NSFOCUS ADS
User Guide

Version: V4.5R90F01 (2018-07-31)

Contents

Figures

Tables

Preface

Scope

This document, using NSFOCUS Anti-Distributed Denial of Service System (ADS) NX5-4020 as an example, describes the features and usage of the web-based manager and console-based manager of NSFOCUS ADS NX3-2000 series (ADS NX3-2020/NX3-2020E/NX3-2010), ADS NX3-200E/600E/800E, NX5-4000 series (ADS NX5-4020/4020E), NX5-6000 series (ADS NX5-6025/6025E), NX5-8000 series (ADS NX5-8000), and NX5-10000 series (ADS NX5-10000).

This document provides guidance for you in use of the products. Descriptions in this guide may slightly differ from actual products due to version upgrade or other reasons.

Note	Unless otherwise specified, figures and texts in this manual use ADS NX5-4020 as an example.

Audience

This document is intended for the following users:

- System administrator
- Network administrator
- Users who wish to know main techniques and usage of this product

This document assumes that you have a basic knowledge of the following areas:

- Linux and Windows operating systems
- TCP/IP protocol

Organization

Chapter	Description
1 Introduction	Describes features of ADS devices.
2 Web-based Manager	Describes basic information of the web-based manager.
3 System Administration	Describes common operations and methods for system administration and maintenance.

Chapter	Description
4 Real-Time Monitoring	Describes details about real-time monitoring.
5 Policies	Describes contents and configuration methods of protection policies.
6 Diversion and Injection	Describes contents and configuration methods of diversion and injection rules.
7 Logs	Describes contents and query methods of various types of log.
8 Advanced Applications	Describes advanced functions that include packet capturing and pattern matching.
9 Operation and Maintenance	Describes how to query the protection status and perform network diagnosis.
10 Console-based Management	Describes methods for logging in and managing the console of ADS devices.
A Acronyms and Abbreviations	Describes explanation of abbreviations that appear in this article.
B Default Parameters	Describes default parameters of the ADS devices.
C IPv4/IPv6 Support	Describes ADS modules' support for IPv4 and IPv6.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
Note	Reminds users to take note.
Tip	Indicates a tip to make your operations easier.
Caution	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Customer Support

Email: support@nsfocusglobal.com

Portal: https://nsfocus.desk.com/

Contacts:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong: +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

1 Introduction

1.1 Product Overview

ADS devices provide a widely-applicable, high-performance solution to protect Internet applications from massive Distributed Denial-of-Service (DDoS) attacks. Its powerful protection capability meets high performance and scalability requirements of large-scale enterprises and operators for defending today's complex and varying network attacks.

A single ADS device can be deployed on demand to divert and clean traffic on the target device or zone without any impact on other network traffic. The multi-level protection mechanism embedded in the device enables the system to discover and block hazardous traffic while transmitting legitimate traffic as usual, so that business systems continue without disruption even in face of severe network attacks.

1.2 Typical Deployment

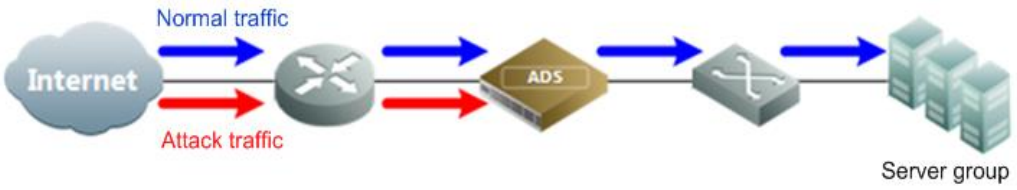
Currently, ADS devices can be deployed in in-path mode or out-of-path mode based on different network environments. The following sections detail the two modes.

Note	ADS NX3-2010/2020/2020E, NX3-200E/600E/800E, NX5-4020/4020E, and NX5-6025/6025E support both in-path and out-of-path modes, whereas ADS NX5-8000 and NX5-10000 support only the out-of-path mode.

1.2.1 In-Path Deployment

In-path deployment is suitable for enterprises' intranets that are characterized by fewer servers and smaller outgoing bandwidth. In this mode, an ADS device is transparently deployed at the network entry to detect, analyze, and block DDoS attacks. Figure 1-1 shows the deployment topology.

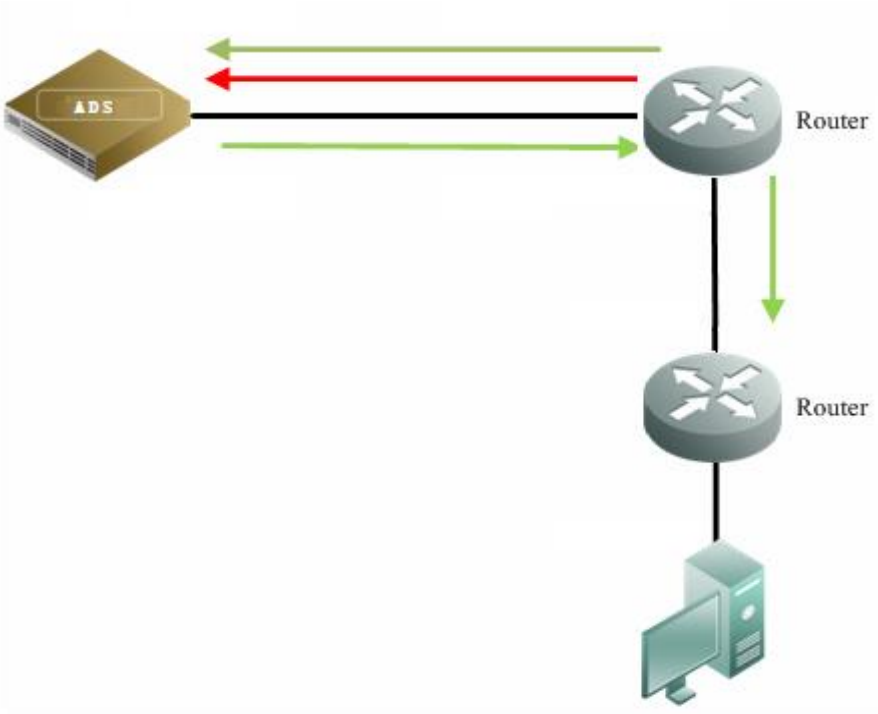
Figure 1-1 In-path deployment of an ADS device



1.2.2 Out-of-Path Deployment

To protect crucial businesses of Internet data centers (IDCs), Internet content providers (ICPs), or telecom carriers, ADS devices can be deployed in out-of-path mode, which employs the traffic diversion mechanism. In this mode, an ADS device is deployed at the network entry to collaborate with other routers, performing traffic diversion and injection on one line to protect servers on the network. Figure 1-2 shows the deployment topology.

Figure 1-2 Out-of-path deployment of an ADS device



2 Web-based Manager

The web-based manager enables you to manage and configure the ADS device in a more intuitive man-machine interaction environment.

This chapter describes basic information of the web-based manager, as shown in the following table.

Section	Description
Login	Describes methods for logging in to the system.
System User	Describes user types and permissions.
Web Page Layout	Describes the web page layout.
Common Icons and Buttons	Describes meanings of common icons and buttons.

2.1 Login

To log in to the web-based manager, perform the following steps:

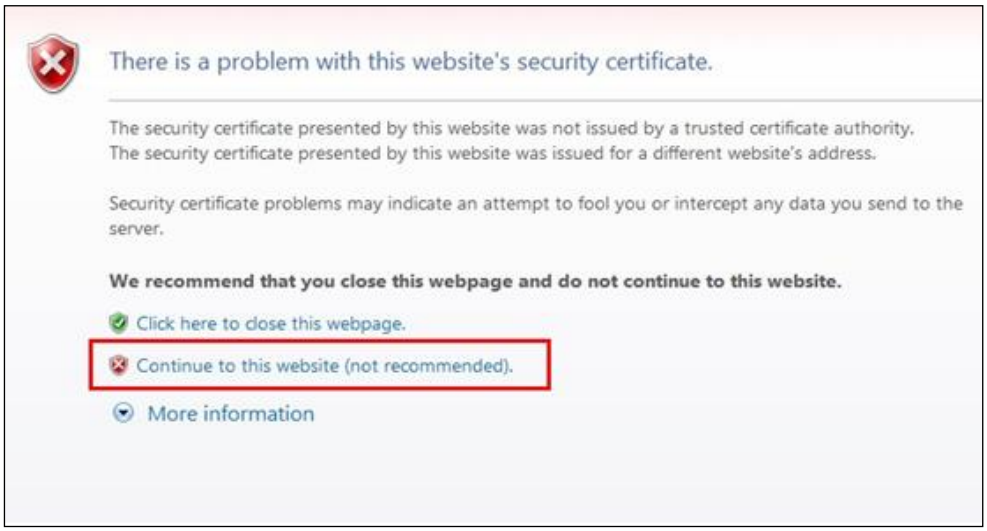
Step 1 Verify that the client host communicates properly with an ADS device (open port 443 if the traffic passes through a firewall).

Step 2 Start the IE browser and access the web-based manager's IP address by HTTPS.

As the ADS device supports both IPv4 and IPv6 protocols, you can type an IPv4 address (for example, **https://192.168.1.1**) or IPv6 address (for example, **https://[2001::107]**).

After you type the IP address and press **Enter**, the following security alert page appears.

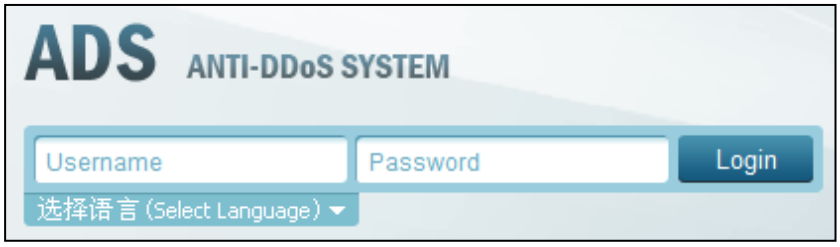
Figure 2-1 Alert page



Step 3 Click **Continue to this website (not recommended)** to accept the channel secured by the NSFOCUS ADS certificate.

The login page shown in Figure 2-2 appears.

Figure 2-2 Login page of the ADS device



Step 4 Select the language, type a correct user name and password (the initial user name is **admin** and the password is **nsfocus**), and click **Login** or press **Enter**.

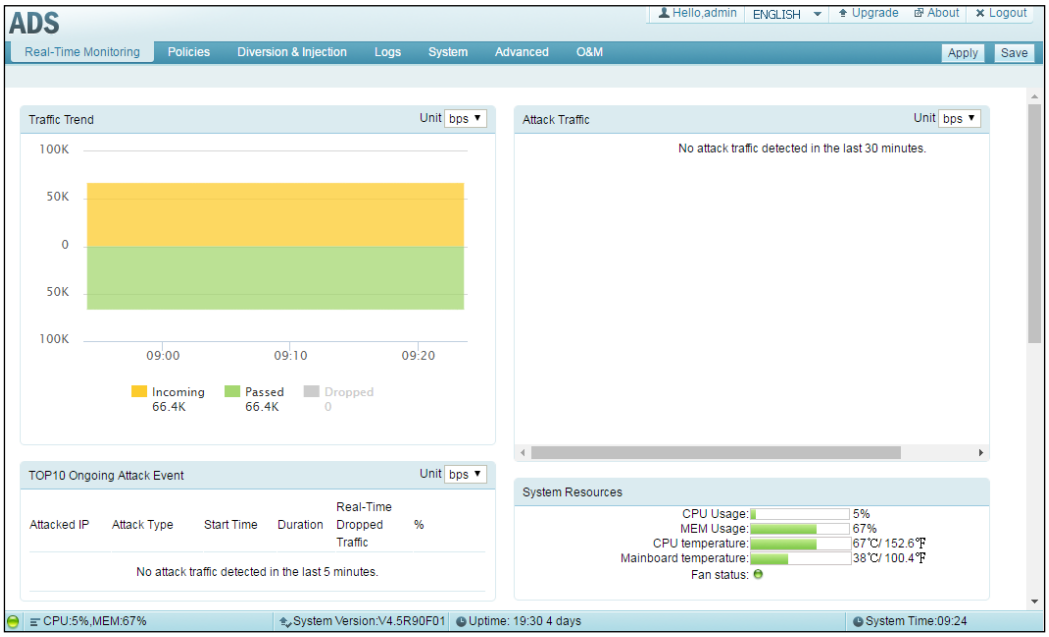
Your selection of a language from the **Select Language** drop-down list does not change the UI language of the web-based manager used by other users from different IP addresses.

Note	If you log in with the initial user name and password, the **Region and Time Settings** page and **Change Initial Password** page will appear successively. You should change the region, system time zone, system time, as well as the initial password before logging in to the device. For details, see the NSFOCUS ADS Installation Guide.

A license must be imported after initial login to the system. After a valid license is successfully imported, log in to NSFOCUS ADS again.

The following window appears, indicating that you have successfully logged in.

Figure 2-3 Window displayed after successful login



Note	Note the following during login: • You are advised to use an IE browser of 8.0 through 10.0 or a Chrome browser with a resolution of 1024x768 or higher. If you use the IE-based tabbed browsers (such as MyIE and Maxthon) or browsers that are not based on the IE core (such as Opera), pages may be displayed improperly. • Before login, check whether the option of blocking pop-ups is selected in the browser. If yes, deselect it. • The browser you use must support JavaScript, cookies, and frames. • Possible causes for login failures: incorrect user name, incorrect password, and upper/lower case confusion. • You must import the license after the first login. For details, see section 3.4.1 License. • The system will return to the login page if you remain inactive for a period specified by **Auto Idle Logout**. In this case, you need to log in again to continue using the system. For details, see section 3.2.1 Login Security Settings.

----End

2.2 System User

User roles of the ADS devices include superuser (**admin** by default), CLI user (**routerman** by default), custom user, common user, administrator, and audit user. Table 2-1 lists permissions of these users.

Table 2-1 User permissions

User Role	Configuration Permission	Viewing Permission
Superuser	Default system user **admin**, who has all permissions for the web-based manager. This role cannot be created or deleted.	
CLI user	Has permissions for login to the console and management of the system.	
Custom user	Has permissions for traffic diversion and injection (manual mode), packet capture, NSFOCUS Threat Intelligence (NTI), and system management (modification of his or her own account information).	Has permissions for real-time monitoring, traffic diversion and injection, logs (detailed information and statistical graphs of the attack log, and the traffic diversion log), system management (basic system configuration and interface configuration), statistical graphs of attack traffic, and BGP neighbor status.
Common user	Has permissions for system management (modification of his or her own account information).	Has permissions for real-time monitoring and system management (basic system settings and interface settings).
Administrator	Has permissions for protection policies, traffic diversion and injection, and logs (detailed information and statistical graphs of the attack log, statistical graphs of attack traffic, and the traffic diversion log), and system management (basic configuration, interface configuration, and modification of his or her own account information).	Has permissions for real-time monitoring information, protection policies, diversion and injection, logs (detailed information and statistical graphs of the attack log, statistical graphs of attack traffic, and the traffic diversion log), and system management information (basic system settings and interface settings).
Audit user	Has permissions for system management (modification of his or her own account information).	Has permissions for real-time monitoring, the login log, and the operation log.

Note	You are advised to change the initial password immediately after login with the default user account. For details on initial passwords, see appendix B Default Parameters.

2.3 Web Page Layout

After a successful login, the user **admin** opens the homepage. Figure 2-4 shows the web page layout.

Users with different permissions may view different information under the main menu, sub-menus, and work area of the system, but can view the same information and have the same permissions for the status bar and shortcut operation area.

Figure 2-4 Web page layout

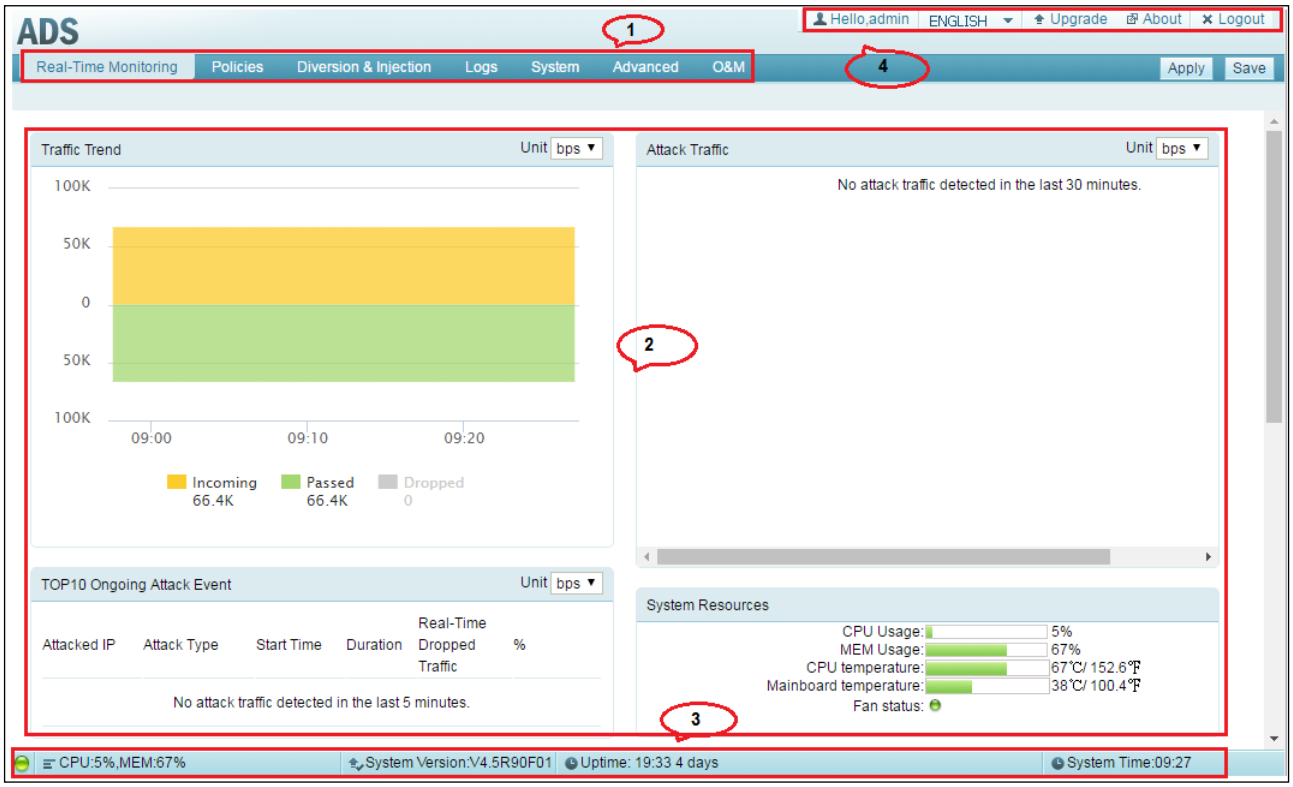


Table 2-2 describes the web page layout.

Table 2-2 Web page layout

SN	Area	Description
1	Menu bar	Main menus of the system.
2	Work area	Area where you can perform configurations and operations and view data.
3	Status bar	Displaying current device information, software version and system time. For details, see section 4.2 System Information.
4	Quick access bar	Providing frequently used buttons for quick access to the corresponding module. See Table 2-3 for details.

Table 2-3 explains buttons in the quick access bar.

Table 2-3 Common buttons

Button	Function
ENGLISH	Switches to another language.
Upgrade	Switches to the system upgrade window.

Button	Function
About	Displays information about the current ADS device.
Logout	Logs you out of the system.
Connect to NSFOCUS Cloud	Allows you to download NSFOCUS mobile software. After ADS connects to the cloud, you can monitor the ADS status via a mobile phone. This function is available only when **Region** is set to **Chinese mainland** in the **Region and Time Settings** dialog box.

Note	For the sake of account security, you are advised to click Logout when exiting the system.

2.4 Common Icons and Buttons

Table 2-4 describes functions of common icons and buttons on the web-based manager.

Table 2-4 Buttons and icons

Button	Function
	Edits an item.
	Deletes an item.
	Starts an operation.
	Stops an ongoing operation.
Apply	Makes the configuration in the acitive work area take effect immediately.
Save	Saves the current configuration and writes it to the firmware.
	Views the current configuration.

3 System Administration

This chapter dwells upon common ways to manage ADS devices, containing the following sections:

Section	Description
Local Settings	Describes how to configure basic system information, interfaces, and users.
Security Configuration	Describes how to configure login security settings and unlock a locked IP address.
Log Services	Describes how to configure system log services and export logs via SFTP/SSH.
Others	Describes how to update the system, manage the license, enable remote assistance, and view version information.

3.1 Local Settings

This section covers the following topics:

- Basic Information
- Interface Configuration
- User Management
- Management Mode Configuration
- Configuration File Management
- Bandwidth Overrun Limit Configuration
- Hardware Alert Thresholds
- Management Interface Access Control
- HA Configuration
- (Optional) Bypass Configuration
- Collaboration Configuration

3.1.1 Basic Information

ADS supports the IPv4/IPv6 dual-stack, that is, it supports both IPv4 and IPv6 protocols. As a dual-stack node, ADS can be configured with IPv4 and IPv6 addresses, which are respectively used for communication with IPv4 nodes and IPv6 nodes.

Note	Dual stack is an effective technology for IPv4-to-IPv6 transition. Powered by this technology, network nodes support both IPv4 and IPv6 stacks. The source node selects the same protocol stack as the one used by the destination node for communication and the network device selects the same protocol stack as the one used by packets when processing and forwarding packets.

You can view and modify basic information of the current ADS such as device ID, IPv4 address, IPv6 address, netmask, and gateway address.

Choose **System** > **Local Settings** > **Basic Settings**. The **Basic Settings** page appears, as shown in Figure 3-1.

Figure 3-1 Basic Settings page

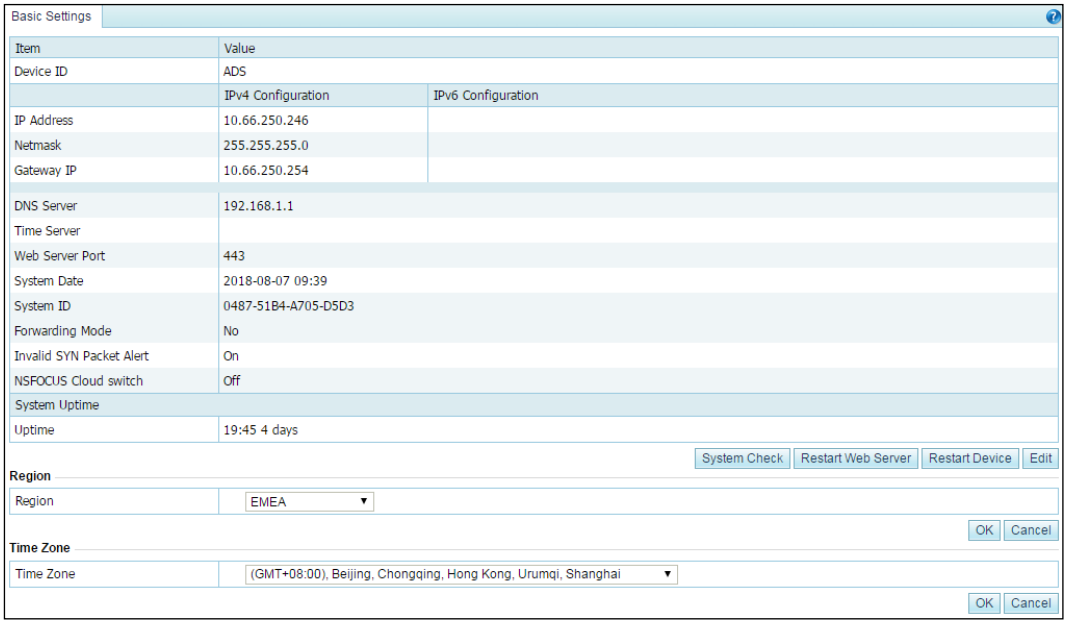


Table 3-1 Basic system settings

Parameter	Description
Device ID	Device model. It cannot exceed 26 characters.
IP Address/Netmask	IPv4 address/netmask or IPv6 address/prefix length of the management interface of ADS. Note • ADS supports the IPv4/IPv6 dual-stack. Therefore, you can configure the IPv4 or IPv6 address for the management interface according to the actual network deployment. • The device administrator can use this IP address to exercise remote device management via HTTPS, perform log-related operations, and send emails.
Gateway IP	IPv4/v6 address of the gateway for the management interface.

Parameter	Description
DNS Server	IP address of the DNS server used by the management interface of the current ADS device.
Time Server	IP address or domain name of a server that synchronizes time on the current ADS and other NSFOCUS devices. After this is specified, all connected NSFOCUS devices will synchronize the time with the time server automatically. Note If you type a domain name here, you must configure the DNS server. If you do not want to specify the DNS server, you must type an IP address for the time server.
Web Server Port	Web server port used for accessing the web-based manager of ADS.
System Date	System time. By default, the current system time is displayed.
System ID	Unique ID of ADS. It is used for applying for the device license.
Forwarding Mode	This mode is used for network troubleshooting. The value **Yes** indicates that the current ADS directly forwards packets without any check.
Invalid SYN Packet Alert	• After **Invalid SYN Packet Alert** is set to **On**, when detecting a SYN packet smaller than 64 bytes, ADS logs a SYN_INVALID event, generates a sound alert, and drops the illegitimate packet. • After **Invalid SYN Packet Alert** is set to **Off**, when detecting a SYN packet smaller than 64 bytes, ADS does not log SYN_INVALID attacks or generate a sound alert, but drops illegitimate packets.
NSFOCUS Cloud Switch	Controls whether to turn on the NSFOCUS cloud service. • **On**: indicates that the cloud service is enabled. The **Connect to NSFOCUS Cloud** link is displayed in the upper-right corner of the web-based manager. • **Off**: indicates that the cloud service is disabled.
Uptime	Length of time during which the current ADS operates properly.

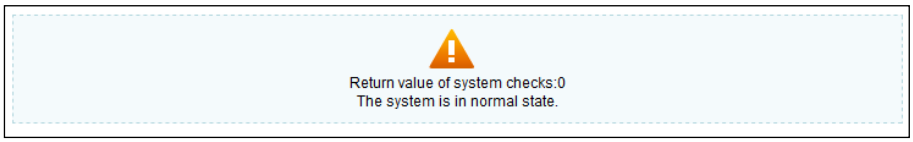
On the **Basic Settings** page shown in Figure 3-1, you can perform the following operations:

- Edit basic system information.

  Click **Edit** to open the **Modify basic settings** page. Modify parameter settings and click **OK** to commit the changes.
- Check the system status.

  Click **System Check** to check whether the system operates properly. Then the system returns check results, as shown in Figure 3-2.

Figure 3-2 System check results



A few seconds later, the system returns to the **Basic Settings** page.

- Change the web server port.

a. Click **Edit** to open the **Modify basic settings** page and modify the web server port.

It can be 443 (default) or an integer ranging from 18000 to 20000. A conflicting port may make the web service inaccessible. If **Web Server Port** is set to another number than 443, management by a third-party device or ADS M may be affected.

For example, change **Web Server Port** to **18000**. Then the accessible address of ADS is changed to https://*.*.*.*:18000.

b. Configure parameters and click **OK** to return to the **Basic Settings** page.

c. Click **Restart Web Server** on the page shown in Figure 3-1.

- Restart the device remotely.

Click **Restart Device** to restart the current ADS remotely.

- Configure the region where ADS is located.

The **Region** area shows the current geographic region of ADS. Select a region from the **Region** drop-down box and click **OK**.

To make the region setting take effect, you must restart the system.

Note	When **Region** is set to **Chinese mainland**: • By default, the threat intelligence sharing switch is turned on and the China-based server is used. • The NSFOCUS Cloud switch is turned on by default. When **Region** is set to any other areas than **Chinese mainland**: • By default, the threat intelligence sharing switch is turned off. When the switch is turned on, the international server is used. • The NSFOCUS Cloud switch is turned off by default.

- Configure the time zone.

The **Time Zone** area shows the current time zone information of ADS. You can select a time zone from the drop-down list and click **OK** to save the setting.

After the configuration, you need to restart the system to make the new time zone take effect.

3.1.2 Interface Configuration

The number and type of interfaces vary with ADS models.

- ADS NX3-2010/2020/2020E, NX5-4020/4020E, and NX5-6025/6025E support the following types of interface cards:
  - 8 x 1000M electrical port

  - 8 x 1000M optical port
  - 4 x 1000M electrical port
  - 4 x 1000M optical port
  - 2 x 10G optical port
- ADS NX5-8000 supports the following types of interface cards:
  - 8 x 1000M electrical port
  - 8 x 1000M optical port
  - 2 x 10G optical port
- ADS NX3-200E/600E/800E supports only interface cards of 6 x 1000M electrical port.
- ADS NX5-10000 supports the following types of interface cards:
  - 4 x 1000M electrical port
  - 20 x 10G optical port
  - 6 x 100G optical port
  - 4 x 40G optical port

On the interface configuration page, the administrator can enable or disable all working interfaces and change the working mode of 1000M electrical ports.

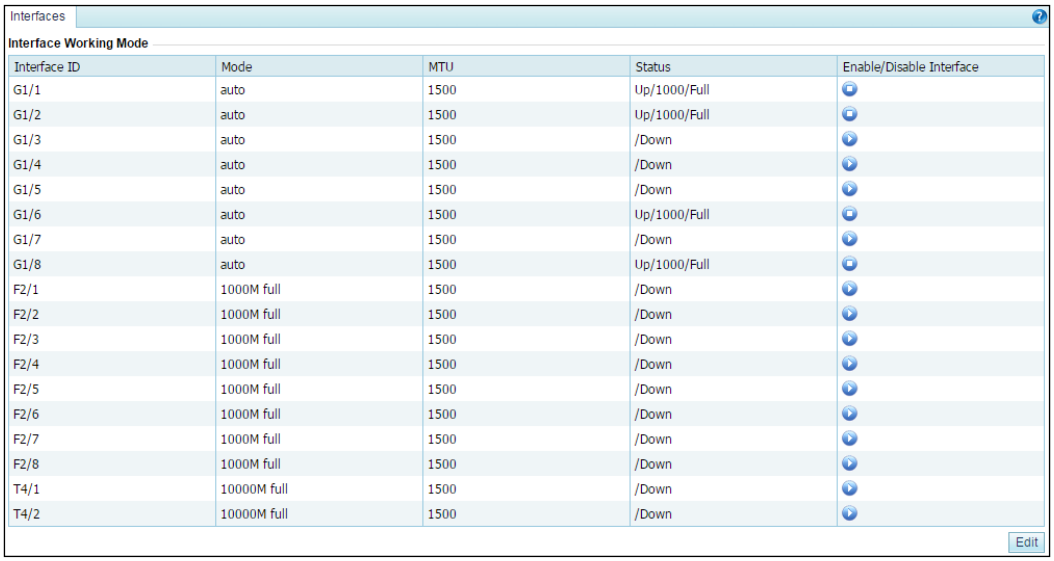
This section describes those operations in detail.

Enabling or Disabling Working Interfaces

Step 1 Choose **System** > **Local Settings** > **Interfaces**.

Figure 3-3 shows the interface working mode of ADS NX5-4020.

Figure 3-3 Interface working mode of ADS NX5-4020



Interfaces

Interface Working Mode

Interface ID	Mode	MTU	Status	Enable/Disable Interface
G1/1	auto	1500	Up/1000/Full	
G1/2	auto	1500	Up/1000/Full	
G1/3	auto	1500	/Down	
G1/4	auto	1500	/Down	
G1/5	auto	1500	/Down	
G1/6	auto	1500	Up/1000/Full	
G1/7	auto	1500	/Down	
G1/8	auto	1500	Up/1000/Full	
F2/1	1000M full	1500	/Down	
F2/2	1000M full	1500	/Down	
F2/3	1000M full	1500	/Down	
F2/4	1000M full	1500	/Down	
F2/5	1000M full	1500	/Down	
F2/6	1000M full	1500	/Down	
F2/7	1000M full	1500	/Down	
F2/8	1000M full	1500	/Down	
T4/1	10000M full	1500	/Down	
T4/2	10000M full	1500	/Down	

Edit

Table 3-2 describes interface working mode parameters.

Table 3-2 Interface working mode parameters

Parameter	Description
Interface ID	ADS NX3-2010/2020/2020E, NX3-200E/600E/800E, NX5-4020/4020E, and NX5-6025/6025E: • T4/1 and T4/2: 10G optical ports • G1/1–G1/8:1000M electrical ports • F2/1–F2/8: 1000M optical ports ADS NX5-8000: • T4/1 and T4/2: 10G optical ports • G1/1–G1/8:1000M electrical ports • F2/1–F2/8: 1000M optical ports ADS NX5-10000: • 100GE 1/1–100GE 1/6: 100G optical ports • 40GE 1/1–40GE 1/4: 40G optical ports • T1/1–T1/20: 10G optical ports • G1/1–G1/4: 1000M electrical ports Note Interface numbers here are provided for illustration only. They may differ from the actual numbers as boards may be inserted into other slots.
Mode	The default value is **auto**, indicating that the interface is working in auto negotiation mode. • **10M full**: indicates that the interface is currently operating at 10 Mbps and in full duplex mode. • **10M half**: indicates that the interface is currently operating at 10 Mbps and in half duplex mode. • **100M full**: indicates the interface is currently operating at 100 Mbps and in full duplex mode. • **100M half**: indicates the interface is currently operating at 100 Mbps and in half duplex mode. • **1000M full**: indicates the interface is currently operating at 1000 Mbps and in full duplex mode.
MTU	The MTU is **1500** for all working interfaces and cannot be edited.
Status	• **Up**: indicates that the current interface is up. • **Down**: indicates the current interface is down. • **1000/Full** indicates the working mode of the current interface.

Step 2 To enable or disable an interface, click or in the **Enable/Disable Interface** column.

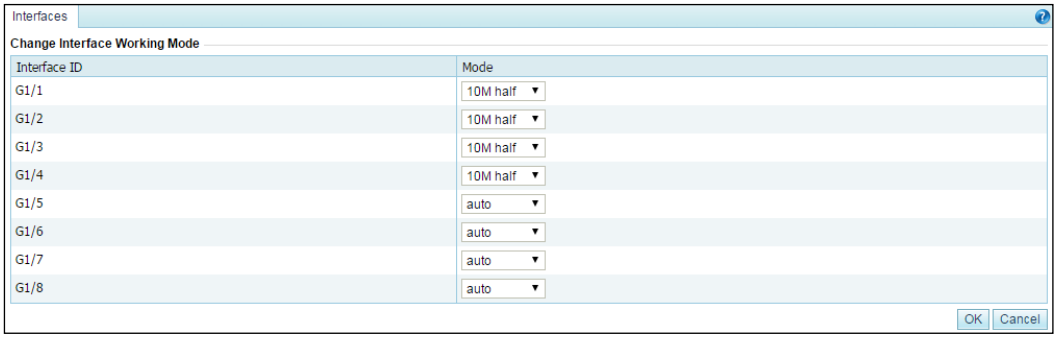
----End

Changing the Working Mode of 1000M Electrical Ports

ADS NX5-4020 is used as an example here.

On the **Interface** page in Figure 3-3, click **Edit** to change the working mode of 1000M electrical ports (G1/1 through G1/8).

Figure 3-4 Changing the working mode of 1000M electrical ports

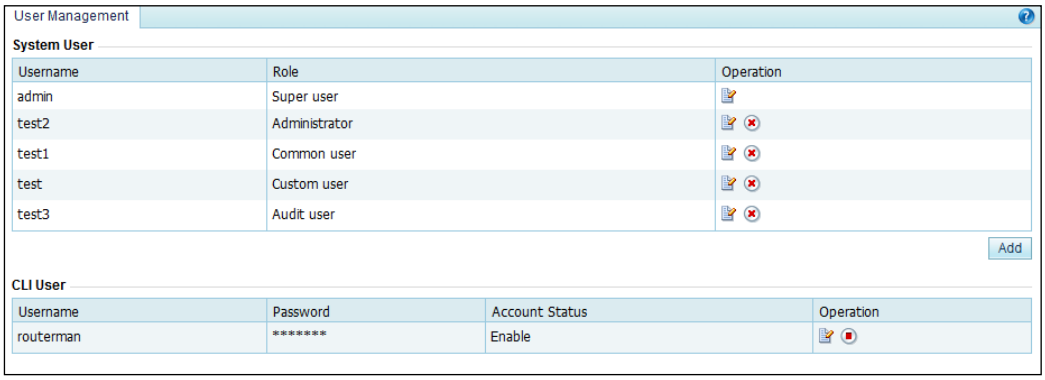


After changing the working mode, click **OK** to save the settings.

3.1.3 User Management

As shown in Figure 3-5, the **User Management** page displays all system users. Initially, only the default web user **admin** and the CLI user **routerman** are available.

Figure 3-5 System users



User roles include the following:

- Superuser (**admin** by default)
- CLI user (**routerman** by default)
- Custom user
- Common user
- Administrator
- Audit user

For permissions of these user roles, see Table 2-1.

Adding a User

Click **Add** in the **System User** area to add a system user. On the page shown in Figure 3-6, configure the user name and login password, and select a role to limit the user's permissions.

Figure 3-6 Adding a system user

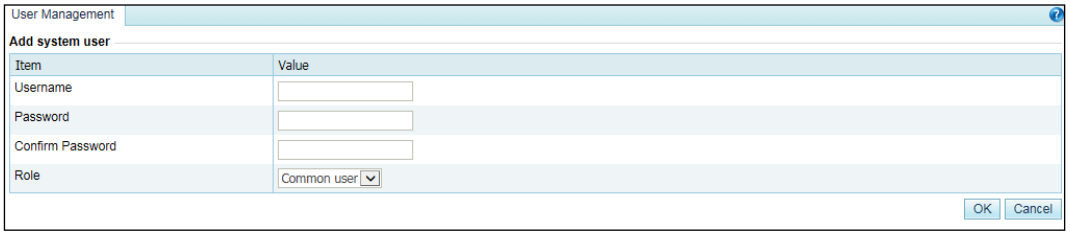


Table 3-3 describes parameters for adding a user

Parameter	Description
Username	Specifies the user name of the new account, which is 4 to 20 characters long. The minimum user name length is determined by the **Min User Name Length** value specified under **System** > **Security Configuration** > **Login Security Settings**. Also, the user name can only consist of letters, digits, and underscores.
Password	Specifies the password of the new account, which should contain 6 to 30 characters and whose minimum length depends on the **Min Length** value specified for **Password Strength Check** under **System** > **Security Configuration** > **Login Security Settings**.
Confirm Password	Specifies a repeat entry of the password for accuracy.
Role	Specifies the role of the new account, which can be **Custom user**, **Common user**, **Administrator**, and **Audit user**. For details about permissions of each user role, see Table 2-1.

Editing a User

Click in the **Operation** column of a user to edit the user's account information.

Note

- You cannot delete the superuser (**admin**) or edit its permissions.
- Only **admin** can edit user accounts and other users can only change their own passwords.

Deleting a User

Click in the **Operation** column of a user to delete this user.

Only **admin** can delete users.

Enabling a CLI User

Only **admin** can enable or disable CLI users.

By default, CLI users are disabled. In the CLI user list, click in the **Operation** column to enable a CLI user. For first enabling, the web page redirects you to the password page, as shown in Figure 3-7.

The password must be 6 to 20 characters long. The CLI user name is set by the system and cannot be edited. After the password is configured, you will not be prompted to set it if you enable it again.

Figure 3-7 Configuring the password of a CLI user

Item	Value
Username	routerman
New Password	
Confirm Password	

Editing a CLI User

Click in the **Operation** column of a CLI user to change the user's password.

Figure 3-8 Changing the password of a CLI user

User Management

Modify CLI User

Item	Value
Username	routerman
New Password	
Confirm Password	

OK Cancel

3.1.4 Management Mode Configuration

This section describes how to configure the management mode and HTTP authentication synchronization.

3.1.4.1 Configuring the Management Mode

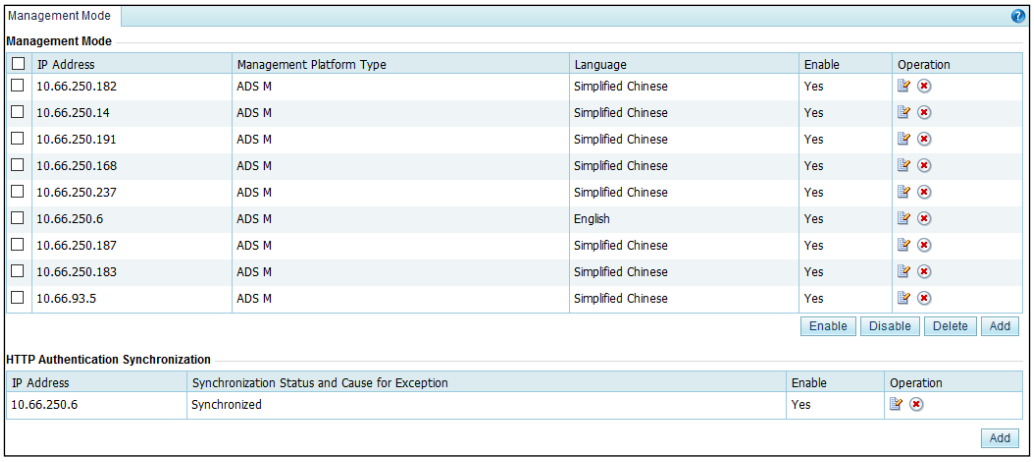
Currently, the administrator can exercise centralized management and monitoring over ADS in the following ways (third-party management and ADS M management cannot be enabled simultaneously):

- Third-party management: allows the administrator to use a third-party program to manage ADS.
- ESPC/ESPP management: allows the ADS daemon to upload files to ESPC or ESPP.
- ADS M management: allows the ADS daemon to upload files to ADS M and ADS M to dispatch configuration to ADS. After this is selected, users can conduct centralized management and maintenance of ADS devices via ADS M.

To enable and configure the management mode, perform the following steps:

Step 1 Choose **System** > **Local Settings** > **Management Mode**.

Figure 3-9 Management Mode page



Step 2 Click **Add** in the lower- right corner of the **Management Mode** area to open the **Add Mgmt Mode Config** page.

Figure 3-10 Add Mgmt Mode Config page

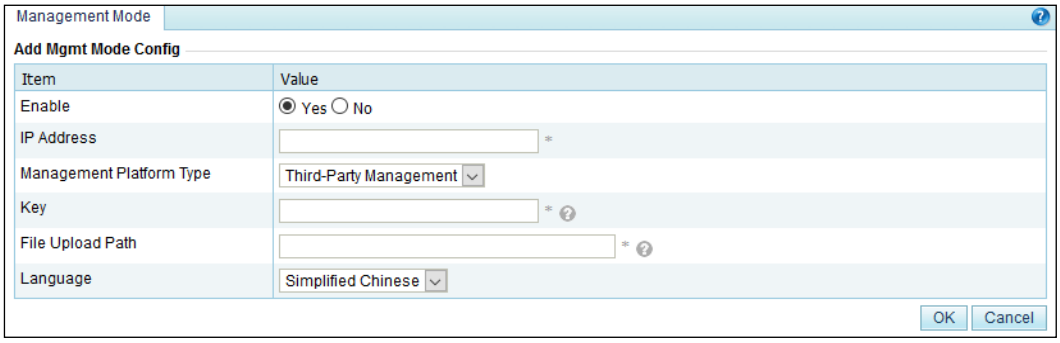


Table 3-4 describes management mode parameters.

Table 3-4 Management mode parameters

Parameter	Description
Accept Management	Controls whether ADS accepts centralized management.

Parameter	Description
	• **Yes**: indicates that ADS is subject to centralized management. • **No**: indicates that ADS is not subject to centralized management.
IP Address	IP address of ADS M or the third-party device to which ADS submits data. You can type either an IPv4 or IPv6 address. This is required when **ADS M** or **Third-Party Management** is selected as the management platform. Note Currently, ADS can submit data to five management devices simultaneously.
Domain Name/IP Address	Domain name or IP address of ESPC/ESPP to which ADS submits data. You can type either an IPv4 or IPv6 address. This is required when **ESPC/ESPP** is selected as the management platform.
Management Platform Type	Type of the device to which ADS submits data. The value can be one of the following: • **ADS M** • **ESPC/ESPP** • **Third-Party Management**: third-party device
Key	Specifies the key used for configuring the web API. This parameter is available only when **Third-Party Management** is selected as the management platform. The key must be a combination of 6 to 15 uppercase letters, lowercase letters, and digits.
File Upload Path	Specifies an interface from which files are uploaded to a third-party management platform. Such a file upload path, for example, https://192.168.0.1:31943/devicelog, consists of an IP address, port number, and URI. If ADS is accessed via port 443, the port number can be omitted here.
Language	Specifies the language of messages sent by ADS to ADS M. Generally, after you configure protection policies on ADS M for ADS, ADS returns related messages.

Step 3 Configure parameters and click **OK** to save the settings.

Step 4 Select the newly added management mode and click **Enable** to enable the management mode.

----End

3.1.4.2 Configuring HTTP Authentication Synchronization

Step 1 Choose **System** > **Local Settings** > **Management Mode** to open the management mode page shown in Figure 3-9.

In the **HTTP Authentication Synchronization** area, the **Synchronization Status and Cause for Exception** column shows the current synchronization status and the **Enable** column shows whether HTTP authentication synchronization is enabled.

Step 2 Click **Add** in the lower- right corner of the **HTTP Authentication Synchronization** area.

Figure 3-11 Configuring HTTP authentication synchronization

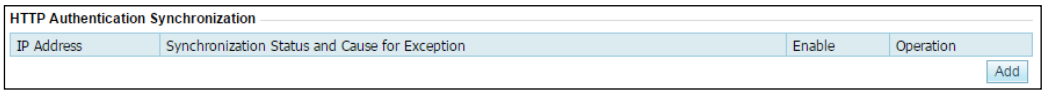


Table 3-5 describes parameters for configuring HTTP authentication synchronization.

Table 3-5 Parameters for configuring HTTP authentication synchronization

Parameter	Description
Enable	Controls whether to enable the HTTP authentication synchronization function. • **Yes**: enables this function. • **No**: disables this function.
IP Address	Specifies the IP address to which HTTP authentication information is synchronized. Both IPv4 and IPv6 addresses are allowed here. **Note** Only one IP address is allowed each time.

Step 3 Configure parameters and click **OK** to complete the configuration.

----End

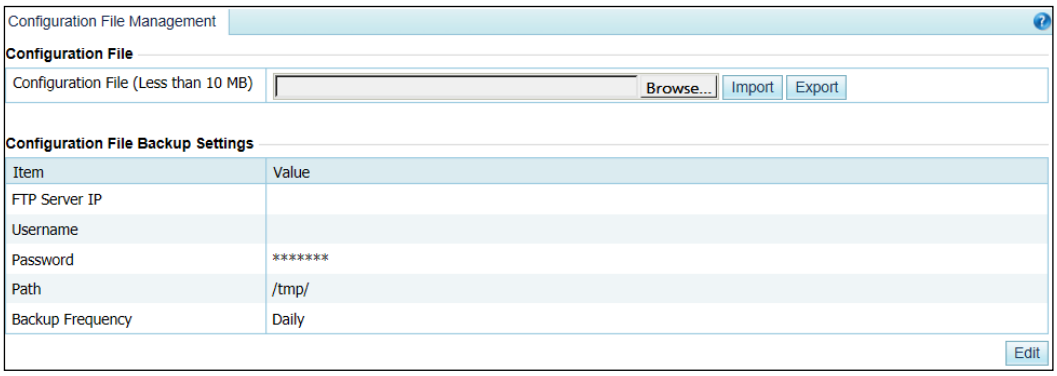
3.1.5 Configuration File Management

The configuration file contains all the configured policies and system settings of the system. The configuration file is an encrypted file with the extension **.conf**.

Exporting a Configuration File

On the **Configuration File Management** page shown in Figure 3-12, click **Export** to export a configuration file with the default file name **collapsar.conf**.

Figure 3-12 Configuration file management



Note	You are advised not to change the name of the exported configuration file, **collapsar.conf**.

Importing a Configuration File

On the page shown in Figure 3-12, click **Browse** and select a configuration file from the local host. Then click **Import** to import the configuration information and restore the system back to the state right before the configuration file was exported.

Pay attention to the following while importing or exporting a configuration file:

- The size of the configuration file should be no greater than 1 MB; otherwise, the import would fail.
- Configuration files cannot be imported across product models.
- Configuration files cannot be imported between devices running in different modes even if they are of the same model.

Backing Up a Configuration File

You can regularly back up configuration files to the FTP server. On the page shown in Figure 3-12, click **Edit** and set configuration file backup parameters.

Figure 3-13 Configuration file backup

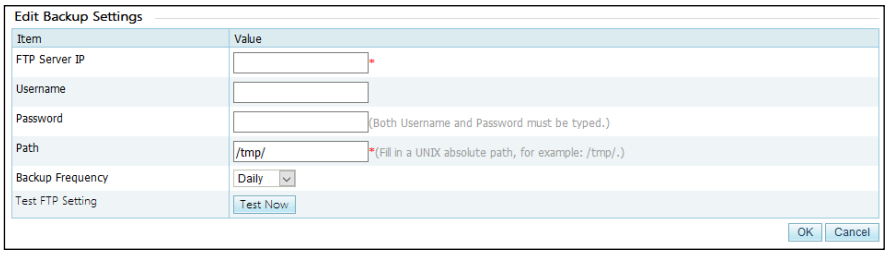


Table 3-6 describes configuration file backup parameters.

Table 3-6 Configuration file backup parameters

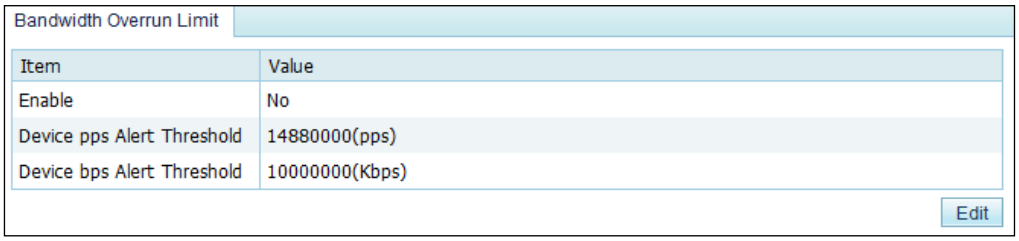
Parameter	Description
FTP Server IP	IP address of the FTP server.
Username	User name for logging in to the remote FTP server.
Password	Password for logging in to the remote FTP server.
Path	Path to save the data uploaded to the remote FTP server.
Backup Frequency	Specifies how often the configuration file is backed up, which can be **Daily**, **Weekly**, or **Monthly**.

3.1.6 Bandwidth Overrun Limit Configuration

After two bandwidth overrun thresholds are configured, if the total traffic on ADS exceeds either of them, the system reports an alert, which is displayed in red, prompting bandwidth overrun. Also, the system logs system operation messages when the alert is generated and ends.

Step 1 Choose **System** > **Local Settings** > **Bandwidth Overrun Limit**.

Figure 3-14 Bandwidth Overrun Limit page



Step 2 Click **Edit**.

Figure 3-15 Editing bandwidth overrun thresholds

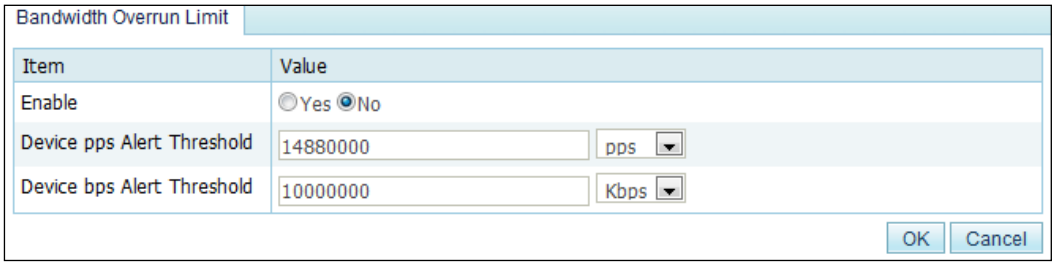


Table 3-7 describes bandwidth overrun thresholds.

Table 3-7 Bandwidth overflow thresholds

Parameter	Description
Enable	Controls whether to enable the bandwidth overrun alerting. • **Yes**: enables the function. • **No**: disables the function.
Device pps Alert Threshold	Alert triggering threshold for overall traffic in pps. A bandwidth overrun alert is generated when this threshold is exceeded.
Device bps Alert Threshold	Alert triggering threshold for overall traffic in bps. A bandwidth overrun alert is generated when this threshold is exceeded.

Step 3 Set parameters and click **OK** to complete the configuration.

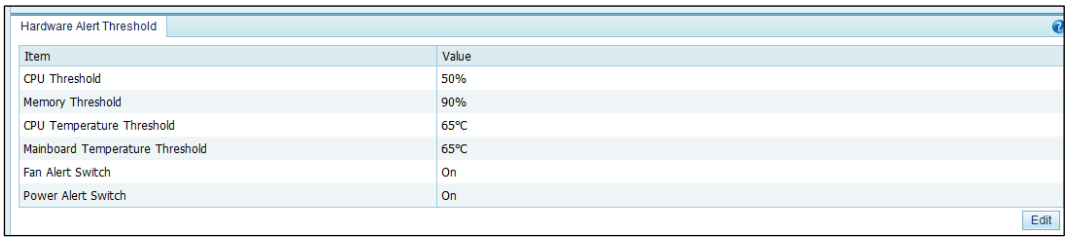
----End

3.1.7 Hardware Alert Thresholds

You can set alert thresholds for various types of hardware by performing the following steps:

Step 1 Choose **System** > **Local Settings** > **Hardware Alert Threshold**.

Figure 3-16 Hardware Alert Threshold page



Step 2 Click **Edit**.

Figure 3-17 Editing hardware alert thresholds

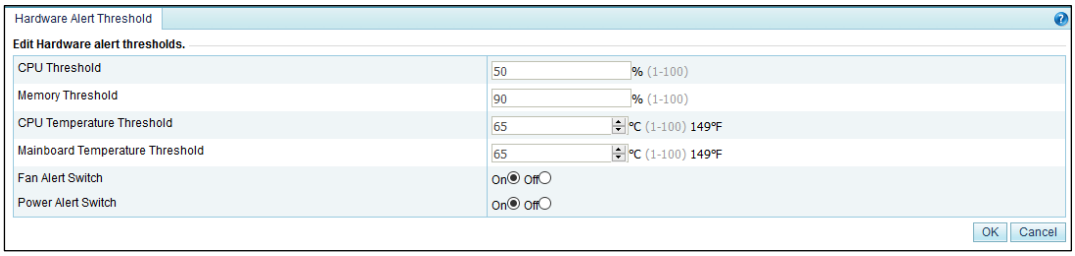


Table 3-8 describes hardware alert thresholds.

Table 3-8 Hardware alert thresholds

Parameter	Description
CPU Threshold	Specifies the percentage of CPU usage that will trigger an alert.
Memory Threshold	Specifies the percentage of memory usage that will trigger an alert.
CPU Temperature Threshold	Specifies the temperature of the CPU that will trigger an alert.
Mainboard Temperature Threshold	Specifies the temperature of the mainboard that will trigger an alert.
Fan Alert Switch	Controls whether to turn the fan switch on. If it is turned on, an alert will be triggered when a fan fails.
Power Alert Switch	Controls whether to turn the power switch on. If it is turned on, an alert will be triggered when the power supply fails. **Note** This parameter is available only for some ADS NX5-8000 devices.

Step 3 Set parameters and click **OK** to complete the configuration.

----End

3.1.8 Management Interface Access Control

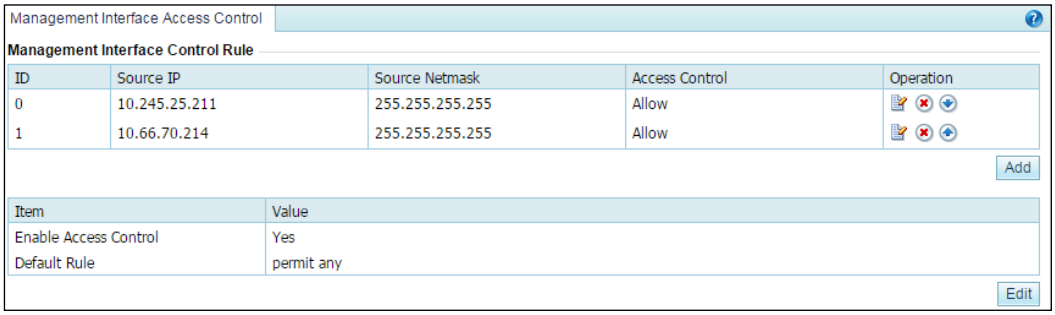
The management interface access control is disabled by default. After being enabled, it can be disabled via the console. After source IP addresses/segments are specified for access to the management interface, those beyond the specified range cannot access ADS, whether via web, Telnet, or ping. In addition, the system can dynamically identify external IP addresses to which ADS connects, such as NSFOCUS Cloud or other collaborative platforms, and allow access from these IP addresses.

3.1.8.1 Creating a Management Interface Access Control Rule

To create a management interface access control rule, perform the following steps:

Step 1 Choose **System** > **Local Settings** > **Management Interface Access Control**.

Figure 3-18 Management Interface Access Control page



Step 2 Click **Add**.

Figure 3-19 Creating a management interface access control rule

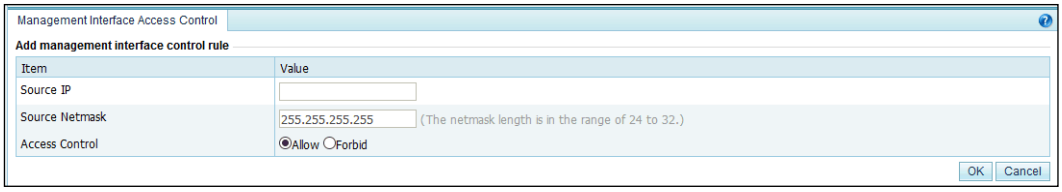


Table 3-9 describes parameters for creating a management interface access control rule.

Table 3-9 Parameters for creating a management interface access control rule

Parameter	Description
Source IP	Specifies a source IP address/segment that is allowed or forbidden to access ADS. Only IPv4 is supported.
Source Netmask	Specifies the subnet mask of the source IP address/segment.
Access Control	Specifies an action to be taken by ADS for traffic from the specified IP

Parameter	Description
	address/segment: • **Allow**: allows the specified IP address/segment to access ADS. • **Forbid**: forbids the specified IP address/segment to access ADS.

Step 3 Set parameters and click **OK**.

A new management interface access control rule is thus created.

Step 4 Click **Edit**.

Figure 3-20 Editing management interface access control

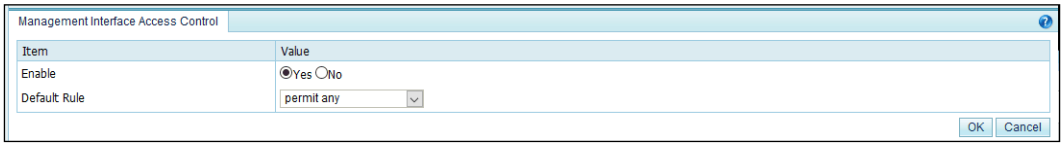


Table 3-10 describes parameters for controlling the management interface access control function.

Table 3-10 Parameters for controlling the management interface access control function

Parameter	Description
Enable	Controls whether to enable the management interface access control function. • **Yes**: enables the function. • **No**: disables the function.
Default Rule	Specifies a default rule. • **permit any**: allows any IP addresses other than those denied access in management interface access control rules to access ADS. • **forbid all**: forbids any IP addresses other than those allowed access in management interface access control rules to access ADS. After this option is selected, only IP addresses allowed access in management interface access control rules can access ADS.

Step 5 Set parameters and click **OK** to complete the configuration.

----End

3.1.8.2 Changing the Rule Match Sequence

When there is more than one management interface access control rule, the rule on top is matched first and, if it is a hit, no other rules will be checked for a match. You can adjust the sequence of rules to change their priority.

On the page shown in Figure 3-18, click or in the **Operation** column of a rule to move it up or down.

3.1.8.3 Editing a Management Interface Access Control Rule

You can edit parameter settings of a management interface access control rule after it is configured. To do that, perform the following steps:

Step 1 On the page shown in Figure 3-18, click in the **Operation** column of a rule.

Step 2 Edit parameter settings and then click **OK** to save the changes and return to the rule list page.

----End

3.1.8.4 Deleting a Management Interface Access Control Rule

On the page shown in Figure 3-18, click in the **Operation** column of a rule and click **OK** in the confirmation dialog box to delete this rule.

3.1.9 HA Configuration

Note	ADS NX5-10000 does not support HA configuration.

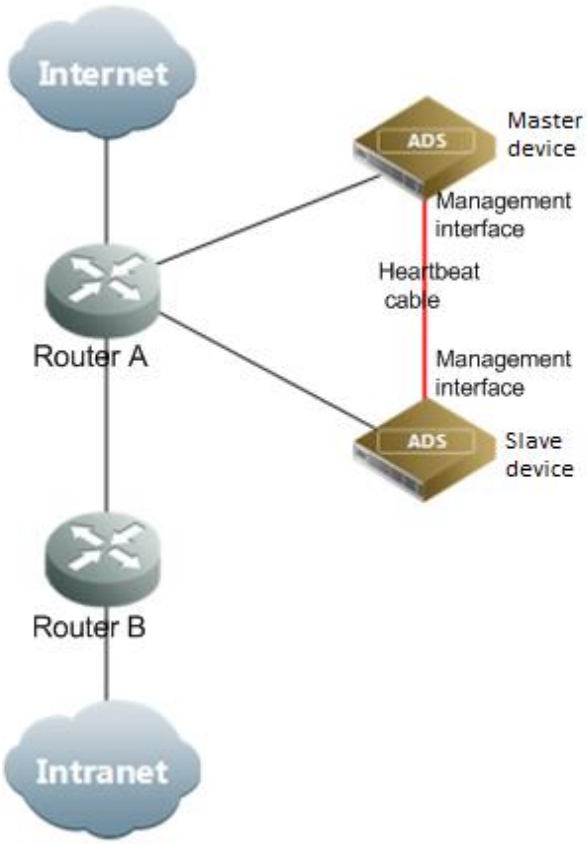
Currently, ADS supports two dual-system hot standby modes: active-active and active-standby.

In active-active mode, one ADS device functions as the master device, and the other as the slave device. Both the master and slave devices handle services and achieve load balancing. If the master device fails, the slave device takes over all work and traffic handled by the former, ensuring to the maximum extent that services are available.

In active-standby mode, one ADS device functions as the master device, and the other as the slave device. By default, the master device handles all traffic and synchronizes heartbeat information and real-time status to the slave device that is only a backup device and does not handle services. If the master device fails, the slave device takes over all work and traffic handled by the former, ensuring to the maximum extent that services are available.

Currently, ADS supports the dual-system hot standby function only when deployed in out-of-path mode. As shown in Figure 3-21, the master and slave devices are connected by heartbeat interfaces (management interfaces on devices) to synchronize heartbeat information and real-time status and establish the BGP neighbor relationship with the peer router.

Figure 3-21 HA topology



Note	• Usually, ADS is deployed on the backbone network. Currently, HA can be implemented only in the case of BGP diversion. • Currently, once the master device fails, the slave device automatically takes over all services from the master device. • If **Syn Diversion Config After Entering a Cluster** is enabled in HA advanced configurations on both the master and slave devices, the master device will automatically take back services after it recovers. Otherwise, the administrator needs to manually stop the BGP diversion on the slave device and enable BGP diversion on the master device.

For dual-system hot standby deployment, the administrator first needs to perform the following interface configuration on the two devices (see section 10.2.1 Configuring IPv4 Network Settings for details):

- Configure the heartbeat interface (management interface).

  The heartbeat interface is used by the master device to synchronize the specified configuration file to the slave device. For details, see section 3.1.9.2 HA File Synchronization Configuration. The heartbeat interfaces on the master and slave devices must be reachable for each other.
- Configure other communication interfaces.

After the interface configuration, enable the dual-system hot standby function and configure HA by completing the following:

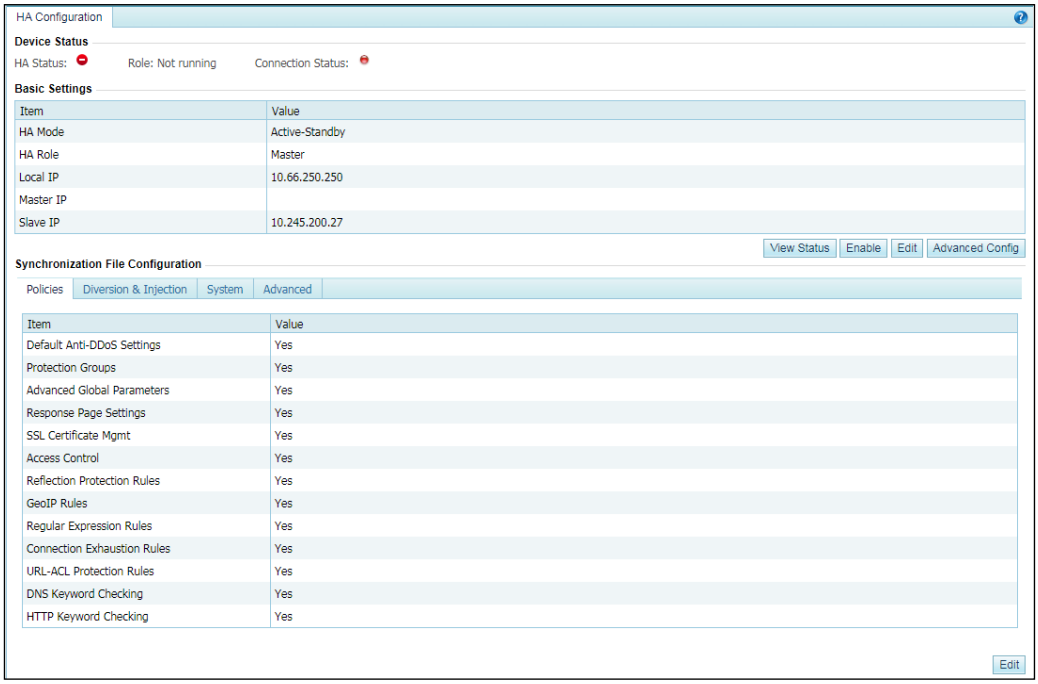
- Basic settings
- Synchronization file configuration

3.1.9.1 Basic HA Settings

Before enabling HA, you need to perform basic HA configuration on both the master the slave devices. To do that, perform the following steps:

Step 1 Choose **System** > **Local Settings** > **HA Configuration**.

Figure 3-22 HA Configuration page



Step 2 Click **Edit** in the lower-right corner of the **Basic Settings** area to open the editing page.

Figure 3-23 Editing basic settings

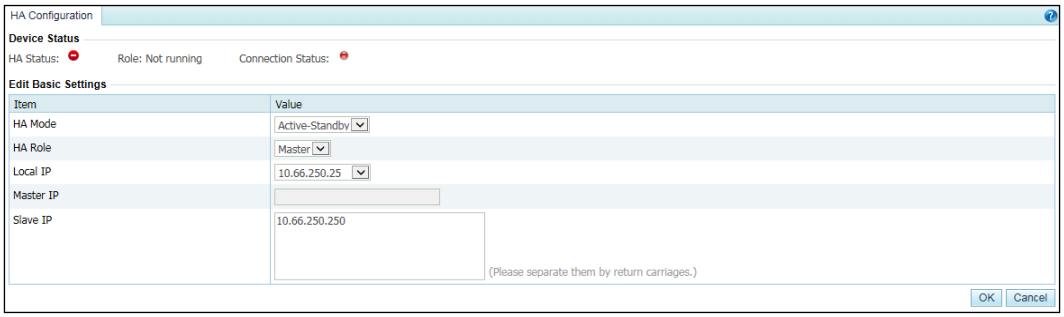


Table 3-11 describes parameters of basic HA settings.

Table 3-11 Parameters of basic HA settings

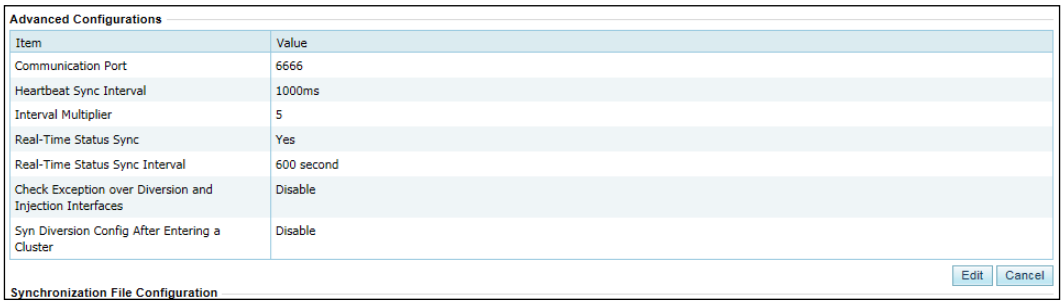
Parameter	Description
HA Mode	HA mode, which can be **Active-Active** or **Active-Standby**.
HA Role	Role played by the current device in dual-system hot standby mode. In active-standby mode: • **Master**: indicates that this device works as a master device. After HA is enabled, it starts handling services until a failure occurs. • **Slave**: indicates that this device acts as a slave device. After HA is enabled, this device is in backup state and starts handling services only when the master device fails. In active-active mode: • **Master**: indicates that this device works as a master device. After HA is enabled, it starts handling services until a failure occurs. • **Slave**: indicates that this device acts as a slave device. After HA is enabled, this device is in backup state and handles services the same as the master device, to achieve load balancing. If the master device fails, the slave device takes over all services.
Local IP	IP address of the management interface on the current device, which can be an IPv4 or IPv6 address.
Master IP	IP address of the master device, which can be an IPv4 or IPv6 address. Note • This parameter needs to be set only when **HA Role** is set to **Slave**. • The route between **Master IP** and **Slave IP** must be reachable.
Slave IP	IP address of the slave device, which can be an IPv4 or IPv6 address. Note • This parameter needs to be set only when **HA Role** is set to **Master**. • The route between **Master IP** and **Slave IP** must be reachable.

Step 3 Set parameters and click **OK** to save the settings.

Step 4 (Optional) Set advanced HA configurations.

a. Click **Advanced Config** in the lower-right corner of the **Basic Settings** area.

Figure 3-24 Advanced Configurations area



b. Click **Edit**.

Figure 3-25 Editing advanced settings

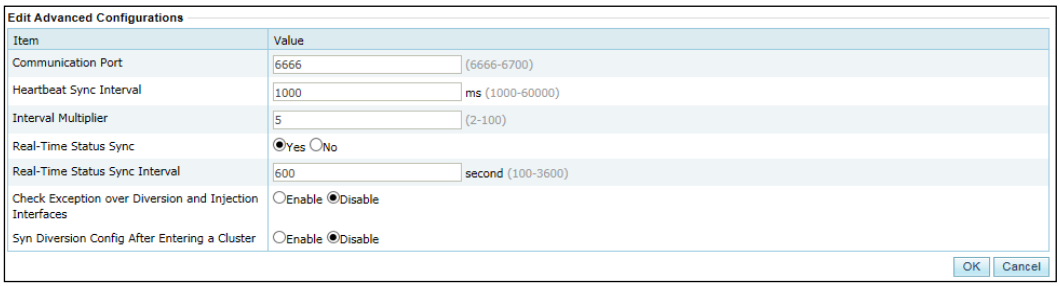


Table 3-12 describes the advanced HA configuration parameters.

Table 3-12 Advanced HA configuration parameters

Parameter	Description
Communication Port	Port for HA communication.
Heartbeat Sync Interval	Interval for the active device to synchronize keepalive information to the standby device, in milliseconds. The **Heartbeat Sync Interval** values on the master and slave devices should be as close as possible to avoid possible HA connection establishment failures.
Interval Multiplier	An auxiliary parameter for detecting heartbeat timeouts when an HA connection is established. The **Interval Multiplier** values on the master and slave devices should be as close as possible to avoid possible HA connection establishment failures.
Real-Time Status Sync	Whether to enable real-time status synchronization. **Real-Time Status Sync** should be enabled on both the master and slave devices so that files can be synchronized between the two devices.
Real-time Status Sync Interval	Interval at which the master device to synchronize specified configuration files to the slave device.
Check Exception over Diversion and Injection Interfaces	Controls whether to check the status of diversion and injection interfaces. When an exception is detected on the diversion or injection interface, a master/slave switchover is triggered.
Syn Diversion Config	After an ADS device joins a cluster, the diversion status of the peer is

Parameter	Description
After Entering a Cluster	synchronized to this device.

Step 5 Click **OK** to save the settings.

----End

3.1.9.2 HA File Synchronization Configuration

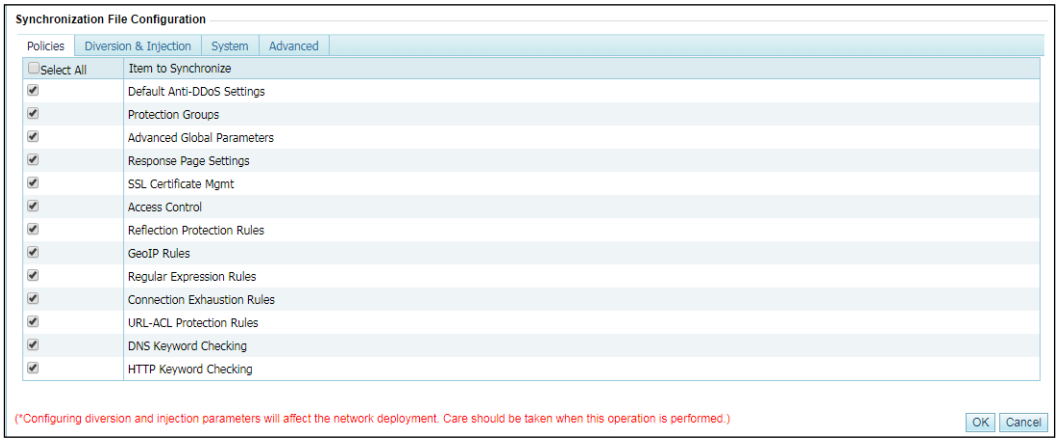
After configuring basic HA settings on both the master and slave devices, you need to specify files to be synchronized, including configurations of policies, diversion and injection, system, and advanced applications.

To specify files to be synchronized, perform the following steps:

Step 1 Choose **System** > **Local Settings** > **HA Configuration**.

Step 2 Click **Edit** in the lower- right corner of the **Synchronization File Configuration** area to open the editing page.

Figure 3-26 Policy configurations to be synchronized



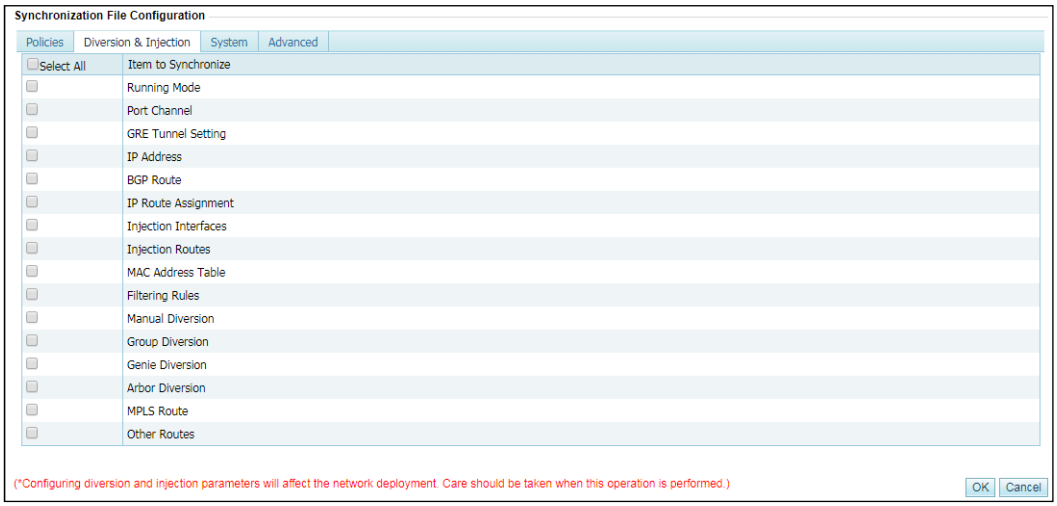
Step 3 Select desired configurations and click **OK**.

Step 4 Click the **Diversion & Injection** tab.

The area for selecting diversion and injection configurations to be synchronized appears, as shown in Figure 3-27.

Note	Synchronizing diversion and injection configurations may cause network interruption or other problems. Be careful and perform such synchronization only when necessary.

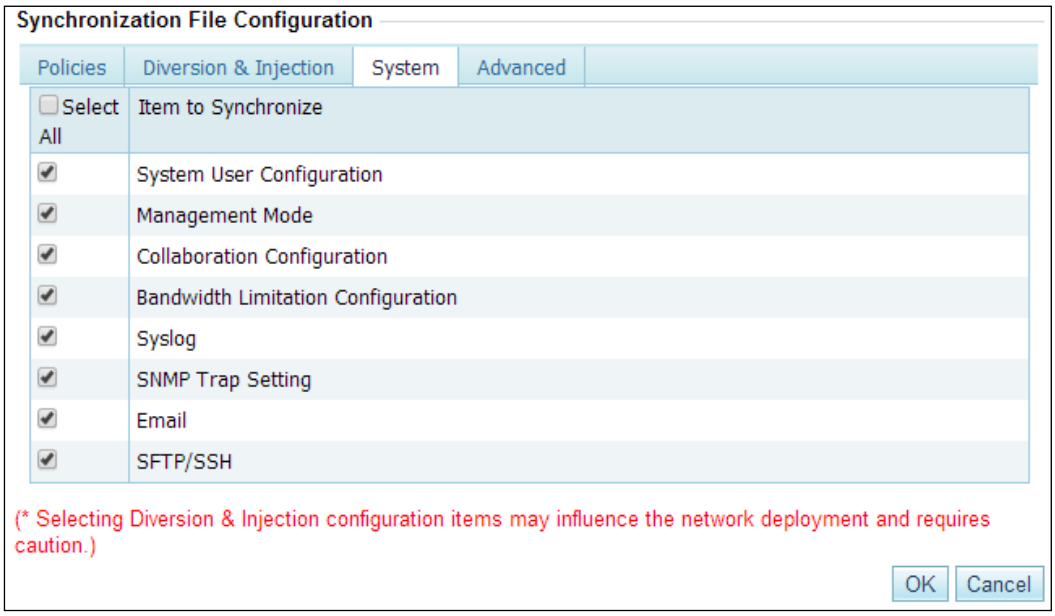
Figure 3-27 Diversion and injection configurations to be synchronized



Step 5 Select desired configurations and click **OK**.Click the **System** tab.

The area for selecting system configurations to be synchronized appears, as shown in Figure 3-28.

Figure 3-28 System configurations to be synchronized

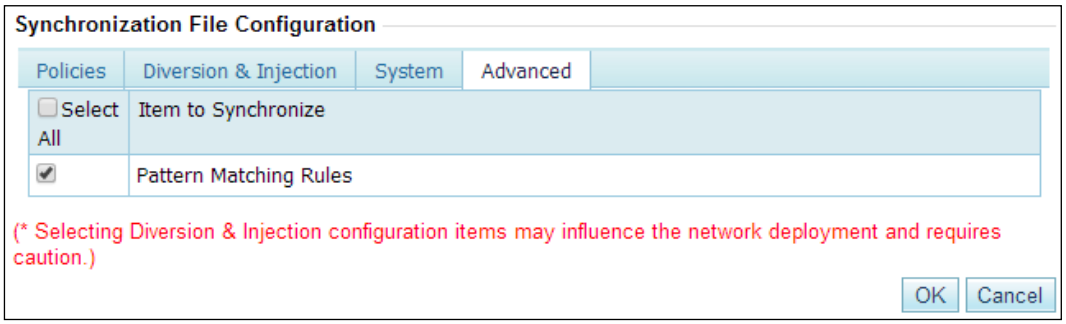


Step 6 Select desired configurations and click **OK**.

Step 7 Click the **Advanced** tab.

The area for selecting advanced configurations to be synchronized appears, as shown in Figure 3-29.

Figure 3-29 Advanced configurations to be synchronized



Step 8 Select the configuration and click **OK**.

----End

3.1.9.3 Enabling HA

After completing basic HA settings and file synchronization configuration on both the master and slave devices, you can enable HA on them separately by clicking **Enable** in the lower-right corner of the **Basic Settings** area on the **HA Configuration** tab page shown in Figure 3-22.

After HA is enabled, the **HA Configuration** tab page on a master device is as shown in Figure 3-30, and that on a slave device is as shown in Figure 3-31.

Figure 3-30 HA Configuration tab page on a master device

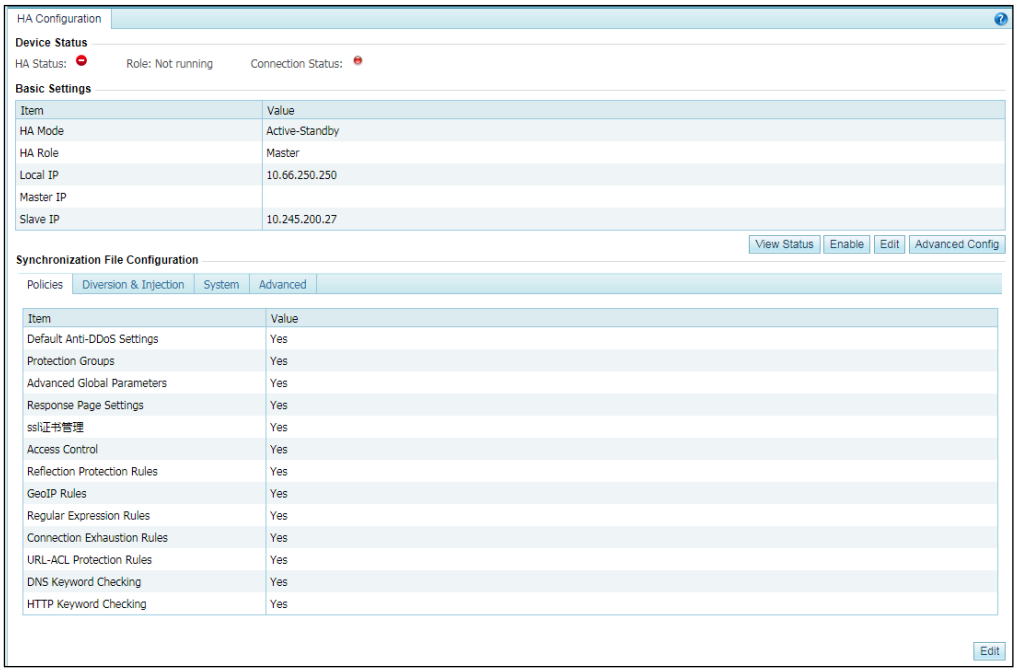
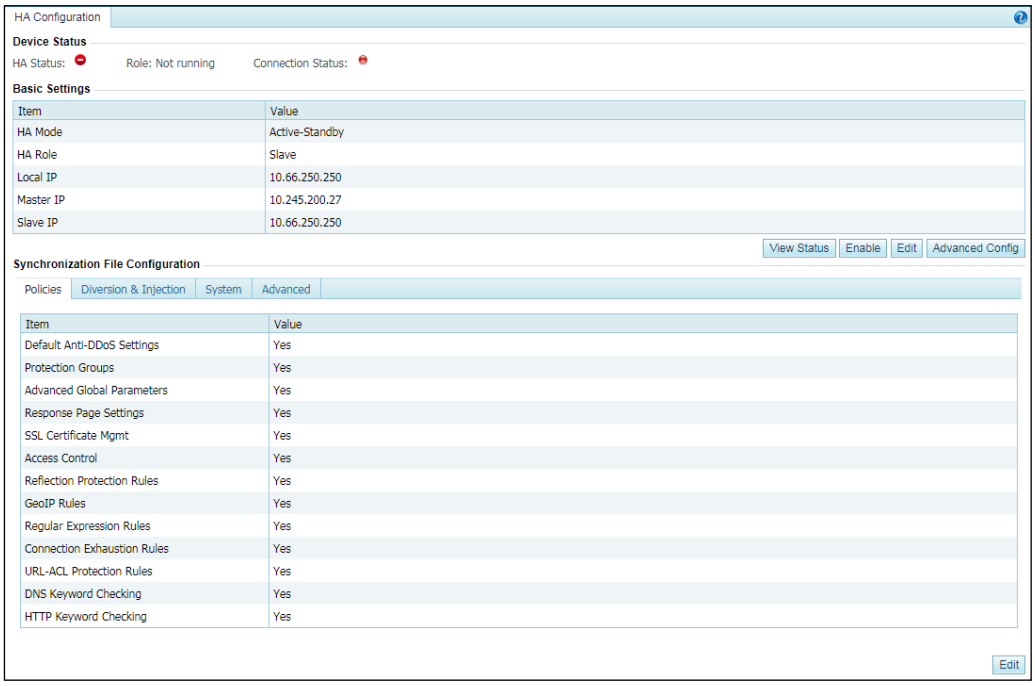


Figure 3-31 HA Configuration tab page on a slave device



3.1.9.4 Disabling HA

After HA is enabled, in the lower-right corner of the **Basic Settings** area on the **HA Configuration** tab page shown in Figure 3-22, the **Enable** button changes to **Disable**. You can click **Disable** to disable HA.

Generally, you need to disable HA before editing such parameters as **HA Mode**, **HA Role**, **Local IP**, **Master IP**, **Slave IP**, and **Heartbeat Sync Interval**.

3.1.9.5 Viewing HA Status

After HA is enabled, the work status, role, connection status, and peer list of HA are displayed in the **Device Status** area shown in Figure 3-22.

To view the detailed status of HA configuration, you can click the **View Status** in the lower-right corner of the **Basic Settings** area shown in Figure 3-22.

Figure 3-32 shows the status viewing result on a master device in active-active mode, and Figure 3-33 shows that on a slave device in active-active mode.

Figure 3-32 Status viewing result on a master device

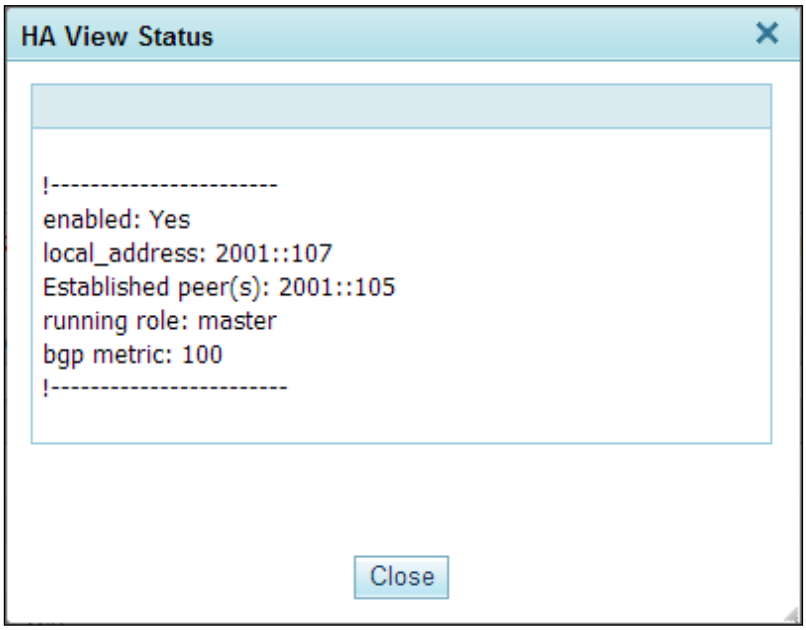
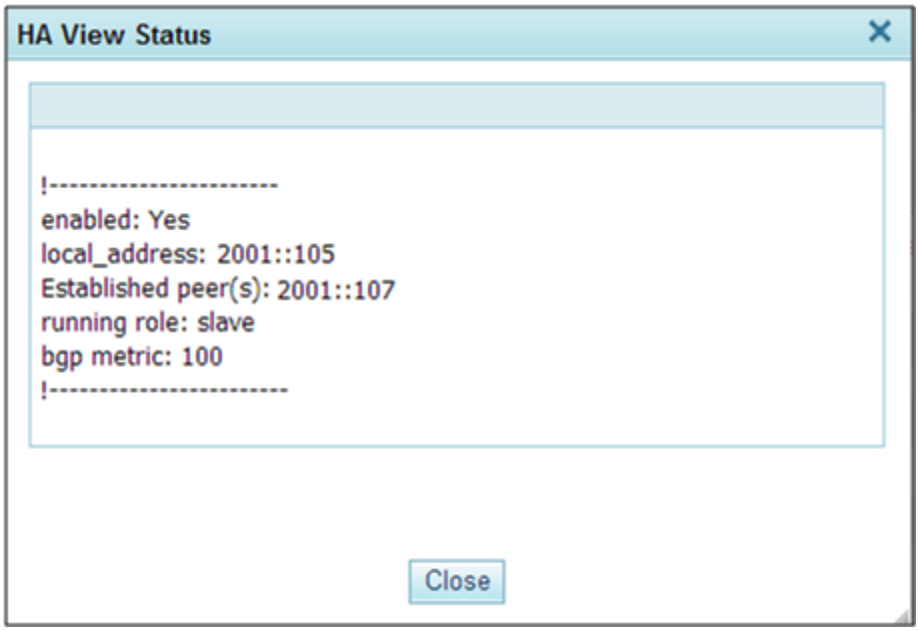


Figure 3-33 Status viewing result on a slave device



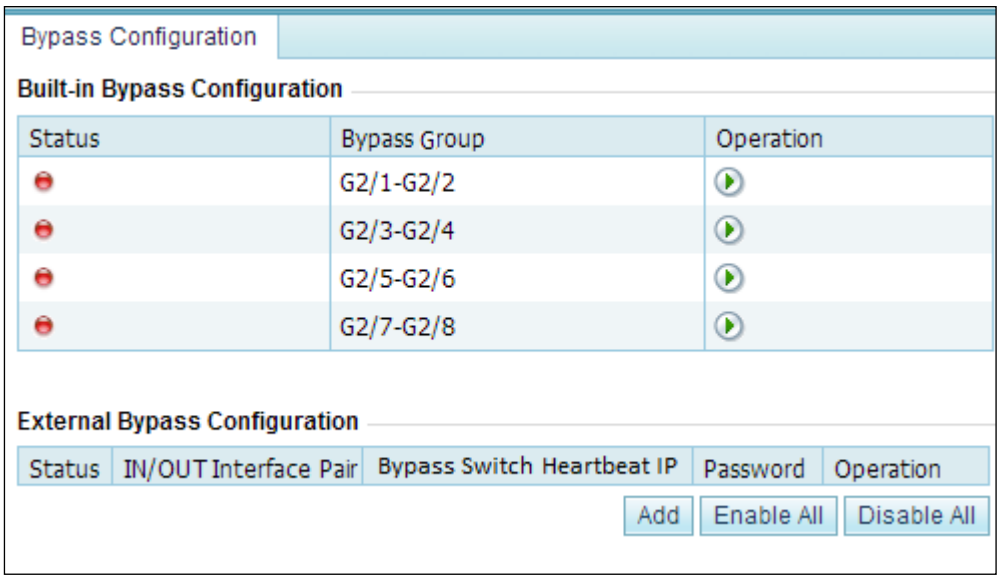
3.1.10 (Optional) Bypass Configuration

The bypass function is available only for ADS devices running in in-path mode. Currently, ADS NX5-8000 and ADS NX5-10000 does not support bypass configuration.

This function ensures uninterrupted network communications when ADS fails. ADS devices provide the built-in bypass function.

To configure this function, choose **System** > **Local Settings** > **Bypass Configuration**.

Figure 3-34 Bypass Configuration page



3.1.10.1 **Built-in Bypass**

The built-in bypass function is disabled by default, as shown in Figure 3-34.

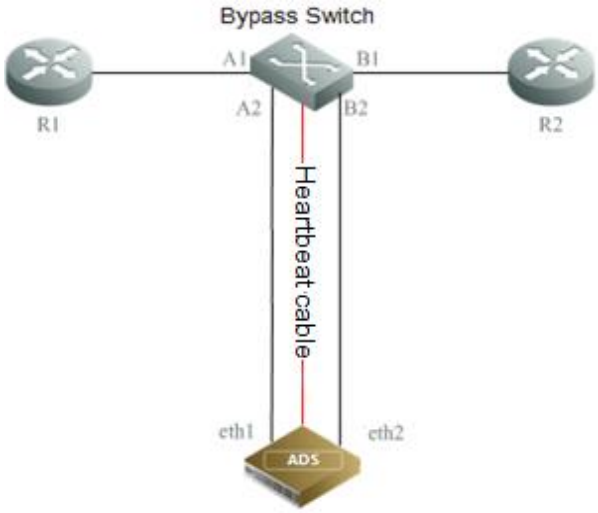
- To enable this function, click in the **Operation** column. Then the indicator in the **Status** column turns to , indicating that the built-in bypass function is enabled. At the same time, the button in the **Operation** column turns to .
- To disable this function, click in the **Operation** column. Then the indicator in the **Status** column turns to , indicating that the built-in bypass function is disabled.

3.1.10.2 **External Bypass**

The external bypass function can only be enabled on optical interfaces. This function is only available for ADS NX5-4020 and ADS NX3-2020/-2020E/2010 in in-path mode. External bypass devices of NSFOCUS devices are called NSF-BS.

Figure 3-35 shows the topology for the interaction between ADS and the bypass switch.

Figure 3-35 Topology for the interaction between ADS and the bypass switch



When any of the following occurs:

- the ADS is powered off;
- the heartbeat interface is Down; or
- the interface check function is enabled,

the associated work group interface is Down, and the bypass switch automatically switches to the bypass mode so that the traffic is transmitted to the next-hop device, bypassing ADS. This ensures uninterrupted network communications.

Note	If any of the following occurs, the bypass switch automatically switches to the bypass mode: • ADS's engine quits. • ADS is restarted. • ADS hangs. • NSF-BS is manually switched to the bypass state via the web-based manager. • The route is unreachable between the management interface on ADS and the heartbeat interface on NSF-BS, for example, when the physical connection is broken. • ADS is powered off. • The IN and OUT interfaces used by ADS to connect to NSF-BS are in different states, that is, one interface is Up and the other is Down. • NSF-BS is manually switched to the bypass state via a heartbeat interface or serial port. If any of the following occurs, the NSF-BS is automatically switched to the non-bypass mode: • NSF-BS is manually switched to the non-bypass state via the web-based manager. • The NSF-BS is manually switched to the non-bypass state via a heartbeat interface or serial port. • The heartbeat synchronization succeeds after a previous failure, that is, the route becomes reachable between the management interface on ADS and the heartbeat interface on NSF-BS.

Caution	In in-path mode, ADS enters the bypass state by default when started. If you want ADS to implement protection, you must manually disable the external bypass so that ADS can switch to the normal protection state.

On the **External Bypass** area shown in Figure 3-34, you can manage the bypass function as follows:

Adding an External Bypass Group

Click **Add** to the lower right of the external bypass configuration table to add an external bypass group. See Figure 3-36.

Figure 3-36 Adding an external bypass group

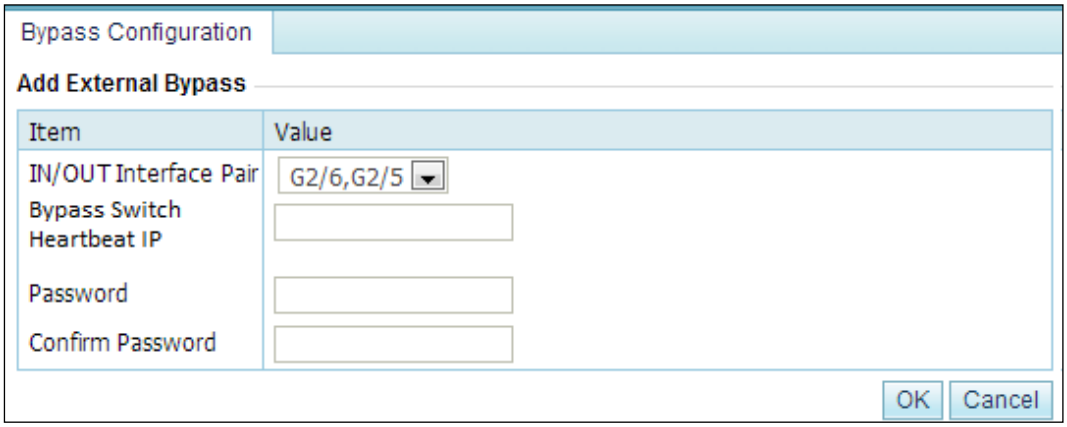


Table 3-13 describes parameters of the external bypass group.

Table 3-13 Parameters of the external bypass group

Parameter	Description
IN/OUT Interface Pair	A pair of IN and OUT interfaces used by ADS to connect to the bypass switch.
Bypass Switch Heartbeat IP	IP address used by the external switch to communicate with ADS. For details on installation and usage of the external switch, refer to the related user guide shipped with the switch.
Password	Password used for login to the bypass switch. For the password, refer to the related user guide shipped with the switch.
Confirm Password	Login password typed for confirmation.

Editing an External Bypass Group

Click in the **Operation** column of an external bypass group to modify its configuration. Then click **OK** to save the changes.

Deleting an External Bypass Group

Click in the **Operation** column of an external bypass group and then click **OK** to delete the group.

Enabling External Bypass Groups

On ADS, you can enable one or all external bypass groups:

- To enable one group, click in the **Operation** column. Then the indicator in the **Status** column turns to , indicating that the bypass group is enabled.
- To enable all external groups, click **Enable All** to the lower right of the external bypass table and click **OK** in the displayed dialog box.

Disabling External Bypass Groups

On ADS, you can disable one or all external bypass groups:

- To disable a bypass group, click in the **Operation** column. Then the indicator in the **Status** column turns to , indicating that the bypass group is disabled.
- To disable all bypass groups, click **Disable All** to the lower right of the external bypass table and click **OK** in the displayed dialog box.

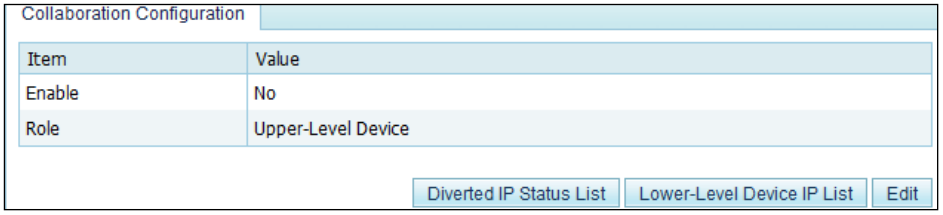
3.1.11 Collaboration Configuration

Note	• ADS NX5-10000 does not support collaboration configuration. • This module supports only IPv4 addresses.

ADS devices can work in hierarchical mode to provide better security protection: Once detecting that traffic exceeds a specified threshold, a lower-level ADS instructs the upper-level ADS with more powerful processing capabilities to divert the traffic for processing. After processing, the upper-level ADS injects the legitimate traffic back to the lower-level ADS.

Choose **System** > **Local Settings** > **Collaboration Configuration**. The **Collaboration Configuration** page appears, as shown in Figure 3-37.

Figure 3-37 Collaboration Configuration page



3.1.11.1 Managing Upper-Level ADS Devices

Configuring an Upper-Level ADS

To configure an upper-level ADS, perform the following steps:

Step 1 On the **Collaboration Configuration** page shown in Figure 3-37, click **Edit** and set **Enable** to **Yes** and **Role** to **Upper-Level Device**, as shown in Figure 3-38.

Note	For an upper-level device, you must set **Enable** to **Yes** and specify an IP address for the lower-level device in **Management Mode** under **System** > **Local Settings**.

Figure 3-38 Configuring an upper-level ADS

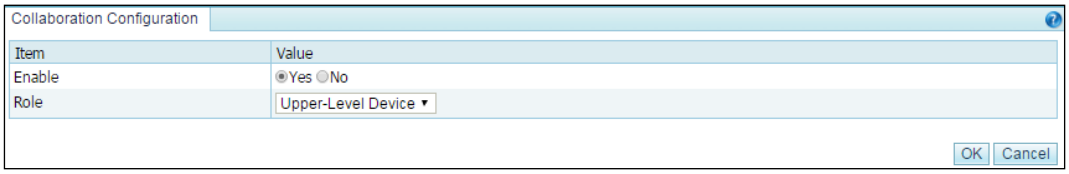


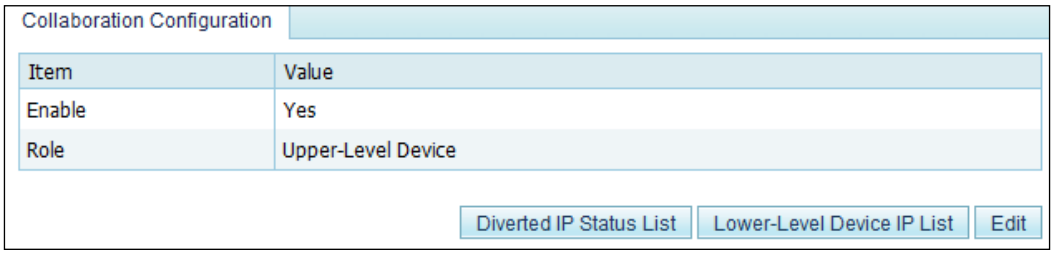
Table 3-14 describes parameters for configuring an upper-level ADS.

Table 3-14 Parameters for configuring an upper-level ADS

Parameter	Description
Enable	Controls whether to enable collaboration between lower-level and upper-level ADS devices. • **Yes**: enables the collaboration function. • **No**: disables the collaboration function. If **Yes** is selected, you need to set **Accept Management** to **Yes** on the **Management Mode** page (**System** > **Local Settings**). For details, see section 3.1.4 Management Mode Configuration.
Role	Role of the device. Here **Upper-Level Device** should be selected.

Step 2 Click **OK** to return to the **Collaboration Configuration** page.

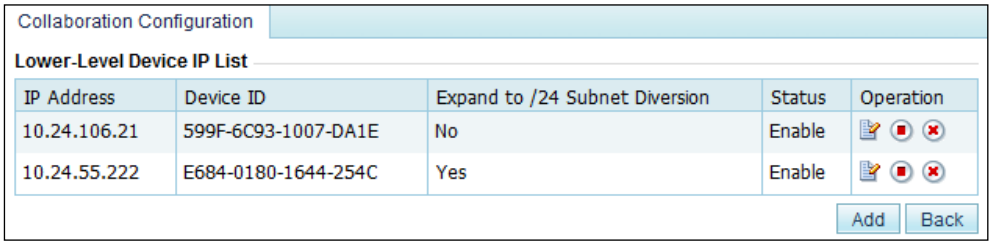
Figure 3-39 Collaboration Configuration page



Step 3 Click **Lower-Level Device IP List**.

IP addresses of lower-level ADS devices are displayed. See Figure 3-40.

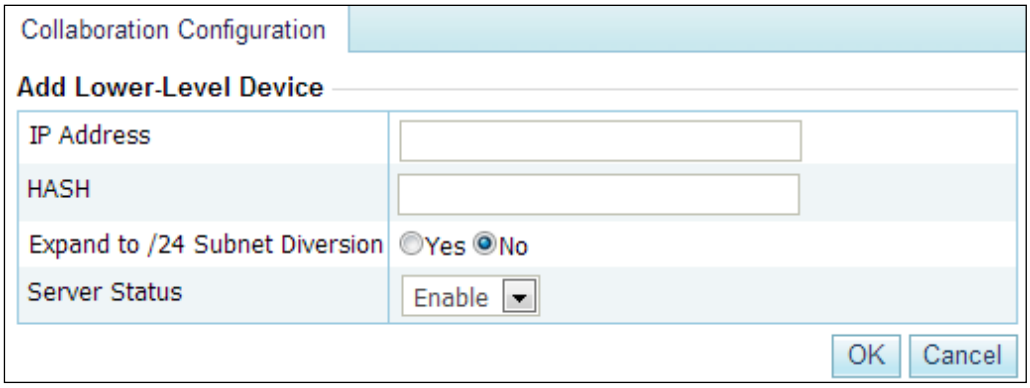
Figure 3-40 List of IP addresses of lower-level devices



Step 4 Click **Add** to add a lower-level device.

Type the IP address and hash value of the lower-level device and leave other parameters at their default values.

Figure 3-41 Adding a lower-level ADS



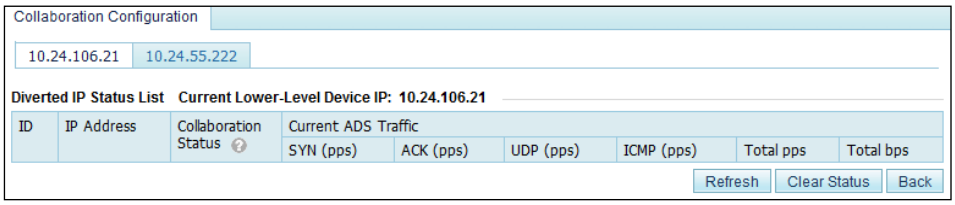
Step 5 Click **OK** to complete the configuration.

----End

Viewing Diverted IP Status List

On the **Collaboration Configuration** page shown in Figure 3-37, click **Diverted IP Status List** to view IP addresses notified to the current ADS by lower-level ADS devices for traffic diversion and traffic information on the current ADS.

Figure 3-42 Viewing diverted traffic



3.1.11.2 Managing Lower-Level ADS Devices

Configuring a Lower-Level ADS

To configure a lower-level ADS, perform the following steps:

Step 1 On the **Collaboration Configuration** page shown in Figure 3-37, click **Edit** and set **Enable** to **Yes** and **Role** to **Lower-Level Device**, as shown in Figure 3-43.

Figure 3-43 Configuring a lower-level ADS

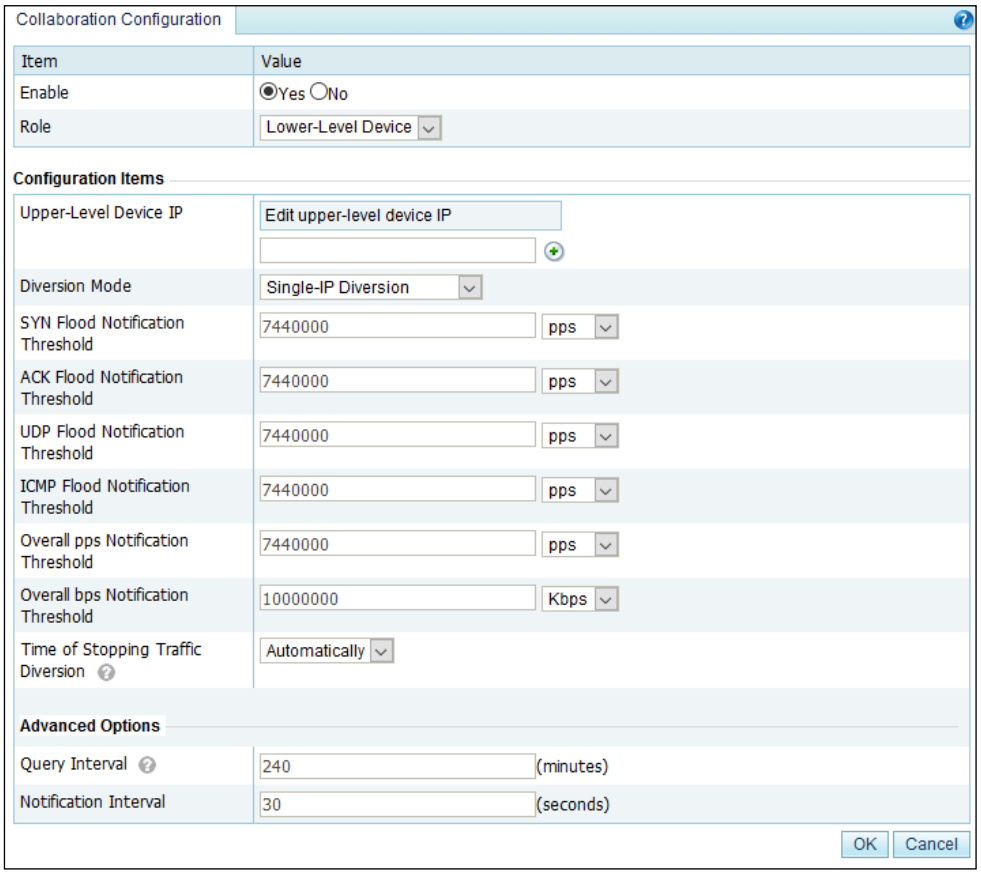


Table 3-15 describes parameters for configuring a lower-level ADS.

Table 3-15 Parameters for configuring a lower-level ADS

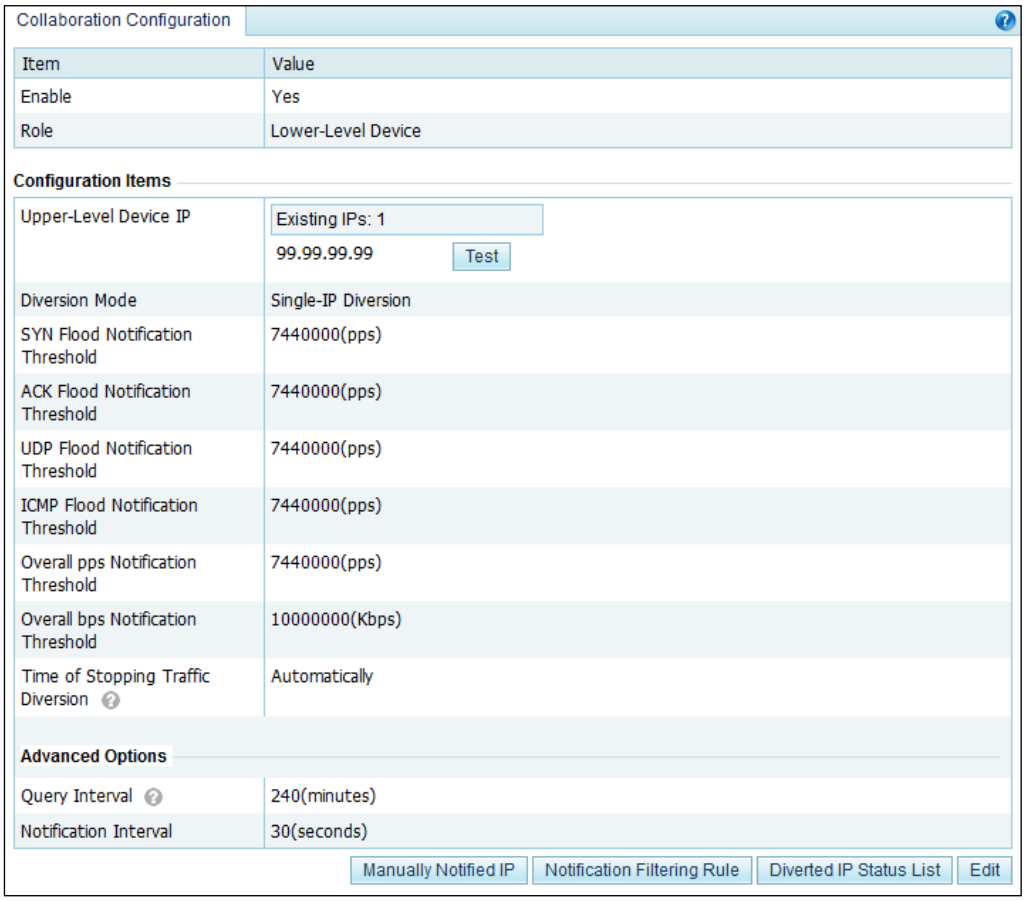
Parameter	Description
Enable	Controls whether to enable collaboration between lower-level and upper-level ADS devices. • **Yes**: enables the collaboration function. • **No**: disables the collaboration function. **Note** The lower-level device instructs the upper-level ADS to divert traffic when finding that traffic exceeds a notification threshold.
Role	Role of the device. Here **Lower-Level Device** should be selected.
Upper-Level Device IP	IP address of the management interface of the upper-level ADS.
Diversion Mode	Mode of traffic diversion between upper-level and lower-level devices. • **Single-IP Diversion**: indicates that traffic diversion is triggered when traffic destined for a single IP address exceeds a threshold.

Parameter	Description
	• **Device Overall Threshold**: indicates that traffic diversion is triggered when the overall traffic of the lower-level device exceeds a threshold.
SYN Flood Notification Threshold	Threshold for SYN flood traffic. When the traffic rate of SYN packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
ACK Flood Notification Threshold	Threshold for ACK flood traffic. When the traffic rate of ACK packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
UDP Flood Notification Threshold	Threshold for UDP flood traffic. When the traffic rate of UDP packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
ICMP Flood Notification Threshold	Threshold for ICMP flood traffic. When the traffic rate of ICMP packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
Overall pps Notification Threshold	Threshold for overall traffic in pps. When the traffic rate reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
Overall bps Notification Threshold	Threshold for overall traffic in bps. When the traffic rate reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
Time of Stopping Traffic Diversion	• **Automatically**: The lower-level ADS determines whether to send notifications to the upper-level ADS for stopping traffic diversion. • **Scheduled**: If this is selected, you also need to specify how many minutes later traffic diversion will be stopped. The lower-level ADS sends notifications to the upper-level ADS for stopping traffic diversion only when the scheduled time expires. Note When the upper-level ADS diverts traffic, the lower-level ADS suspends protection for the related IP address. After the upper-level ADS's traffic diversion stops, the lower-level ADS resumes protection for this IP address.
Query Interval	Interval at which the lower-level device queries the upper-level device about the current traffic destined for an IP address after the traffic destined for this IP address is diverted. The interval should be longer than 5 minutes; otherwise, route flapping may occur.
Notification Interval	Interval at which the lower-level device resends a diversion notification to the upper-level ADS after a failed diversion notification. The recommend value is 30 to 60 seconds.

Step 2 Click **OK**.

The lower-level ADS configuration page appears, as shown in Figure 3-44.

Figure 3-44 Lower-level ADS configuration



Step 3 Click **Test** to check whether the connection between the upper-level and lower-level devices succeeds.

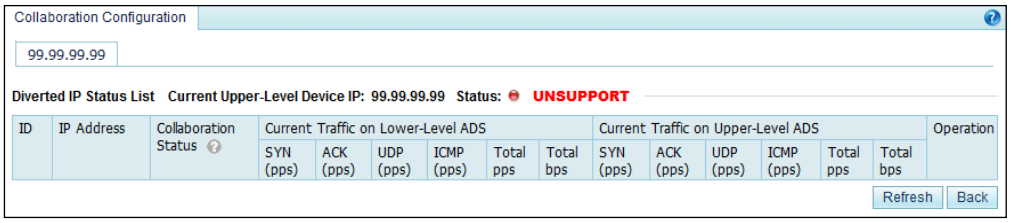
If the icon appears to the left of the **Test** button, the connection succeeds.

----End

Viewing Diverted IP Status List

On the **Collaboration Configuration** page shown in Figure 3-44, click **Diverted IP Status List** to view the current traffic on the upper-level and lower-level ADS devices. See Figure 3-45.

Figure 3-45 Status of diverted traffic

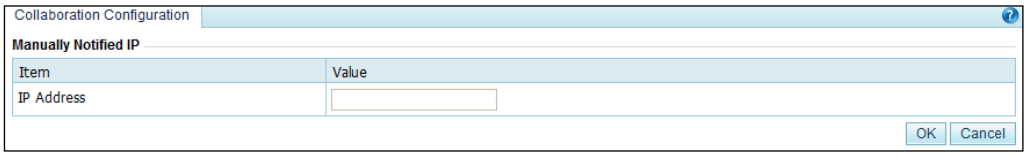


Specifying IP Addresses for Manual Diversion

Sometimes you want an upper-level ADS to divert traffic destined for certain IP addresses. For this purpose, you should specify IP addresses by performing the following steps:

Step 1 On the **Collaboration Configuration** page shown in Figure 3-44, click **Manually Notified IP**.

Figure 3-46 Configuring manually notified IP addresses



Step 2 Type a desired IP address and click **OK** to complete the configuration.

If multiple IP addresses are required, add them one by one.

----End

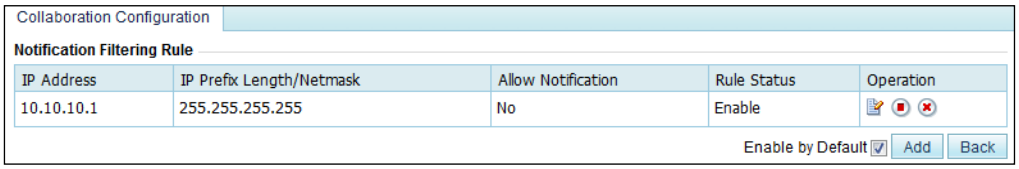
Configuring Notification Filtering Rules

The upper-level ADS can successfully divert traffic destined for the specified IP addresses upon a manual or automatic notification only when notification filtering rules are configured.

To create a notification filtering rule, perform the following steps:

Step 1 On the **Collaboration Configuration** page shown in Figure 3-44, click **Notification Filtering Rule**.

Figure 3-47 Notification filtering rule page



Step 2 Click **Add**.

Figure 3-48 Adding a notification filtering rule

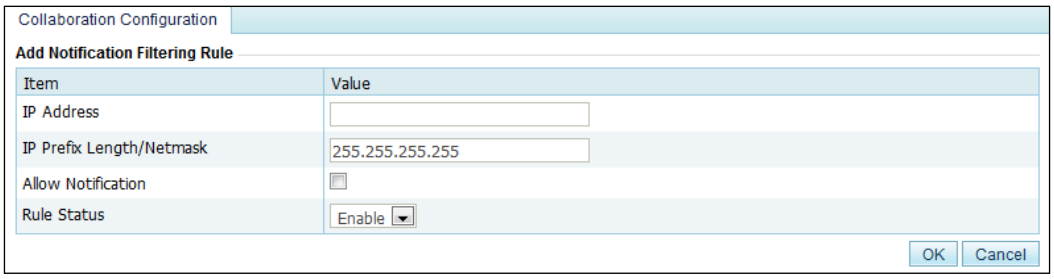


Table 3-16 describes parameters for creating a notification filtering rule.

Table 3-16 Parameters for creating a notification filtering rule

Parameter	Description
IP Address	Destination IP address or segment of traffic to be manually diverted to the upper-level device.
IP Prefix Length/Netmask	Prefix length or netmask of the IP address. The default value is **255.255.255.255**.
Allow Notification	Whether notification is allowed for the IP address. The upper-level device can receive notification regarding the IP address only after **Allow Notification** is selected.
Rule Status	Controls whether to enable this rule. • **Yes**: enables this rule. • **No**: disables this rule.

Step 3 Set parameters and click **OK** to complete the configuration.

----End

3.2 Security Configuration

This section covers the following topics:

- Login Security Settings
- Locked User Management
- Authentication Configuration

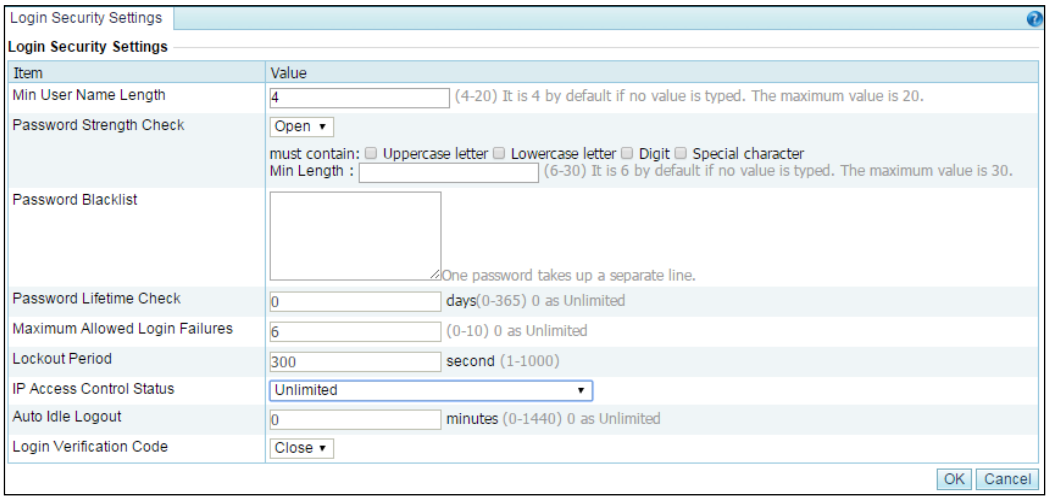
3.2.1 Login Security Settings

This section describes how to configure login security parameters.

The procedure is as follows:

Step 1 Choose **System > Security Configuration > Login Security Settings**, and then click **Modify**. See Figure 3-49.

Figure 3-49 Configuring login security parameters



Step 2 On the page that appears, configure login security parameters.

Table 3-17 describes parameters on this page.

Table 3-17 Login security parameters

Parameter	Description
Min User Name Length	Specifies the minimum length of user names. The value range is 4–20, with **4** as the default.
Password Strength Check	Specifies the type of characters to be automatically checked for password strength when you configure or change the password. Only a password conforming to the requirement can be successfully set. • **Close**: omits the password strength check. • **Open**: performs the password strength check. If this is selected, the password complexity and minimum length must be specified. • **must contain**: specifies the types of characters (digits, special characters, uppercase letters, and lowercase letters) that must be contained. You should select two or more types. • **Min Length**: specifies the minimum length of user names. The value range is 6–30, with **6** as the default.
Password Blacklist	Blacklisted passwords, with each in a separate line. None of those can be used as the password of a user account.
Password Lifetime Check	Specifies the lifetime of the password that is successfully configured. A password whose lifetime has expired must be changed. The value ranges from 0 to 365 days. The value **0** indicates that this function is disabled.
Maximum Allowed Login Failures	Specifies the maximum number of consecutive failed login attempts in the allowed login interval. The value ranges from 0 to 10. The value **0** indicates that this function is disabled, that is, the number of consecutive failed login attempts is not limited.
Lockout Period	Specifies how long a user will be locked after **Maximum Allowed Login Failures** is exceeded. During the lockout period, the user is prevented from

Parameter	Description
	logging in to the system. The value ranges from 1 to 1000 seconds. You are advised to set it to a value no smaller than 180 seconds.
IP Access Control Status	Controls whether to control access from certain IP addresses. • **Unlimited**: allows access to the device from all IP addresses. • **Allow access from the following IP addresses**: allows access to the device from IP addresses listed below. • **Block access from the following IP addresses**: blocks access to the device from IP addresses listed below. When you access ADS from a blocked IP address, the system displays "You cannot log in from the current IP address. Please contact the administrator to check access control settings." on the login page.
Auto Idle Logout	Specifies the time, in minutes, that a user is allowed to remain idle. When this period expires, a user is logged out and has to log in again before continuing using this system. The value ranges from 0 to 1440. You are advised to set it to a value no greater than 10. The value **0** indicates that this function is disabled.
Login Verification Code	Controls whether to allow use of login verification codes. • **Open**: allows use of login verification codes, indicating that a user can successfully log in to ADS only after typing a correct verification code. • **Close**: disallows use of login verification codes.

Step 3 Click **OK** to save the settings.

----End

3.2.2 Locked User Management

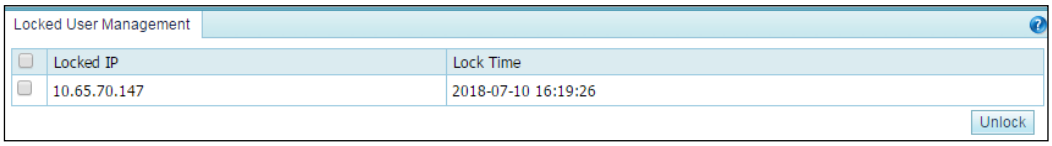
A user's account will be automatically locked after the number of failed login attempts exceeds the specified value. During the lockout period, the user cannot log in again. After the lockout period expires, the account will be automatically unlocked. You can also go to the **Locked User Management** page to manually unlock the account.

Note	Only the user **admin** can unlock user accounts.

The procedure is as follows for **admin** to unlock a user account:

Step 1 Choose **System > Security Configuration > Locked User Management**.

Figure 3-50 Locked User Management page



Step 2 Select the IP address to be unlocked and click **Unlock**.

----End

3.2.3 Authentication Configuration

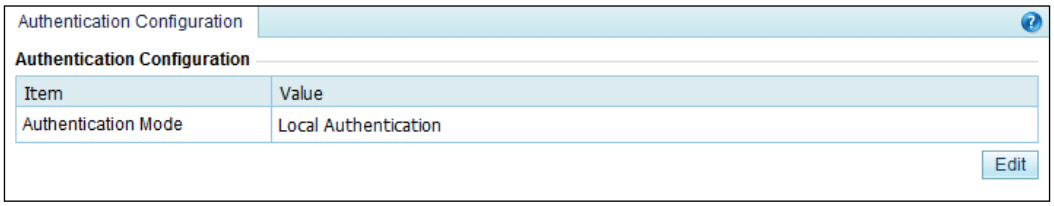
When a user logs in to the web-based manager of ADS, the following authentication modes are supported:

- Local authentication: The user can log in to ADS only if a correct user name and password are entered. The system user **admin** can only be locally authenticated.
- Radius authentication: The user can log in to ADS only if a correct user name, password, and key are entered. After **Authentication Mode** is set to **Radius Authentication**, Radius authentication is required for all users except the system user **admin**.

The procedure is as follows for **admin** to configure the authentication mode:

Step 1 Choose **System** > **Security Configuration** > **Authentication Configuration**.

Figure 3-51 Authentication Configuration page



Step 2 Click **Edit** to configure the authentication mode.

Figure 3-52 Editing authentication parameters

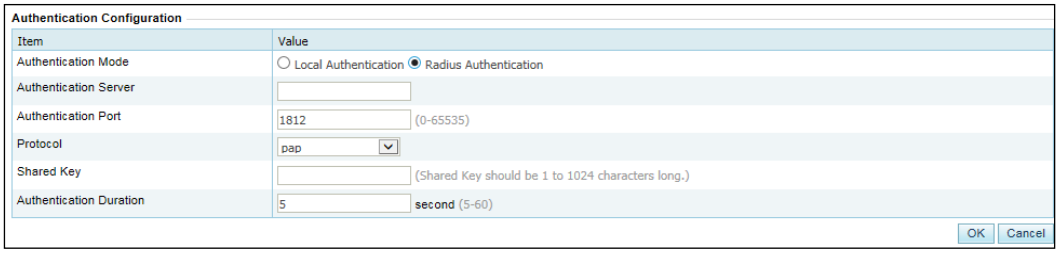


Table 3-18 Parameters for configuring the authentication mode

Parameter	Description
Authentication Mode	Specifies the authentication mode, which can be **Local Authentication** or **Radius Authentication**.
Authentication Server	Specifies the IP address of the Radius authentication server. Both IPv4 and IPv6 addresses are supported.
Authentication Port	Specifies the port on which the Radius authentication server listens for authentication requests. The default Radius authentication port is **1812**.
Protocol	Specifies the authentication mode of the Radius authentication server. This parameter can be set to **pap**, **spap**, **chap**, **mschapv1**, or **mschapv2**.
Shared Key	Specifies the shared key that serves as a password between the Radius server and a Radius client. The shared key configured on ADS must be the same as that configured on the Radius server; otherwise, ADS cannot communicate with the Radius server.
Authentication Duration	Specifies the duration of Radius authentication, after which ADS returns the success or failure of the authentication information.

Step 3 Click **OK** to save the settings.

----End

3.3 Log Services

This section covers the following topics:

- Syslog Configuration
- SNMP Configuration
- Email Configuration
- SFTP/SSH Configuration

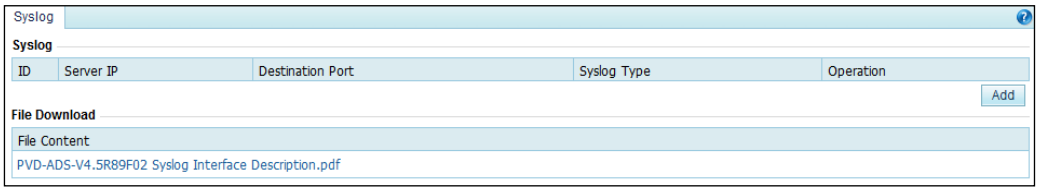
3.3.1 Syslog Configuration

After configuration, ADS can send specified logs to the remote syslog server through the communication interface.

Step 1 Choose **System** > **Log Services** > **Syslog**.

Before configuration, you can download the related syslog interface description file. In Figure 3-53, you can click the file name in the **File Download** area to download the syslog file to a local disk drive.

Figure 3-53 Configuring syslog



Step 2 Click **Add** to add a syslog server.

Note	A maximum of 10 syslog servers can be added. Syslog configurations are independent. When one syslog server fails, other servers can still receive syslog messages. Syslog servers can share a device ID and port number.

Figure 3-54 Configuring a syslog server

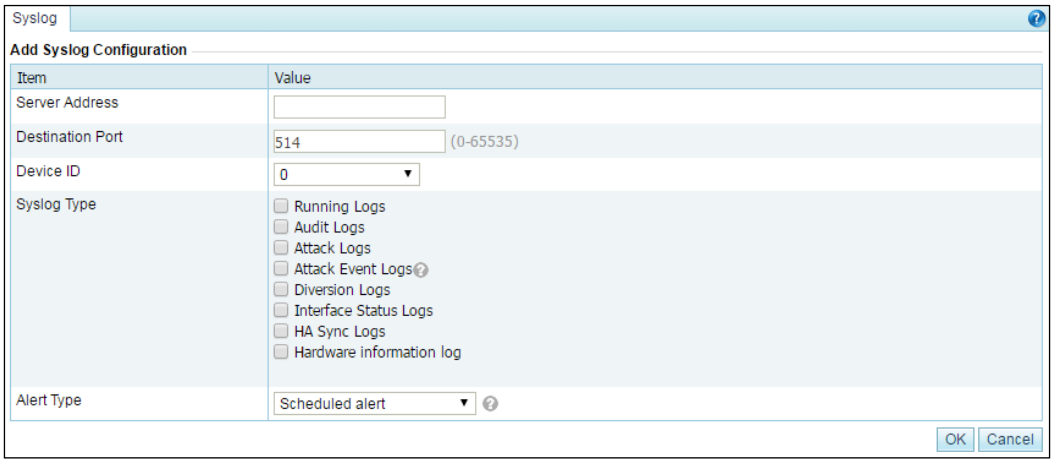


Table 3-19 Parameters for configuring a Syslog server

Parameter	Description
Server Address	IPv4 or IPv6 address of the syslog server.
Destination Port	Port of the syslog server.
Device ID	Uniquely identifies the device that sends log messages to the syslog server. It is an important parameter, ranging from 0 to 7.
Syslog Type	Specifies the type of log messages that are sent to the syslog server, which can be: • Running log • Audit log • Attack log • Attack event log

Parameter	Description
	• Diversion log • Interface status log • HA sync log • Hardware information log By default, the system sends log messages every 30 seconds.
Alert Type	Specifies the type of alerts, which can be either of the following: • **Scheduled alert**: sends alerts every 30 seconds. • **Threshold exceeding alert**: sends alerts when a threshold is exceeded. This parameter is valid only for the running log and hardware information log. If **Threshold exceeding alert** is selected, you need to further set hardware alert thresholds. For details, see section 3.1.7 Hardware Alert Thresholds.

Step 3 Configure parameters and click **OK** to save the settings.

----End

3.3.2 SNMP Configuration

Simple Network Management Protocol (SNMP) is used to ensure the transmission of management information between two arbitrary nodes on the network, so that the network administrator can query information, modify information, locate faults, and diagnose faults on any network node.

SNMP adopts the polling mechanism with basic function sets and is especially applicable to small, fast, and low-price environments. The SNMP implementation is based on the UDP protocol and so can connect to various products.

SNMP configuration on ADS includes:

- SNMP agent: configures ADS to collect information that can be reported to the network management station (NMS). SNMP V2C and SNMP V3 are supported.
- SNMP trap: configures ADS to collect trap messages, namely SNMP server-related information.

After SNMP is configured, ADS will send SNMP trap messages to SNMP NMS in an unsoliciated manner.

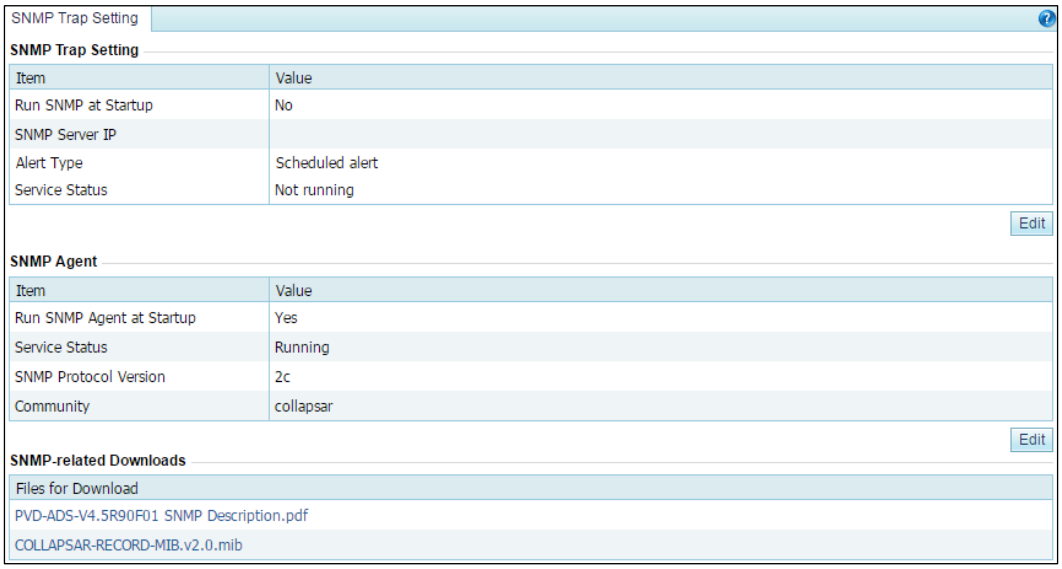
To configure SNMP, perform the following steps:

Step 1 Choose **System** > **Log Services** > **SNMP Setting**.

The **SNMP Trap Setting** page appears, as shown in Figure 3-55.

Before configuration, you can download the related SNMP description or MIB file by clicking a file name in the **SNMP-related Downloads** area to download the file to a local disk drive.

Figure 3-55 SNMP Trap Setting page



Step 2 Click **Edit** in the **SNMP Trap Setting** area and **SNMP Agent** area respectively to modify SNMP trap and SNMP agent parameters.

Table 3-20 describes SNMP Trap parameters.

Table 3-20 SNMP Trap parameters

Parameter	Description
Run SNMP at Startup	Controls whether to launch the SNMP trap service when ADS is started. • **Yes**: launches the SNMP trap service when ADS is started. • **No**: does not launch the SNMP trap service when ADS is started.
SNMP Server IP	IPv4 or IPv6 address of the SNMP server.
Alert Type	Specifies the type of alerts, which can be either of the following: • **Scheduled alert**: sends alerts every 30 seconds. • **Threshold exceeding alert**: sends alerts when a threshold is exceeded. This parameter is valid only for the system operation log and hardware information log. If **Threshold exceeding alert** is selected, you need to further set hardware alert thresholds. For details, see section 3.1.7 Hardware Alert Thresholds.
Service Status	Running status of the SNMP server.
Run SNMP at Startup	Controls whether to launch the SNMP agent when ADS is started. • **Yes**: launches the SNMP agent when ADS is started. • **No**: does not launch the SNMP agent when ADS is started.
Service Status	Running status of the SNMP agent server
SNMP Protocol Version	SNMP protocol supported by the SNMP agent, which can be SNMPv2c or SNMPv3
Community	Community supported by the SNMP agent. When the SNMP agent function is

Parameter	Description
	disabled, this parameter is unavailable.

Step 3 Set parameters and click **OK** to save the settings.

----End

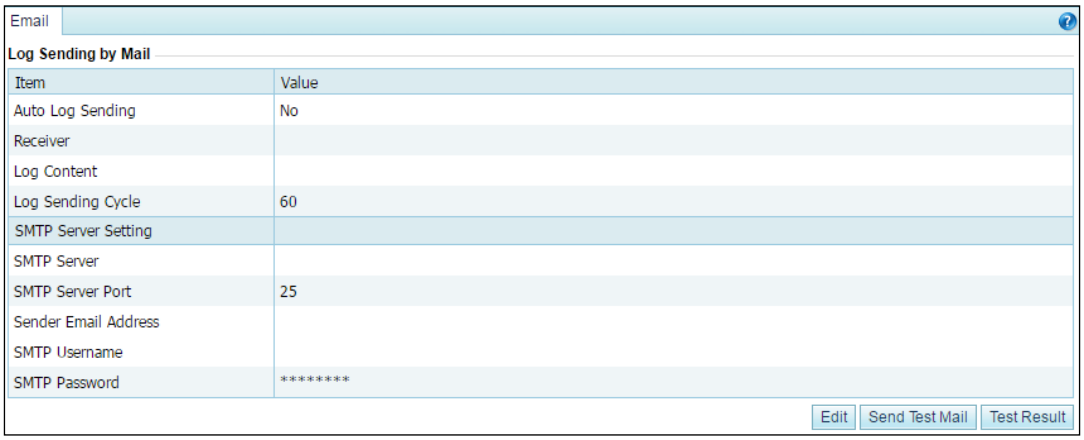
3.3.3 Email Configuration

Email configuration is required when ADS is configured to send one or multiple types of log to a specified email address.

To configure email parameters, perform the following steps:

Step 1 Choose **System** > **Log Services** > **Email**.

Figure 3-56 Log sending by email



Step 2 Click **Edit**.

Figure 3-57 Editing log sending parameters

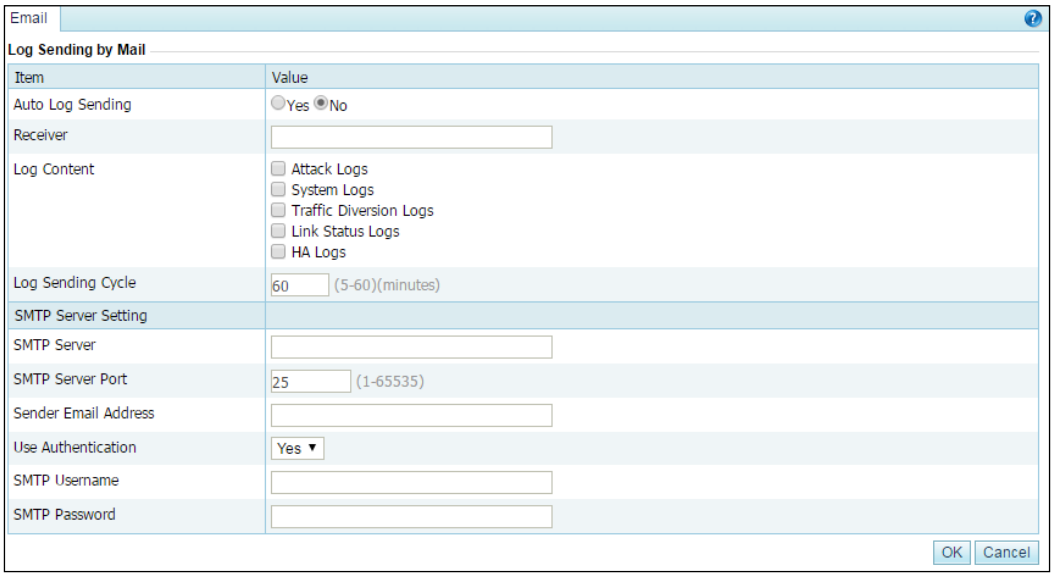


Table 3-21 describes parameters for configuring log sending by email.

Table 3-21 Parameters for configuring log sending by email

Parameter	Description
Auto Log Sending	Controls whether the system sends the selected log to a specific email address. The value **Yes** indicates that the system sends the selected log to a specific email address. If this function is enabled, you need to configure **Receiver** and **Log Content**.
Receiver	Email address that receives the log.
Log Content	Log to be sent, which can be the attack log, system log, traffic diversion log, link status log, and HA log. By default, the system sends log messages every 60 minutes.
Log Sending Cycle	Specifies how frequently emails are to be sent. The value range is 5 to 60 minutes.
SMTP Server	IP address or domain name of the SMTP server that sends emails. You can type either an IPv4 or IPv6 address.
SMTP Server Port	Specifies a port for the SMTP server to transmit emails.
Sender Email Address	Email address that sends logs.
Use Authentication	Specifies whether to authenticate the SMTP user sending emails. • **Yes**: authenticates the user that sends emails. • **No**: does not authenticate the user that sends emails.
SMTP Username/SMTP Password	User name and password for sending emails. The two parameters are available only when you select **Yes** for **Use Authentication**.

Step 3 Configure parameters and click **OK** to save the settings.

Step 4 Send a test mail.

After email parameters are configured, click **Send Test Mail** to check whether parameters are correctly configured. In the dialog box shown in Figure 3-58, type the email address to receive the test mail.

Figure 3-58 Send Test Mail dialog box

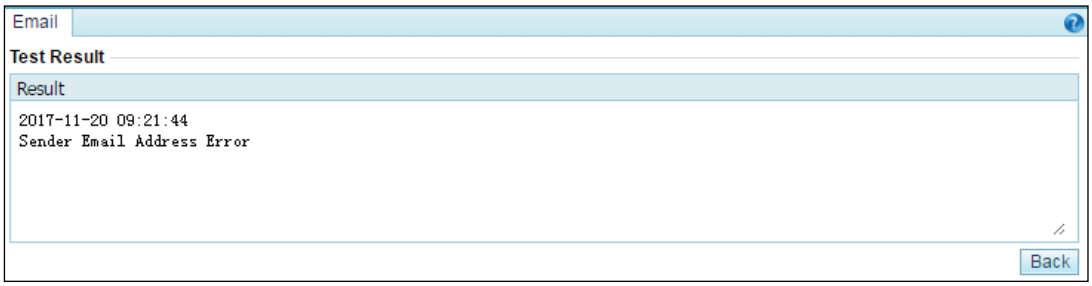
Step 5 Type the receiving address and then click **Send**.

ADS then sends a test mail to the specified address.

Step 4 View the test result.

Click **Test Result**. Then the test result is displayed, as shown in Figure 3-59.

Figure 3-59 Email test result



Note	After email parameters are configured, when the engine fails for three times, the system will automatically send engine fault logs to the specified email address.

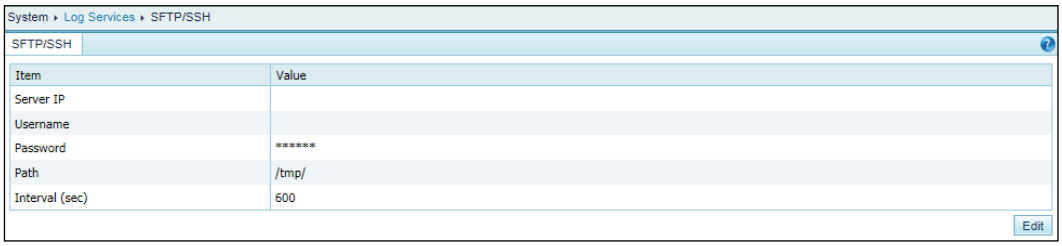
----End

3.3.4 SFTP/SSH Configuration

As shown in Figure 3-60, ADS can be configured to export logs of the protected server to a specified directory via SFTP or SSH.

Step 1 Choose **System** > **Log Services** > **SFTP/SSH**.

Figure 3-60 SFTP/SSH page



Step 2 Click **Edit** to the lower right of the table.

Figure 3-61 Editing SFTP/SSH settings

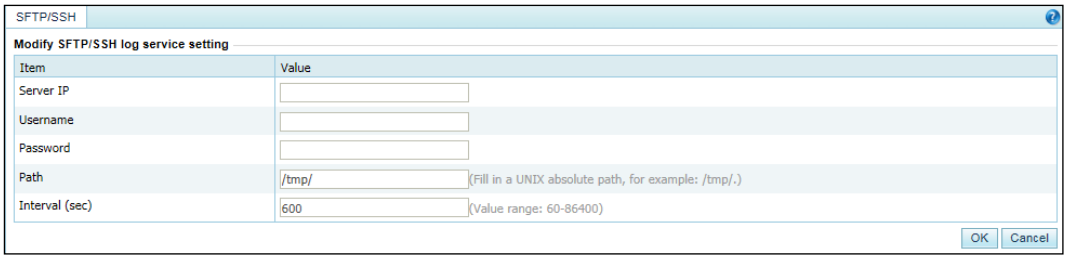


Table 3-22 describes parameters for exporting logs via SFTP or SSH.

Table 3-22 Parameters for exporting logs via SFTP or SSH

Parameter	Description
Server IP	IPv4 address of the SFTP/SSH server that receives logs from ADS. Note Currently, IPv6 addresses are not allowed.
Username	User name for logging in to the SFTP/SSH server.
Password	Password for logging in to the SFTP/SSH server.
Path	Path on the SFTP/SSH server for saving logs.
Interval(sec)	Interval (unit: second) for exporting logs via SFTP or SSH. The value ranges from 60 to 86400, that is, 1 minute to 1 day.

Step 3 Configure parameters and click **OK** to save the settings.

----End

3.4 Others

This section covers the following topics:

- License
- System Update
- Remote Assistance
- SSL Certificate Import
- One-Click Information Collection
- Version Information
- Web API File Download

3.4.1 License

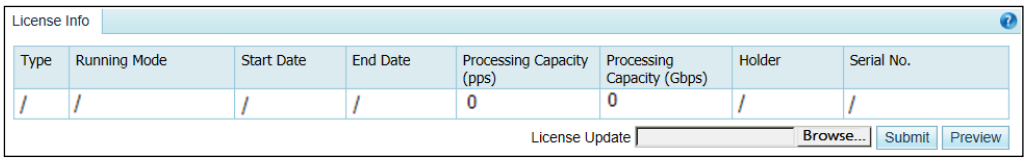
ADS licenses fall into the following types:

- **Trial**: After this type of license expires, users cannot continue to use ADS.
- **Paid**: After this type of license expires, users can still use ADS, but cannot update it.

After ADS is installed, you need to import a license before using it. After a successful import, license information is displayed.

Choose **System** > **Others** > **License Info**. The initial license information page appears, as shown in Figure 3-62.

Figure 3-62 License Info page before the import of a license



After a license is imported, license information is displayed, as shown in Figure 3-63.

Figure 3-63 License Info page after the import of a license

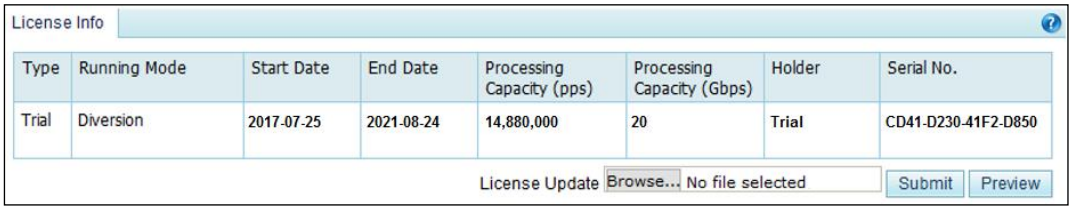


Table 3-23 describes ADS device license parameters.

Table 3-23 ADS device license parameters

Parameter	Description
Type	Two values are available: **Trial** and **Paid**.
Running Mode	Four values are available: **In-path**, **Cluster probe**, **Diversion**, and **In-path cluster**.
Start Date	Date when the license is produced.

Parameter	Description
	Note The current service indicates the authorized ADS upgrade service.
End Date	Date when the license is terminated. If a trial license expires, you cannot update ADS, which will later work in packet forwarding mode without providing any protection. If a paid license expires, you cannot update ADS, which will still provide protection. Note The current service indicates the authorized ADS upgrade service.
Processing Capacity (pps)	Maximum number of packets that ADS can process per second.
Processing Capacity (Gbps)	Maximum bandwidth for traffic cleaning. Note If the traffic exceeds the specified maximum bandwidth, ADS will log a system operation alert message.
Holder	Customer who owns the current ADS device.
Serial No.	Serial number of the current ADS device.

On the **License Info** page, you can perform the following operations:

- Previewing a license

  To the lower right of the license information table, click **Browse t**o select a license file from a local disk drive and then click **Preview** to preview details about the file.

- Importing a license

  To the lower right of the license information table, click **Browse** to select a license file from a local disk drive and then click **Submit** to import it. After the license is imported, it takes effect immediately. You can refresh the page to update license information.

Note	• To get a license file, contact NSFOCUS technical support. • The license file name cannot contain special characters or Chinese characters.

3.4.2 System Update

You can manually import the update file to update ADS.

Note	If the version of the update package is equal to or earlier than the current version, the system cannot be updated.

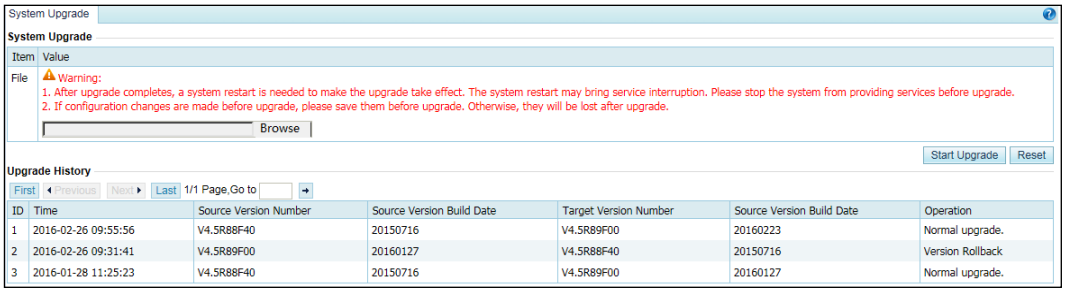
To update ADS, perform the following steps:

Step 1 Contact NSFOCUS technical support for ADS update packages.

Make sure that the package matches your product.

Step 2 Choose **System** > **Others** > **System Upgrade**.

Figure 3-64 System Upgrade page

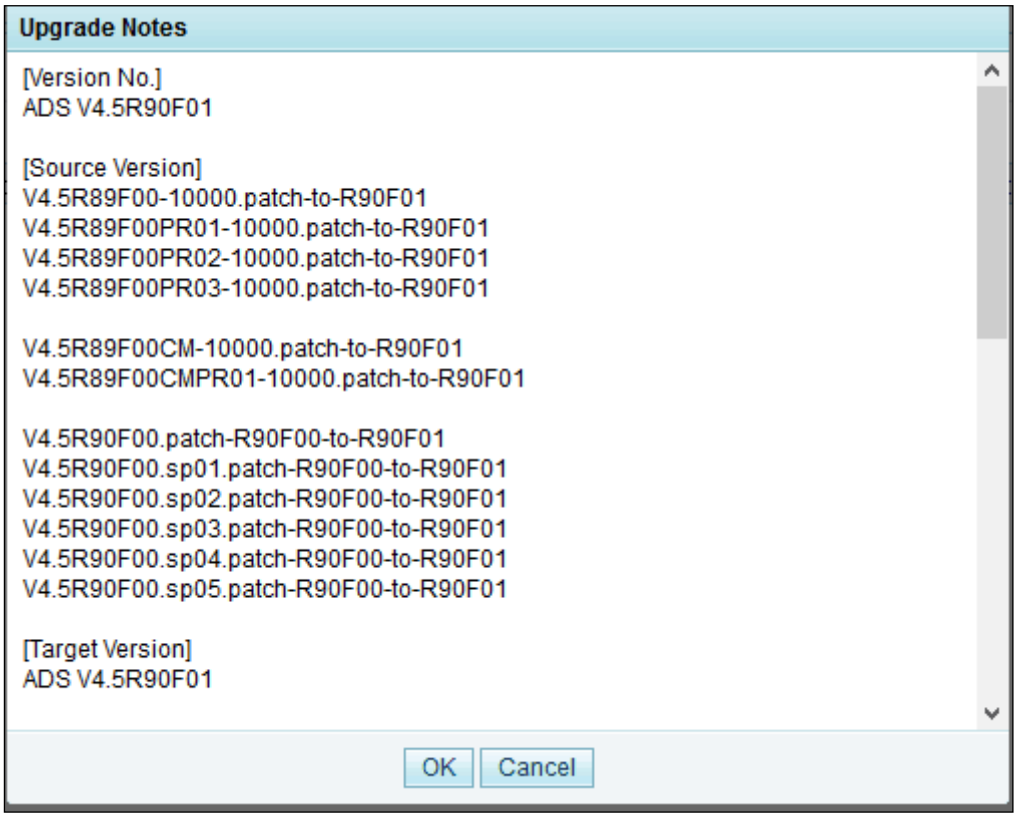


Step 3 Click **Browse** and select the desired update package.

The **Upgrade Notes** page appears.

Note	This page appears only when the source version is V4.5R89F03 or later.

Figure 3-65 Upgrade notes page



Step 4 Click **OK** to start updating the device.

Note	The update process may take a long time. Wait until an update success message appears. If problems emerge after the update and version rollback is needed, the system can only be rolled back to the source version. For details, see section 10.2.9 Rolling Back the Version.

Step 5 After an update success message appears, restart the system as prompted.

Note	If you do not restart the system at this moment, clicking **Save** in the right-upper corner of the page will not work. If you need to save settings previously configured, you must restart the system. Alternatively, you can save the settings before updating the system.

Step 6 Re-log in to the system, and choose **System** > **Others** > **System Upgrade** to view version information and check whether the update succeeds.

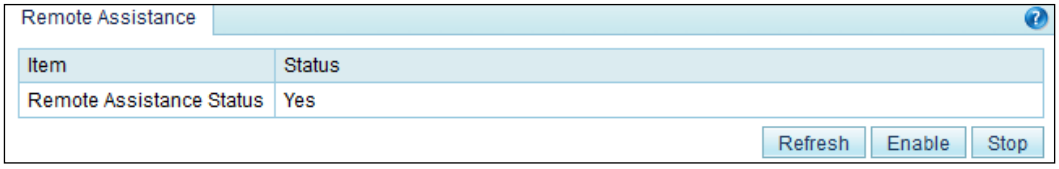
Alternatively, you can view the current version information in the **Upgrade History** table in the **System Upgrade** page shown in Figure 3-64.

----End

3.4.3 Remote Assistance

When a failure occurs in the system, you may need to contact NSFOCUS technical support for remote assistance. For this purpose, enable remote assistance on the **Remote Assistance** page shown in Figure 3-66. This function is disabled by default. For this function, SSH is used for remote login, running on port 22.

Figure 3-66 Remote assistance



Meanings of the buttons are as follows:

- **Refresh**: shows the status of the current remote assistance service.
- **Enable**: enables the remote assistance service.
- **Stop**: stops the remote assistance service.

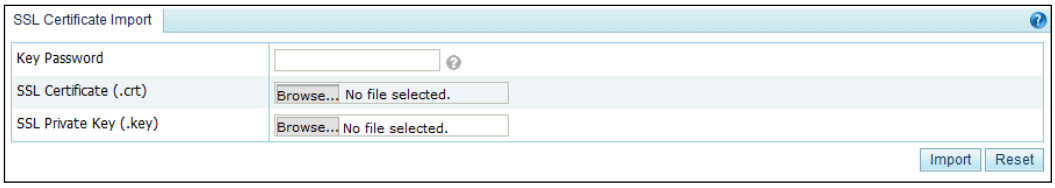
3.4.4 SSL Certificate Import

The SSL certificate can be imported manually. After the certificate is successfully imported, the system automatically restarts the web server to make the new certificate take effect.

To import the SSL certificate, perform the following steps:

Step 1 Choose **System** > **Others** > **SSL Certificate Import**.

Figure 3-67 SSL Certificate Import page



Step 2 Browse respectively to the SSL certificate file and private key file and then click **Import** to import the SSL certificate.

If a password is set for the private key of the SSL certificate to be imported, type the correct password before the certificate import.

After the import succeeded, the system displays the message "Succeeded in importing the SSL certificate. The web server is restarting … Please refresh the page later."

----End

3.4.5 One-Click Information Collection

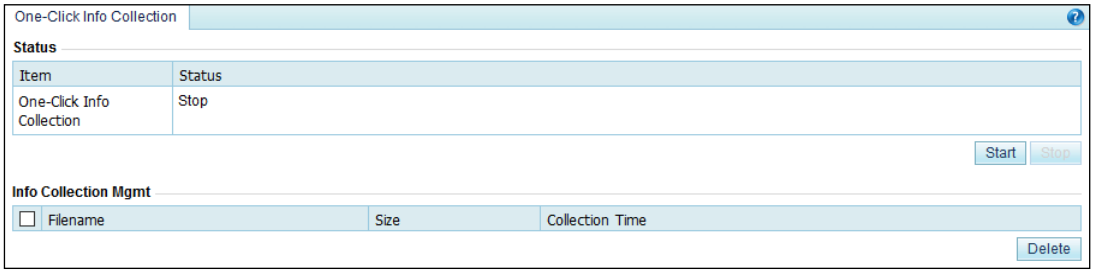
When ADS fails, you can collect device information by using the one-click information collection function, and deliver such information to NSFOCUS technical support, who therefore do not need to log in to ADS for collection of such information.

The one-click information collection function collects system configuration information, system status information, and logs and generates a related **.info** file.

To collect the preceding information, perform the following steps:

Step 1 Choose **System** > **Others** > **One-Click Info Collection**.

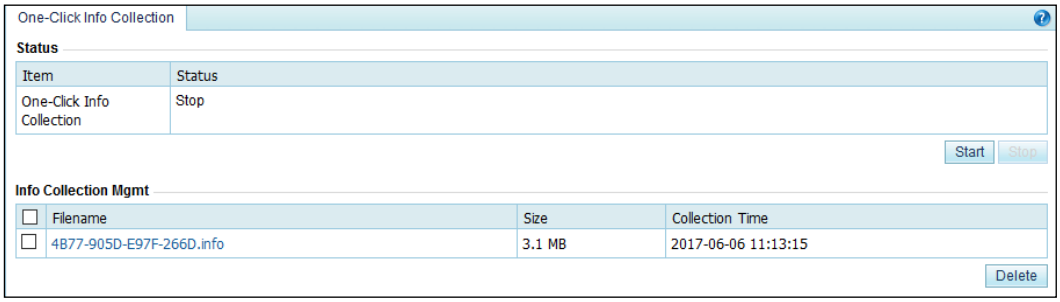
Figure 3-68 One-Click Info Collection page



Step 2 Click **Start** to start collecting device information.

After fault information is successfully collected, an informatio n file is displayed in the **Info Collection Mgmt** list, as shown in Figure 3-69.

Figure 3-69 One-click information collection result



Step 3 Click the file name in the **Filename** column and download it to a local disk drive.

You can then send this file to NSFOCUS technical support for troubleshooting.

----End

3.4.6 Version Information

Choose **System** > **Others** > **Version Info**. The **Version Info** page displays the version number and the email address of NSFOCUS technical support, as shown in Figure 3-70.

Figure 3-70 Version information

Version Info

Item	Value
Version	V4.5R90F00
Build Date	20171117
Email	support@nsfocus.com

3.4.7 Web API File Download

You can download the web API file that describes API communication interfaces from the web-based manager of ADS.

Choose **System > Others > Web API File Download**.

On the page shown in Figure 3-71, you can click a file name in the **Files for Download** area to download the file to a local disk drive.

Figure 3-71 Web API File Download page

Web API File Download

Files for Download

NSFOCUS ADS V4.5R89F03 Web API Description.pdf

4 Real-Time Monitoring

The real-time monitoring module provides real-time traffic information and attack information for you to have a full understanding of the current network status.

This chapter details real-time monitoring information, as shown in the following table.

Section	Description
Real-Time System Status	Describes real-time monitoring traffic of the system.
System Information	Describes basic current system operating information.

4.1 Real-Time System Status

The system monitors incoming and outgoing traffic, attack traffic, and interface status and displays monitoring information in real time.

This section covers the following topics:

- Traffic Trend
- Attack Traffic Trend
- Top 10 Ongoing Attack Events
- System Resources
- Collaboration Status
- System Interfaces

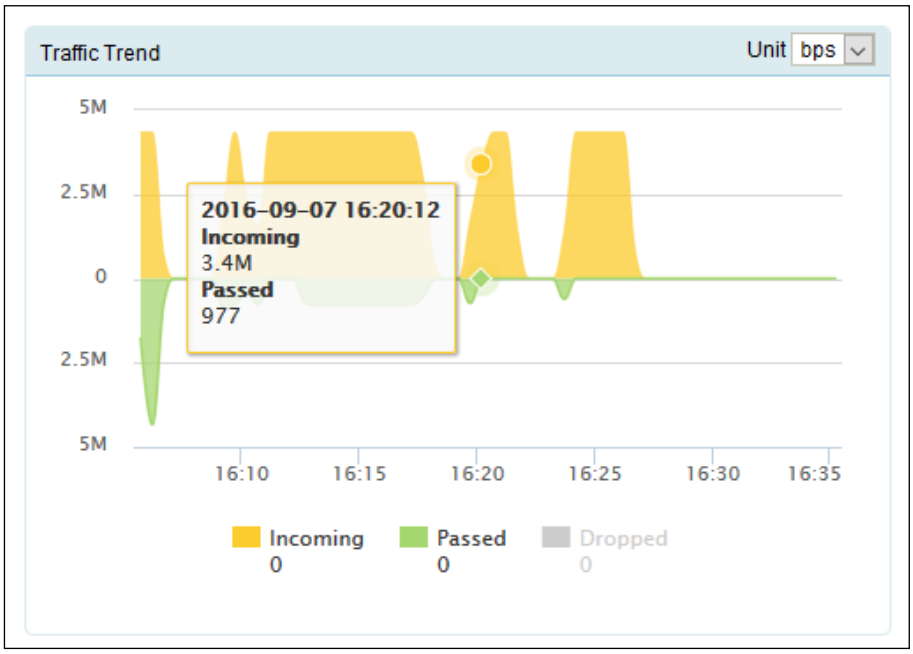
Traffic Trend

On the **Real-Time Monitoring** page, the **Traffic Trend** area shows the incoming and outgoing traffic and dropped traffic of the ADS device in the last 30 minutes, as shown in Figure 4-1. Here, the orange curve indicates the trend of incoming traffic, the green curve indicates the trend of outgoing traffic, and the red curve indicates the trend of dropped traffic. The traffic curves are automatically updated every 30 seconds.

When pointing to a traffic graph, you can view the incoming traffic, outgoing traffic, and dropped traffic at a specific time. For example, at 16:20:12 on September 7, 2016, the incoming traffic is 3.4 Mbps, outgoing traffic is 977 bps, and dropped traffic is 0 bps.

You can select the traffic unit from the **Unit** drop-down box in the upper-right corner of this area.

Figure 4-1 Traffic graph curves



Attack Traffic Trend

On the **Real-Time Monitoring** page, the **Attack Traffic** area presents the attack traffic dropped by the current ADS device in the last 30 minutes, as shown in Figure 4-2. When pointing to the traffic graph, you can view the dropped traffic at a specific time. For example, at 17:12:33 on August 7, 2018, the chargen amplification attack traffic is 914.4 kbps.

Table 4-1 shows mappings between attack traffic types and curve colors.

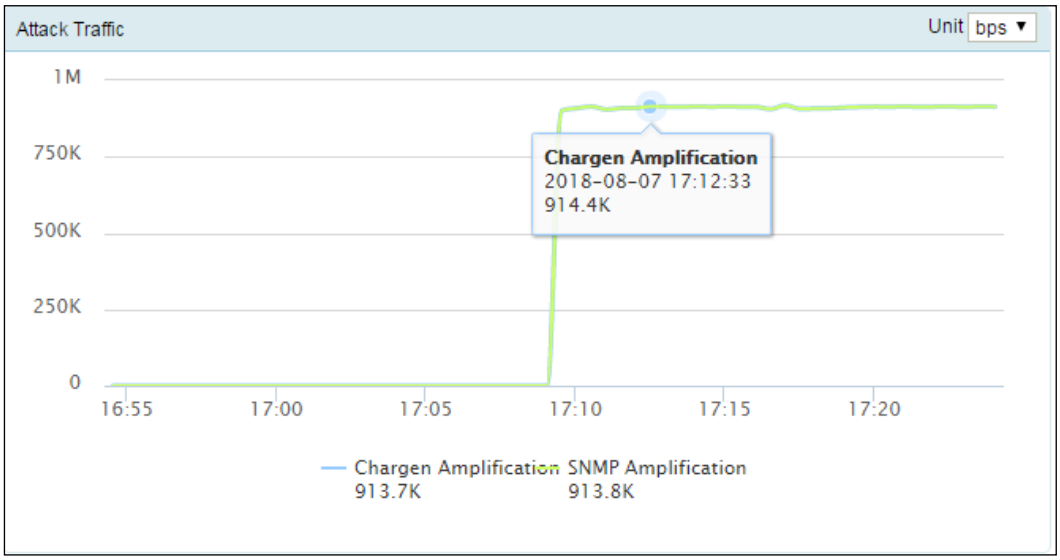
Table 4-1 Mappings between attack types and curve colors

Attack Type	Color Indication
SYN flood	SYN Flood
ACK flood	ACK Flood
UDP flood	UDP Flood
ICMP flood	ICMP Flood
TCP misuse	TCP Misuse
TCP connection flood	TCP Connection Flood
TCP fragment	TCP Fragment
ICMP fragment	ICMP Fragment

Attack Type	Color Indication
HTTP flood	HTTP Flood
HTTPS flood	HTTPS Flood
SIP flood	SIP Flood
DNS query flood	DNS Query Flood
DNS amplification	DNS Amplification
SSDP amplification	SSDP Amplification
NTP amplification	NTP Amplification
Chargen amplification	Chargen Amplification
SNMP amplification	SNMP Amplification
Memcache amplification	Memcache Amplification
Manual strategy	Manual Strategy
Amplification	Amplification
UDP fragment	UDP Fragment
DNS flood	DNS Flood
LAND flood	LAND Flood
HTTP slow attack	HTTP Slow Attack
FIN/RST flood	FIN/RST Flood

You can select the traffic unit from the **Unit** drop-down box in the upper-right corner of this area.

Figure 4-2 Attack traffic trend graph

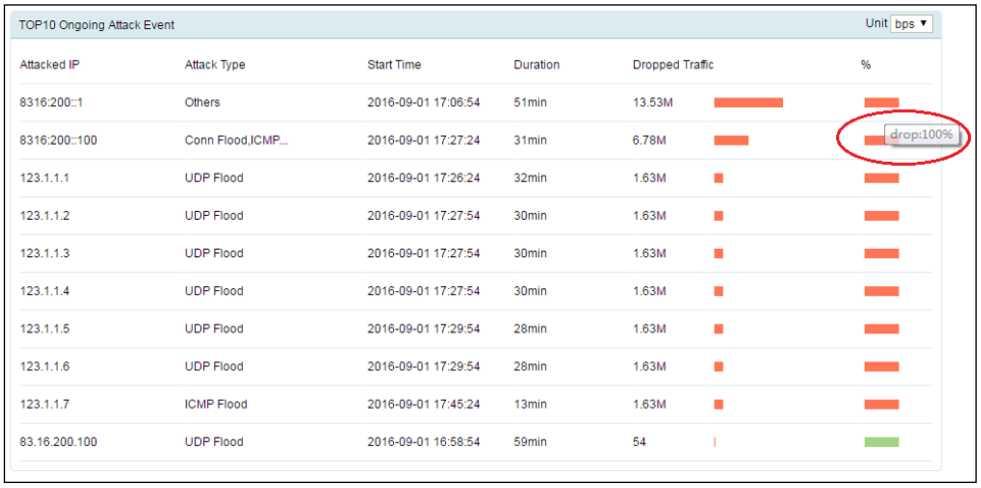


Top 10 Ongoing Attack Events

On the **Real-Time Monitoring** page, the **TOP10 Ongoing Attack Event** area shows information about top 10 traffic attack events, including the attack IP address, attack type, start time, duration, dropped traffic, and percentage of dropped traffic. Such top attack events are sorted in the descending order of dropped traffic. When pointing to the percentage column of an attack event, you can check the percentage of dropped traffic to the total traffic of the destination IP address. As shown in Figure 4-3, the percentage of the first attack event is 0%.

You can select the traffic unit from the **Unit** drop-down box in the upper-right corner of this area.

Figure 4-3 Top 10 ongoing attack events



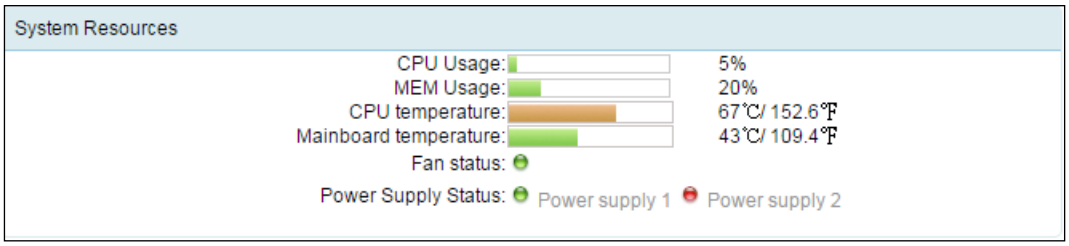
Attacked IP	Attack Type	Start Time	Duration	Dropped Traffic	%
8316:200::1	Others	2016-09-01 17:06:54	51min	13.53M	
8316:200::100	Conn Flood,ICMP...	2016-09-01 17:27:24	31min	6.78M	
123.1.1.1	UDP Flood	2016-09-01 17:26:24	32min	1.63M	
123.1.1.2	UDP Flood	2016-09-01 17:27:54	30min	1.63M	
123.1.1.3	UDP Flood	2016-09-01 17:27:54	30min	1.63M	
123.1.1.4	UDP Flood	2016-09-01 17:27:54	30min	1.63M	
123.1.1.5	UDP Flood	2016-09-01 17:29:54	28min	1.63M	
123.1.1.6	UDP Flood	2016-09-01 17:29:54	28min	1.63M	
123.1.1.7	ICMP Flood	2016-09-01 17:45:24	13min	1.63M	
83.16.200.100	UDP Flood	2016-09-01 16:58:54	59min	54	

System Resources

On the **Real-Time Monitoring** page, the **System Resources** area shows the status of various system resources in real time, including the CPU usage, memory usage, CPU temperature, mainboard temperature, fan status, and power supply status. For fan status and power supply status, indicates that the fans or power supply works properly and indicates the opposite.

Note	The power supply status is displayed only for some ADS NX5-8000 devices.

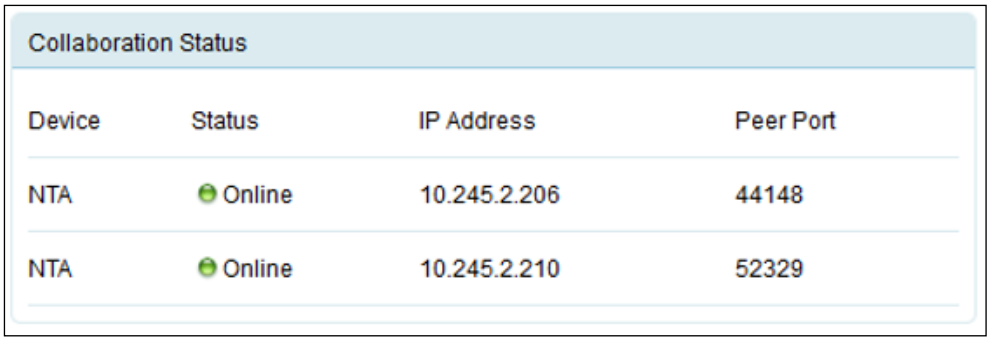
Figure 4-4 System resources



Collaboration Status

On the **Real-Time Monitoring** page, the **Collaboration Status** area shows the status of collaboration between the current ADS and another device. Figure 4-5 shows the status of collaboration between ADS and NSFOCUS NTA. indicates that the device collaborating with ADS is online. If the device is offline, it will not be listed here.

Figure 4-5 Collaboration status



Interface Status

On the **Real-Time Monitoring** page, the **System Interfaces** area shows the connection status of interfaces on ADS (means "online"; means "offline"), and real-time traffic (both

pps and bps) of each interface. **Total** indicates total traffic of all interfaces. The information is automatically updated every 10 seconds.

By default, information about all interfaces is displayed. As shown in Figure 4-6, clicking **Display Online Interfaces** in the drop-down box in the upper-left corner displays information only about online interfaces.

Figure 4-6 Interface status of ADS

System Interfaces — Display All Interfaces

Interface	Status	IN(pps)	OUT(pps)	IN(bps)	OUT(bps)
T1/1	Up	0	0	0	0
T1/2	Up	0	0	0	0
T2/1	Down	0	0	0	0
T2/2	Down	0	0	0	0
T3/1	Down	0	0	0	0
T3/2	Down	0	0	0	0
G4/1	Up	0.2	0.2	154	127
G4/2	Up	0	0	0	0
G4/3	Up	2K	0	1.8M	0
G4/4	Down	0	0	0	0
G4/5	Up	1.2	0.7	970	462
G4/6	Down	0	0	0	0
G4/7	Down	0	0	0	0
G4/8	Down	0	0	0	0
Total		2K	0.9	1.8M	589

The number and type of interfaces vary with device models. Interfaces on the device that you are using may be different from those described here.

4.2 System Information

All users can view system information. The status bar displays basic system information, including hardware CPU and memory usage, system version, system uptime, and system time, as shown in Figure 4-7.

The green indicator ( ) indicates that the device works properly and the red indicator ( ) indicates that the device works improperly.

Figure 4-7 System information

5 Policies

This chapter details protection policies.

Section	Description
Anti-DDoS Policies	Describes how to configure anti-DDoS policies.
Access Control Policies	Describes how to configure access control policies.

5.1 Anti-DDoS Policies

This section covers the following topics:

- Default Anti-DDoS Parameters
- Policy Configuration for Protection Groups
- Protection Group Management
- Advanced Global Parameters
- Response Page Settings
- Policy Auto-Learning
- SSL Certificate Management

5.1.1 Default Anti-DDoS Parameters

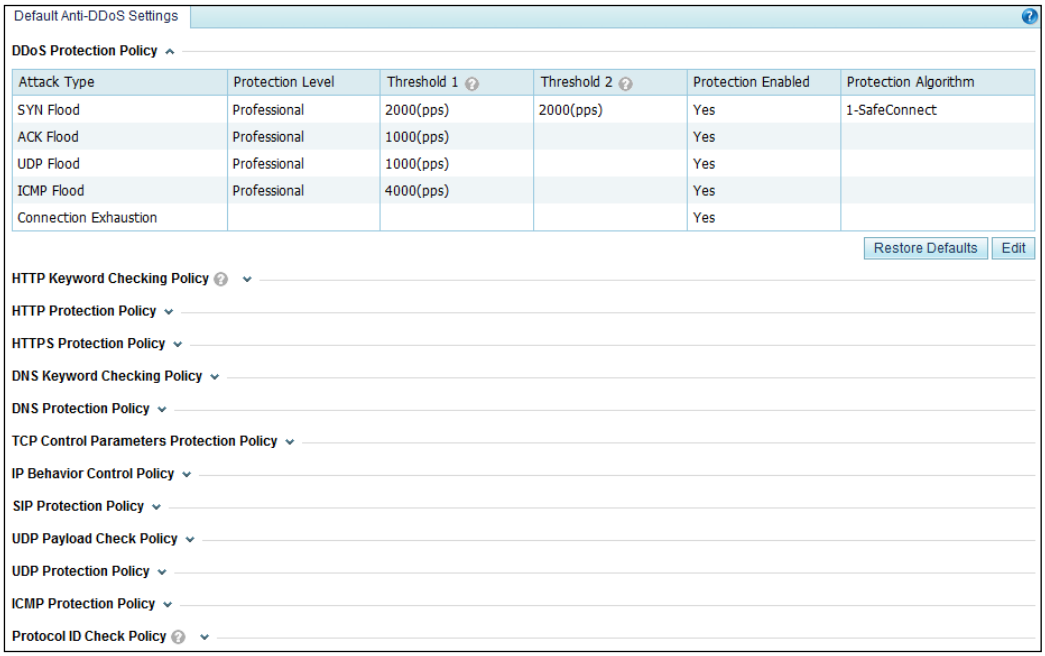
Default anti-DDoS policies include the following:

- DDoS Protection Policy
- HTTP Keyword Checking Policy
- HTTPS Protection Policy
- HTTP Protection Policy
- DNS Keyword Checking Policy
- DNS Protection Policy
- TCP Control Parameters Protection Policy
- IP Behavior Control Policy
- SIP Protection Policy
- UDP Payload Check Policy
- UDP Protection Policy

- ICMP Protection Policy
- Protocol ID Checking Policy

Choose **Policies > Anti-DDoS > Default Anti-DDoS Settings**. On the **Default Anti-DDoS Settings** page, you can click **Edit** to edit a default policy or **Restore Defaults** to restore a default policy.

Figure 5-1 Default Anti-DDoS Settings page

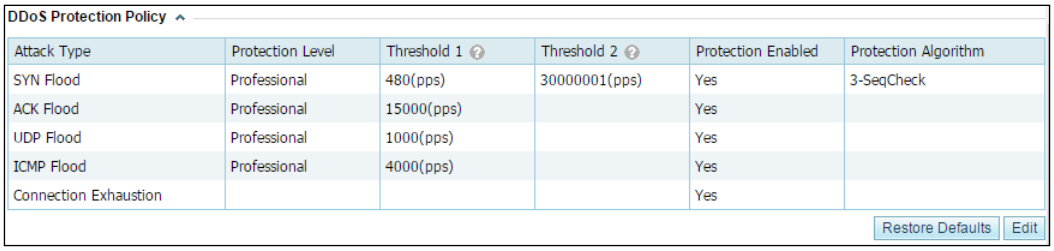


5.1.1.1 DDoS Protection Policy

An anti-DDoS policy is a policy for protection against DDoS attacks.

Figure 5-2 shows parameters of the default anti-DDoS policy.

Figure 5-2 DDoS Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-3.

Figure 5-3 Editing the default anti-DDoS policy

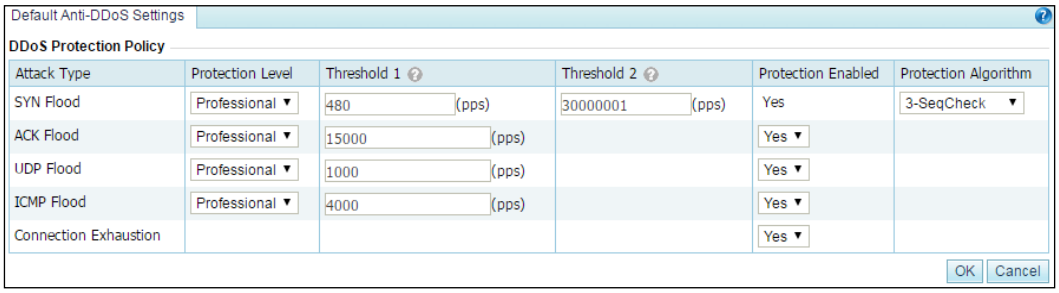


Table 5-1 describes parameters of the DDoS protection policy.

Table 5-1 Parameters of the default anti-DDoS policy

Parameter	Description
Attack Type	Types of DDoS attacks that can be blocked.
Protection Level	Priority for blocking attacks. Two values are available: **Default** and **Professional**. Thresholds in **Default** mode are predefined by the system and thus cannot be changed, while thresholds in **Professional** mode can be changed as required.
Threshold 1	The value varies with DDoS attack types. See the following descriptions.
Threshold 2	The value varies with DDoS attack types. See the following descriptions.
Protection Enabled	Controls whether to enable the protection. • **Yes**: enables this type of protection. • **No**: disables this type of protection.
Algorithm	Different algorithms are adopted to defend against different types of DDoS attacks. See the following descriptions.

SYN Flood

- **Threshold 1**: specifies the SYN traffic rate above which SYN flood protection is triggered. If the rate (pps) of SYN traffic to a destination exceeds the specified value, SYN flood protection is triggered. The value ranges from 0 to 48000000. You can configure this parameter only when the protection level is set to **Professional**. For the **Default** protection level, the predefined value is used and cannot be changed.
- **Threshold 2**: specifies the rate above which ADS sends reverse detection packets in response to SYN packets, after SYN flood protection is triggered. The value ranges from 1 to 240000000. A greater value means a better protection effect but a higher load on the ADS device. You can configure this parameter only when the protection level is set to **Professional**. For the **Default** protection level, the predefined value is used and cannot be changed.

Note	• Reverse detection indicates that the ADS device detects whether a client is launching attacks by sending detection packets to the client. • A greater **Threshold 2** value may cause higher CPU usage. You are advised to limit the CPU usage below 55%.

- **Protection Enabled**: By default, SYN flood protection is enabled and cannot be disabled.
- **Algorithm**
  - **0-SynCheck** applies to symmetrical networks only**.**
  - **1-SafeConnect** and **2-DynaCheck** apply to both symmetrical and asymmetrical networks. When ADS is deployed in out-of-path mode, you can only select **1-SafeConnect** or **2-DynaCheck**.

ACK Flood

Threshold 1: specifies the ACK traffic rate above which ACK flood protection is triggered. If the rate (pps) of ACK traffic to a destination exceeds the specified value, ACK flood protection is triggered. The value ranges from 1 to 240000000. You can configure this parameter only when the protection level is set to **Professional**. For the **Default** protection level, the predefined value is used and cannot be changed.

Under most environments, you are advised to set the protection level to **Default**.

UDP Flood

Threshold 1: specifies the UDP traffic rate above which UDP flood protection is triggered. If the rate (pps) of UDP traffic to a destination exceeds the specified value, UDP flood protection is triggered. The value ranges from 0 to 48000000.

Under most environments, you are advised to set the protection level to **Default**.

ICMP Flood

Threshold 1: specifies the ICMP traffic rate above which ICMP flood protection is triggered. If the rate (pps) of ICMP traffic to a destination exceeds the specified value, ICMP flood protection is triggered. The value ranges from 0 to 48000000.

Under most environments, you are advised to set the protection level to **Default**.

Connection Exhaustion

Connection exhaustion protection can work only when connection exhaustion rules are configured. You can only select **Yes** or **No** for it. (For how to configure connection exhaustion rules, see section 5.2.7 Connection Exhaustion Rules.)

Note	• Generally, the system adopts default anti-DDoS settings. For professional settings, contact NSFOCUS technical support. • You should apply protection algorithms to the anti-DDoS policy according to the actual network environment and the deployment mode. Otherwise, network interruption may occur.

5.1.1.2 HTTP Keyword Checking Policy

HTTP keyword checking is a process by which ADS checks specific fields in HTTP attack traffic against keywords and then takes the specified action against those packets that match a rule.

Figure 5-4 shows the current HTTP keyword checking rules.

Note	• Under a default policy, at most 10 HTTP keyword checking rules can be referenced. • When multiple rules are referenced, the HTTP keyword checking policy matches attack packets with these rules in a top-down manner. In principle, the matching stops once a rule is hit. An administrator may need to adjust the rule sequence as required. • When multiple rules are hit, ADS performs protection based on the first rule.

Figure 5-4 HTTP Keyword Checking Policy area

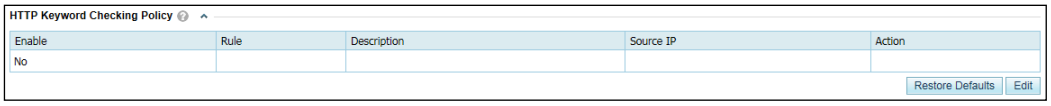


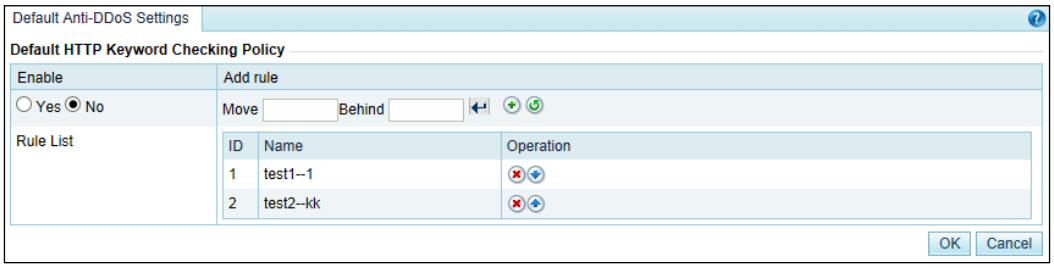
Table 5-2 describes parameters of the HTTP keyword checking policy.

Table 5-2 Parameters of the default HTTP keyword checking policy

Parameter	Description
Enable	Controls whether to enable the default HTTP keyword checking policy.
Rule	Name of each rule included in the policy.
Description	Brief description of each rule.
Source IP	Specifies the source IP address whose traffic will be checked against the default HTTP keyword checking policy.
Action	Specifies the action that ADS will take against the source IP address (host). For details, see section 5.2.6 HTTP Keyword Checking.

Click **Edit** to open the policy editing page.

Figure 5-5 Editing the default HTTP keyword checking policy

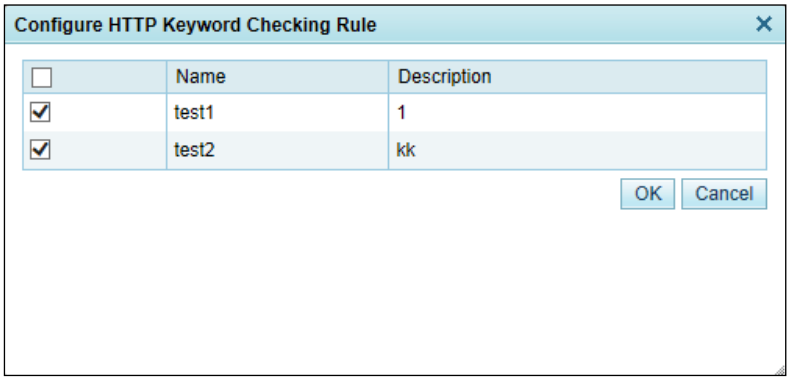


On this page, you can edit the HTTP keyword checking policy as follows:

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- Adjust rule sequence: Click or to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3** indicates that the first rule will be put under the third rule. Click to commit the change.
- **Add rule**: Click to open the rule configuration page. Select one or more rules and then click **OK**.

  For the creation of an HTTP keyword checking rule, see section 5.2.6 HTTP Keyword Checking.

Figure 5-6 Configuring HTTP keyword checking rules



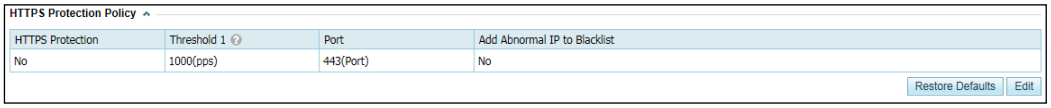
5.1.1.3 HTTPS Protection Policy

Note	This module does not support IPv6. Therefore, you can configure only IPv4 addresses here.

The default HTTPS protection policy is actually an HTTPS connection protection policy. With this policy, the system checks HTTPS packets from clients. When **Add Abnormal IP to**

Blacklist is set to **Yes**, the system adds source IP addresses that match the HTTPS protection algorithm to the blacklist. Figure 5-7 shows parameters of the HTTPS protection policy.

Figure 5-7 HTTPS Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-8.

Figure 5-8 Editing the default HTTPS protection policy

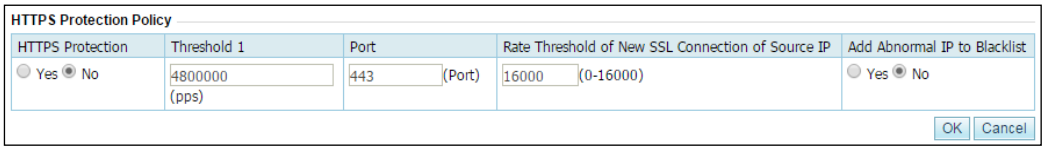


Table 5-3 describes parameters of the HTTPS protection policy.

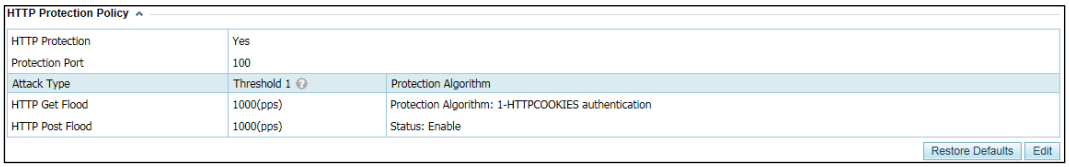
Table 5-3 Parameters of the HTTPS protection policy

Parameter	Description
HTTPS Protection	Controls whether to enable HTTPS protection.
Threshold 1	Specifies the HTTPS traffic rate, above which HTTPS protection is triggered. If the rate (pps) of HTTPS traffic to a destination exceeds the specified value, HTTPS protection is triggered. The value ranges from 0 to 48000000.
Port	Specifies the port to be protected. The value ranges from 0 to 65535, with **443** as the default. HTTPS protection is triggered only when the destination port number of attack packets matches the specified port. The port configured for the HTTP protection policy must be different from that for the HTTPS protection policy.
Rate Threshold of New SSL Connection of Source IP	Specifies the rate of new SSL connections of source IP addresses, above which HTTPS protection is triggered. The value range is 0–16000.
Add Abnormal IP to Blacklist	Controls whether to add abnormal IP addresses to the blacklist. The value **Yes** indicates that, when the IP address of a client fails the check with the HTTPS protection algorithm, the system will add this IP address to the blacklist.

5.1.1.4 HTTP Protection Policy

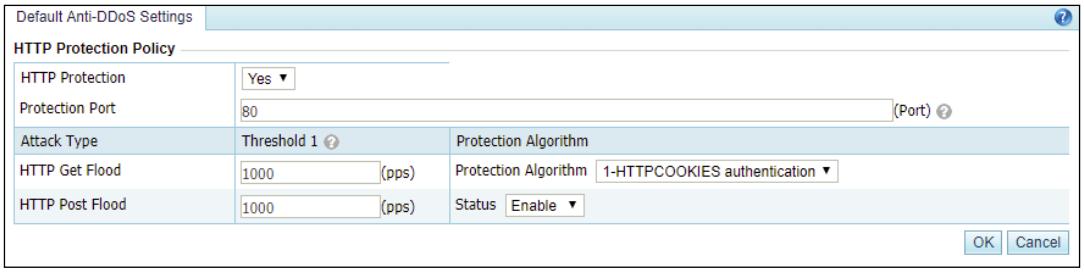
With the default HTTP protection policy, the system checks HTTP packets from clients and drops data that does not meet conditions specified in the policy. Figure 5-9 shows parameters of the default HTTP protection policy.

Figure 5-9 HTTP Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-10.

Figure 5-10 Editing the default HTTP protection policy



A default HTTP protection policy's parameters, varying with HTTP request methods, are described as follows:

Protection Port

This specifies the port number corresponding to the destination IP address of HTTP packets. A maximum of five ports or port ranges are allowed, which must be separated by the comma. The value range is 0–65535. The ports configured for the HTTP protection policy must be different from those for the HTTPS protection policy.

HTTP GET Flood

- **Threshold 1**: specifies the HTTP GET traffic rate above which HTTP GET flood protection is triggered. If the rate (pps) of HTTP GET traffic to a destination exceeds the specified value, HTTP GET flood protection is triggered. The value ranges from 0 to 48000000.
- **Protection Algorithm**:
  - **0_TAG authentication** and **1_HTTPCOOKIES authentication** verify the destination IP address by adding authentication information into HTTP packets.
  - **2_URL authentication** adds information similar to cookies into the URL request.
  - **3_ASCII image authentication** and **4_BMP image authentication** add a verification code.
  - **5_Dynamic script protection** performs verification by adding key values to URLs.

  The default algorithm is **1_HTTPCOOKIES authentication**. Select an algorithm as required.

HTTP POST Flood

Threshold 1: specifies the HTTP POST traffic rate above which HTTP POST flood protection is triggered. If the rate (pps) of HTTP POST traffic to a destination exceeds the specified value, HTTP POST flood protection is triggered. The value ranges from 0 to 48000000.

5.1.1.5 DNS Keyword Checking Policy

DNS keyword checking is a process by which ADS checks specific fields in DNS attack traffic against keywords and then takes the specified action against those packets that match a rule.

Figure 5-11 shows about the current DNS keyword checking rules.

Note	• Under a default policy, at most 10 DNS keyword checking rules can be referenced. • When multiple rules are referenced, the DNS keyword checking policy matches attack packets with these rules in a top-down manner. In principle, the matching stops once a rule is hit. An administrator may need to adjust the rule sequence as required. • When multiple rules are matched, ADS performs protection based on the first rule.

Figure 5-11 DNS Keyword Checking Policy area

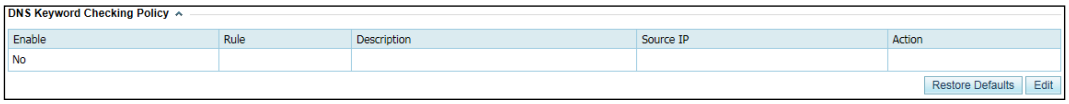


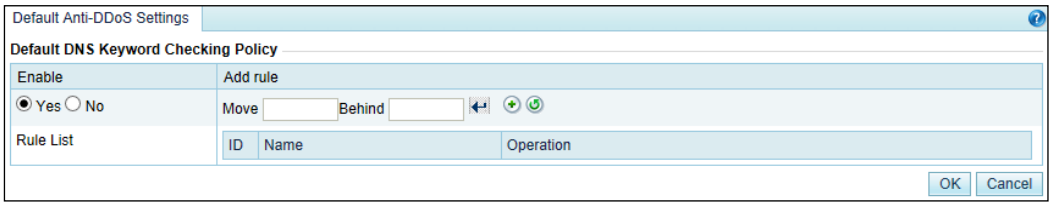
Table 5-4 describes parameters of the DNS keyword checking policy.

Table 5-4 Parameters of the default DNS keyword checking policy

Parameter	Description
Enable	Controls whether to enable the default DNS keyword checking policy.
Rule	Name of each rule included in the policy.
Description	Brief description of each rule.
Source IP	Specifies the source IP address from which traffic will be checked against the default DNS keyword checking policy.
Action	Specifies the action that ADS will take against the source IP address (host). For details, see section 5.2.5 DNS Keyword Checking.

Click **Edit** to open the policy editing page.

Figure 5-12 Editing the default DNS keyword checking policy

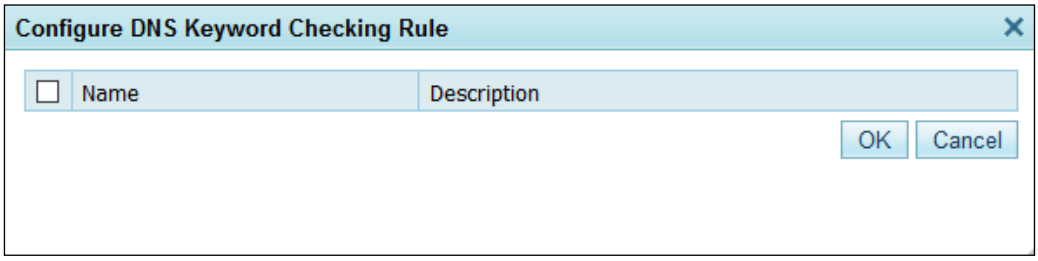


On this page, you can edit the DNS keyword checking policy as follows:

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- Adjust rule sequence: Click or to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3** indicates that the first rule will be put under the third rule. Click to commit the change.
- **Add rule**: Click to open the policy configuration page. Select one or more rules and then click **OK**.

  For the creation of a DNS keyword checking rule, see section 5.2.5 DNS Keyword Checking.

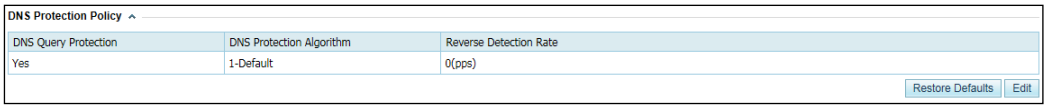
Figure 5-13 Configuring DNS keyword checking rules



5.1.1.6 DNS Protection Policy

DNS protection is a policy against DNS attacks and spoofing. Figure 5-14 shows the current DNS protection policy.

Figure 5-14 DNS Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-15.

Figure 5-15 Editing the default DNS protection policy

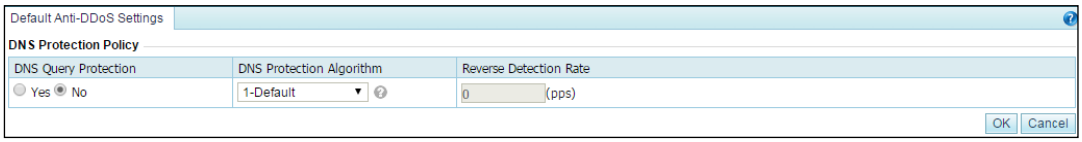


Table 5-5 describes parameters of the DNS protection policy.

Table 5-5 Parameters of the default DNS protection policy

Parameter	Description
DNS Query Protection	Controls whether to enable DNS query protection. **Yes** indicates that ADS can protect the DNS server on the intranet.
DNS Protection Algorithm	Specifies an algorithm for DNS protection. Options include **1-Default**, **2-TCP_BIT**, **3-DNS_CNAME, and 4-DNS retransmission.** **3-DNS_CNAME does not support IPv6.**
Reverse Detection Rate	Specifies the maximum rate of reverse detection packets. The value ranges from 1 to 240000000.

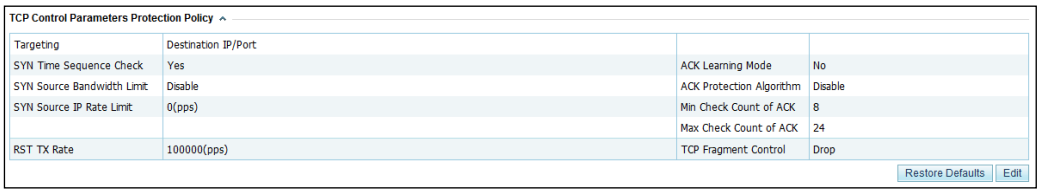
Note	DNS protection is triggered when the number of UDP packets transmitted per second exceeds the specified threshold. For the setting of UDP flood thresholds, see section 5.1.1.1 DDoS Protection Policy.

The default DNS protection settings are effective for general usage. To change the protection algorithm, contact technical support engineers of NSFOCUS.

5.1.1.7 TCP Control Parameters Protection Policy

Figure 5-16 shows parameters of the TCP control parameters protection policy.

Figure 5-16 TCP Control Parameters Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-17.

Figure 5-17 Editing the default TCP control parameters protection policy

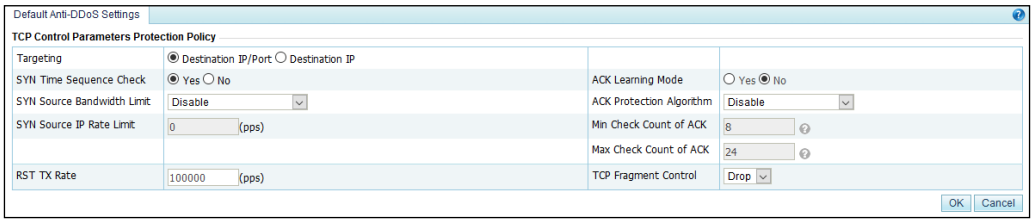


Table 5-6 describes parameters of the TCP control policy.

Table 5-6 Parameters of the TCP control policy

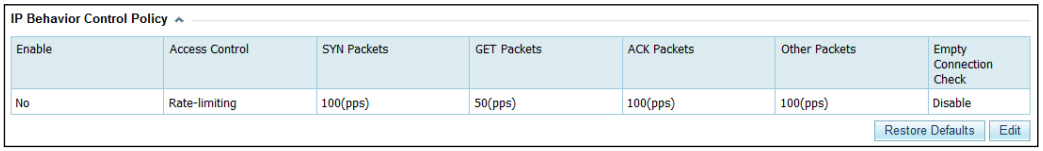
Parameter	Description
Targeting	Specifies how to identify a target server to be protected. • **Destination IP/Port**: indicates that the server to be protected is identified by the destination IP address and port. • **Destination IP**: indicates that the server to be protected is identified by only the destination IP address.
SYN Time Sequence Check	Controls whether to check the SYN time sequence.
SYN Source Bandwidth Limit	Works with **SYN Source IP Rate Limit** to limit the bandwidth used by the source host to send SYN packets. It has the following values: • **Disable**: disables this function. • **Drop and add to blacklist**: adds the IP address of the source host to the blacklist when the SYN packet forwarding rate of the source host exceeds the specified value. • **Drop**: drops subsequent packets when the SYN packet forwarding rate of the source host exceeds the specified value.
SYN Source IP Rate Limit	Works with **SYN Source Bandwidth Limit** to specify the maximum packet forwarding rate (pps) for the source host of SYN packets. The value ranges from 1 to 2000000.
ACK Learning Mode	Controls whether to enable the ACK learning mode. The ACK learning mode can be enabled only when **Protection Enabled** is set to **No** in the **DDoS Protection Policy** area on the **Default Anti-DDoS Settings** page. After the ACK learning mode is enabled, the system learns the packets sent by the client and adds the source IP addresses meeting the specified conditions to the trust list. The ACK learning mode takes effect only when **Protection Enabled** is set to **No** for both SYN flood attacks and ACK flood attacks in the **DDoS Protection Policy** area on the **Default Anti-DDoS Settings** page.
ACK Protection Algorithm	When ACK flood protection is enabled, you can configure the ACK protection algorithm, which can be **Disable**, **Time Sequence Check**, or **ACK Check**, with **Disable** as the default value. • **Disable**: indicates that the default algorithm will be used for ACK protection. • **ACK Check**: indicates that the packets properly responding to the ACK check will be allowed through. Otherwise, these packets will be dropped.

Parameter	Description
	• **Time Sequence Check**: For two identical ACK packets, if their sending interval is between **Min Check Count of ACK** and **Max Check Count of ACK**, they will be allowed through. Otherwise, they will be dropped.
Min Check Count of ACK	This parameter is used with **Max Check Count of ACK**. The value ranges from 1 to 300 (8 counts equals 1 second), with **8** as the default. The ACK packet check count of a client must be within the range. Otherwise, the client is deemed to have abnormal behaviors and will receive strict packet checks.
Max Check Count of ACK	This parameter is used with **Min Check Count of ACK**. The value ranges from 1 to 300 (8 counts equals 1 second), with **24** as the default. The ACK packet check count of a client must be within the range. Otherwise, the client is deemed to have abnormal behaviors and will receive strict packet checks.
RST TX Rate	Maximum TX rate of RST packets. The value ranges from 0 to 4000000, with **100000** as the default. The value **0** indicates that no RST packets are sent.
TCP Fragment Control	Controls whether to drop TCP fragments. • **Allow**: allows TCP fragments in IPv4 to pass through. • **Drop**: drops TCP fragments in IPv4.

5.1.1.8 IP Behavior Control Policy

The system regards source IP addresses of packets that have been authenticated with the DDoS protection policy as trusted IP addresses. However, to protect against DDoS attacks from trusted IP addresses, the system needs to further process packets from trusted IP addresses. This process is called "IP behavior control". By limiting the TX rate of source IP addresses whose packet forwarding rate exceeds the threshold or adding such IP addresses to the blacklist, the system can effectively defend against botnet attacks. Figure 5-18 shows IP behavior control parameters.

Figure 5-18 IP Behavior Control Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-19.

Figure 5-19 Editing the default IP behavior control policy

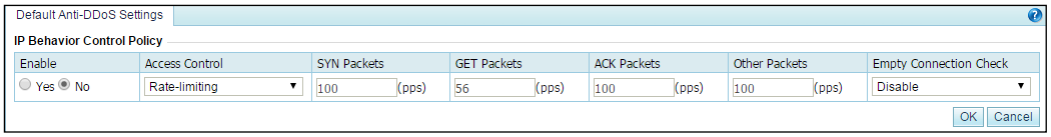


Table 5-7 describes IP behavior control parameters.

Table 5-7 IP behavior control parameters

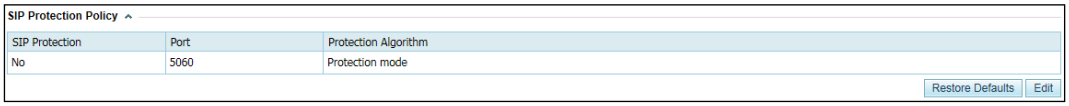
Parameter	Description
Enable	Controls whether to enable IP behavior control.
Access Control	Action the system takes to exert access control for trusted IP addresses whose packet forwarding rate (pps) exceeds the threshold. It has the following values: • **Rate-limiting**: limits the traffic rate. • **Drop and add to blacklist**: adds an IP address to the blacklist and block packets from this IP address when its traffic exceeds the specified value. To select this value, you must enable the blacklist function first. For details, see section 5.2.9 Blacklist.
SYN Packets	Specifies the maximum rate (pps) at which a trusted IP address can send SYN packets. The value ranges from 1 to 11840000. More SYN packets than allowed will be dropped and an attack event will be logged.
GET Packets	Specifies the maximum rate (pps) at which a trusted IP address can send GET packets. The value ranges from 1 to 11840000. More GET packets than allowed will be dropped and an attack event will be logged. Note This setting works only for ports specified in the default HTTP protection policy.
ACK Packets	Specifies the maximum rate (pps) at which a trusted IP address can send ACK packets. The value ranges from 1 to 11840000. More ACK packets than allowed will be dropped and an attack event will be logged.
Other Packets	Specifies the maximum rate (pps) at which a trusted IP address can send other packets than SYN, GET, and ACK packets. The value ranges from 1 to 11840000.
Empty Connection Check	Checks whether empty connections exist. It has the following values: • **Disable**: disables the empty connection check function. • **Drop and add to blacklist**: adds the IP address of the source host to the blacklist when the SYN or TCP packets are destined for an empty connection. • **Drop**: drops the current SYN or TCP packets that are destined for an empty connection. This function does not support IPv6. Therefore, you can use only IPv4 addresses when configuring this function.

5.1.1.9 **SIP Protection Policy**

Note	This module does not support IPv6. Therefore, you can use only IPv4 addresses during policy configuration.

With the SIP protection policy, the system provides protection against packets using the Session Initiation Protocol (SIP). Figure 5-20 shows parameters of the SIP protection policy.

Figure 5-20 SIP Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-21.

Figure 5-21 Editing the default SIP protection policy

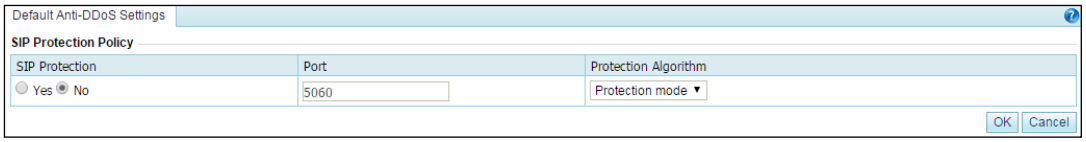


Table 5-8 describes parameters of the SIP protection policy.

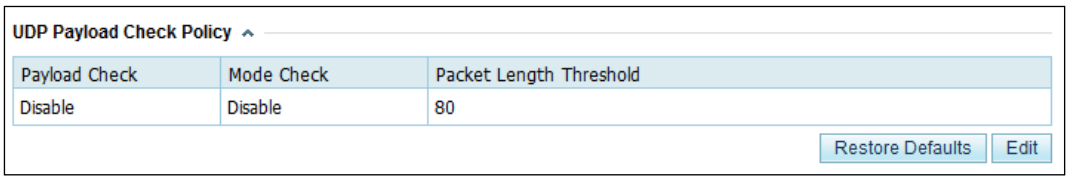
Table 5-8 Parameters of the default SIP protection policy

Parameter	Description
SIP Protection	Controls whether to enable the SIP protection policy.
Port	Port corresponding to the destination IP address. The value ranges from 0 to 65535, with **5060** as the default. SIP protection is triggered only when the destination port number of attack packets matches the specified port.
Protection Algorithm	Protection algorithm. If this parameter is set to **Protection mode**, the system performs protection against register attacks and invite attacks, and identifies attack packets via interaction with register and invite packets. If this parameter is set to **Learning mode**, the system performs protection against invite attacks. When a client sends an invite packet without any register packet, the system drops the invite packet.

5.1.1.10 UDP Payload Check Policy

With the UDP payload check policy, the system inspects the payload of UDP packets from clients and drops packets that do not meet specified conditions. Figure 5-22 shows UDP payload inspection parameters.

Figure 5-22 UDP Payload Check Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-23.

Figure 5-23 Editing the default UDP payload check policy

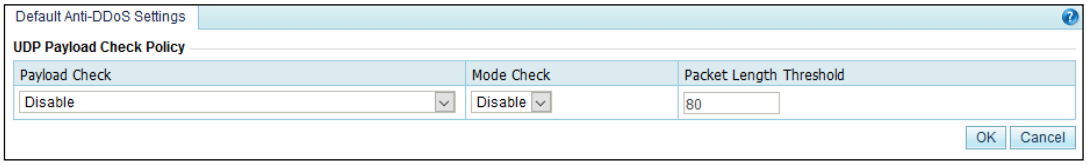


Table 5-9 describes UDP payload inspection parameters.

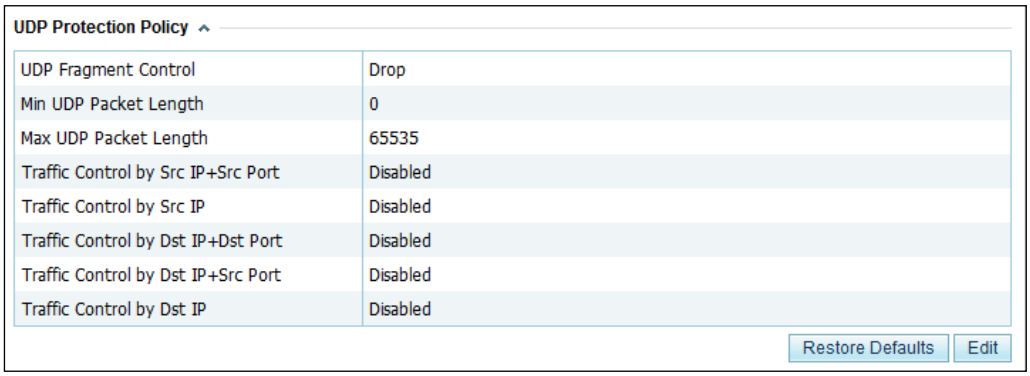
Table 5-9 UDP payload inspection parameters

Parameter	Description
Payload Check	Specifies whether to check the UDP payload and post-check actions. It has the following values: • **Disable**: disables UDP payload inspection. • **Discard UDP packets with payload length of 0**: drops packets whose payload length is 0. • **Discard UDP packets with payload length of 0 for attacked target**: drops packets whose payload length is 0 only when the target is being attacked.
Mode Check	Specifies whether to enable mode checks.
Packet Length Threshold	Maximum packet length. Based on this parameter value, ADS randomly selects several checkpoints where packets containing certain signatures are blocked.

5.1.1.11 UDP Protection Policy

With the UDP protection policy, the system checks UDP connection requests from clients, and drops requests that do not meet specified conditions. Figure 5-24 shows parameters of the default UDP protection policy.

Figure 5-24 UDP Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-25.

Figure 5-25 Editing the default UDP protection policy

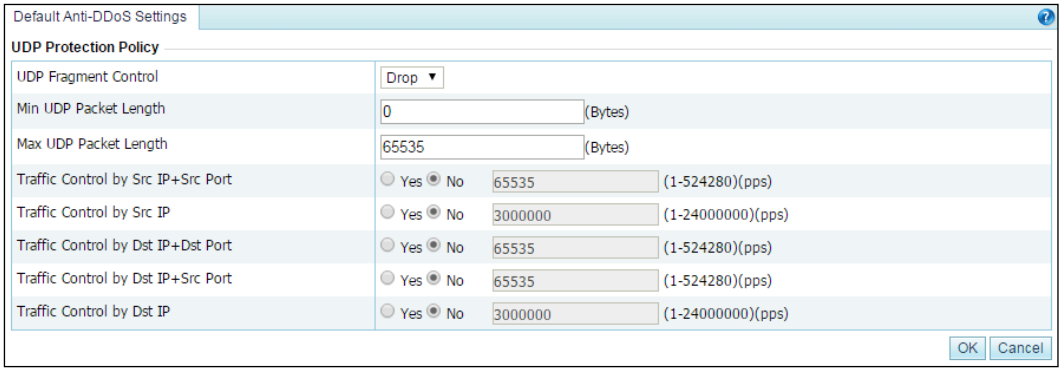


Table 5-10 describes parameters of the UDP protection policy.

Table 5-10 Parameters of the default UDP protection policy

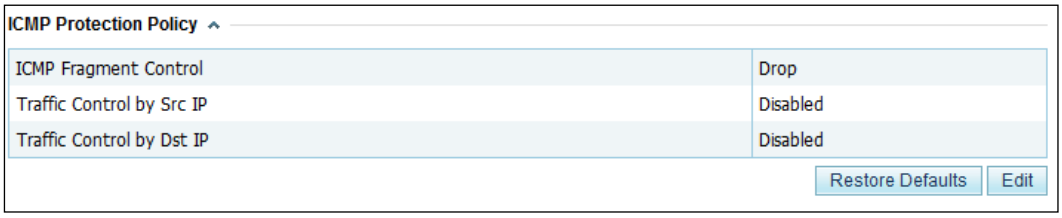
Parameter	Description
UDP Fragment Control	Controls whether to drop detected UDP fragments in IPv4. • **Allow**: allows UDP fragments to pass through. • **Drop**: drops UDP fragments.
Min UDP Packet Length	Specifies the minimum packet length in bytes. The system drops the packets that are below the defined minimum length. The value range is 0–65535, with **0** as the default value.
Max UDP Packet Length	Specifies the maximum packet length in bytes. The system drops the packets that are beyond the defined maximum length. The default value is **65535**.
Traffic Control by Src IP+Src Port	Specifies the maximum number of UDP fragments that are allowed to pass through per second with the same source IP address and source port. Excess UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–524280, with **65535** as the default value.

Parameter	Description
Traffic Control by Src IP	Specifies the maximum number of UDP fragments that are allowed to pass through per second with the same source IP address. Excess UDP fragments will be dropped. This parameter is enabled by default. The value range is 1–24000000, with **3000000** as the default value.
Traffic Control by Dst IP+Dst Port	Specifies the maximum number of UDP fragments that are allowed to pass through per second with the same destination IP address and destination port. Excess UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–524280, with **65535** as the default value.
Traffic Control by Dst IP+Src Port	Specifies the maximum number of UDP fragments that are allowed to pass through per second with the same destination IP address and source port. Excess UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–524280, with **65535** as the default value.
Traffic Control by Dst IP	Specifies the maximum number of UDP fragments that are allowed to pass through per second with the same destination IP address. Excess UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–24000000, with **3000000** as the default value.

5.1.1.12 ICMP Protection Policy

With the ICMP protection policy, the system checks ICMP connection requests from clients, and drops requests that do not meet specified conditions. Figure 5-26 shows parameters of the ICMP protection policy.

Figure 5-26 ICMP Protection Policy area



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-27.

Figure 5-27 Editing the default ICMP protection policy

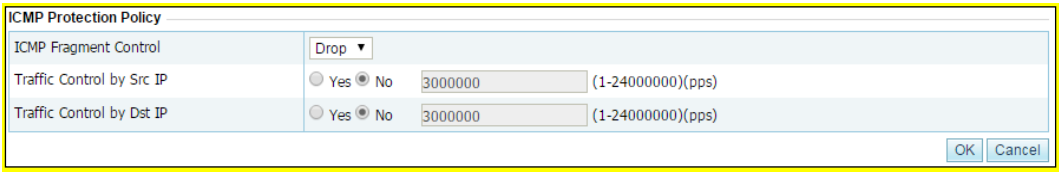


Table 5-11 describes parameters of the ICMP protection policy.

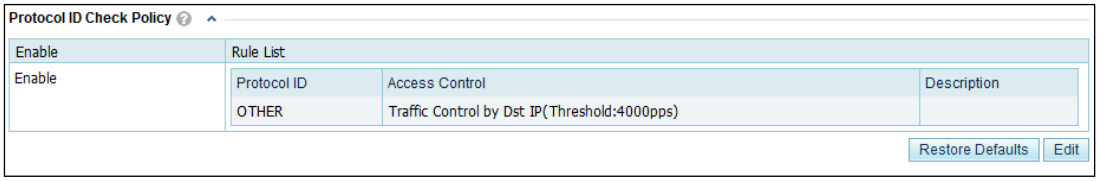
Table 5-11 Parameters of the ICMP protection policy

Parameter	Description
ICMP Fragment Control	Controls whether to drop the detected ICMP fragments. • **Allow**: allows ICMP fragments to pass through. • **Drop**: drops ICMP fragments.
Traffic Control by Src IP	Specifies the maximum number of ICMP fragments that are allowed to pass through per second from each source IP address. Excess ICMP fragments will be dropped. By default, it is disabled. The value range is 1–24000000, with **3000000** as the default value.
Traffic Control by Dst IP	Specifies the maximum number of ICMP fragments that are allowed to pass through per second to each destination IP address. Excess ICMP fragments will be dropped. By default, it is disabled. The value range is 1–24000000, with **3000000** as the default value.

5.1.1.13 Protocol ID Checking Policy

The protocol ID checking policy allows users to define different protection actions for other protocols than TCP, UDP, ICMP, and ICMPv6. Figure 5-28 shows protocol ID checking parameters. The checking rule with **Protocol ID** set to **OTHER** is predefined and cannot be deleted. For this rule, the default access control action is **Traffic Control by Dst IP** (the threshold is 4000 pps), which can also be set to **Allow**, **Drop**, or **Drop and add to blacklist**.

Figure 5-28 Protocol ID checking policy



You can click **Edit** to the lower right of the list to edit the parameters, as shown in Figure 5-29.

Figure 5-29 Editing the default protocol ID checking policy

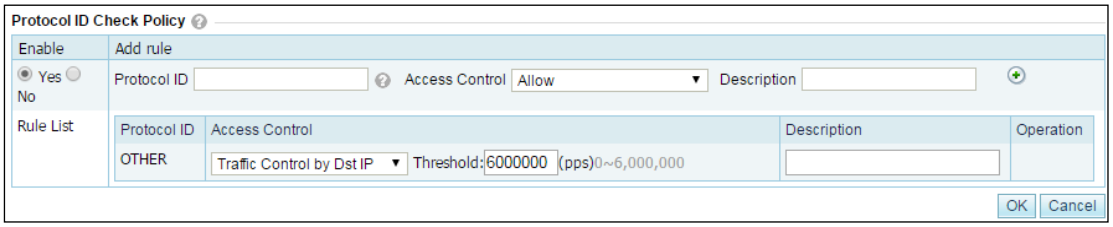


Table 5-12 describes parameters of a protocol ID checking policy.

Table 5-12 Parameters of a protocol ID checking policy

Parameter	Description
Enable	Controls whether to enable this policy. • **Yes**: enables this policy • **No**: disables this policy.
Protocol ID	Specifies the protocol ID which ranges from 0 to 255, excluding 1, 6, 17, and 58.
Access Control	Specifies the access control action applied to detected packets of this protocol ID, which can be one of the following: • **Allow**: allows packets of this protocol ID to pass through. • **Drop**: drops packets of this protocol ID. • **Drop and add to blacklist**: drops packets of this protocol ID and adds the source IP address of the packets to the blacklist. If **Protocol ID** is **OTHER**, **Access Control** can also be **Traffic Control by Dst IP** in addition to the preceding actions. **Threshold** specifies the maximum number of packets that are allowed to pass through per second with the same destination IP address. Excess packets will be dropped. The value range is 0–6000000, with **4000** as the default value.
Description	Brief information of this protocol ID checking rule. It cannot exceed 15 characters.

5.1.2 Policy Configuration for Protection Groups

A protection group is a collection of one or more customer's machines that are protected by ADS devices using the same policy.

In addition to all policies on the **Anti-DDoS Policy** page, group protection involves the following policies:

- Reflection protection policy
- TCP regular expression protection policy
- Port check policy
- UDP regular expression protection policy
- Watermark protection policy

Note that contents of DDoS protection policies, HTTPS protection policies, and HTTP protection policies for groups are different from those of the default anti-DDoS policies. The three types of policies are described in the following sections. For details on other policies, see section 5.1.1 Default Anti-DDoS Parameters.

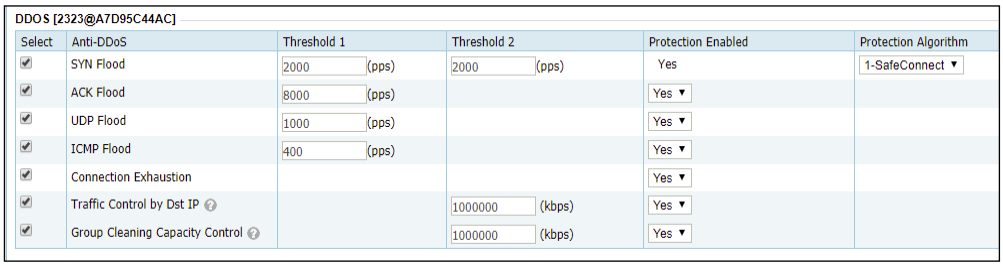
All policies, except the TCP regular expression protection policy and port check policy, are selected by default, indicating that these policies are enabled. Slow attack protection in the HTTP protection policy is disabled by default.

Note	The HTTPS protection policy, the 3-DNS algorithm 3 for DNS protection, the empty connection check function, and watermark protection for a protection group do not support IPv6. Therefore, you can type only IPv4 addresses when configuring the preceding.

5.1.2.1 DDoS Protection Policies

The DDoS protection policies are as shown in the following figure.

Figure 5-30 DDoS protection policies of a protection group



DDOS [2323@A7D95C44AC]

Select	Anti-DDoS	Threshold 1	Threshold 2	Protection Enabled	Protection Algorithm
☑	SYN Flood	2000 (pps)	2000 (pps)	Yes	1-SafeConnect
☑	ACK Flood	8000 (pps)		Yes	
☑	UDP Flood	1000 (pps)		Yes	
☑	ICMP Flood	400 (pps)		Yes	
☑	Connection Exhaustion			Yes	
☑	Traffic Control by Dst IP		1000000 (kbps)	Yes	
☑	Group Cleaning Capacity Control		1000000 (kbps)	Yes	

The DDoS protection policy module also involves the following protection functions:

- The function of traffic control by destination IP address controls the number of packets to an IP address. When **Protection Enabled** of **Traffic Control by Dst IP** is set to **Yes**, excess packets will be dropped.
- The group cleaning capacity control function controls the total number of packets to a group. When **Protection Enabled** of **Group Cleaning Capacity Control** is set to **Yes**, excess packets will be dropped.

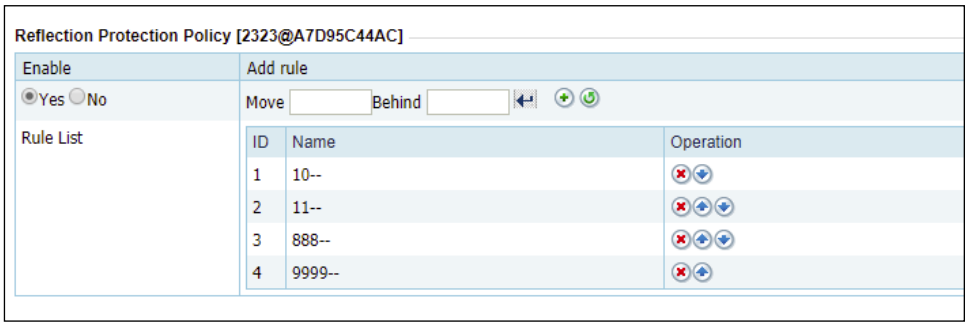
5.1.2.2 Reflection Protection Policy

If you have configured reflection protection rules, you can enable the reflection protection policy for a protection group and reference the created reflection protection rules. For details on reflection protection rules, see section 5.2.2.1 Creating a Reflection Protection Rule.

Figure 5-31 shows the reflection protection policy configuration of a protection group.

Note	• When multiple rules are referenced, the reflection protection policy matches attack packets with these rules in a top-down manner. In principle, the matching stops once a rule is hit. An administrator may need to adjust the rule sequence as required. • When multiple rules are matched, ADS performs protection based on the first rule.

Figure 5-31 Reflection protection policy of a protection group



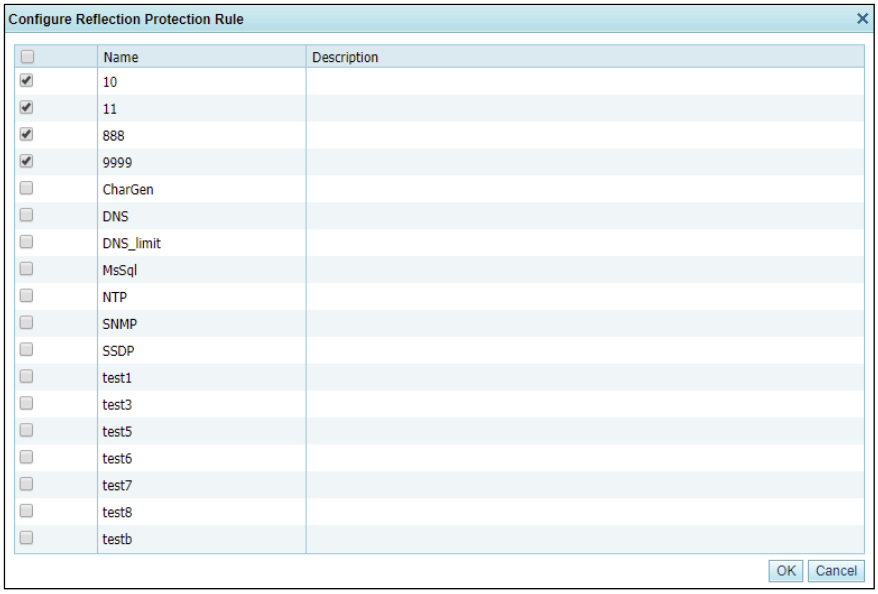
You can perform the following operations on the reflection protection policy:

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- Rearrange rules: Click or to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3** indicates that the first rule will be put below the third rule. Click to commit the change.
- **Add rule**: Click to open the rule configuration page shown in Figure 5-32. Select one or more rules and then click **OK**.

  For the creation of a reflection protection rule, see section 5.2.2.1 Creating a Reflection Protection Rule.

  Delete a rule: Click to delete a rule.

Figure 5-32 Adding reflection protection rules



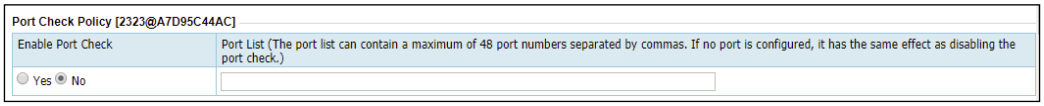
5.1.2.3 Port Check Policy

The port check policy indicates that after the port check function is enabled, the system checks the data arriving at the specified port but discards the data to other ports.

Figure 5-33 shows the port check policy settings.

You can select **Yes** or **No** to enable or disable the policy. After the policy is enabled, you can add a maximum of 48 ports that are separated by the comma.

Figure 5-33 Port check policy of a protection group



5.1.2.4 HTTPS Protection Policy

HTTPS protection policies are classified into two types:

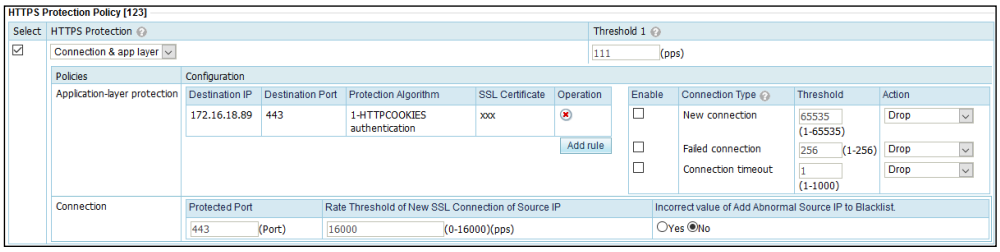
- Connection protection: With the HTTPS connection protection policy, the system checks HTTPS packets from clients. When **Add Abnormal IP to Blacklist** is set to **Yes**, the system adds source IP addresses that match the HTTPS protection algorithm to the blacklist.
- Application-layer protection: The system configures an SSL certificate for specified destination IP addresses and ports and then authenticates clients with HTTPS protection algorithms and controls SSL connections. Packets that fail the check will be dropped or their source IP addresses will be added to the blacklist.

Note	The HTTPS application-layer protection policy is available only to ADS NX3-800E/2020E, NX5-4020E/6025E, NX5-8000 and NX5-10000.

This section describes the application-layer protection function. For details on HTTPS connection protection, see section 5.1.1.3 HTTPS Protection Policy.

Figure 5-34 shows HTTPS protection policies.

Figure 5-34 HTTPS protection policies of a protection group



In the upper-left corner of the area shown in Figure 5-34, select an HTTPS protection mode, which can be one of the following:

- **None**: disables HTTPS protection policies.
- **Connection only**: enables connection protection only.
- **App layer only**: enables application-layer protection only.
- **Connection & app layer**: enables both connection protection and application-layer protection.

If both types of HTTPS protection are enabled, only the destination IP address and port put under application-layer protection are checked against the application-layer protection policy, while other ports are checked against the connection protection policy.

To configure an application-layer protection policy, perform the following steps:

Step 1 Create an application-layer protection rule.

Click **Add Rule** and set parameters in the dialog box that appears.

Figure 5-35 Creating an application-layer protection rule

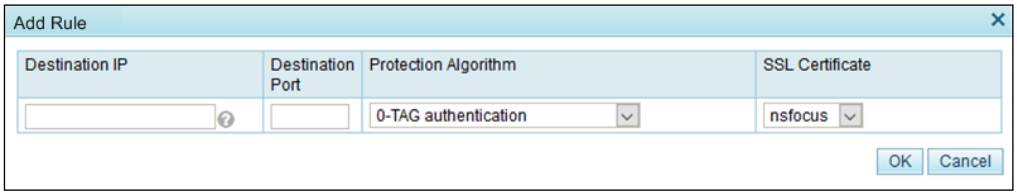


Table 5-13 lists parameters for creating an application-layer protection rule.

Table 5-13 Parameters of an application-layer protection rule

Parameter	Description
Destination IP	Destination IP address to protect. Such an IP address should be within the IP address range covered by the protection group.
Destination Port	Port of the destination IP address to protect. The value range is 0–65535.
Protection Algorithm	Protection algorithm used in this rule.
SSL Certificate	SSL certificate used in this rule. The default certificate is **nsfocus**. You can also import others as required. For how to import an SSL certificate, see section 5.1.7 SSL Certificate Management.

Step 2 After the configuration is complete, click **OK** to return to the HTTPS protection policy page.

Step 3 Configure control items.

Table 5-14 Control items of an application-layer protection rule

Parameter	Description
Enable	Controls whether to check the number of new connections, failed connections, and timeout connections to the destination port to protect.

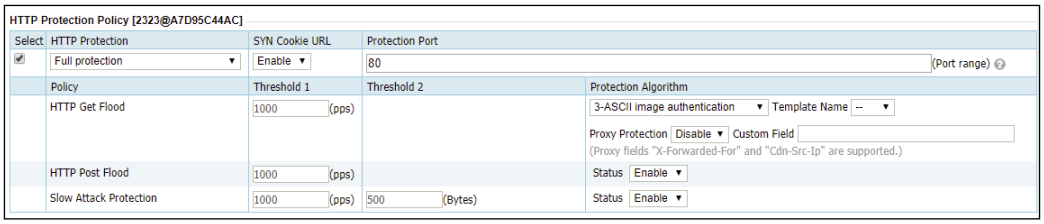
Parameter	Description
Control Item	Connection control items. Such items only work for destination IP addresses and ports under application-layer protection. • **New connection**: limits the number of new HTTPS connections initiated by a source IP address to the specified destination port. • **Failed connection**: limits the number of new HTTPS connections a source IP address fails to initiate to the specified destination port. Failed connections include failures in SSL/TLS handshake, renegotiation, and HTTPS packet parsing. • **Timeout connection**: limits the number of new HTTPS connections a source IP address initiates to the specified destination port. A timeout connection means either an incomplete SSL/TLS handshake or no HTTPS packet interaction after the SSL/TLS handshake is complete.
Threshold	Threshold of each control item. The threshold range is different for the three types of connections: • New connection: 1–65535 • Failed connection: 1–256 • Timeout connection: 1–1000
Action	Action taken on packets from clients or IP addresses of clients, which can be either of the following: • **Drop**: If a client fails to be authenticated by an HTTPS protection algorithm, the system drops packets sent by (or from) this client if they contain the specified signature. • **Add to blacklist**: If a client fails to be authenticated by an HTTPS protection algorithm, the system identifies its IP address as an abnormal one and adds it to the blacklist to block it. You need to enable the blacklist function before setting this action. For details on the blacklist, see section 5.2.9 Blacklist.

----End

5.1.2.5 HTTP Protection Policy

Figure 5-36 shows HTTP protection policies.

Figure 5-36 HTTP protection policies



HTTP protection policies cover the following items:

- HTTP GET flood protection: As long as HTTP protection is enabled, the system automatically activates HTTP GET flood protection, regardless of the setting of **HTTP Protection**.

If **HTTP Protection** is set to **Only on the rules of URL protection**, protection is performed based on the rules of URL-ACL protection. In this case, SYN cookie URL cannot be enabled.

- HTTP POST flood protection: This type of protection is activated only if the following conditions are met:
  - HTTP protection is enabled and **HTTP Protection** is set to **Full protection** or **Only on the rules of URL protection**.
  - Status is set to **Enable** for HTTP POST flood protection.

  If **HTTP Protection** is set to **Not protect**, **Status** of this type of protection changes to **Disable** automatically.
- SYN cookie URL: SYN cookie URL protection can be enabled only when the following conditions are met:
  - HTTP protection is enabled and **HTTP Protection** is set to **Full protection**.
  - HTTP POST flood protection is enabled.

  Enabling SYN cookie URL disables proxy protection. To disable SYN cookie URL for a protection group, you must disable SYN cookie URL for all URL rules of the protection group in advance.

  Setting **HTTP Protection** to **Only on the rules of URL protection** disables SYN cookie URL.
- Slow attack protection: This type of protection can be enabled only when HTTP protection is enabled and **HTTP Protection** is set to **Full protection**.

  Setting **HTTP Protection** to **Not protect** or **Only on the rules of URL protection** disables slow attack protection.
- Proxy protection: After HTTP GET flood protection is enabled, you can enable proxy protection.

  Enabling proxy protection disables SYN cookie URL.

Compared with the global HTTP protection policy, such a policy for a protection group adds the following contents:

HTTP GET Flood

- **Protection Algorithm**:
  - **0_TAG authentication** and **1_HTTPCOOKIES authentication** verify the destination IP address by adding authentication information to HTTP packets.
  - **2_URL authentication** adds information similar to cookies into URL requests.
  - **3_ASCII image authentication** and **4_BMP image authentication** add a verification code.
  - **5_Dynamic script protection** performs verification by adding key values to URLs.
  - **6_Legend authentication** and **7_FCS check** check the packets of the "Legend" game and the flash server.
  - **8_Pattern matching check** matches a signature string that is defined under **Advanced > Pattern Matching** (see section 8.2 Pattern Matching Rules for the configuration of pattern matching).

The default algorithm is **1_HTTPCOOKIES authentication**. Please select an appropriate algorithm according to the particular situation.

Note	• **6_Legend authentication**, **7_FCS check** and **8_Pattern matching check** are available only when **SYN Cookie URL** is enabled during protection group configuration. • Enabling SYN cookie URL disables the **0_TAG authentication** and **1_HTTPCOOKIES authentication** algorithms.

- **Template Name**: If **4_BMP image authentication is** selected, you need to select the response page that contains a CAPTCHA code image. For response page settings, see section 5.1.5 Response Page Settings.
- **Proxy Protection**: You are advised to enable this function if a proxy server exists on the customer network.
- **Custom Field**: After proxy protection is enabled, you can configure the custom proxy field (X-Forwarded-For or Cdn-Src-Ip) so that ADS can accurately identify the actual IP address.

Slow Attack Protection

Slow attack protection is triggered if the transmission rate of HTTP packets to a destination IP address is above threshold 1 and the payload size of such packets is below threshold 2.

Threshold 1: threshold for the rate (pps) of transmitting HTTP packets to a destination IP address

Threshold 2: threshold for the payload size of HTTP packets to a destination IP address

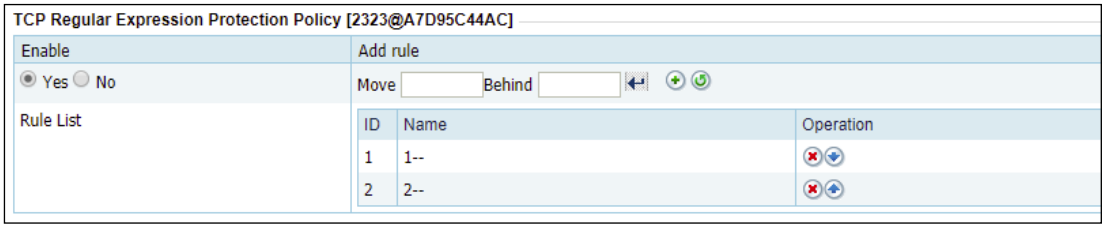
5.1.2.6 TCP Regular Expression Protection Policy

After configuring regular expression rules, you can enable the TCP regular expression protection and reference created regular expression rules. For details on regular expression rules, see section 5.2.4 Regular Expression Rules.

Figure 5-37 shows the page for configuring the TCP regular expression protection policy.

Note	• When multiple rules are referenced, the TCP regular expression protection policy matches attack packets with these rules in a top-down manner. In principle, the matching stops once a rule is hit. An administrator may need to adjust the rule sequence as required. • When multiple rules are matched, ADS performs protection based on the first rule.

Figure 5-37 TCP regular expression protection policy

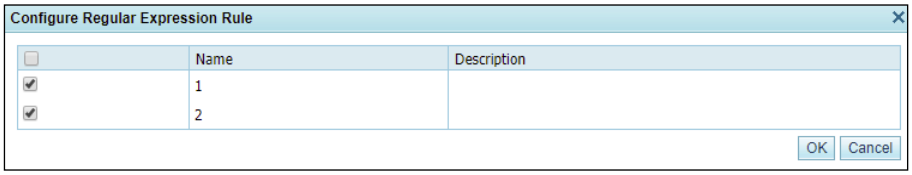


You can perform the following operations on the TCP regular expression protection policy:

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- Rearrange rules: Click or to move a rule one level up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3** indicates that the first rule will be put below the third rule. Click to commit the change.
- **Add rule**: Click to open the rule addition dialog box shown in Figure 5-38. Select one or more rules and then click **OK**.

  For how to create a regular expression rule, see section 5.2.4 Regular Expression Rules.
- Delete a rule: Click to delete a rule.

Figure 5-38 Adding regular expression rules



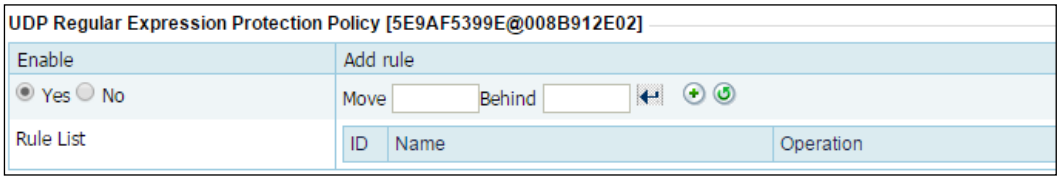
5.1.2.7 UDP Regular Expression Protection Policy

After configuring regular expression rules, you can enable the UDP regular expression protection policy and reference created regular expression rules. For details on regular expression rules, see section 5.2.4 Regular Expression Rules.

Figure 5-39 shows the page for configuring the UDP regular expression protection policy.

Note	• When multiple rules are referenced, the UDP regular expression protection policy matches attack packets with these rules in a top-down manner. In principle, the matching stops once a rule is hit. An administrator may need to adjust the rule sequence as required. • When multiple rules are matched, ADS performs protection based on the first rule.

Figure 5-39 UDP regular expression protection policy



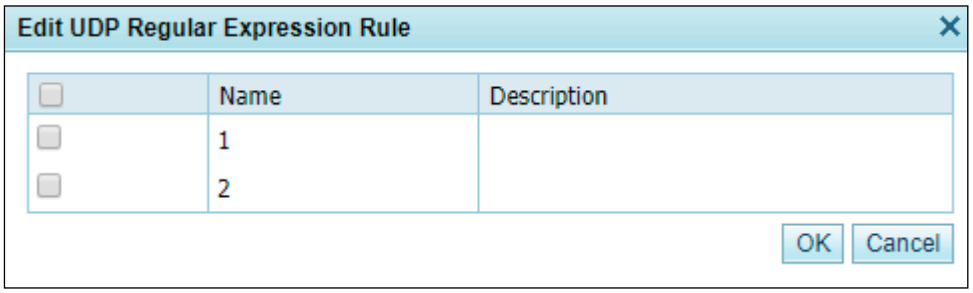
You can perform the following operations on the UDP regular expression protection policy:

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- Rearrange rules: Click or to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3**

indicates that the first rule will be put below the third rule. Click to commit the change.

- **Add rule**: Click to open the rule configuration dialog box shown in Figure 5-40. Select one or more rules and then click **OK**.
- For how to create a regular expression rule, see section 5.2.4 Regular Expression Rules. Delete a rule: Click to delete a rule.

Figure 5-40 Adding UDP regular expression rules

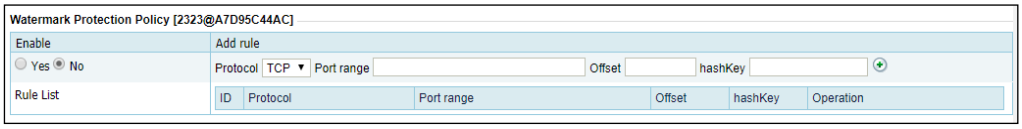


5.1.2.8 Watermark Protection Policy

If you add watermarks to your legitimate traffic, you can configure watermark rules on ADS and enable the watermark protection policy so that ADS can differentiate between normal packets and attack packets according to the configured watermark rules.

Figure 5-41 shows the watermark protection policy.

Figure 5-41 Watermark protection policy



You can perform the following operations on the watermark protection policy:

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- **Add rule**: Set **Protocol** (UDP or TCP), **Port Range**, **Offset** (0–1480), and **Hash Key** (must be a decimal integer), and click to add a watermark protection rule. **Port Range** can be a single port, port range, or multiple ports. Multiple ports must be separated by the comma.
- Delete a rule: Click to delete a rule.

After the watermark protection policy is enabled, ADS will allow packets that match this rule to pass through and drop mismatching ones.

A maximum of eight watermark rules can be created for a protection group.

5.1.3 Protection Group Management

Some networks serve a large number of users who have various anti-DDoS requirements. In response, the ADS device provides the protection group function, which allows the administrator to provide different protection policies for various users.

A protection group is a collection of one or more customer's machines that are protected by ADS devices using the same policy. ADS supports a maximum of 65535 IP addresses in total.

ADS can automatically generate protection groups based on policy auto-learning results. For details, see section 5.1.6 Policy Auto-Learning.

This section covers the following topics:

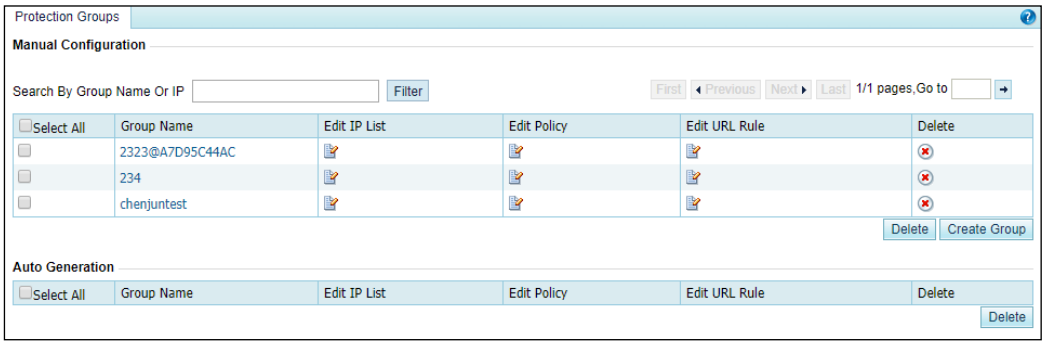
- Creating a Protection Group
- Viewing Protection Groups
- Editing a Protection Group (including IP address list, policies, and URL rules)
- Deleting a Protection Group

5.1.3.1 Creating a Protection Group

To create a protection group, perform the following steps:

Step 1 Choose **Policies** > **Anti-DDoS** > **Protection Groups** to open the protection group list.

Figure 5-42 Protection groups



Step 2 Configure basic information of a protection group.

To the lower right of the list, click **Create Group** to create a protection group, as shown in Figure 5-43.

Figure 5-43 Basic information of a protection group

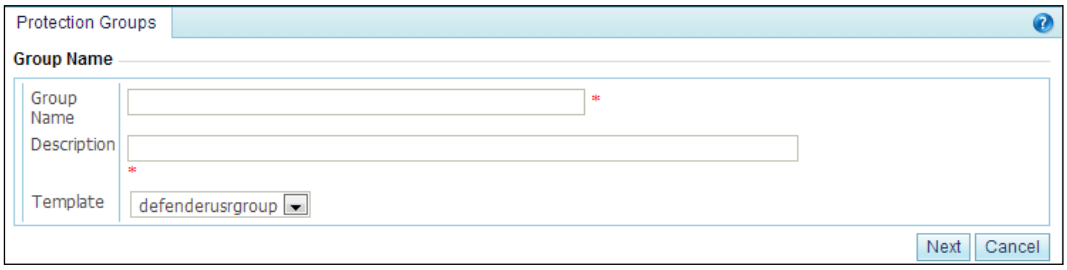


Table 5-15 describes parameters for creating a protection group.

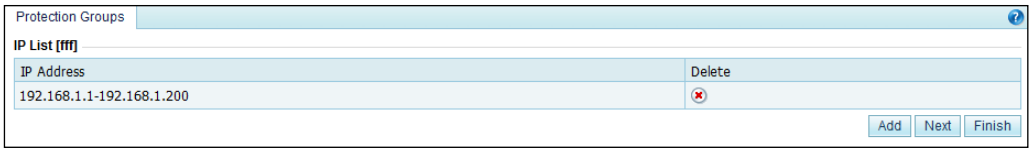
Table 5-15 Parameters for creating a protection group

Parameter	Description
Group Name	Name of the group. It must consist of 1 to 200 letters, digits, or underscores, and cannot be the same as an existing group name.
Description	Description of a group. It supports a maximum of 80 characters.
Template	The default value is **defenderusrgroup**, indicating that all policies are selected.

Step 3 Configure the IP address range of the protection group.

After basic information of the protection group is configured, click **Next** to open the **IP List** page.

Figure 5-44 IP List page



You can add IP segments (one by one). If you do not want to add IP segments, click **Next** to skip this step or click **Finish** to end the creation of the protection group.

Note	The ADS device supports the IPv4/IPv6 dual-stack, and therefore protection groups support both IPv4 and IPv6 address ranges.

- Add IP address ranges.

a. Click **Add** to the lower right of the IP address list to add IP address ranges, as shown in Figure 5-45.

Figure 5-45 Adding IP address ranges

Table 5-16 describes parameters of an IP segment.

Table 5-16 Parameters of an IP segment

Parameter	Description
IP address format	You can type IPv4 or IPv6 addresses or segments, with each one in a separate line, in the following formats: • Individual IP addresses: If individual IP addresses such as 192.168.1.1 and 2::2 are typed, the page automatically displays them as 192.168.1.1-192.168.1.1 and 2::2-2::2. • IP address/netmask: IPv4 address with a netmask ranging from 16 to 32, such as 192.168.1.0/24; or IPv6 address with a netmask ranging from 1 to 128, such as 192.168.1.0/24 or fe80::250:56ff:fec0:0/114. • Start IP-End IP: an IPv4 address range within a /24 segment, such as 192.168.1.1-10; or IPv6 address with a maximum of 16 bytes, such as 1::1-ffff. The IP addresses or IP segments cannot conflict with those in existing groups.

b. Set parameters and click **OK** to save the settings.

- Delete IP segments.

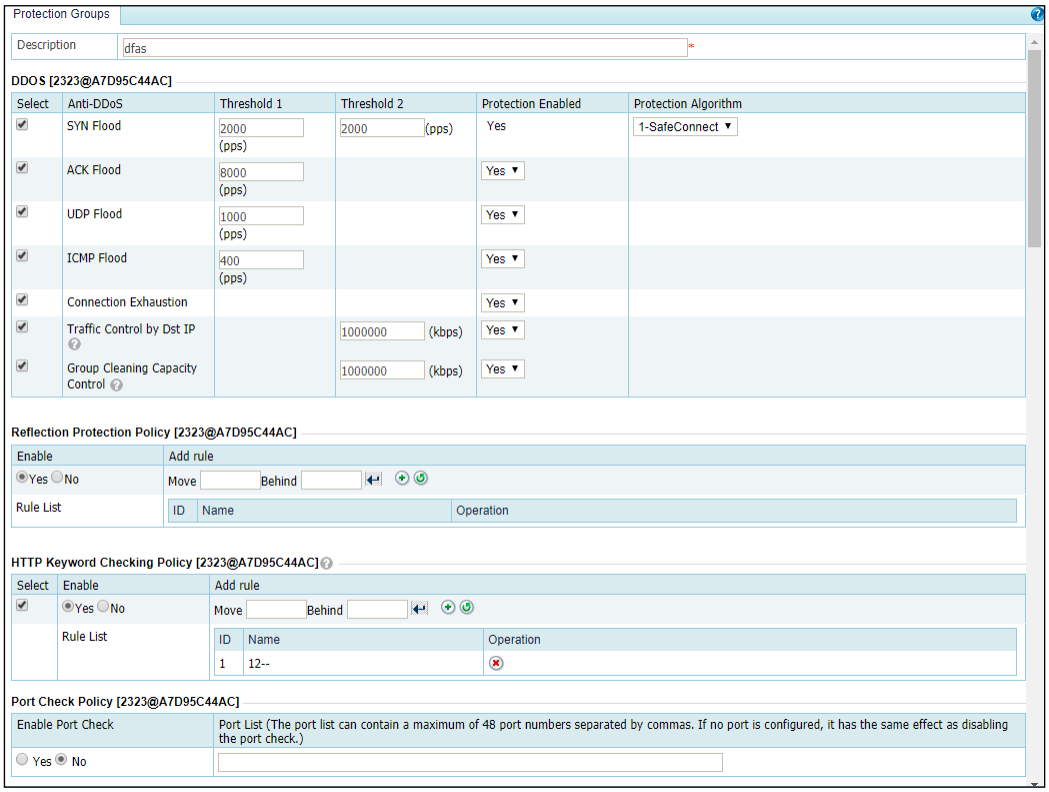
  Click ⊗ to the right of an IP segment, as shown in Figure 5-44, and then click **OK** in the confirmation dialog box to delete the IP segment.

Note	IP segments configured for different protection groups must contain different IP addresses.

Step 4 Configure policies for the protection group.

After configuring IP segments, click **Next** to configure policies. For details on policy configurations of protection groups, see section 5.1.2 Policy Configuration for Protection Groups.

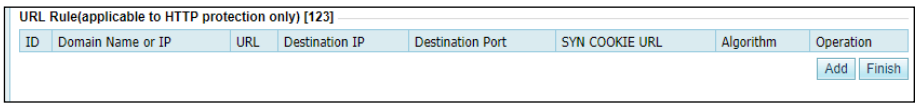
Figure 5-46 Configuring policies



Step 5 Configure a URL rule for the protection group.

After configuring policies, click **Next** to add a URL rule.

Figure 5-47 List of URL rules



- Configure a URL rule.
  - Click **Add** to the lower right of the URL rule list to configure a URL rule.

Figure 5-48 Configuring a URL rule

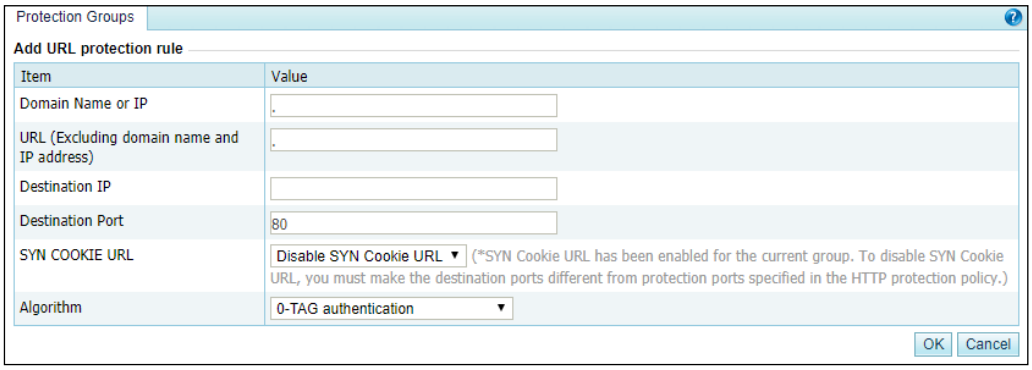


Table 5-17 describes parameters of a URL rule.

Table 5-17 Parameters of a URL rule

Parameter	Description
Domain Name or IP	Domain name or IP address of a URL protection object. The symbol "." indicates that this rule is valid for all domain names and IP addresses.
URL (Excluding domain name and IP address.)	Relative path of a URL protection object, that is, URL excluding the domain name or IP address. The symbol "." indicates that this rule is valid for all URLs.
Destination IP	IP address of the server. You can type IPv4 or IPv6 addresses according to the actual network deployment. Note The destination IP address must be included in the IP address range of the corresponding protection group.
Destination Port	TCP port of the server.
SYN COOKIE URL	Controls whether to enable **SYN COOKIE URL**. • If **SYN COOKIE URL** is enabled, a client attempting to access a server can access the server only after being authenticated by the ADS device, to protect the server from SYN cookie attacks. • Whether **SYN COOKIE URL** is enabled determines the number of available options for the **Algorithm** parameter. • Whether **SYN COOKIE URL** can be enabled depends on whether **SYN COOKIE URL** is enabled for HTTP protection in Step 4.
Algorithm	Protection algorithm for packets that match URL rules. This parameter is used in conjunction with **SYN COOKIE URL**. If **SYN COOKIE URL** is enabled, you can choose from algorithm 2 through 8; if **SYN COOKIE URL** is disabled, you can only choose from algorithm 0 through 5.

– Set parameters and click **OK** to save the settings.

- Modify a URL rule.

  Click to the right of a URL rule to modify parameters of this rule.

- Delete a URL rule.

  Click to the right of a URL rule and then click **OK** in the confirmation dialog box to delete the rule.

Step 6 After a URL rule is configured, click **Finish** to the lower right of the URL rule list.

Step 7 After the preceding configuration, click **Apply** in the upper-right corner of the web page to make the settings take effect.

----End

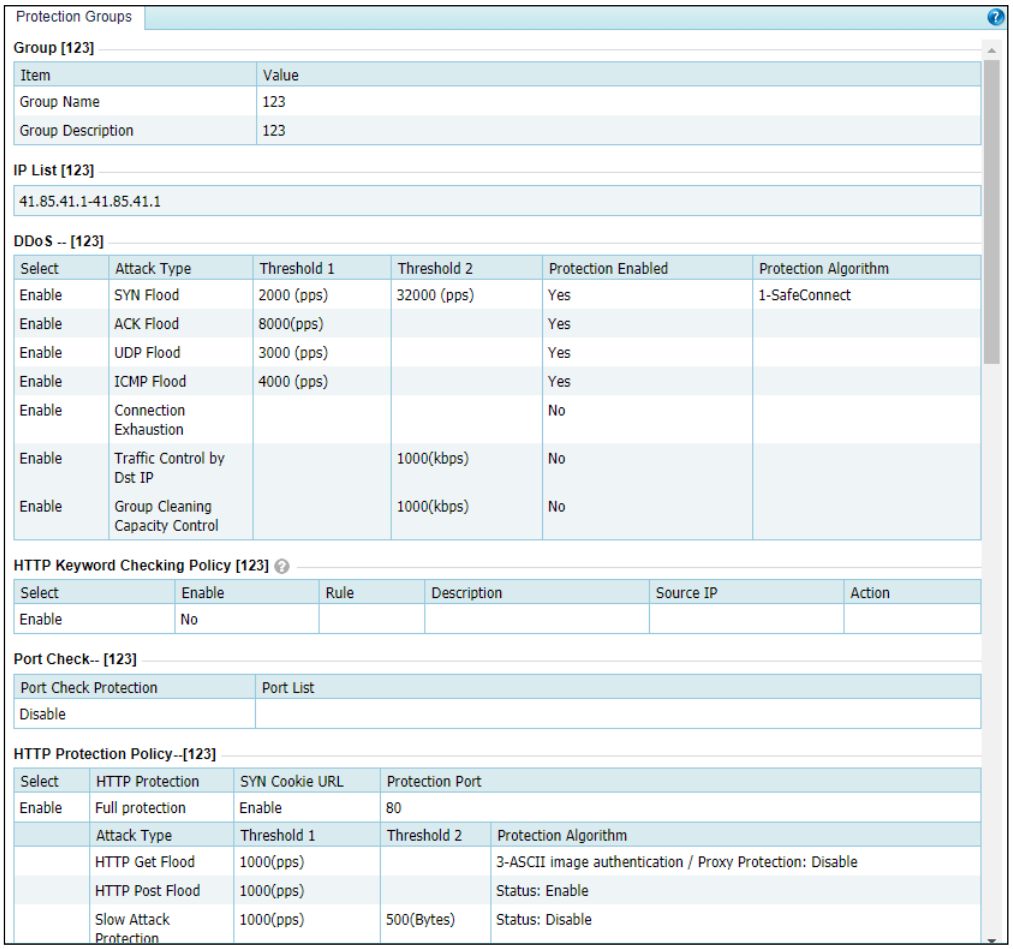
5.1.3.2 Searching for Protection Groups

On the page shown in **Figure 5-42**, you can type a protection group name or an IP address in the group, and then click Filter to search for a protection group.

5.1.3.3 Viewing Protection Groups

On the protection group list as shown in Figure 5-42, click the name of a protection group to view details. See Figure 5-49.

Figure 5-49 Viewing details of a protection group



Protection Groups

Group [123]

Item	Value
Group Name	123
Group Description	123

IP List [123]

41.85.41.1-41.85.41.1

DDoS -- [123]

Select	Attack Type	Threshold 1	Threshold 2	Protection Enabled	Protection Algorithm
Enable	SYN Flood	2000 (pps)	32000 (pps)	Yes	1-SafeConnect
Enable	ACK Flood	8000(pps)		Yes	
Enable	UDP Flood	3000 (pps)		Yes	
Enable	ICMP Flood	4000 (pps)		Yes	
Enable	Connection Exhaustion			No	
Enable	Traffic Control by Dst IP		1000(kbps)	No	
Enable	Group Cleaning Capacity Control		1000(kbps)	No	

HTTP Keyword Checking Policy [123]

Select	Enable	Rule	Description	Source IP	Action
Enable	No				

Port Check-- [123]

Port Check Protection	Port List
Disable	

HTTP Protection Policy--[123]

Select	HTTP Protection	SYN Cookie URL	Protection Port	
Enable	Full protection	Enable	80	
	Attack Type	Threshold 1	Threshold 2	Protection Algorithm
	HTTP Get Flood	1000(pps)		3-ASCII image authentication / Proxy Protection: Disable
	HTTP Post Flood	1000(pps)		Status: Enable
	Slow Attack Protection	1000(pps)	500(Bytes)	Status: Disable

5.1.3.4 Editing a Protection Group

You can edit the IP address range, policies, and URL rules of a protection group. Note that the protection group name cannot be changed.

- Edit the IP address range of a protection group.

  On the protection group list, click in the **Edit IP List** column to reset the IP address range of a protection group.

  After editing the IP address range, click **OK** to save the settings. Click **Next** to edit policies.
- Edit policies for a protection group.

  On the protection group list, click in the **Edit Policy** column to reset policies applied to a protection group.

  After editing prevention policies, you can click **Cancel** to undo the changes and return to the protection group list. Alternatively, you can click **Next** to edit URL rules applied to a protection group and then click **Finish** to save settings.
- Edit URL rules for a protection group.

  On the protection group list, click in the **Edit URL Rule** column to reset URL rules applied to a protection group.

  After editing URL rules, click **Finish** to save settings.

5.1.3.5 Deleting a Protection Group

You can delete one protection group or more groups in batches on the ADS device.

- Method 1: On the protection group list shown in Figure 5-42, click in the **Operate** column of a protection group and click **OK** in the confirmation dialog box to delete the protection group.
- Method 2: On the protection group list shown in Figure 5-42, select one or more protection groups (or select the **Select All** check box to select all protection groups) to be deleted, click **Delete** to the lower right of the protection group list, and then click **OK** in the confirmation dialog box to delete the selected protection groups.

Note	After a protection group is deleted, customer's machines are protected by default anti-DDoS policies, instead of using policies of the protection group.

5.1.4 Advanced Global Parameters

You can configure trust control parameters.

The procedure is as follows:

Step 1 Choose **Policies** > **Anti-DDoS** > **Advanced Global Parameters.**

Step 2 Click **Edit** and configure the length of time an IP address is trusted based on the protection algorithm on the page shown in Figure 5-50.

Figure 5-50 Advanced Global Parameters page

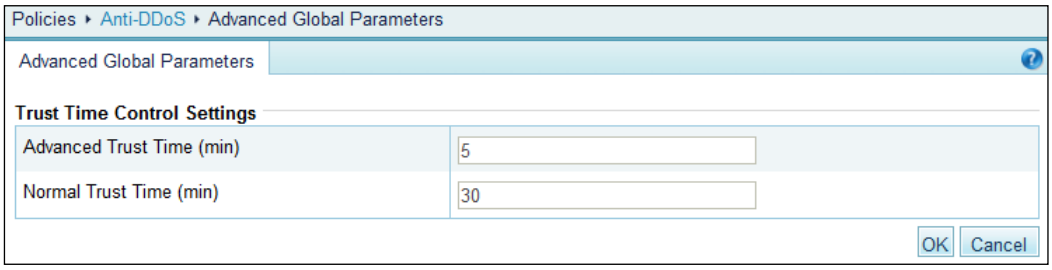


Table 5-18 describes advanced global parameters.

Table 5-18 Advanced global parameters

Parameter	Description
Advanced Trust Time (min)	Time during which a source IP address authenticated with the advanced algorithm stays in the trust list. The value ranges from 1 to 3600, with **5** as the default.
Normal Trust Time (min)	Time during which a source IP address authenticated with the common algorithm stays in the trust list. The value ranges from 1 to 3600, with **30** as the default.

Step 3 After the parameter configuration is complete, click **OK** to save the settings.

----End

5.1.5 Response Page Settings

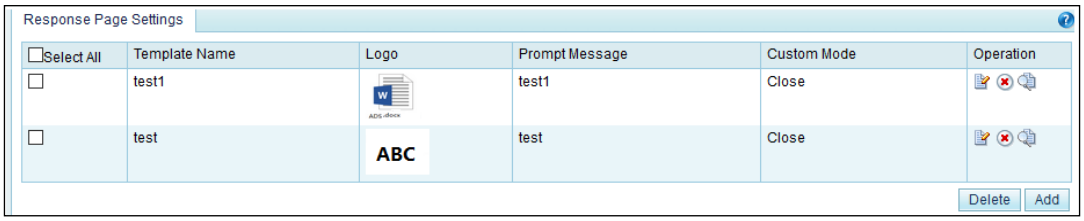
If **4-BMP image authentication** is specified as the algorithm for the HTTP protection policy and a template is specified, a client attempting to access a server through ADS needs to input a code for authentication in the automatically displayed response page. The client can access the server only after it is successfully authenticated. This section describes how to add, edit, delete, and preview response pages.

5.1.5.1 Creating a Response Page

To create a response page, perform the following steps:

Step 1 Choose **Policies** > **Anti-DDoS** > **Response Page Settings**.

Figure 5-51 Response Page Settings tab page



Step 2 Click **Add**.

The **Response Page Settings** page appears, as shown in Figure 5-52.

The response page can be displayed in either of the following modes:

- Common mode: By default, the response page is displayed in common mode.
- Custom mode: The response page is displayed in custom mode only after **Custom Mode** is selected.

Response page templates in different modes can coexist.

Figure 5-52 Response Page Settings page

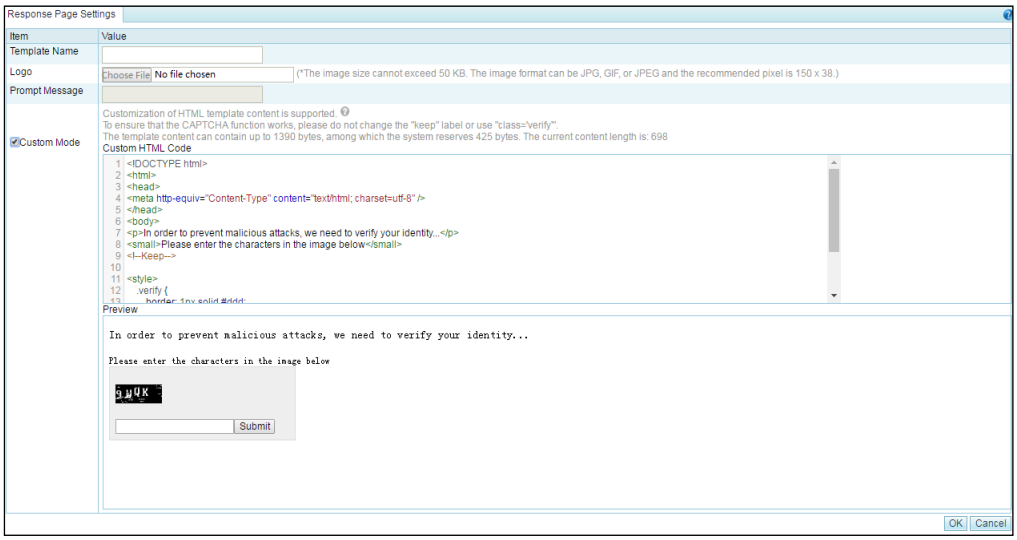


Table 5-19 describes parameters for creating a response page.

Table 5-19 Parameters for creating a response page

Parameter	Description
Template Name	Specifies the name of a response page.
Logo	Specifies the logo of a response page. The image can be in jpg, png, gif, or jpeg format and must be within 50 KB. A pixel size of 150*38 (unit: P) is recommended.
Prompt Message	Specifies the prompt message displayed under the logo.
Custom Mode	Allows users to modify the response page template by directly modifying the HTML code.

Step 3 Click **Choose File** and select an image.

Step 4 Configure parameters, and then click **OK**.

----End

Note	A maximum of 64 response page templates can be added.

5.1.5.2 Editing a Response Page

You can edit an existing response page by performing the following steps:

Step 1 On the page shown in Figure 5-51, click in the row of a response page.

Step 2 Configure parameters of the response page, and then click **OK** to save settings and return to the response page list.

----End

5.1.5.3 Deleting Response Pages

You can delete one response page (using method 1) or multiple response pages (using method 2) in batches.

- Method 1: On the tab page shown in Figure 5-51, click in the **Operation** column of a response page and then click **OK** in the confirmation dialog box to delete the response page.
- Method 2: On the tab page shown in Figure 5-51, select one or more response pages (or select the **Select All** check box to select all response pages), click **Delete** to the lower right of the list, and then click **OK** in the confirmation dialog box to delete the selected response pages.

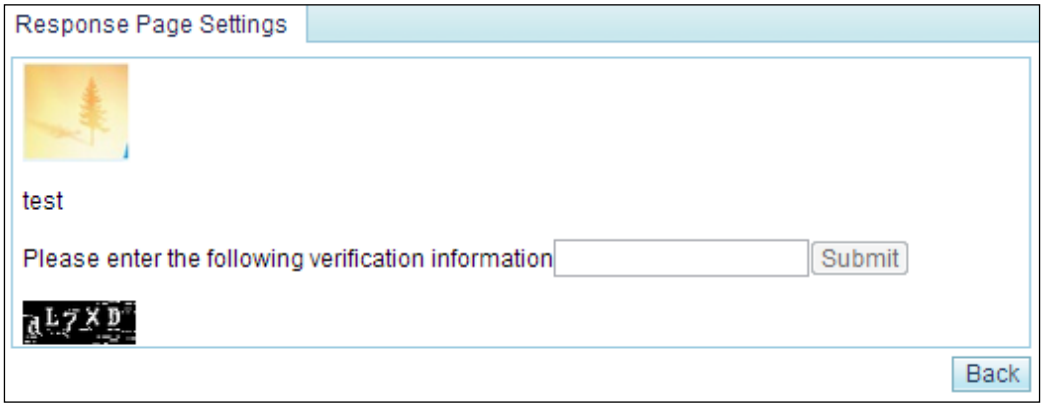
5.1.5.4 Previewing a Response Page

After a response page is configured, you can perform the following steps to preview it:

Step 1 On the page shown in Figure 5-51, click in the row of a response page.

Information on the previewed page can be viewed but cannot be edited.

Figure 5-53 Response page preview



Step 2 Click **Back** to return to the response pages list.

----End

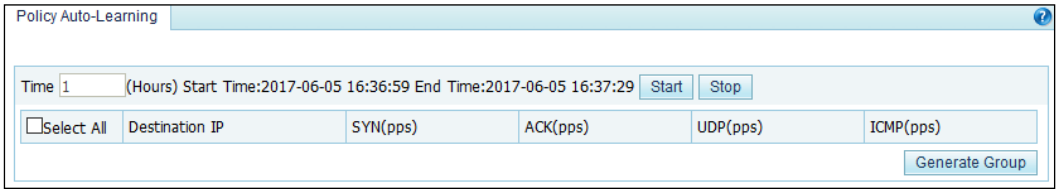
5.1.6 Policy Auto-Learning

ADS supports policy auto-learning. This means ADS can collect and analyze statistics on normal SYN, ACK, UDP, and ICMP packets, generate protection policies based on built-in algorithms, and create protection group templates.

To configure policy self-learning, perform the following steps:

Step 1 Choose **Policies** > **Anti-DDoS** > **Policy Auto-Learning**.

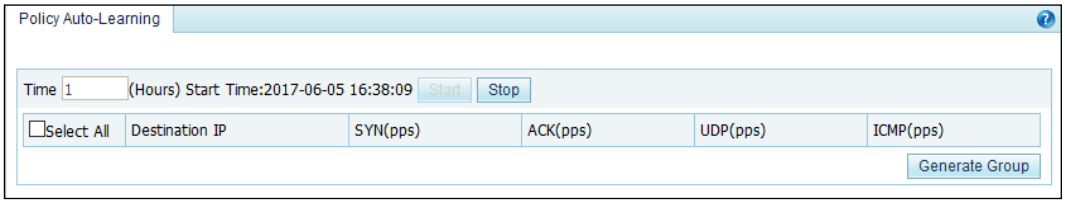
Figure 5-54 Policy Auto-Learning page



Step 2 Set the time (**1** by default), and click **Start**.

ADS starts to collect statistics, as shown in Figure 5-55.

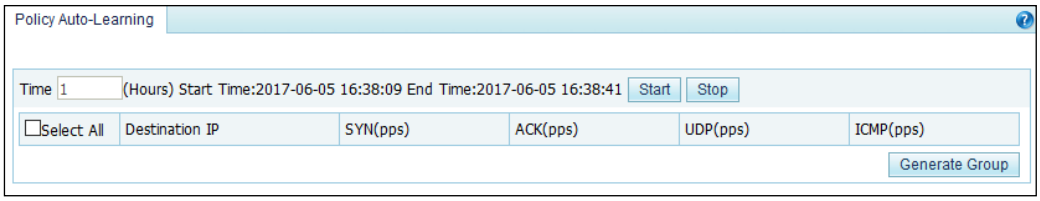
Figure 5-55 Starting learning



Step 3 Wait until the specified learning time expires, or click **Stop** to stop the learning process.

ADS then displays a learning record on the **Policy Auto-Learning** page. A learning record contains the destination IP address, SYN packet rate, ACK packet rate, UDP packet rate, and ICMP packet rate in pps.

Figure 5-56 Auto-learning record



Step 4 Select the check box in the row of a learning record, and click **Generate Group**.

The system generates a protection group based on the learning record and at the same time deletes the learning record.

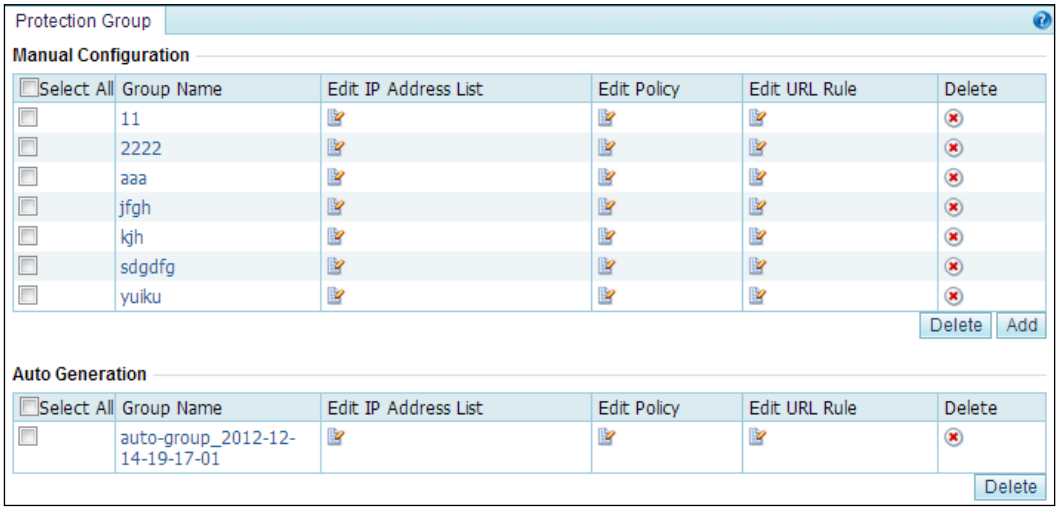
Step 5 Choose **Policies** > **Anti-DDoS** > **Protection Groups**.

The **Protection Groups** page appears, as shown in Figure 5-57.

You can view, edit, and delete the automatically generated protection group in the **Auto Generation list**. By default, automatically generated protection groups are named in the **auto-group_***N* format. *N* indicates the generation time. For example, 2012-12-04-14-58-41 indicates that the generation time is 14: 58:41 on December 4, 2012. For how to configure protection groups, see section 5.1.2 Policy Configuration for Protection Groups.

Note	If a protection group cannot be generated based on the learning record due to a conflict with existing groups, the page shown in *Figure 5-56* will display the conflicting protection groups.

Figure 5-57 Viewing automatically generated protection groups



----End

5.1.7 SSL Certificate Management

If the HTTPS application-layer protection policy is configured, an SSL certificate is required for ADS to decrypt HTTPS packets before matching packets with this policy. This section describes how to import and manage SSL certificates uploaded by users.

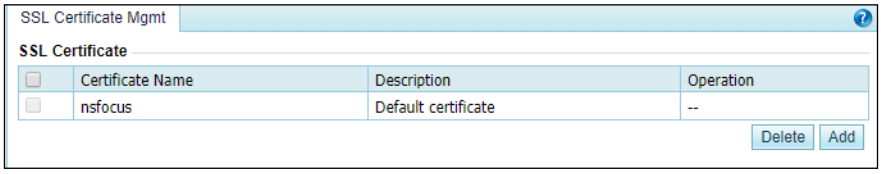
ADS provides the **nsfocus** certificate upon delivery. This certificate cannot be edited or deleted. You can add other certificates as required.

5.1.7.1 Adding an SSL Certificate

To add an SSL certificate, perform the following steps:

Step 1 Choose **Policies** > **Anti-DDoS** > **SSL Certificate Mgmt**.

Figure 5-58 SSL certificate management



Step 2 Click **Add**.

Figure 5-59 Adding an SSL certificate

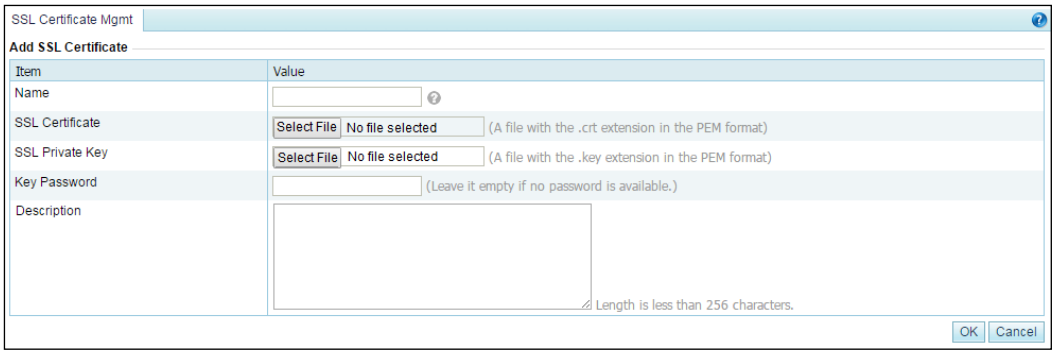


Table 5-20 describes parameters of an SSL certificate.

Table 5-20 Parameters of an SSL certificate

Parameter	Description
Name	Name of the SSL certificate. The certificate name is at most 15-character long and can only contain digits, uppercase letters, and lowercase letters.
SSL Certificate	Click **Select File** to select an SSL certificate file.
SSL Private Key	Click **Select File** to select an SSL private key file.
Key Password	If a password is set for the private key of the SSL certificate to be imported, type the correct password; otherwise, leave it empty.
Description	Description of the SSL certificate.

Step 3 Configure parameters and click **OK** to import the SSL certificate.

After the certificate is successfully imported, you can view it on the **SSL Certificate Mgmt** page.

Note	A certificate can be imported only once. A maximum of 20 different certificates are allowed here.

----End

5.1.7.2 Editing an SSL Certificate

To edit an SSL certificate, perform the following steps:

Step 1 On the SSL certificate list shown in Figure 5-58, click in the **Operation** column of a certificate.

Step 2 Edit parameters and click **OK** to save the settings and return to the SSL certificate list.

----End

5.1.7.3 Deleting an SSL Certificate

On the SSL certificate list shown in Figure 5-58, click in the **Operation** column of a certificate and click **OK** in the displayed confirmation dialog box to delete the certificate.

5.2 Access Control Policies

The system provides the access control list (ACL), blacklist, and whitelist functions to make certain specific applications more easily controlled. This section covers the following topics:

- Access Control Rules
- Reflection Protection Rules
- GeoIP Rules
- Regular Expression Rules
- DNS Keyword Checking
- HTTP Keyword Checking
- Connection Exhaustion Rules
- URL-ACL Protection Rules
- Blacklist
- Whitelist

5.2.1 Access Control Rules

Access control rule allows ADS to control the traffic passing through it and determine how (allow, protect, or drop) to handle packets matching this rule via software based on the protocol, source/destination IP address, and source/destination port.

The system sorts all access control rules saved on the device according to the following principles. It matches packets passing through the device with access control rules in sequence and stops the match once a matched rule is hit. You can also rearrange access control rules to adjust the rule matching sequence.

This section covers the following topics:

- Creating an Access Control Rule
- Creating Access Control Rules in Batches
- Enabling/Disabling Access Control Rules
- Rearranging Access Control Rules
- Editing an Access Control Rule
- Deleting Access Control Rules

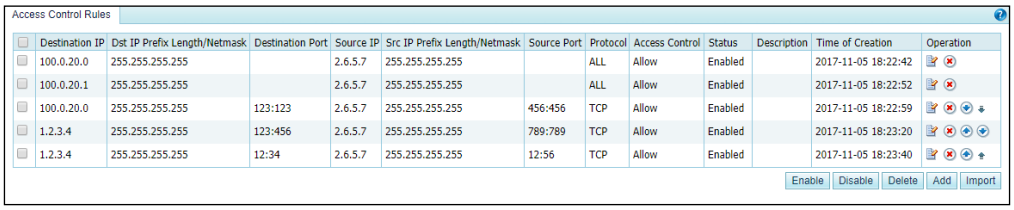
5.2.1.1 Creating an Access Control Rule

To create an access control rule, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Access Control Rules**.

Initially, the rule list is empty.

Figure 5-60 List of access control rules



Destination IP	Dst IP Prefix Length/Netmask	Destination Port	Source IP	Src IP Prefix Length/Netmask	Source Port	Protocol	Access Control	Status	Description	Time of Creation	Operation
100.0.20.0	255.255.255.255		2.6.5.7	255.255.255.255		ALL	Allow	Enabled		2017-11-05 18:22:42	
100.0.20.1	255.255.255.255		2.6.5.7	255.255.255.255		ALL	Allow	Enabled		2017-11-05 18:22:52	
100.0.20.0	255.255.255.255	123:123	2.6.5.7	255.255.255.255	456:456	TCP	Allow	Enabled		2017-11-05 18:22:59	
1.2.3.4	255.255.255.255	123:456	2.6.5.7	255.255.255.255	789:789	TCP	Allow	Enabled		2017-11-05 18:23:20	
1.2.3.4	255.255.255.255	12:34	2.6.5.7	255.255.255.255	12:56	TCP	Allow	Enabled		2017-11-05 18:23:40	

Step 2 Click **Add**.

Figure 5-61 Creating an access control rule

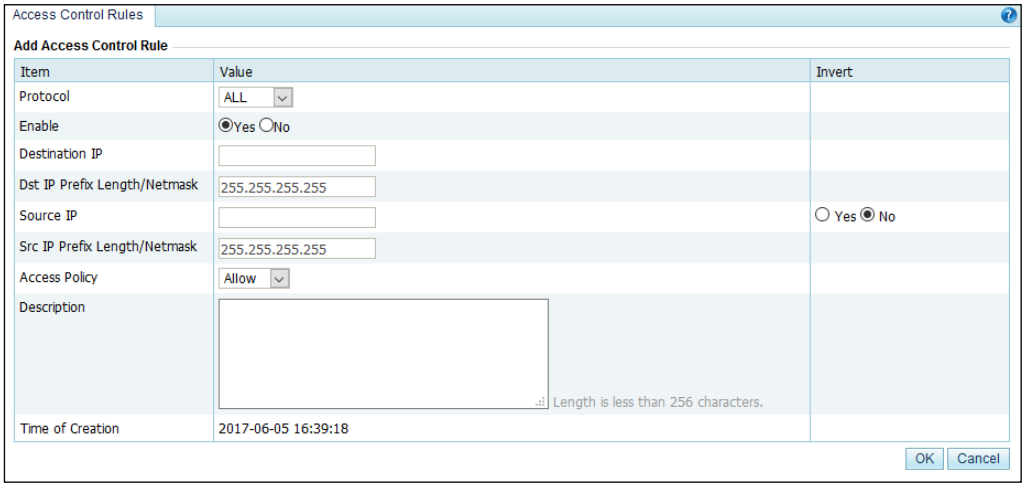


Table 5-21 describes parameters for creating an access control rule.

Table 5-21 Parameters for creating an access control rule

Parameter	Description
Protocol	Protocol that a packet uses. Five values are available: **TCP**, **UDP**, **ICMP**, **ICMPv6**, and **All**. **All** means all the four protocols.
Enable	Controls whether to enable the access control rule. • **Yes**: enables the rule. • **No**: disables the rule.
Destination IP	IP address of the server to be protected. You can type an IPv4 or IPv6 address according to the actual network deployment. The value **0.0.0.0** indicates all destination IP addresses.
Dst IP Prefix/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the destination IP address.
Destination Port	Server port to be protected. This parameter is available only when **Protocol** is set to **TCP** or **UDP**. You can specify a port ranging from 0 to 65535.
Source IP	Client IP address to be protected. You can type IPv4 or IPv6 addresses according to the actual network deployment.
Src IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the client IP address.
Source Port	Source port to be protected against. This parameter is available only when **Protocol** is set to **TCP** or **UDP**. You can specify a port ranging from 0 to 65535. If this parameter is not specified, the ADS device enables the access control policy for all connections of the source IP address.
Access Policy	Action performed by the ADS device on packets with specified signatures. It has the following options: • **Allow:** allows such packets to pass through. • **Drop**: drops the packets once they are detected. • **Protect**: enables a protection policy when the packets pass through the device.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time generated by the system on the creation of the rule. It cannot be edited.
Invert	Controls whether to invert the operation. The value **Yes** indicates the ADS device inverts the parameter setting. For example, if you invert the source IP address 192.168.7.21, all IP addresses except 192.168.7.21 will be protected against.

Step 3 Set parameters and click **OK** to save the settings.

----End

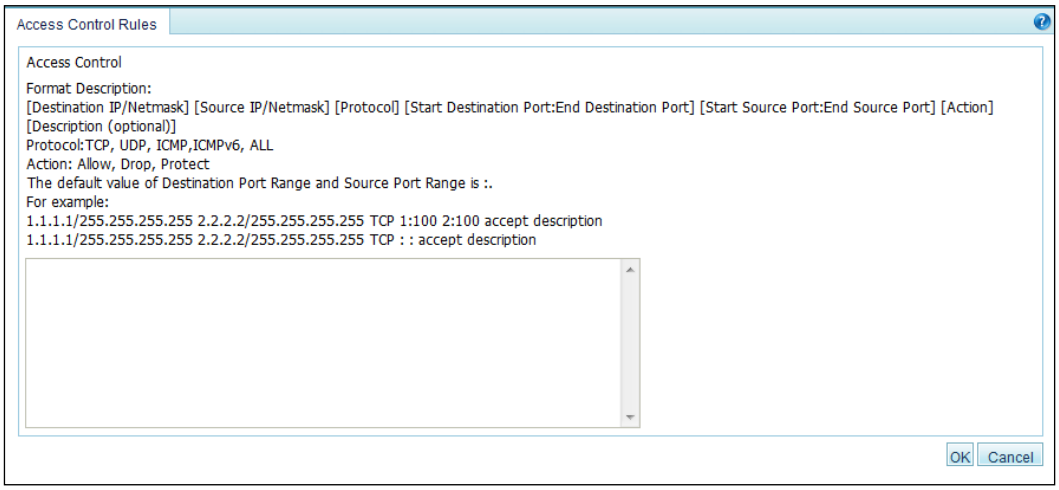
5.2.1.2 Creating Access Control Rules in Batches

You can create access control rules in batches on the ADS device by performing the following steps:

Step 1 Choose **Policies** > **Access Control** > **Access Control Rules**.

Step 2 Click **Import**.

Figure 5-62 Creating access control rules in batches



Step 3 Type multiple access control rules as prompted.

Pay attention to the following format specifications:

- [destination IP/netmask] [source IP/subnet mask] [protocol] [start of destination port:end of destination port] [start of source port:end of source port] [action]
- Protocol: **TCP**, **UDP**, **ICMP**, **ICMPv6**, and **All**.
- Action: **Allow**, **Drop**, and **Protect**.
- If the value range of **Destination Port** and **Source Port** is not defined, the semicolon (:) is used to replace their values by default.

Note	The ADS device supports the IPv4/IPv6 dual-stack. Therefore, you can configure either IPv4 addresses or IPv6 addresses in access control rules.

Step 4 After the parameter configuration is complete, click **OK** to save the settings.

----End

5.2.1.3 Enabling/Disabling Access Control Rules

The ADS system can control the data passing through the device only based on enabled access control rules. Disabled access control rules are invalid.

The ADS device allows the administrator to enable or disable access control rules in batches, thereby avoiding frequent deletions and additions. If some access control rules are not required currently, you can disable them.

On the **Access Control Rules** page, **Status** is **Enabled** for enabled rules and **Disabled** for disabled rules.

Enabling Access Control Rules

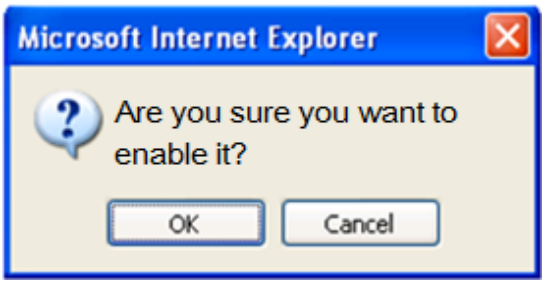
To enable access control rules, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Access Control Rules**.

Step 2 Select one or more disabled access control rules (select the **Select All** check box to select all rules) and click **Enable**.

A dialog box appears, as shown in Figure 5-63.

Figure 5-63 Enabling access control rules



Step 3 Click **OK** to enable the selected rules.

Then, the ADS device can control the data passing through it based on such rules.

----End

Disabling Access Control Rules

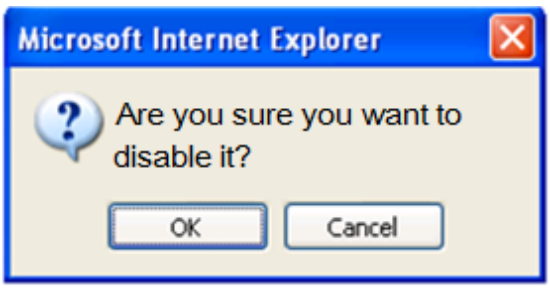
To disable access control rules, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Access Control Rules**.

Step 2 Select one or more enabled access control rules (select **the Select All** check box to select all rules) and click **Disable**.

The following dialog box appears, as shown in Figure 5-64.

Figure 5-64 Disabling access control rules



Step 3 Click **OK** to disable the selected rules.

Then, the ADS device allows the data matching the rules to pass through.

----End

5.2.1.4 Rearranging Access Control Rules

Access control rules are matched in a top-down manner. If multiple access control rules are available, you can rearrange the rules to change the rule matching sequence. As rules with the following settings have the highest priority, they are always at the top of the rule list and cannot be moved:

- The destination IP address is 0.0.0.0 (indicating that all destination IP addresses) and both the source port and destination port are empty.
- The destination IP address is 0.0.0.0 (indicating that all destination IP addresses) and either the source port or destination port is empty.
- The destination IP address is not 0.0.0.0 and both the source port and destination port are empty.
- The destination IP address is not 0.0.0.0 and either the source port or destination port is empty.

Rules that can be moved have lower priorities than the preceding rules and therefore are after those rules.

You can click buttons in the **Operation** column to move access control rules:

- Click to move a rule one place up.
- Click to move a rule one place down.
- Click to move a rule to the top of the list, i.e. after rules with the highest priority.
- Click to move a rule to the bottom of the list.

5.2.1.5 Editing an Access Control Rule

After configuring access control rules, you can edit rule parameters by performing the following steps:

Step 1 Choose **Policies** > **Access Control** > **Access Control Rules**.

Step 2 Click to edit rule parameters.

Step 3 After editing parameters, click **OK** to save settings and return to the access control rule list.

----End

5.2.1.6 Deleting Access Control Rules

You can delete one access control rule or multiple rules in batches on the ADS device by using the following methods:

- Method 1: Choose **Policies** > **Access Control** > **Access Control Rules**. Click in the **Operation** column of a rule and click **OK** in the confirmation dialog box to delete this rule.
- Method 2: Choose **Policies** > **Access Control** > **Access Control Rules**. Select one or more access control rules (or select the **Select All** check box to select all rules) to be deleted, click **Delete** to the lower right of the rule list, and then click **OK** in the confirmation dialog box to delete the selected rules.

Note	Frequently adding or deleting access control rules is not advised. If an access control rule is not useful currently, disable it.

5.2.2 Reflection Protection Rules

A reflection protection rule is a software means through which ADS protect against reflection attack traffic passing through it. Specifically, ADS matches packets against such a rule based on the protocol, source port, and other signatures and handles (such as dropping, dropping and adding to the black list, or limiting the rate) matching packets as indicated in the rule.
All reflection protection rules saved on the device are automatically sorted. The system matches packets passing through the device with reflection protection rules referenced in the policy in sequence. Once a rule is hit, the system stops the match.
This section covers the following topics:

- Creating a Reflection Protection Rule
- Editing a Reflection Protection Rule
- Deleting Reflection Protection Rules

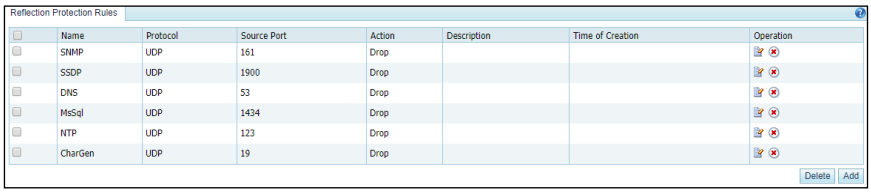
5.2.2.1 Creating a Reflection Protection Rule

Step 1 Choose **Policies** > **Access Control** > **Access Control Rules**.

The reflection protection rule list is displayed, as shown in Figure 5-65.

Initially, the list provides six predefined rules: Chargen, SSDP, NTP, DNS, SNMP, and MS SQL.

Figure 5-65 Reflection protection rules



Step 2 Click **Add**.

A dialog box for creating a reflection protection rule appears, as shown in Figure 5-66.

Figure 5-66 Creating a reflection protection rule

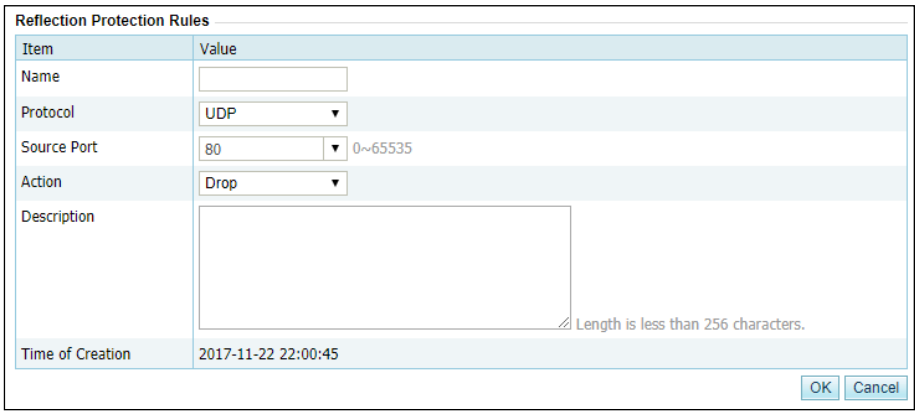


Table 5-22 describes parameters for creating a reflection protection rule.

Table 5-22 Parameters of a reflection protection rule

Parameter	Description
Name	Name of the reflection protection rule. The name must be unique.
Protocol	Protection type. The only value is **UDP**.
Source Port	Source port of the client to be protected against. You can click the drop-down box to select a port number.
Action	Action taken on packets passing through ADS: • **Drop**: drops such packets. • **Drop and add to blacklist**: drops such packets and adds their source IP addresses to the blacklist. Before selecting this option, you must enable the blacklist. For details on the blacklist, see section 5.2.9 Blacklist • **Rate-limiting**: indicates that the maximum number of packets matching this rule that are allowed to pass through per second should not exceed the threshold specified here. Excess packets will be dropped. The value range is 1–65535 pps, with **1000** as the default value.
Description	Presents description of the new rule, which can contain a maximum of 256 characters.
Time of Creation	Indicates the time automatically generated by the system on the creation of the new rule. It cannot be edited.

Step 3 Configure parameters and click **OK** to save the settings.

----End

5.2.2.2 Editing a Reflection Protection Rule

All reflection protection rules can be edited.

Step 1 On the page shown in Figure 5-65, click in the **Operation** column of a reflection protection rule to edit parameters of this rule.

Step 2 Edit parameter settings and click **OK** to save the changes and return to the reflection protection rule list.

----End

5.2.2.3 Deleting Reflection Protection Rules

You can delete one reflection protection rule or delete rules in batches.

Method 1: On the page shown in Figure 5-65, click in the **Operation** column of a reflection protection rule click **OK** in the confirmation dialog box to delete this rule.

Method 2: On the page shown in Figure 5-65, select one or more reflection protection rules (or select the check box in the table header to select all rules), click **Delete** to the lower right of the list, and click **OK** in the confirmation dialog box to delete the selected rules.

5.2.3 GeoIP Rules

The GeoIP library provides mappings between IP addresses and countries. After importing a GeoIP library and configuring a GeoIP rule, you enable ADS to control traffic from certain IP addresses based on geographic locations. In addition, you can configure ADS to take an action (allow, protect, or drop) against packets that are found to match the rule based on the destination IP address and source country.

All GeoIP rules saved on the device are automatically sorted. When a packet reaches ADS, the system matches the packet against GeoIP rules in sequence from the first to the last. After the packet triggers a rule, the system takes the action specified in the rule and stops matching it against other GeoIP rules. GeoIP rules are sorted according to the following principles:

- Rules are automatically sorted in descending order of priority.
- When IPv4 addresses are involved, the rule with the IP address of 0.0.0.0/0.0.0.0 and rules with the netmask of less than 24 bits are all high-priority rules.
- When IPv6 addresses are involved, rules with the prefix length of less than 120 bits are high-priority rules.

This section covers the following topics:

- Creating a GeoIP Rule
- Importing and Exporting a GeoIP Library

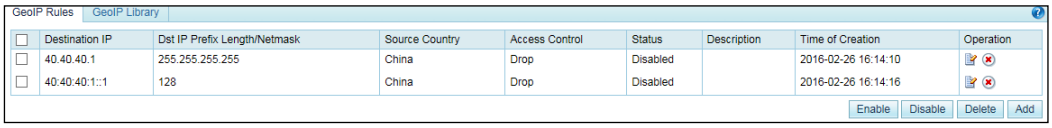
5.2.3.1 Creating a GeoIP Rule

Initially, the GeoIP rule list is empty. To create a GeoIP rule, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **GeoIP Rules**.

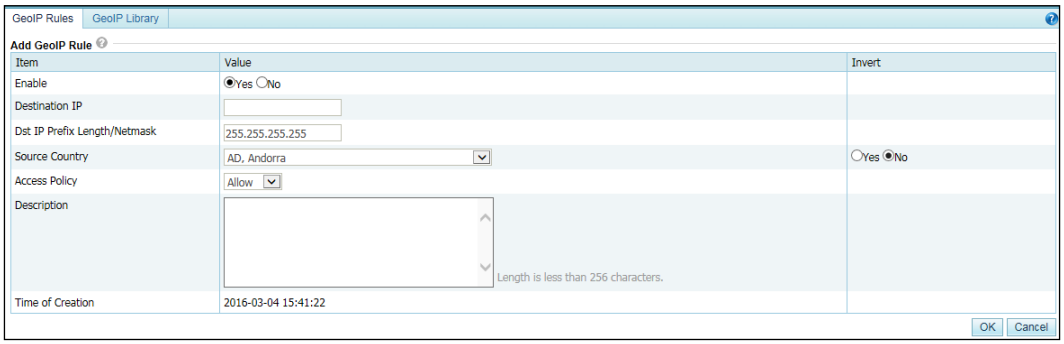
The **GeoIP Rules** page appears, as shown in Figure 5-67.

Figure 5-67 List of GeoIP rules



Step 2 Click **Add** to the lower right of the list.

Figure 5-68 Creating a GeoIP rule



Step 3 On the **Add GeoIP Rule** page, configure parameters.

Table 5-23 Parameters for creating a GeoIP rule

Parameter	Description
Enable	Controls whether to enable the new GeoIP rule. • **Yes**: enables the new rule. • **No**: disables the new rule.
Destination IP	Specifies the IP address of the server under protection. You can type an IPv4 or IPv6 address as required.
Dst IP Prefix Length/Netmask	Specifies the prefix length (for IPv6 address) or netmask (for IPv4 address) of the destination IP address.
Source Country	Specifies the country to which source IP addresses belong.
Access Policy	Specifies the action to be taken against packets that match this rule. It can be any of the following: • **Allow**: allows such packets to pass through ADS. • **Drop**: drops such packets. • **Protect**: does not take any action against such packets at this step, but will still check them against other protection rules.
Description	Presents description of the new rule, which cannot contain more than 256 characters.
Time of Creation	Indicates the time automatically generated by the system on the creation of the new rule. It cannot be edited.
Invert	Controls whether to invert the setting. **Yes** indicates that the setting will be inverted and **No** indicates the opposite.

Step 4 Click **OK** to save the settings.

----End

In addition to creating a GeoIP rule, you can enable, disable, edit, and delete such a rule. The procedures are the same as those for access control rules. For details, see related descriptions in section 5.2.1 Access Control Rules.

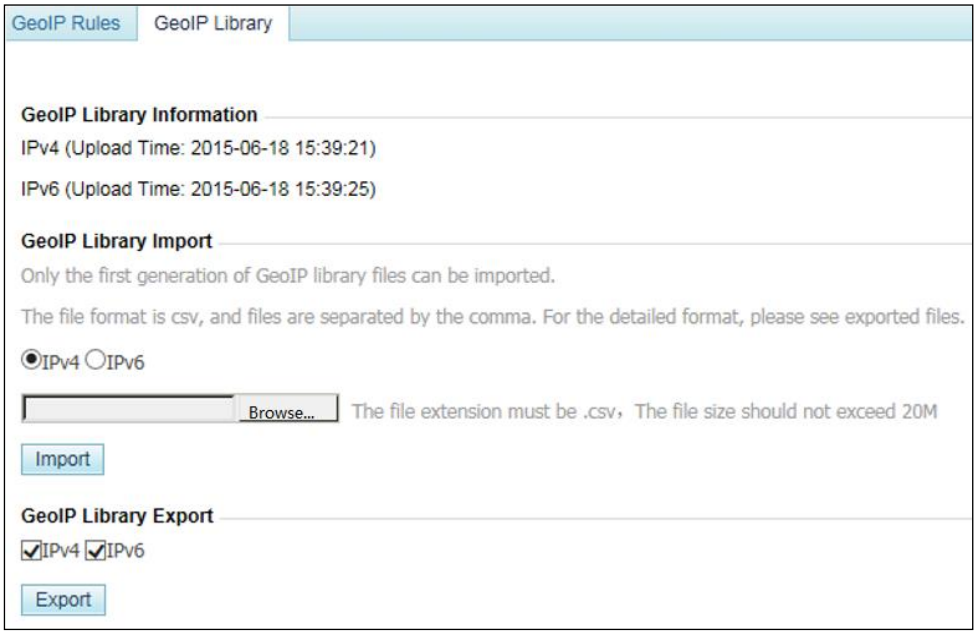
5.2.3.2 Importing and Exporting a GeoIP Library

The GeoIP library supports both IPv4 and IPv6 addresses. When importing a GeoIP library, you must select the file type, which must be **.csv**. The file to be imported cannot exceed 20 MB.

To import and export a GeoIP library, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **GeoIP Rules** > **GeoIP Library**.

Figure 5-69 Viewing the GeoIP library



Step 2 Import or export a GeoIP library.

- Importing a GeoIP library

a. Select an IP protocol, click **Browse**, and then select a file to be imported.

b. Click **Import** to import the GeoIP library.

After the successful import, the IP protocol and upload time are displayed in the **GeoIP Library Information** area. The new library, after being imported, can take effect immediately. However, if ADS is restarted or powered off, library information is lost. To save it as a permanently effective database, you must click **Save** in the upper-right corner after importing the file.

- Exporting a GeoIP library

Select **IPv4** or **IPv6**, or both, and then click **Export** in the **GeoIP Library Export** area.

----End

5.2.4 Regular Expression Rules

Regular expression rules are available for the ADS device to control, via software, the traffic passing through it. ADS can determine how to process (allow, drop, drop and add to blacklist, drop and disconnect, or limit the rate) packets matching such a rule based on signatures such as the regular expression, offset, depth, and minimum payload length.

A maximum of 32 regular expression rules can be configured. The system matches packets passing through the device with regular expression rules in sequence and stops the match once a matched rule is hit.

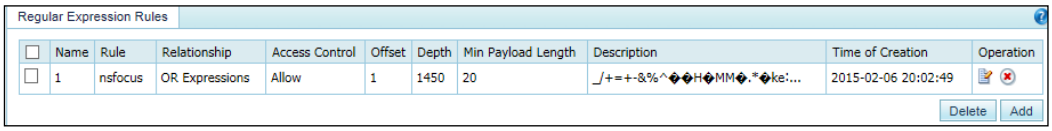
A regular expression rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting a regular expression rule are the same as those for access control rules.

To create a regular expression rule, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Regular Expression Rules**.

Initially, the rule list is empty.

Figure 5-70 List of regular expression rules



Step 2 Click **Add**.

Figure 5-71 Creating a regular expression rule

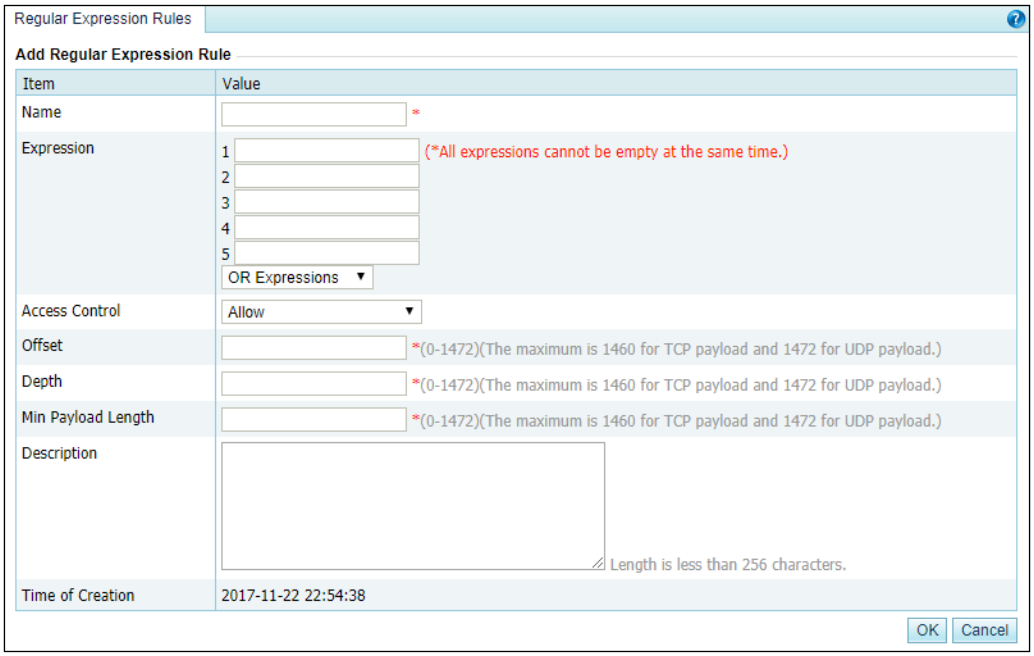


Table 5-24 describes parameters for creating a regular expression rule.

Table 5-24 Parameters for creating a regular expression rule

Parameter	Description
Name	Unique name of the regular expression rule.

Parameter	Description
Expression	Expressions for the rule. You can enter a maximum of five expressions and then select **OR Expressions** or **AND Expressions**.
Access Control	Specifies the action the ADS device takes for packets with specified signatures. It has the following values: • **Allow**: allows such packets to pass through. • **Drop**: drops such packets once they are detected. • **Drop and add to blacklist**: drops such packets and adds their source IP addresses to the blacklist. Before selecting this option, you must enable the blacklist. For details on the blacklist, see section 5.2.9 Blacklist. • **Drop and disconnect**: drops such packets and disconnects the connection to their destination IP addresses. • **Rate-limiting**: indicates that the maximum number of packets matching this rule that are allowed to pass through per second should not exceed the threshold specified here. Excess packets will be dropped. The value range is 1–6000000 pps, with **4000** as the default value.
Offset	Payload offset, counted from the first byte in the payload field of a TCP packet.
Depth	Specifies how deep the rule is matched. It is expressed in bytes.
Min Payload Length	Length of the payload below which the packet is not matched with regular expression rules. This does not affect subsequent protection actions.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

Step 3 Set parameters and click **OK** to save the settings.

----End

5.2.5 DNS Keyword Checking

DNS keyword checking is a process by which ADS controls, via software, DNS traffic flowing through the ADS device. In addition, ADS specifies the method (allow, drop, add to blacklist, add to whitelist, or limit the rate) of processing data packets flowing through the device that match the DNS keyword checking rule based on source IP addresses and specific DNS fields. DNS keyword checking blocks traffic from illegitimate users, but does not indiscriminately block all packets from a source IP address. This reduces the possibility of blocking legitimate IP addresses.

You can configure up to 32 DNS keyword checking rules, which can take effect only after being referenced in a group protection policy or default protection policy. When a packet reaches ADS, the system matches the packet against DNS keyword checking rules in sequence. Once the packet hits a rule, the system takes the action specified in the rule and stops matching the packet against other rules.

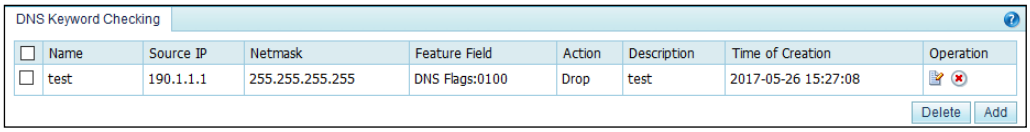
A DNS keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting DNS keyword checking rules are the same as those for access control rules.

To create a DNS keyword checking rule, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **DNS Keyword Checking**.

Initially, the rule list is empty.

Figure 5-72 List of DNS keyword checking rules



Step 2 Click **Add**.

Figure 5-73 Creating a DNS keyword checking rule

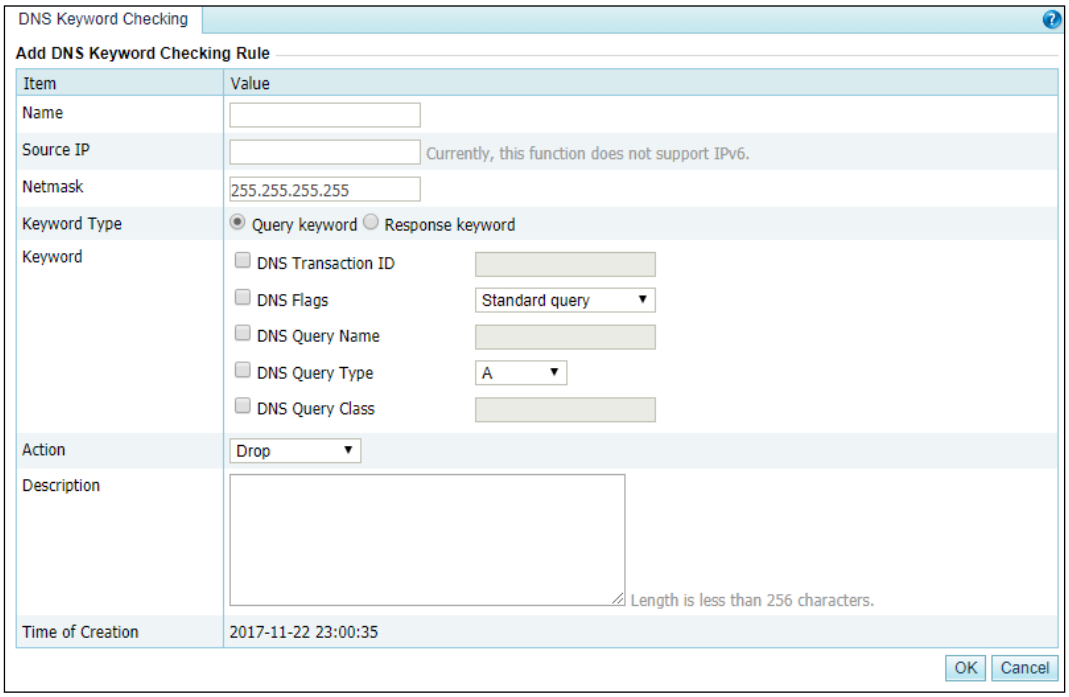


Table 5-25 describes parameters for creating a DNS keyword checking rule.

Table 5-25 Parameters of a DNS keyword checking rule

Parameter	Description
Name	Name of the DNS keyword checking rule, containing 1–20 characters of letters, digits, and/or underscores.
Source IP	Specifies the source IP address. The value **0.0.0.0** indicates all source IP addresses.
Netmask	Specifies the netmask of the source IP address.
Keyword Type	Specifies what kind of packets will be checked. Options include **Query keyword** and **Response keyword**.
Keyword	Specifies the type of keywords to be checked. You can select one or more.

Parameter	Description
Action	Specifies the action to be taken against a packet that matches a DNS keyword checking rule. It can be any of the following: • **Allow**: indicates that a packet with the specified signature will be allowed through ADS and, after that, will not be checked against any pattern matching rules. • **Drop**: indicates that ADS drops a packet with the specified signature. • **Drop+Blacklist**: indicates that ADS drops a packet with the specified signature and adds its source IP address to the blacklist. To select this option, you must enable the blacklist function in advance. For details about this function, see section 5.2.9 Blacklist. • **Allow+Whitelist**: indicates that ADS allows a packet with the specified signature to pass through and adds its IP address to the whitelist. To select this option, you must enable the whitelist function in advance. For details about this function, see section 5.2.10 Whitelist. • **Rate-limiting**: indicates that the maximum number of packets matching this rule that are allowed to pass through per second should not exceed the threshold specified here. Excess packets will be dropped. The value range is 1–6000000 pps, with **4000** as the default value.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

Step 3 Set parameters and click **OK** to save the settings.

----End

5.2.6 HTTP Keyword Checking

HTTP keyword checking is a process by which ADS software controls HTTP traffic flowing through the ADS device. In addition, ADS specifies the method (allow, drop, disconnect, add to blacklist, add to whitelist, or limit the rate) of processing data packets flowing through the device that match the HTTP keyword checking rule based on source IP addresses and specific HTTP fields. HTTP keyword checking blocks traffic from illegitimate users, but does not indiscriminately block all packets from a source IP address. This reduces the possibility of blocking legitimate IP addresses.

You can configure up to 32 HTTP keyword checking rules, which can take effect only after being referenced in a group protection policy or default protection policy. When a packet reaches ADS, the system matches the packet against HTTP keyword checking rules in sequence. Once the packet hits a rule, the system takes the action specified in the rule and stops matching the packet against other rules.

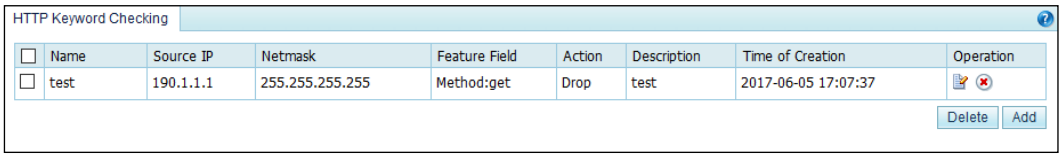
An HTTP keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting HTTP keyword checking rules are the same as those for access control rules.

To create an HTTP keyword checking rule, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **HTTP Keyword Checking**.

Initially, the rule list is empty.

Figure 5-74 List of HTTP keyword checking rules



Step 2 Click **Add**.

Figure 5-75 Creating an HTTP keyword checking rule

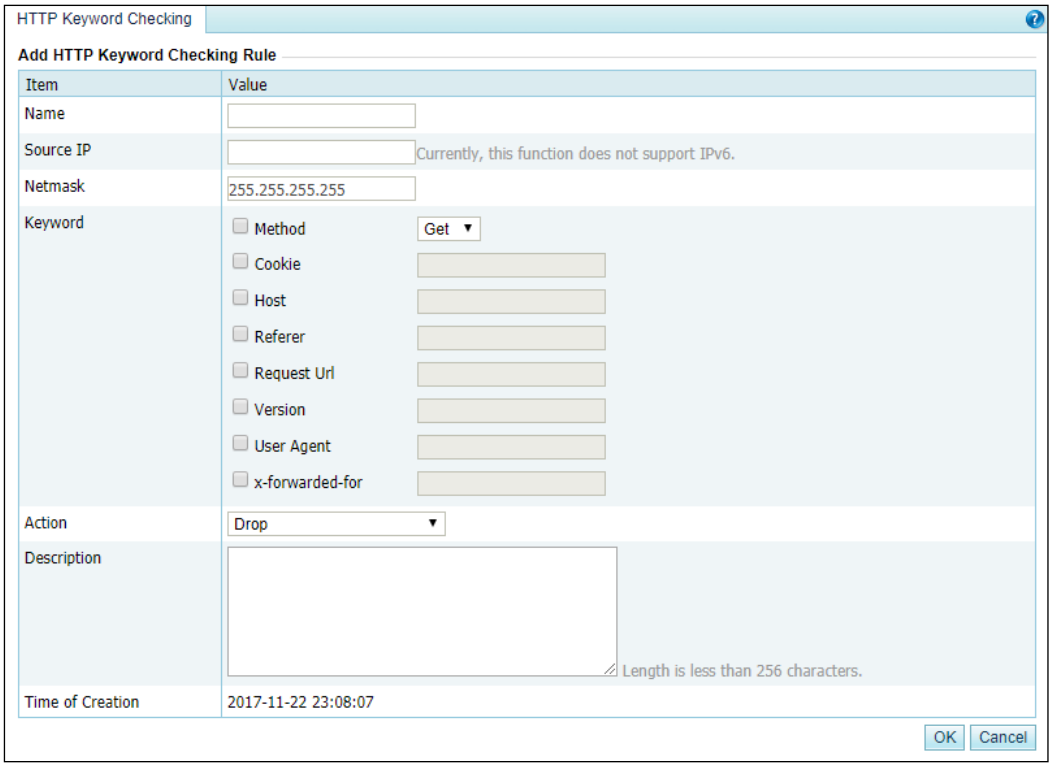


Table 5-26 describes parameters for creating an HTTP keyword checking rule.

Table 5-26 Parameters of an HTTP keyword checking rule

Parameter	Description
Name	Name of the HTTP keyword checking rule, containing 1–20 characters of letters, digits, and/or underscores.
Source IP	Specifies the source IP address. The value **0.0.0.0** indicates all source IP addresses.
Netmask	Specifies the netmask of the source IP address.
Keyword	Specifies the type of keywords to be checked. You can select one or more.
Action	Specifies the action to be taken against a packet that matches an HTTP keyword checking rule. It can be any of the following:

Parameter	Description
	• **Allow**: indicates that a packet with the specified signature will be allowed through ADS. • **Drop**: indicates that ADS drops a packet with the specified signature. • **Drop+Blacklist**: indicates that ADS drops a packet with the specified signature and adds its source IP address to the blacklist. To select this option, you must enable the blacklist function in advance. For details about this function, see section 5.2.9 Blacklist. • **Drop+Disconnect**: indicates ADS drops a packet with the specified signature and disconnects the current connection. • **Drop+Blacklist+Disconnect**: indicates that ADS drops a packet with the specified signature, disconnects the current connection, and adds its source IP address to the blacklist. To select this option, you must enable the blacklist function in advance. • **Allow+Whitelist**: indicates that ADS allows a packet with the specified signature to pass through and adds its source IP address to the whitelist. To select this option, you must enable the whitelist function in advance. For details about this function, see section 5.2.10 Whitelist. • **Rate-limiting**: indicates that the maximum number of packets matching this rule that are allowed to pass through per second should not exceed the threshold specified here. Excess packets will be dropped. The value range is 1–6000000 pps, with **4000** as the default value.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

Step 3 Set parameters and click **OK** to save the settings.

----End

5.2.7 Connection Exhaustion Rules

A connection exhaustion rule protects against connection exhaustion attacks by restricting the number of IP connections in a specified network segment. This section covers the following topics:

- Creating a Connection Exhaustion Rule
- Editing a Connection Exhaustion Rule
- Deleting Connection Exhaustion Rules

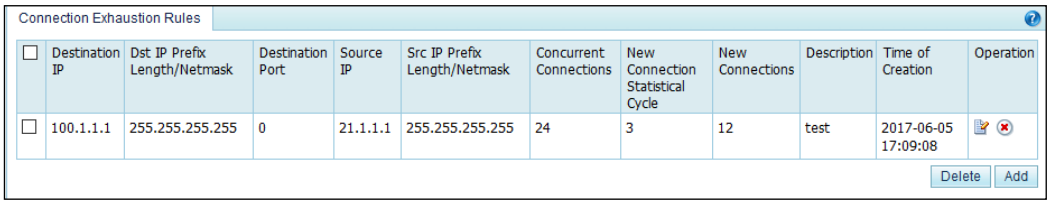
5.2.7.1 Creating a Connection Exhaustion Rule

To create a connection exhaustion rule, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Connection Exhaustion Rules**.

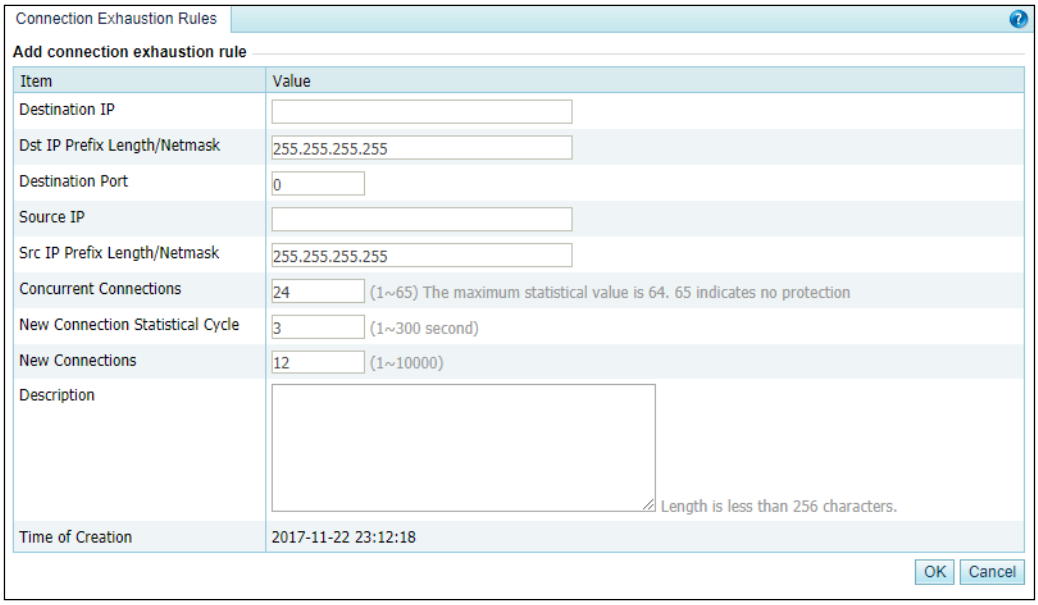
Initially, the rule list is empty.

Figure 5-76 List of connection exhaustion rules



Step 2 Click **Add**.

Figure 5-77 Creating a connection exhaustion rule



Note	A maximum of 128 connection exhaustion rules can be added. A connection exhaustion rule can take effect only when connection exhaustion is enabled in a protection group policy or default protection policy. Meanwhile, the blacklist function must be enabled for the use of connection exhaustion rules.

Table 5-27 describes parameters for creating a connection exhaustion rule.

Table 5-27 Parameters for creating a connection exhaustion rule

Parameter	Description
Destination IP	IP address of the server to be protected. You can type an IPv4 or IPv6 address according to the actual network deployment.
Dst IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address of the server to be protected.
Destination Port	Server ports to be protected. The port number ranges from 0 to 65535.
Source IP	Client IP address to be protected. You can type IPv4 or IPv6 addresses according to

Parameter	Description
	the actual network deployment.
Src IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the client IP address.
Concurrent Connections	Threshold of allowed concurrent connections from a source IP address. If this threshold is exceeded, the system considers the source IP address abnormal and adds it to the blacklist. The value ranges from 1 to 65. **65** indicates no protection.
New Connection Statistical Cycle	Period during which new connections from the source IP address to the destination (IP address and port) are counted. The value ranges from 1 to 300 seconds.
New Connections	Threshold of allowed new connections from a source IP address within the specified statistical cycle. If this threshold is exceeded, the system considers the source IP address abnormal and adds it to the blacklist. The value ranges from 1 to 10000. Setting the source IP address and netmask to 0.0.0.0/0.0.0.0 indicates all source IP addresses.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

Step 3 Set parameters and click **OK** to save the settings.

----End

5.2.7.2 Editing a Connection Exhaustion Rule

After configuring connection exhaustion rules, you can edit rule parameters by performing the following steps:

Step 1 Choose **Policies** > **Access Control** > **Connection Exhaustion Rules**.

Step 2 Click in the **Operation** column to edit parameters of a rule.

Step 3 After editing parameters, click **OK** to save settings and return to the connection exhaustion rule list.

----End

5.2.7.3 Deleting Connection Exhaustion Rules

You can delete one connection exhaustion rule or multiple rules in batches on the ADS device by adopting either of the following methods:

- Method 1: Choose **Policies** > **Access Control** > **Connection Exhaustion Rules**. Click in the **Operation** column of a rule and then click **OK** in the confirmation dialog box to delete a rule.
- Method 2: Choose **Policies** > **Access Control** > **Connection Exhaustion Rules**. Select one or more connection exhaustion rules (or select the **Select All** check box to select all rules) to be deleted, click **Delete** to the lower right of the rule list, and then click **OK** in the confirmation dialog box to delete the selected rules.

5.2.8 URL-ACL Protection Rules

A URL-ACL rule controls access to URLs of a server and is usually used together with connection exhaustion rules. This section covers the following topics:

- Creating a URL-ACL Protection Rule
- Editing a URL-ACL Protection Rule
- Deleting a URL-ACL Protection Rule
- Changing the Priority of a URL-ACL Protection Rule

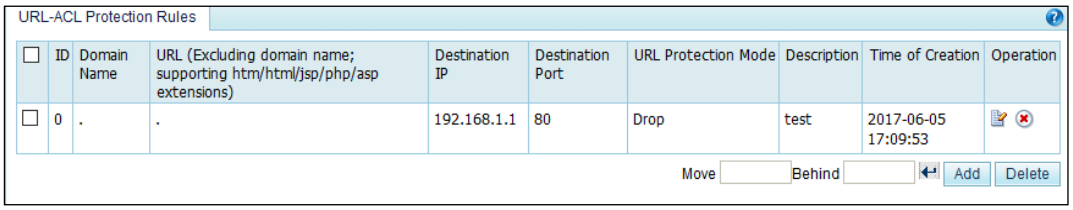
5.2.8.1 Creating a URL-ACL Protection Rule

To create a URL-ACL rule, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **URL-ACL Protection Rule**.

Initially, the rule list is empty.

Figure 5-78 List of URL-ACL rules



Step 2 Click **Add**.

Figure 5-79 Creating a URL-ACL rule

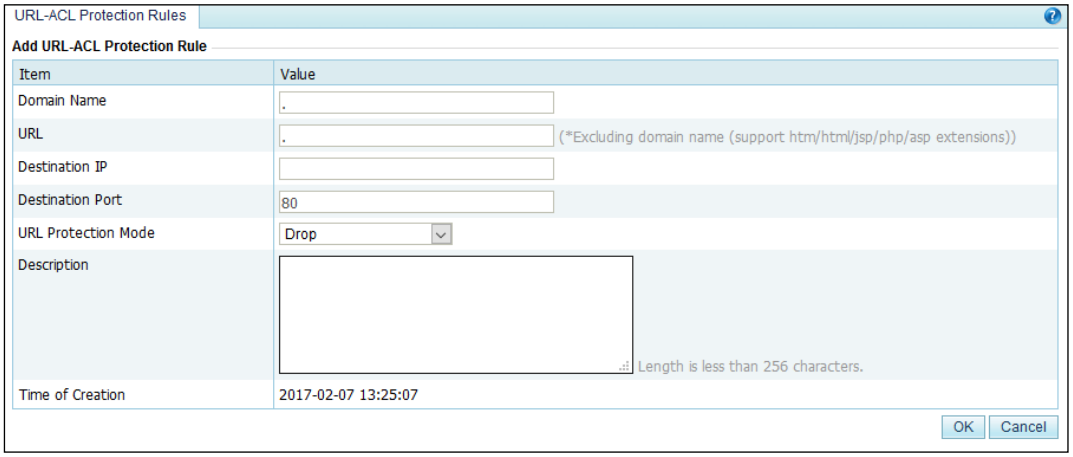


Table 5-28 describes parameters for creating a URL-ACL rule.

Table 5-28 Parameters for creating a URL-ACL rule

Parameter	Description
Domain Name	Domain name of a URL protection object. The symbol "." indicates that this rule is valid for all domain names.
URL	Relative path of a URL protection object, that is, URL excluding the domain name. The symbol "." indicates that this rule is valid for all URLs.
Destination IP	IP address of the server. You can type an IPv4 or IPv6 address according to the actual network deployment.
Destination Port	TCP port of the server.
URL Protection Mode	Action to be taken on packets that match this rule. The value can be one of the following: • **Drop**: drops packets. • **Trust**: allows packets to pass. • **Block proxy**: blocks the proxy if it is possible to use the proxy to transfer packets. • **Limit source IP speed**: limits the rate above which packets from the source IP address are forwarded.
Threshold	Maximum rate above which packets are forwarded. The value ranges from 1 to 10000, in pps. ADS will drop excess (depending on your choice) packets. This parameter is available only when **URL Protection Mode** is set to **Limit source IP speed**.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

Step 3 Set parameters and click **OK** to save the settings.

----End

5.2.8.2 Editing a URL-ACL Protection Rule

After configuring URL-ACL rules, you can edit rule parameters by performing the following steps:

Step 1 Choose **Policies** > **Access Control** > **URL-ACL Protection Rule**.

Step 2 Click in the **Operation** column to edit parameters of the rule.

Step 3 After editing parameters, click **OK** to save settings and return to the URL-ACL rule list.

----End

5.2.8.3 Deleting a URL-ACL Protection Rule

You can delete one URL-ACL rule or multiple rules in batches on the ADS device by adopting either of the following methods:

Method 1: Choose **Policies** > **Access Control** > **URL-ACL Protection Rule**. Click in the **Operation** column of a rule and then click **OK** in the confirmation dialog box to delete a rule.

Method 2: Choose **Policies** > **Access Control** > **URL-ACL Protection Rule**. Select one or more URL-ACL rules (or select the **Select All** check box to select all rules) to be deleted, click **Delete** to the lower right of the rule list, and then click **OK** in the confirmation dialog box to delete selected rules.

5.2.8.4 Changing the Priority of a URL-ACL Protection Rule

On the **URL-ACL Protection Rule** page, you can change the order of rules. Rules are sorted in the descending order of priority, that is, rule 0 has the highest priority to match packets.

Change the priority of the URL-ACL rules in the following ways:

- Use icons and to change the order of URL-ACL rules.
- Type the ID of the target rule to be adjusted below the list, and then click .

5.2.9 Blacklist

The blacklist policy is used to filter source IP addresses of packets. Once a source IP address matches an address on the blacklist, the ADS device blocks packets from this IP address without performing further detection. Therefore, this policy improves the detection performance of the ADS device.

Addresses can be added to the blacklist using either of the following methods:

- You can manually add IP addresses to the blacklist or import a blacklist file.
- The algorithm automatically adds IP addresses to the blacklist.

IP addresses can be automatically added to the blacklist in the following ways:

- Once attack packets are filtered out through pattern matching, the source IP address of such packets is automatically added to the blacklist. For description of pattern matching, see section 8.2 Pattern Matching Rules.
- When **URL Protection Mode** is set to **Drop** for URL-ACL rules, the ADS device adds the source IP to the blacklist once detecting an HTTP request amid IP packets and matching the source IP address with a URL-ACL rule.
- When **URL Protection Mode** is set to **Block proxy** for URL-ACL rules, the ADS device adds the IP address of the proxy server to the blacklist when detecting an HTTP request from a proxy server in packets and matching the source IP address with a URL-ACL rule.
- After **Slow attack protection** is triggered, if the blacklist function is enabled, the system adds source IP addresses of matching packets to the blacklist.
- After a TCP control policy is triggered, if **SYN Source Bandwidth Limit** is set to **Drop and add to blacklist**, the system adds the source IP address of corresponding packets to the blacklist.
- After an IP behavior control policy is triggered, if **SYN Source Bandwidth Limit** or **Empty Connection Check** is set to **Drop and add to blacklist**, the system adds the source IP address of corresponding packets to the blacklist.
- After an HTTPS protection policy is triggered, if **Add Abnormal IP to Blacklist** is set to **Yes**, the system adds the source IP address of the client that fails to be authenticated with the HTTPS protection algorithm to the blacklist.
- After a TCP regular expression rule is triggered, the system adds the source IP address that matches the regular expression rule to the blacklist.
- If **Add Abnormal IP to Blacklist** is set to **Yes**, the system adds source IP addresses that fail the HTTP keyword check to the blacklist.

- If **Add Abnormal IP to Blacklist** is set to **Yes**, the system adds source IP addresses that fail the DNS keyword check to the blacklist.
- If the number of new connections from a source IP address exceeds the threshold within the new connection statistical cycle of a connection exhaustion rule, ADS deems this IP address abnormal and automatically adds it to the blacklist.

This section describes how to enable or disable a blacklist, add a blacklist entry manually, delete a blacklist entry, and clear a blacklist.

Note	• You can add, delete, or clear blacklist entries only when the blacklist function is enabled. • The whitelists has a higher priority than the blacklist. Therefore, if the source IP address of packets is included in both the blacklist and whitelist, the ADS device allows such packets to pass through.

You can perform the following operations regarding the blacklist:

- Enabling and Disabling the Blacklist Function
- Adding a Blacklist Entry
- Viewing Blacklist Entries
- Deleting Blacklist Entries
- Clearing Blacklist Entries
- Searching the Blacklist
- Importing a Blacklist File
- Viewing the Import Result
- Exporting a Blacklist File

Enabling and Disabling the Blacklist Function

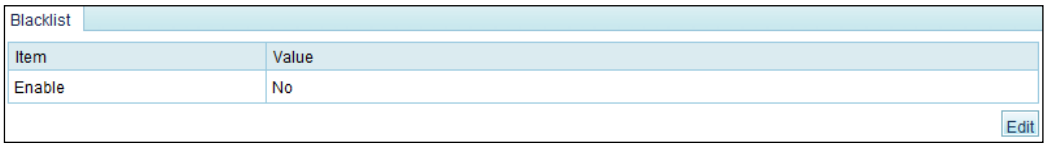
Enabling the Blacklist Function

To enable the blacklist function, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Blacklist**.

Initially, the blacklist function is disabled.

Figure 5-80 Blacklist status

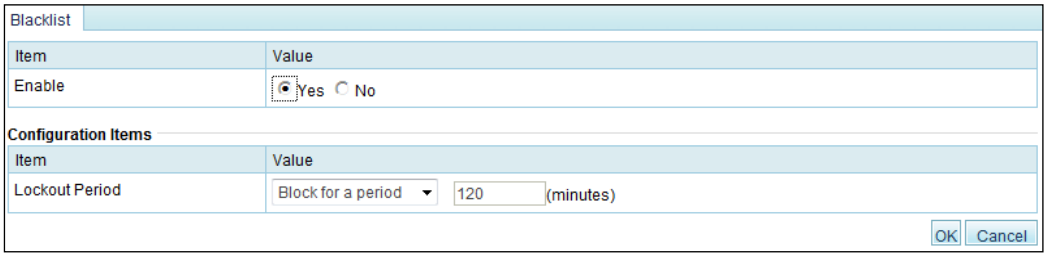


Step 2 Click **Edit** and then select **Yes** to enable the blacklist function. See Figure 5-81.

The lockout period refers to the duration when a blacklisted IP address is blocked. The option **Block for a period** indicates that the IP address is blocked and packets from this address are

dropped in the specified period. The option **Block permanently** indicates that the IP address is permanently blocked and packets from this address are always dropped.

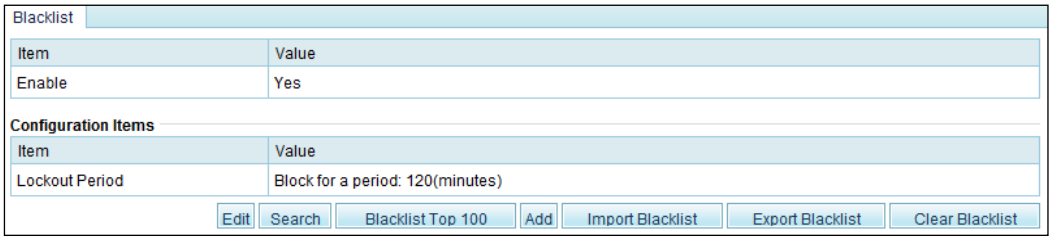
Figure 5-81 Enabling the blacklist policy



Step 3 Click **OK** to return to the previous page.

As shown in Figure 5-82, the blacklist function is enabled and blacklist configuration items are available.

Figure 5-82 Blacklist function enabled



----End

Disabling the Blacklist Function

To disable the blacklist function, perform the following steps:

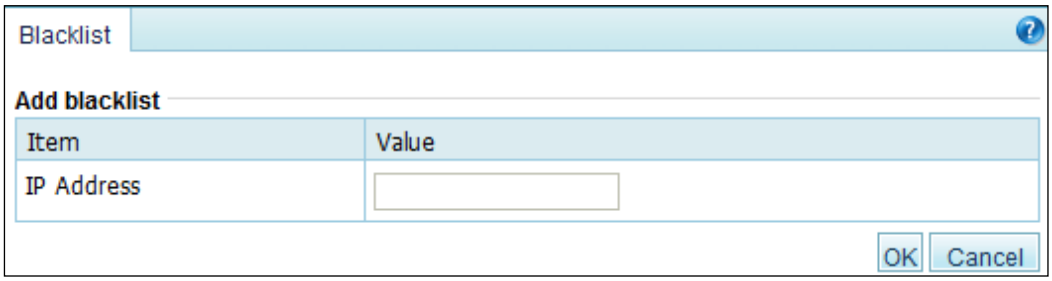
On the page shown in Figure 5-81, select **No**. Then the value of **Enable** turns to **No**, as shown in Figure 5-80.

Adding a Blacklist Entry

To add a blacklist entry manually, perform the following steps:

Step 1 On the page shown in Figure 5-82, click **Add** to add a blacklist entry.

Figure 5-83 Adding a blacklist entry



Step 2 On the page shown in Figure 5-83, type the source IP address (IPv4 address only) of packets to be blocked, and then click **OK** to save the settings.

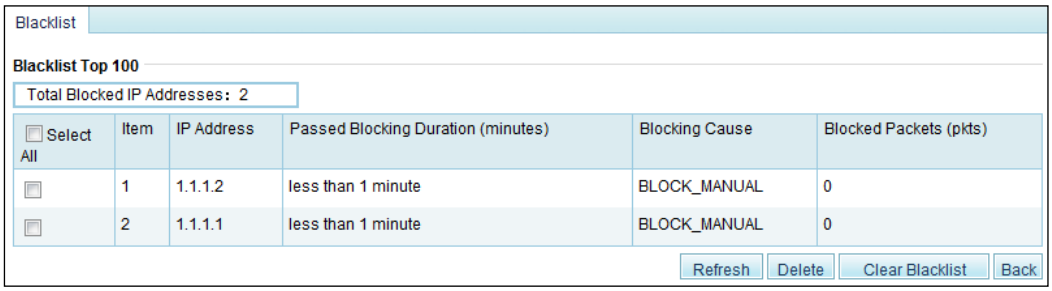
----End

Viewing Blacklist Entries

On the page shown in Figure 5-82, click **Blacklist Top 100**. The system displays a maximum of 100 IP addresses blocked recently, as shown in Figure 5-84.

Note	When the blacklist contains more than 100 IP addresses, the system displays only the most recent 100 ones. Blacklisted IP addresses not displayed are also valid.

Figure 5-84 Viewing blacklist entries



Deleting Blacklist Entries

To delete a blacklist entry, perform the following steps:

Step 1 On the page shown in Figure 5-82, select one or more blacklist entries and then click **Delete**.

Step 2 In the confirmation dialog box, click **OK**.

----End

Clearing Blacklist Entries

To clear blacklist entries, perform the following steps:

Step 1 On the page shown in Figure 5-82 or Figure 5-84, click **Clear Blacklist**.

Step 2 In the confirmation dialog box, click **OK**.

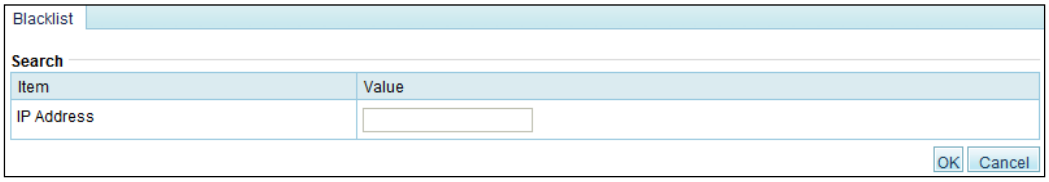
----End

Searching the Blacklist

To search the blacklist for an IP address, perform the following steps:

Step 1 On the page shown in Figure 5-82, click **Search**.

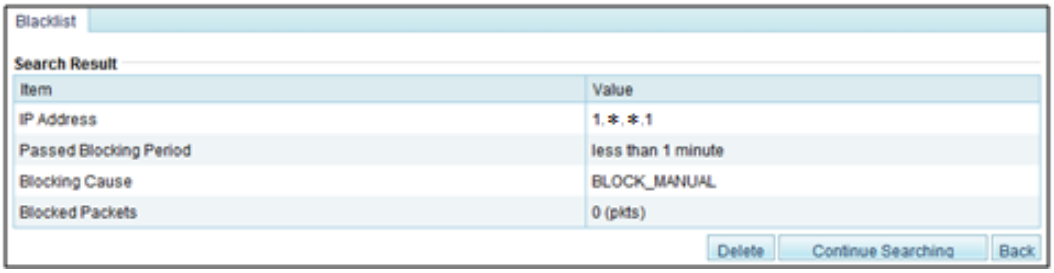
Figure 5-85 Searching for an IP address



Step 2 On the **Search** page shown in Figure 5-85, type an IP address, and click **OK**.

The blacklist search result is displayed, as shown in Figure 5-86.

Figure 5-86 Blacklist search result



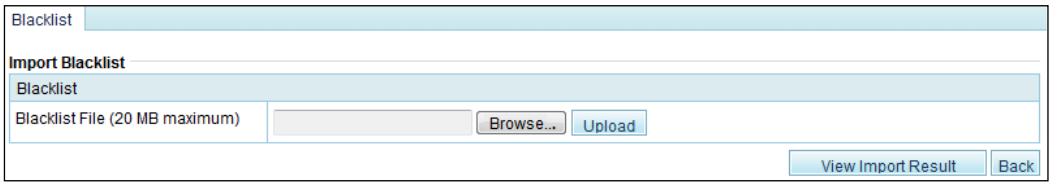
----End

Importing a Blacklist File

To import a blacklist file, perform the following steps:

Step 1 On the page shown in Figure 5-82, click **Import Blacklist**.

Figure 5-87 Importing a blacklist file



Note	The blacklist file must be a **.txt** file whose filename does not contain Chinese characters; otherwise, the file cannot be imported.

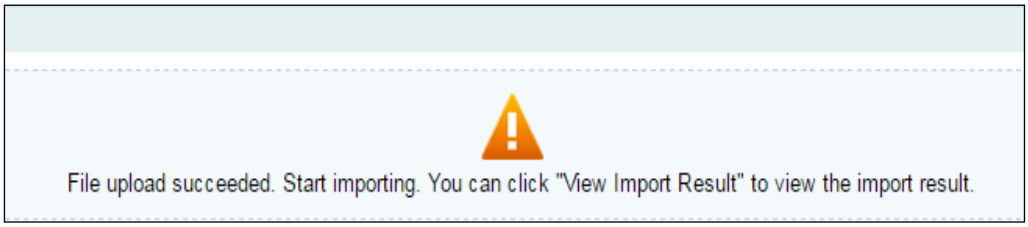
Step 2 On the page shown in Figure 5-87, click **Browse**.

Step 3 Select the blacklist file and click **Open** to return to the blacklist import page.

Step 4 Click **Upload**.

After the upload is complete, the system prompts that the file is successfully imported, as shown in Figure 5-88.

Figure 5-88 Import success prompt



After the blacklist file is imported, the system automatically switches to the page shown in Figure 5-87.

----End

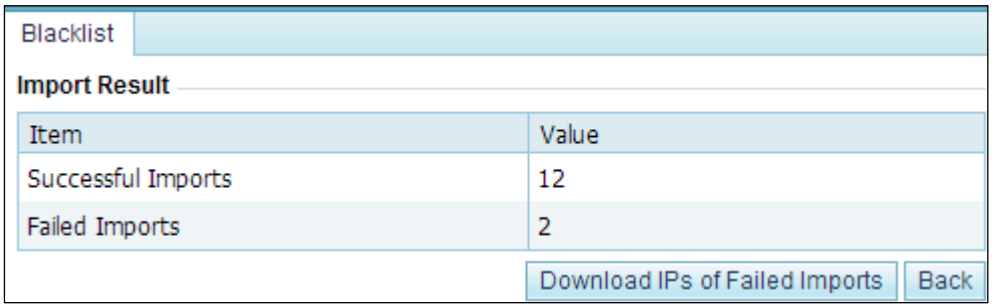
Viewing the Import Result

To view the import result, perform the following steps:

Step 1 On the page shown in Figure 5-87, click **View Import Result**.

Then the number of IP addresses successfully imported and that of IP addresses failing to be imported are displayed, as shown in Figure 5-89.

Figure 5-89 Viewing import results



Step 2 Click **Back** to return to the blacklist configuration page.

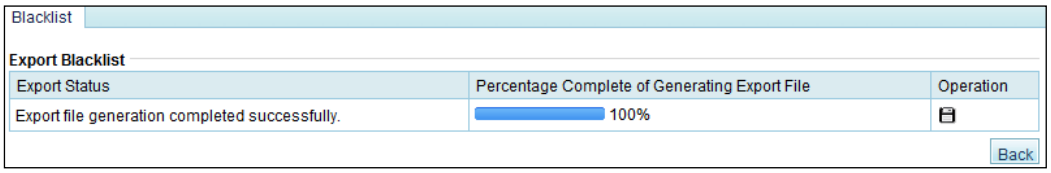
----End

Exporting a Blacklist File

To export a blacklist file, perform the following steps:

Step 1 On the page shown in Figure 5-82, click **Export Blacklist**.

Figure 5-90 Exporting a blacklist file



Step 2 Click in the **Operation** column

Step 3 In the pop-up download box, click **Save**.

The blacklist file is thus saved in a local disk drive.

----End

5.2.10 Whitelist

After the whitelist function is enabled, ADS checks whether the source IP address of packets matches any address (an IPv4 address or IPv6 address) in the whitelist. If the matched address is found, the ADS engine allows these packets to pass through, without executing access control rules or protection algorithms, thereby improving the system performance.

Note	The whitelist has a higher priority than the blacklist. Therefore, if the source IP address of packets is included in both the blacklist and whitelist, the ADS device allows such packets to pass through.

You can perform the following operations regarding the whitelist:

- Enabling and Disabling the Whitelist Function
- Importing a Whitelist File
- Viewing the Import Result
- Querying the Whitelist
- Clearing the Whitelist
- Clearing the Configuration
- Downloading the Configuration
- Reloading the Whitelist File

Enabling and Disabling the Whitelist Function

By default, the whitelist function is disabled on the ADS device. you need to enable this function before using it.

Enabling the Whitelist Function

To enable the whitelist function, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Whitelist**.

By default, the whitelist function is disabled.

Figure 5-91 Whitelist configuration page

Step 2 Select the **Enable Whitelist** check box to enable the whitelist.

----End

Disabling the Whitelist Function

If the whitelist function is enabled, deselect **Enable Whitelist** to disable the whitelist, as shown in Figure 5-91.

Importing a Whitelist File

You can add trusted IPv4 or IPv6 addresses by importing a whitelist file on the ADS device. After the whitelist file is imported, the ADS device checks the IP address format and then loads the list of trusted IP addresses to its engine. The new whitelist file will overwrite the existing file saved on the device.

The whitelist file is in format of **.txt**, with one IP address per line. The following uses IPv4 addresses as an example to illustrate the format:

- 10.10.10.10
- 172.16.10.10

- 192.168.10.10

Note	• Since the ADS device supports the IPv4/IPv6 dual-stack, you can configure IPv4 or IPv6 addresses in the whitelist file according to the actual network deployment. • The whitelist file name supports English letters and digits. The file must be within 1 MB. It is recommended that the file contain a maximum of 50,000 IP addresses. • Select the **Enable Whitelist** checkbox before you import a whitelist file; otherwise, the imported whitelist cannot take effect.

To import a whitelist file, perform the following steps:

Step 1 Choose **Policies** > **Access Control** > **Whitelist** and click **Select File** on the whitelist configuration page.

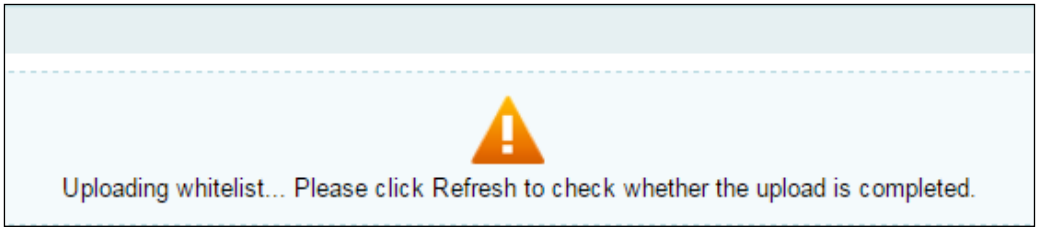
Step 2 Select the whitelist file and click **Open**.

Figure 5-92 Importing the whitelist file

Step 3 Click **Import**.

A message is displayed, prompting that the import is in progress, as shown in Figure 5-93.

Figure 5-93 Import progress message



After the whitelist file is imported, the system returns to the whitelist configuration page.

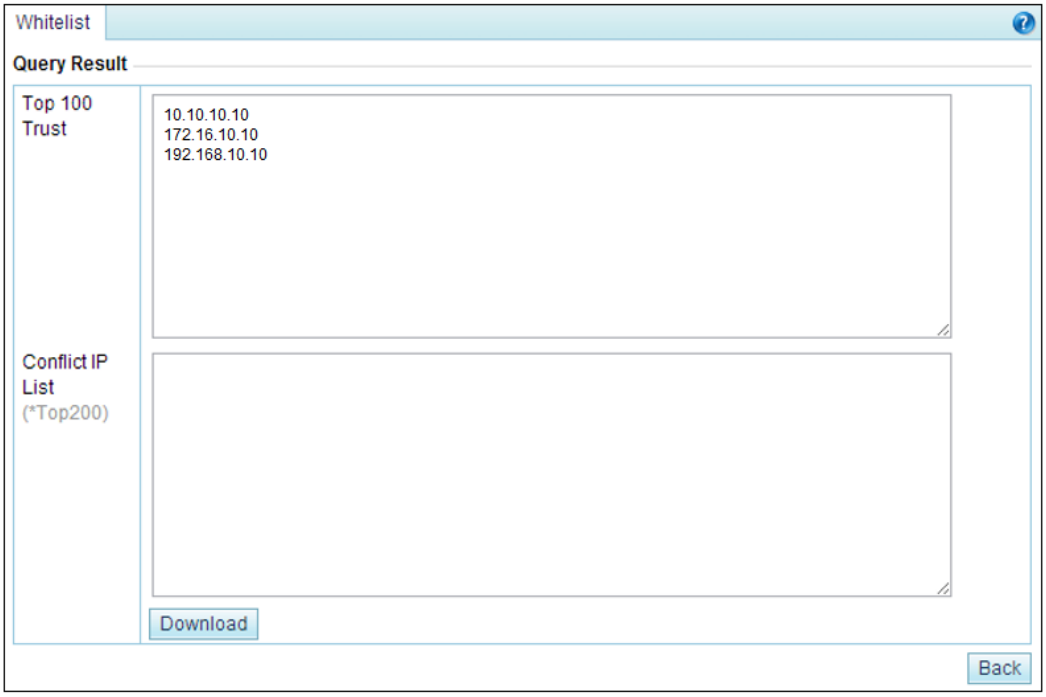
----End

Viewing the Import Result

After the list of trusted IP addresses is loaded to the engine, you can view the import result on the web-based manager by performing the following steps:

Step 1 Click **View Import Result** on the whitelist configuration page shown in Figure 5-91 to view information that is successfully imported to the whitelist. See Figure 5-94.

Figure 5-94 Viewing the import result



TOP 100 Trust shows top 100 IP addresses that are saved in the configuration file; **Conflict IP List** shows conflicting IP addresses that fail to be imported.

Step 2 After viewing the result, click **Back** to return to the whitelist configuration page.

----End

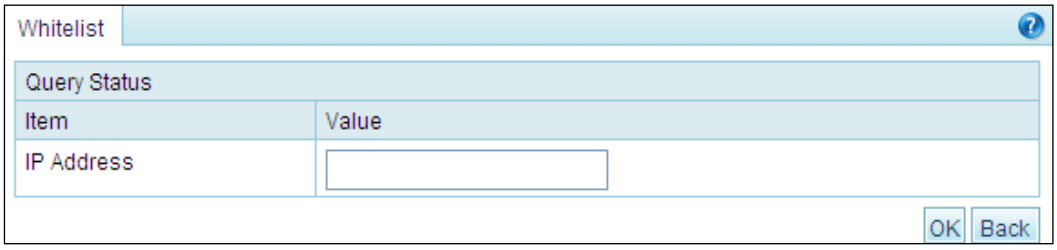
Querying the Whitelist

Querying the whitelist, you can check whether an IPv4 or IPv6 address is trusted. If the source IP address of packets is trusted, the ADS device allows such packets to pass through, without executing the access control rules or protection algorithms.

To query the whitelist, perform the following steps:

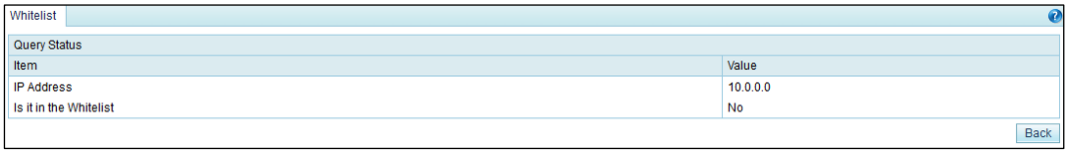
Step 1 On the whitelist configuration page shown in Figure 5-91, click **Query** to open the **Query Status** page.

Figure 5-95 Querying the whitelist



Step 2 Type the IP address to be queried in the textbox and click **OK** to check whether the IP address is trusted.

Figure 5-96 Whitelist query result



Step 3 After viewing the result, click **Back** to return to the whitelist configuration page.

----End

Clearing the Whitelist

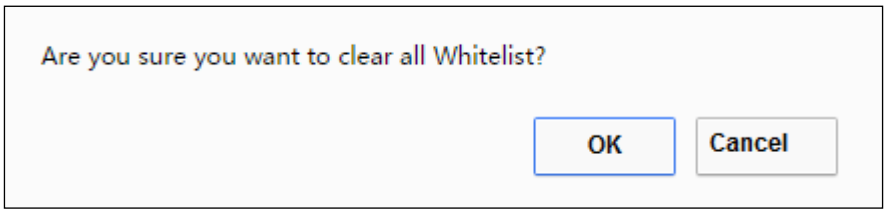
By clearing the whitelist, you can only delete the trust status of all IP addresses listed in the whitelist on the engine, but cannot delete the whitelist file. If IP addresses in this whitelist need to be re-trusted after the whitelist is cleared, you need to reload the whitelist file. For details, see Reloading the Whitelist File.

To clear the whitelist, perform the following steps:

Step 1 Click **Clear white list** on the whitelist configuration page shown in Figure 5-91.

Then, a dialog box appears, asking you whether to clear the whitelist, as shown in Figure 5-97.

Figure 5-97 Clearing trust relationships



Step 2 Click **OK** to save the settings.

----End

Clearing the Configuration

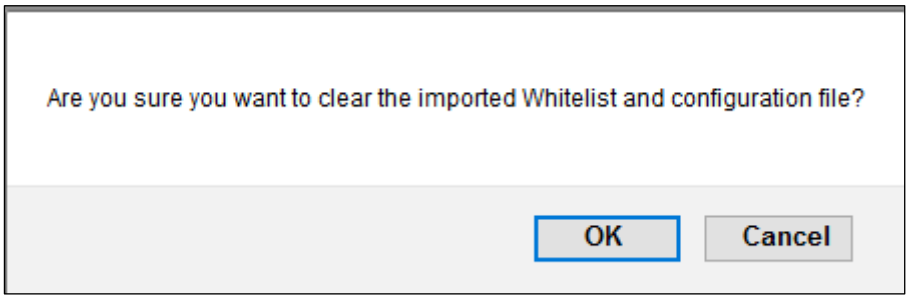
By clearing the configuration, you can delete the whitelist file and trust relationships of IP addresses on the engine. You are advised to back up the whitelist file before clearing the configuration. For details, see Downloading the Configuration.

To clear the configuration, perform the following steps:

Step 1 Click **Clear** on the whitelist configuration page shown in Figure 5-91.

Then, a dialog box appears, asking you whether to delete the whitelist file and all trusted entries, as shown in Figure 5-98.

Figure 5-98 Clearing the configuration



Step 2 Click **OK** to save the settings.

----End

Downloading the Configuration

You can download the whitelist file to a local disk drive for backup.

To download the configuration, perform the following steps:

Step 1 Click **Download** on the whitelist configuration page shown in Figure 5-91.

Step 2 Click **Save** and select a file path to save the whitelist file in the related directory.

----End

Reloading the Whitelist File

Through reloading, the ADS device clears the existing list of trusted IP addresses and loads new trusted IP addresses to the engine.

To reload a whitelist, click **Reload** on the whitelist configuration page shown in Figure 5-91.

6 Diversion and Injection

This chapter provides detailed information about traffic diversion and injection.

Section	Description
General Settings	Describes how to configure the system running mode and interface IP addresses.
Diversion Route	Describes how to configure a diversion route.
Traffic Injection	Describes how to configure an injection rule.
Traffic Diversion	Describes how to configure traffic diversion information.
Advanced Route Setting	Describes how to configure an advanced route.
Syslog Diversion Configuration	Describes how to configure syslog-based traffic diversion.

Under **Diversion & Injection**, you can configure routes as well as diversion and injection rules for the ADS device in out-of-path mode. These rules can be configured only when the current running mode is **Diversion**.

Note	In in-path mode, only the **General Settings** menu is available under **Diversion & Injection**, while **Diversion Route**, **Traffic Injection, Traffic Diversion, Advanced Route Setting, and Syslog Diversion Config** are unavailable.

6.1 General Settings

This section covers the following topics:

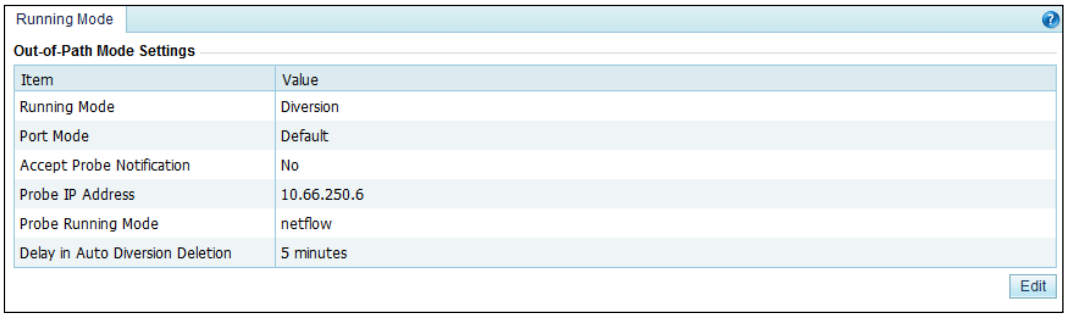
- Running Mode
- Port Channel Configuration
- GRE Tunnel Configuration
- IP Address Configuration

6.1.1 Running Mode

In out-of-path deployment mode, you need to configure the running mode for ADS. The detailed procedure is as follows:

Step 1 Choose **Diversion & Injection** > **General Settings** > **Running Mode** to switch to the out-of-path deployment mode.

Figure 6-1 Running mode of the ADS device (diversion mode)



Step 2 Click **Edit** to edit parameters in out-of-path mode.

Figure 6-2 Editing the running mode of the ADS device (diversion mode)

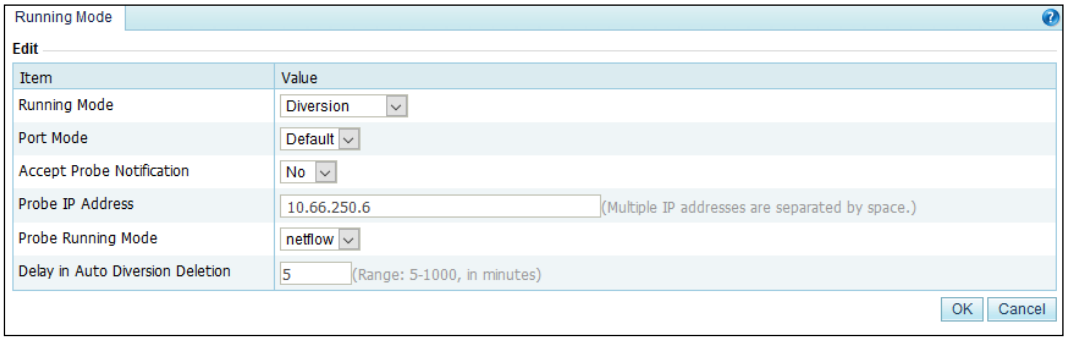


Table 6-1 describes parameters in out-of-path mode.

Table 6-1 Parameters in out-of-path mode

Parameter	Description
Running Mode	Current running mode of the ADS device. It has the following options: • **In-path**: indicates that a single ADS detection device is deployed in in-path mode. • **Diversion**: indicates that an NSFOCUS detection device and multiple ADS devices are deployed in out-of-path mode. • **Cluster probe**: indicates that multiple NSFOCUS detection devices are deployed in out-of-path mode. • **In-path cluster**: indicates that multiple ADS devices are deployed in in-path mode.

Parameter	Description
	Note • ADS NX5-8000 and NX5-10000 do not support the in-path running mode. • The running mode is determined by the system license. To change the running mode, please contact NSFOCUS technical support for a new license.
Port Mode	Mode of the current port. Only **Default** is available for ADS devices.
Accept Probe Notification	Controls whether to receive notifications from ADS when an attack event is detected. The value **Yes** indicates that the NSFOCUS detection device instructs the current ADS device to handle attacks that are detected. Note This parameter is required only when **Running Mode** is set to **Diversion**.
Probe IP Address	IP address of an NSFOCUS NTA or ADS M that coordinates with the ADS device. You can type one or more IP addresses separated by spaces. Note • This parameter is required only when **Running Mode** is set to **Diversion**. • Currently, NSFOCUS NTA only supports IPv4 addresses, while NSFOCUS ADS M supports both IPv4 and IPv6 addresses.
Probe Running Mode	Running mode of NSFOCUS ADS detection devices. It has the following values: • **netflow**: indicates that ADS devices check the traffic output by the router in netflow format for abnormal traffic. • **span**: indicates that ADS devices check mirrored traffic for abnormal traffic. Note This parameter is required only when **Running Mode** is set to **Diversion**.
Delay in Auto Diversion Deletion	After receiving a deletion diversion notification, ADS deletes the diversion after an automatic delay. The value should be in the range of 5–1000 minutes. If ADS receives a diversion deletion notification, and then receives a diversion setup notification before **Delay in Auto Diversion Deletion** expires, ADS automatically ignores the diversion deletion notification and continues to divert traffic.

Step 3 Set parameters and click **OK** to save the settings.

----End

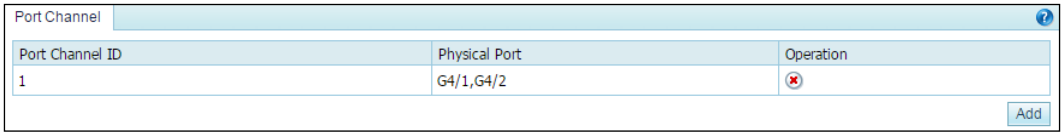
6.1.2 Port Channel Configuration

The Port channel allows a combination of arbitrary available interfaces on the device. The MAC address of the port channel is that of the interface with the smallest ID. For example, after G1/1 and G1/2 interfaces of ADS NX5-4020 are combined into a port channel, the MAC address of the port channel is that of the G1/1 interface.

Note	The number of ports varies with ADS series, but the procedure for configuring the port channel is the same. This section uses ADS NX5-4020 as an example to describe how to configure the port channel.

Choose **Diversion & Injection** > **General Settings** > **Port Channel** to open the port channel configuration page. See Figure 6-3.

Figure 6-3 Port Channel page



Creating a Port Channel

Currently, only ports of the same type can be added to a port channel, for example, 1000M electrical ports and 1000M optical ports cannot be merged into one port channel. The same is true for 1000M and 10G optical ports. To the lower right of the port channel list shown in Figure 6-3, click **Add**. The **Add Port Channel Interface** page appears, as shown in Figure 6-4.

Figure 6-4 Creating a port channel for the ADS device

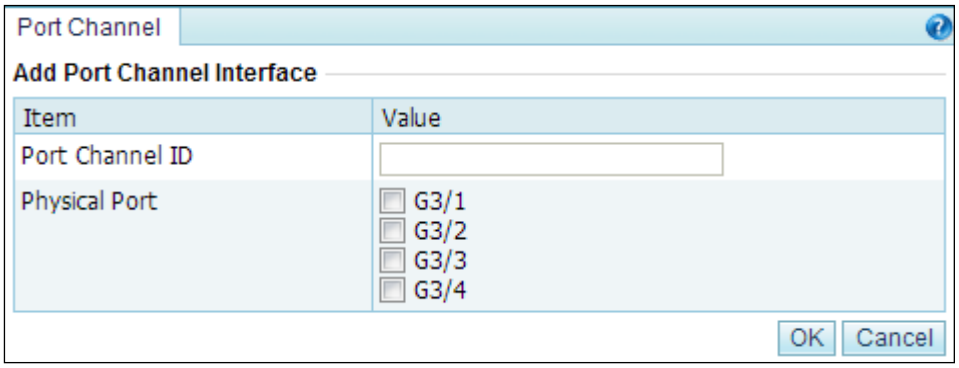


Table 6-2 describes parameters for creating a a port channel.

Table 6-2 Parameters for creating a a port channel

Parameter	Description
Port Channel ID	ID of the port channel. The value is an integer ranging from 0 to 31.
Physical Port	Available physical ports on the current ADS device. Note A port channel has one or several port IDs, but each port ID can be included

Parameter	Description
	in only one port channel.

Deleting a Port Channel

On the port channel list in Figure 6-3, click in the **Operation** column to delete a port channel.

Note	Port channels in use cannot be deleted.

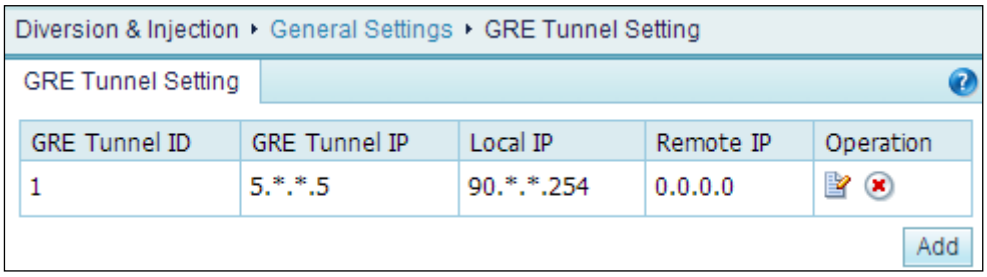
6.1.3 GRE Tunnel Configuration

GRE tunnel accomplishes data communication between two private networks. When one intranet is reachable for another via a route, the GRE tunnel encapsulates intranet packets (directed towards an intranet IP address in the other network) in IP packets on routes by default and sends them. On arriving at the peer IP address, the packets will be automatically decapsulated and then forwarded to the destination IP address in the intranet.

Note	Currently, the ADS device does not support GRE tunnel injection with encapsulated IPv6 headers. Therefore, in dual-stack mode, IPv6 packets re-injected through the GRE tunnel must be encapsulated with an IPv4 packet header.

Figure 6-5 shows the GRE tunnel configuration page.

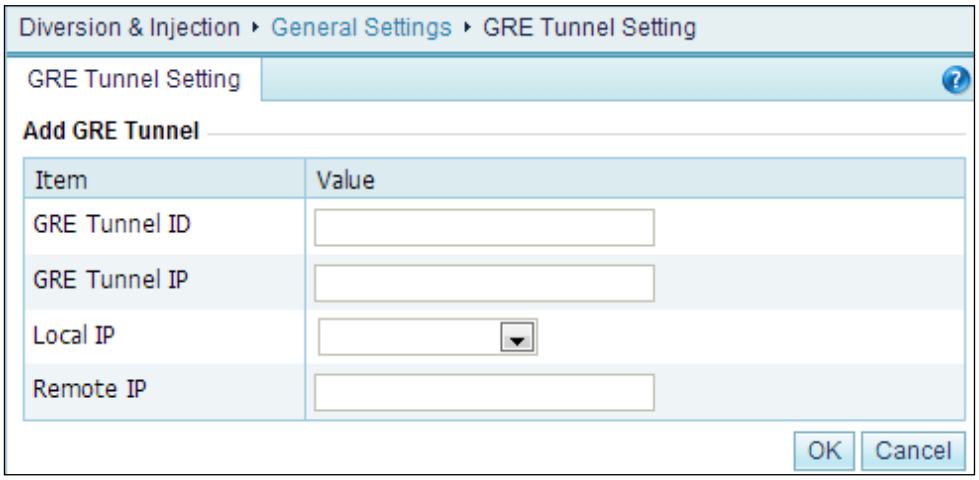
Figure 6-5 GRE Tunnel Setting page



Creating a GRE Tunnel

Step 1 To the lower right of the GRE tunnel list, click **Add**.

Figure 6-6 Creating a GRE tunnel



Step 2 On the **Add GRE Tunnel** page, configure parameters.

Table 6-3 describes parameters for creating a GRE tunnel.

Table 6-3 Parameters for creating a GRE tunnel

Parameter	Description
GRE Tunnel ID	GRE tunnel ID. The value is an integer ranging from 1 to 1023.
GRE Tunnel IP	IP address of the GRE tunnel. Generally, it is an internal IPv4 or IPv6 address.
Local IP	Source IP address of the GRE tunnel. This parameter can be set to an IPv4 address.
Remote IP	Destination IP address of the GRE tunnel. This parameter can be set to an IPv4 address.

Step 3 Click **OK** to save the settings.

----End

Modifying a GRE Tunnel

In Figure 6-5, click in the **Operation** column to edit GRE tunnel configuration. The configuration of GRE tunnels in use cannot be edited.

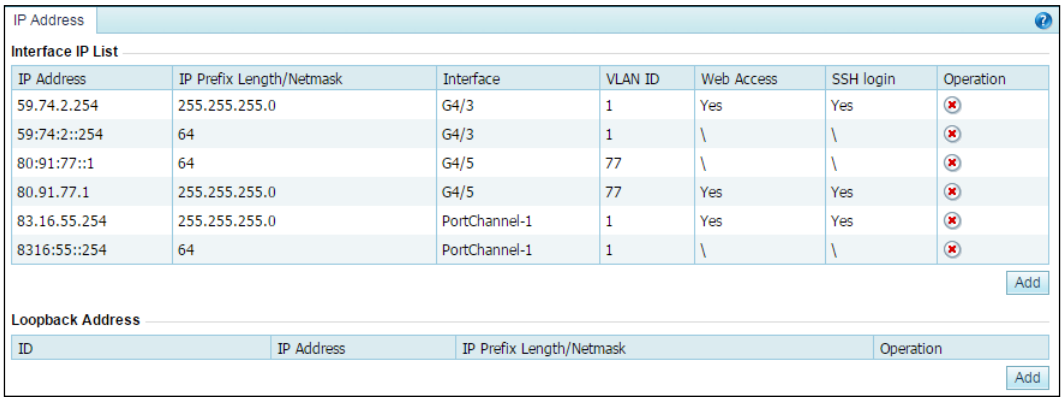
Deleting a GRE Tunnel

In Figure 6-5, click in the **Operation** column to delete a GRE tunnel. GRE tunnels in use cannot be deleted.

6.1.4 IP Address Configuration

As shown in Figure 6-7, in **Diversion** running mode, configure the IP addresses and loopback addresses for two interfaces that are used by ADS.

Figure 6-7 IP address list in diversion mode



Note	The number of interfaces varies with ADS series, but the procedure for configuring *interface* IP addresses is the same. This section uses ADS NX5-4020 as an example to describe how to configure IP addresses.

Adding an IP Address

To the lower right of the interface IP list, click **Add** to add an IP address. The **Add interface IP** page appears, as shown in Figure 6-8.

Figure 6-8 Adding an IP address

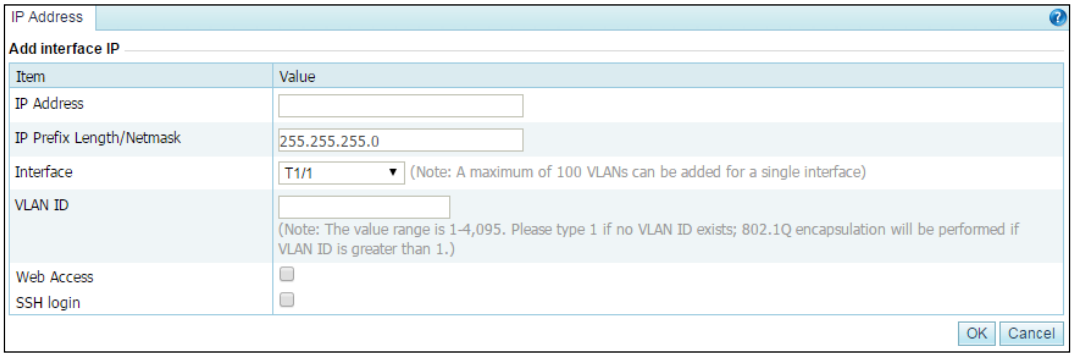


Table 6-4 describes parameters of an interface.

Table 6-4 Interface parameters

Parameter	Description
IP Address	IP address of a specified interface on the ADS device. You can type an IPv4 or IPv6 address according to the actual network deployment. The IPv4 address cannot be in the same /24 subnet as IP addresses of other interfaces. The IPv6 address embedded with an IPv4 address is not recommended.

Parameter	Description
	Note An interface can have multiple IP addresses.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the specified port.
Interface	Available ports on the current ADS device.
VLAN ID	ID of the VLAN that is connected to the interface.
Web Access	Controls whether the interface allows access via web.
SSH Login	Controls whether the interface allows access via SSH.

Deleting an IP Address

In Figure 6-7, click in the **Operation** column to delete an IP address. IP addresses being used cannot be deleted.

Adding a Loopback Address

Click **Add** to the lower right of the loopback address list to add a loopback address. The **Add Loopback Address** page appears, as shown in Figure 6-9.

Figure 6-9 Adding a loopback address

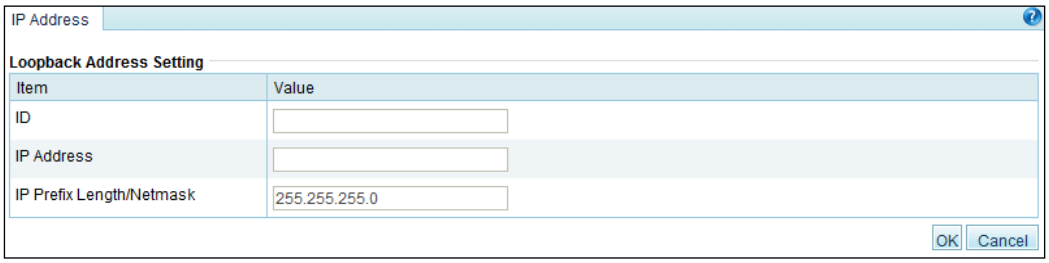


Table 6-5 describes parameters of a loopback address.

Table 6-5 Parameters of a loopback address

Parameter	Description
ID	Loopback address ID. The value is an integer ranging from 0 to 128.
IP Address	IP address of a loopback route to be added. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address.

Deleting a Loopback Address

In Figure 6-7, click in the **Operation** column to delete a loopback address. Loopback addresses in use cannot be deleted.

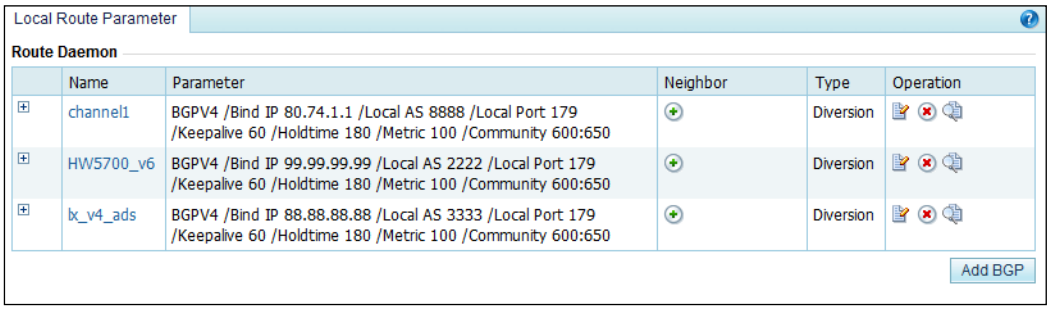
6.2 Diversion Route

The ADS device needs a dynamic routing protocol for diversion. To enable the dynamic routing protocol, you need to configure route parameters.

6.2.1 BGP Route

As shown in Figure 6-10, only BGP routes are displayed on the **Local Route Parameter** page.

Figure 6-10 Local route parameters



Creating a BGP Route

In Figure 6-10, click **Add BGP** to the lower right of the route daemon list to configure local BGP parameters. See Figure 6-11.

Figure 6-11 Creating a BGP route

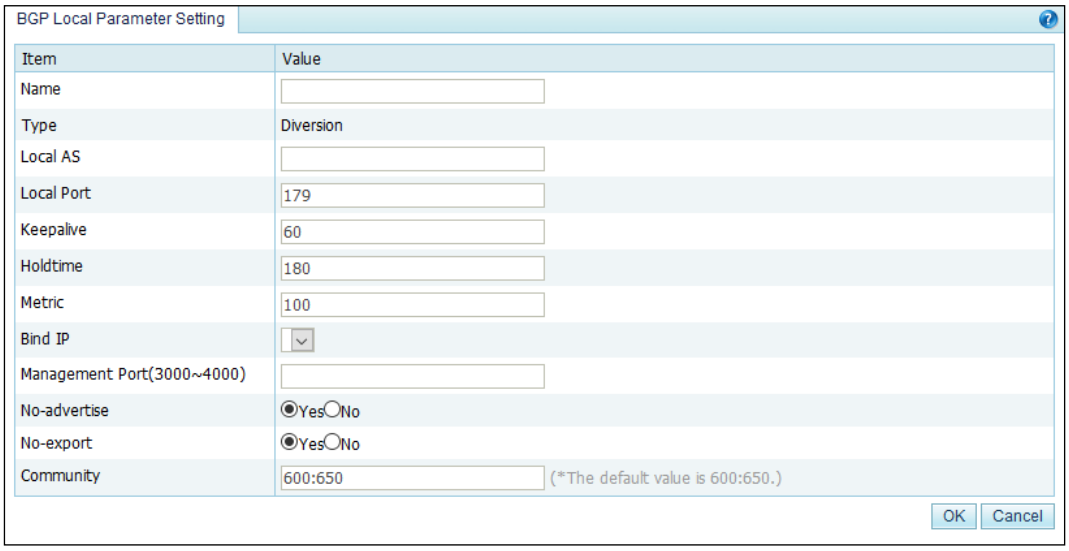


Table 6-6 describes parameters for creating a BGP route.

Table 6-6 Parameters for creating a BGP route

Parameter	Description
Name	Route daemon name.
Local AS	Autonomous system (AS) number of a BGP route daemon. **Note** You are advised to use the AS with number over 65000 and not to use a private domain that is already used by other countries.
Local Port	BGP port of the route daemon. Generally, the default port **179** is used.
Bind IP	Local IP address of the route daemon. You can type an IPv4 or IPv6 address according to the actual network deployment.
Management Port(3000~4000)	Management port of the route daemon. The port number ranges from 3000 to 4000.
Community	Community of the BGP route. The default value is **600:650**.

Other parameters including **Keepalive**, **Holdtime**, **Metric**, **No-advertise**, and **No-export** correspond to certain fields of the BGPv4 protocol.

Editing a BGP Route

On the route daemon list shown in Figure 6-10, click in the **Operation** column to edit a route.

Note	Modifying BGP settings during the running of the HA function may cause traffic switchover, and is not recommended.

Deleting a BGP Route

On the route daemon list shown in Figure 6-10, click in the **Operation** column to delete a route.

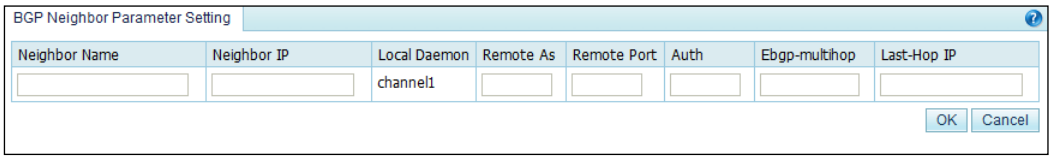
Viewing the Route Status

On the route daemon list shown in Figure 6-10, click in the **Operation** column to view status of the route.

Adding a BGP Neighbor

A BGP route is the only route that has neighbors. On the route daemon list shown in Figure 6-10, click in the **Neighbor** column to add a BGP neighbor. See Figure 6-12.

Figure 6-12 Adding a BGP neighbor



Note	After a neighbor is added, click to check whether it is connected.

Table 6-7 describes parameters of a BGP neighbor

Table 6-7 Parameters of a BGP neighbor

Parameter	Description
Neighbor Name	BGP neighbor name.
Neighbor IP	IP address of the BGP neighbor. Both IPv4 and IPv6 addresses are allowed.
Remote As	Autonomous system of the BGP neighbor.
Remote Port	Remote port of the BGP neighbor. The default port number is **179**.
Auth	Authentication password. This parameter is required only when you encrypt the BGP neighbor.
Ebgp-multihop	Maximum number of hops allowed by the External Border Gateway Protocol

Parameter	Description
	(EBGP).
Last-Hop IP	IP address of the router directly connecting to the ADS device. Both IPv4 and IPv6 addresses are allowed.

Hiding or Displaying a BGP Neighbor

All neighbors are displayed in the list by default. You can click ⊟ to hide neighbors of a route or click ⊞ to display all of them.

Other Operations on a BGP Neighbor

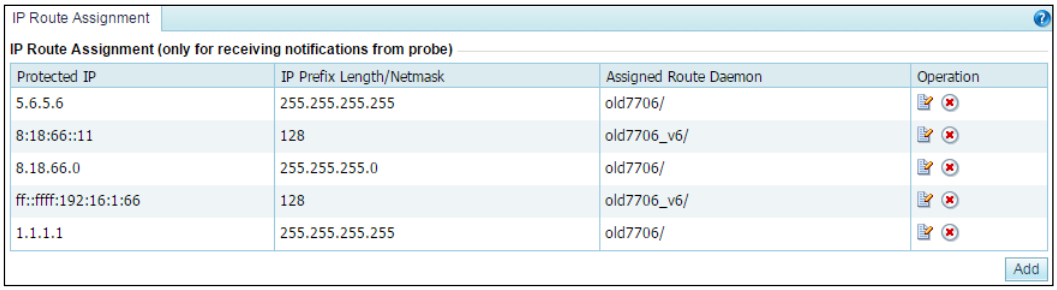
After all BGP neighbors are displayed, you can click to modify information of a neighbor, click to delete a neighbor, click to check whether a neighbor can be pinged, or click to view the connection status of a neighbor.

Note	After you click , if the link works properly, the ping output displays the status of only the first five packets.

6.2.2 IP Route Assignment

IP routes enable the current ADS device to receive notifications (configured together with diversion filtering rules) from an NSFOCUS ADS detection device and to decide which route daemon sends notifications. See Figure 6-13.

Figure 6-13 IP route assignment



Creating an IP Route

In Figure 6-13, click **Add** to the lower right of the **IP Route Assignment** list. On the **Add IP Route Assignment** page, configure parameters and then click **OK**.

Figure 6-14 Creating an IP route

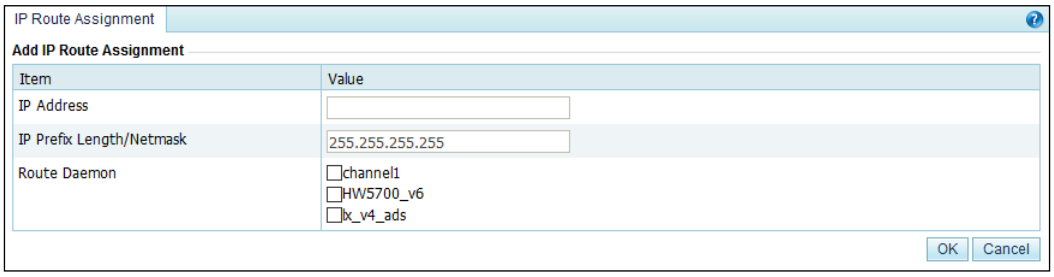


Table 6-8 describes parameters for creating an IP route.

Table 6-8 Parameters for creating an IP route

Parameter	Description
IP Address	IP address to which a route is assigned. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address.
Route Daemon	Route daemon that sends a routing notification.

Editing an IP Route

On the IP route assignment list shown in Figure 6-13, click in the **Operation** column to edit an IP route.

Deleting an IP Route

On the IP route assignment list shown in Figure 6-13, click in the **Operation** column to delete an IP route.

Note	For how to configure diversion filtering rules, see section *6.4.1* Filtering Rules.

6.3 Traffic Injection

This section covers the following topics:

- Injection Interfaces
- Injection Routes
- MAC Address Table

6.3.1 Injection Interfaces

Note	The number of interfaces varies with ADS series, but the procedure for configuring injection interfaces is the same. This section uses ADS NX5-4020 as an example to describe how to configure injection interfaces.

To configure an injection interface, you need to configure parameters about the injection interface including interface IP address and netmask, VLAN ID, and physical port of the interface. The injection interface determines the physical port and packet encapsulation format for traffic re-injection.

This section covers the following topics:

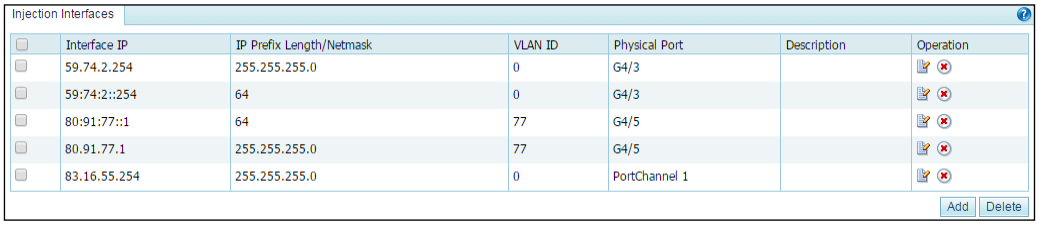
- Adding an Injection Interface
- Editing an Injection Interface
- Deleting Injection Interfaces

6.3.1.1 Adding an Injection Interface

To add an injection interface, perform the following steps:

Step 1 Choose **Diversion & Injection** > **Traffic Injection** > **Injection Interfaces**.

Figure 6-15 Injection interface list


Injection Interfaces

Interface IP	IP Prefix Length/Netmask	VLAN ID	Physical Port	Description	Operation
59.74.2.254	255.255.255.0	0	G4/3		
59:74:2::254	64	0	G4/3		
80:91:77::1	64	77	G4/5		
80.91.77.1	255.255.255.0	77	G4/5		
83.16.55.254	255.255.255.0	0	PortChannel 1		

Add Delete

Step 2 Click **Add** to open the page for adding an injection interface.

Figure 6-16 Adding an injection interface

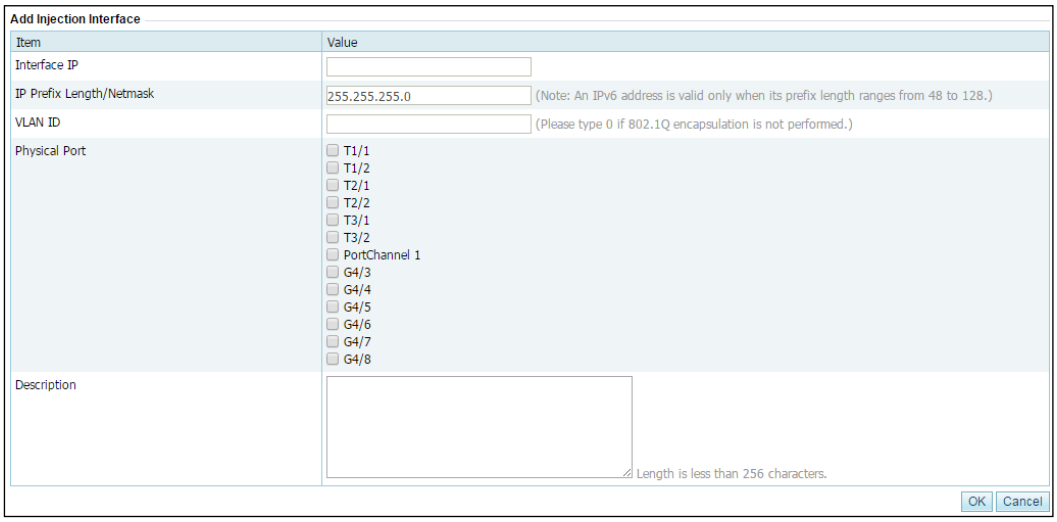


Table 6-9 describes parameters of an injection interface.

Table 6-9 Parameters of an injection interface

Parameter	Description
Interface IP	IP address of the injection interface. You can type an IPv4 or IPv6 address according to the actual network deployment. • If **Interface IP** is set to an IPv4 address, it can be either a network address in the format of *.*.*.0/24 or a broadcast address in the format of *.*.*.255/24. • If **Interface IP** is set to an IPv6 address, the IPv6 prefix length range is 48–128 bits.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the interface IP address.
VLAN ID	VLAN ID of the injection interface. The value is an integer ranging from 0 to 4094.
Physical Port	Physical port of the injection interface. You can select multiple physical ports.

Note	IP address configured on the injection interface is a source IP address of the ARP query packets, which is mainly used by the ADS device to learn the next-hop MAC address. Other devices cannot communicate with this IP address. • When VLAN ID is not 0, all packets will be encapsulated with the IEEE 802.1Q protocol and then be forwarded. • When VLAN ID is 0, all packets will be encapsulated with a common Ethernet protocol. If the injection interface has several physical ports, traffic is forwarded in load balancing mode on these interfaces.

Step 3 Set parameters and click **OK** to save the settings.

----End

6.3.1.2 Editing an Injection Interface

After configuring injection interfaces, you can edit interface parameters by performing the following steps:

Step 1 On the injection interface list shown in Figure 6-15, click in the **Operation** column of an interface to edit interface parameters.

Step 2 After editing interface parameters, click **OK** to save the settings and return to the injection interface list.

----End

6.3.1.3 Deleting Injection Interfaces

You can delete one injection interface or multiple interfaces in batches on ADS devices.

- Method 1: On the injection interface list shown in Figure 6-15, click in the **Operation** column of an interface and then click **OK** in the confirmation dialog box to delete an injection interface.
- Method 2: Select one or more injection interfaces (or select the **Select All** check box to select all injection interfaces) to be deleted, click **Delete** to the lower right of the interface list, and then click **OK** in the confirmation dialog box to delete the selected interfaces.

6.3.2 Injection Routes

This section covers the following topics:

- Creating an Injection Route
- Creating Injection Routes in Batches
- Viewing Rule Status of Injection Routes
- Viewing Link Connectivity of Injection Routes
- Viewing Injection Routes
- Learning MAC Address
- Enabling and Disabling Injection Routes
- Resetting Link Switch Count
- Editing Injection Routes
- Deleting Injection Routes
- Editing Advanced Configurations

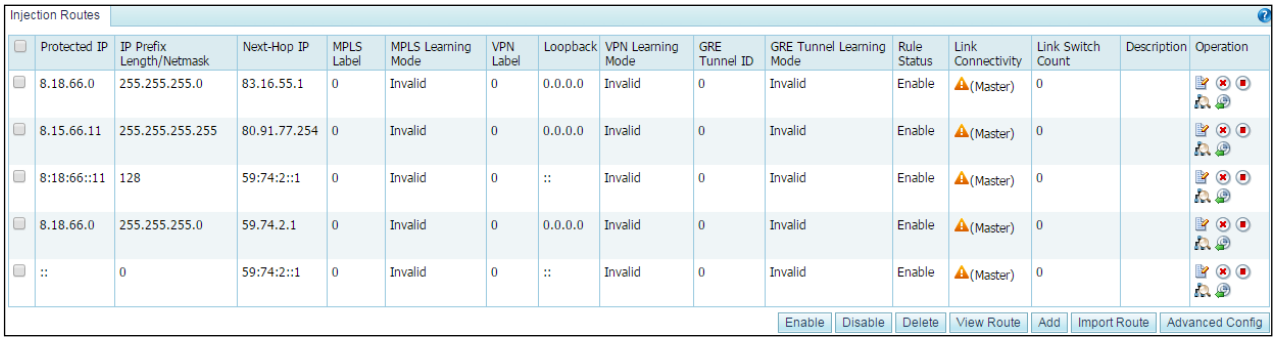
ADS supports multiple injection routes. If multiple routes have the same priority, ADS injects traffic along all the routes and checks the connectivity of all the routes. Once a route fails, ADS automatically invalidates the route and injects traffic along the other routes subsequently. If multiple injection routes have different priorities, ADS injects traffic along the route with the highest priority, and uses the other routes as standby routes. In this case, ADS checks the connectivity of all the routes. If the route with the highest priority fails, ADS considers it as an invalid one and injects traffic along the route with the highest priority among the standby routes. This master-slave mechanism among routes achieves high availability.

6.3.2.1 Creating an Injection Route

To create an injection route, perform the following steps:

Step 1 Choose **Diversion & Injection** > **Traffic Injection** > **Injection Routes** to open the **Injection Routes** page, as shown in Figure 6-17.

Figure 6-17 Injection routes



Step 2 Click **Add**.

Figure 6-18 Creating an injection route

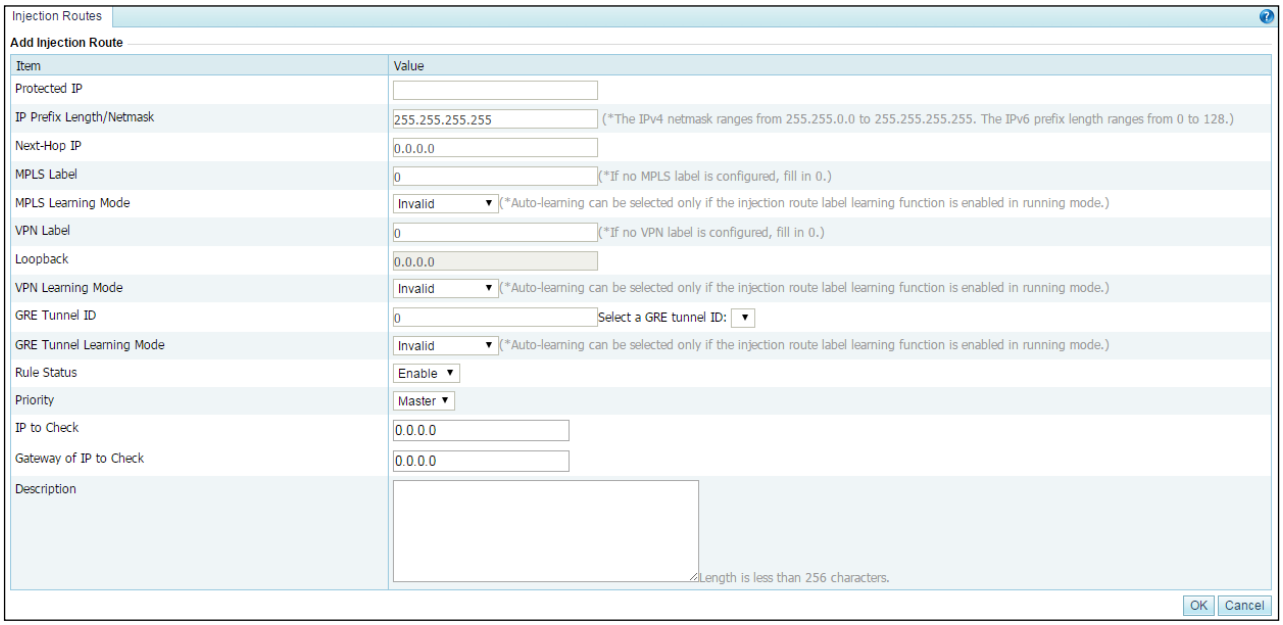


Table 6-10 describes parameters for creating an injection route.

Table 6-10 Parameters for creating an injection route

Parameter	Description
Protected IP	IP address or IPv4 segment of a protected host. You can type an IPv4 or IPv6 address according to the actual network deployment.

Parameter	Description
	Note Currently, you can add an injection route for IP addresses in the /16 or /24 subnet, but not for those in the /4 subnet.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be protected. The netmask of an IPv4 address must range from 255.255.0.0 to 255.255.255.255. The prefix length of an IPv6 address must be in the range of 0 to 128.
Next-Hop IP	Next-hop IP address of the traffic destined for the protected IP address (or IP segment). The next-hop IP address is often bundled with the injection interface of the ADS device. You can type an IPv4 or IPv6 address according to the actual network deployment.
MPLS Label	MPLS label of the packet forwarded by the injection route. Type **0** if the MPLS label is not configured.
MPLS Learning Mode	Specifies how to learn MPLS labels. It has the following values: • **Manual setting**: indicates that you need to specify the MPLS label manually. • **Auto-learning**: indicates that the ADS device automatically learns MPLS labels. • **Invalid**: indicates that no MPLS label is configured.
VPN Label	VPN label. Type **0** if no VPN label is configured.
VPN Learning Mode	Specifies how to learn the VNP label. It has the following values: • **Manual setting**: indicates that you need to specify the VPN label manually. • **Auto-learning**: indicates that the ADS device automatically learns VPN labels. • **Invalid**: indicates that no VPN label is configured.
Loopback	Loopback IP address set by the system.
GRE Tunnel ID	ID of a GRE tunnel. Leave it at the default value **0** if no GRE tunnel is configured.
GRE Tunnel Learning Mode	Specifies how to learn the GRE tunnel label. It has the following values: • **Auto-learning**: indicates that the ADS system automatically learns CRE tunnel labels. In this case, **Enable Injection MPLS Label Learning** must be set to **Yes** in **Running Mode**. • **Manual setting**: indicates that a GRE tunnel label needs to be configured manually. • **Invalid:** indicates that no GRE tunnel label is configured.
Rule Status	Controls whether to query the injection status. It has the following values: • **Enable**: indicates that the system queries the injection rule when forwarding packets. • **Disable**: indicates that the system does not query the injection rule when forwarding packets.

Parameter	Description
Priority	Route priority. The default value is **Master**. • **Master**: indicates a higher priority. • **Slave**: indicates a lower priority.
IP to Check	IP address to be pinged when the connectivity of the current route is checked. The default value is **0.0.0.0**, indicating that the next-hop IP address is used as the IP to check.
Gateway of IP to Check	The gateway of the IP address to be pinged when the connectivity of the current route is checked. The default value is **0.0.0.0**, indicating that no corresponding static route is configured. If **IP to Check** and **Gateway of IP to Check** are set to other values than the default ones, the system automatically adds a static route to **IP to Check** and with the next hop as **Gateway of IP to Check**.

Note	When **Next-Hop IP Address** is set to 0.0.0.0, the ADS device performs layer 2 forwarding. Assume that the protected IP address is 192.168.1.0, the netmask is 255.255.255.0, and the next-hop IP address is 0.0.0.0. Then the next-hop IP address of the traffic destined for 192.168.1.1 is 192.168.1.1, and that of 192.168.1.2 is 192.168.1.2. The rest may be deduced by analogy.

Step 3 Set parameters and click **OK** to save the settings.

----End

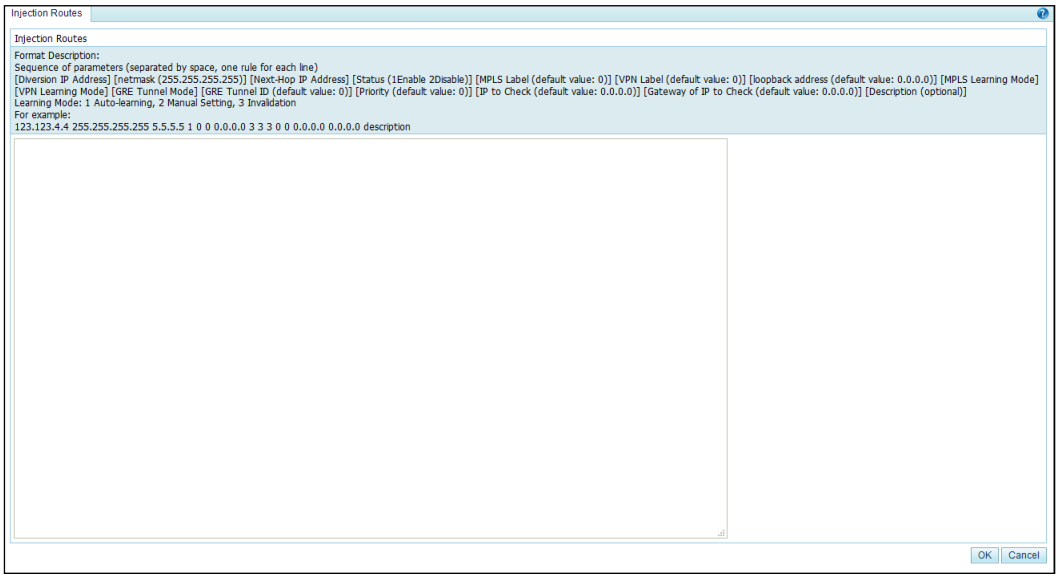
6.3.2.2 Creating Injection Routes in Batches

You can create injection routes in batches on the ADS system by performing the following steps:

Step 1 Click **Import Route** to the lower right of the injection route list.

A page appears, as shown in Figure 6-19.

Figure 6-19 Creating injection routes in batches



Step 2 Type multiple injection routes as prompted.

Pay attention to the following format specifications:

- An injection route is typed in the following format: [diversion IP address] [netmask (255.255.255.255)] [next-hop IP address] status (1Enable 2Disable)] [MPLS label (default value: 0)] [VPN label (default value: 0)] [loopback address (default value: 0.0.0.0)] [MPLS learning mode] [VPN learning mode] [GRE tunnel mode] [GRE tunnel ID (default value: 0)] [peer_lsr_id (default value: 0.0.0.0)]. For two learning modes, the value **1** indicates self-learning, the value **2** indicates manual setting, and the value **3** indicates invalid.
- An injection route example is as follows: 123.123.4.4 255.255.255.255 5.5.5.5 1 0 0 0.0.0.0 3 3 3 0 0.0.0.0
- Parameters of each injection route are separated by spaces.
- Each line can contain only one injection route.

Step 3 After the parameter configuration is complete, click **OK** to save the settings.

----End

6.3.2.3 Viewing Rule Status of Injection Routes

After routes are configured and applied, you can view rule status of the routes in the **Rule Status** column in Figure 6-17. The rule status could be one of the following:

- **Enable**: The rule is manually enabled, and the link is connected or not checked.
- **Enable (Block)**: The rule is enabled, but cannot be used because the link is disconnected for the injection route.
- **Disable (Block)**: The rule is disabled by the system because the injection link is disconnected and the number of link switches exceeds the specified number.
- **Disable**: The rule is manually disabled.

6.3.2.4 Viewing Link Connectivity of Injection Routes

After routes are configured and applied, you can view link connectivity of the routes in the **Link Connectivity** column in Figure 6-17. The link connectivity could be one of the following:

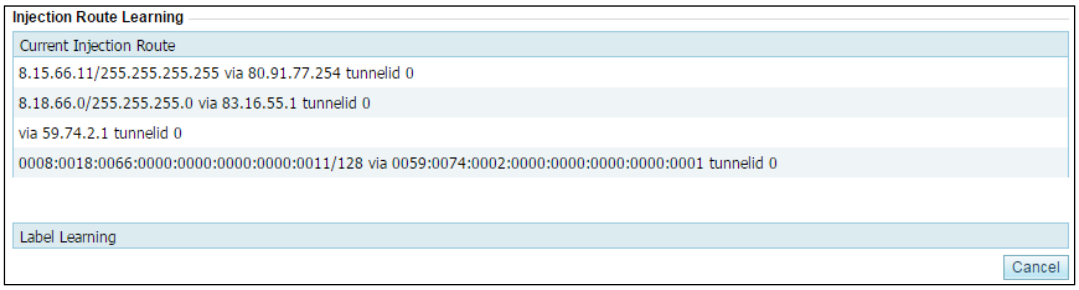
- : The link of this injection route functions properly. That is, ADS can successfully ping the **IP to Check** of the injection route.
- : The link of this injection route is faulty. That is, ADS fails to ping the **IP to Check** of the injection route. In this case, traffic cannot be injected along this route.
- : The link of this injection route is in unstable status. ADS does not check this injection route.
- : The link of this injection route is in unstable status. ADS is checking this injection route.

6.3.2.5 Viewing Injection Routes

After injection routes are configured and applied, you can view information about such routes and MPLS labels learned by the device. The detailed procedure is as follows:

Step 1 Click **View Route** to the lower right of the injection route list to view current injection routes and learned labels.

Figure 6-20 Viewing injection routes and learned labels



- **Current Injection Route** lists current injection routes on the device.
- **Label Learning** lists MPLS labels learned by the device. An MPLS label is a local short identifier with a fixed length. It is used to identify the Forwarding Equivalence Class (FEC) to which a group belongs.

Note	MPLS labels are often classified into layer 1 labels and layer 2 labels. To enable MPLS label learning support on the device, you need to first enable the Label Distribution Protocol (LDP) and then configure MPLS labels. To use layer 2 MPLS labels on the device, you also need to configure VPN labels.

Step 2 After viewing injection routes, click **Cancel** to return to the injection route list.

----End

6.3.2.6 Learning MAC Address

The MAC address self-learning function allows the ADS device to learn the MAC addresses of the protected IP addresses by sending ARP broadcast messages. The mapping between the protected IP addresses and the MAC addresses learned by the ADS device is displayed in the MAC address table. For the mapping details, see section 6.3.3 MAC Address Table.

To view MAC addresses learned by the ADS device, click to the right of an injection route, as shown in Figure 6-17.

Note	• If the ADS device takes a long time to learn the MAC address of a protected IPv6 address, you are advised to manually bind the protected IP address and the MAC address. • If the prefix length of the IPv6 address is not 128 bits and the next hop is not a specific IP address, MAC learning will be unavailable.

6.3.2.7 Enabling and Disabling Injection Routes

On the ADS device, only enabled injection routes are valid, while disabled ones are invalid. The operations of enabling and disabling injection routes free you from redundant deletions and additions. If some injection routes are not required currently, disable them.

You can enable or disable a single injection route or more routes in batches.

Enabling Injection Routes

- Method 1: On the injection route list as shown in Figure 6-17, click in the **Operation** column of a disabled route to enable it. Then, the status icon of this route turns to .
- Method 2: On the injection route list shown in Figure 6-17, select one or more injection routes (or select the **Select All** check box to select all injection routes) to be deleted, click **Enable** to the lower right of the route list, and click **OK** in the confirmation dialog box to enable the selected routes.

Disabling Injection Routes

- Method 1: On the injection route list shown in Figure 6-17, click in the **Operation** column of an enabled route to disable it. Then, the status icon of this route turns to .
- Method 2: On the injection route list shown in Figure 6-17, select one or more injection routes (or select the **Select All** check box to select all injection routes) to be deleted, click **Disable** to the lower right of the route list, and then click **OK** in the confirmation dialog box to disable the selected routes.

6.3.2.8 Resetting Link Switch Count

You can view the number of link switches (from valid to invalid) of an injection route in the **Link Switch Count** column in Figure 6-17.

You can click in the **Operation** column of an injection route to reset the number of link switches to **0**.

6.3.2.9 Editing Injection Routes

After configuring injection routes, you can edit route parameters by performing the following steps:

Step 1 On the injection route list in Figure 6-17, click in the **Operation** column of a route to edit route parameters.

Step 2 After editing parameters, click **OK** to save the settings and return to the injection route list.

----End

6.3.2.10 Deleting Injection Routes

You can delete one injection route or more routes in batches on the ADS device.

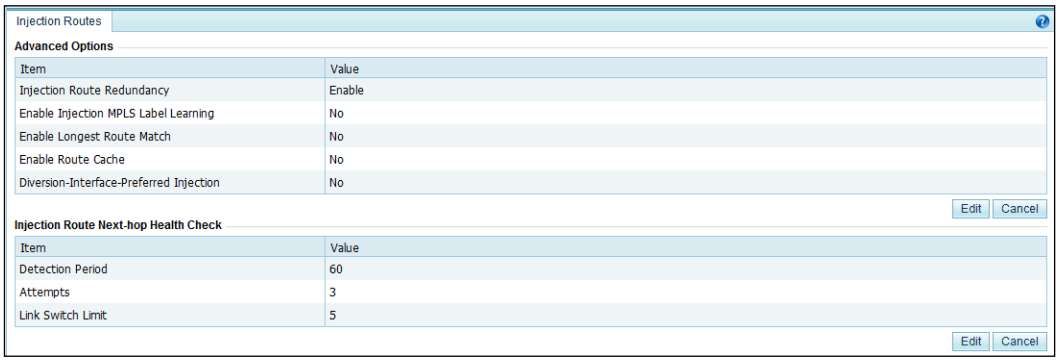
- Method 1: On the injection route list shown in Figure 6-17, click in the **Operation** column of a route and click **OK** in the confirmation dialog box to delete an injection route.
- Method 2: Select one or more injection routes (or select the **Select All** check box to select all injection routes) to be deleted, click **Delete** to the lower right of the route list, and click **OK** in the confirmation dialog box to delete the selected routes.

6.3.2.11 Editing Advanced Configurations

You can edit advanced configurations that apply to all injection routes.

Click **Advanced Config** in the lower-right corner of the injection route list shown in Figure 6-17. The page for editing advanced configurations appears, as shown in Figure 6-21.

Figure 6-21 Editing advanced configurations.



Then you can click **Edit** and start to edit advanced configurations.

Table 6-11 describes advanced options of injection routers.

Table 6-11 Parameters for advanced options of injection routers

Parameter		Description
Advanced Options	Injection Route Redundancy	Specifies whether to enable the injection route redundancy function.

Parameter		Description
		The **Injection Route Next-hop Health Check** area appears only when this function is enabled. Note The injection route redundancy function cannot be enabled simultaneously with either of injection MPLS label learning or diversion-interface-preferred injection.
	Enable Injection MPLS Label Learning	Controls whether to enable injection MPLS label learning. The default value is **No**. Injection MPLS label learning needs to be enabled only when MPLS injection is enabled. Note If injection MPLS label learning is enabled while MPLS injection is disabled, ordinary injection routes cannot be dispatched. Injection MPLS label learning cannot be enabled simultaneously with the injection route redundancy function.
	Enable Longest Route Match	Controls whether to enable longest route match. The default value is **No**. After longest route match is enabled, among routes destined for the same destination IP address, the system selects one based on their netmask lengths. The one with the longest netmask will be selected.
	Enable Route Cache	Controls whether to enable route cache. The default value is **No**. Route cache needs to be enabled only when longest route match is enabled. Enabling route cache is like having a fast forwarding table. The system does not need to check the entire injection route table every time.
	Diversion-Interface-Preferred Injection	Controls whether to enable diversion-interface-preferred injection. The default value is **No**. After it is enabled, traffic will be preferentially injected over the diversion interface, ensuring that traffic is diverted and injected over the same interface. Note To enable diversion-interface-preferred injection, you need to enable longest route match in advance. Diversion-interface-preferred injection and injection redundancy cannot be enabled simultaneously. To enable diversion-interface-preferred injection, you need to ensure that the injection route over the diversion interface has the highest priority or all injection routes have the same priority.
Injection Route Next-hop Health Check	Detection Period	Controls the interval between two link availability checks. The value ranges from 10 to 600, in seconds. The default value is **60**.
	Attempts	Controls the allowed number of attempts to check injection link availability. The value ranges from 1 to 10, and the default value is **3**. If a link remains unavailable after the specified number of check attempts, the link is considered invalid.
	Link Switch Limit	Controls the maximum number of link status switches before the priority of a link is degraded. The value ranges from 0 to 10, and the default value is **5**. The value **0** indicates no limit on the number

Parameter		Description
		of link status switches. Note The link status changing from Up to Down is counted as one time of switching, but changing from Down to Up is not. After the number of link status switches exceeds the specified maximum number, the link will be disabled and can be enabled manually only.

6.3.3 MAC Address Table

The MAC address table specifies the mapping between IP addresses and MAC addresses on the ADS device for fast data forwarding. The MAC address table can be added manually or learned by the ADS device dynamically. For details on dynamic learning of MAC addresses, see section 6.3.2.6 Learning MAC Address. This section covers the following topics:

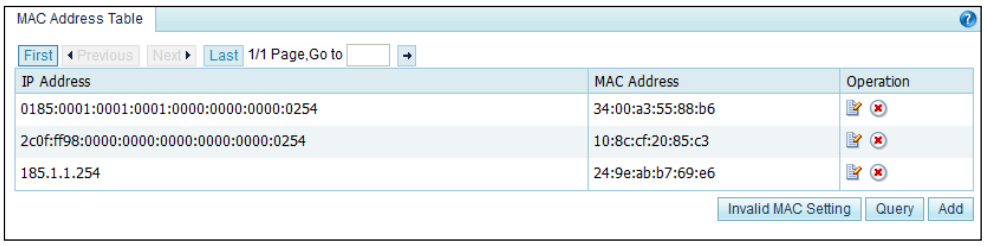
- Adding a MAC Address Entry
- Editing a MAC Address Entry
- Deleting a MAC Address Entry
- Querying MAC Addresses
- Configuring Invalid MAC Addresses

6.3.3.1 Adding a MAC Address Entry

To add a MAC address entry, perform the following steps:

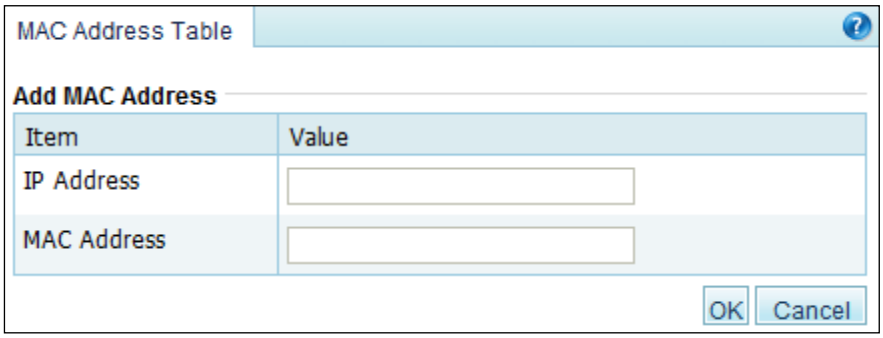
Step 1 Choose **Diversion & Injection** > **Traffic Injection** > **MAC Address Table** to open the configuration page for the MAC address table.

Figure 6-22 MAC address table



Step 2 Click **Add** to the lower right of the MAC address table to open the page for adding the mapping between an IP address and a MAC address.

Figure 6-23 Adding the mapping between an IP address and a MAC address



Step 3 Type the IP address and MAC address and click **OK** to save the settings.

Note	The ADS device supports the IPv4/IPv6 dual-stack. Therefore, you can configure IPv4 or IPv6 addresses in the MAC address table.

----End

6.3.3.2 Editing a MAC Address Entry

After configuring MAC address entries, you can edit parameters of this entry by performing the following steps:

Step 1 On the page shown in Figure 6-22, click in the **Operation** column of a MAC address to edit its parameters.

Step 2 After editing parameters, click **OK** to save the settings and return to the MAC address table.

----End

6.3.3.3 Deleting a MAC Address Entry

You can delete MAC address entries one by one on the ADS device.

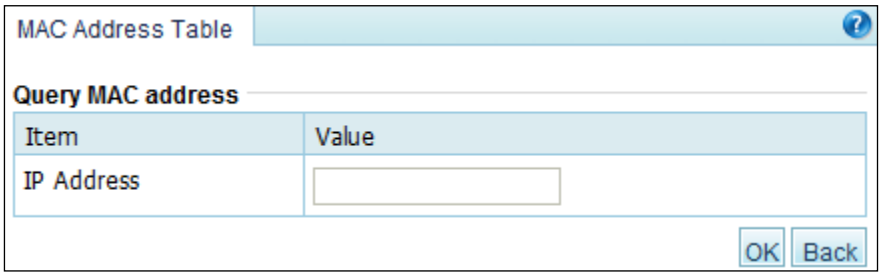
In the MAC address table shown in Figure 6-22, click in the **Operation** column of a MAC address entry and then click **OK** to delete an entry.

6.3.3.4 Querying MAC Addresses

To query the MAC address mapped to an IPv4 or IPv6 address, perform the following steps:

Step 1 In Figure 6-22, click **Query** to the lower right of the MAC address table to open the MAC address query page.

Figure 6-24 Querying the MAC address mapped to an IP address



Step 2 Type the IPv4 or IPv6 address and click **OK**.

Then, the MAC address mapped to this IP address is displayed.

Step 3 Click **Back** to return to the MAC address table.

----End

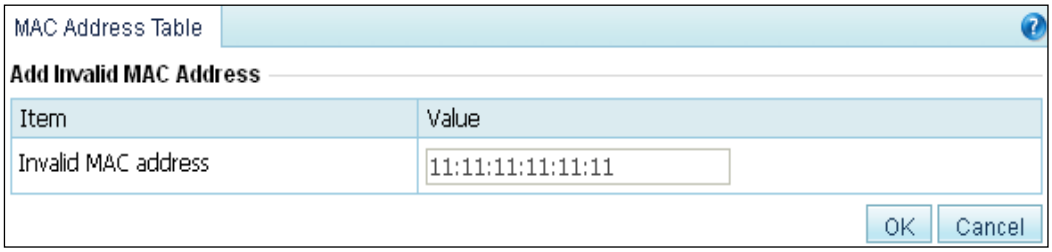
6.3.3.5 Configuring Invalid MAC Addresses

If the MAC address of an IP packet is the same as an invalid MAC address configured on the ADS device, the system drops the packet automatically.

To add an invalid MAC address, perform the following steps:

Step 1 In Figure 6-22, click **Invalid MAC Setting** to the lower right of the MAC address table to open the page for configuring invalid MAC addresses. See Figure 6-25.

Figure 6-25 Configuring invalid MAC addresses



Step 2 Configure invalid addresses.

The default invalid MAC address is **11:11:11:11:11:11**. You can configure other invalid addresses as required and then click **OK** to save the settings.

Note	MAC addresses typed on the web page must be separated by colons.

----End

6.4 Traffic Diversion

This section covers the following topics:

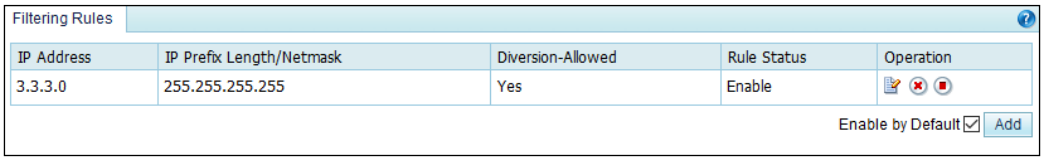
- Filtering Rules
- Manual Diversion
- Group Diversion
- Diversion Routing Table

6.4.1 Filtering Rules

A diversion filtering rule enables the ADS device to filter attack traffic transmitted from NSFOCUS ADS detection devices, to determine whether to send routing notifications, and to activate diversion automatically.

As shown in Figure 6-26, diversion filtering rules are listed by time of addition. The device matches rules (of **Enable** status) from top to bottom and uses the default rule if no rule is matched.

Figure 6-26 Filtering rules



Creating a Diversion Filtering Rule

In Figure 6-26, click **Add** to the lower right of the list. On the **Add Diversion Filtering Rule** page, configure parameters and click **OK**.

Figure 6-27 Creating a diversion filtering rule

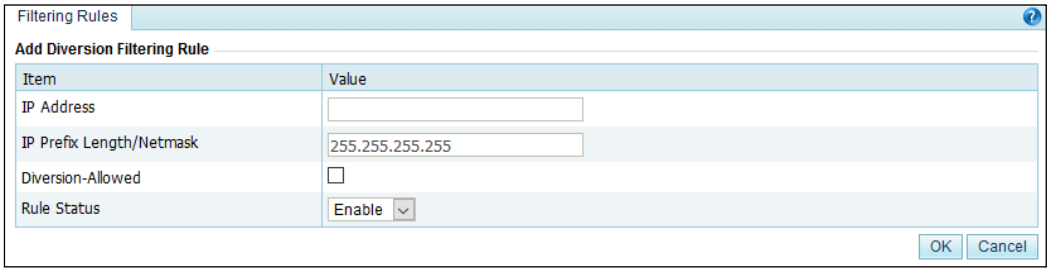


Table 6-12 describes parameters for creating a diversion filtering rule.

Table 6-12 Parameters for creating a diversion filtering rule

Parameter	Description
IP Address	IP address or segment to be protected. You can type an IPv4 or IPv6 address according to the actual network deployment.

Parameter	Description
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be protected. This parameter allows you to configure a network segment.
Diversion-Allowed	Controls whether to enable diversion. A check in the checkbox indicates that the ADS device allows diversion. This check box is deselected by default, indicating that the ADS device does not allow diversion.
Rule Status	Controls whether to enable the rule immediately after the rule is added. It has the following values: • **Enable**: enables a diversion filter rule immediately after it is added. • **Disable**: disables the diversion filter rule that can be enabled later manually.

Editing a Diversion Filtering Rule

On the diversion filtering rule list shown in Figure 6-26, click in the **Operation** column to edit a rule.

Deleting a Diversion Filtering Rule

On the diversion filtering rule list shown in Figure 6-26, click in the **Operation** column to delete a rule.

Changing the Status of a Diversion Filtering Rule

On the diversion filtering rule list shown in Figure 6-26, click in the **Operation** column to change the status **Enable** to **Disable**, and click to change the status **Disable** to **Enable**.

Changing the Priority of a Diversion Filtering Rule

On the diversion filtering rule list shown in Figure 6-26, click and to change the priority of the rules in the list.

6.4.2 Manual Diversion

In a cluster, a manual diversion policy is used to divert traffic of an IP address to different ADS devices. After a manual diversion policy is added or deleted, it will take effect immediately and be displayed on or disappear from the list, without requiring a click on the **Save** button.

Note	In manual diversion mode, each time ADS diverts traffic to only one /24 subnet address to the ADS device. If you want the ADS device to divert traffic to multiple /24 subnet addresses, please configure multiple manual traffic diversion rules.

This section covers the following topics:

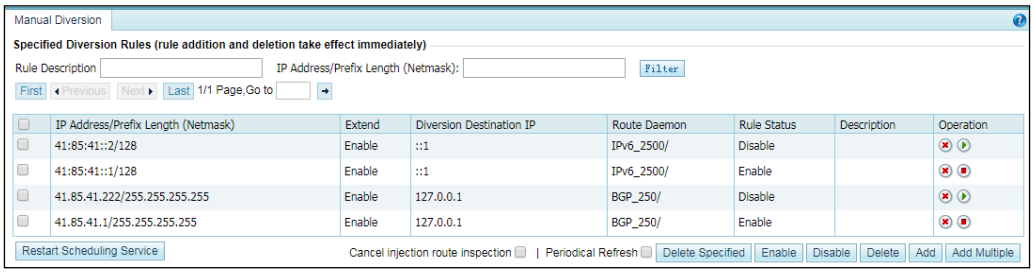
- Creating a Manual Traffic Diversion Rule
- Creating Manual Diversion Rules in Batches
- Enabling and Disabling Manual Diversion Rules
- Filtering Manual Diversion Rules
- Deleting Manual Diversion Rules
- Deleting a Specified Route
- Refreshing Routes Periodically
- Canceling Injection Route Inspection
- Restarting the Scheduling Service

6.4.2.1 Creating a Manual Traffic Diversion Rule

To create a traffic diversion rule, perform the following steps:

Step 1 Choose **Diversion & Injection** > **Traffic Diversion** > **Manual Diversion** to open the diversion rule configuration page.

Figure 6-28 Traffic diversion rules



Step 2 Click **Add**.

Figure 6-29 Creating a traffic diversion rule

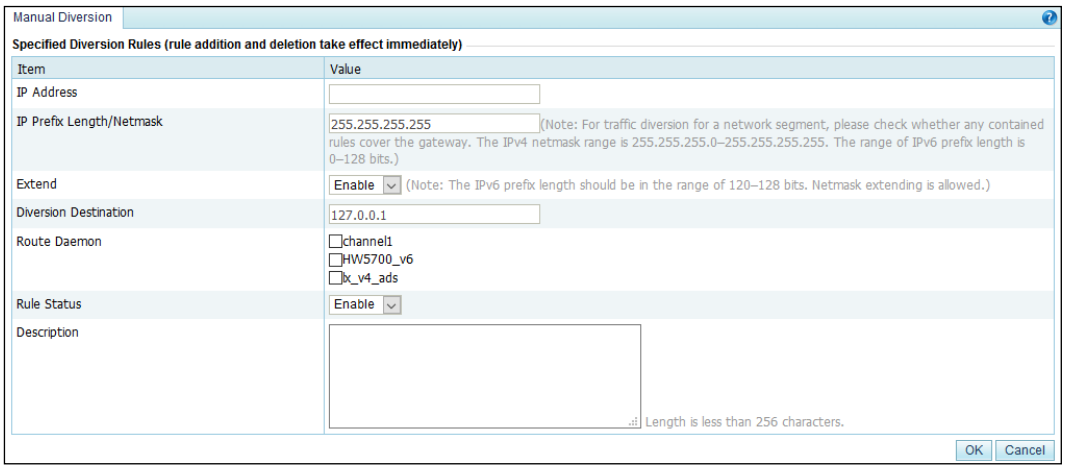


Table 6-13 describes parameters for creating a diversion rule.

Table 6-13 Parameters for creating a diversion rule

Parameter	Description
IP Address	IP address or IP segment to be protected, usually the IP address of the protected server. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be diverted. Note The netmask of an IPv4 address to be protected can range from 255.255.255.0 to 255.255.255.255.
Extend	Controls whether diversion rules can be set for specific IP addresses in a subnet. • **Enable**: indicates that diversion rules can be set for specific IP addresses in a subnet. • **Disable**: indicates that diversion rules can only be set to the subnet, instead of specific IP addresses in the subnet.
Diversion Destination	Next-hop IP address of the route notification sent from the route daemon. It is usually the IP address of the diversion interface of the ADS device or ::1. The default value is **127.0.0.1**.
Route Daemon	Route daemon that sends a routing notification.
Rule Status	Controls whether to enable the rule immediately after the rule is added. It has the following values: • **Enable**: enables a diversion filter rule immediately after it is added. • **Disable**: disables the diversion filter rule that can be enabled later manually.

Step 3 Set parameters and click **OK** to save the settings.

Note	To ensure the injection of the diverted traffic, you must configure the injection route and injection MAC address correctly before manual diversion.

Step 4 Click **Apply** in the upper-right corner of the web-based manager to make the settings take effect.

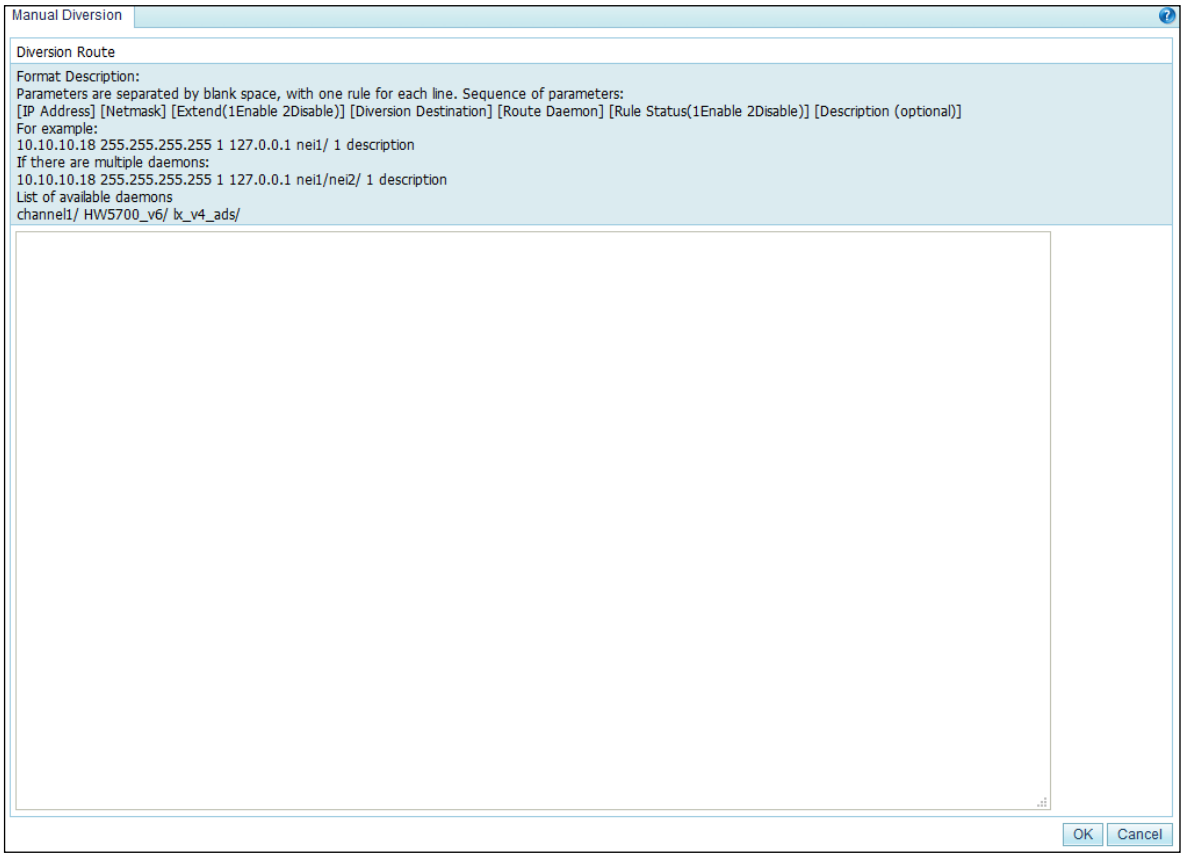
----End

6.4.2.2 Creating Manual Diversion Rules in Batches

To simplify operations, you can create manual diversion rules in batches on the ADS device by performing the following steps:

Step 1 Click **Add Multiple** to the lower right of the rule list on the page shown in Figure 6-28.

Figure 6-30 Creating traffic diversion rules in batches



Step 2 Type multiple manual diversion rules as prompted.

Pay attention to the following format specifications:

- Type a manual diversion rule as follows: [IP address] [netmask] [route daemon], for example, 10.10.10.18 255.255.255.255 nei1. For multiple daemons, a manual diversion rule is added as follows: 10.10.10.18 255.255.255.255 nei1/nei2/.
- Three types of daemons are available: bgp, ospf, and rip.
- Parameters of a manual diversion rule are separated by spaces.
- Each line can contain only one manual diversion rule.

Step 3 After configuring parameters, click **OK** to save the settings.

----End

6.4.2.3 Enabling and Disabling Manual Diversion Rules

On the ADS device, only enabled manual diversion rules are valid, while disabled ones are invalid. Enabling and disabling manual diversion rules frees you from redundant deletions and additions. If some manual diversion rules are not required currently, disable them.

You can enable or disable a single manual diversion rule or more rules in batches.

Enabling Manual Diversion Rules

- Method 1: On the manual diversion rule list shown in Figure 6-28, click in the **Operation** column of a disabled rule to enable it. Then, the status icon of this rule turns to .
- Method 2: On the manual diversion rule list shown in Figure 6-28, select one or more rules (or select the **Select All** check box to select all manual diversion rules) to be enabled, click **Enable** to the lower right of the rule list, and click **OK** in the confirmation dialog box to enable the selected rules.

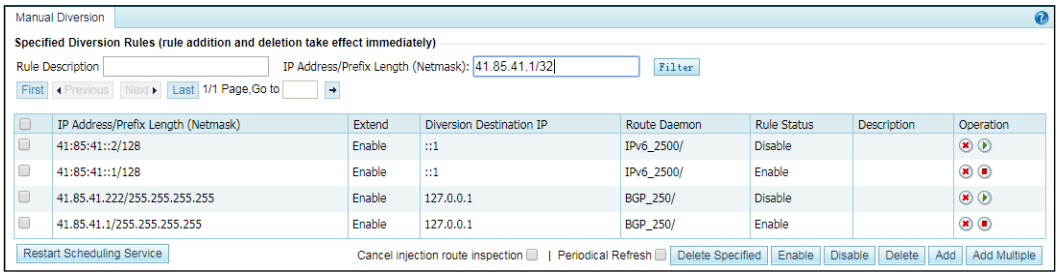
Disabling Manual Diversion Rules

- Method 1: On the manual diversion rule list shown in Figure 6-28, click in the **Operation** column of an enabled rule to disable it. Then, the status icon of this rule turns to .
- Method 2: On the manual diversion rule list shown in Figure 6-28, select one or more rules (or select the **Select All** check box to select all manual diversion rules) to be dissabled , click **Disable** to the lower right of the rule list, and click **OK** in the confirmation dialog box to disable the selected rules.

6.4.2.4 Filtering Manual Diversion Rules

On the **Manual Diversion** page shown in Figure 6-28, type a keyword in the **Rule Description** text box or type an IP address and subnet in the **IP Address/Prefix Length (Netmask)** text box and click **Filter**. Manual diversion rules meeting the specified conditions will be displayed, as shown in Figure 6-31.

Figure 6-31 Filtering manual diversion rules



6.4.2.5 Deleting Manual Diversion Rules

You can delete a single manual diversion rule or more rules in batches on the ADS device. This section describes how to delete unused diversion rules. For details on deleting diversion rules that are being used, see section 6.4.2.6 Deleting a Specified Route.

- Method 1: On the manual diversion rule list shown in Figure 6-28, click in the **Operation** column and click **OK** in the confirmation dialog box to delete a rule.
- Method 2: On the manual diversion rule list shown in Figure 6-28, select one or more rules (or select the **Select All** check box to select all manual diversion rules) to be deleted, click **Delete** to the lower right of the rule list, and then click **OK** in the confirmation dialog box to delete the selected rules.

Note	For details on deleting diversion rules that are being used, see section *6.4.2.6* Deleting a Specified Route.

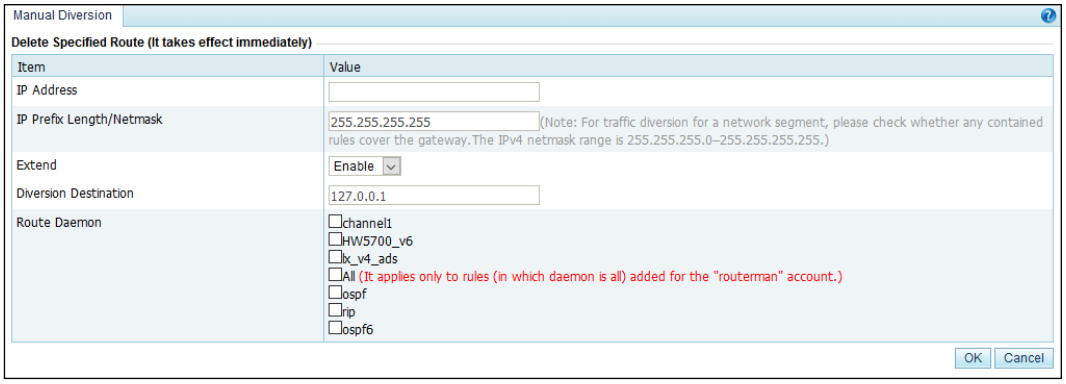
6.4.2.6 Deleting a Specified Route

Delete Specified is used to delete diversion rules that are being used. The detailed procedure is as follows:

Step 1 On the manual diversion rule list in Figure 6-28, click **Delete Specified** to open the diversion rule deletion page.

See Table 6-13 for descriptions of parameters in the **Delete Specified Route** dialog box.

Figure 6-32 Deleting a specified diversion rule



Step 2 Type the information about a diversion rule to be deleted and click **OK** to make the settings take effect.

----End

6.4.2.7 Refreshing Routes Periodically

After **Periodical Refresh** is selected, the route daemon information in manual diversion rules is refreshed every 60 seconds by default.

If the periodical route refresh function is enabled before manual diversion is interrupted, the ADS device refreshes the route daemon information and re-diverts the traffic immediately after detecting a BGP route failure. If the periodical route refresh function is not enabled, the ADS device does not refresh the route daemon information or re-divert the traffic information even it has detected a BGP route failure.

On the manual diversion rule list shown in Figure 6-28, you can select the **Periodical Refresh** check box to enable the periodical route refresh function or deselect it to disable the periodical route refresh function.

6.4.2.8 Canceling Injection Route Inspection

If **Cancel injection route inspection** is selected, manually configured diversion rules can be used without injection route inspection. If the **Cancel injection route inspection** check box is

not selected, the system will perform injection route inspection for a diversion rule to be enabled. The diversion rule can be successfully enabled only if the IP address of the injection route is valid.

On the page shown in Figure 6-28, you can select the **Cancel injection route inspection check box to disable injection route inspection, or deselect it to enable injection route inspection.**

6.4.2.9 Restarting the Scheduling Service

Restarting the scheduling service is used to reload manual diversion settings and make settings take effect. This prevents the engine restart from interrupting other services.

On the tab page shown in Figure 6-28, you can click **Restart Scheduling Service** and then click **OK** in the confirmation dialog box, to restart the scheduling service.

6.4.3 Group Diversion

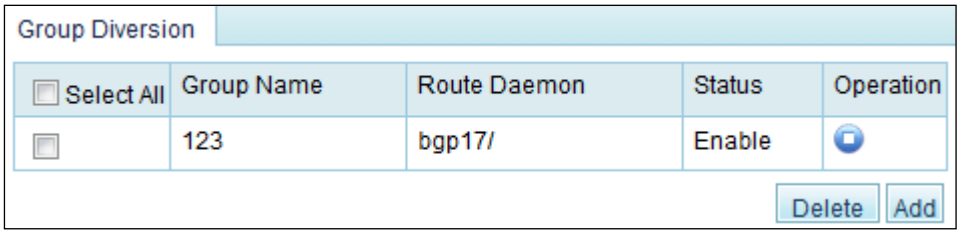
Group diversion rules are used to divert the traffic destined for a protection group to the diversion interface on the ADS device. This section describes how to add, delete, enable, and disable group diversion rules.

Creating a Group Diversion Rule

To create a group diversion rule, perform the following steps:

Step 1 Choose **Diversion & Injection** > **Traffic Diversion** > **Group Diversion**.

Figure 6-33 Group diversion rules



Step 2 Click **Add**.

Figure 6-34 Creating a group diversion rule

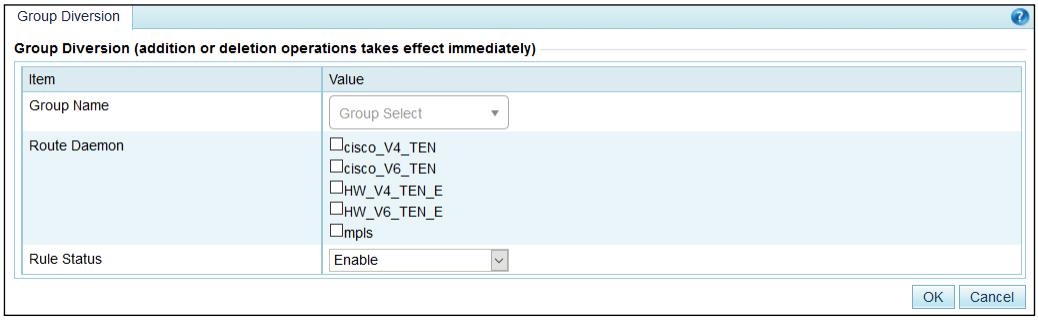


Table 6-14 describes parameters for creating a group diversion rule.

Table 6-14 Parameters for creating a group diversion rule

Parameter	Description
Group Name	Protection group whose traffic is to be diverted. Fuzzy search is supported. For details on configuring a protection group, see section 5.1.2 Policy Configuration for Protection Groups.
Route Daemon	Route daemon.
Rule Status	Controls whether to enable the group diversion rule. • **Enable**: enables the group diversion rule. • **Disable**: disables the group diversion rule.

Step 3 Set parameters and click **OK** to save the settings.

----End

Deleting Group Diversion Rules

To delete group diversion rules, perform the following steps:

On the group diversion rule list shown in Figure 6-33, select one or more group diversion rules (or select the **Select All** check box to select all rules) to be deleted, click **Delete** to the lower right of the group diversion rule list, and click **OK** in the confirmation dialog box to delete the selected rules.

Enabling/Disabling Group Diversion Rules

Enabled group diversion rules are valid, while disabled rules are invalid.

On the group diversion rule list, **Status** is displayed as **Enable** for enabled rules and **Disable** for disabled rules.

- To delete group diversion rules, perform the following steps:

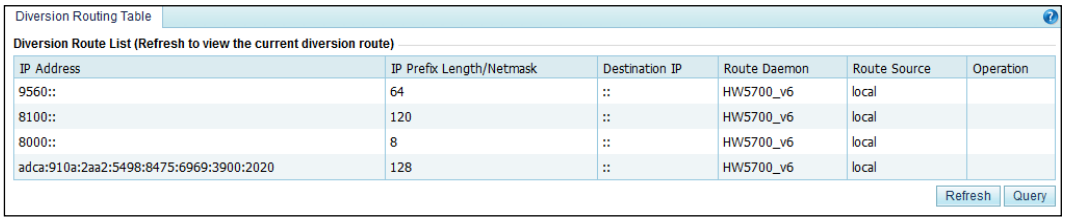
  On the group diversion rule list shown in Figure 6-33, click in the **Operation** column of a group diversion rule to enable it.
- To disable a group diversion rule, perform the following steps:

  On the group diversion rule list shown in Figure 6-33, click in the **Operation** column of a group diversion rule to disable it.

6.4.4 Diversion Routing Table

As shown in Figure 6-35, a diversion routing table stores diversion routes that are being used by the ADS device. It is automatically generated based on traffic diversion policies and diversion notifications from NSFOCUS ADS detection devices. Click **Refresh** to view the latest diversion routes of the system.

Figure 6-35 Diversion routing table



IP Address	IP Prefix Length/Netmask	Destination IP	Route Daemon	Route Source	Operation
9560::	64	::	HW5700_v6	local	
8100::	120	::	HW5700_v6	local	
8000::	8	::	HW5700_v6	local	
adca:910a:2aa2:5498:8475:6969:3900:2020	128	::	HW5700_v6	local	

Searching for a Diversion Route

Step 1 In Figure 6-35, click **Query** to the lower right of the diversion routing table.

The **Query Diversion Route** page appears, as shown in Figure 6-36.

Figure 6-36 Searching for diversion routes

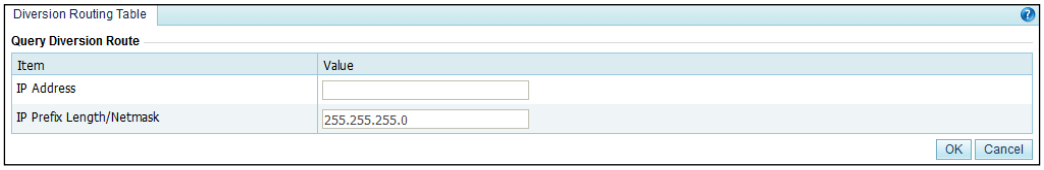


Table 6-15 describes parameters of a diversion route.

Table 6-15 Parameters of a diversion route

Parameter	Description
IP Address	IP address or IP segment specified by **IP Address** in the diversion routing table. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be searched for. **Note** The netmask of an IPv4 address to be searched for must be 255.255.255.255.

Step 2 After parameters are configured, click **OK** to query the results.

Step 3 After querying the results, click **Back** to return to the diversion route list.

----End

6.5 Advanced Route Setting

This section covers the following topics:

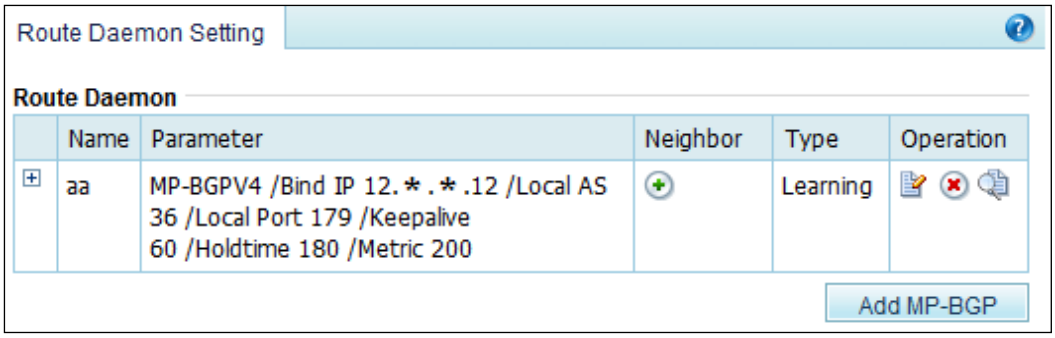
- MPLS Route

- Other Routes

6.5.1 MPLS Route

As shown in Figure 6-37, you can configure MPLS routes to accomplish layer 2 label learning between VPNs.

Figure 6-37 List of MPLS routes



Creating an MPLS Route

In Figure 6-37, click **Add MP-BGP** to the lower right of the route daemon list. On the **MP-BGP Local Parameter Setting** page, configure parameters and then click **OK**.

Figure 6-38 Creating an MPLS route

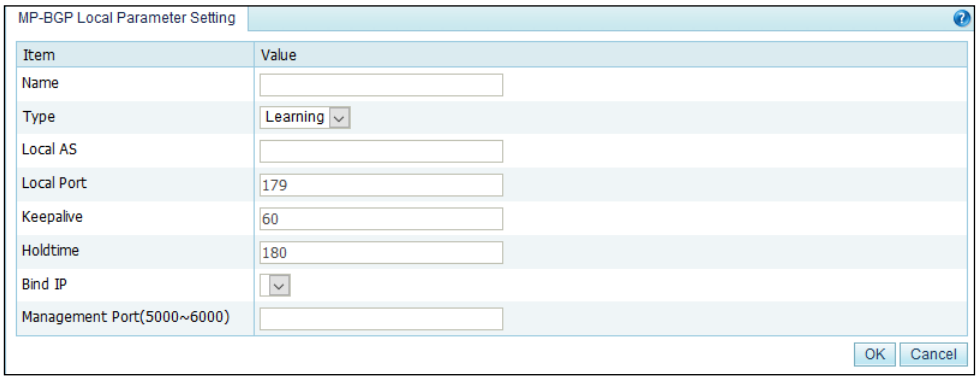


Table 6-16 describes parameters for creating an MPLS route.

Table 6-16 Parameters for creating an MPLS route

Parameter	Description
Name	Route daemon name.
Type	Type of the route. Currently, only **Learning** is available for selection.
Local AS	AS number of a BGP route daemon.
Local Port	BGP port of the route daemon. Generally, the default port **179** is used.

Parameter	Description
Bind IP	Local IPv4 address of a route daemon.
Management Port(5000~6000)	Management port of the route daemon. The port ranges from 5000 to 6000.

Other parameters such as **Keepalive** and **Holdtime** correspond to certain fields within the BGPv4 protocol.

Editing a Route

In the list of MPLS routes shown in Figure 6-37, click in the **Operation** column to edit the corresponding route.

Deleting a Route

On the list of MPLS routes shown in Figure 6-37, click in the **Operation** column to delete the corresponding route.

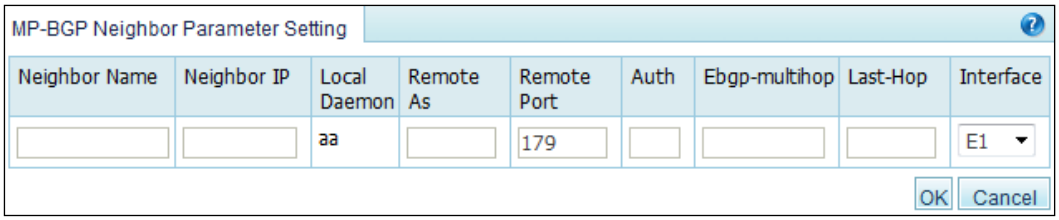
Viewing Route Status

On the list of MPLS routes shown in Figure 6-37, click in the **Operation** column to view status of the corresponding route.

Adding a Neighbor

On the list of local routes shown in Figure 6-37, click in the **Neighbor** column to add a neighbor for the MPLS route. See Figure 6-39.

Figure 6-39 Adding a neighbor for MPLS route



Note	After adding a neighbor, click to check whether the neighbor is connected.

Viewing Neighbor Status

In the list of local routes, click in the **Operation** column to view connection status of the MPLS neighbor.

Hiding a Neighbor

Neighbors of each route are displayed in the MPLS route list initially. Click ⊟ of a route to hide its neighbors and click ⊞ to display them.

6.5.2 Other Routes

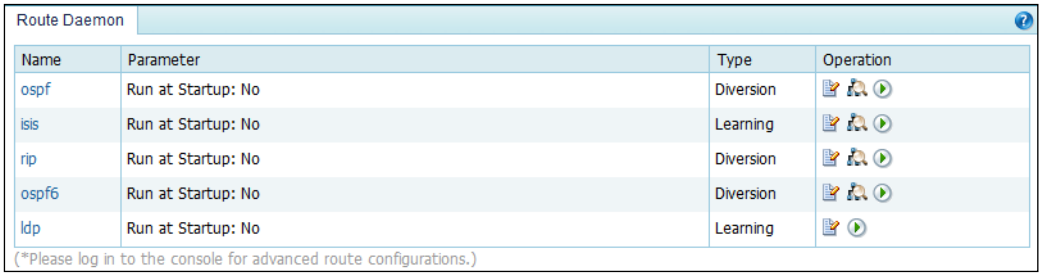
In addition to routing protocols described above, the ADS device supports such advanced routing protocols as OSPF, ISIS, RIP, OSPF6, and LDP.

Currently, the administrator **admin**, can configure LDP routes or view, enable, or disable OSPF, ISIS, RIP, OSPF6, and LDP routes on the web-based manager, while the CLI administrator, **routerman**, can configure OSPF, ISIS, RIP, and OSPF6 routes on the CLI.

Configuring an LDP Route

Step 1 After logging in to the web-based manager, choose **Diversion & Injection** > **Advanced Route Setting** > **Others** to open the list of other routes.

Figure 6-40 List of other routes



Step 2 Click in the **Operation** column to edit LDP route parameters.

Figure 6-41 Editing LDP route parameters

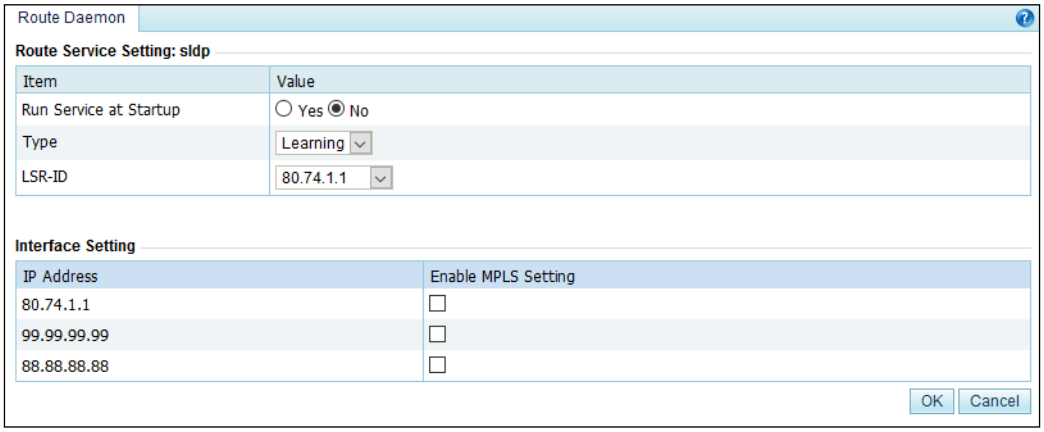


Table 6-17 describes LDP route parameters.

Table 6-17 LDP route parameters

Parameter	Description
Run Service at Startup	Controls whether to run LDP upon system startup. • **Yes**: indicates that the system runs LDP upon system startup. • **No**: indicates that the system does not run LDP upon system startup.
Type	Route type. The default route type is **Learning**.
LSR-ID	Label switching router ID.
Interface Setting	Interfaces on which MPLS and LDP are enabled.

Step 3 Set parameters and click **OK** to save the settings.

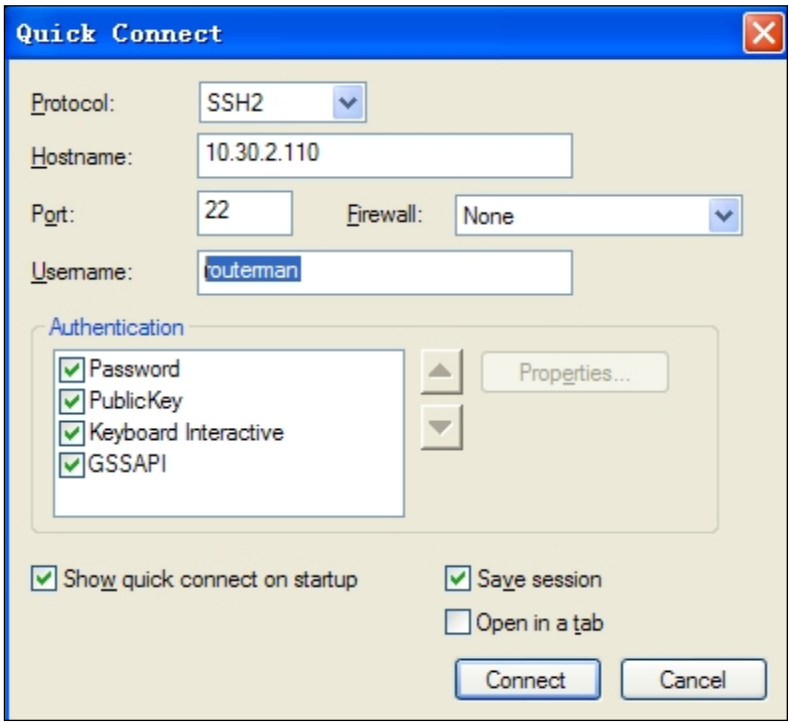
----End

Configuring OSPF, ISIS, RIP, and OSPF6 Routes

Here, the OSPF route is used as an example to describe the route configuration procedure.

Step 1 Log in to the ADS device in SSH mode as the CLI administrator, **routerman**.

Figure 6-42 ADS login in SSH mode



Step 2 Enable OSPF on the interface via the CLI.

Figure 6-43 Editing OSPF route parameters

```
COLLAPSAR-4000#router ospf session
Trying 127.*.*.1...
                    Connected to 127.*.*.1.
                                          Escape character is '^]'.

Hello, this is Quagga (version 0.99.5).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password:
```

Step 3 After the parameter configuration is complete, save the settings and exit.

----End

Viewing Route Status

After logging in to the web-based manager, the administrator **admin** can click to view the status of a route of a specific protocol in the route protocol list shown in Figure 6-40.

Enabling/Disabling the Route Protocol

After logging in to the web-based manager, the administrator **admin** can click to enable a route of a specific protocol or click to disable a route in the route protocol list as shown in Figure 6-40.

Note	Routes under **Others** cannot be deleted.

6.6 Syslog Diversion Configuration

ADS can collaborate with abnormal traffic detection devices from other vendors, such as Genie, Arbor, Samurai, and Kuanguang, to jointly protect customers' networks against DDoS attacks.

Third-party devices provide effective abnormal traffic detection. After accurately locating the potential attack source and attack target, such a device handles the event according to the syslog-based diversion settings configured on ADS. If the diversion type is set to **Auto**, it notifies ADS, which then automatically diverts the abnormal traffic for cleaning. After filtering the traffic, ADS injects the normal traffic back into the network. If the diversion type is set to **Manual**, it notifies ADS, which, in turn, notifies the O&M personnel, who will then decide whether to divert the traffic.

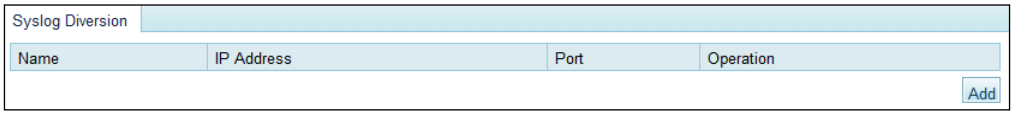
Note	For Genie and Arbor devices, the diversion type can be either **Auto** or **Manual**. For Samurai and Kuanguang devices, the diversion type can only be **Auto**.

6.6.1 Diversion Configuration

To configure syslog-based traffic diversion, perform the following steps:

Step 1 Choose **Diversion & Injection** > **Syslog Diversion Config** > **Diversion Config**.

Figure 6-44 Syslog-based diversion rule list



Step 2 Click **Add**.

Figure 6-45 Creating a diversion rule

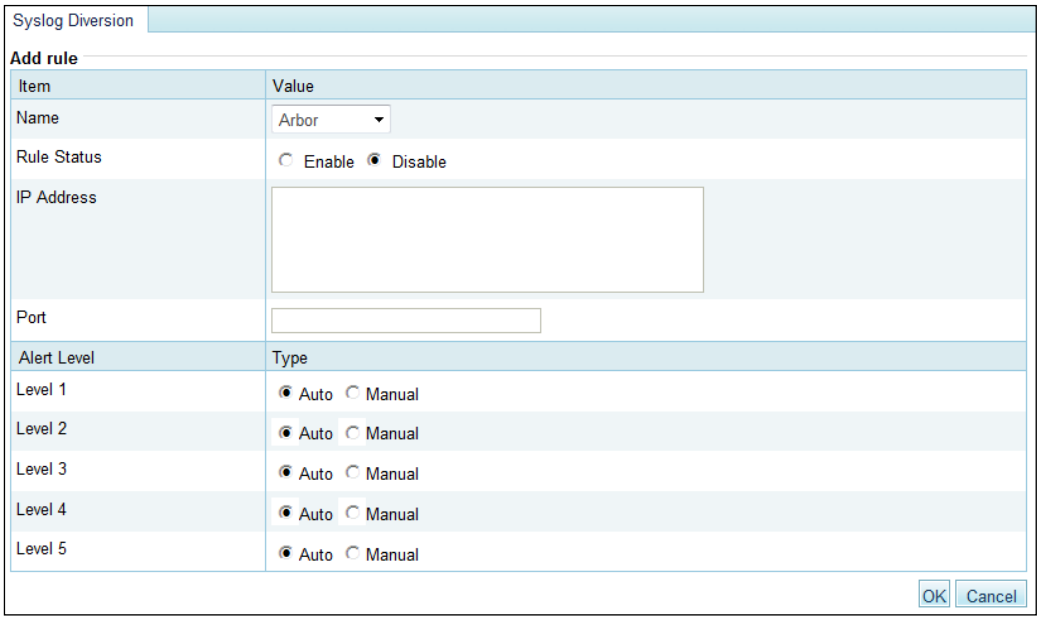


Table 6-18 describes parameters for creating a syslog-based diversion rule.

Table 6-18 Parameters for creating a syslog-based diversion rule

Parameter	Description
Name	Specifies the type of the device to collaborate with ADS for syslog-based traffic diversion. It can be **Genie**, **Arbor**, **Samurai**, or **Kuanguang**.

Parameter	Description
Rule Status	Status of the rule. The rule takes effect only after it is enabled.
IP Address	IP address of the third-party device.
Port	Port for communicating with the third-party device.
Alert Level	Specifies the alert level that will trigger traffic diversion. This parameter is available only for Genie and Arbor devices. • On a Genie ATM device, alert levels for abnormal traffic are classified into critical and warning. **Auto** indicates that the Genie ATM device, after detecting abnormal traffic of the corresponding alert level, notifies ADS, which then automatically diverts such traffic for cleaning. **Manual** indicates that the Genie ATM device, after detecting abnormal traffic, notifies ADS, which, in turn, notifies the O&M personnel, who will then determine whether to divert the traffic. • On an Arbor device, alert levels for abnormal traffic are classified into five levels (level 1 to level 5). **Auto** indicates that the Arbor device, after detecting abnormal traffic of the corresponding alert level, notifies ADS, which then automatically diverts such traffic for cleaning. **Manual** indicates that the Arbor device, after detecting abnormal traffic, notifies ADS, which, in turn, notifies the O&M personnel, who will then determine whether to divert the traffic.

Step 3 After configuring parameters, click **OK** to save the settings.

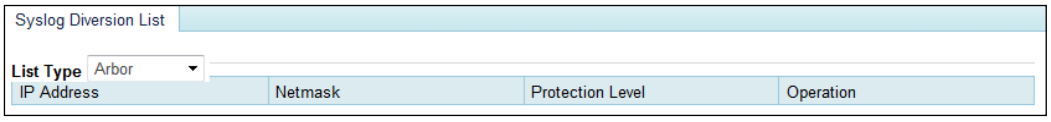
----End

6.6.2 Diversion Rule List

After syslog-based traffic diversion is configured, information about traffic diversion associated with this device is automatically displayed in the **Syslog Diversion List**. This list displays information about third-party devices that initiate abnormal traffic diversion, including the IP address/netmask, alert level, and operation type.

Diversion information can be displayed here only after manual diversion is configured and abnormal traffic has been diverted.

Figure 6-46 Syslog diversion list



7 Logs

This chapter dwells upon current system logs, containing the following sections:

Section	Description
Attack Logs	Provides details about attack logs.
System Logs	Provides various logs about system operation.
Log Analysis	Provides details about log processing.

7.1 Attack Logs

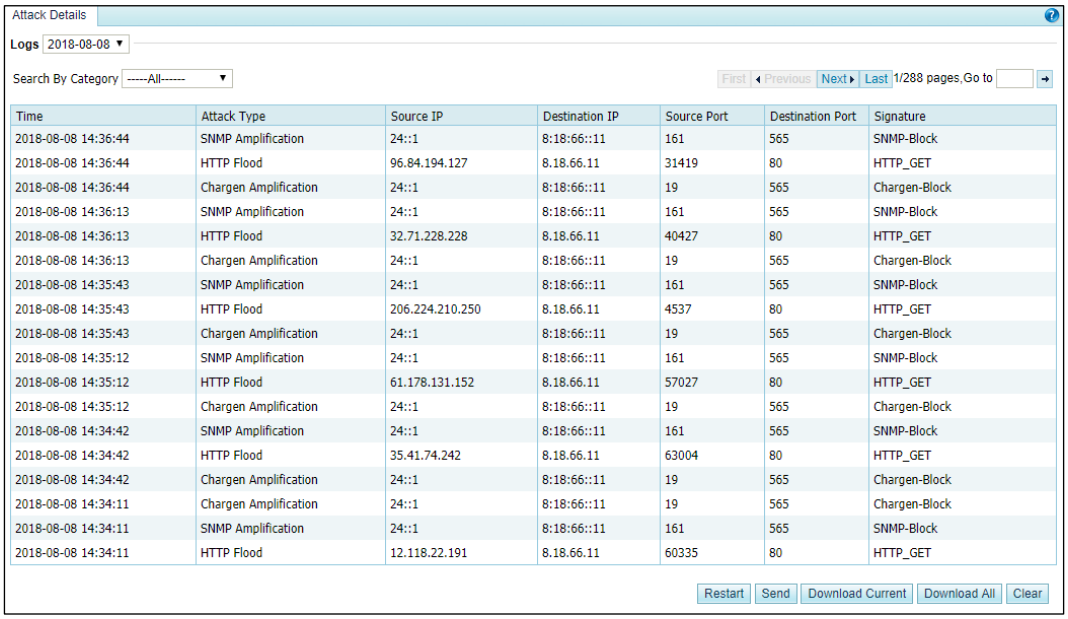
All attack logs are displayed in two ways for easier viewing: statistical graph and data table.

7.1.1 Attack Details

You can view attack logs of the last 15 days, as shown in Figure 7-1. By default, attack logs of the current day are listed.

You can select the dimension from the **Search by Category** drop-down box to search for logs by attack type, source IP address, destination IP address, source port, destination port, and signature. If you select **All** from this drop-down box, all logs are searched for.

Figure 7-1 Attack logs



Time	Attack Type	Source IP	Destination IP	Source Port	Destination Port	Signature
2018-08-08 14:36:44	SNMP Amplification	24::1	8:18:66::11	161	565	SNMP-Block
2018-08-08 14:36:44	HTTP Flood	96.84.194.127	8.18.66.11	31419	80	HTTP_GET
2018-08-08 14:36:44	Chargen Amplification	24::1	8:18:66::11	19	565	Chargen-Block
2018-08-08 14:36:13	SNMP Amplification	24::1	8:18:66::11	161	565	SNMP-Block
2018-08-08 14:36:13	HTTP Flood	32.71.228.228	8.18.66.11	40427	80	HTTP_GET
2018-08-08 14:36:13	Chargen Amplification	24::1	8:18:66::11	19	565	Chargen-Block
2018-08-08 14:35:43	SNMP Amplification	24::1	8:18:66::11	161	565	SNMP-Block
2018-08-08 14:35:43	HTTP Flood	206.224.210.250	8.18.66.11	4537	80	HTTP_GET
2018-08-08 14:35:43	Chargen Amplification	24::1	8:18:66::11	19	565	Chargen-Block
2018-08-08 14:35:12	SNMP Amplification	24::1	8:18:66::11	161	565	SNMP-Block
2018-08-08 14:35:12	HTTP Flood	61.178.131.152	8.18.66.11	57027	80	HTTP_GET
2018-08-08 14:35:12	Chargen Amplification	24::1	8:18:66::11	19	565	Chargen-Block
2018-08-08 14:34:42	SNMP Amplification	24::1	8:18:66::11	161	565	SNMP-Block
2018-08-08 14:34:42	HTTP Flood	35.41.74.242	8.18.66.11	63004	80	HTTP_GET
2018-08-08 14:34:42	Chargen Amplification	24::1	8:18:66::11	19	565	Chargen-Block
2018-08-08 14:34:11	Chargen Amplification	24::1	8:18:66::11	19	565	Chargen-Block
2018-08-08 14:34:11	SNMP Amplification	24::1	8:18:66::11	161	565	SNMP-Block
2018-08-08 14:34:11	HTTP Flood	12.118.22.191	8.18.66.11	60335	80	HTTP_GET

Table 7-1 describes attack log parameters.

Table 7-1 Attack log parameters

Parameter	Description
Time	Time when the attack occurs.
Attack Type	Type of the attack.
Source IP/Port	Source IP address and port of the attack.
Destination IP/Port	Destination IP address and port of the attack.
Signature	Signature defined by the system for various types of attacks. For example, the signature of SYN flood attacks is **SYN-CHECK**.

To the upper right of the log table, you can operate on attack logs as follows:

- Restart the log service.

  Click **Restart** to restart the log service program.
- Send logs.

  Click **Send** to send current attack logs to a specific email address.
- Download logs.

  Click **Download Current** to download logs of a specific day or click **Download All** to download all logs. This makes it easier for you to search for and handle logs.
- Clear logs.

  Click **Clear** to clear all the attack information on the current day.

7.1.2 Statistical Graph

At the bottom of the **Statistical Graph** page, you can click **Pie Chart** to view the proportion of each type of attacks or click **Bar Chart** to view the number of attacks of each type on the current day. See Figure 7-2 and Figure 7-3.

Figure 7-2 Attack proportion

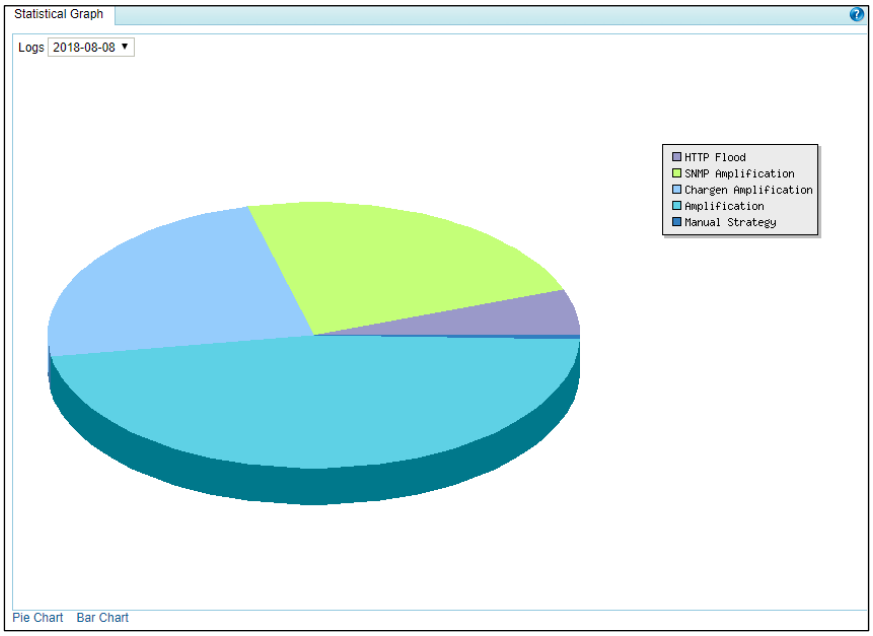
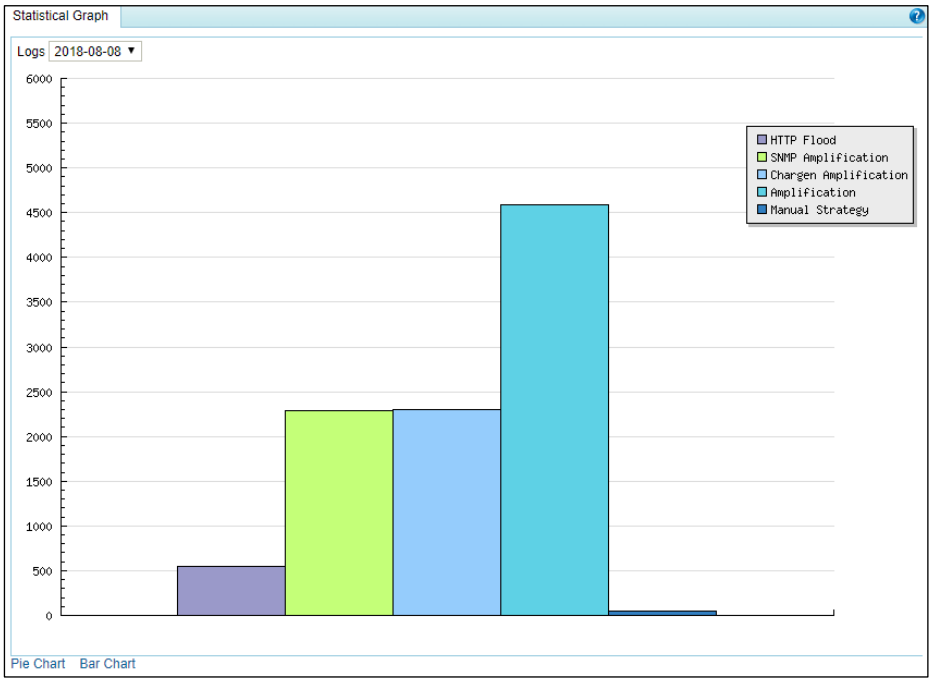


Figure 7-3 Number of attacks of each type



7.2 System Logs

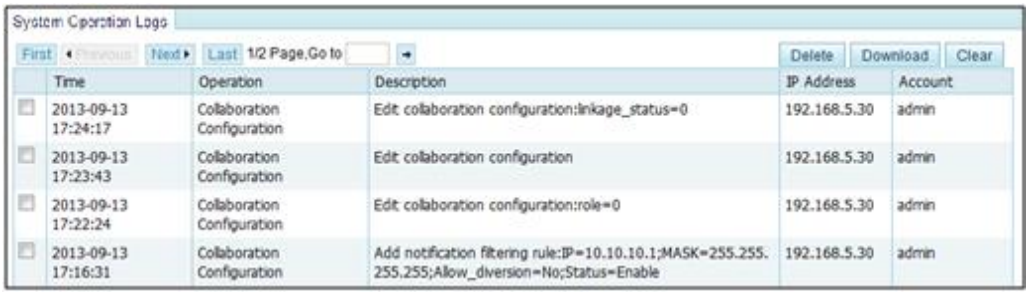
System logs include the following:

- System Operation Logs
- System Login Logs
- Link Status Logs
- Traffic Diversion Logs
- HA Synchronization Logs
- Syslog Diversion Logs

7.2.1 System Operation Logs

As shown in Figure 7-4, the system operation log table displays main operations of users in the system.

Figure 7-4 System operation logs



Time	Operation	Description	IP Address	Account
2013-09-13 17:24:17	Collaboration Configuration	Edit collaboration configuration:linkage_status=0	192.168.5.30	admin
2013-09-13 17:23:43	Collaboration Configuration	Edit collaboration configuration	192.168.5.30	admin
2013-09-13 17:22:24	Collaboration Configuration	Edit collaboration configuration:role=0	192.168.5.30	admin
2013-09-13 17:16:31	Collaboration Configuration	Add notification filtering rule:IP=10.10.10.1;MASK=255.255.255.255;Allow_diversion=No;Status=Enable	192.168.5.30	admin

Table 7-2 describes parameters of system operation logs.

Table 7-2 Parameters of system operation logs

Parameter	Description
Time	Time when a user performs an operation.
Operation	Operation performed by a user.
Description	Details about an operation.
IP Address	IP address of the host on which the operation is performed.
Account	Account of the user that performs the operation.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download operation logs to a local disk drive in text format.
- Clear logs.

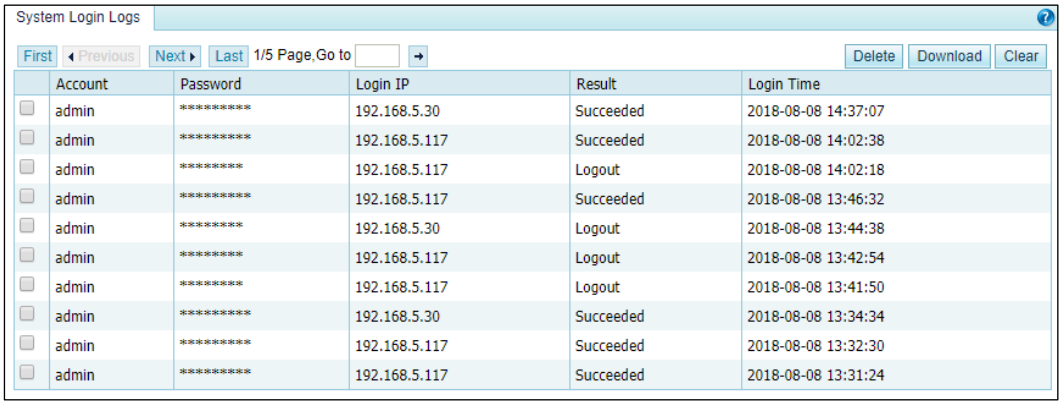
  Click **Clear** and **OK** in the confirmation dialog box to clear all the current operation logs.
- Delete logs.

  Select one or more logs and click **Delete** to delete the selected logs.

7.2.2 System Login Logs

As shown in Figure 7-5, the system login log table displays system login details.

Figure 7-5 System login logs



Account	Password	Login IP	Result	Login Time
admin	**********	192.168.5.30	Succeeded	2018-08-08 14:37:07
admin	**********	192.168.5.117	Succeeded	2018-08-08 14:02:38
admin	*********	192.168.5.117	Logout	2018-08-08 14:02:18
admin	**********	192.168.5.117	Succeeded	2018-08-08 13:46:32
admin	*********	192.168.5.30	Logout	2018-08-08 13:44:38
admin	*********	192.168.5.117	Logout	2018-08-08 13:42:54
admin	*********	192.168.5.117	Logout	2018-08-08 13:41:50
admin	**********	192.168.5.30	Succeeded	2018-08-08 13:34:34
admin	**********	192.168.5.117	Succeeded	2018-08-08 13:32:30
admin	**********	192.168.5.117	Succeeded	2018-08-08 13:31:24

Table 7-3 describes parameters of system login logs.

Table 7-3 Parameters of system login logs

Parameter	Description
Account	User name used by a user for login

Parameter	Description
Password	Password used by a user for login
Local IP	IP address of a login user
Result	Whether the login succeeded or failed
Login Time	Time when an account logs in

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download login logs to a local disk drive in text format.
- Clear logs.

  Click **Clear** and **OK** in the confirmation doalog box to clear all current login logs.
- Delete logs.

  Select one or more logs and click **Delete** to delete the selected logs.

7.2.3 Link Status Logs

As shown in Figure 7-6, the link status log table displays the interface connection status (UP to DOWN or DOWN to UP) of ADS.

Figure 7-6 Link status logs

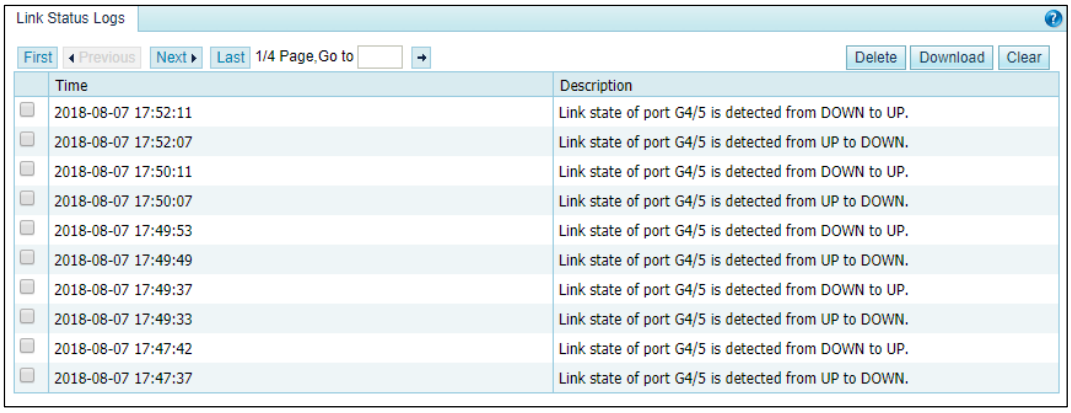


Table 7-4 describes parameters of link status logs.

Table 7-4 Parameters of link status logs

Parameter	Description
Time	Time when the status of an interface changes.
Description	Status change details of an interface.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download link status logs to a local disk drive in text format.
- Clear logs.

  Click **Clear** and **OK** in the confirmation dialog box to clear all current link status logs.
- Delete logs.

  Select one or more logs and click **Delete** to delete the selected logs.

7.2.4 Traffic Diversion Logs

As shown in Figure 7-7, the traffic diversion log table displays the route operations performed by ADS upon receiving alerts from NSFOCUS ADS detection devices, as well as manual diversion routing operations performed on the web-based manager. Logs can be retained for 10 days at most.

Note	Traffic diversion logs can be viewed only in diversion modes.

Figure 7-7 Traffic diversion logs

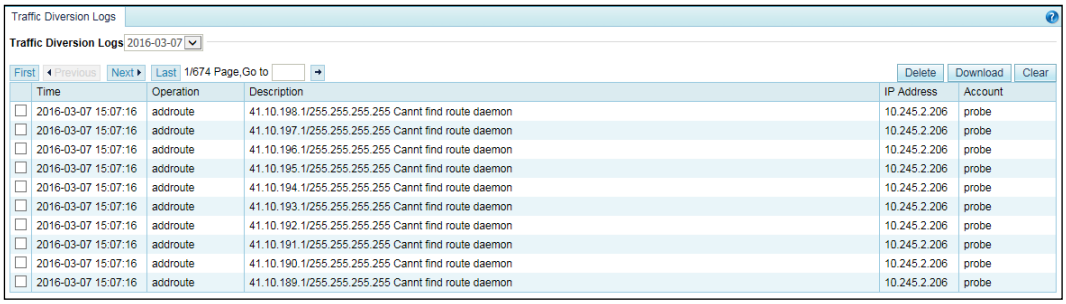


Table 7-5 describes parameters of traffic diversion logs.

Table 7-5 Parameters of traffic diversion logs

Parameter	Description
Time	Time when traffic diversion happens.
Operation	Type of traffic diversion operations.
Description	Destination IP address and of the traffic to be diverted, netmask of the destination IP address, and the diversion destination IP address. If the operation is **Change Status**, changes of the status will also be displayed.
IP Address	IP address of ADS that diverts the traffic or NSFOCUS NTA that detects attack traffic. Both IPv4 and IPv6 addresses are allowed.
Account	User name (for example, **admin**) that performs traffic diversion or device name (for example, **probe**) of NSFOCUS NTA.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download traffic diversion logs to a local disk drive in text format.
- Clear logs.

  Click **Clear** and OK in the confirmation dialog box to clear all current traffic diversion logs.
- Delete logs.

  Select one or more logs and click **Delete** to delete the selected logs.

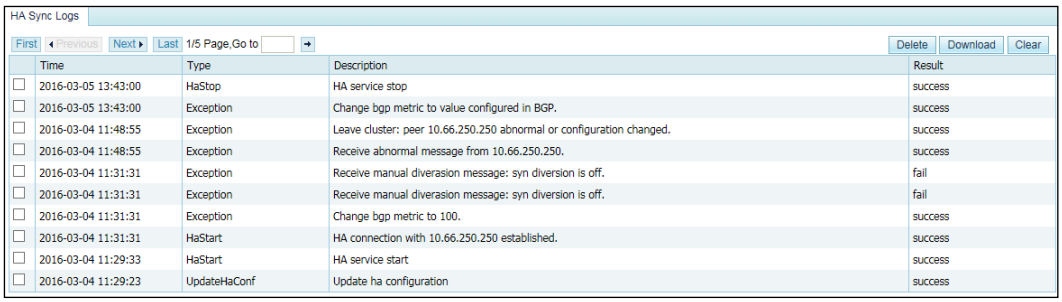
7.2.5 HA Synchronization Logs

Note	Currently, as ADS NX5-10000 lacks support for the HA function, it does not support query of HA synchronization logs.

When the keepalive information, synchronization information (MAC address, diversion information, and protection group information), and engine failure information is synchronized between active and standby ADS devices, the two devices record such operations as HA synchronization logs for statistics and analysis.

Choose **Logs** > **System Logs** > **HA Sync Logs.** The **HA Sync Logs** page appears, as shown in Figure 7-8.

Figure 7-8 HA synchronization logs



Time	Type	Description	Result
2016-03-05 13:43:00	HaStop	HA service stop	success
2016-03-05 13:43:00	Exception	Change bgp metric to value configured in BGP.	success
2016-03-04 11:48:55	Exception	Leave cluster: peer 10.66.250.250 abnormal or configuration changed.	success
2016-03-04 11:48:55	Exception	Receive abnormal message from 10.66.250.250.	success
2016-03-04 11:31:31	Exception	Receive manual diverasion message: syn diversion is off.	fail
2016-03-04 11:31:31	Exception	Receive manual diverasion message: syn diversion is off.	fail
2016-03-04 11:31:31	Exception	Change bgp metric to 100.	success
2016-03-04 11:31:31	HaStart	HA connection with 10.66.250.250 established.	success
2016-03-04 11:29:33	HaStart	HA service start	success
2016-03-04 11:29:23	UpdateHaConf	Update ha configuration	success

Table 7-6 describes parameters of HA synchronization logs.

Table 7-6 Parameters of HA synchronization logs

Parameter	Description
Time	Time when a log is recorded.
Type	What type of information a log records. • **HaStart**: indicates that the log records HA connection establishment. • **Exception**: indicate that the log records exceptions.

Parameter	Description
	• **SyncConf**: indicates that the log records file and heartbeat synchronization.
Description	Log details.
Result	Operation result, which could be **success** or **fail**.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download HA synchronization logs to a local disk drive in text format.
- Clear logs.

  Click **Clear** and **OK** in the confirmation dialog box to clear all current HA synchronization logs.
- Delete logs.

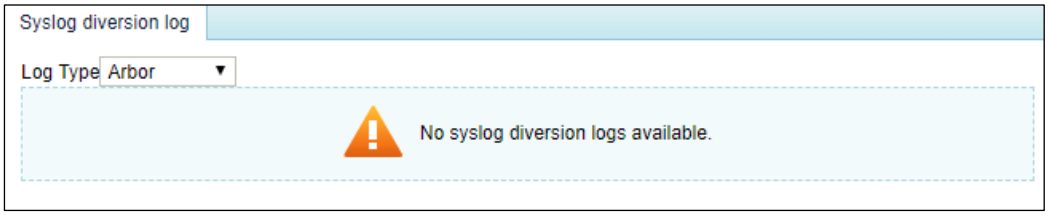
  Select one or more logs and click **Delete** to delete the selected logs.

7.2.6 Syslog Diversion Logs

As shown in 0, the syslog diversion log list displays logs generated during collaboration between NSFOCUS ADS and a third-party device from Genie, Arbor, Samurai, or Kuanguang. Logs can be retained for 10 days at most.

Note	• Syslog diversion logs can be viewed only in diversion mode. • Currently, ADS uses only IPv4 addresses to collaborate with third-party devices in either IPv4 or dual-stack mode.

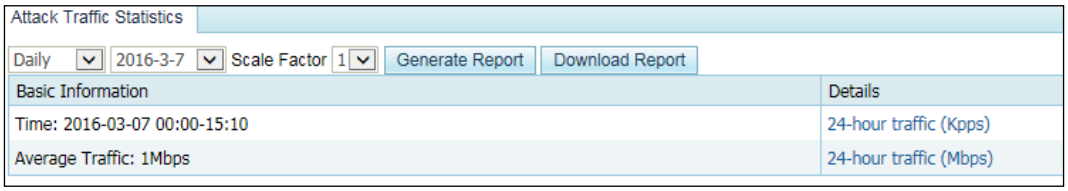
Figure 7-9 Syslog diversion logs



7.3 Log Analysis

As shown in Figure 7-10, you can set query conditions and click **Generate Report** to generate reports in chronological order. ADS supports three types of reports: daily report, weekly report, and monthly report. Note that the scale factor cannot be changed for a daily report. In addition, you can click **Download Report** to download the generated report to a local disk drive.

Figure 7-10 Attack traffic statistics



Daily Attack Traffic Report

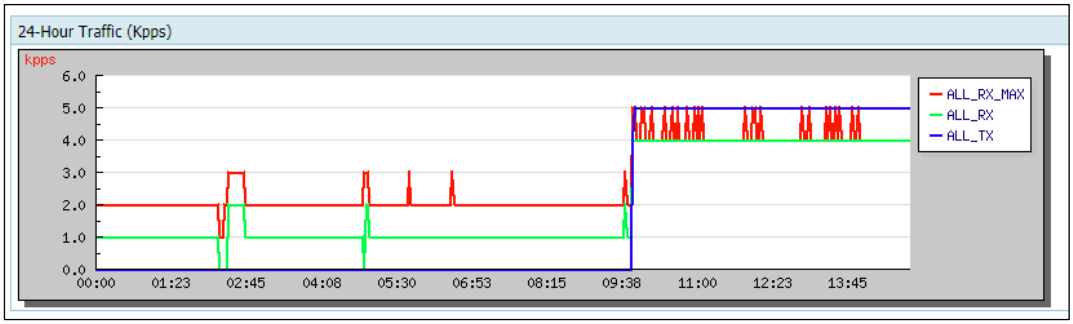
The **Basic Information** column includes statistical time, average incoming traffic, average normal incoming traffic, and average outgoing traffic (unit: Mbps) about attacks on a specific day.

The **Details** column contains the following information:

- 24-hour traffic (kpps)

  As shown in Figure 7-11, incoming/outgoing traffic (unit: kpps) of a specific day is displayed.

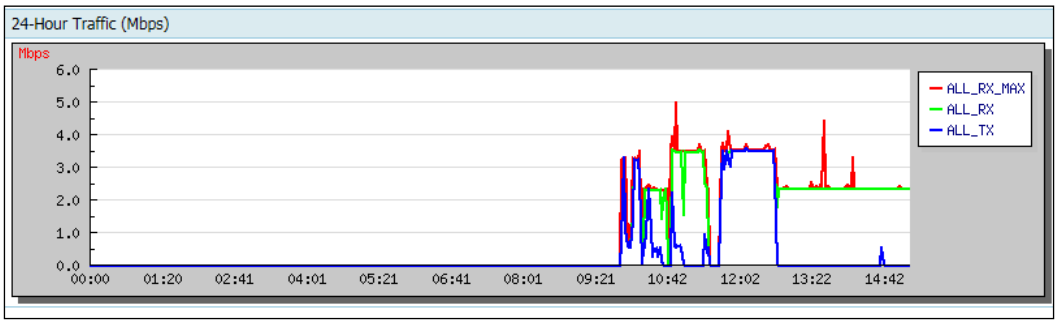
Figure 7-11 24-hour traffic (kpps)



- 24-hour traffic (Mbps)

  As shown in Figure 7-12, incoming/outgoing traffic (unit: Mbps) of a specific day is displayed.

Figure 7-12 24-hour traffic (Mbps)



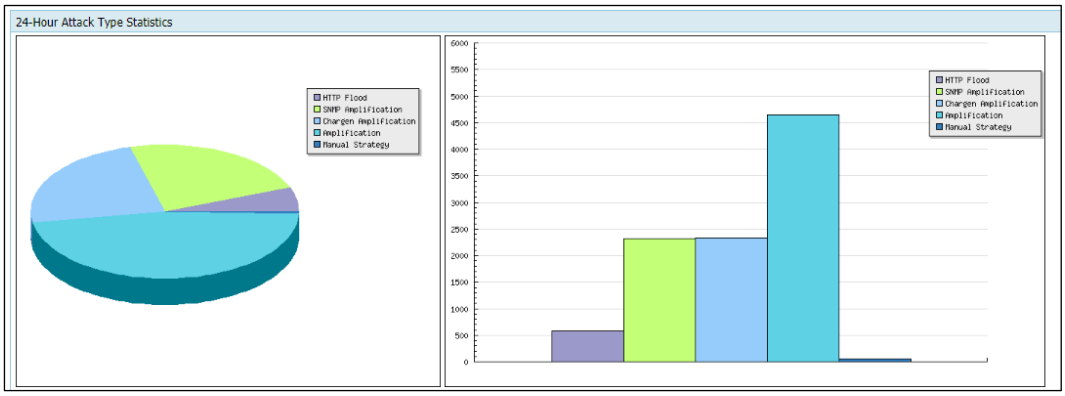
- 24-hour attack type statistics

  As shown in Figure 7-13, types of attacks on a specific day are displayed in a pie chart and a bar chart.

  – Pie chart: Proportion of each type of attacks on the current day.

  – Bar chart: Number of each type of attack logs on the current day.

Figure 7-13 24-hour attack type statistics



- 24-hour attacked IP statistics

  As shown in Figure 7-14, attacked IP addresses and attack traffic on a specific day are displayed in the list.

Figure 7-14 24-hour attacked IP statistics

24-Hour Attacked IP Statistics(Top5)

Attacked IP	SYN Flood	ACK Flood	ICMP Flood	UDP Flood	Connection Flood	Stream Flood
40.40.40.1	0	0	0	0	8	0
0040:0040:0040:0001:0000:0000:0000:0001	0	0	0	0	16	0

Weekly Attack Traffic Report

A weekly report is similar to a daily report, except that the statistical period is one week.

Monthly Attack Traffic Report

A monthly report is similar to a daily report, except that the statistical period is one month.

Note	The system can generate data only when it is running.

8 Advanced Applications

This chapter dwells upon two advanced functions of the system, containing the following sections:

Section	Description
Packet Capture Management	Describes a tool usually used to analyze transmitted packets in the network.
Pattern Matching Rules	Describes a protection rule used to filter packets based on signature patterns.
Collaboration with NTI	Describes how to configure collaboration between ADS and NTI.

8.1 Packet Capture Management

Packet capture is the act of capturing network packets that meet the specified conditions, so as to provide evidence for electronic forensics. ADS supports manual packet capture and automatic packet capture.

8.1.1 Configuring Manual Packet Capture

Manual packet capture configuration varies with ADS devices.

- For devices with a memory of smaller than 8 GB, such as ADS NX3-200E/600E, ADS NX3-2020/2010, ADS NX5-4020, and ADS NX5-6025:
  - A maximum of six packet capture tasks can be configured and saved.
  - A maximum of two packet capture tasks can be enabled at the same time.
  - A maximum of five packet capture files can be saved in total.
- For devices with a memory of greater than 8 GB, such as ADS NX3-800E/2020E, ADS NX5-4020E/6025E, ADS NX5-8000 and ADS NX5-10000:
  - A maximum of six packet capture tasks can be configured and saved.
  - A maximum of three packet capture tasks can be enabled at the same time.
  - A maximum of 10 packet capture files can be saved in total.

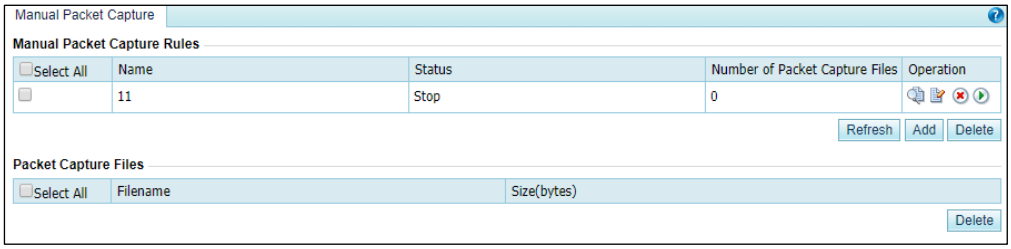
8.1.1.1 Creating a Manual Packet Capture Task

To configure a manual packet capture task, perform the following steps:

Step 1 Choose **Advanced** > **Packet Capture** > **Manual Packet Capture**.

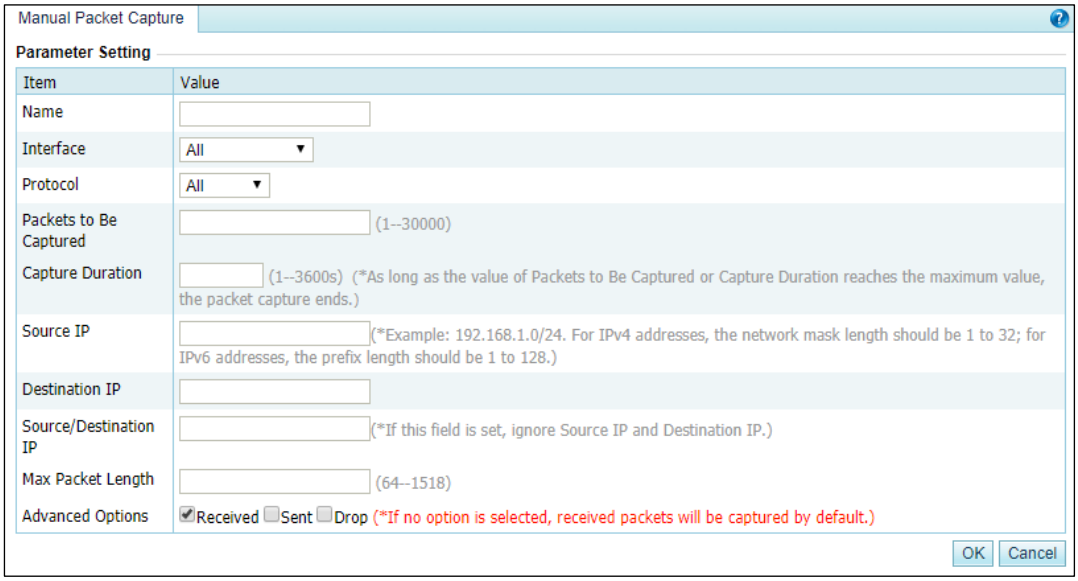
In the upper part of the **Manual Packet Capture** page, the status of packet capture tasks is displayed. For an ongoing packet capture task, **Status** is displayed as **Running**. Otherwise, **Status** is displayed as **Stop**. In the lower part of the page, packet capture files are listed for completed packet capture tasks.

Figure 8-1 Manual Packet Capture page



Step 2 Click **Add** to create a manual packet capture rule.

Figure 8-2 Creating a manual packet capture rule



Step 3 Configure parameters.

Table 8-1 describes parameters for creating a manual packet capture rule.

Table 8-1 Parameters for creating a manual packet capture rule

Parameter	Description
Name	Name of the packet capture rule.
Interface	Interface on which packets are captured for this task. **All** indicates that packets are captured on all interfaces.
Protocol	Protocol used by packets to be captured. Values can be **All**, **TCP**, **UDP**, and **ICMP**, **ICMPV6**, and **Custom**, with **All** as the default value. When **Protocol** is set to **Custom**, you can set a protocol port number, which must

Parameter	Description
	be in the range of 0–255.
Packets to Be Captured	Number of packets to be captured. The value ranges from 1 to 30,000.
Capture Duration	Specifies how long a capture task can last at most. The value range is 1–3600 in seconds. The system stops capturing packets when either the setting of **Packets to Be Captured** or that of **Capture Duration** is met.
Source IP	Source IP address of this task. This parameter is optional. If the source IP address is empty, it indicates that packets from any IP address can be captured. Note The source IP address can be an IPv4 or IPv6 address.
Destination IP	Destination IP address of this task. This parameter is optional. If the destination IP address is empty, it indicates that packets destined to any IP address can be captured. Note The destination IP address can be an IPv4 or IPv6 address.
Source/Destination IP	Source or destination IP address of the task. This parameter is optional. If you set this parameter, ignore **Source IP** and **Destination IP**. Note Both IPv4 and IPv6 addresses are allowed.
Source Port	Source port of this task. This parameter is optional. If the source port is empty, it indicates that packets from any port can be captured.
Destination Port	Destination port of this task. This parameter is optional. If the destination port is empty, it indicates that packets to any port can be captured.
Source/Destination Port	Source or destination port of the task. This parameter is optional. If this parameter is specified, the system ignores both **Source Port** and **Destination Port**.
Max Packet Length	Maximum length of the packet to be captured. The value ranges from 64 to 1518.
Advanced Options	This parameter is optional. Options are as follows: • **Received**: indicates that ADS captures received packets. • **Sent**: indicates that ADS captures packets that are sent. • **Drop**: indicates that ADS captures dropped packets. If none is selected, received packets will be captured by default.

Step 4 Click **OK**.

The new manual packet task starts only after you click **Start**.

----End

8.1.1.2 Starting a Manual Packet Capture Task

In the **Manual Packet Capture Rules** area shown in Figure 8-1, click in the **Operation** column of a manual packet capture task to start this task.

When the packet capture task is in progress, **Status** is displayed as **Running**, and the forensics file is displayed on the file list. When the packet capture task is completed, **Status** is displayed as **Stop**.

8.1.1.3 Stopping a Manual Packet Capture Task

In the **Manual Packet Capture Rules** area shown in Figure 8-1, click in the **Operation** column of a manual packet capture task to stop this task.

After the packet capture task is stopped, **Status** is displayed as **Stop**.

8.1.1.4 Viewing a Manual Packet Capture Task

In the **Manual Packet Capture Rules** area shown in Figure 8-1, click in the **Operation** column of a manual packet capture task to view its configuration information.

Click **Refresh** to view the current status of manual packet capture tasks.

8.1.1.5 Editing a Manual Packet Capture Task

To edit a manual packet capture task, perform the following steps:

Step 1 In the **Manual Packet Capture Rules** area shown in Figure 8-1, click in the **Operation** column of a manual packet capture task.

Step 2 Edit parameters, click **OK** to save the settings, and return to the **Manual Packet Capture** page.

----End

8.1.1.6 Deleting a Manual Packet Capture Task

You can delete manual packet capture tasks one by one or in batches as follows:

- Method 1: In the **Manual Packet Capture Rules** area shown in Figure 8-1, click in the **Operation** column of a manual packet capture task and click **OK** in the confirmation dialog box to delete this task.
- Method 2: In the **Manual Packet Capture Rules** area shown in Figure 8-1, select one or more manual packet capture tasks (or select the **Select All** check box to select all manual packet capture tasks), click **Delete** in the lower-right corner of the area, and click **OK** in the confirmation dialog box to delete the selected tasks.

Note	Ongoing packet capture tasks cannot be deleted.

8.1.1.7 Downloading a Manual Packet Capture File

After a manual packet capture task is ended, a packet capture file is generated and added to the file list, as shown in the **Packet Capture Files** area shown in Figure 8-1. You can click the name of a packet capture file to download it or view its details.

8.1.1.8 Deleting a Packet Capture File

Step 1 In the **Manual Packet Capture Rules** area shown in Figure 8-1, select one or more packet capture files (or select the **Select All** check box to select all files) and click **Delete**.

Step 2 Click **OK** in the confirmation dialog box.

Note	Packet capture files of ongoing tasks cannot be deleted.

----End

8.1.2 Creating Automatic Packet Capture

Automatic packet capture configuration varies with ADS devices.

- For devices with a memory of smaller than 8 GB, such as ADS NX3-200E/600E, ADS NX3-2020/2010, ADS NX5-4020, and ADS NX5-6025:
  - A maximum of two packet capture tasks can be configured and saved.
  - A maximum of two packet capture tasks can be enabled at the same time.
  - A maximum of 10 packet capture files can be saved in total (at most 10 packet capture files for each task).
- For devices with a memory of greater than 8 GB, such as ADS NX3-800E, ADS NX5-6025E, ADS NX5-8000 and ADS NX5-10000:
  - A maximum of three packet capture tasks can be configured and saved.
  - A maximum of three packet capture tasks can be enabled at the same time.
  - A maximum of 10 packet capture files can be saved in total (at most 10 packet capture files for each task).

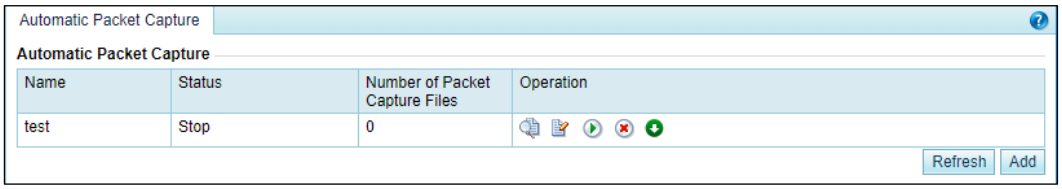
8.1.2.1 Creating an Automatic Packet Capture Task

To configure an automatic packet capture task, perform the following steps:

Step 1 Choose **Advanced** > **Packet Capture** > **Automatic Packet Capture**.

The status of packet capture tasks is displayed. For an ongoing packet capture task, **Status** is displayed as **Running**. Otherwise, **Status** is displayed as **Stop**.

Figure 8-3 Automatic Packet Capture page



Step 2 Click **Add** to create an automatic packet capture rule.

Step 3 Configure parameters for an automatic packet capture rule.

Figure 8-4 Configuring an automatic packet capture rule

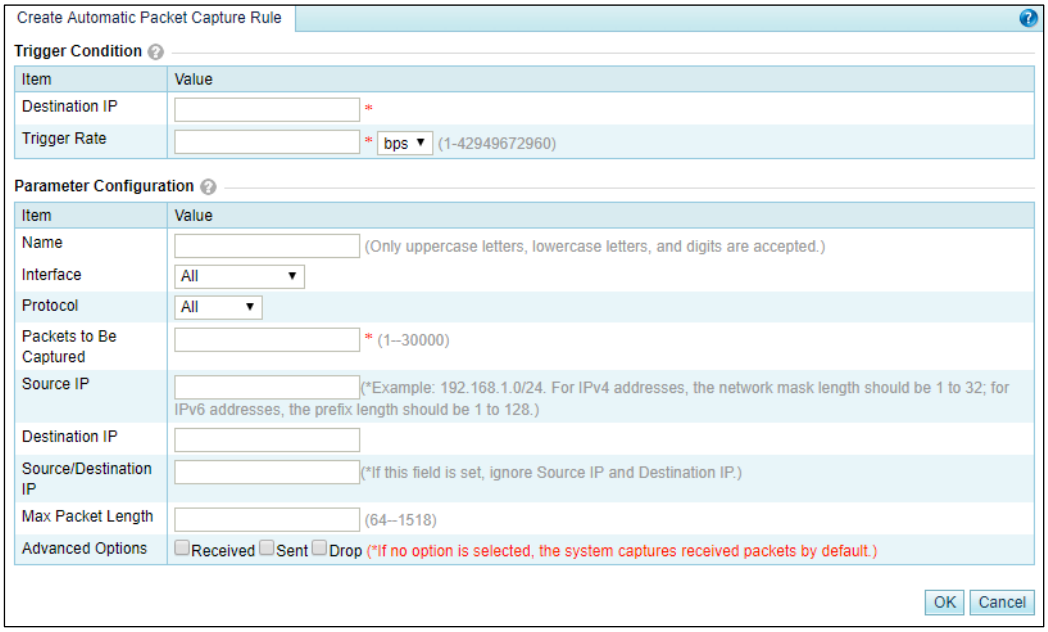


Table 8-2 describes some parameters for automatic packet capture. For details, see Table 8-1.

Table 8-2 Automatic packet capture parameters

Parameter	Description
Destination IP	Specifies the destination IP address for this packet capture task.
Trigger Rate	Specifies the number of packets received by the destination IP address per second that will trigger automatic packet capture. The value range is 1–4294967295 pps or 1–42949672960 bps.

Step 4 Click **OK** to complete the configuration.

The automatic packet capture task starts only when specified conditions are triggered.

----End

8.1.2.2 Managing an Automatic Packet Capture Task

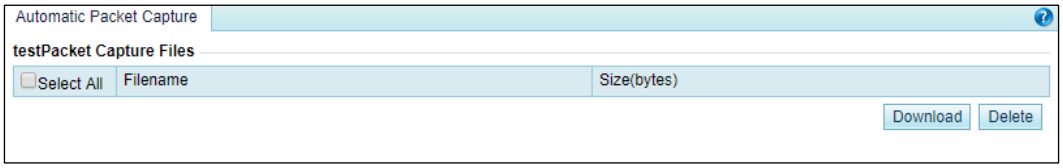
After automatic packet capture tasks are configured, you can manually start or stop them. In addition, you can refresh, view, edit and delete such tasks in the same way as manual packet capture tasks.

Note	When the number of automatic packet capture files reaches the upper limit, after you start a new automatic packet capture task, the system will automatically clear the existing automatic packet capture files.

8.1.2.3 Managing Automatic Packet Capture Files

In Figure 8-3, click in the **Operation** column of an automatic packet capture task to open the packet capture file list, as shown in Figure 8-5.

Figure 8-5 Automatic packet capture file list



You can download, view, and delete automatic packet capture files in the same way as manual packet capture files.

8.2 Pattern Matching Rules

To defend against unknown attacks, ADS can adopt the pattern matching function to filter out packets with certain signatures based on signature matching. The key of the process is to find typical signatures of packets of unknown attacks.

This section covers the following topics:

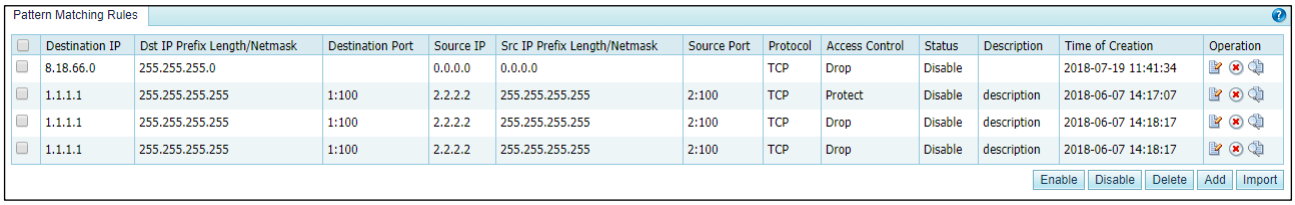
- Creating a Pattern Matching Rule
- Creating Pattern Matching Rules in Batches
- Enabling and Disabling Pattern Matching Rules
- Modifying Pattern Matching Rules
- Deleting Pattern Matching Rules
- Viewing Pattern Matching Rules

8.2.1 Creating a Pattern Matching Rule

To create a pattern matching rule, perform the following steps:

Step 1 Choose **Advanced** > **Pattern Matching** > **Pattern Matching Rules**.

Figure 8-6 **Pattern Matching Rules** page



Destination IP	Dst IP Prefix Length/Netmask	Destination Port	Source IP	Src IP Prefix Length/Netmask	Source Port	Protocol	Access Control	Status	Description	Time of Creation	Operation
8.18.66.0	255.255.255.0		0.0.0.0	0.0.0.0		TCP	Drop	Disable		2018-07-19 11:41:34	
1.1.1.1	255.255.255.255	1:100	2.2.2.2	255.255.255.255	2:100	TCP	Protect	Disable	description	2018-06-07 14:17:07	
1.1.1.1	255.255.255.255	1:100	2.2.2.2	255.255.255.255	2:100	TCP	Drop	Disable	description	2018-06-07 14:18:17	
1.1.1.1	255.255.255.255	1:100	2.2.2.2	255.255.255.255	2:100	TCP	Drop	Disable	description	2018-06-07 14:18:17	

Step 2 Click **Add**.

Figure 8-7 Creating a pattern matching rule (TCP)

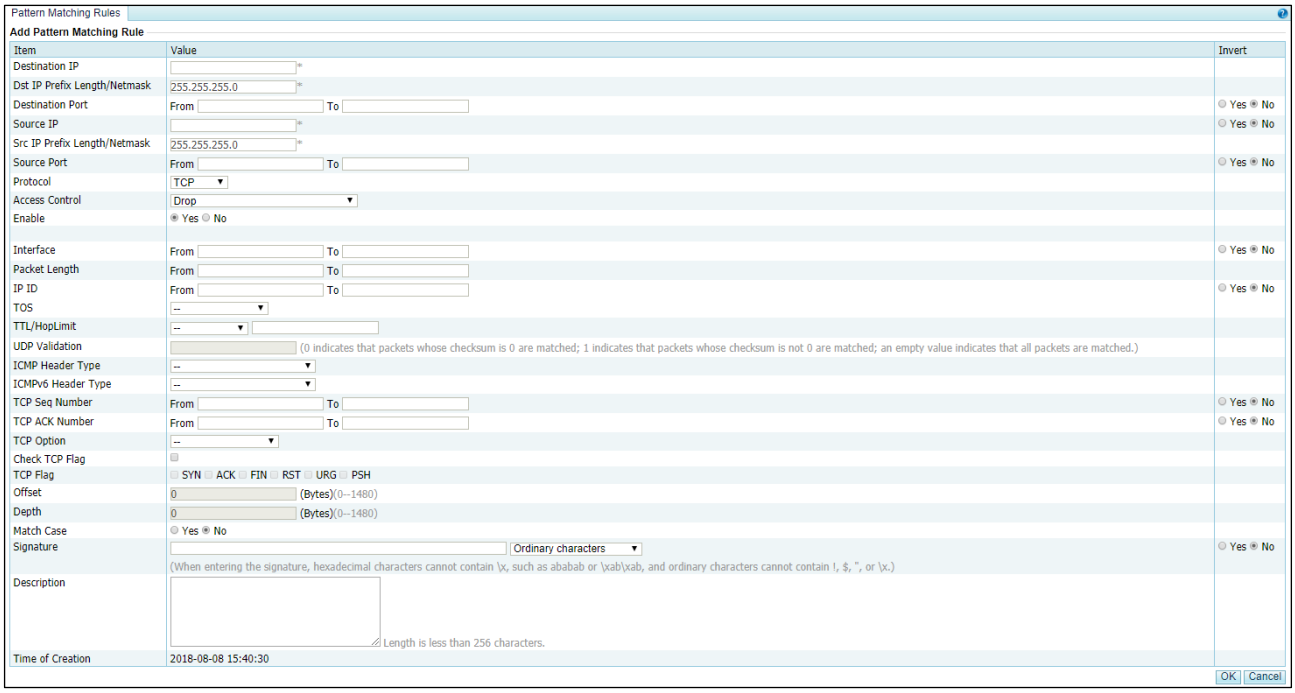


Table 8-3 describes parameters for creating a pattern matching rule

Table 8-3 Parameters of creating a pattern matching rule

Parameter	Description
Destination IP	Destination IP address of packets matching this rule. You can type an IPv4 or IPv6 address according to the actual network deployment.
Dst IP Prefix Length/Netmask	Prefix length (for IPv6 protocol) or netmask (for IPv4 protocol) of the destination IP address.
Destination Port	Destination port range. This is required only when **Protocol** is set to **TCP** or **UDP**. For example, 1049–5094 indicates packets with the destination port in the range from 1049 to 5094. If only **1049** is filled, it indicates that only packets with the destination port 1049 will be deemed to match this rule.
Source IP	Source IP address of packets to be matched with this rule. You can type an IPv4 or IPv6 address according to the actual network deployment.

Parameter	Description
Src IP Prefix Length/Netmask	Prefix length (for IPv6 protocol) or netmask (for IPv4 protocol) of the source IP address.
Source Port	Source port range. This is required only when **Protocol** is set to **TCP** or **UDP**. For example, 1049–5094 indicates packets with the source port in the range from 1049 to 5094. If only **1049** is filled, it indicates that only packets with the source port 1049 will be deemed to match this rule.
Protocol	Values are **TCP**, **UDP**, **ICMP**, and **ICMPv6**.
Access Control	Action performed by ADS on packets matching this rule. • **Protect** indicates that ADS allows packets matching this rule to pass through. • **Drop** indicates that ADS drops packets matching this rule. • **Drop and add to blacklist** indicates that ADS drops packets matching this rule and adds their source IP addresses to the blacklist. • **Drop and disconnect** indicates that ADS drops packets matching this rule and sends an RST packet to the server to interrupt the connections. • **Drop,add to blacklist,and disconnect** indicates that ADS drops packets matching this rule, adds their source IP addresses to the blacklist, and sends an RST packets to the server to interrupt connections. • **Rate-limiting** indicates that the maximum number of packets matching this rule that are allowed to pass through per second should not exceed the threshold specified here. Excessive packets will be dropped. The value range is 1–6000000 pps, with **4000** as the default value. Note If **Access Control** is set to **Drop and add to blacklist** or **Drop**,**add to blacklist,and disconnect**, you also need to enable the blacklist function. Otherwise, the blacklist is invalid. For details, see section 5.2.9 Blacklist.
Enable	**Controls whether to enable this rule. The value Yes** indicates this rule is enabled.
Interface	Range of the interfaces (working interfaces on the front panel of ADS) through which packets are transmitted.
Packet Length	Length range of packets to be matched with this rule.
IP ID	IP identification in an IPv4 header. Either a specific value or a value range is allowed. The value range is 0–65536.
TOS	Service type. Values include **Min latency**, **Max throughput**, **Highest reliability**, **Min cost**, and **Common service**.
TTL/HopLimit	Matching method of the TTL value, which can be **Greater than**, **Smaller than**, or **Equal to**.
UDP Validation	Checksum of UDP packets. This is available only when **Protocol** is set to **UDP**.
ICMP Header Type	Type of the ICMP packet header. This is available only when **Protocol** is set to **ICMP**.
ICMPv6 Header Type	Type of the ICMPv6 packet header. This is available only when **Protocol** is set to **ICMPv6**.
TCP Seq Number	TCP sequence number in a TCP header. Either a specific value or a value range is allowed. The value range is 0–4294967295.

Parameter	Description
TCP ACK Number	TCP acknowledgement number in a TCP header. Either a specific value or a value range is allowed. The value range is 0–4294967295.
TCP Option	Three options are available: **Max Packet Length**, **Window Scale**, and **Timestamp**. This is available only when **Protocol** is set to **TCP**.
Check TCP Flag	Controls whether to check TCP flags. Selection of this check box indicates that ADS will check TCP flags in packets.
TCP Flag	Flag bit of the TCP packet header, which can be **SYN**, **ACK**, **FIN**, **RST**, **URG**, and **PSH**. This is available only when **Protocol** is set to **TCP**.
Offset	Number of bytes from the start of the packet body to a given position where the search starts. Its value should be smaller than the total length of the packet body. For TCP packets, the packet body includes the TCP header. For UDP packets, the packet body refers to the payload.
Depth	Maximum number of bytes allowed for searching. The depth is equal to the total length of packet body minus the offset.
Match Case	**Controls whether signature characters are case sensitive.** Only English letters are under this restriction.
Signature	Signature characters to be searched for. Special and unprintable characters need to be translated into hex format (for example, translate carriage return and line feed into \x0d\x0a). You can also leave this field empty. In this case, **Offset** and **Depth** are both **0**, which cannot be changed. Requirements for typing ordinary characters are as follows: • Special characters (! $ ") and spaces, and GBK encoded characters (Chinese) are not supported. • Characters preceded with \\x will be interpreted as hexadecimal characters. As \x is used to differentiate hexadecimal characters from ordinary characters, characters preceded with \x are not allowed if **Ordinary characters** is selected. Requirements for typing hexadecimal characters are as follows: • Hexadecimal characters with or without \x, such as \x67\x1f and 671f, are supported. • Only single-byte characters, like \x67\x1f, are allowed. • Double-byte characters, like \x671f\x1a, are not allowed. • Characters like \x6\x1a are not allowed. • Spaces are not allowed. You can select **Ordinary characters** or **Hexadecimal characters** for **Signature**. You are advised to copy the signature characters from the packet capture file and paste them to the **Signature** text box. If certain characters are not required, delete them. The following shows how to copy signature characters from Wireshark: Use Wireshark to open a captured packet, right-click the target signature character line, and choose **Copy** > **Bytes** > **Hex Stream** to copy the selected hexadecimal character line.
Description	Brief description of this rule.

Parameter	Description
Time of Creation	Time when the rule is created, which is automatically generated by the system.

Note	The **Invert** column is available for some parameters. Suppose that you specify **202.114.1.242** as the source IP address and **255.255.255.0** as the netmask. If you select **Yes** for **Invert**, packets with a source IP address beyond the range 202.114.1.1–202.114.1.254 are deemed to match the configured rule.

Step 3 Set parameters and click **OK** to save the settings.

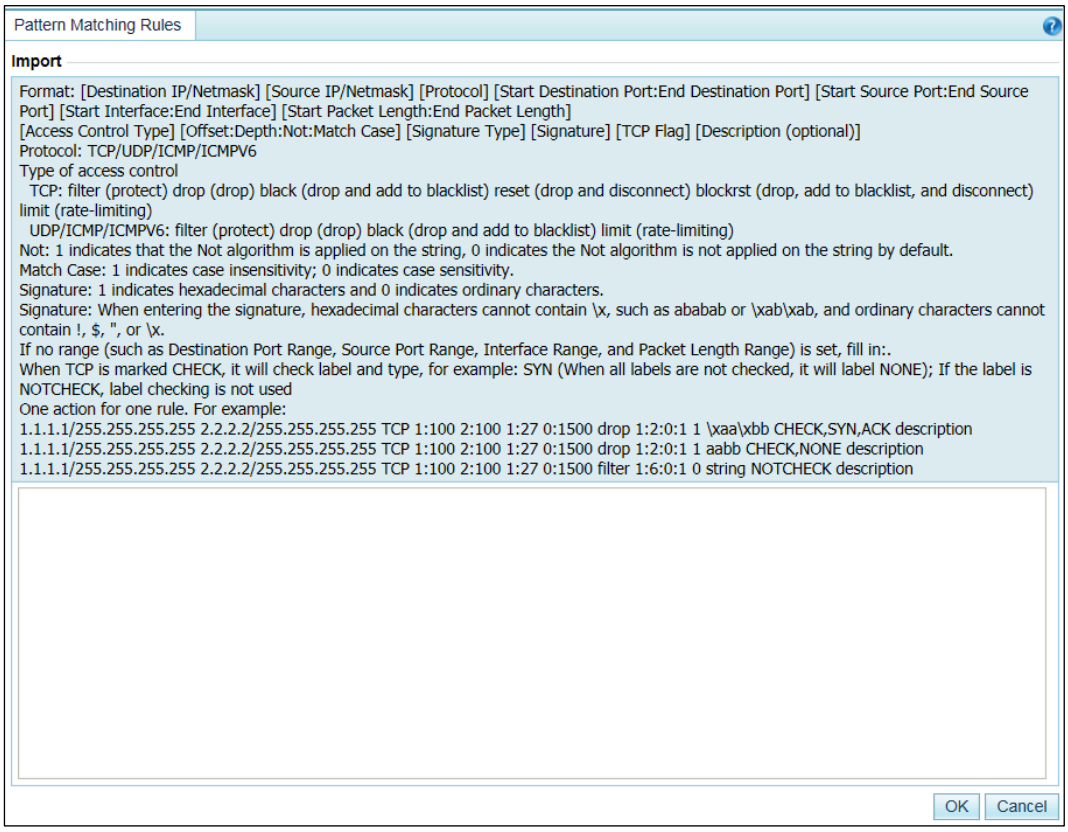
----End

8.2.2 Creating Pattern Matching Rules in Batches

You can create pattern matching rules in batches on ADS by performing the following steps:

Step 1 On the **Pattern Matching Rules** page shown in Figure 8-6, click **Import** below the table to create pattern matching rules in batches.

Figure 8-8 Creating pattern matching rules in batches



Step 2 Type pattern matching rules as prompted.

Pay attention to the following format specifications:

- Parameters of each pattern matching rule are separated by spaces.
- Each rule should take up one line.

Step 3 After the parameter configuration is completed, click **OK** to save the settings.

----End

8.2.3 Enabling and Disabling Pattern Matching Rules

On ADS, only enabled pattern matching rules are valid, while disabled ones are invalid. Enabling and disabling pattern matching rules can free you from frequent deletion and addition operations. If some pattern matching rules are not required currently, you can disable them.

Enabling Pattern Matching Rules

Enable pattern matching rules that are disabled.

On the **Pattern Matching Rules** page shown in Figure 8-6, select one or more pattern matching rules (or select the **Select All** check box to select all rules), click **Enable** below the table, and then click **OK** in the confirmation dialog box to enable the selected rules.

Disabling Pattern Matching Rules

Disable pattern matching rules that are enabled.

On the **Pattern Matching Rules** page shown in Figure 8-6, select one or more pattern matching rules (or select the **Select All** check box to select all rules), click **Disable** below the table, and then click **OK** in the confirmation dialog box to disable the selected rules.

8.2.4 Modifying Pattern Matching Rules

After configuring pattern matching rules, you can edit rule parameters by performing the following steps:

Step 1 On the **Pattern Matching Rules** page shown in Figure 8-6, click in the **Operation** column to edit parameters of a rule, as shown in Figure 8-7.

Step 2 Click **OK** to save the settings and return to the **Pattern Matching Rules** page.

----End

8.2.5 Deleting Pattern Matching Rules

You can delete one pattern matching rule or multiple rules in batches on ADS in one of the following ways:

- On the **Pattern Matching Rules** page shown in Figure 8-6, click in the **Operation** column and then click **OK** in the confirmation dialog box to delete a rule.
- On the **Pattern Matching Rules** page shown in Figure 8-6, select one or more pattern matching rules (or select the **Select All** check box to select all rules on the list) to be deleted, click **Delete** below the table, and then click **OK** in the confirmation dialog box to delete the selected rules.

8.2.6 Viewing Pattern Matching Rules

On the **Pattern Matching Rules** page shown in Figure 8-6, click in the **Operation** column of a pattern matching rule to view its information.

After viewing rules, click **Back** to return to the **Pattern Matching Rules** page.

8.3 Collaboration with NTI

Note	ADS NX5-10000 does not support collaboration with NTI.

ADS can collaborate with NTI. Specifically, ADS uploads blacklisted source IP addresses to NTI, which sends the data to ADS. For high-risk IP addresses, ADS automatically lists them on the blacklist and blocks packets from these addresses.

To use this function, you need to buy an additional license. For details, contact NSFOCUS technical support.

Choose **Advanced** > **Advanced Protection** > **NTI**. The **NTI** page appears, as shown in Figure 8-9.

Figure 8-9 NTI page

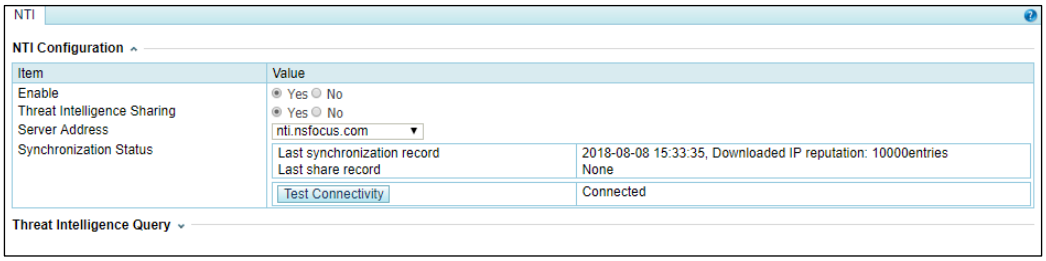


Table 8-4 describes NTI-related parameters.

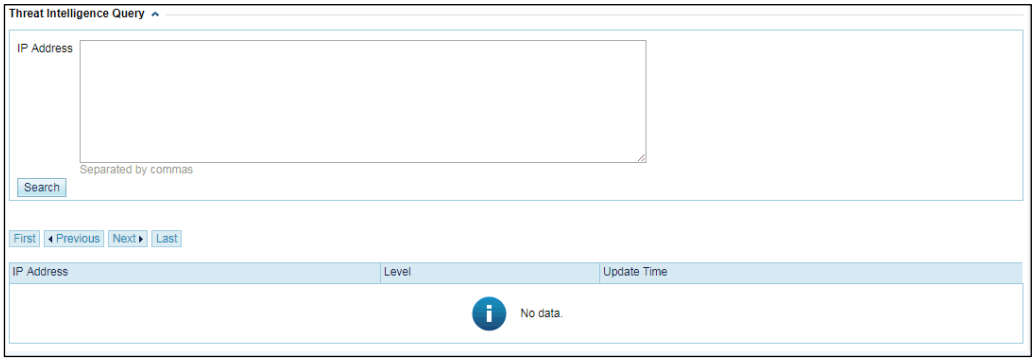
Table 8-4 NTI-related parameters

Parameter	Description
Enable	Controls whether to enable collaboration with NTI. After this function is enabled, ADS immediately downloads data from NTI and refreshes the current blacklist. For high-risk IP addresses, ADS will block packets from them.
Threat Intelligence Sharing	Controls whether to share threat intelligence with NTI. After this function is enabled, ADS reports the discovered high-risk IP addresses to NTI. If you need to enables this function, you are advised to enable the blacklist function

Parameter	Description
	at the same time. Only in this way can ADS automatically upload the local blacklisted source IP addresses to NTI.
Server Address	Specifies the URL of NSFOCUS's threat intelligence server. • For use on the Chinese mainland, choose **nti.nsfocus.com**. • For use in other countries and regions, choose **nti.nsfocusglobal.com**. ADS must be connected to the Internet before collaborating with NTI.
Synchronization Status	• **Last synchronization record**: provides information about the last synchronization from NTI. This information is automatically updated on a daily basis. • **Last share record**: provides information about the last upload of data to NTI. This information is automatically updated on an hourly basis.
Test Connectivity	A button for you to test whether ADS is properly connected to NTI. After you click this button, if **Connected** is displayed, ADS can properly communicate with NTI; if another word is displayed, you must check the network status to ensure the proper communication between ADS and NTI.

You can also query the threat intelligence in NTI from ADS. In the area shown in Figure 8-10, type one or more IP addresses separated by commas (;), and then click **Search** to check whether specific IP addresses exist in NTI. The matched IP addresses are displayed in the lower part of the page together with the credit level and update time.

Figure 8-10 Threat Intelligence Query area



9 Operation and Maintenance

This chapter contains the following sections:

Section	Description
Device Protection Status	Describes how to check the trust status of source IP addresses and the protection status of destination IP addresses.
Network Diagnosis	Describes how to diagnose network faults.

9.1 Device Protection Status

This section covers the following:

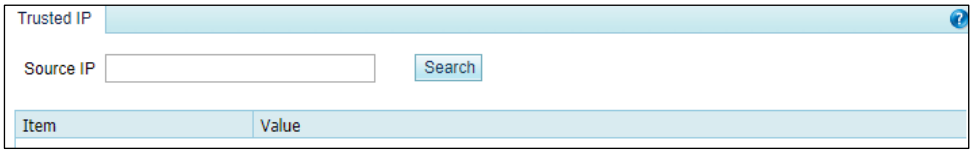
- Device Protection Status
- Network Diagnosis

9.1.1 Checking the Trust Status

To check the trust status of source IP addresses, perform the following steps:

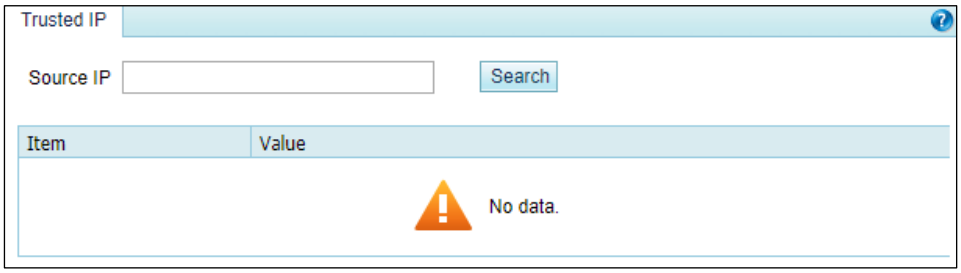
Step 1 Choose **O&M** > **Device Protection Status** > **Trusted IP**.

Figure 9-1 Trusted IP page



Step 2 Type a source IP address and click **Search**. Then the trust information of this address is displayed, such as the trust level, remaining time of the current trust status, and trust reason.

Figure 9-2 Viewing the trust information of a source IP address



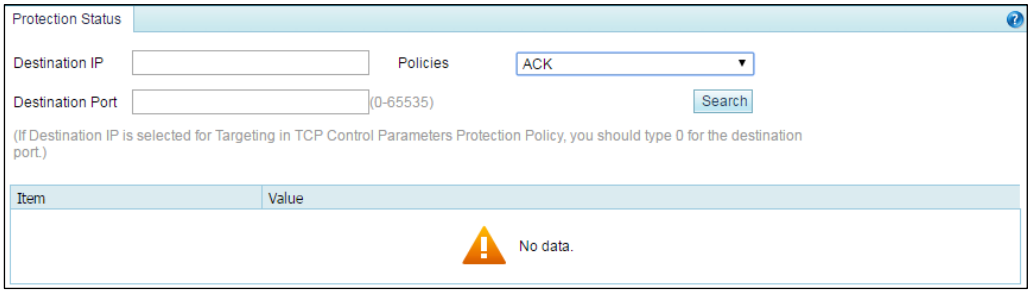
----End

9.1.2 Checking the Protection Status

To check the protection status of a destination IP address for which traffic is being diverted for cleaning, perform the following steps:

Step 1 Choose **O&M** > **Device Protection Status** > **Protection Status**.

Figure 9-3 Protection Status page



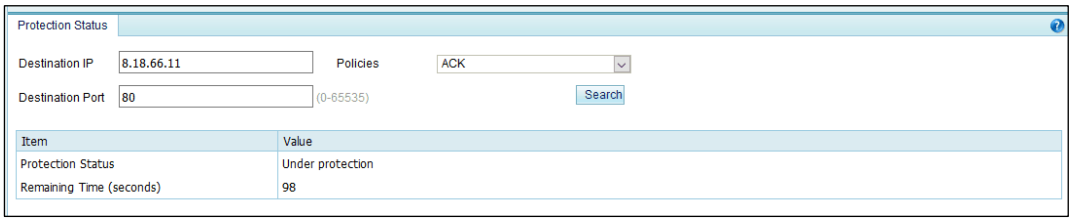
Step 2 Configure query parameters.

Table 9-1 Parameters for querying the protection status of a destination IP address

Parameter	Description
Destination IP	Destination IP address to be queried. You can type an IPv4 or IPv6 address according to the actual network deployment scenario.
Policies	Protection policies applied to this destination IP address.
Destination Port	Destination port. This is required only when **Protocol** is set to other protocols than **UDP** or **ICMP**.

Step 3 Click **Search** to query the protection status of this IP address and the remaining time of the protection status.

Figure 9-4 Viewing the protection status of a destination IP address



----End

9.2 Network Diagnosis

When the system fails, you can troubleshoot it and locate the fault with the following network diagnosis tools available on ADS:

- Ping
- Port Check
- Tcpdump

9.2.1 Ping

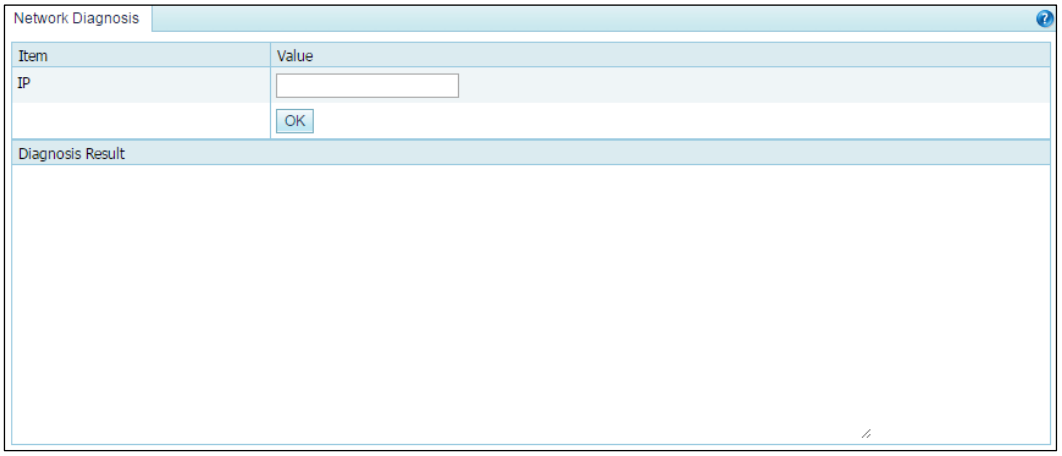
Ping is used to check whether a host is alive or connects to the network.

To use this function, perform the following steps:

Step 1 Choose **O&M** > **Network Diagnosis** > **Ping**.

The default diagnosis tool is ping, as shown in Figure 9-5.

Figure 9-5 Network diagnosis – ping



Step 2 Type an IP address and click **OK**.

The ping result will then be displayed in the text box below.

----End

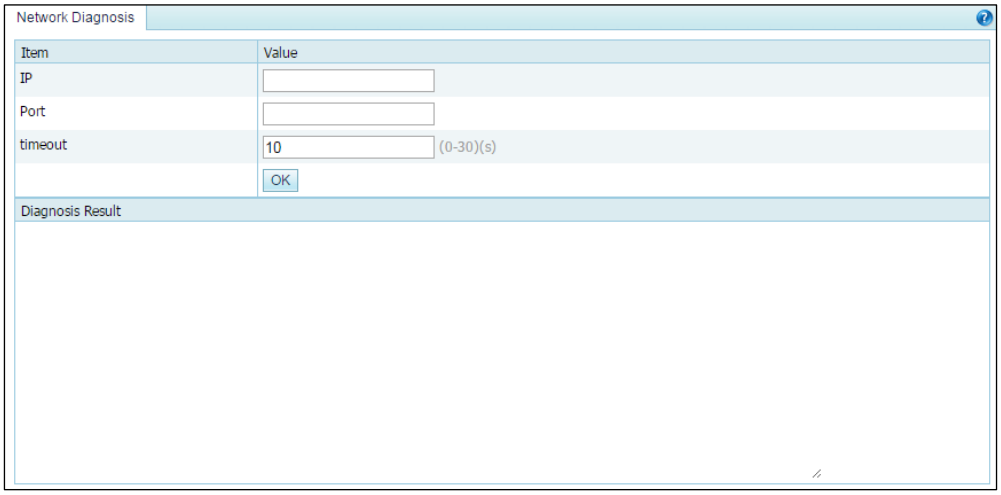
9.2.2 Port Check

When ADS collaborates with other devices or sends data to other devices, you can check whether the peer port is reachable, so as to verify whether a firewall is configured or whether the corresponding service is disabled on the peer device.

To use this function, perform the following steps:

Step 1 Choose **O&M** > **Network Diagnosis** > **Port Check**.

Figure 9-6 Network diagnosis – port check



Step 2 Configure port check parameters.

Table 9-2 Port check parameters

Parameter	Description
IP	Peer IP address to be checked.
Port	Peer port to be checked.
Timeout	Timeout of the port check, which can be 0 to 30 seconds.

Step 3 Click **OK**.

The port check result will then be displayed in the text box below.

----End

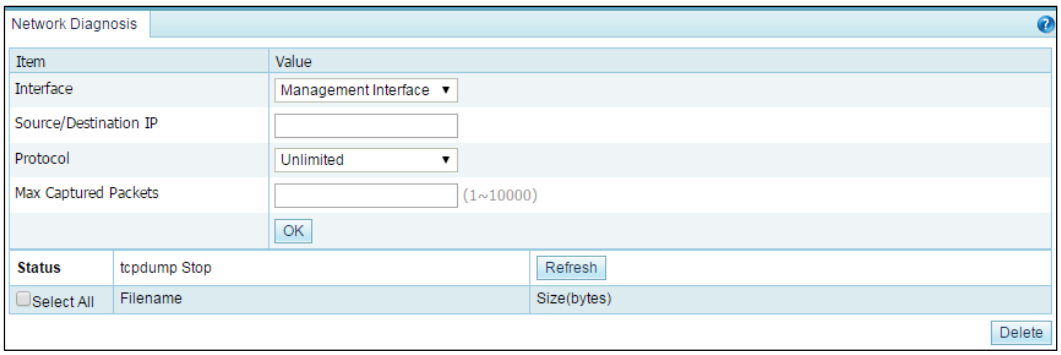
9.2.3 Tcpdump

Tcpdump is used to intercept and analyze packets being transmitted or received over a network as defined by a user. The user can check the status of and troubleshoot network interface cards (NICs) based on such analysis.

To use this function, perform the following steps:

Step 1 Choose **O&M** > **Network Diagnosis** > **Tcpdump**.

Figure 9-7 Network diagnosis – tcpdump



Step 2 Configure tcpdump parameters.

Table 9-3 Tcpdump parameters

Parameter	Description
Interface	Specifies a working interface or the management interface for capturing packets.
Source/Destination IP	Specifies the source or destination IP address of packets to be captured. No value indicates all IP addresses.
Protocol	Specifies a protocol so that packets transmitted by using this protocol will be captured. You can select **Unlimited**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**.
Max Captured Packets	Specifies the maximum number of packets to be captured. The value ranges from 1 to 10000.

Step 3 Click **OK**.

The tool then captures packets as specified and saves them in a .cap file, which is displayed in the list, as shown in Figure 9-7.

Step 4 Download a packet capture file.

In the packet capture file list, click the name of a packet capture file to download it to a local disk drive. Such files can be opened with Ethereal or Wireshark.

Step 5 Delete packet capture files.

Select the check box(es) of a file or multiple files and then click **Delete** to delete the selected file(s).

Note that packet capture files of ongoing tasks cannot be deleted.

----End

10 Console-based Management

Via a serial connection, you can access the console-based manager to perform operations such as initial configuration, status detection, and restoration of initial configuration, which cannot be conducted on the web-based manager.

This chapter describes how to log in to and manage the console, containing the following sections:

Section	Description
Login to the Console	Describes how to log in to the console-based manager.
Details	Describes how to manage various initial settings of the device.

10.1 Login to the Console

Before logging in to the console, you need to prepare the following:

- One computer
- One serial cable included in the accessory box
- Terminal software (such as the HyperTerminal software included in Microsoft Windows) that can establish communication to the ADS device via the console
- Connection of ADS to the computer with a console cable

Here, the HyperTerminal software included in a Microsoft Windows XP operating system is taken as an example to describe how to connect ADS to terminal software:

To log in to the ADS console, perform the following steps:

Step 1 Use the terminal software to log in to the console via a serial port.

For details on serial port parameters, see appendix B Default Parameters.

Step 2 Type the initial user name and password= of the console administrator.

If the user name and password are correct, you will successfully log in to the console.

Note	Note that you can only operate on the keyboard on the console. Type a sequence number as prompted and press **Enter** to open the console management menu.

----End

10.2 Details

After you successfully log in to the console of ADS, the main menu is displayed, as shown in Figure 10-1. Type a sequence number as prompted and press **Enter** to open a menu.

For the initial login, the system asks you to change the initial password. You must change the password before performing other operations. For details on changing the password, see section 10.2.4 Changing the Console Password.

Figure 10-1 Main menu of the console

```
Welcome to Nsfocus ADS
========================================
      1.  IPv4 Network setting
      2.  IPv6 Network setting
      3.  DNS setting
      4.  Console Password change
      5.  Datetime setting
      6.  All Default setting
      7.  Web Password Default setting
      8.  Console time out setting
      9.  Rollback system
      10. System state check
      11. Management interface ACL status
      12. Logout
========================================
Your password is the initial password.
Please choose "Console Password Change" to customize a new one.
Input your selection:
```

10.2.1 Configuring IPv4 Network Settings

On the main menu, type **1** and press **Enter** to open the IPv4 address configuration screen. Type the IPv4 address, netmask, and gateway address, with each followed by a carriage return. The system displays the settings, as shown in Figure 10-2.

After confirming the settings, type **y** and press **Enter** to save the settings and return to the main menu.

Figure 10-2 IPv4 network settings

```
Current network setting:
     IP=10.30.2.105
NETMASK=255.255.0.0
GATEWAY=10.30.255.254
Input your network setting:
Input the IP address(10.30.2.105):
Input the netmask(255.255.0.0):
Input the gateway(10.30.255.254):


Your network setting is:
     IP=10.30.2.105
NETMASK=255.255.0.0
GATEWAY=10.30.255.254
Are you sure to save and enable this setting(y/n):
```

10.2.2 Configuring IPv6 Network Settings

On the main menu, type **2** and press **Enter** to open the IPv6 address configuration screen. Type the IPv6 address, prefix length, and gateway address, with each followed by a carriage return. The system displays the settings, as shown in Figure 10-3.

After confirming the settings, type **y** and press **Enter** to save the settings and return to the main menu.

Figure 10-3 IPv6 network settings

```
Current network setting:
  IP_v6_link=
          inet6 addr: fe80::210:f3ff:fe2a:a24a/64 Scope:Link
IP_v6_global=
          inet6 addr: 2001::98/64 Scope:Global
 GATEWAY_v6=null
Input your network setting:
Input the IP address(2001::98):
Input the netmask(64):
Input the gateway:


Your network setting is:
      IP_v6=2001::98/64
 GATEWAY_v6=
Are you sure to save and enable this setting(y/n):
```

10.2.3 Configuring DNS Settings

On the main menu, type **3** and press **Enter** to open the DNS configuration screen.

As shown in Figure 10-4, type the IP address of the DNS server as prompted, and press **Enter** to save the settings and return to the main menu.

Figure 10-4 Configuring the DNS server

```
Input the DNS address(192.168.1.1):192.168.1.2
Mon Mar 26 14:48:17 CST 2012
Mon Mar 26 14:48:17 CST 2012
tar: removing leading '/' from member names
DNS changed!
```

10.2.4 Changing the Console Password

On the main menu, type **4** and press **Enter** to change the login password of the console, as shown in Figure 10-5.

Type the current password and new password, and press **Enter**. Then the system displays a message notifying you whether the password is successfully changed.

Figure 10-5 Changing the console password

```
Note: a good password should have different characters such as [A-Z][a-z][0-9][!@#$%
],and no less than 8 characters

Thu Mar 28 09:11:17 CST 2013
Changing password for admin
old password:
```

Note	Please set the login password of the console as prompted. See appendix B Default Parameters for the initial account of the console.

10.2.5 Setting System Time

On the main menu, type **5** and press **Enter** to set system time, as shown in Figure 10-6.

Type the new system date and time (format: 2013-03-26 14:52:12), and then press **Enter** to save the settings and return to the main menu.

Figure 10-6 Setting system time

```
Datetime set:
Current date is 2012-03-26 14:52:12
Input the new date:
```

Caution	Changing system time may interrupt BGP routes and suspend traffic diversion. Please handle with caution.

10.2.6 Restoring Default Settings

On the main menu, type **6** and press **Enter** to restore default settings, including network settings and password of the web administrator. This operation takes effect immediately.

Note that the IP address of the management interface is restored as follows:

- If the management interface is configured with an IPv6 address, the IPv6 address is cleared.
- If the management interface is configured with an IPv4 address, the default IPv4 address is restored.

10.2.7 Restoring Initial Password of Web Administrator

On the main menu, type **7** and press **Enter** to restore the initial password of the web administrator, as shown in Figure 10-7.

Type **y** as prompted and press **Enter** to restore the initial password, **nsfocus**.

Figure 10-7 Restoring the initial password of the web administrator

```
Input your selection:7
Warning: it will reset web password as default
Are you sure to continue(y/n)?:
```

10.2.8 Setting the Console Timeout Value

On the main menu, type **8** and press **Enter** to open the console timeout setting window.

Figure 10-8 Setting the console timeout value

```
Console time out value is 10 minutes.
================================
      1. Enable console time out
      2. Disable console time out
      3. Set console time out value
      4. return
================================
Input your selection:
```

In the window shown in Figure 10-9, you can perform the following operations:

- Type **1** and press **Enter** to enable the console timeout function.

  The console timeout function is enabled by default. The default timeout value is **10** minutes.
- Type **2** and press **Enter** to disable the console timeout function.
- Type **3** and press **Enter**. Then you can specify the console timeout value in minutes, which must be an integer in the range of 1 to 60.

Figure 10-9 Setting the timeout value

```
Console time out is close.
==================================
      1. Enable console time out
      2. Disable console time out
      3. Set console time out value
      4. return
==================================
Input your selection:3
Time value in minute[1~60]:
```

- Type **4** and press **Enter** to return to the main menu.

10.2.9 Rolling Back the Version

Note	This function works only for ADS V4.5R88F30 and later, but not for ADS V4.5R90F01 currently.

On the main menu, type **9** and press **Enter** to open the version rollback window.

Figure 10-10 Rolling back the version

```
Welcome to Nsfocus ADS
======================================
      1.  IPv4 Network setting
      2.  IPv6 Network setting
      3.  DNS setting
      4.  Console Password change
      5.  Datetime setting
      6.  All Default setting
      7.  Web Password Default setting
      8.  Console time out setting
      9.  Rollback system
      10. System state check
      11. Management interface ACL status
      12. Logout
======================================
Your password is the initial password.
Please choose "Console Password Change" to customize a new one.
Input your selection:9
This operation will rollback system to last avaliable version.
And it will reboot system automatically if rollback succeed. Are you sure want to rollback system[y|n]?y
It will rollback to version V4.5R88F30 (build date: 20150127). Are you sure to continue?[y|n]
y
Start to rollback system and it will take a few minutes. Please wait.......
[  371.646461] EXT2-fs (sda1): warning: mounting unchecked fs, running e2fsck is recommended
Rollback succeed and it will reboot system after a few seconds.
```

In the window shown in Figure 10-10, type **y** and press **Enter**. Then the current version is rolled back to the previous one, that is, the one before the upgrade. Note that the version can be rolled back only once.

10.2.10 Viewing System Information

On the main menu, type **10** and press **Enter**. Then system information is displayed. As shown in Figure 10-11, the system information shows that the system is normally started. This function is used to check the startup status of the device.

Figure 10-11 Viewing system information

```
Input your selection:10
Current system is ready, system hash id: 9104-4884-99BE-B6F6.
```

10.2.11 Configuring the Management Interface Access Control Function

On the main menu, type **11** and press **Enter** to open the management interface access control setting window.

Figure 10-12 Configuring the management interface access control function

```
The management interface ACL function has been enabled.
The default ACL action is permit
Management interface ACL list:
10.66.70.214        255.255.255.255     permit
10.245.25.211       255.255.255.255     permit
Do you want to disable management interface ACL function?[yes/no]
```

In the window shown in Figure 10-12, type **yes** and press **Enter** to disable the management interface access control function or type **no** and press **Enter** to return to the previous menu, with the current status of this function unchanged.

10.2.12 Exiting the Console

On the main menu, type **12** and press **Enter** to log out of the console-based manager.

A Acronyms and Abbreviations

ACL	access control list
ARP	Address Resolution Protocol
CGI	Common Gateway Interface
CSRF	cross-site request forgery
CSS/XSS	cross-site scripting
DDoS	distributed denial-of-service
HTTP	Hypertext Transfer Protocol
IDC	Internet Data Center
IP	Internet Protocol
LAN	local area network
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
NSFOCUS WAF	NSFOCUS Web Application Firewall
SQL	Structured Query Language
URL	Uniform Resource Locator
WAN	wide area network

B Default Parameters

B.1 Default Console Parameters

IP Address	192.168.1.100
Netmask	255.255.255.0
Gateway	192.168.1.1

B.2 Default Web Administrator Account

User Name	admin
Password	nsfocus

B.3 Default Console Administrator Account

User Name	admin
Password	nsfocus

B.4 Default CLI Administrator Account

User Name	routerman

B.5 Console Specification

Baud Rate	115200 bps
Data Bits	8

C IPv4/IPv6 Support

The following table lists the support of ADS NX series' modules for IPv4 and IPv6.

Module	Function	IPv4	IPv6
Real-Time Monitoring			
Policies	SYN flood detection	√	√
	ACK flood detection	√	√
	UDP flood detection	√	√
	ICMP flood detection	√	√
	HTTP protection	√	√
	HTTPS protection	√	×
	DNS protection algorithms 1 and 2	√	√
	DNS protection algorithm 3	√	×
	DNS protection algorithm 4	√	√
	TCP control parameters	√	√
	TCP control parameters – TCP fragment control	√	×
	IP behavior control	√	×
	SIP protection – default DDoS	√	×
	SIP protection – groups	√	√
	UDP payload check – payload check	√	√
	UDP payload check – mode check	√	×
	UDP protection – UDP fragment control	√	×
	ICMP fragment control	√	×
	UDP protection – drop UDP fragments – groups	√	×
	UDP protection – maximum packet length	√	√
	UDP protection – traffic control by Src IP + Src port	√	√
	UDP protection – traffic control by Dst IP + Dst port	√	√
	UDP protection – traffic control by Src IP	√	√

Module	Function	IPv4	IPv6
	UDP protection – traffic control by Dst IP	√	√
	UDP protection – minimum packet length	√	√
	UDP protection – traffic control by Dst IP + Src port	√	√
	ICMP traffic rate limiting	√	√
	Watermark protection	√	×
	Protocol ID check	√	√
	Group traffic control	√	√
	Port check	√	√
	URL rules	√	√
	Advanced global parameters	√	√
	Policy auto-learning	√	√
	Access control rules	√	√
	Reflection protection rules	√	√
	GeoIP rules	√	√
	Regular expression rules	√	×
	Hardware access control rules	√	√
	Connection exhaustion rules	√	×
	URL-ACL protection rules	√	√
	Blacklist	√	×
	Whitelist	√	√
	HTTP keyword checking	√	×
	DNS keyword checking	√	×
Diversion & Injection	Running mode	√	√
	Port channel configuration	√	√
	IP address configuration	√	√
	Working interface access control (web and SSH)	√	×
	BGP diversion	√	√
	OSPF diversion	√	√
	ISIS diversion	√	×
	RIP diversion	√	×
	LDP diversion	√	×
	IP route assignment	√	√
	Injection interface	√	√

Module	Function	IPv4	IPv6
	Layer 2 injection	√	√
	Layer 3 injection	√	√
	MPLS injection	√	×
	MPLS VPN injection	√	×
	GRE tunnel injection	√	×
	MAC address table	√	√
	Filtering rules	√	√
	Manual diversion	√	√
	Group diversion	√	√
	Diversion routing table	√	√
	MPLS route	√	×
	Syslog diversion configuration – collaboration with Genie devices	√	×
	Syslog diversion configuration – collaboration with Arbor devices	√	×
	Syslog diversion configuration – collaboration with Samurai devices	√	×
	Syslog diversion configuration – collaboration with Kuanguang devices	√	×
Collaboration	Collaboration with ADS M	√	√
	Collaboration with ESPP	√	×
	Collaboration with NTA V4.5.61.2	√	×
	Collaboration with NTA V4.5R90F01	√	√
Logs	Attack logs	√	√
	System operation logs	√	√
	System login logs	√	√
	Link status logs	—	—
	Traffic diversion logs	√	√
	HA synchronization logs	√	√
	Syslog diversion logs	√	×
System	Basic settings	√	√
	Interface link configuration	—	—
	System user management	√	√
	Management mode configuration	√	√
	Configuration file management	√	√

Module	Function	IPv4	IPv6
	HA configuration	√	√
	Management interface access control	√	×
	Collaboration configuration	√	×
	Bandwidth overrun limit	√	×
	Login security settings	√	×
	Locked user management	√	×
	Authentication configuration	√	√
	Syslog configuration	√	√
	SNMP trap configuration	√	√
	SNMP agent setting	√	×
	Email configuration	√	√
	SFTP/SSH log export	√	×
	License interface	—	—
	License speed limit	—	—
	System upgrade	—	—
	Remote assistance	—	—
	SSL certificate import	—	—
	One-click information collection	—	—
	Version information	—	—
Advanced	Packet capture management	√	√
	Pattern matching rules	√	√
NTI	Upload	√	√
	Synchronization	√	×
	Query	√	×