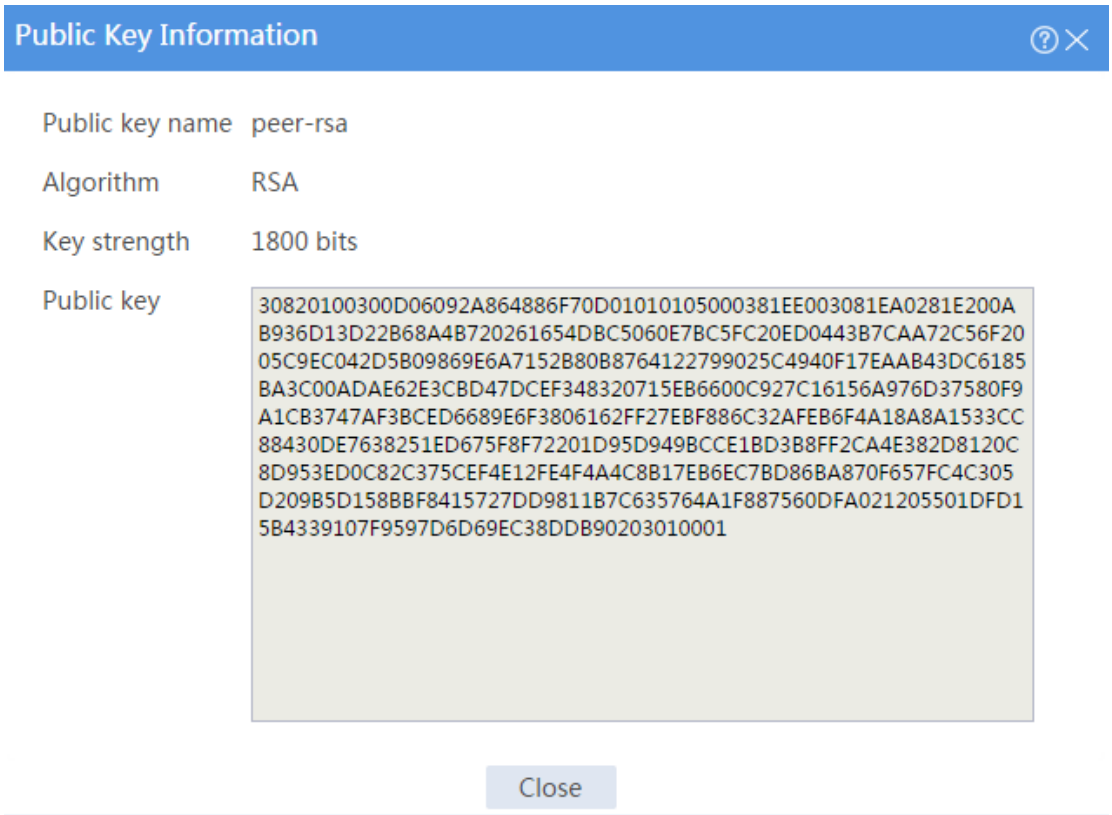
2. Display information about the peer public key configured on Device B.

   # On the top navigation bar, click **Objects**.

From the navigation pane, **Public Key Management** > **Peer Public Keys**.

Click the **Details** icon for public key **peer-rsa**.

Figure 6 Manually configured peer host public key



Example: Importing a peer host public key from a public key file

Network configuration

As shown in Figure 7, to prevent illegal access from Device A to Device B, Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, use the following procedure to configure the public key of Device A on Device B:

- Create RSA key pairs on Device A and export the RSA host public key to a file.
- Import the RSA host public key of Device A from the public key file to Device B.

Figure 7 Network diagram

Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedures

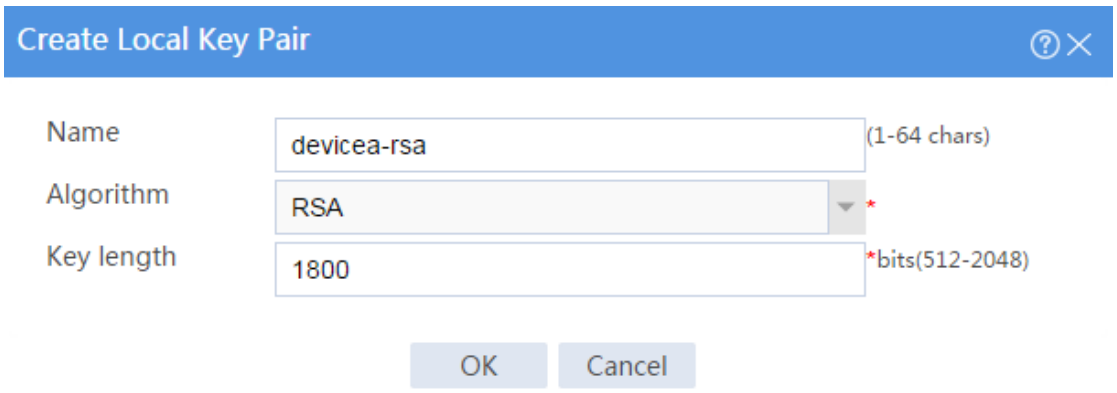
Configuring Device A

On the top navigation bar, click **Objects**.

From the navigation pane, select **Public Key Management** > **Local Key Pairs**.

Click **Create**. The **Create Local Key Pair** page opens.

Figure 8 Creating a local key pair



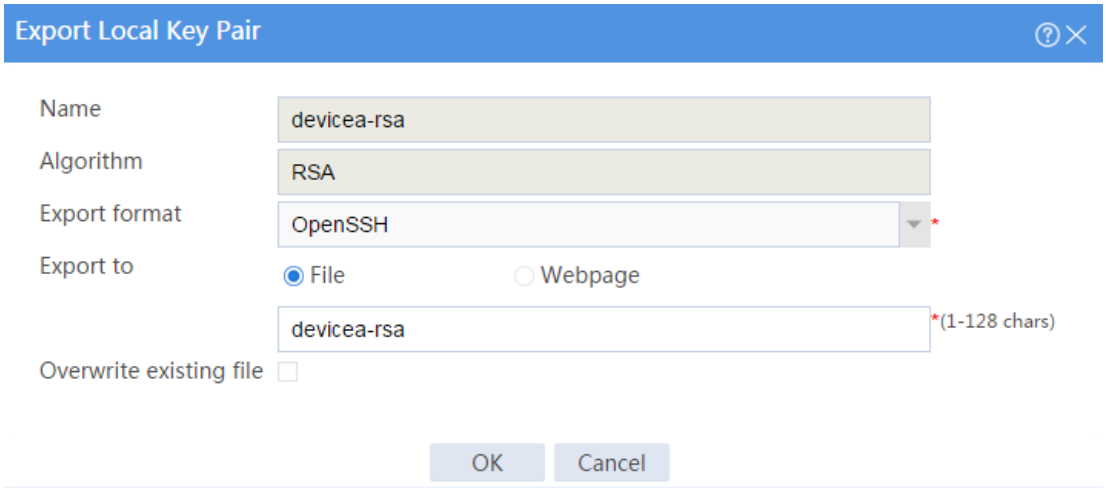
Create an RSA local key pair as follows:

- Enter key pair name **devicea-rsa**.
- Select the **RSA** algorithm.
- Enter key length **1800**.

Click **OK**.

Select key pair **devicea-rsa**, and then click **Export**. The **Export Local Key Pair** page opens.

Figure 9 Exporting a local host public key



Select the **OpenSSH** export format, export the host public key to a file named **devicea-rsa**, and then click **OK**.

After the key is exported to file **devicea-rsa**, transfer the file to the peer device (Device B). (Details not shown.)

Configuring Device B

On the top navigation bar, click **Objects**.

From the navigation pane, select **Public Key Management** > **Local Key Pairs**.

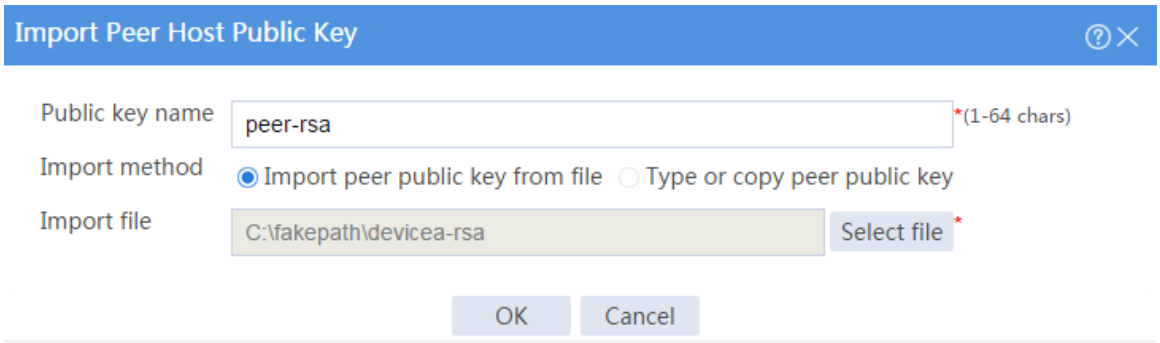
Click **Import**. The **Import Peer Host Public Key** page opens.

Configure the peer host public key as follows:

- Enter public key name **peer-rsa**.
- Select the **Import peer public key from file** import method.
- Select the path of public key file **devicea-rsa**.

Click **OK**.

Figure 10 Importing the peer host public key from a public key file



Verifying the configuration

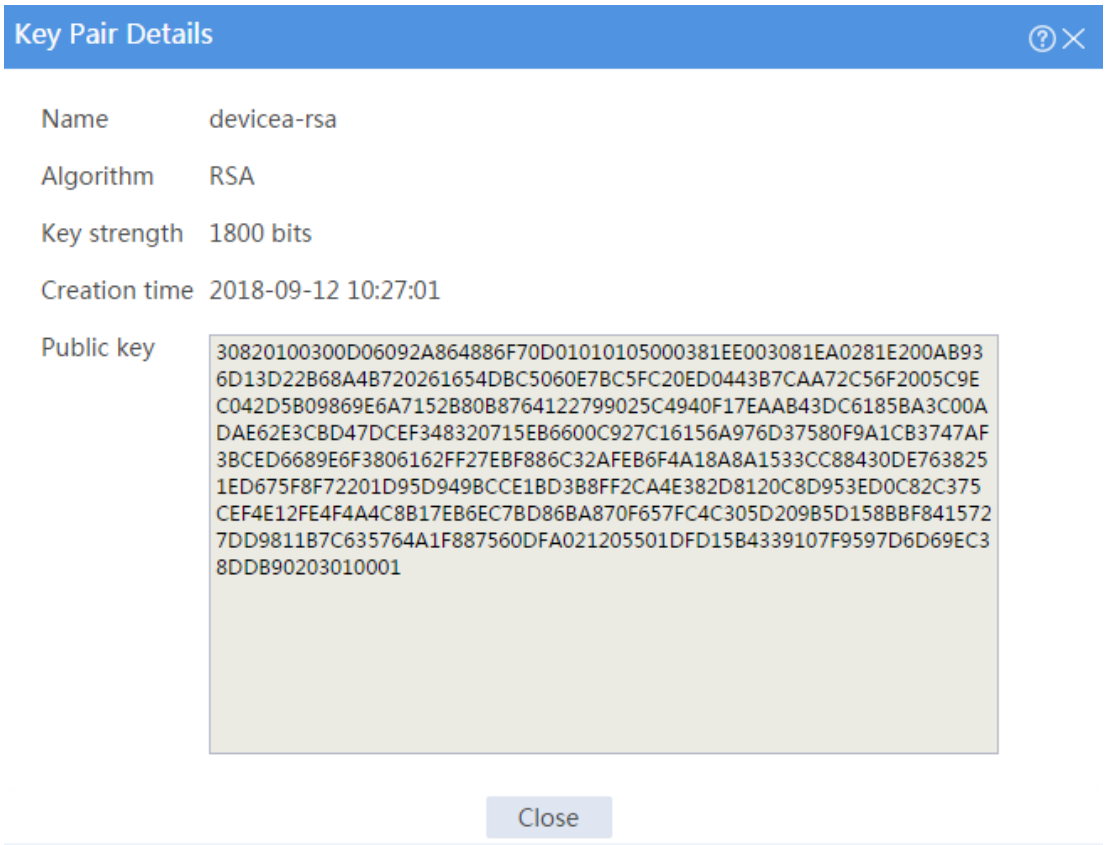
1. Display information about the local public key on Device A.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Public Key Management** > **Local Key Pairs**.

   # Click the **Details** icon for key pair **devicea-rsa** to open the **Key Pair Details** page. The **Public key** field displays the content of the public key.

Figure 11 Local host public key information



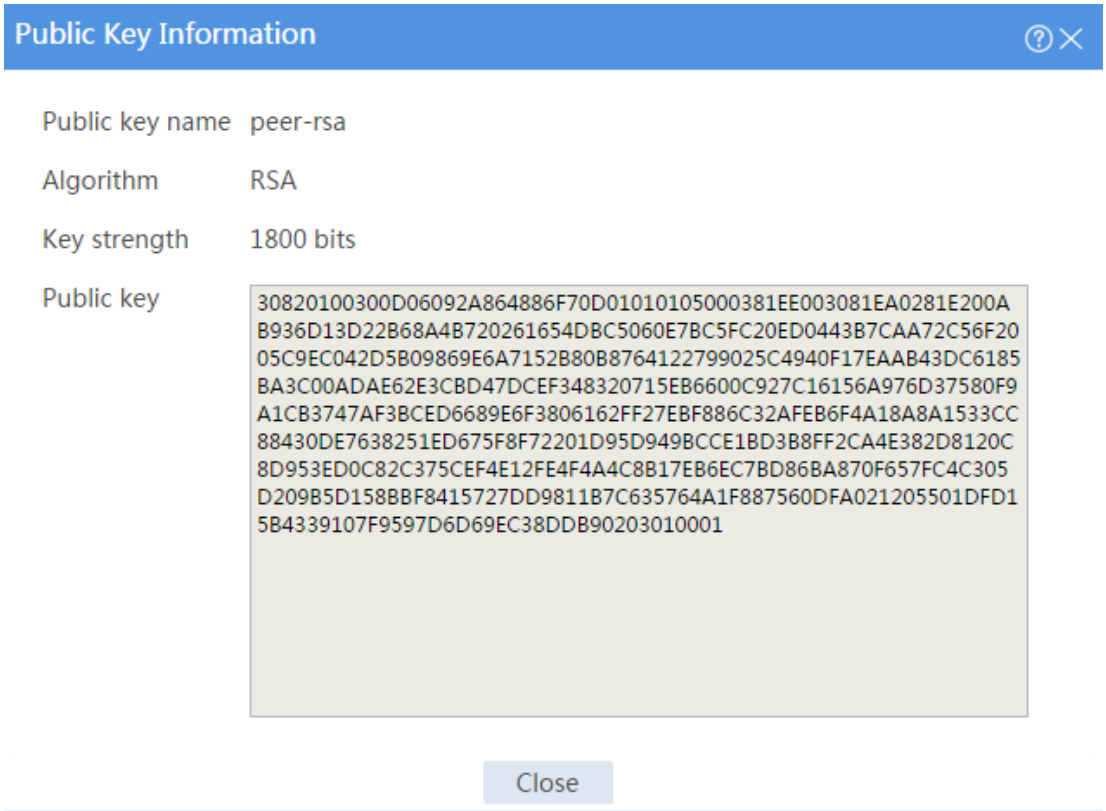
2. Display information about the peer public key configured on Device B.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Public Key Management** > **Peer Public Keys**.

   # Click the **Details** icon for public key **peer-rsa**.

Figure 12 Peer host public key imported from a public key file



SSL decryption configuration examples

Contents

Introduction

The following information provides SSL decryption configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedure and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of SSL decryption.

Restrictions and guidelines

When configuring SSL decryption, make sure the security policies allow the source and destination security zones to intercommunicate with the **Local** security zone.

After SSL decryption is configured, the IPS capture action becomes invalid.

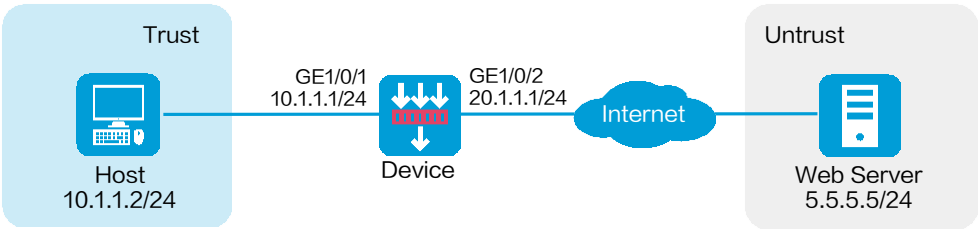
SSL decryption supports decrypting HTTPS, SMTPS, IMAPS, and POP3S protocol packets.

Example: Configuring SSL decryption

Network configuration

As shown in Figure 1, the device acts as the security gateway of an enterprise. The device cannot inspect SSL-encrypted packets (such as HTTPS packets), masking the security threats inside of the packets. To improve the internal network security, configure SSL decryption on the device to decrypt HTTPS packets for IPS inspection.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

1. Assign IP addresses to interfaces:

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 10.1.1.2/24.

   c. Use the default settings for other parameters.

   d. Click **OK**.

   # Add GE 1/0/2 to the **Untrust** security zone and set its IP address to 20.1.1.1/24 in the same way you configure GE 1/0/1.

2. Configure settings for routing:

   This example configures a static route to reach the Web server, and the next hop in the route is 20.1.1.2.

   # On the top navigation bar, click **Network**.

   # From the navigation pane, select **Routing** > **Static Routing**.

   # On the **IPv4 Static Routing** tab, click **Create**.

   # In the dialog box that opens, configure a static IPv4 route to reach the Web server:

   a. Enter destination IP address **5.5.5.0**.

   b. Enter mask length **24**.

   c. Enter next hop address **20.1.1.2**.

   d. Use the default settings for other parameters.

   e. Click **OK**.

3. Import the trusted SSL decryption certificate:

   # On the top navigation bar, click **Policies**.

From the navigation pane, select **Application Proxy** > **SSL Decryption Certificates**.

Click **Import**.

In the dialog box that opens, configure the following settings, as shown in Figure 2:

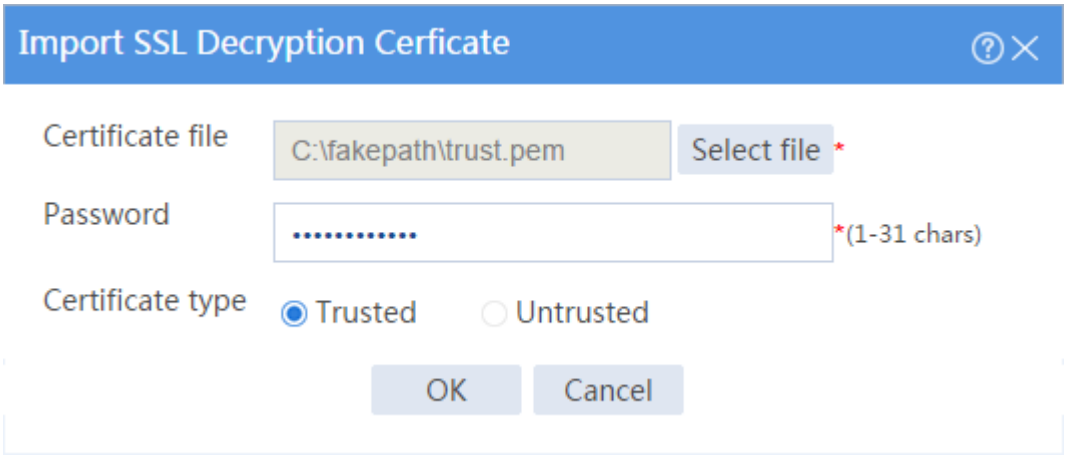
a. Select file **trust.pem**.

b. Enter the password of the file.

c. Set the certificate type to **Trusted**.

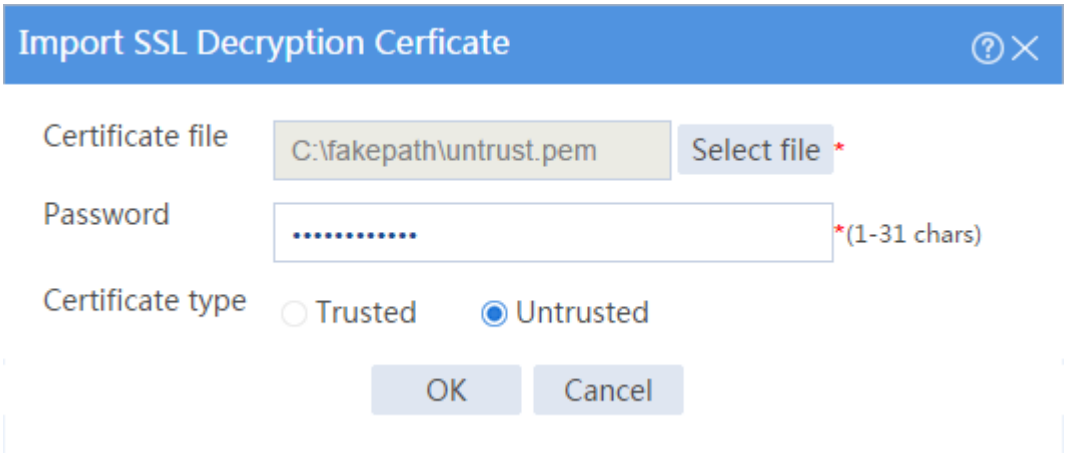
Click **OK**.

Figure 2 Importing the trusted SSL decryption certificate



Import the untrusted SSL decryption certificate in the same way you import the trusted SSL decryption certificate, as shown in Figure 3.

Figure 3 Importing the untrusted SSL decryption certificate



4. Install and trust the trusted SSL decryption certificate on the browser from the internal network. (Details not shown.)
5. Configure a proxy policy:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Application Proxy** > **Proxy Policy**.

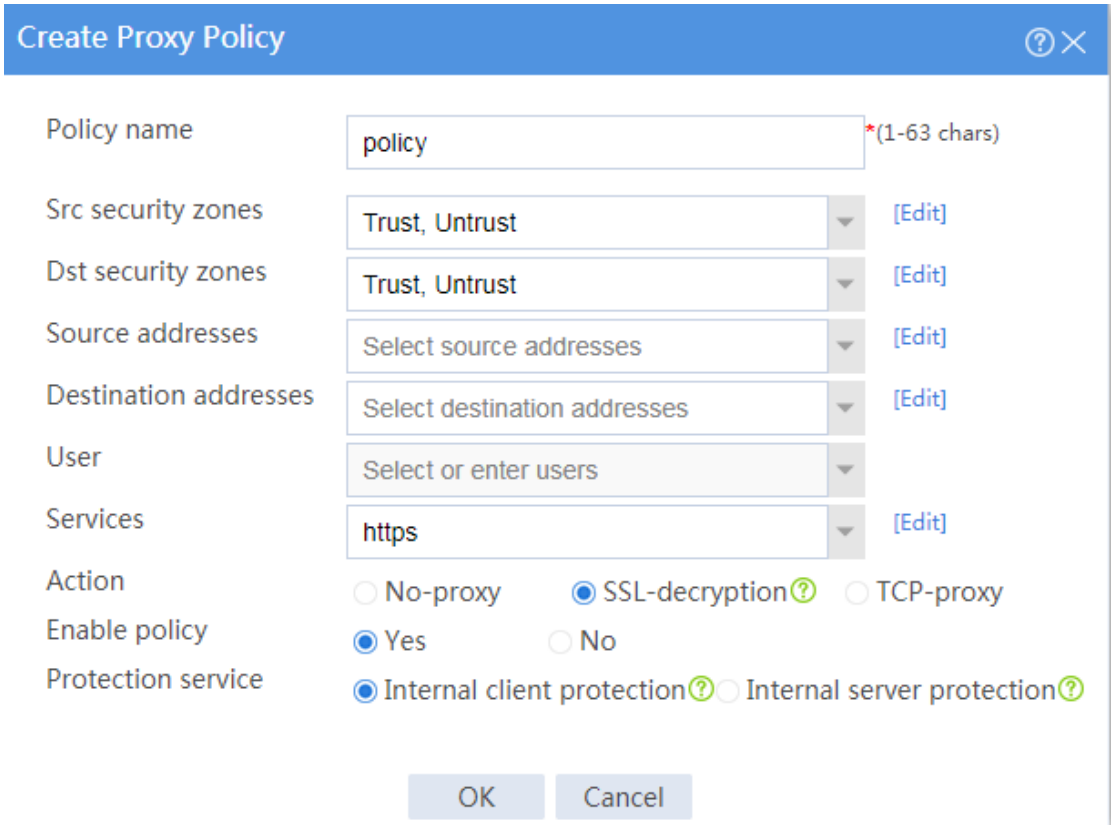
   # Click **Create**.

   # In the dialog box that opens, configure a proxy policy:

   - Enter policy name **policy1**.
   - Select source security zones **Trust** and **Untrust**.
   - Select destination security zones **Trust** and **Untrust**.
   - Select service **https**.
   - Select action **SSL-decryption**.
   - Enable the policy.
   - Select **Internal client protection** as the protection service.

   # Click **OK**. The device performs decryption on HTTPS packets that match the proxy policy.

Figure 4 Creating a proxy policy



6. Configure IPS. For more information, see "IPS configuration examples."
7. Configure security policies:

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**, and then click **Create a policy**.

   # Configure security policy **trust-untrust** for IPS inspection on the traffic from the internal network to the external network:

   - Enter policy name **trust-untrust**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select type **IPv4**.
   - Select action **Permit**.
   - Select source IPv4 address **10.1.1.0/24**.

- Select IPS profile **ips** in the **Content security** area.
- Use the default settings for other parameters.
- Click **OK**.

Configure security policy **untrust-trust** for IPS inspection on the traffic from the external network to the internal network:

- Enter policy name **untrust-trust**.
- Select source zone **Untrust**.
- Select destination zone **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Select source IPv4 addresses **10.1.1.0/24**.
- Select IPS profile **ips** in the **Content security** area.
- Use the default settings for other parameters.
- Click **OK**.

Create security policy **trust-local** to ensure that the device can act as a proxy server to proxy the traffic from the client to the server:

- Enter policy name **trust-local**.
- Select source zones **Trust** and **Local**.
- Select destination zones **Local** and **Trust**.
- Select type **IPv4**.
- Select action **Permit**.
- Use the default settings for other parameters.
- Click **OK**.

Create security policy **untrust-local** to ensure that the device can act as a proxy client to proxy the traffic from the server to the client:

- Enter policy name **untrust-local**.
- Select source zones **Untrust** and **Local**.
- Select destination zones **Local** and **Untrust**.
- Select type **IPv4**.

- Select action **Permit**.
- Use the default settings for other parameters.
- Click **OK**.

8. Activate the configuration.

   After you complete the security policy configuration, click **Activate** to activate security policy acceleration.

Verifying the configuration

Verify that the device can perform SSL decryption on HTTPS packets, and then perform IPS inspection on the encrypted packets.

MAC address learning through a Layer 3 device configuration examples

Contents

Introduction

The following information provides configuration examples for MAC address learning through a Layer 3 device.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

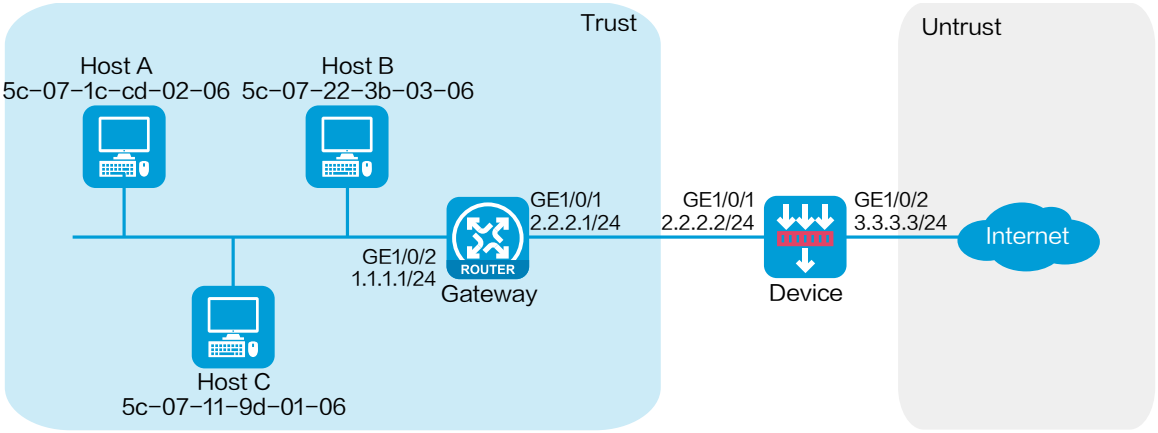
The following information is provided based on the assumption that you have basic knowledge of the feature of MAC address learning through a Layer 3 device.

Example: Configuring MAC address learning through a Layer 3 device

Network configuration

As shown in Figure 1, hosts in an internal network are connected to the device through a Layer 3 gateway and the device is connected to the Internet. Configure MAC address learning through a Layer 3 device to ensure that the device can learn the MAC addresses of the hosts. Configure security policies to allow only Host A and Host B in the internal network to access the network.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on R8560 of the NFNX3-HDB3080 device.

Procedure

Configuring the gateway

1. Assign IP addresses to interfaces and configure routing features to ensure network reachability. (Details not shown.)
2. Specify SNMPv2 and create a read-only community with the plaintext form name **public**.

Configuring the device

1. Assign IP addresses to interfaces and add the interfaces to security zones.

   # On the top navigation bar, click the **Network** tab.

   # From the navigation pane, select **Interface Configuration** > **Interfaces**.

   # Click the **Edit** icon for GE 1/0/1.

   # In the dialog box that opens, configure the interface:

   a. Select the **Trust** security zone.

   b. On the **IPv4 Address** tab, enter the IP address and mask of the interface. In this example, enter 2.2.2.2/24.

      Retain the default configuration for the remaining parameters.

   c. Click **OK**.

Add GE 1/0/2 to the **Untrust** security zone and set its IP address/mask to **3.3.3.3/24** in the same way you configure GE 1/0/1.

2. Configure routing settings.

This example configures a static route. To use dynamic routing, configure dynamic routing protocols as required.

On the top navigation bar, click **Network**.

From the navigation pane, select **Routing** > **Static Routing**.

Click **Create**.

In the dialog box that opens, configure a static route.

a. Enter destination IP address **1.1.1.0**.

b. Enter mask length **24**.

c. Enter next hop address **2.2.2.1**.

d. Retain the default setting for the other parameters.

Click **OK**.

3. Create a Layer 3 device.

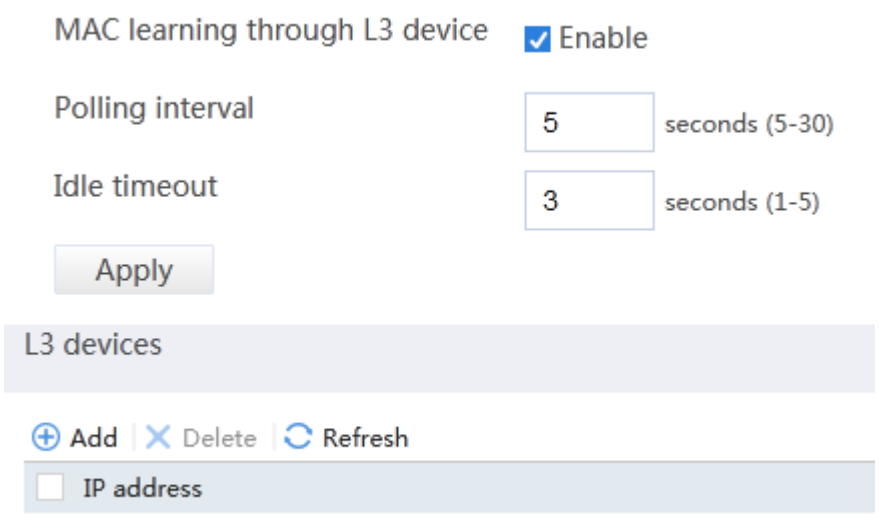
On the top navigation bar, click **System**.

From the navigation pane, select **Maintenance** > **MAC Leaning Through L3 Device** > **L3 Device Access Setting**.

Enable MAC learning through a L3 device and configure the polling interval and idle timeout for SNMP requests.

Click **Apply**.

Figure 2 Enabling MAC learning through a Layer 3 device

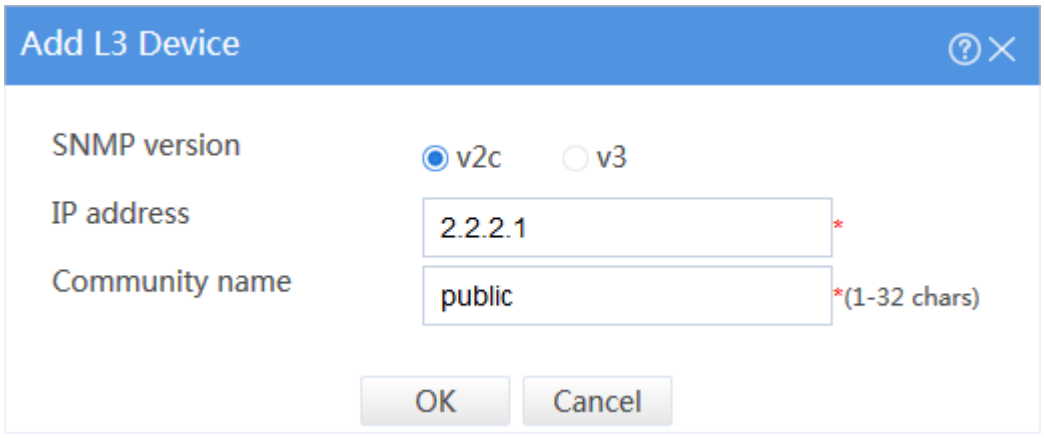


In the **L3 Devices** area, click **Add**.

In the dialogue box that opens, enter the Layer 3 device's IP address **2.2.2.1** and community name **public**.

Click **OK**.

Figure 3 Creating a Layer 3 device



4. Create a MAC address object group **groupmac** and add MAC addresses of Host A and Host B to the object group.

   # On the top navigation bar, click **Objects**.

   # From the navigation pane, select **Object Groups** > **MAC Address Object Groups**.

   # Click **Create**.

   # In the dialog box that opens, configure the MAC address object group:

   a. Enter group name **groupmac**.

   b. Click **Add**.

   c. In the dialog box that opens, select the **MAC address** type, and then enter Host A's MAC address **5c-07-1c-cd-02-06**.

   d. Click **OK**.

   e. Repeat steps b to d to add Host B's MAC address **5c-07-22-3b-03-06** to the object group.

5. Create a security policy from zone **Local** to zone **Trust** to allow the device to access the gateway.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **policy1**.
   - Select source zone **Local**.
   - Select destination zone **Trust**.
   - Select action **Permit**.
   - Select source IPv4 address **2.2.2.0/24**.

- Select destination IPv4 address **2.2.2.0/24**.

Click **OK**.

6. Create a security policy from zone **Trust** to zone **Untrust** to allow Host A and Host B to access the Internet.

   # On the top navigation bar, click **Policies**.

   # From the navigation pane, select **Security Policies** > **Security Policies**.

   # Click **Create**.

   # In the dialog box that opens, configure a security policy:

   - Enter policy name **policy2**.
   - Select source zone **Trust**.
   - Select destination zone **Untrust**.
   - Select action **Permit**.
   - Select Source IP/MAC address **groupmac**.

   # Click **OK**.

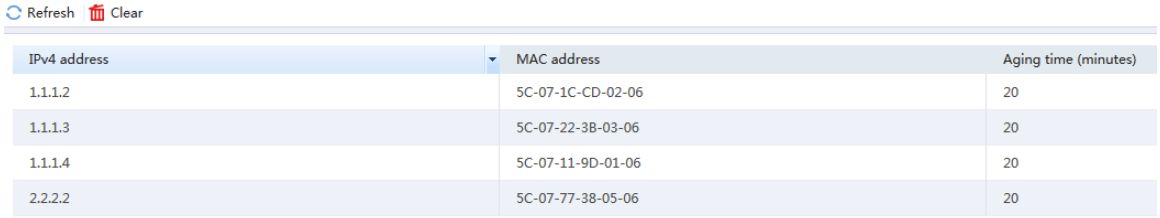
Verifying the configuration

1. View the ARP entries learned by the device.

   # On the top navigation bar, click **System**.

   # From the navigation pane, select **Maintenance** > **MAC Leaning Through L3 Device** > **Learned ARP entries**.

Figure 4 Learned ARP entries



2. Verify that Host A and Host B can access the Internet but Host C cannot.