NSFOCUS ADS

User Guide

Version: V4.5R90F05 (2023-11-15)

Confidentiality: RESTRICTED

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided "AS-IS" *without guarantees of any kind, express or implied*. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

Contents

Preface

Scope

This document describes the features and usage of the web-based manager and console-based manager of NSFOCUS Anti-DDoS System (ADS), covering the following series and models:

- ADS NX3-800E
- ADS NX3-HD1000
- ADS NX3 2000 series (ADS NX3-2020E)
- ADS NX3-HD2500
- ADS NX5 4000 series (ADS NX5-4020E)
- ADS NX5 6000 series (ADS NX5-6025E)
- ADS NX5-8000
- ADS NX5-10000/12000
- ADS NX5-HD5000/6000
- ADS NX5-HD4500/6500
- ADS NX5 HD8500
- ADS NX5-20000
- ADS NX1-VN (virtual ADS, namely, vADS)

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 document are all based on ADS NX5-4020E.

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.
4 Real-Time Monitoring	Describes details about real-time monitoring.

Chapter	Description
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, pattern matching, NTI, and carpet bombing protection.
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.
11. Initial Configuration	Describes how to complete intial configurations upon the installation of ADS.
12. System Maintenance	Describes how to upgrade the system and how to perform common troubleshooting tasks.
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.

Change History

Version	Description
V4.5R90F05	• New functions: application layer protection – non-decrypted traffic protection, programmable rules, carpet bombing protection, and password + certificate UKey authentication. • Optimized functions: packet capture, license expiration warning, botnet and IP behavior control policy, HTTPS protection policy, maximum number of various rules, management interface access control rule, main menu of the console-based manager, and user management.
V4.5R90F04SP03	• New functions: group-specific exception IP, Windows server for LDAP, and device shutdown. • Optimized functions: SNMP settings, and log sending by email.
V4.5R90F04	• New functions: common UDP watermark protection algorithm, group-specific access control rule, group-specific NTI, web API log, and license expiration warning. • Optimized functions: global NTI, global ACL rule, MAC address configurations, and system logs.
V4.5R90F03SP02	• Updated the structure based on the new template. • Added descriptions about the following new functions: UDP session authentication policy, disk usage, password + email

Version	Description
	authentication, group-specific GeoIP rule, and attack-triggered packet capture.

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.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- 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

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

- Email: info-support@nsfocus.com

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 against 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, depending on the network environment. The following sections detail the two modes.

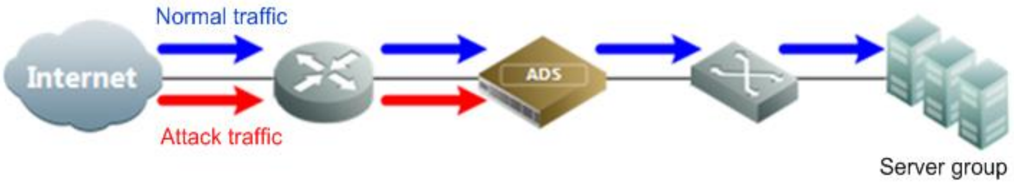
Note

- ADS NX3-2020E, NX3-800E, NX3-HD2500, NX3-HD1000, NX5-HD4500, NX5-4020E, NX5-6025E, NX5-HD5000, NX5-HD6000, NX5-HD6500, NX5-HD8500, and NX5-8000 support both in-path and out-of-path deployment modes, whereas ADS NX5-10000/12000/20000 supports the out-of-path deployment mode only.
- When vADS uses a virtual network adapter, it can be deployed only in out-of-path mode. For details about deployment of a virtual network adapter, see the *NSFOCUS ADS NX1-VN Installation and Deployment Guide*.

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.

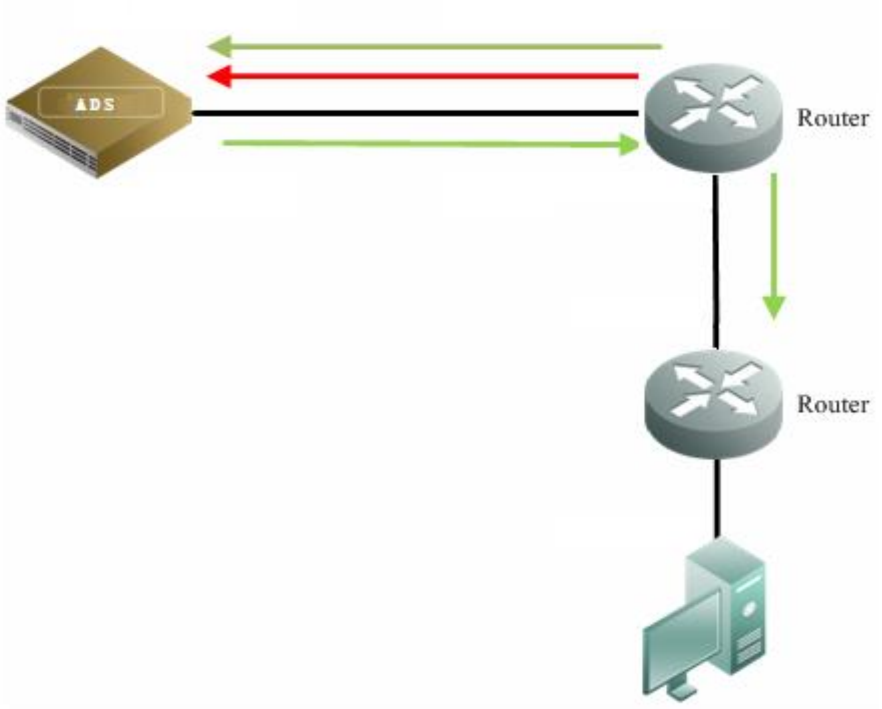
Figure 1-1 In-path deployment of an ADS device



1.2.2 Out-of-Path Deployment

To protect mission critical systems 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 Users	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

This section uses a Chrome browser as an example to describe how to log in to the web-based manager of ADS.

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

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

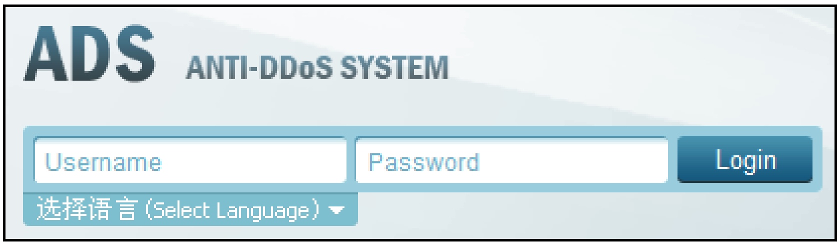
As the ADS device supports both IPv4 and IPv6 protocols, you can type an IPv4 address (for example, **https://192.168.1.100**) or IPv6 address (for example, **https://[2001::107]**).

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

Step 3 Click **Advanced** and then **Proceed to xxxx (unsafe)**.

The login page shown in Figure 2-1 appears.

Figure 2-1 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. - If you are authenticated by password + email, you need to type a correct password and verification code provided via email. The user account will be locked after several failed verification code attempts. - If you are authenticated by password + certificate, you need to click **Download Application** in the lower-left corner of the login page to download and install the UKey program. Then insert the UKey into your PC. You can log in to the system only after typing a correct user name and password, and providing a correct digital certificate.

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

Note	
	Note the following during login: - You are advised to use 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 Users

User roles of the ADS devices include superuser (**admin** by default), CLI user (**routerman** by default), custom user, common user, administrator, auditor, and custom access 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, logs (detailed information and statistical graphs of the attack log, statistical graphs of attack traffic, and the traffic diversion log), system management (basic configuration, interface configuration, and modification of his or her own account information), advanced application, and O&M.	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), system management information (basic system settings and interface settings), advanced application, and O&M..
Auditor	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.
Custom access user	Customizable.	Customizable.

Note

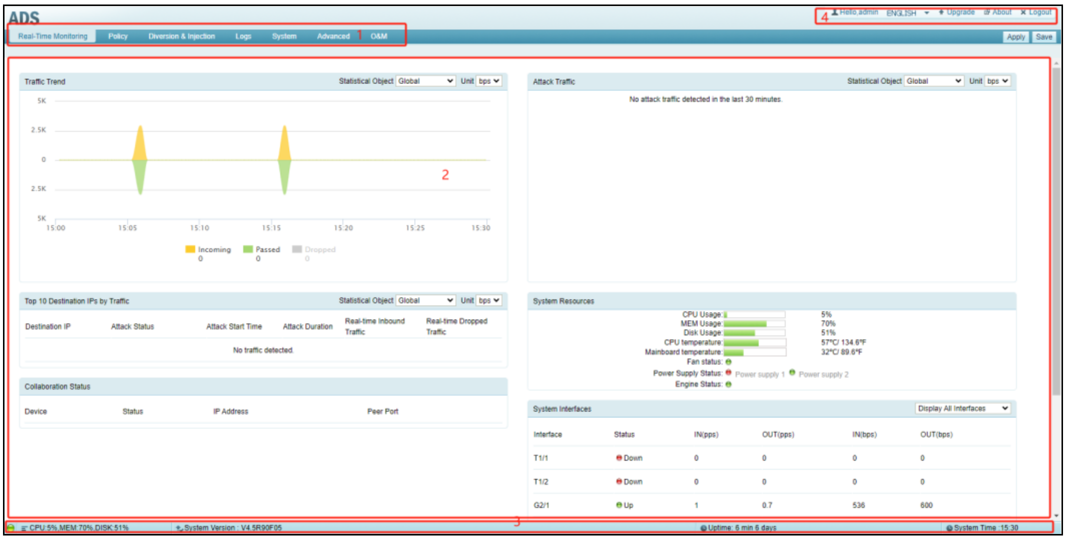
You are advised to change the initial password immediately after login with the default user account. For details on initial passwords, see appendix B Default Parameters.

2.3 Web Page Layout

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



No attack traffic detected in the last 30 minutes.

Destination IP	Attack Status	Attack Start Time	Attack Duration	Real-time Inbound Traffic	Real-time Dropped Traffic
No traffic detected.					

CPU Usage:	5%
MEM Usage:	70%
Disk Usage:	51%
CPU temperature:	57°C/ 134.6°F
Mainboard temperature:	32°C/ 89.6°F
Fan status:	●
Power Supply Status:	● Power supply 1 ● Power supply 2
Engine Status:	●

Device	Status	IP Address	Peer Port

Interface	Status	IN(pps)	OUT(pps)	IN(bps)	OUT(bps)
T1/1	● Down	0	0	0	0
T1/2	● Down	0	0	0	0
G2/1	● Up	1	0.7	536	600

CPU:5%,MEM:70%,DISK:51% System Version : V4.5R90F05 Uptime: 6 min 6 days System Time :15:30

Table 2-2 describes the web page layout.

Table 2-2 Web page layout

No.	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.

Button	Function
⬆ Upgrade	Switches to the system upgrade window.
⧉ About	Displays information about the current ADS device.
✖ Logout	Logs you out of the system.

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.

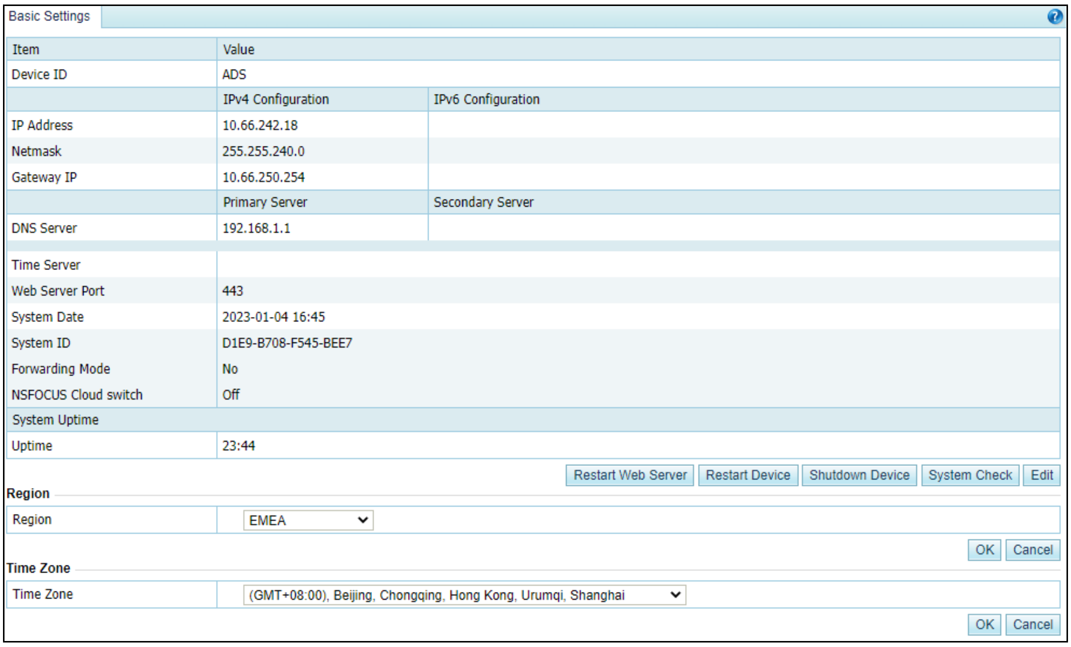
Note

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



Basic Settings

Item	Value	
Device ID	ADS	
	IPv4 Configuration	IPv6 Configuration
IP Address	10.66.242.18	
Netmask	255.255.240.0	
Gateway IP	10.66.250.254	
	Primary Server	Secondary Server
DNS Server	192.168.1.1	
Time Server		
Web Server Port	443	
System Date	2023-01-04 16:45	
System ID	D1E9-B708-F545-BEE7	
Forwarding Mode	No	
NSFOCUS Cloud switch	Off	
System Uptime		
Uptime	23:44	

Region

Region	EMEA

Time Zone

Time Zone	(GMT+08:00), Beijing, Chongqing, Hong Kong, Urumqi, Shanghai

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 that the IP segment 172.16.1.0/24 is reserved for internal communication. 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.

Parameter	Description
Gateway IP	IPv4/v6 address of the gateway for the management interface.
H Port IP Configuration/H Port IP Netmask	The H port is used as a heartbeat interface for ADS to implement high availability (HA) in in-path mode. Therefore, you need to configure the IPv4 address and related subnet mask or IPv6 address and related prefix length for this port here. Note It is recommended that you configure an IP address in another network segment for the H port than the one used by the management port to avoid loops.
DNS Server	IP addresses of the primary and secondary DNS servers used by the management interface of the current ADS device. Only when the primary DNS server malfunctions can the secondary be used.
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.
NSFOCUS Cloud Switch	Controls whether to turn on the NSFOCUS cloud service.
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:

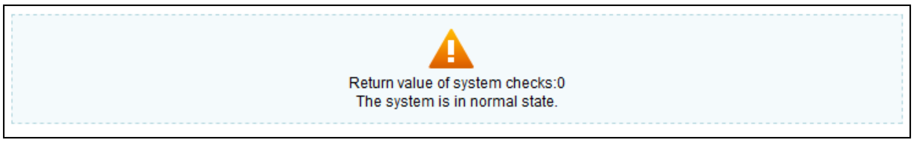
- Edit basic system information.

  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



Return value of system checks:0
The system is in normal state.

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.

- Shut down the device remotely.

Click **Shutdown Device** to shut down the current ADS remotely.

Note	When a 6U device (ADS NX5-10000 or ADS NX5-12000) starts, the status LED (STA) of a device without boards appears yellow, while that of a device with boards appears green. After shutdown, the status LED (STA) of a device with boards no longer appears green.

- 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**, the NSFOCUS Cloud switch is turned on by default. • When **Region** is set to any other region than **Chinese mainland**, 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 settings.

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 NX3-2020E, NX5-4020E, and NX5-6025E 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 NX3-800E uses six 1000M electrical ports as working interfaces and supports one expansion slot. The expansion slot supports the following types of interface cards: 8 x 1000M electrical port, 8 x 1000M optical port, 4 x 1000M electrical port, and 4 x 1000M optical port.
- ADS NX5-10000/12000/20000 supports interface cards up to the following configuration:
  - 4 x 1000M electrical port
  - 6 x 100G optical port
  - 4 x 40G optical port
  - 20 x 10G optical port
- ADS NX3-HD2500/NX5-HD4500/NX5-HD6500/NX5-HD8500 supports 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
  - 4 x 10G optical port
  - 2 x 10G optical port
- ADS NX3-HD1000/NX5-HD5000/NX5-HD6000 supports the following types of interface cards:
  - 6 x 1000M electrical port + 4 x 1000M optical port
  - 4 x 1000M electrical port + 4 x 1000M optical port
  - 8 x 1000M electrical port
  - 4 x 1000M optical port
  - 2 x 10G optical port
  - 4 x 10G 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.

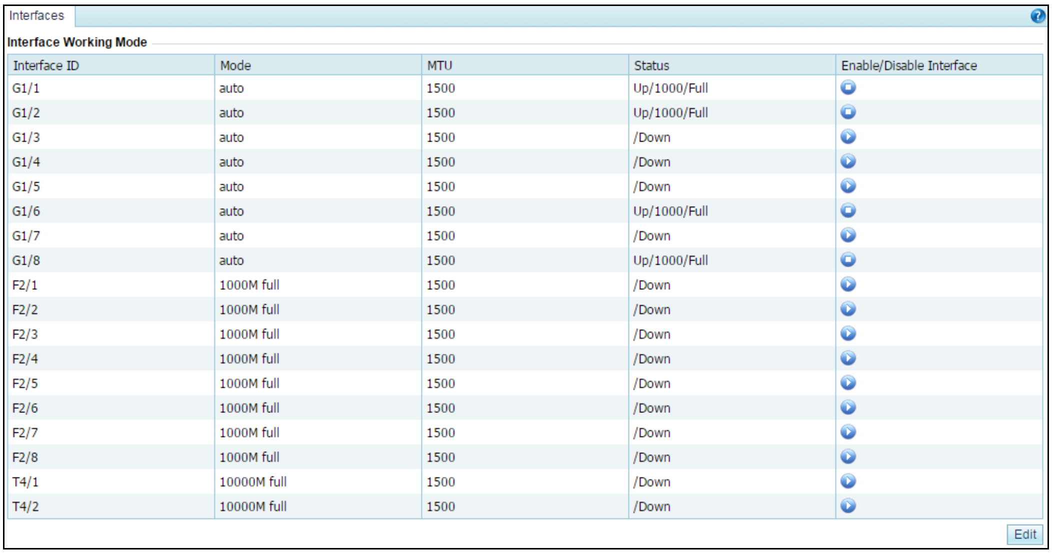
This section describes those operations in detail.

Enabling or Disabling Working Interfaces

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

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

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



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	▶

Table 3-2 describes interface working mode parameters.

Table 3-2 Interface working mode parameters

Parameter	Description
Interface ID	ADS NX3-800E: • G3/1–G3/8:1000M electrical ports • F4/1–F4/8: 1000M optical ports ADS NX3-4020E: • T1/1 and T1/2: 10G optical ports • G3/1–G3/8:1000M electrical ports • F4/1–F4/8: 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

Parameter	Description
	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.

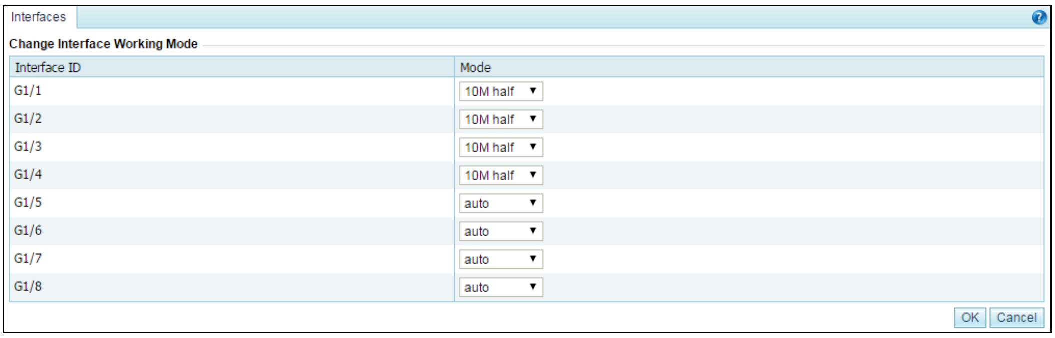
----End

Changing the Working Mode of 1000M Electrical Ports

ADS NX5-4020E 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



Change Interface Working Mode

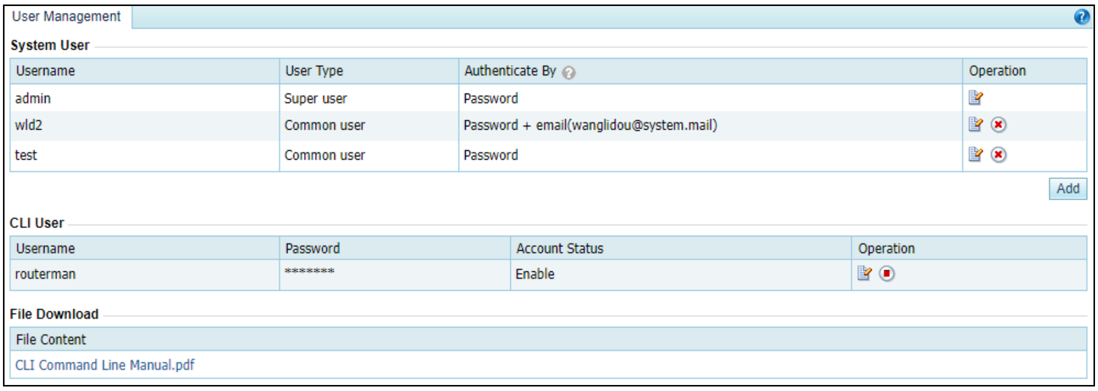
Interface ID	Mode
G1/1	10M half
G1/2	10M half
G1/3	10M half
G1/4	10M half
G1/5	auto
G1/6	auto
G1/7	auto
G1/8	auto

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

3.1.3 User Management

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

Figure 3-5 System users



User Management

System User

Username	User Type	Authenticate By	Operation
admin	Super user	Password	✎
wld2	Common user	Password + email(wanglidou@system.mail)	✎ ⊗
test	Common user	Password	✎ ⊗

CLI User

Username	Password	Account Status	Operation
routerman	*******	Enable	✎ ●

File Download

File Content
CLI Command Line Manual.pdf

User roles include the following:

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

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

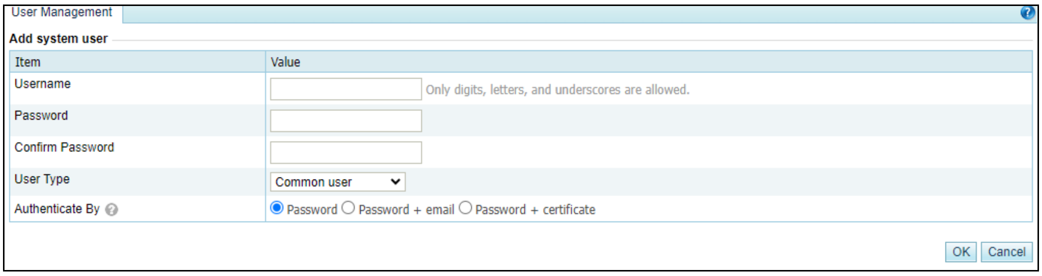
Under **File Download**, you can click the *CLI Command Line Manual* link to download this user guide.

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.

A user, after being added, can be edited and deleted.

Figure 3-6 Adding a system user

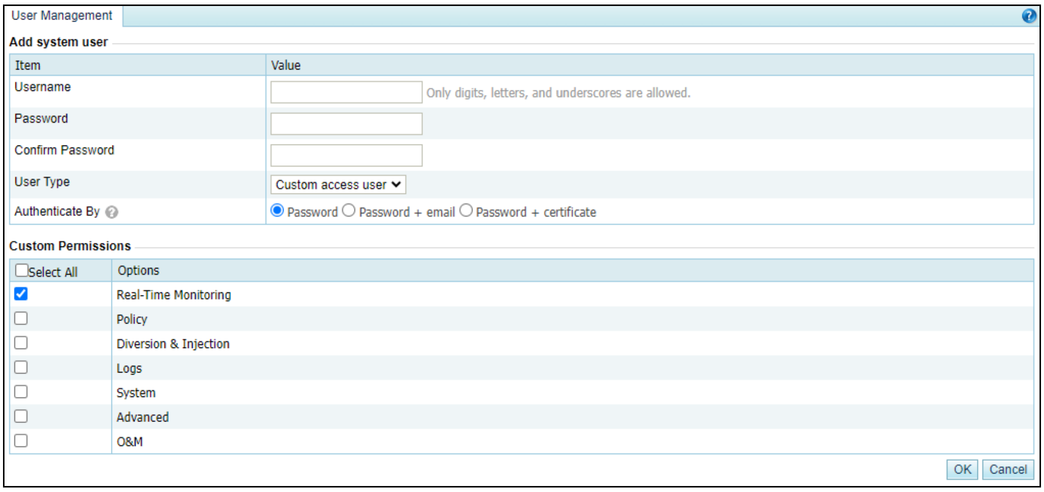


User Management

Add system user

Item	Value
Username	Only digits, letters, and underscores are allowed.
Password	
Confirm Password	
User Type	Common user
Authenticate By	● Password ○ Password + email ○ Password + certificate

Figure 3-7 Adding a system user – custom access user



User Management

Add system user

Item	Value
Username	Only digits, letters, and underscores are allowed.
Password	
Confirm Password	
User Type	Custom access user
Authenticate By	● Password ○ Password + email ○ Password + certificate

Custom Permissions

☐Select All	Options
☑	Real-Time Monitoring
☐	Policy
☐	Diversion & Injection
☐	Logs
☐	System
☐	Advanced
☐	O&M

Table 3-3 describes parameters for adding a user.

Table 3-3 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.
User Type	Specifies the role of the new account, which can be **Custom user**, **Common user**, **Administrator**, **Audit user**, and **Custom access user**. For details about permissions of each user role, see Table 2-1. For the selection of **Custom access user**, you also need to specify permissions for this role, as shown in Figure 3-7.
Authenticate By	Specifies the login authentication method, which can be **Password**, **Password + email**, or **password + certificate**. • For **Password + email, you need to type an email address.** • For **Password + certificate**, you need to insert a UKey into the USB port of the ADS device, and click ➔ next to **Digital Certificate** to generate a digital certificate and write the information to the UKey. Note • For email verification, you need to configure a correct SMTP server under **System** > **Log Services** > **Email**. For details, see Email Configuration. • If the system user **admin** is authenticated by password + email, firstly ensure the correctness of the email address and the availability of the

Parameter	Description
	email service. • To download the UKey program, click **Download Application** in the lower-left corner of the login page.

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.

The password must be 6 to 30 characters long. The minimum length of passwords depends on the **Min Length** value specified under **System** > **Security Configuration** > **Login Security Settings**. 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.

Editing a CLI User

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

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:

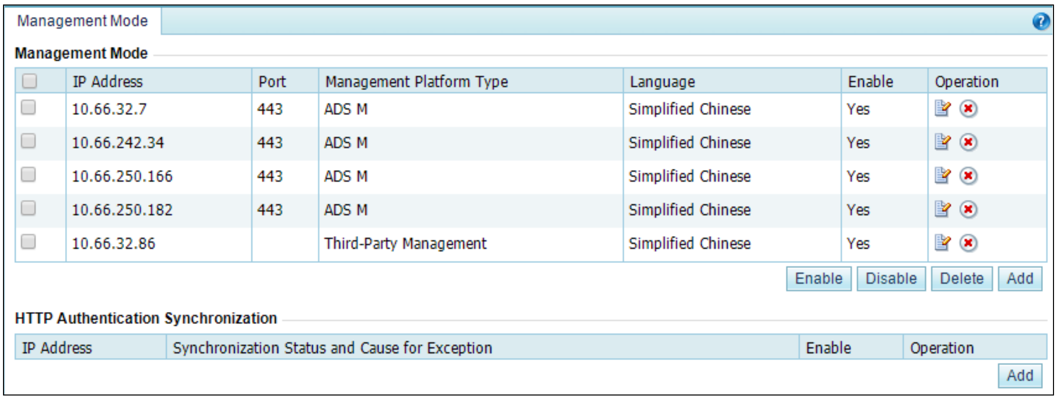
- Third-party management: allows the administrator to use a third-party program to manage ADS.

- 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 3-8 Management Mode page



Management Mode

Management Mode

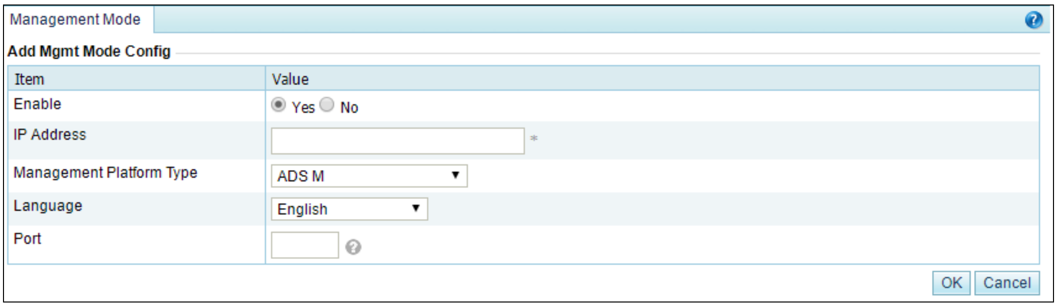
□	IP Address	Port	Management Platform Type	Language	Enable	Operation
□	10.66.32.7	443	ADS M	Simplified Chinese	Yes	✎ ✖
□	10.66.242.34	443	ADS M	Simplified Chinese	Yes	✎ ✖
□	10.66.250.166	443	ADS M	Simplified Chinese	Yes	✎ ✖
□	10.66.250.182	443	ADS M	Simplified Chinese	Yes	✎ ✖
□	10.66.32.86		Third-Party Management	Simplified Chinese	Yes	✎ ✖

HTTP Authentication Synchronization

IP Address	Synchronization Status and Cause for Exception	Enable	Operation

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

Figure 3-9 Add Mgmt Mode Config page



Management Mode

Add Mgmt Mode Config

Item	Value
Enable	● Yes ○ No
IP Address	*
Management Platform Type	ADS M ▼
Language	English ▼
Port	

Table 3-4 describes management mode parameters.

Table 3-4 Management mode parameters

Parameter	Description
Enable	Controls whether ADS accepts centralized management. • **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

Parameter	Description
	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
Port	Specifies a port for ADS to collaborate with ADS M. This parameter is available only when **ADS M** is selected as the management platform. The default port is **443**.
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. This parameter is available only when **Third-Party Management** is selected as the management platform. Only HTTPS is supported.
Language	Specifies the language of messages sent by ADS to ADS M, ESPC/ESPP, or a third-party platform. Generally, after you configure protection policies for ADS via ADS M, 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 3-8.

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.

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 can be configured.

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

----End

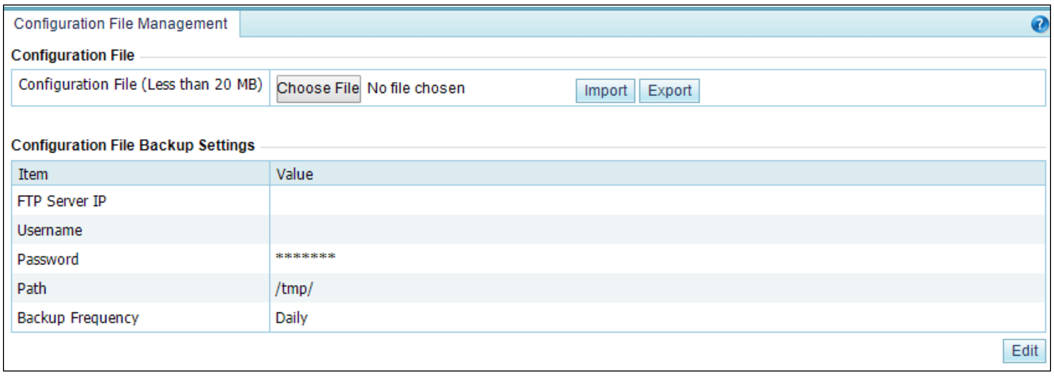
3.1.5 Configuration File Management

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

Choose **System** > **Local Settings** > **Configuration File Management**, as shown in Figure 3-10. Click **Export** to export a configuration file with the default file name **collapsar.conf**.

Figure 3-10 Configuration file management



Configuration File Management

Configuration File

Configuration File (Less than 20 MB)	Choose File No file chosen	Import Export

Configuration File Backup Settings

Item	Value
FTP Server IP	
Username	
Password	*******
Path	/tmp/
Backup Frequency	Daily

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 3-10, click **Choose File** 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.

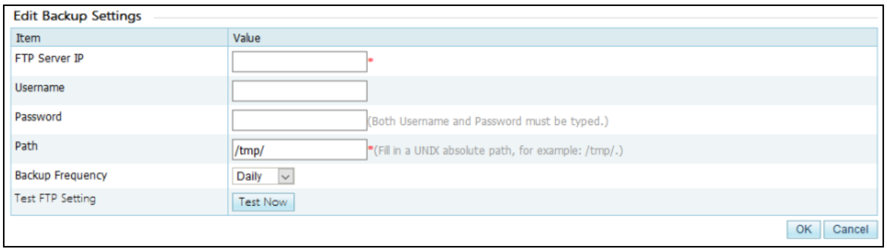
Pay attention to the following while importing or exporting a configuration file:

- The size of the configuration file should be no greater than 20 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 3-10, click **Edit** and set configuration file backup parameters.

Figure 3-11 Configuration file backup



Edit Backup Settings

Item	Value
FTP Server IP	*
Username	
Password	(Both Username and Password must be typed.)
Path	/tmp/ *(Fill in a UNIX absolute path, for example: /tmp/.)
Backup Frequency	Daily
Test FTP Setting	Test Now

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.

Choose **System > Local Settings > Bandwidth Overrun Limit**. Click **Edit** in the dialog box that appears. Table 3-7 describes bandwidth overrun thresholds. Set parameters and click **OK** to complete the configuration.

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.

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**.

Step 2 Click **Edit**.

Table 3-8 describes hardware alert thresholds. The altert thresholds for hardware and virtual devices are different.

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.
Disk Threshold	Specifies the percentage of disk 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 motherboard 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 ADS *NX3-HD2500, NX5-HD4500, NX5-HD6500, and NX5-HD8500* and some NX5-8000 devices.

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

----End

3.1.8 Management Interface Access Control

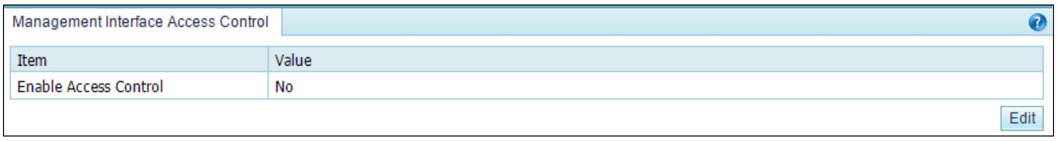
The management interface access control is disabled by default. After being enabled, it can be disabled via the console. After source IP addresses/segments or MAC addresses are specified for access to the management interface, those beyond the specified range cannot access ADS, whether via web, Telnet, 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 3-12 Management Interface Access Control page (access control disabled by default)



Management Interface Access Control

Item	Value
Enable Access Control	No

Step 2 Enable management interface access control and create a default rule.

a. Click **Edit**.

Table 3-9 describes parameters for editing the management interface access control function.

Table 3-9 Parameters for controlling the management interface access control function

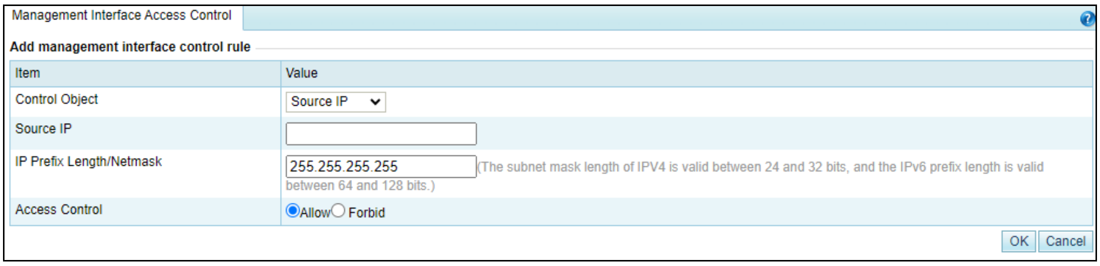
Parameter	Description
Enable	Controls whether to enable the management interface access control function. • **Yes**: enables the function. • **No**: disables the function.
Default Rule	Specifies a default rule. • **permit any**: allows any IP addresses other than those denied access in management interface 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.

b. Set parameters and click **OK** to complete the configuration.

Step 3 Create a management interface access control rule.

a. Click **Add**.

Figure 3-13 Creating a management interface access control rule



Management Interface Access Control

Add management interface control rule

Item	Value
Control Object	Source IP
Source IP	
IP Prefix Length/Netmask	255.255.255.255 (The subnet mask length of IPV4 is valid between 24 and 32 bits, and the IPv6 prefix length is valid between 64 and 128 bits.)
Access Control	● Allow ○ Forbid

Table 3-10 describes parameters for creating a management interface access control rule.

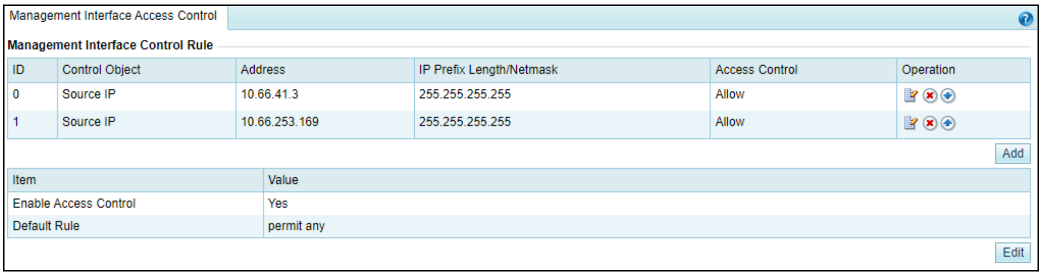
Table 3-10 Parameters for creating a management interface access control rule

Parameter	Description
Control Object	Specifies use of a source IP address or MAC address for access control. Note Exercise caution when configuring this. You are advised to select **Source MAC** only when the management device directly connects to the device or they are in the same layer 2 network environment.
Source IP/Source MAC	Specifies a source IP address/segment or a MAC address that is allowed or forbidden to access ADS.
IP Prefix Length/Netmask	Specifies the subnet mask of the source IP address/segment. This parameter is available only when **Control Object** is set to **Source IP**. • The netmask length for IPv4 addresses ranges from 24 to 32 bits. • The netmask length for IPv6 addresses ranges from 64 to 128 bits.
Access Control	Specifies an action to be taken by ADS for traffic from the specified IP address/segment or MAC address: • **Allow**: allows the specified IP address/segment or MAC address to access ADS. • **Forbid**: forbids the specified IP address/segment or MAC address to access ADS.

Step 4 Set parameters and click **OK**.

A new management interface access control rule is thus created, as shown in Figure 3-14.

Figure 3-14 List of management interface access control rules



Management Interface Access Control

Management Interface Control Rule

ID	Control Object	Address	IP Prefix Length/Netmask	Access Control	Operation
0	Source IP	10.66.41.3	255.255.255.255	Allow	📝 ✖ ⬇
1	Source IP	10.66.253.169	255.255.255.255	Allow	📝 ✖ ⬆

Item	Value
Enable Access Control	Yes
Default Rule	permit any

----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 3-14, 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 3-14, 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 3-14, 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**
>
> HA can be implemented in in-path mode not only between two ADS devices of the same model but also between the following different models:
>
> - ADS NX3-HD2500 and ADS NX3–2020E
> - ADS NX5-HD4500 and ADS NX5-4020E
> - ADS NX3-2020E/NX5-4020E/NX5-6025E and ADS NX5-HD6500
> - ADS NX3-800E and ADS NX3-HD1000.

Currently, ADS, whether in in-path or out-of-path mode, supports two dual-system hot standby modes: active-active and active-standby.

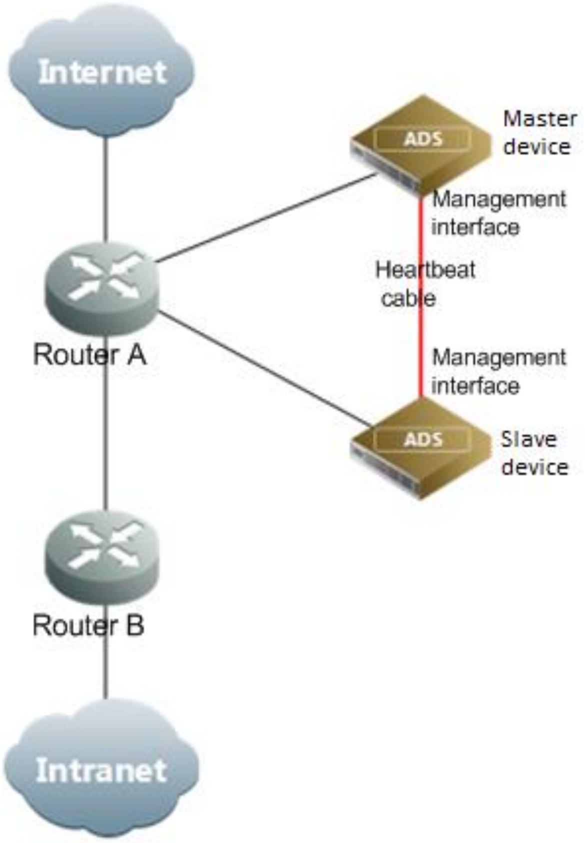
- In active-active mode, one ADS device functions as the primary device, and the other as the secondary device. Both the primary and secondary devices handle services and achieve load balancing. If the primary device fails, the secondary device takes over all work and traffic handled by the former, ensuring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

3.1.9.1 HA Configuration on ADS in Out-of-Path Mode

This section describes how to configure ADS deployed in out-of-path mode to implement HA by giving an example of configuring such devices to work in active-standby mode.

As shown in Figure 3-15, the primary and secondary devices are connected by their 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 3-15 Network topology for ADS in out-of-path mode to implement HA



Note	• Usually, ADS is deployed on the backbone network. Currently, HA can be implemented only in the case of BGP diversion. • Currently, once the primary device fails, the secondary device automatically takes over all services from the primary device. • If **Syn Diversion Config After Entering a Cluster** is enabled in HA advanced configurations on both the primary and secondary devices, the primary device will automatically take back services after it recovers. Otherwise, the administrator needs to manually stop the BGP diversion on the secondary device and enable BGP diversion on the primary 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 primary device to synchronize the specified configuration file to the secondary device. For details, see File Synchronization Configuration. The heartbeat interfaces on the primary and secondary 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:

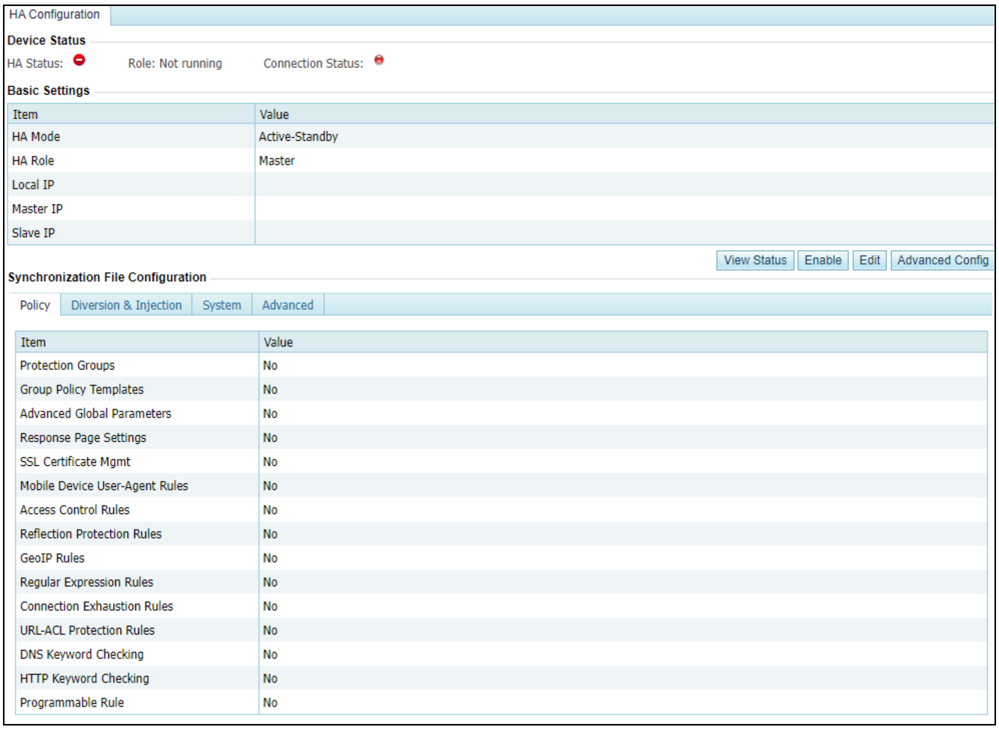
- Basic settings
- Synchronization file configuration

Basic HA Settings

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

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

Figure 3-16 HA Configuration page



Device Status

HA Status: ⛔ Role: Not running Connection Status: ●

Basic Settings

Item	Value
HA Mode	Active-Standby
HA Role	Master
Local IP	
Master IP	
Slave IP	

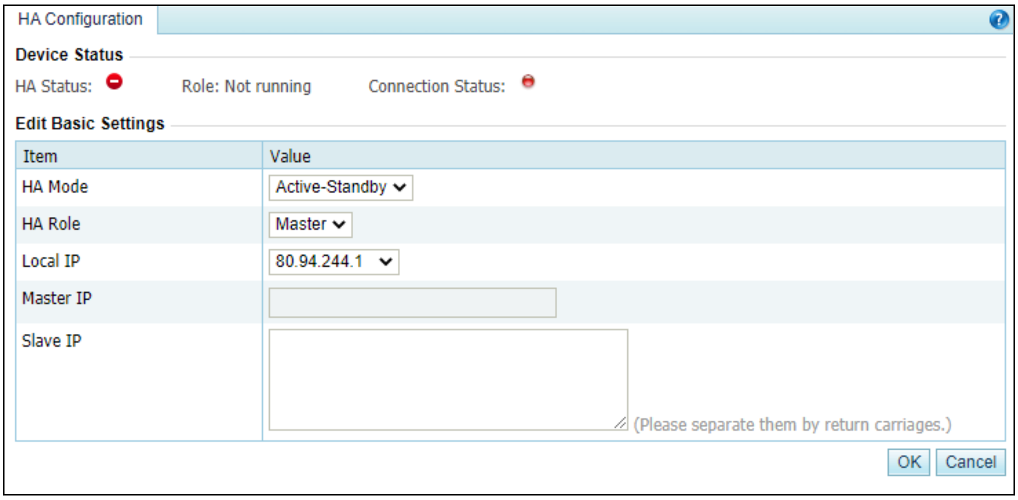
Synchronization File Configuration

Item	Value
Protection Groups	No
Group Policy Templates	No
Advanced Global Parameters	No
Response Page Settings	No
SSL Certificate Mgmt	No
Mobile Device User-Agent Rules	No
Access Control Rules	No
Reflection Protection Rules	No
GeoIP Rules	No
Regular Expression Rules	No
Connection Exhaustion Rules	No
URL-ACL Protection Rules	No
DNS Keyword Checking	No
HTTP Keyword Checking	No
Programmable Rule	No

Step 2 Modify basic settings of HA.

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

Figure 3-17 Editing basic settings



Device Status

HA Status: ⛔ Role: Not running Connection Status: ●

Edit Basic Settings

Item	Value
HA Mode	Active-Standby
HA Role	Master
Local IP	80.94.244.1
Master IP	
Slave IP	(Please separate them by return carriages.)

Table 3-11 describes parameters of basic HA settings.

Table 3-11 Parameters of basic HA settings

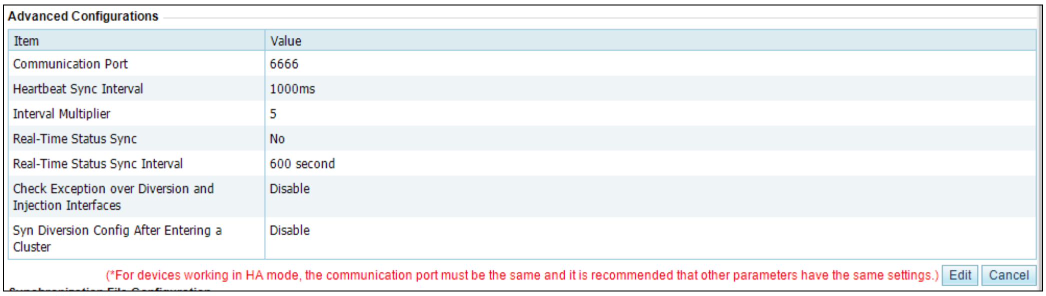
Parameter	Description
HA Mode	HA mode, which can be **Active-Active** or **Active-Standby**.
HA Role	Role played by the current device in dual-system hot standby mode. In active-standby mode: • **Master**: indicates that this device works as a primary device. After HA is enabled, it starts handling services until a failure occurs. • **Slave**: indicates that this device acts as a secondary device. After HA is enabled, this device is in backup state and starts handling services only when the primary device fails. In active-active mode: • **Master**: indicates that this device works as a primary device. After HA is enabled, it starts handling services until a failure occurs. • **Slave**: indicates that this device acts as a secondary device. After HA is enabled, this device is in backup state and handles services the same as the primary device, to achieve load balancing. If the primary device fails, the secondary 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. Note that the IP segment 172.16.1.0/24 is reserved for internal communication.
Master IP	IP address of the primary 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 secondary 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.

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

Step 3 (Optional) Modify advanced HA configurations.

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

Figure 3-18 Advanced Configurations area



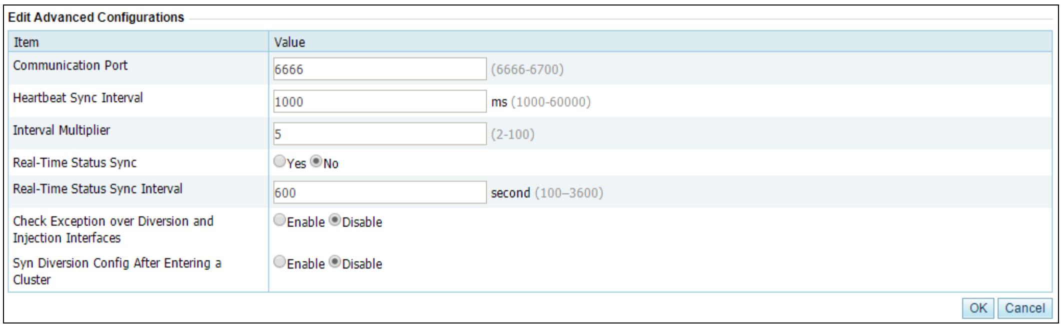
Advanced Configurations

Item	Value
Communication Port	6666
Heartbeat Sync Interval	1000ms
Interval Multiplier	5
Real-Time Status Sync	No
Real-Time Status Sync Interval	600 second
Check Exception over Diversion and Injection Interfaces	Disable
Syn Diversion Config After Entering a Cluster	Disable

(*For devices working in HA mode, the communication port must be the same and it is recommended that other parameters have the same settings.)

b. Click **Edit**.

Figure 3-19 Editing advanced settings



Edit Advanced Configurations

Item	Value
Communication Port	6666 (6666-6700)
Heartbeat Sync Interval	1000 ms (1000-60000)
Interval Multiplier	5 (2-100)
Real-Time Status Sync	○Yes ●No
Real-Time Status Sync Interval	600 second (100–3600)
Check Exception over Diversion and Injection Interfaces	○Enable ●Disable
Syn Diversion Config After Entering a Cluster	○Enable ●Disable

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. Note The **Heartbeat Sync Interval** values on the primary and secondary 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. Note The **Interval Multiplier** values on the primary and secondary 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.

Parameter	Description
	Note **Real-Time Status Sync** should be enabled on both the primary and secondary devices so that files can be synchronized between the two devices.
Real-time Status Sync Interval	Interval at which the primary device to synchronize specified configuration files to the secondary 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 primary/secondary switchover is triggered.
Syn Diversion Config After Entering a Cluster	After an ADS device joins a cluster, the diversion status of the peer is synchronized to this device.

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

----End

File Synchronization Configuration

After configuring basic HA settings on both the primary and secondary devices, you can specify which policy, diversion and injection, system, and advanced configurations are to be synchronized.

Policies

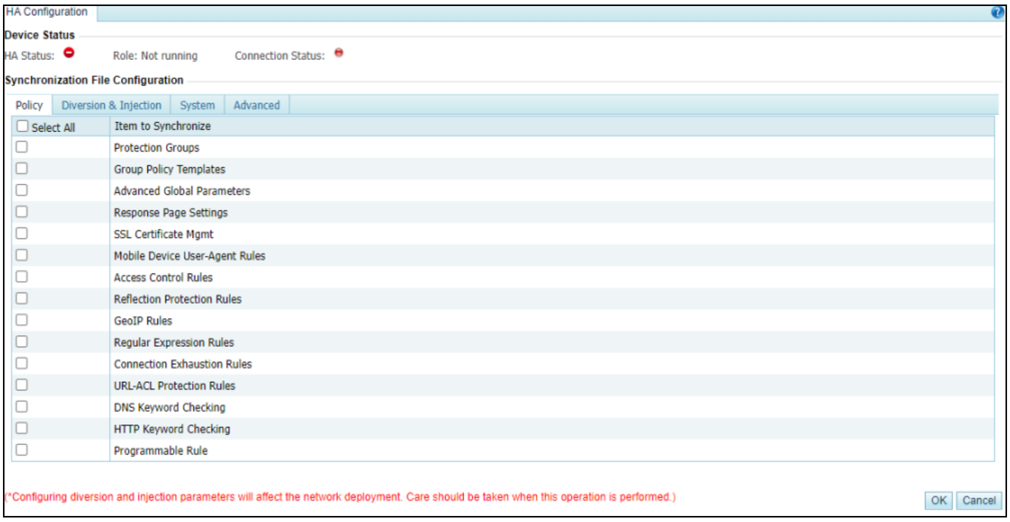
To specify policy configurations to be synchronized, perform the following steps:

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

The **Policies** tab page is displayed by default in the **Synchronization File Configuration** area, as shown in Figure 3-16.

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

Figure 3-20 Policy configurations to be synchronized



HA Configuration

Device Status

HA Status: ● Role: Not running Connection Status: ●

Synchronization File Configuration

□ Select All	Item to Synchronize
□	Protection Groups
□	Group Policy Templates
□	Advanced Global Parameters
□	Response Page Settings
□	SSL Certificate Mgmt
□	Mobile Device User-Agent Rules
□	Access Control Rules
□	Reflection Protection Rules
□	GeoIP Rules
□	Regular Expression Rules
□	Connection Exhaustion Rules
□	URL-ACL Protection Rules
□	DNS Keyword Checking
□	HTTP Keyword Checking
□	Programmable Rule

(*Configuring diversion and injection parameters will affect the network deployment. Care should be taken when this operation is performed.)

Step 3 Select the desired configuration(s) and click **OK**.

----End

Diversion and Injection

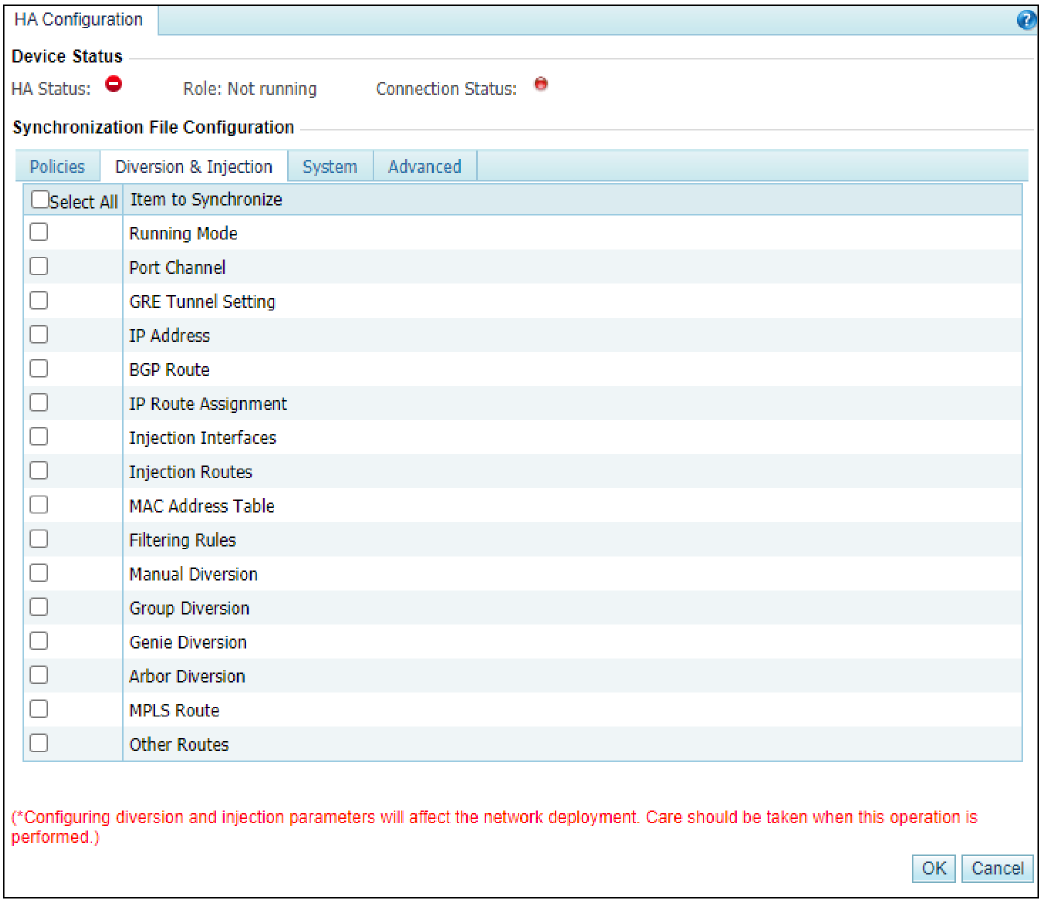
To specify diversion and injection configurations to be synchronized, perform the following steps:

Step 1 On the page shown in Figure 3-16, click the **Diversion & Injection** tab.

Caution

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

Figure 3-21 Diversion and injection configurations to be synchronized



HA Configuration

Device Status

HA Status: ● Role: Not running Connection Status: ●

Synchronization File Configuration

Policies | Diversion & Injection | System | Advanced

□Select All	Item to Synchronize
□	Running Mode
□	Port Channel
□	GRE Tunnel Setting
□	IP Address
□	BGP Route
□	IP Route Assignment
□	Injection Interfaces
□	Injection Routes
□	MAC Address Table
□	Filtering Rules
□	Manual Diversion
□	Group Diversion
□	Genie Diversion
□	Arbor Diversion
□	MPLS Route
□	Other Routes

(*Configuring diversion and injection parameters will affect the network deployment. Care should be taken when this operation is performed.)

OK Cancel

Step 2 Select the desired configuration(s) and click **OK**.

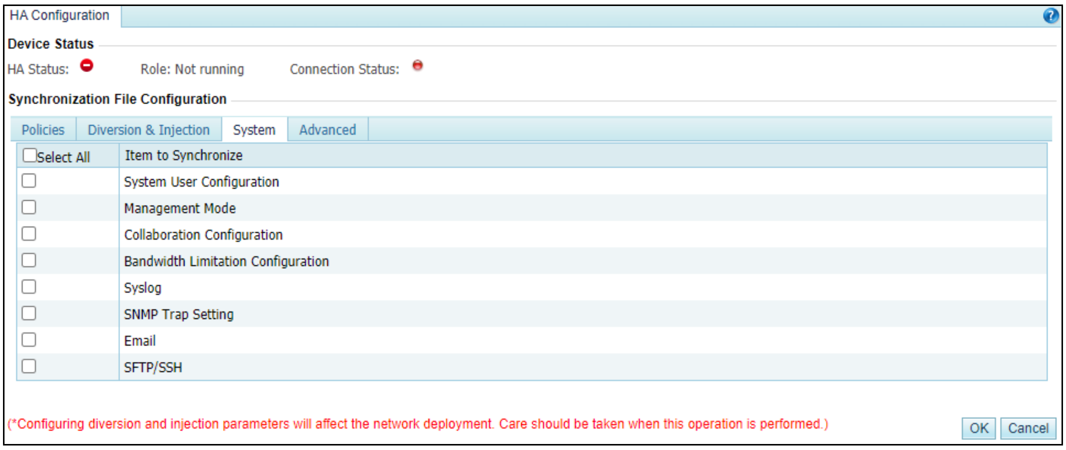
----End

System

To specify system configurations to be synchronized, perform the following steps:

Step 1 On the page shown in Figure 3-20, click the **System** tab.

Figure 3-22 System configurations to be synchronized



HA Configuration

Device Status

HA Status: ● Role: Not running Connection Status: ●

Synchronization File Configuration

□Select All	Item to Synchronize
□	System User Configuration
□	Management Mode
□	Collaboration Configuration
□	Bandwidth Limitation Configuration
□	Syslog
□	SNMP Trap Setting
□	Email
□	SFTP/SSH

(*Configuring diversion and injection parameters will affect the network deployment. Care should be taken when this operation is performed.)

Step 2 Select the desired configuration(s) and click **OK**.

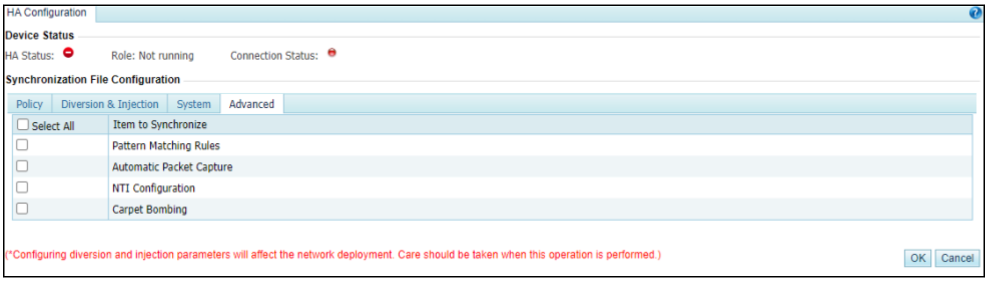
----End

Advanced Configuration

To specify advanced configurations to be synchronized, perform the following steps:

Step 1 On the page shown in Figure 3-20, cllick the **Advanced** tab.

Figure 3-23 Advanced configurations to be synchronized



HA Configuration

Device Status

HA Status: ● Role: Not running Connection Status: ●

Synchronization File Configuration

□Select All	Item to Synchronize
□	Pattern Matching Rules
□	Automatic Packet Capture
□	NTI Configuration
□	Carpet Bombing

(*Configuring diversion and injection parameters will affect the network deployment. Care should be taken when this operation is performed.)

Step 2 Select the desired configuration(s) and click **OK**.

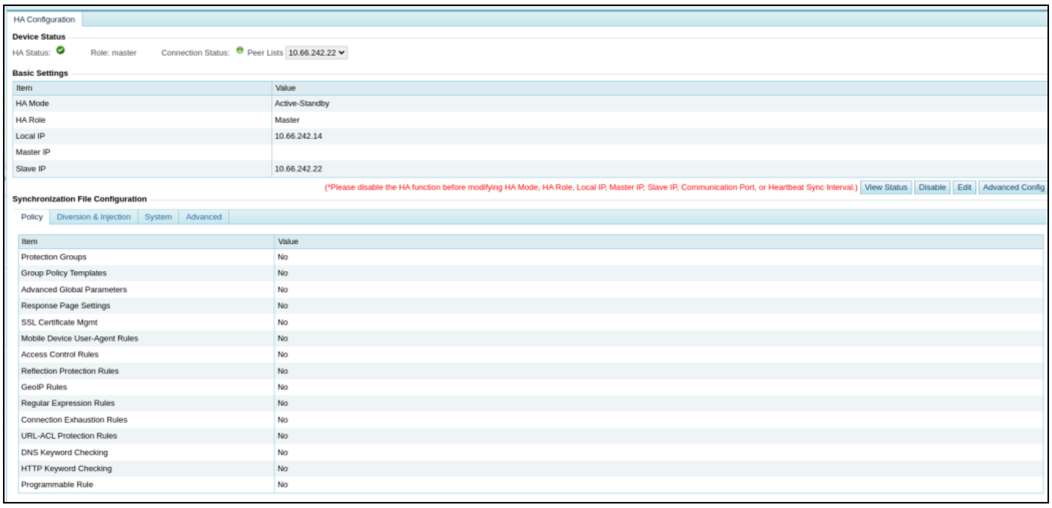
----End

Enabling HA

After completing basic HA settings and file synchronization configuration on both the primary and secondary 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 3-16.

After HA is enabled, the **HA Configuration** tab page on a primary device is as shown in Figure 3-24, and that on a secondary device is as shown in Figure 3-25.

Figure 3-24 HA Configuration page on a primary device

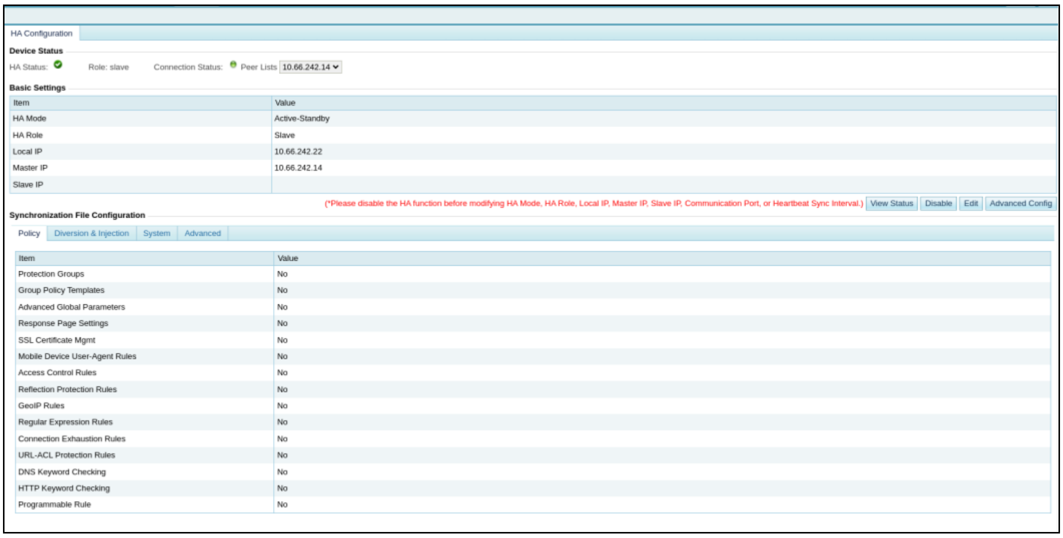


Item	Value
HA Mode	Active-Standby
HA Role	Master
Local IP	10.66.242.14
Master IP	
Slave IP	10.66.242.22

(*Please disable the HA function before modifying HA Mode, HA Role, Local IP, Master IP, Slave IP, Communication Port, or Heartbeat Sync Interval.)

Item	Value
Protection Groups	No
Group Policy Templates	No
Advanced Global Parameters	No
Response Page Settings	No
SSL Certificate Mgmt	No
Mobile Device User-Agent Rules	No
Access Control Rules	No
Reflection Protection Rules	No
GeoIP Rules	No
Regular Expression Rules	No
Connection Exhaustion Rules	No
URL-ACL Protection Rules	No
DNS Keyword Checking	No
HTTP Keyword Checking	No
Programmable Rule	No

Figure 3-25 HA Configuration page on a secondary device



Item	Value
HA Mode	Active-Standby
HA Role	Slave
Local IP	10.66.242.22
Master IP	10.66.242.14
Slave IP	

(*Please disable the HA function before modifying HA Mode, HA Role, Local IP, Master IP, Slave IP, Communication Port, or Heartbeat Sync Interval.)

Item	Value
Protection Groups	No
Group Policy Templates	No
Advanced Global Parameters	No
Response Page Settings	No
SSL Certificate Mgmt	No
Mobile Device User-Agent Rules	No
Access Control Rules	No
Reflection Protection Rules	No
GeoIP Rules	No
Regular Expression Rules	No
Connection Exhaustion Rules	No
URL-ACL Protection Rules	No
DNS Keyword Checking	No
HTTP Keyword Checking	No
Programmable Rule	No

Disabling HA

After HA is enabled, in the lower-right corner of the **Basic Settings** area on the **HA Configuration** page shown in Figure 3-16, 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**.

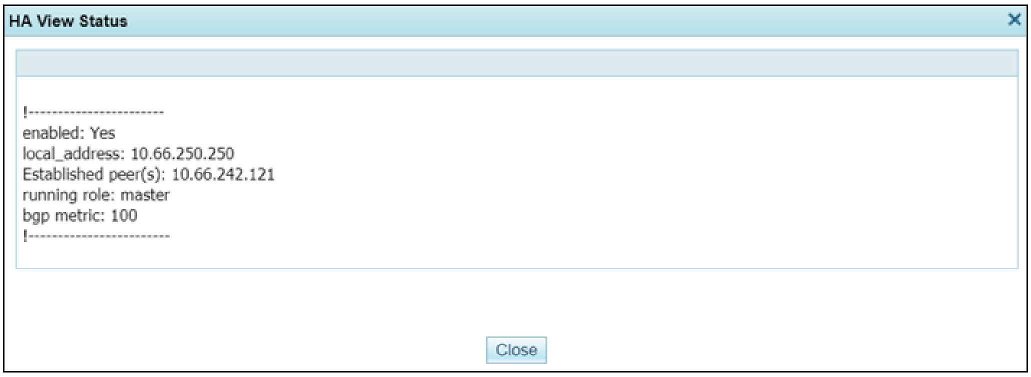
Viewing HA Status

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 3-16.

To view the detailed status of HA configuration, you can click **View Status** in the lower-right corner of the **Basic Settings** area shown in Figure 3-16.

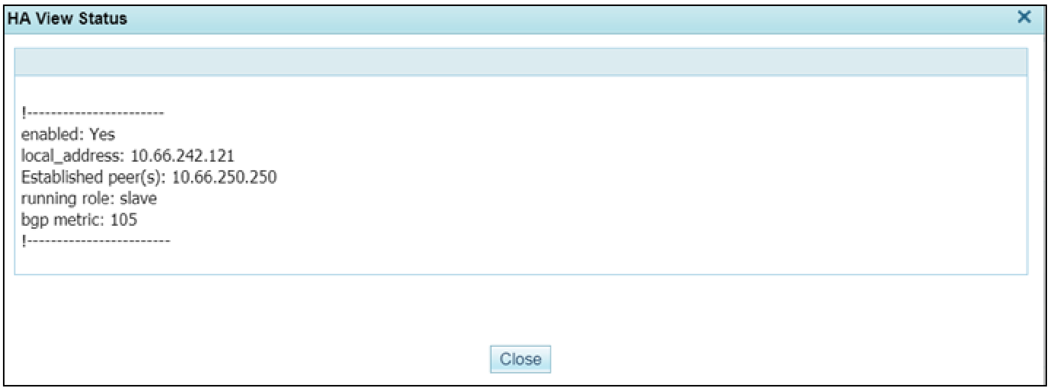
Figure 3-26 shows the HA status information of a primary device in active-standby mode, and Figure 3-27 shows that of a secondary device in active-standby mode.

Figure 3-26 HA status information of a primary device



```
!-----------------------
enabled: Yes
local_address: 10.66.250.250
Established peer(s): 10.66.242.121
running role: master
bgp metric: 100
!------------------------
```

Figure 3-27 HA status information of a secondary device



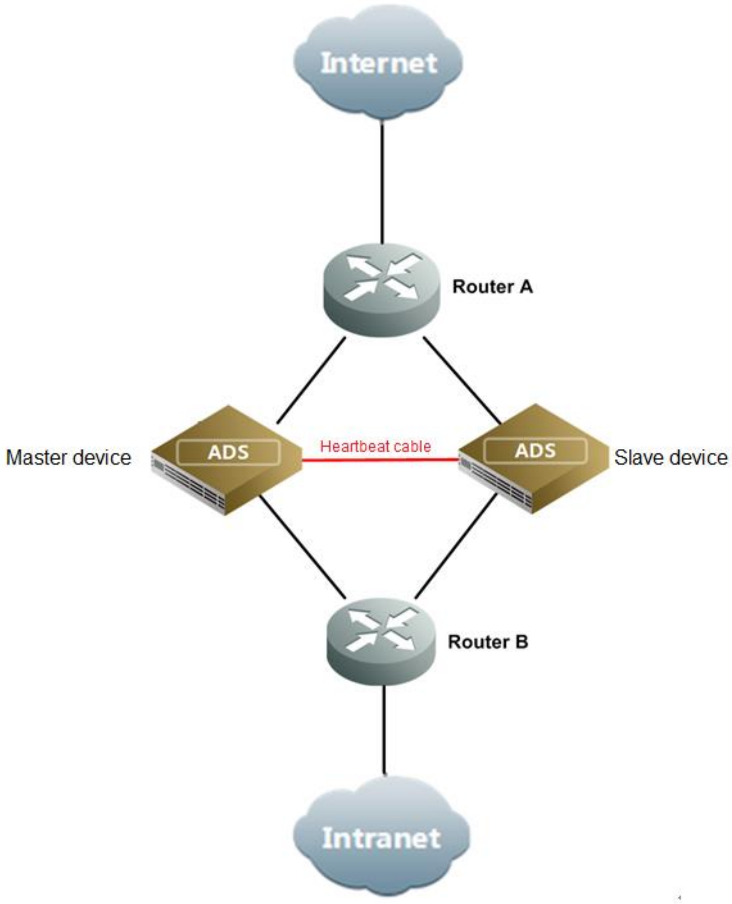
```
!-----------------------
enabled: Yes
local_address: 10.66.242.121
Established peer(s): 10.66.250.250
running role: slave
bgp metric: 105
!------------------------
```

3.1.9.2 HA Configuration on ADS in In-Path Mode

On ADS in in-path mode, if the bypass function is enabled，the HA function is unavailable.

When ADS is deployed in in-path mode, the topology for it to implement HA is as shown in Figure 3-28.

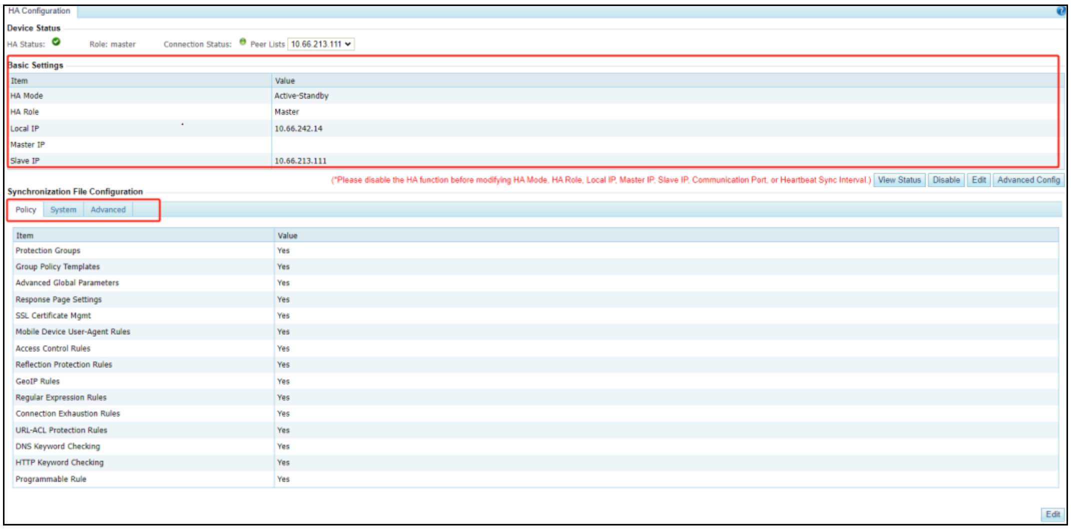
Figure 3-28 Network topology for ADS in in-path mode to implement HA



HA configuration on ADS in in-path mode is similar to that on ADS in out-of-path mode. For details, see section 3.1.9.1 HA Configuration on ADS in Out-of-Path Mode. Note the following differences in the **HA Configuration** page:

- **Advanced Configurations**: **Check Exception over Diversion and Injection Interfaces** and **Syn Diversion Config After Entering a Cluster** are unavailable on ADS in in-path mode.
- **Synchronization File Configuration**: The **Diversion & Injection** tab is unavailable on ADS in in-path mode.

Figure 3-29 HA configuration on ADS in in-path mode



Device Status

HA Status: ✓ Role: master Connection Status: ● Peer Lists 10.66.213.111

Basic Settings

Item	Value
HA Mode	Active-Standby
HA Role	Master
Local IP	10.66.242.14
Master IP	
Slave IP	10.66.213.111

(*Please disable the HA function before modifying HA Mode, HA Role, Local IP, Master IP, Slave IP, Communication Port, or Heartbeat Sync Interval.)

Synchronization File Configuration

Item	Value
Protection Groups	Yes
Group Policy Templates	Yes
Advanced Global Parameters	Yes
Response Page Settings	Yes
SSL Certificate Mgmt	Yes
Mobile Device User-Agent Rules	Yes
Access Control Rules	Yes
Reflection Protection Rules	Yes
GeoIP Rules	Yes
Regular Expression Rules	Yes
Connection Exhaustion Rules	Yes
URL-ACL Protection Rules	Yes
DNS Keyword Checking	Yes
HTTP Keyword Checking	Yes
Programmable Rule	Yes

3.1.10 (Optional) Bypass Configuration

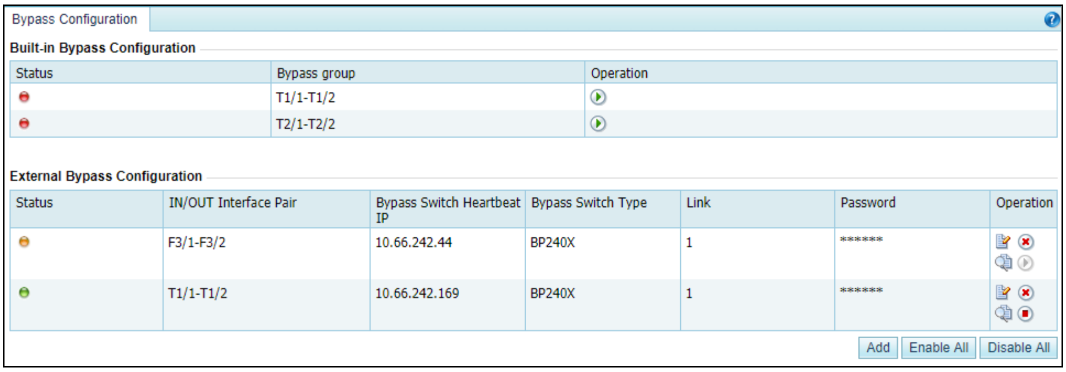
The bypass function is available only for ADS devices running in in-path mode. Currently, ADS NX5-10000 and NX1-VN do not support bypass configuration.

Note	On ADS in in-path mode, if the HA function is enabled, the bypass function is unavailable.

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

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

Figure 3-30 Bypass Configuration page



Built-in Bypass Configuration

Status	Bypass group	Operation
●	T1/1-T1/2	▶
●	T2/1-T2/2	▶

External Bypass Configuration

Status	IN/OUT Interface Pair	Bypass Switch Heartbeat IP	Bypass Switch Type	Link	Password	Operation
●	F3/1-F3/2	10.66.242.44	BP240X	1	******	✎ ⊗ ▶
●	T1/1-T1/2	10.66.242.169	BP240X	1	******	✎ ⊗ ■

Note that the **Link** column appears in the table, indicating the link ID of the external bypass switch, only when the switch type is **BP240X**.

3.1.10.1 Built-in Bypass

The built-in bypass function is disabled by default, as shown in Figure 3-30. You can specify an interface group as built-in bypass interfaces.

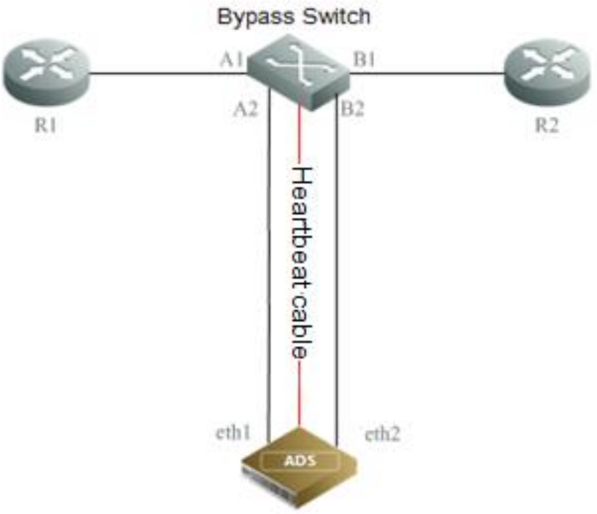
- To enable this function, click ▶ in the **Operation** column. Then the indicator in the **Status** column turns to ●, indicating that the built-in bypass function is enabled. At the same time, the button in the **Operation** column turns to ■.
- To disable this function, click ■ in the **Operation** 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 in in-path mode. External bypass devices from NSFOCUS are called NSF-BS.

Figure 3-31 shows the topology for the interaction between ADS and the bypass switch.

Figure 3-31 Topology for the interaction between ADS and the bypass switch



When any of the following occurs:

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

the associated working interfaces are 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.

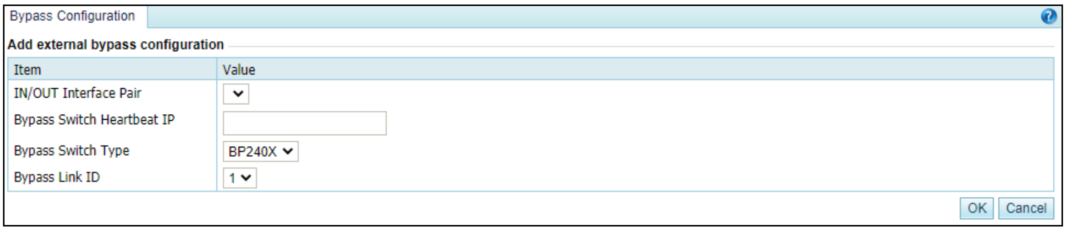
Caution	In in-path mode, ADS enters the bypass state by default when started. If you want ADS to implement protection, you must manually disable the external bypass so that ADS can switch to the normal protection state.

Choose **System** > **Local Settings** > **Bypass Configuration**. In the **External Bypass** area shown in Figure 3-30, 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 3-32.

Figure 3-32 Adding an external bypass group



Bypass Configuration

Add external bypass configuration

Item	Value
IN/OUT Interface Pair	
Bypass Switch Heartbeat IP	
Bypass Switch Type	BP240X
Bypass Link ID	1

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.
Bypass Switch Type	Specifies a model of the external bypass switch, which can be **BP240X**, **BP2301**, **BP2201**, or **BP2100**.
Bypass Link ID	Specifies the link ID of the external bypass switch. This is available only when **BP240X** is selected as the bypass switch. Other models support only one link by default.
Password	Password used for login to the bypass switch. This is available only when **BP2100** is selected as the bypass switch. For the password, refer to the related user guide shipped with the switch.
Confirm Password	Login password typed for confirmation. This is available only when **BP2100** is selected as the bypass switch.

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.

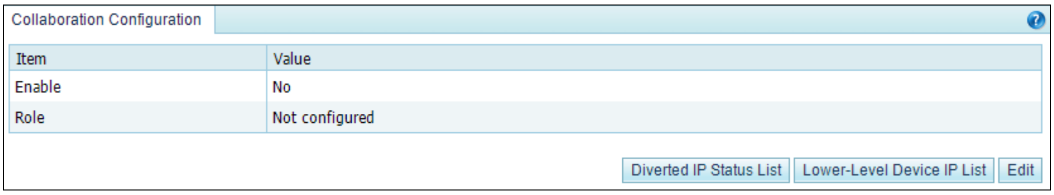
3.1.11 Collaboration Configuration

Note	ADS NX5-10000 does not support collaboration configuration.

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 3-33.

Figure 3-33 Collaboration Configuration page



Collaboration Configuration

Item	Value
Enable	No
Role	Not configured

3.1.11.1 Managing Upper-Level ADS Devices

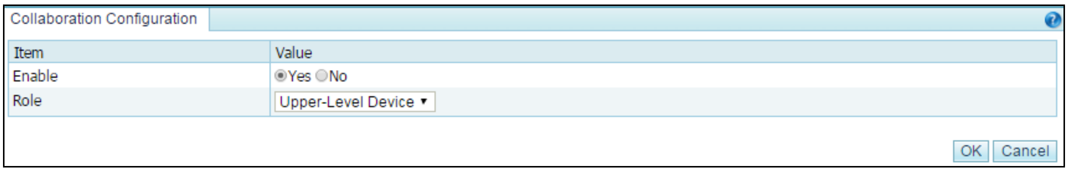
Configuring an Upper-Level ADS

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

Step 1 On the **Collaboration Configuration** page shown in Figure 3-33, click **Edit** and set **Enable** to **Yes** and **Role** to **Upper-Level Device**, as shown in Figure 3-34.

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

Figure 3-34 Configuring an upper-level ADS



Collaboration Configuration

Item	Value
Enable	● Yes ○ No
Role	Upper-Level Device ▾

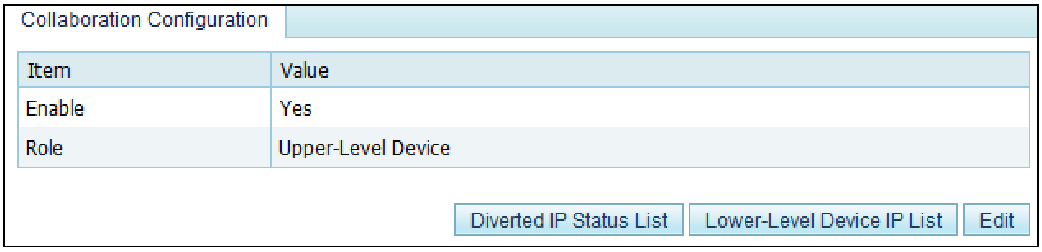
Table 3-14 describes parameters for configuring an upper-level ADS.

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. Note To enable collaboration, you need to set **Enable** to **Yes** in the **Management Mode** area (**System** > **Local Settings** > **Management Mode**). 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 3-35 Collaboration Configuration page



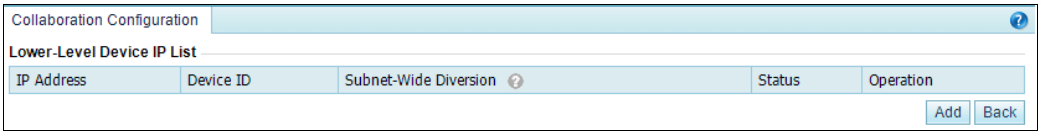
Collaboration Configuration

Item	Value
Enable	Yes
Role	Upper-Level Device

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

IP addresses of lower-level ADS devices are displayed. See Figure 3-36.

Figure 3-36 List of IP addresses of lower-level devices



Collaboration Configuration

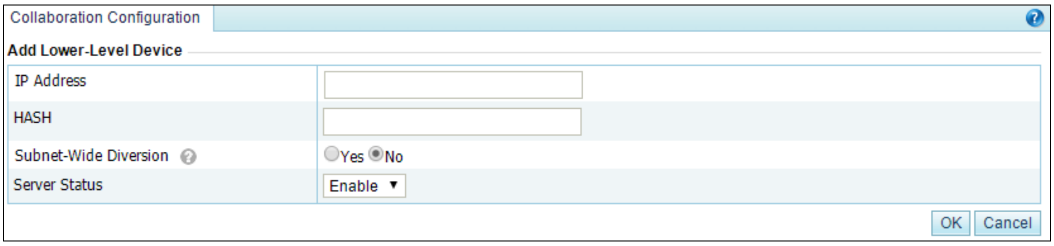
Lower-Level Device IP List

IP Address	Device ID	Subnet-Wide Diversion	Status	Operation

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 3-37 Adding a lower-level ADS



Add Lower-Level Device

IP Address	
HASH	
Subnet-Wide Diversion	○ Yes ● No
Server Status	Enable ▼

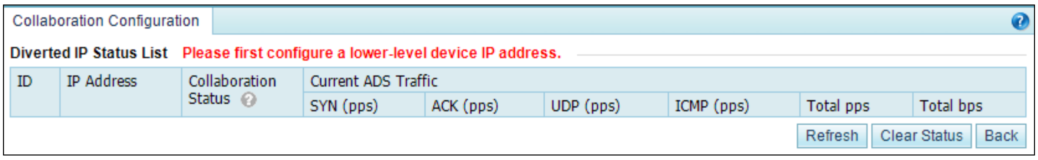
Step 5 Click **OK** to complete the configuration.

----End

Viewing Diverted IP Status List

On the **Collaboration Configuration** page shown in Figure 3-33, 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 3-38 Viewing diverted traffic



Diverted IP Status List Please first configure a lower-level device IP address.

ID	IP Address	Collaboration Status	Current ADS Traffic					
			SYN (pps)	ACK (pps)	UDP (pps)	ICMP (pps)	Total pps	Total bps

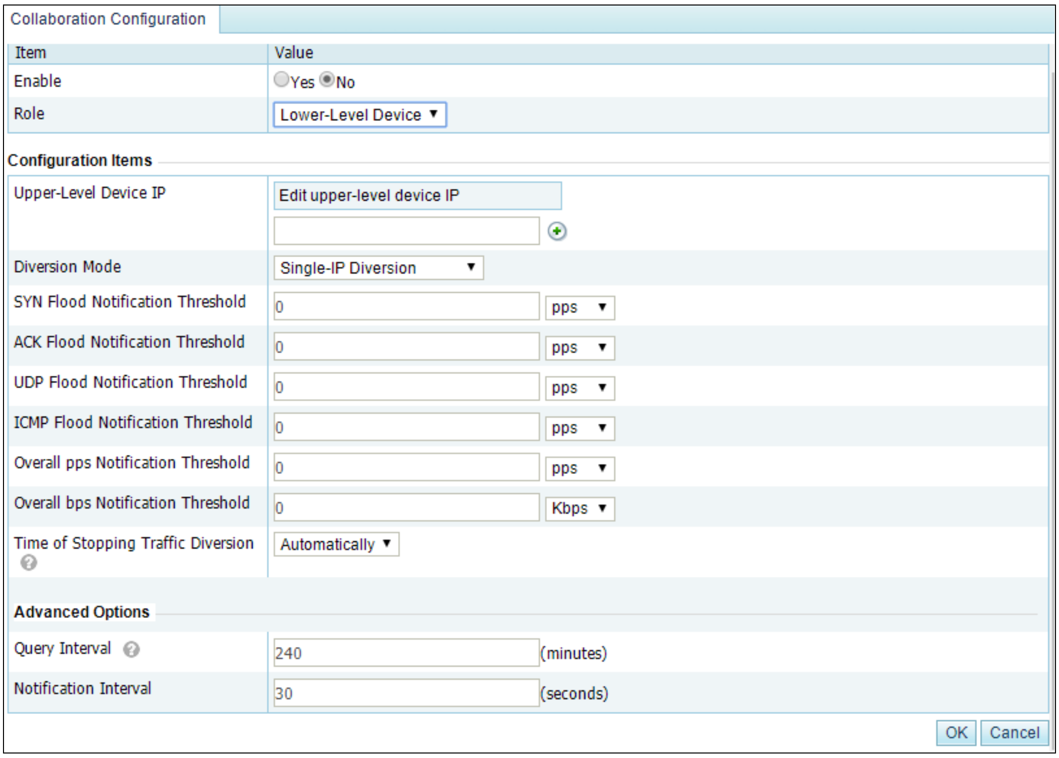
3.1.11.2 Managing Lower-Level ADS Devices

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 3-33, click **Edit** and set **Enable** to **Yes** and **Role** to **Lower-Level Device**, as shown in Figure 3-39.

Figure 3-39 Configuring a lower-level ADS



Collaboration Configuration

Item	Value
Enable	○ Yes ● No
Role	Lower-Level Device ▼

Configuration Items

Upper-Level Device IP	Edit upper-level device IP
Diversion Mode	Single-IP Diversion ▼
SYN Flood Notification Threshold	0 pps ▼
ACK Flood Notification Threshold	0 pps ▼
UDP Flood Notification Threshold	0 pps ▼
ICMP Flood Notification Threshold	0 pps ▼
Overall pps Notification Threshold	0 pps ▼
Overall bps Notification Threshold	0 Kbps ▼
Time of Stopping Traffic Diversion	Automatically ▼

Advanced Options

Query Interval	240 (minutes)
Notification Interval	30 (seconds)

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

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

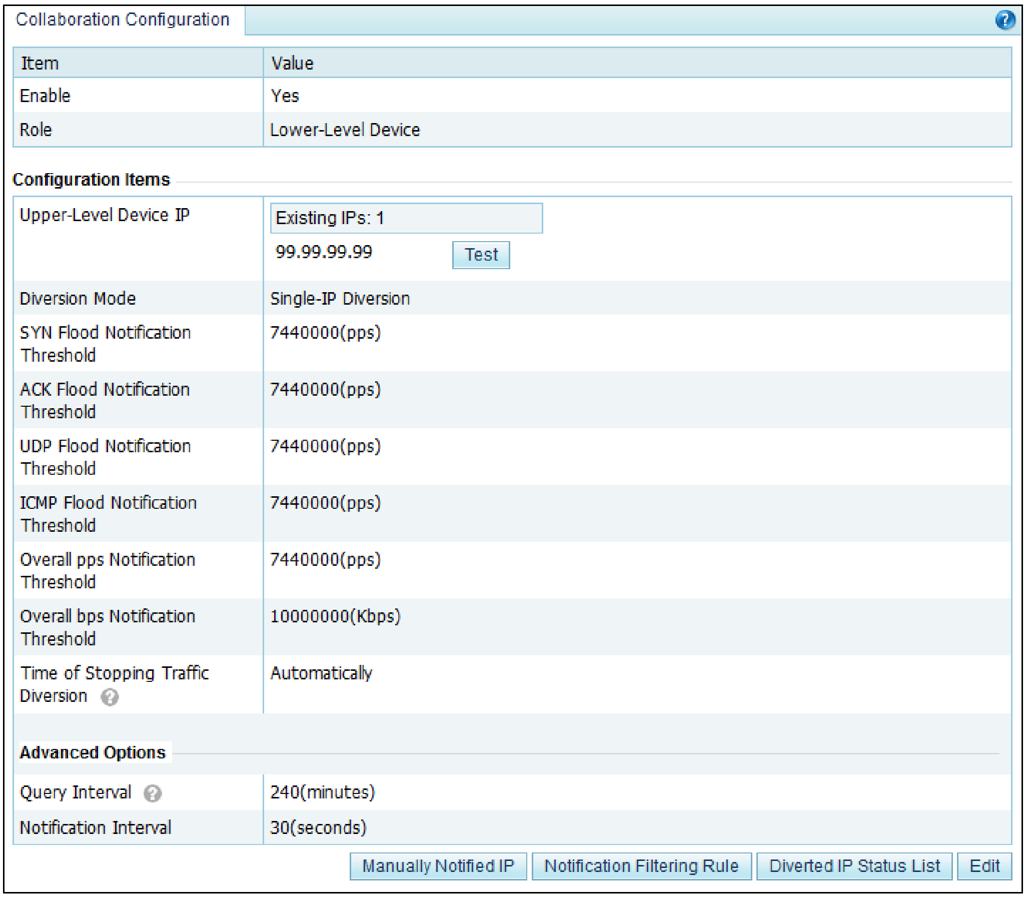
Parameter	Description
Enable	Controls whether to enable collaboration between lower-level and upper-level ADS devices. • **Yes**: enables the collaboration function. • **No**: disables the collaboration function. Note The lower-level device instructs the upper-level ADS to divert traffic when finding 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. Note that the IP segment 172.16.1.0/24 is reserved for internal communication.
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. • **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 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

Parameter	Description
Threshold	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 3-40.

Figure 3-40 Lower-level ADS configuration



Item	Value
Enable	Yes
Role	Lower-Level Device

Configuration Items

Upper-Level Device IP	Existing IPs: 1 99.99.99.99
Diversion Mode	Single-IP Diversion
SYN Flood Notification Threshold	7440000(pps)
ACK Flood Notification Threshold	7440000(pps)
UDP Flood Notification Threshold	7440000(pps)
ICMP Flood Notification Threshold	7440000(pps)
Overall pps Notification Threshold	7440000(pps)
Overall bps Notification Threshold	10000000(Kbps)
Time of Stopping Traffic Diversion	Automatically

Advanced Options

Query Interval	240(minutes)
Notification Interval	30(seconds)

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

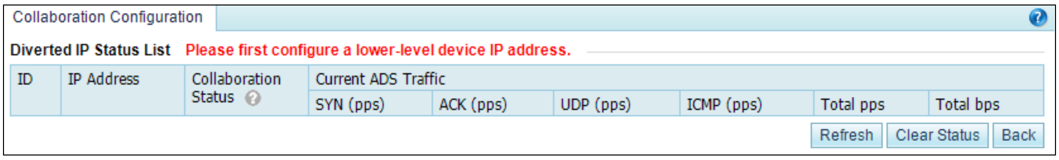
If the icon ✓ appears to the left of the **Test** button, the connection succeeds.

----End

Viewing Diverted IP Status List

On the **Collaboration Configuration** page shown in Figure 3-40, click **Diverted IP Status List** to view the current traffic on the upper-level and lower-level ADS devices. See Figure 3-41.

Figure 3-41 Status of diverted traffic



Diverted IP Status List Please first configure a lower-level device IP address.

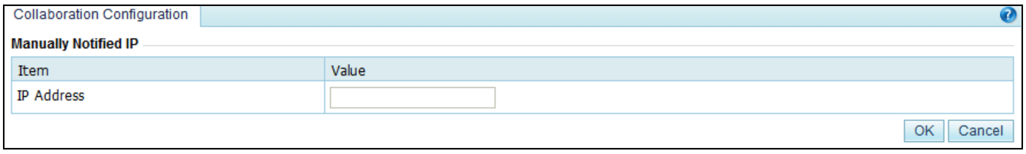
ID	IP Address	Collaboration Status	Current ADS Traffic					
			SYN (pps)	ACK (pps)	UDP (pps)	ICMP (pps)	Total pps	Total bps

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 3-40, click **Manually Notified IP**.

Figure 3-42 Configuring manually notified IP addresses



Manually Notified IP

Item	Value
IP Address	

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

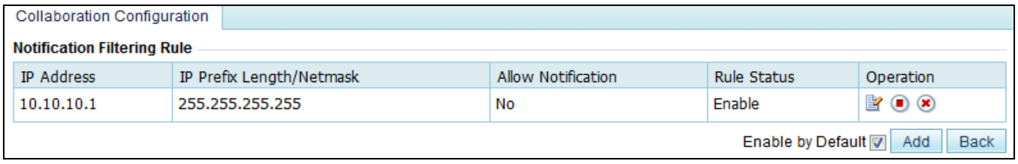
Configuring Notification Filtering Rules

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 3-40, click **Notification Filtering Rule**.

Figure 3-43 Notification filtering rule page

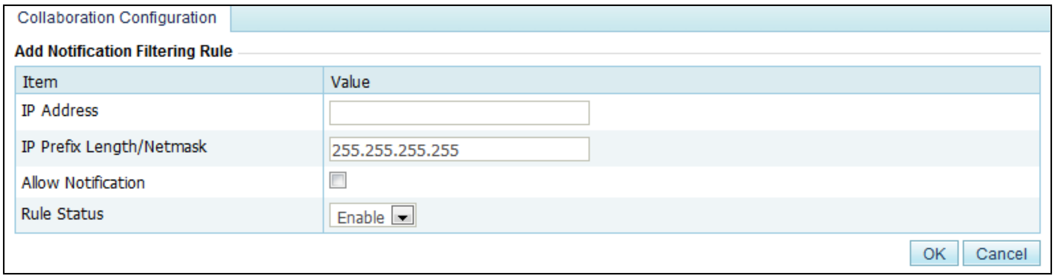


Notification Filtering Rule

IP Address	IP Prefix Length/Netmask	Allow Notification	Rule Status	Operation
10.10.10.1	255.255.255.255	No	Enable	

Step 2 Click **Add**.

Figure 3-44 Adding a notification filtering rule



Add Notification Filtering Rule

Item	Value
IP Address	
IP Prefix Length/Netmask	255.255.255.255
Allow Notification	□
Rule Status	Enable

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. • **Enable**: enables this rule. • **Disable**: 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

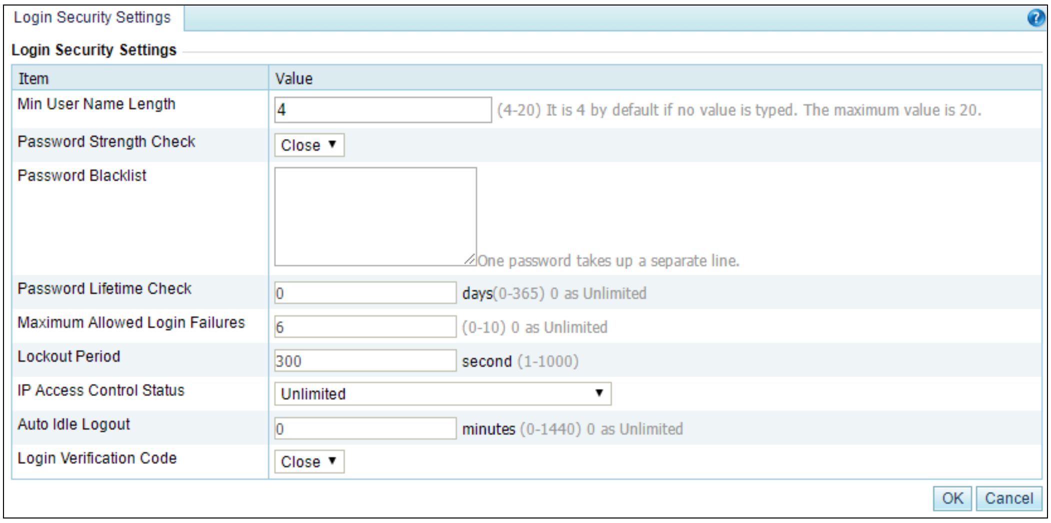
3.2.1 Login Security Settings

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 3-45.

Figure 3-45 Configuring login security parameters



Login Security Settings

Login Security Settings

Item	Value
Min User Name Length	4 (4-20) It is 4 by default if no value is typed. The maximum value is 20.
Password Strength Check	Close
Password Blacklist	One password takes up a separate line.
Password Lifetime Check	0 days(0-365) 0 as Unlimited
Maximum Allowed Login Failures	6 (0-10) 0 as Unlimited
Lockout Period	300 second (1-1000)
IP Access Control Status	Unlimited
Auto Idle Logout	0 minutes (0-1440) 0 as Unlimited
Login Verification Code	Close

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	Blocked 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.

Parameter	Description
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 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

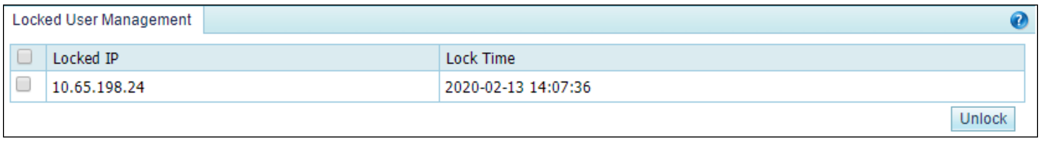
A user's account will be automatically locked after the number of failed login attempts exceeds the specified value. During the lockout period, the user cannot log in again. After the lockout period expires, the account will be automatically unlocked. You can also go to the **Locked User Management** 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 3-46 Locked User Management page



Locked User Management

□	Locked IP	Lock Time
□	10.65.198.24	2020-02-13 14:07:36

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 password authentication modes are supported:

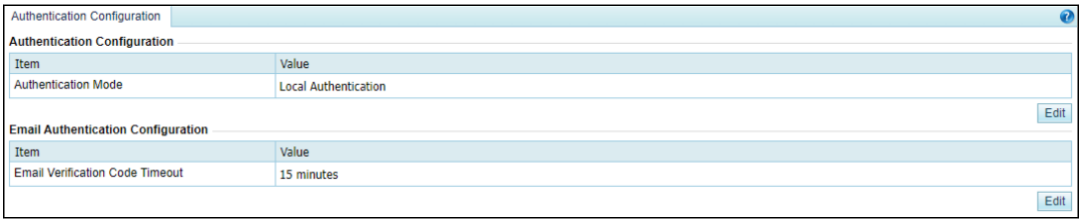
- Local authentication: The user can log in to ADS only if a correct user name and password are entered. The system user **admin** can only be locally authenticated.
- Radius authentication: The user can log in to ADS only if a correct user name, password, and key are entered. After **Authentication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

In addition to password authentication, a user can be authenticated by password + email or password + certificate. For the password + email authentication, the user can log in to ADS after typing a correct password and verification code provided via email. For the password + certificate authentication, the user can log in to ADS after typing a correct password and providing a the UKey certificate.

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

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

Figure 3-47 Authentication Configuration page



Authentication Configuration

Authentication Configuration

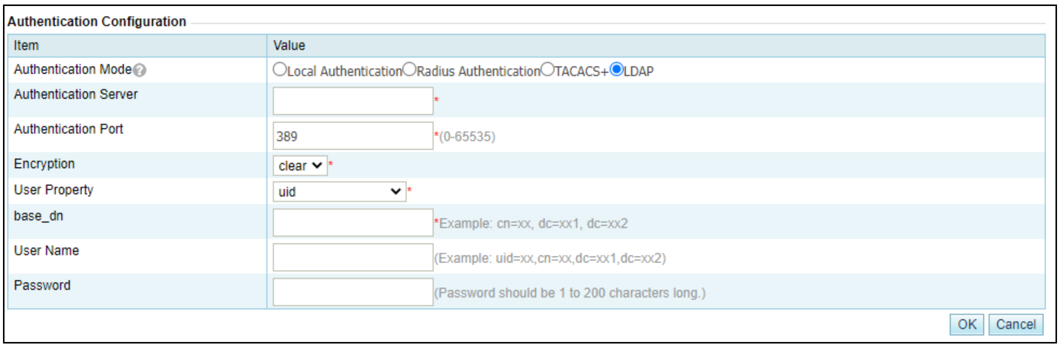
Item	Value
Authentication Mode	Local Authentication

Email Authentication Configuration

Item	Value
Email Verification Code Timeout	15 minutes

Step 2 Click **Edit** in the **Authentication Configuration** area to configure the authentication mode.

Figure 3-48 Editing authentication parameters



Authentication Configuration

Item	Value
Authentication Mode	○Local Authentication ○Radius Authentication ○TACACS+ ●LDAP
Authentication Server	*
Authentication Port	389 *(0-65535)
Encryption	clear *
User Property	uid *
base_dn	*Example: cn=xx, dc=xx1, dc=xx2
User Name	(Example: uid=xx,cn=xx,dc=xx1,dc=xx2)
Password	(Password should be 1 to 200 characters long.)

Table 3-18 Parameters for configuring the authentication mode

Parameter	Description
Authentication Mode	Specifies the authentication mode, which can be **Local Authentication**, **Radius Authentication**, **TACACS+**, or **LDAP**.
Authentication Server	Specifies the IP address or domain name of the authentication server. Both IPv4 and IPv6 addresses are supported. Note You can enter a domain name when the **Authentication Mode** is set to **LDAP**.
Authentication Port	Specifies the port on which the authentication server listens for authentication requests.
Protocol	Specifies the authentication protocol of the authentication server. The options vary with the authentication server. Note This parameter is required when the **Authentication Mode** is set to **Radius Authentication or TACACS+**.
Shared Key	Specifies the shared key that serves as a password of the authentication server. The shared key configured on ADS must be the same as that configured on the authentication server; otherwise, ADS cannot communicate with the server. Note This parameter is required when the **Authentication Mode** is set to **Radius Authentication or TACACS+**.
Authentication Duration	Specifies the authentication duration, after which ADS returns the success or failure of the authentication information. Note This parameter is required when the **Authentication Mode** is set to **Radius Authentication or TACACS+**.

Parameter	Description
Encryption	Specifies the encryption mode of the LDAP network communication. Options include: • **clear**: plaintext communication; • **ssl**: SSL-encrypted communication; • **tls**: TLS-encrypted communication; Note This parameter is required when the **Authentication Mode** is set to **LDAP**.
User Property	Specifies the user authentication mode, which varies with the authentication server. For a Linux authentication server, the value can be **uid**, **cn**, or **displayName. For a Windows authentication server, the value can be sAMAccountName** or **displayName** Note This parameter is required when the **Authentication Mode** is set to **LDAP**.
base_dn	Specifies the top of the LDAP directory tree, namely, the base directory. Note This parameter is required when the **Authentication Mode** is set to **LDAP**.
User Name	Specifies the name of the LDAP user. Note This parameter is optional when the **Authentication Mode** is set to **LDAP**.
User Password	Specifies the password of the LDAP user. Note This parameter is optional when the **Authentication Mode** is set to **LDAP**.

Step 3 Click **OK** to save the authentication configuration.

Step 4 Click **Edit** in the **Email Authentication Configuration area** to set the email verification code timeout to 1–180 minutes. The default value is **15** minutes.

Step 5 Click **OK**.

----End

3.3 Log Services

This section covers the following topics:

- Syslog Configuration
- SNMP Configuration

- Email Configuration
- SFTP/SSH Configuration

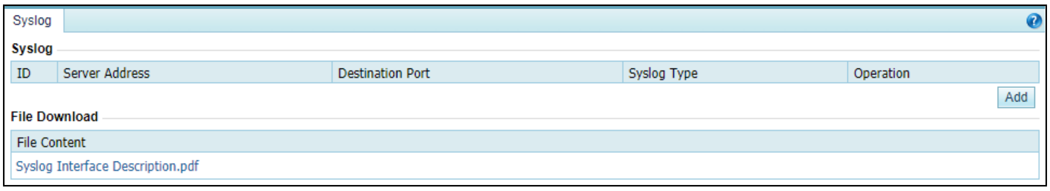
3.3.1 Syslog Configuration

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 3-49, you can click the file name in the **File Download** area to download the syslog file to a local disk drive.

Figure 3-49 Configuring syslog



Syslog

Syslog

ID	Server Address	Destination Port	Syslog Type	Operation

File Download

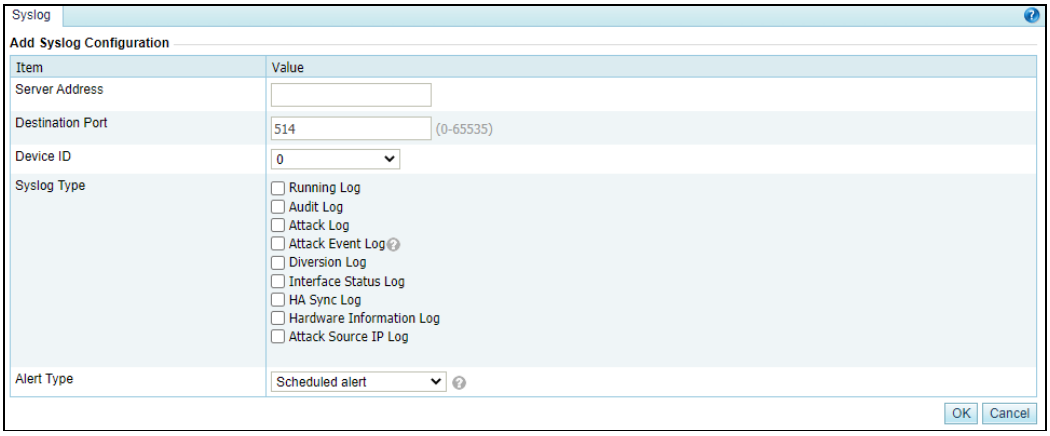
File Content
Syslog Interface Description.pdf

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 3-50 Configuring a syslog server



Syslog

Add Syslog Configuration

Item	Value
Server Address	
Destination Port	514 (0-65535)
Device ID	0
Syslog Type	□ Running Log □ Audit Log □ Attack Log □ Attack Event Log □ Diversion Log □ Interface Status Log □ HA Sync Log □ Hardware Information Log □ Attack Source IP Log
Alert Type	Scheduled alert

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 • Diversion log • Interface status log • HA sync log • Hardware information log • Attack source IP 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. Note • 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). SNMPv2c and SNMPv3 are supported.

- SNMP trap: configures ADS to collect trap messages, namely SNMP server-related information. SNMPv2c and SNMPv3 are supported.

The difference between SNMPv3 and SNMPv2c is that the latter does not encrypt authentication and management data in transit and has no authentication mechanism for data sending and transmission and so is not so secure for network management.

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

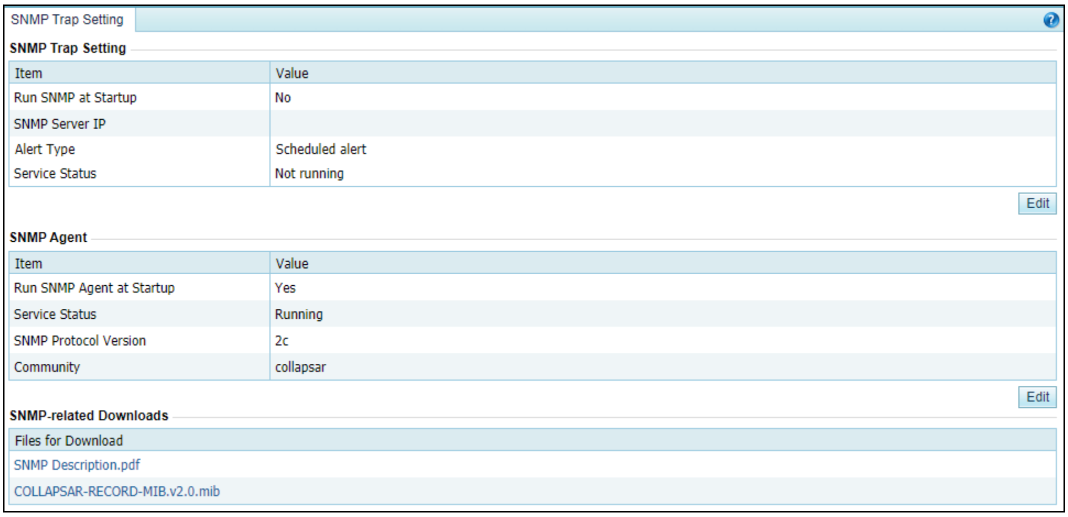
To configure SNMP, perform the following steps:

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

The **SNMP Trap Setting** page appears, as shown in Figure 3-51.

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 3-51 SNMP Trap Setting page



SNMP Trap Setting

SNMP Trap Setting

Item	Value
Run SNMP at Startup	No
SNMP Server IP	
Alert Type	Scheduled alert
Service Status	Not running

SNMP Agent

Item	Value
Run SNMP Agent at Startup	Yes
Service Status	Running
SNMP Protocol Version	2c
Community	collapsar

SNMP-related Downloads

Files for Download
SNMP Description.pdf
COLLAPSAR-RECORD-MIB.v2.0.mib

Step 2 Click **Edit** in the **SNMP Trap Setting** area to modify SNMP Trap parameters.

Table 3-20 and Table 3-21 describe SNMP Trap parameters.

Table 3-20 SNMPv2c 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 Protocol Version	SNMP protocol supported by the SNMP agent. Set it to **v2c**.
SNMP Server IP	IPv4 or IPv6 address of the SNMP server. At most two server IP addresses can be specified to receive logs via SNMP traps.
Alert Type	Specifies the type of alerts, which can be either of the following:

Parameter	Description
	• **Scheduled alert**: sends alerts every 30 seconds. • **Threshold exceeding alert**: sends alerts when a threshold is exceeded. Note 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.

Table 3-21 SNMPv3 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 Protocol Version	SNMP protocol supported by the SNMP agent, which is set to **3.**
Authentication Mode	Specifies the authentication modes for different security levels of the SNMPv3 user. The default value is **No identity authentication**. Options include the following: • **No identity authentication**: does not authenticate users and provides no privacy or encryption function. In this case, only **Username** needs to be set. • **Account Authentication**: provides only authentication. In this case, **Username** and **Password** need to be set. • **Private Key Authentication**: provides both authentication and encryption. In this case **Username, Password**, **Authentication Protocol**, **Private Key Protocol**, and **Private Key Password** need to be set.
Username	Specifies the SNMPv3 server user name.
Password	Specifies the password for the SNMPv3 server user.
Authentication Protocol	Specifies the authentication protocol. Options include **MD5** and **SHA**.
Private Key Protocol	Specifies the cipher algorithm for data transmission. Options include **DES** and **AES**.
Private Key Password	Specifies the key used for encryption.
SNMP Server IP	IPv4 or IPv6 address of the SNMP server. At most two server IP addresses can be specified to receive logs via SNMP traps.
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. Note

Parameter	Description
	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.

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

Step 4 **Click Edit in the SNMP Agent** area to modify SNMP agent parameters.

Table 3-22 and Table 3-23 describe SNMP Trap parameters.

Table 3-22 SNMPv2c Agent parameters

Parameter	Description
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.
SNMP Protocol Version	SNMP protocol supported by the SNMP agent, which is set to **2c**.
Community	Community supported by the SNMP agent. When the SNMP agent function is disabled, this parameter is unavailable.
Service Status	Running status of the SNMP agent server.

Table 3-23 SNMPv3 Agent parameters

Parameter	Description
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.
SNMP Protocol Version	SNMP protocol supported by the SNMP agent. Set it to **3**.
Authentication Mode	Specifies the authentication modes for different security levels of the SNMPv3 user. The default value is **No identity authentication**. Options include the following: • **No identity authentication**: does not authenticate users and provides no privacy or encryption function. In this case, only **Username** needs to be set. • **Account Authentication**: provides only authentication. In this case, **Username** and **Password** need to be set. • **Private Key Authentication**: provides both authentication and encryption. In this case **Username, Password**, **Authentication Protocol**, **Private Key Protocol**, and **Private Key Password** need to be set.
Username	Specifies the SNMPv3 server user name.
Password	Specifies the password for the SNMPv3 server user.

Parameter	Description
Authentication Protocol	Specifies the authentication protocol. Options include **MD5** and **SHA**.
Private Key Protocol	Specifies the cipher algorithm for data transmission. Options include **DES** and **AES**.
Private Key Password	Specifies the key used for encryption.
Service Status	Running status of the SNMP agent server

Step 5 Set parameters and click **OK** to save the settings.

----End

3.3.3 Email Configuration

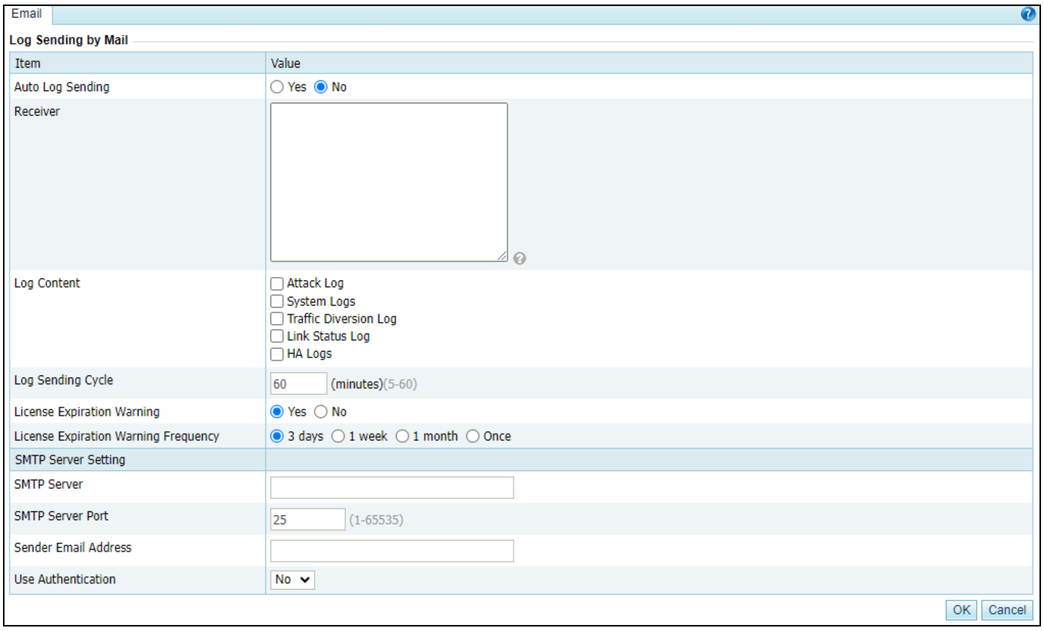
Email configuration is required when ADS is configured to send one or multiple types of log to a specified email address.

To configure email parameters, perform the following steps:

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

Step 1 Click **Edit**.

Figure 3-52 Editing log sending parameters



Email

Log Sending by Mail

Item	Value
Auto Log Sending	○ Yes ● No
Receiver	
Log Content	□ Attack Log □ System Logs □ Traffic Diversion Log □ Link Status Log □ HA Logs
Log Sending Cycle	60 (minutes)(5-60)
License Expiration Warning	● Yes ○ No
License Expiration Warning Frequency	● 3 days ○ 1 week ○ 1 month ○ Once
SMTP Server Setting	
SMTP Server	
SMTP Server Port	25 (1-65535)
Sender Email Address	
Use Authentication	No

Table 3-24 describes parameters for configuring log sending by email.

Table 3-24 Parameters for configuring log sending by email

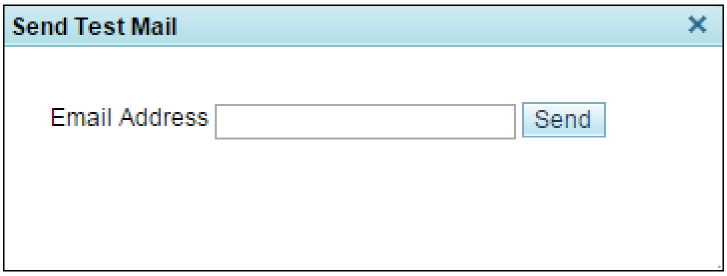
Parameter	Description
Auto Log Sending	Controls whether the system sends the selected logs to a specific email address. The value **Yes** indicates that the system sends the selected logs to a specific email address. If this function is enabled, you need to configure **Receiver** and **Log Content**.
Receiver	Email address that receives logs. A maximum of 10 email addresses are allowed, with each in a separate line.
Log Content	Type of logs to be sent, which can be **Attack Log**, **System Logs**, **Traffic Diversion Log**, **Link Status Log**, and **HA Logs**. 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.
License Expiration Warning	Controls whether to enable the license expiration warning function. If you select **Yes**, alert emails will be sent to users before and after the license expires.
License Expiration Warning Frequency	How often a license expiration warning is sent by email. Options include **3 days**, **1 week**, **1 month**, and **Once**.
SMTP Server	IP address or domain name of the SMTP server that sends emails from ADS to the receiver. You can type either an IPv4 or IPv6 address. At most two server IP addresses can be specified to receive logs via SNMP trap.
SMTP Server Port	Specifies a port for the SMTP server to send emails to the receiver. Value range: 1–65535.
Sender Email Address	Email address that sends logs.
Use Authentication	Specifies whether to authenticate the SMTP user that attempts to send emails. • **Yes**: authenticates the user that attempts to send emails. • **No**: does not authenticate the user that attempts to send emails. If you select **Yes**, you need to configure an SMTP user name and SMTP password.
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 2 Configure parameters and click **OK** to save the settings.

Step 3 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 3-53, type the email address to receive the test mail.

Figure 3-53 Send Test Mail dialog box



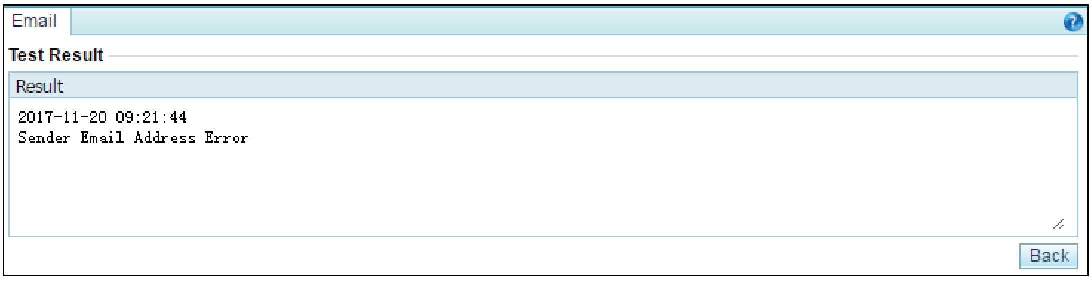
Step 4 Type the receiving address and then click **Send**.

ADS then sends a test mail to the specified address.

Step 5 View the test result.

Click **Test Result**. Then the test result is displayed, as shown in Figure 3-54.

Figure 3-54 Email test result



```
2017-11-20 09:21:44
Sender Email Address Error
```

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.

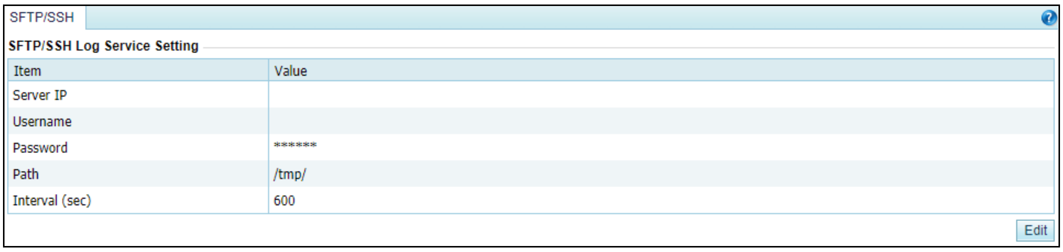
----End

3.3.4 SFTP/SSH Configuration

As shown in Figure 3-55, 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**, and then click **Edit**.

Figure 3-55 Editing SFTP/SSH settings



SFTP/SSH

SFTP/SSH Log Service Setting

Item	Value
Server IP	
Username	
Password	******
Path	/tmp/
Interval (sec)	600

Table 3-25 describes parameters for exporting logs via SFTP or SSH.

Table 3-25 Parameters for exporting logs via SFTP or SSH

Parameter	Description
Server IP	IPv4 or IPv6 address of the SFTP/SSH server that receives logs from ADS.
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 2 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 Inspection
- System Information
- Web API File Download

3.4.1 License

After ADS is installed, you must import a license before using it. License types vary a bit for hardware devices and virtual devices:

- Hardware device: License types include **Trial**, **Interim**, and **Formal**.
- Virtual device (vADS): License types include **Trial**, **Interim**, **Formal**, and **Subscription**.

When a license expires, ADS will provide limited functions, as shown in Table 3-26. What functions are still available depends on the license type.

Table 3-26 Functions available upon license expiry

License Type	Functions Available upon Expiry
Trial	ADS cannot be upgraded and then it will enter the packet forwarding mode, indicating that it will no longer provide protection.
Interim	ADS cannot be upgraded and then it will enter the packet forwarding mode, indicating that it will no longer provide protection.
Formal	ADS can still provide protection, but will no longer be upgraded.
Subscription	vADS cannot be upgraded and then it will enter the packet forwarding mode, indicating that it will no longer provide protection.

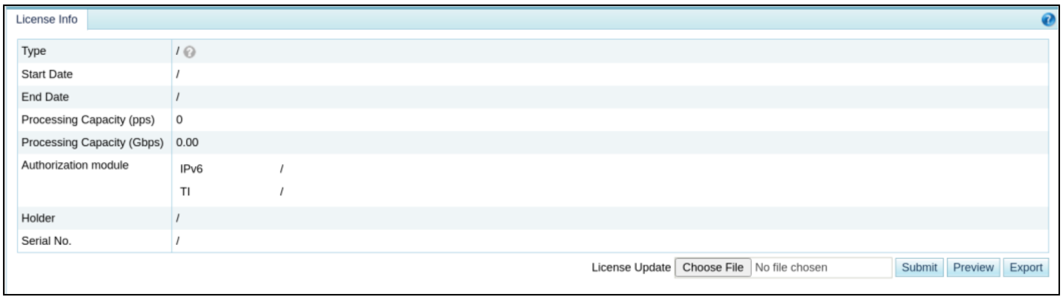
Note

The system displays a warning when the license is about to expire. You can set a period during which you will not be reminded again. To use ADS properly, please timely import a new license as prompted.

- For a formal license, within 30 days before the license expires, the system displays the first warning. You will also receive the warning when the license has expired.
- For a trial license, within seven days before the license expires, the system displays the first warning.

Choose **System** > **Others** > **License Info**. The initial license information page appears, as shown in Figure 3-56.

Figure 3-56 License Info page before the import of a license

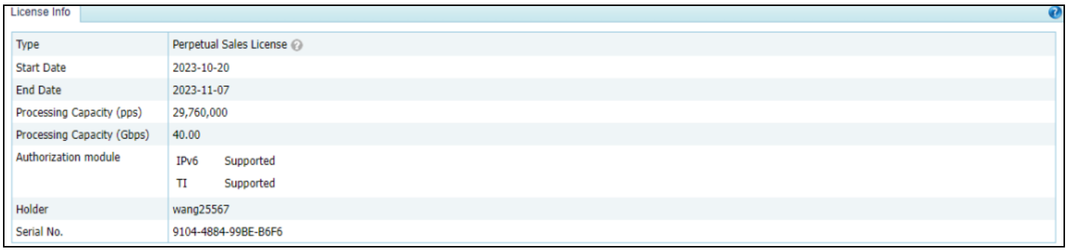


License Info

Type	/
Start Date	/
End Date	/
Processing Capacity (pps)	0
Processing Capacity (Gbps)	0.00
Authorization module	IPv6 / TI /
Holder	/
Serial No.	/

After a license is imported, different license information is displayed for hardware and virtual devices, as shown in Figure 3-57 and Figure 3-58.

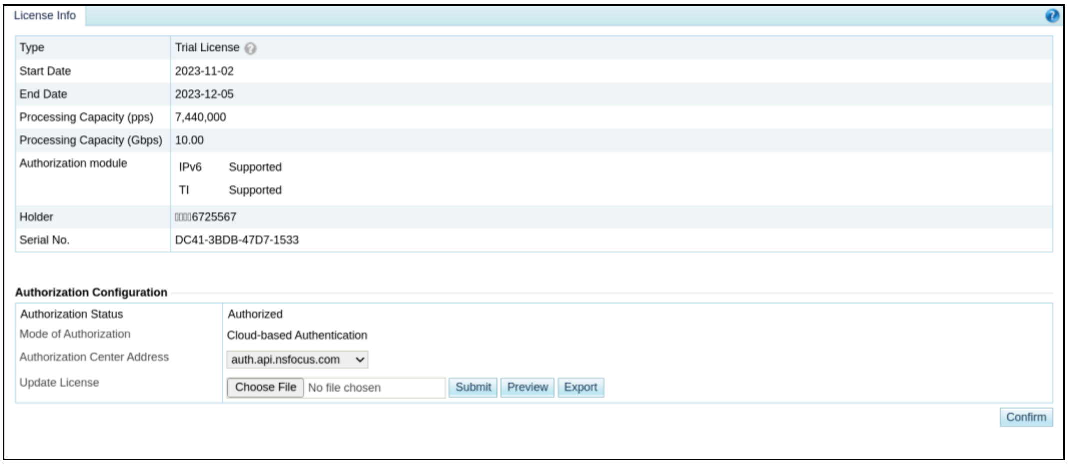
Figure 3-57 License Info page on a hardware device after the import of a license



License Info

Type	Perpetual Sales License
Start Date	2023-10-20
End Date	2023-11-07
Processing Capacity (pps)	29,760,000
Processing Capacity (Gbps)	40.00
Authorization module	IPv6 Supported TI Supported
Holder	wang25567
Serial No.	9104-4884-99BE-B6F6

Figure 3-58 License Info page on a virtual device after the import of a license



License Info

Type	Trial License
Start Date	2023-11-02
End Date	2023-12-05
Processing Capacity (pps)	7,440,000
Processing Capacity (Gbps)	10.00
Authorization module	IPv6 Supported TI Supported
Holder	□□□□6725567
Serial No.	DC41-3BDB-47D7-1533

Authorization Configuration

Authorization Status	Authorized
Mode of Authorization	Cloud-based Authentication
Authorization Center Address	auth.api.nsfocus.com
Update License	Choose File No file chosen

Table 3-27 describes ADS device license parameters.

Table 3-27 ADS device license parameters

Parameter	Description
Type	Type of the license, which can be **Trial**, **Interim**, **Formal**, and **Subscription**. **Note** Only vADS supports the **Subscription** license type.
Start Date	Date when the current service license is produced. **Note** The "current service" indicates the service authorized by the current license.
End Date	Date when the current service license is terminated. When the license expires, ADS will provide limited functions, as shown in Table 3-26. What functions are still available depends on the license type.. **Note** The "current service" indicates the service authorized by the current

Parameter		Description
		license.
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.
Authorization Module		Shows whether the current version supports IPv6 and NTI.
Holder		Customer who owns the current ADS device.
Serial No.		Serial number of the current ADS device.
Authorization Configuration	Authorization Status	Indicates the authorization status of the current virtual device, which can be: • **Authorized**: This is displayed when the address of the cloud authorization center is correct and the connection to the cloud is properly established. • **Offline**: This is displayed when the device, which has been authorized, fails to connect to the cloud. In this state, you can still use the web-based manager for a while. • **Unauthorized**: This is displayed when the device remains offline for more than 15 days. In this state, you cannot use the web-based manager any more.
	Mode of Authorization	Indicates the way the virtual device is authorized. Virtual devices can be authorized via either local authentication or cloud-based authentication. For this purpose, you must ensure vADS can properly connect to the cloud authorization center.
	Authorization Center Address	Specifies the address of the authorization center. • For local authentication, you need to type an IP address plus a port in the format of ip:port. Once the IP address of the authorization center is changed, vADS will initiate reauthentication. • For cloud-based authentication, after the address is correctly configured, vADS automatically sends an authentication request to the cloud every time it is started. During its operation, vADS periodically sends authentication requests to the cloud. Therefore, you must ensure that vADS remains connected to the cloud all the time. Specifies the server URL of the cloud authorization center: • For use on the Chinese mainland, choose **auth.api.nsfocus.com**. • For use in other countries and regions, choose **auth.nsfocusglobal.com**.

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

- Previewing a license

  To the lower right of the license information table, click **Choose File** to 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 **Choose File** 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.

- Exporting a license

To the lower right of the license information table, click **Export** and select a storage path in the dialog box that appears to export the current license to the specified location as a backup.

3.4.2 System Update

You can manually import the update file to update ADS. Before updating the system, do as follows to avoid possible update failures or data loss:

- Contact NSFOCUS technical support for ADS update packages. Make sure that the package matches your product.
- Go to the License page to check whether the license has expired.
- Check whether configuration files and data have been backed up. If not, go to the Configuration File Management page to back up them.

Note	• If the version of the update package is equal to or earlier than the current version, the system cannot be updated. • ADS NX1-VN can only be updated via a package subject to two-layer encryption.

To update ADS, perform the following steps:

Step 1 Choose **System** > **Others** > **System Upgrade**.

Step 2 Click **Choose File** and select the desired update package.

Step 3 Click **Start Upgrade** 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 4 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 5 Re-log in to the system and choose **System** > **Others** > **Version Info** to view version information and check whether the update succeeds.

Step 6 If the update succeeds, click **View** in the **Upgrade Notes** column of the **Upgrade History** table on the **System Upgrade** page to view the update notes.

----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.

By default, this function is disabled. You need to enable it before using the function.

To enable the remote assistance function, follow these steps:

Step 1 Choose **System > Others > Remote Assistance**.

Step 2 Select **Yes** and configure the following parameters for remote assistance.

- **Port**: enter a port number in the range of 1024–65535, excluding 50022. Leaving it empty indicates that a random port will be used.
- **Allowed IP:** you can configure at most three IP addresses.

Step 3 Click **OK** to complete the configuration.

Then the login key used by the specified IP address for remote access to ADS, its QR code, and port are displayed below.

Note	After a user enables the remote assistance function, NSFOCUS technical support will calculate the password, and log in as **engineer** or **develop** depending on the requirements or permissions, to provide remote assistance.

----End

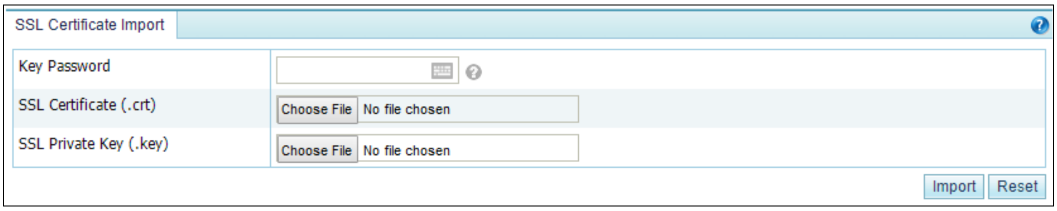
3.4.4 SSL Certificate Import

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 3-59 SSL Certificate Import page



SSL Certificate Import

Key Password

SSL Certificate (.crt) No file chosen

SSL Private Key (.key) No file chosen

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 Inspection

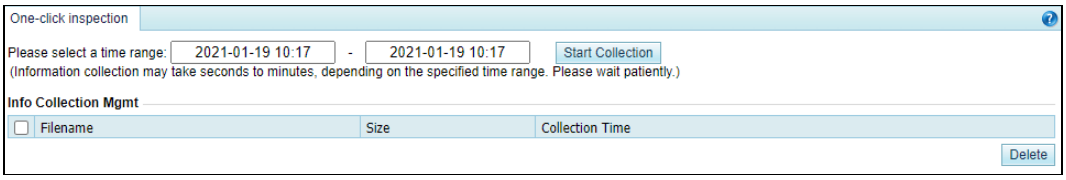
When ADS fails, you can collect device information by using the one-click inspection function, and deliver such information to NSFOCUS technical support, who therefore do not need to log in to ADS for collection of such information.

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

To collect the preceding information, perform the following steps:

Step 1 Choose **System** > **Others** > **One-Click Inspection**.

Figure 3-60 One-Click Inspection page



One-click inspection

Please select a time range: 2021-01-19 10:17 - 2021-01-19 10:17

(Information collection may take seconds to minutes, depending on the specified time range. Please wait patiently.)

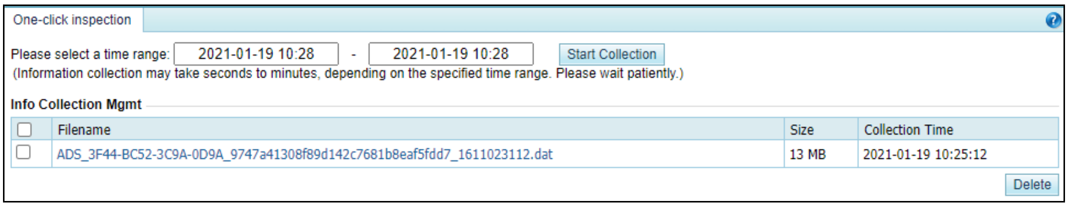
Info Collection Mgmt

□	Filename	Size	Collection Time

Step 2 Set a time range and click **Start Collection** to start collecting device information.

After fault information is successfully collected, an information file is displayed in the **Info Collection Mgmt** list, as shown in Figure 3-61.

Figure 3-61 One-click inspection result



One-click inspection

Please select a time range: 2021-01-19 10:28 - 2021-01-19 10:28 Start Collection

(Information collection may take seconds to minutes, depending on the specified time range. Please wait patiently.)

Info Collection Mgmt

□	Filename	Size	Collection Time
□	ADS_3F44-BC52-3C9A-0D9A_9747a41308f89d142c7681b8eaf5fdd7_1611023112.dat	13 MB	2021-01-19 10:25:12

Delete

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 System Information

Choose **System** > **Others** > **System Info**. The **System Info** page displays the device information, version information, and system uptime.

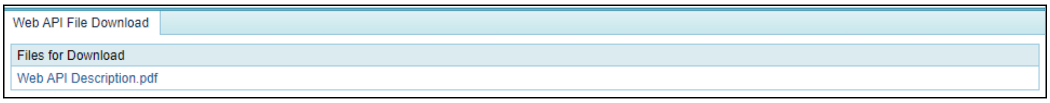
3.4.7 Web API File Download

You can download the web API file that describes API communication interfaces from the web-based manager of ADS. The procedure is as follows:

Step 1 Choose **System** > **Others** > **Web API File Download**.

Step 2 On the page shown in Figure 3-62, click the file name in the **Files for Download** area to download the file to a local disk drive.

Figure 3-62 Web API File Download page



Web API File Download

Files for Download
Web API Description.pdf

----End

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
- Top 10 Destination IPs by Traffic
- System Resources
- Collaboration Status
- System Interfaces

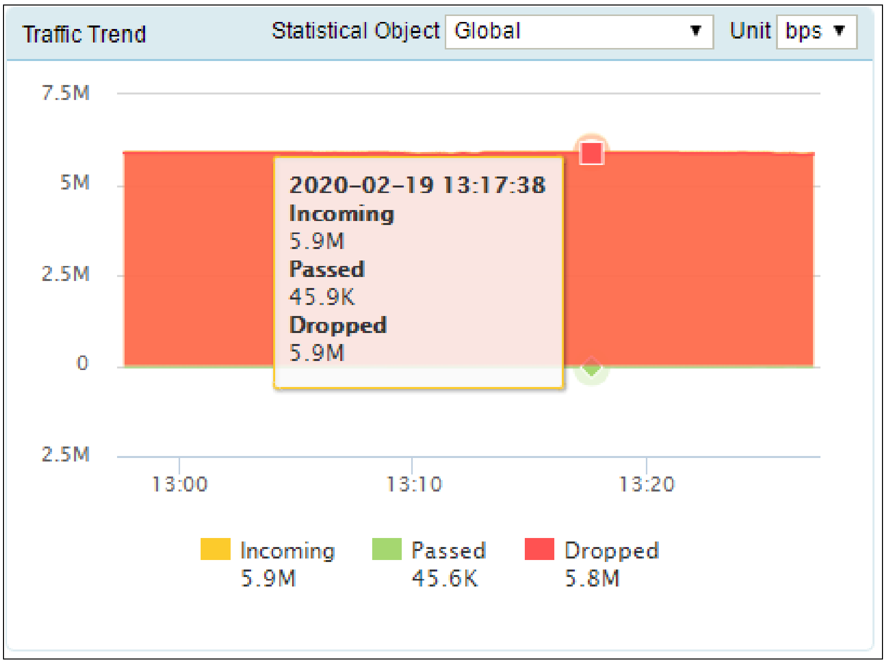
Traffic Trend

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

When pointing to the traffic trend graph, you can view the incoming traffic, outgoing traffic, and dropped traffic at a specific time.

- You can click the drop-down box of **Statistical Object** and select **Global** or a specific protection group to view global traffic information or traffic information of that group.
- You can specify the traffic unit by selecting **bps** or **pps** from the **Unit** drop-down box in the upper-right corner of this area.

Figure 4-1 Traffic trend



Traffic Trend

Statistical Object Global ▼

Unit bps ▼

Attack Traffic

The **Attack Traffic** area presents the attack traffic detected and dropped by the current ADS device in the last 30 minutes, as shown in Figure 4-2. When pointing to the attack traffic graph, you can view the dropped traffic at a specific time.

- You can click the drop-down box of **Statistical Object** and select **Global** or a specific protection group to view global attack traffic information or attack traffic information of that group.
- You can specify the traffic unit by selecting **bps** or **pps** from the **Unit** drop-down box in the upper-right corner of this area.

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

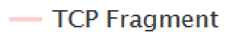
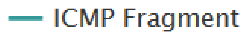
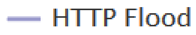
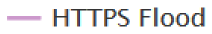
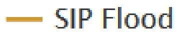
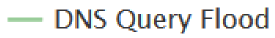
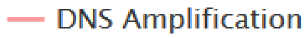
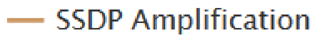
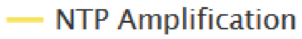
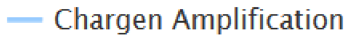
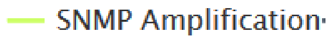
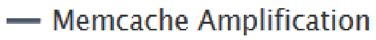
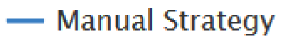
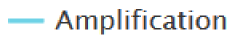
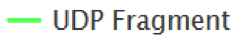
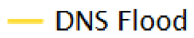
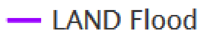
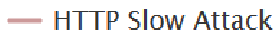
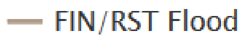
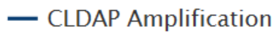
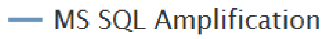
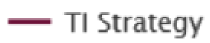
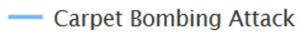
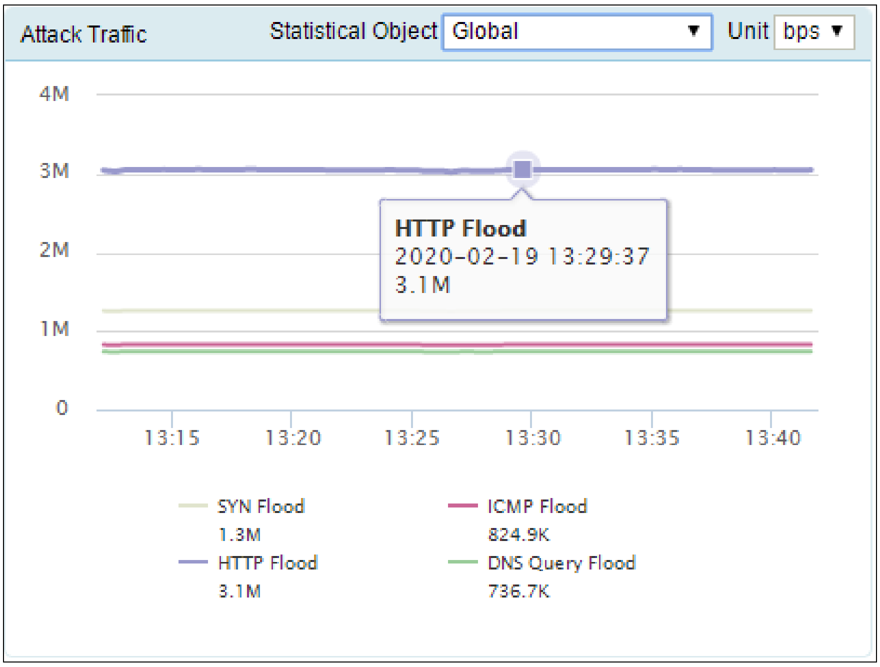
Attack Type	Color Indication
TCP fragment	 TCP Fragment
ICMP fragment	 ICMP Fragment
HTTP flood	 HTTP Flood
HTTPS flood	 HTTPS Flood
SIP flood	 SIP Flood
DNS query flood	 DNS Query Flood
DNS amplification	 DNS Amplification
SSDP amplification	 SSDP Amplification
NTP amplification	 NTP Amplification
Chargen 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
CLDAP Amplification	 CLDAP Amplification
MS SQL Amplification	 MS SQL Amplification
TI Strategy	 TI Strategy
Carpet Bombing Attack	 Carpet Bombing Attack

Figure 4-2 Attack traffic



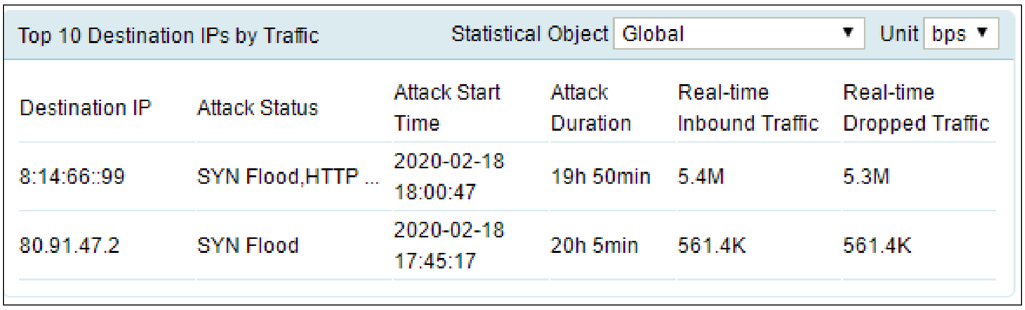
Top 10 Destination IPs by Traffic

The **Top 10 Destination IPs by Traffic** area shows information about top 10 destination IP addresses receiving the most traffic, including the destination IP address, attack status, attack start time, attack duration, real-time incoming traffic, and real-time dropped traffic.

If no packet is dropped for a destination IP address, "---" is displayed in **Attack Status**, **Attack Start Time**, and **Attack Duration** columns.

- You can click the drop-down box of **Statistical Object** and select **Global** or a specific protection group to view global information about top 10 destination IP addresses or top 10 destination IP addresses of that group.
- You can specify the traffic unit by selecting **bps** or **pps** from the **Unit** drop-down box in the upper-right corner of this area.

Figure 4-3 Top 10 destination IP addresses by incoming traffic



Top 10 Destination IPs by Traffic — Statistical Object: Global — Unit: bps

Destination IP	Attack Status	Attack Start Time	Attack Duration	Real-time Inbound Traffic	Real-time Dropped Traffic
8:14:66::99	SYN Flood,HTTP ...	2020-02-18 18:00:47	19h 50min	5.4M	5.3M
80.91.47.2	SYN Flood	2020-02-18 17:45:17	20h 5min	561.4K	561.4K

System Resources

The **System Resources** area displays different information for 6U devices and 1U/2U devices.

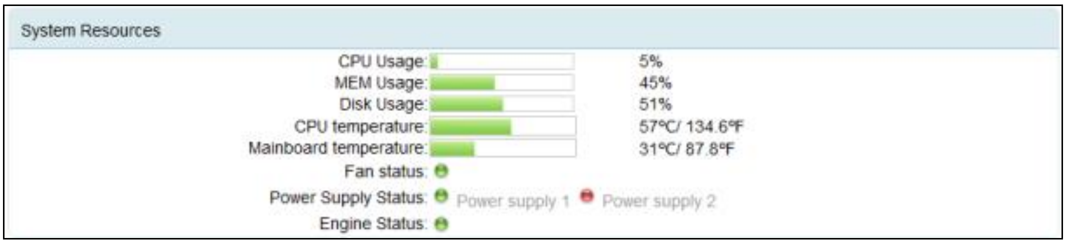
System Resources of 1U/2U Devices

The **System Resources** area shows the status of various system resources in real time, including the CPU usage, memory usage, disk usage, CPU temperature, mainboard temperature, fan status, power supply status, and enginee status. For fan status, power supply status, and enginee status, 🟢 indicates that the fans, power supply, or enginee works properly and 🔴 indicates the opposite.

Note

Only ADS NX3-HD2500, NX5-HD4500, NX5-HD6500, and ADS NX5-HD8500 and some ADS NX5-8000 devices have the power supply status displayed.

Figure 4-4 System resources of 1U/2U devices



System Resources

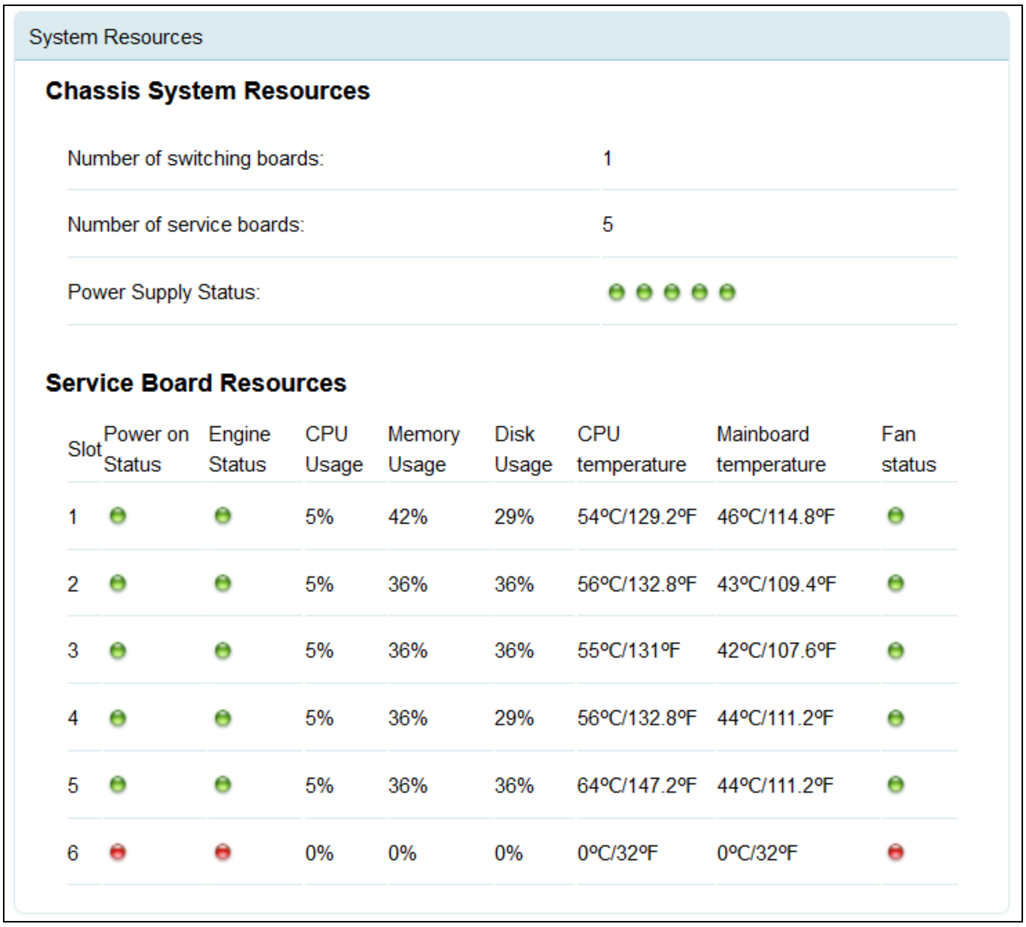
CPU Usage: 5%
MEM Usage: 45%
Disk Usage: 51%
CPU temperature: 57℃/ 134.6℉
Mainboard temperature: 31℃/ 87.8℉
Fan status: 🟢
Power Supply Status: 🟢 Power supply 1 🔴 Power supply 2
Engine Status: 🟢

System Resources of 6U Devices

The 6U devices refer to ADS NX5-10000 and ADS NX5-12000.

The **System Resources** area shows the overall information of 6U devices, including the chassis system resources and service board resource usage. The **Service Board Resources** area displays the status of various service board resources in real time, including the power on status, enginee status, CPU usage, memory usage, disk usage, CPU temperature, mainboard temperature, and fan status. For fan status, power on status, and enginee status, 🟢 indicates that the fans, power supply, or enginee works properly and 🔴 indicates the opposite.

Figure 4-5 System resources for 6U devices



System Resources

Chassis System Resources

Number of switching boards:	1
Number of service boards:	5
Power Supply Status:	🟢 🟢 🟢 🟢 🟢

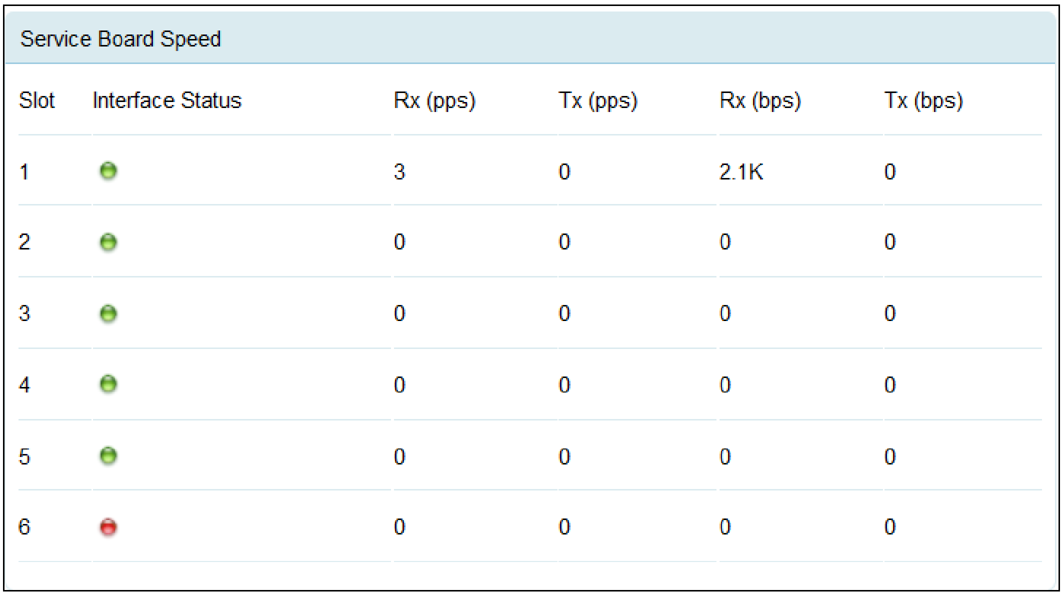
Service Board Resources

Slot	Power on Status	Engine Status	CPU Usage	Memory Usage	Disk Usage	CPU temperature	Mainboard temperature	Fan status
1	🟢	🟢	5%	42%	29%	54ºC/129.2ºF	46ºC/114.8ºF	🟢
2	🟢	🟢	5%	36%	36%	56ºC/132.8ºF	43ºC/109.4ºF	🟢
3	🟢	🟢	5%	36%	36%	55ºC/131ºF	42ºC/107.6ºF	🟢
4	🟢	🟢	5%	36%	29%	56ºC/132.8ºF	44ºC/111.2ºF	🟢
5	🟢	🟢	5%	36%	36%	64ºC/147.2ºF	44ºC/111.2ºF	🟢
6	🔴	🔴	0%	0%	0%	0ºC/32ºF	0ºC/32ºF	🔴

Service Board Speed

The **Service Board Speed** area shows the interface connection status of service boards on a 6U device (🟢 means "online"; 🔴 means "offline"), and total Rx traffic and Tx traffic (both pps and bps) of each interface.

Figure 4-6 Service board speed



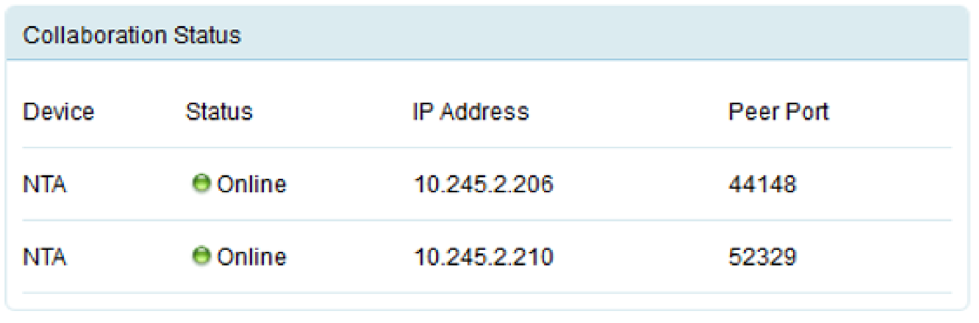
Service Board Speed

Slot	Interface Status	Rx (pps)	Tx (pps)	Rx (bps)	Tx (bps)
1	🟢	3	0	2.1K	0
2	🟢	0	0	0	0
3	🟢	0	0	0	0
4	🟢	0	0	0	0
5	🟢	0	0	0	0
6	🔴	0	0	0	0

Collaboration Status

The **Collaboration Status** area shows the status of collaboration between the current ADS and another device. Figure 4-7 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 4-7 Collaboration status



Collaboration Status

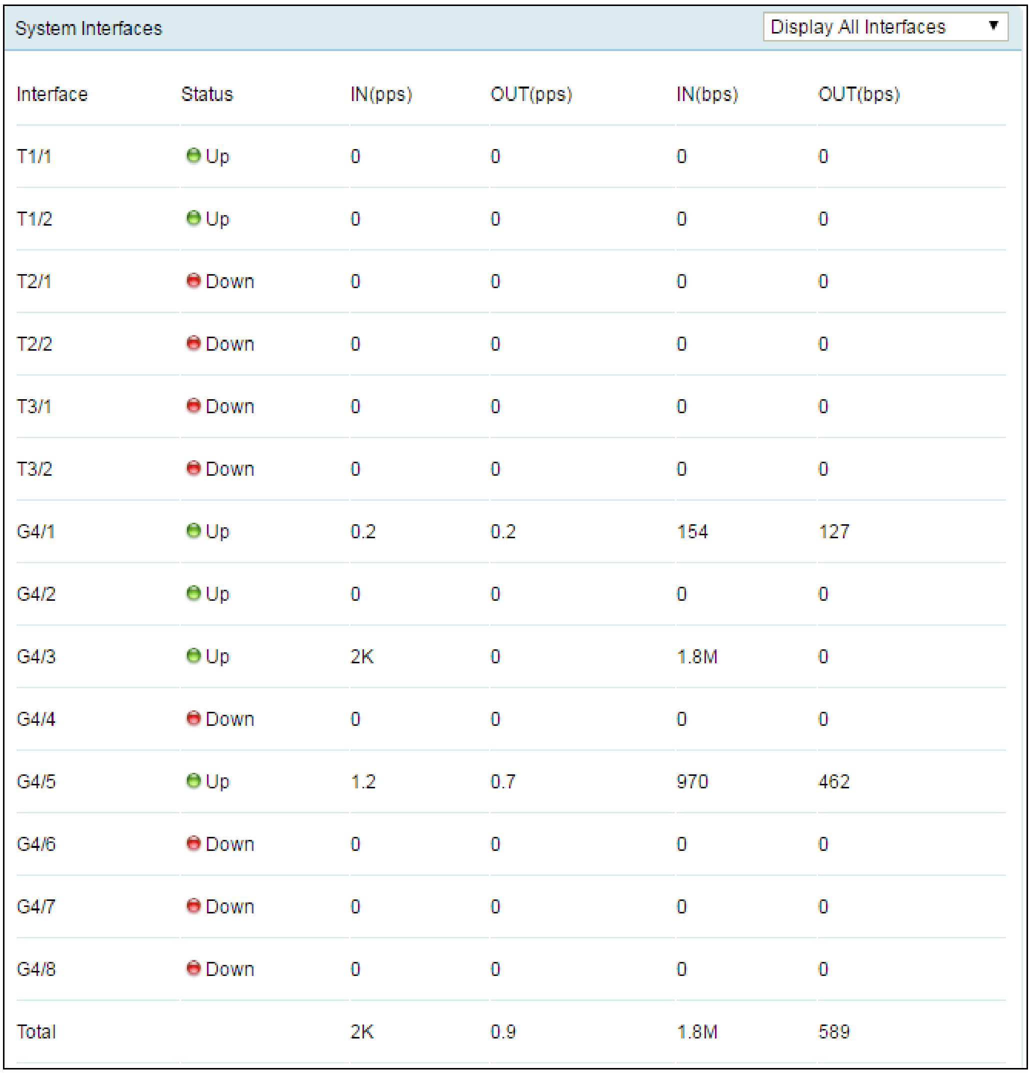
Device	Status	IP Address	Peer Port
NTA	🟢 Online	10.245.2.206	44148
NTA	🟢 Online	10.245.2.210	52329

System Interfaces

The **System Interfaces** area on, for example, ADS NX5-4020E, shows the connection status of interfaces on ADS (🟢 means "online"; 🔴 means "offline"), and real-time incoming and outgoing 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 4-8. Clicking **Display Online Interfaces** in the drop-down box in the upper-left corner of this area displays information only about online interfaces.

Figure 4-8 Interface status of ADS



System 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

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, memory, and disk usage, system version, system uptime, and system time.

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

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:

- Protection Group Management
- Policy Configuration for Protection Groups
- Protection Group Policy Templates
- Advanced Global Parameters
- Response Page Settings
- SSL Certificate Management
- Mobile User-Agent Rules

5.1.1 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.

In addition to manual configuration, ADS can automatically generate protection group policies based on policy auto-learning results. For details, see section 5.1.1.6 Configuring Policy Auto-Learning.

default_protection_group is the default protection group for which the IP address list cannot be edited or deleted or automatic learning is unavailable. By default, when traffic protection is enabled, ADS cleans and protects traffic as indicated in protection policies configured for **default_protection_group**, if no other protection groups are created or matched.

This chapter describes how to configure and manage protection groups manually. It covers the following topics:

- Creating a Protection Group: creating a protection group and configuring the IP list, protection policies, access control policies, and URL rules for this protection group.
- Searching for Protection Groups: searching for a protection group by name or IP address.
- Viewing a Protection Group: viewing settings of a protection group.
- Editing a Protection Group: editing protection group settings, including the IP list, protection policies, access control policies, and URL rules.
- Deleting a Protection Group: deleting one or more protection groups.
- Configuring Policy Auto-Learning: configuring auto-learning parameters, enabling/disabling the auto-learning function, and viewing learning details

5.1.1.1 Creating a Protection Group

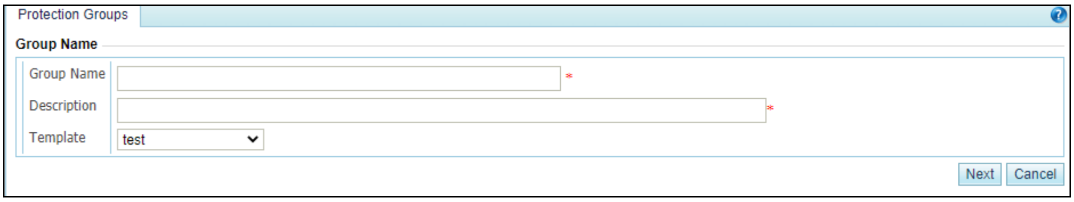
To create a protection group manually, perform the following steps:

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

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 5-1.

Figure 5-1 Basic information of a protection group



Template: test

Table 5-1 describes parameters for creating a protection group.

Table 5-1 Parameters for creating a protection group

Parameter	Description
Group Name	Name of the group. It must be unique and consist of 1 to 200 letters, digits, or underscores.
Description	Description of a group. It can contain a maximum of 80 characters.
Template	Allows users to select a protection group policy template from default templates and those created by the administrator. For template details, see section 5.1.3 Protection Group Policy Templates.

Step 3 Configuring the running mode of the protection group.

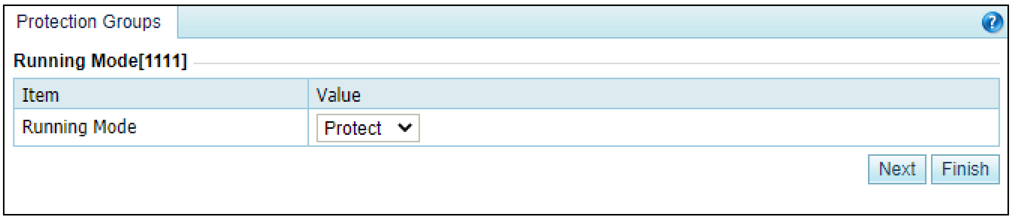
After the protection group is created, click **Next** to configure the running mode for this group.

You can select the running mode from three values: **Protect**, **Inactive**, and **Forward**.

- **Protect**: After protection policies take effect, ADS starts to protect traffic of the protection group.
- **Inactive**: After protection policies take effect, ADS conducts protective analysis of and generates alerts for attacks. Meanwhile, it allows traffic to pass through without protection. Under the System Interfaces tab, you can see that ADS directly forwards traffic without any filtering.
- **Forward**: After protection policies take effect, ADS allows traffic to pass through, without performing attack analysis and protection.

After the running mode is selected, you can click **Next** to go to the next step or click **Finish** to complete the protection group configuration.

Figure 5-2 Configuring the running mode



Protection Groups

Running Mode[1111]

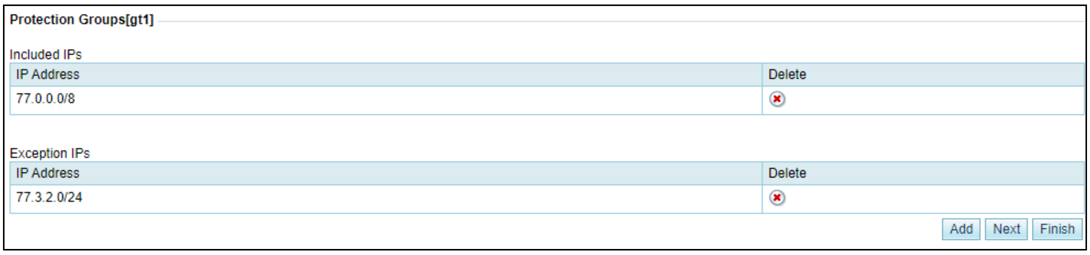
Item	Value
Running Mode	Protect

Step 4 Configure the IP address range of the protection group, including included IP and exception IP address range.

If you do not want to protect certain IP addresses or IP segments within the IP range of the protection group, configure them as exception IP addresses.

After the running mode is configured, click **Next** to open the **IP List** page. You can add IP address ranges one by one. If IP address ranges are not required currently, click **Next** to skip this step or click **Finish** to complete the protection group configuration.

Figure 5-3 IP List page



Protection Groups[gt1]

Included IPs

IP Address	Delete
77.0.0.0/8	⊗

Exception IPs

IP Address	Delete
77.3.2.0/24	⊗

Note	ADS supports the IPv4/IPv6 dual-stack. Therefore, protection groups can involve both IPv4 and IPv6 address ranges.

Adding an IP Address Range

a. Click **Add** to the lower right of the IP list.

Figure 5-4 Adding an IP address range

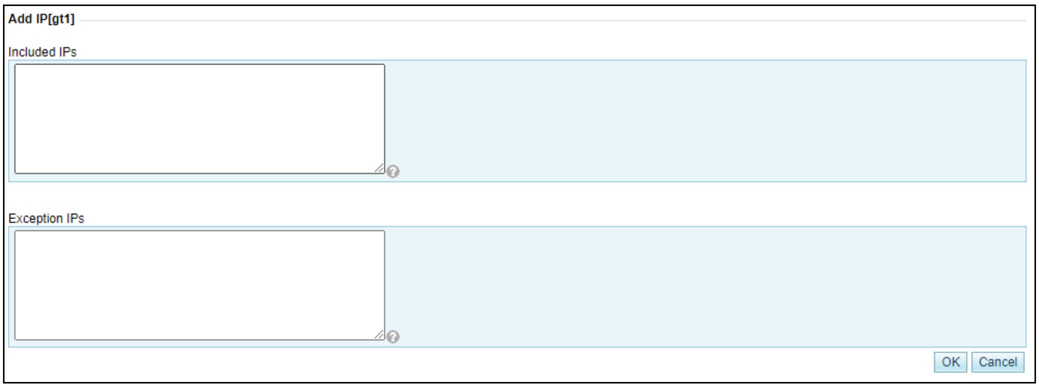


Table 5-2 describes the format of an IP address range.

Table 5-2 Format of an IP address, IP segment, and IP address range

Item	Description
IP address format	You can type IPv4 or IPv6 addresses or segments, with one in each line, in the following formats: • Individual IP address: an IP address such as 192.168.1.1 or 2::2. • IP address/netmask: an IPv4 address with a netmask ranging from 8 to 32, such as 192.168.1.1/24; IPv6 address with a prefix length ranging from 1 to 128, such as fe80::250:56ff:fec0:0/114. • Start IP-End IP: 256 IPv4 address within a /24 segment, such as 192.168.1.1-10; or IPv6 address with a 16-bit prefix, such as 1::1-ffff. Note Protection IP ranges of different protection groups must not overlap. The exception IP configured will not be protected.

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

Deleting an IP Address or IP Address Range

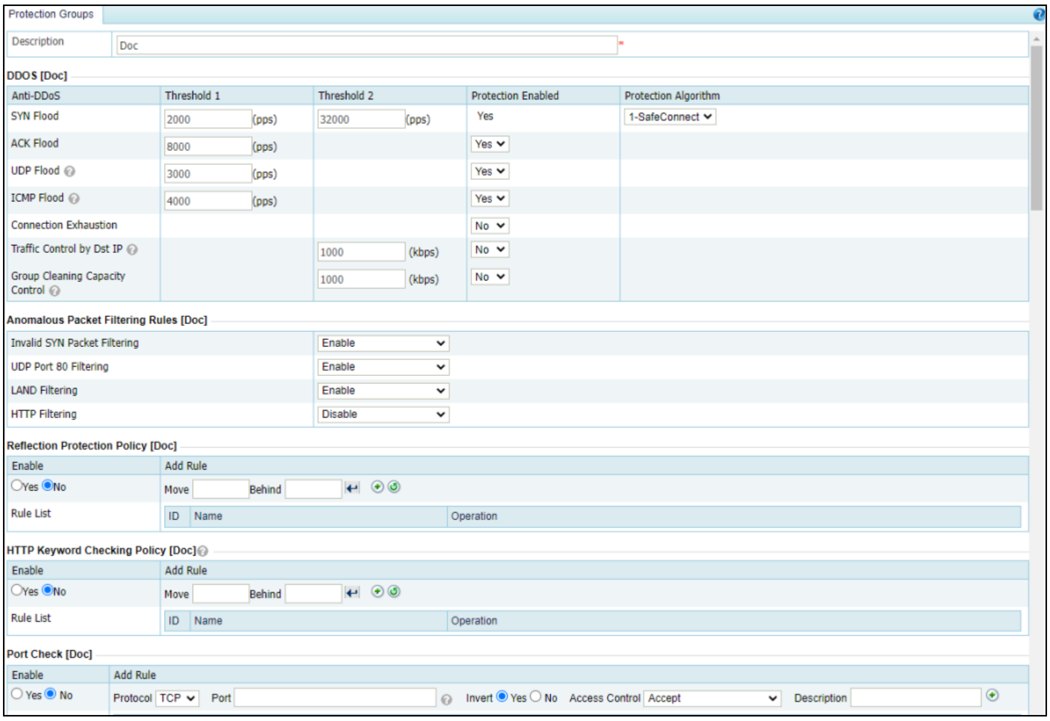
On the IP list shown in Figure 5-3, click ✖ in the **Delete** column of an IP address or IP address range and click **OK** in the confirmation dialog box to delete this IP address or IP address range.

Note	IP address ranges cannot conflict across protection groups.

Step 5 Configure policies for the protection group.

After the IP address range is configured, click **Next** to configure protection policies for this group. For details, see section 5.1.2 Policy Configuration for Protection Groups. If policies are not required currently, click **Next** to skip this step or click **Finish** to complete the protection group configuration.

Figure 5-5 Protection policies for a protection group



Protection Groups

Description: Doc *

DDOS [Doc]

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

Anomalous Packet Filtering Rules [Doc]

Invalid SYN Packet Filtering	Enable
UDP Port 80 Filtering	Enable
LAND Filtering	Enable
HTTP Filtering	Disable

Reflection Protection Policy [Doc]

Enable: ○ Yes ● No

Add Rule: Move Behind

Rule List: ID | Name | Operation

HTTP Keyword Checking Policy [Doc]

Enable: ○ Yes ● No

Add Rule: Move Behind

Rule List: ID | Name | Operation

Port Check [Doc]

Enable: ○ Yes ● No

Add Rule: Protocol TCP Port Invert ● Yes ○ No Access Control Accept Description

Step 6 Configure the access policies for the protection group.

After the protection policies are configured, click **Next** to configure the access policies for the protection group.

Configuring an Access Policy

Setting a Group-specific Access Control Rule

Click **Add** to create an access control rule. For details about this function, see section 5.2 Access Control Policies. The differences are that access control rules configured here are valid only for the group and the **Invert** operation does not work here.

Setting a Group-specific Blocklist

You need to specify whether to enable the blocklist ("blacklist" on the UI), lockout period, and whether to enable proxy monitoring. For details about the blocklist function, see section 5.2.10 Blocklist.

Setting a Group-specific GeoIP Rule

Click **Add** to configure a group-specific GeoIP rule. You need to choose whether to enable the group-specific rule, and specify the source location, access control, and description. For details about the GeoIP rules, see section 5.2.3 GeoIP Rules.

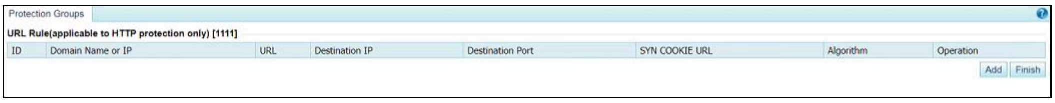
Setting Group-specific NTI

You need to specify whether to enable the group protection and specify the action taken against traffic whose source/destination IP address has a match in the intelligence database. Options include **Block** and **Traffic Control by Dst IP**. For details about NTI, see section 8.4 Collaboration with NTI.

Step 7 Configure a URL protection rule for the protection group.

After protection policies are configured, click **Next** to configure URL protection rules for this group. If URL protection rules are not required currently, click **Next** to skip this step or click **Finish** to complete the protection group configuration.

Figure 5-6 List of URL protection rules of a protection group



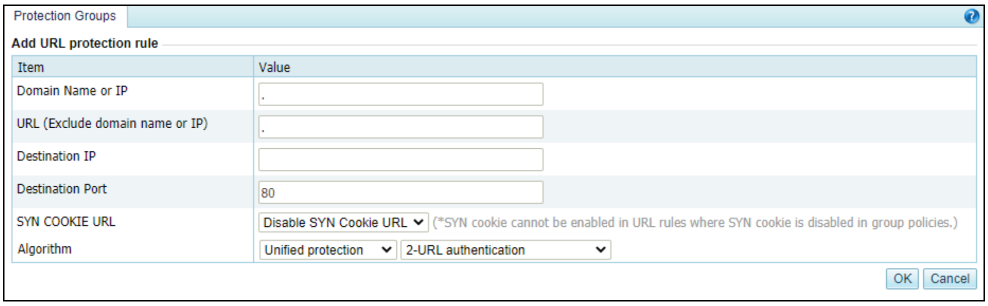
URL Rule(applicable to HTTP protection only) [1111]

ID	Domain Name or IP	URL	Destination IP	Destination Port	SYN COOKIE URL	Algorithm	Operation

Adding a URL Protection Rule

a. To the lower right of the URL protection rule list, click **Add** to add a URL protection rule. Figure 5-8 shows the page for adding a URL protection rule with **Algorithm** set to **Precision protection**.

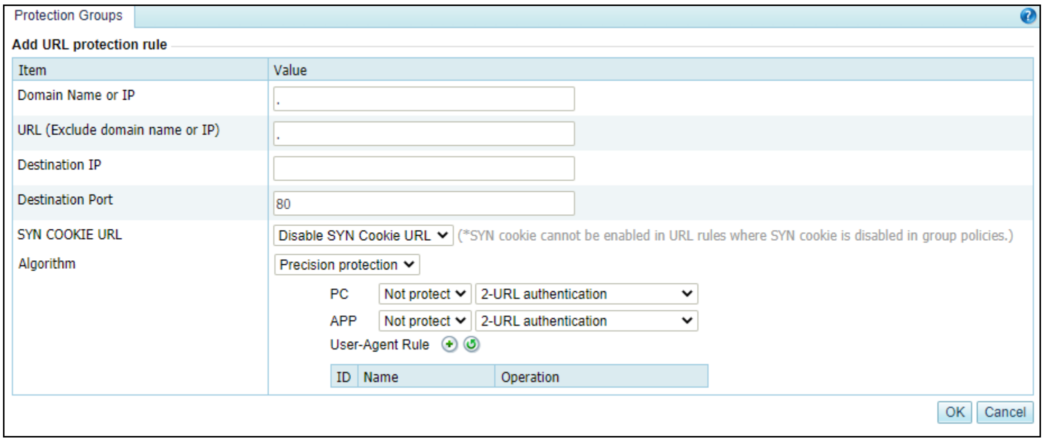
Figure 5-7 Adding a URL protection rule — unified protection



Add URL protection rule

Item	Value
Domain Name or IP	.
URL (Exclude domain name or IP)	.
Destination IP	
Destination Port	80
SYN COOKIE URL	Disable SYN Cookie URL (*SYN cookie cannot be enabled in URL rules where SYN cookie is disabled in group policies.)
Algorithm	Unified protection 2-URL authentication

Figure 5-8 Adding a URL protection rule — precision protection



Protection Groups

Add URL protection rule

Item	Value
Domain Name or IP	.
URL (Exclude domain name or IP)	.
Destination IP	
Destination Port	80
SYN COOKIE URL	Disable SYN Cookie URL (*SYN cookie cannot be enabled in URL rules where SYN cookie is disabled in group policies.)
Algorithm	Precision protection PC: Not protect, 2-URL authentication APP: Not protect, 2-URL authentication User-Agent Rule

ID	Name	Operation

Table 5-3 describes parameters for creating a URL protection rule.

Table 5-3 Parameters for adding a URL protection 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(Exclude domain name or IP)	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 an IPv4 or IPv6 address according to the actual network deployment. Note IP addresses specified in URL protection rules must belong to the protection group in question.
Destination Port	TCP port of the server.
SYN COOKIE URL	If **SYN COOKIE URL** is enabled, a client can access the server only after being authenticated by ADS, so as to protect the server from SYN cookie attacks. The setting of this parameter determines available options for **Algorithm**. The setting of this parameter depends on whether **SYN COOKIE URL** is enabled for HTTP protection.
Algorithm	Protection mode and policy adopted for packets matching URL protection rules. For detailed parameter descriptions, see Table 5-12. Note Protection algorithms are used together with the SYN Cookie URL function. • If SYN Cookie URL is enabled, you can only choose from algorithms 2 through 8. • If SYN Cookie URL is disabled, you can only choose from

Parameter	Description
	algorithms 0 through 5.

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

Modifying a URL Protection Rule

On the URL protection rule list, click ✎ in the **Operation** column of a rule to edit this rule.

Deleting a URL Protection Rule

On the URL protection rule list, click ✖ in the **Operation** column of a URL protection rule and click **OK** in the confirmation dialog box to delete this rule.

Step 8 After a URL protection rule is configured, click **Finish** to the lower right of the rule list.

Step 9 After the preceding configuration, click **Apply** in the upper-right corner of the web page to make the settings take effect.

----End

5.1.1.2 Searching for Protection Groups

On the protection group list, the system automatically lists all existing protection groups (20 per page) in the descending order of the creation time. You can set filtering conditions to list only protection groups meeting the specified conditions.

Step 1 Set filtering conditions.

- Specify group names or IP addresses. Fuzzy matching is supported.
- Specify a running mode. By default, protection groups of all running modes (**Protect**, **Inactive**, and **Forward**) are listed.

Step 2 Click **Filter**.

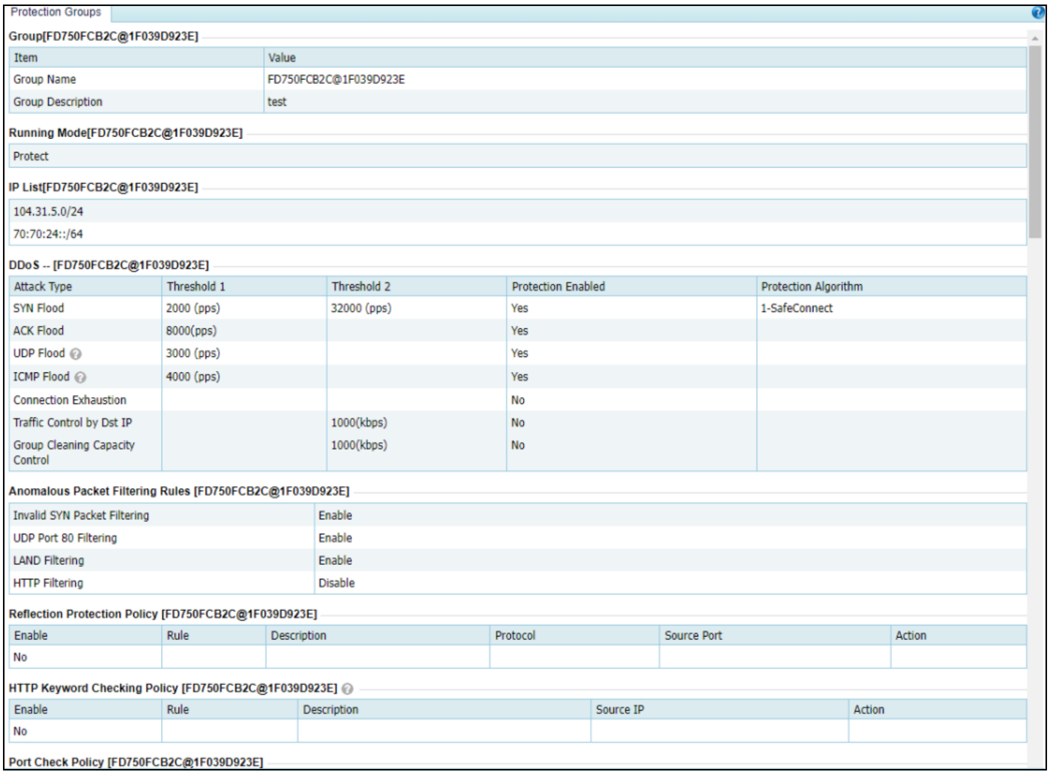
Protection groups meeting the specified conditions are then listed below.

----End

5.1.1.3 Viewing Protection Groups

On the protection group list, click the name of a protection group to view details.

Figure 5-9 Protection group details



Group[FD750FCB2C@1F039D923E]

Item	Value
Group Name	FD750FCB2C@1F039D923E
Group Description	test

Running Mode[FD750FCB2C@1F039D923E]

Protect

IP List[FD750FCB2C@1F039D923E]

104.31.5.0/24
70:70:24::/64

DDoS -- [FD750FCB2C@1F039D923E]

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

Anomalous Packet Filtering Rules [FD750FCB2C@1F039D923E]

Invalid SYN Packet Filtering	Enable
UDP Port 80 Filtering	Enable
LAND Filtering	Enable
HTTP Filtering	Disable

Reflection Protection Policy [FD750FCB2C@1F039D923E]

Enable	Rule	Description	Protocol	Source Port	Action
No					

HTTP Keyword Checking Policy [FD750FCB2C@1F039D923E]

Enable	Rule	Description	Source IP	Action
No				

Port Check Policy [FD750FCB2C@1F039D923E]

After viewing group details, click **Back** to return to the **Protection Groups** page.

5.1.1.4 Editing a Protection Group

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

- Edit the running mode of a protection group

  On the protection group list, click ✎ in the **Running Mode** column to changethe running mode of a protection group.

  After editing the running mode, click **OK** to save the setting. Click **Next** to edit the IP list.

- Edit an IP address range of a protection group.

  On the protection group list, click ✎ in the **IP List** column to edit 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 protection policies for a protection group.

  On the protection group list, click ✎ in the **Protection Policy** column to edit protection policies applied to a protection group.

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

- Edit the access policy for a protection group.
  - Edit group-specific access control rules

    On the protection group list, click **Access Control Rules** in the **Access Policy column** to add, enable, disable, or re-sort access control rules. For details, see section 5.2.1 Access Control Rules.
  - Edit the blocklist

    On the protection group list, click **Blacklist** in the **Access Policy** column. Click **Edit** to edit the blocklist. For details, see section 5.2.10 Blocklist.
  - Edit group-specific GeoIP rules

    On the protection group list, click **GeoIP Rules** in the **Access Policy** column to edit the GeoIP rules for a protection group. For details, see section 5.2.3 GeoIP Rules.
  - Edit group-specific NTI policies

    On the protection group list, click **NTI** in the **Access Policy** column to edit the NTI policy for the protection group. Click **Edit to enable NTI and specify the protection policy.**
- Edit URL protection rules for a protection group.

  On the protection group list, click 📝 in the **URL Rule** column of a protection group to edit URL protection rules of a protection group.

  After editing URL protection rules, click **Finish** to save settings to return to the protection group list.

5.1.1.5 Deleting a Protection Group

You can delete protection groups one by one or in bulk on ADS.

- Method 1: On the protection group list, click ⊗ in the **Delete** column of a group and click **OK** in the confirmation dialog box to delete it.
- Method 2: On the protection group list, select several protection groups (or select check boxes in the **Select All** column), click **Delete** to the lower right of the list, and then click **OK** in the confirmation dialog box to delete them.

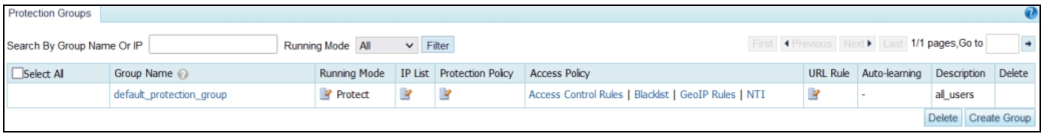
Note	If a protection group is deleted, all its settings, including policies, will be deleted and the customer's machines included in this group are instead protected by policies for the default group **default_protection_group**.

5.1.1.6 Configuring 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 then dispatch such policies manually or automatically to protection groups, depending on the configured policy application mode.

Choose **Policy** > **Anti-DDoS** > **Protection Groups**.

Figure 5-10 Protection Groups page



Running Mode: All

1/1 pages,Go to

□Select All	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
	default_protection_group	Protect			Access Control Rules | Blacklist | GeoIP Rules | NTI		-	all_users	

On this page, you can set auto-learning parameters, enable/disable the auto-learning function, view the auto-learning status, and view auto-learning details.

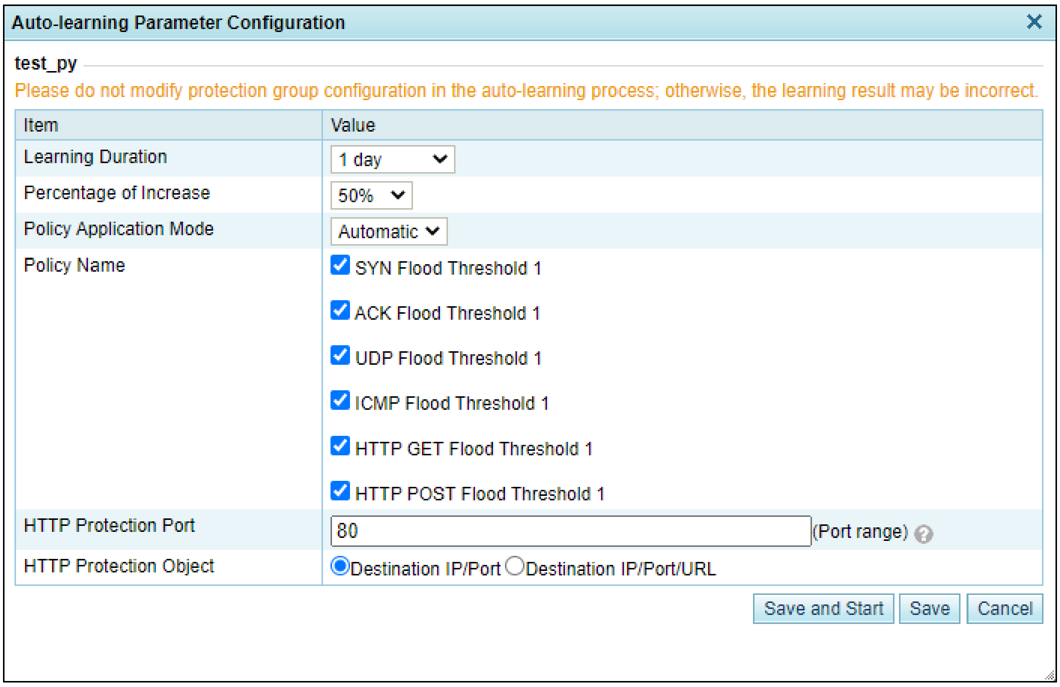
Setting Auto-learning Parameters

Newly created protection groups have no auto-learning function enabled. Their auto-learning status is displayed as "Not started". You can manually enable this function and set related parameters for a specific protection group. The procedure is as follows:

Step 1 On the page shown in Figure 5-10, click ▶ in the **Auto-learning Operation** column of a protection group.

The **Auto-learning Parameter Configuration** dialog box appears, as shown in Figure 5-11.

Figure 5-11 Configuring auto-learning parameters



test_py

Please do not modify protection group configuration in the auto-learning process; otherwise, the learning result may be incorrect.

Item	Value
Learning Duration	1 day
Percentage of Increase	50%
Policy Application Mode	Automatic
Policy Name	☑ SYN Flood Threshold 1 ☑ ACK Flood Threshold 1 ☑ UDP Flood Threshold 1 ☑ ICMP Flood Threshold 1 ☑ HTTP GET Flood Threshold 1 ☑ HTTP POST Flood Threshold 1
HTTP Protection Port	80 (Port range)
HTTP Protection Object	● Destination IP/Port ○ Destination IP/Port/URL

Step 2 Configure parameters.

Table 5-4 Parameters for configuring an auto-learning policy

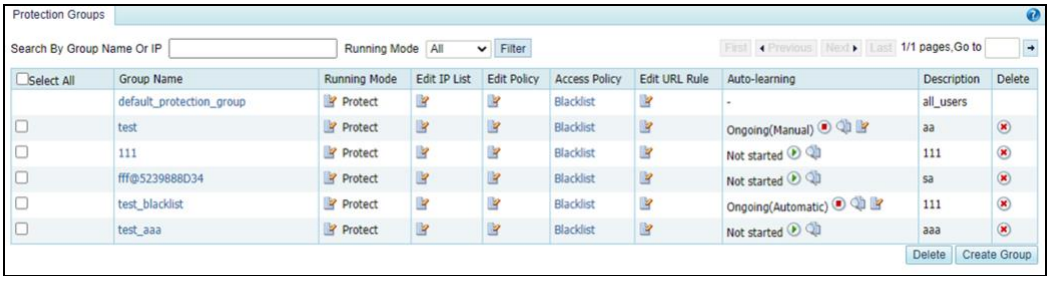
Parameter	Description
Learning Duration	Specifies the auto-learning duration. When this duration expires, ADS automatically stops such learning. Options include **30 minutes**, **1 hour**, **1 day**,

Parameter	Description
	and **1 week**.
Percentage of Increase	Specifies the percentage of increase in thresholds. Auto-learning results are updated in sync with the fluctuating traffic and thresholds dispatched are calculated by using this formula: Maximum value of historical learning results x (1 + Percentage of increase).
Policy Application Mode	Specifies a policy application mode, which can be either of the following: • **Manual**: After auto-learning is complete, you can view the result, select thresholds, change their values, and click **Update Thresholds** to dispatch new thresholds to the related protection group. • **Automatic**: When auto-learning is complete, the auto-learning policy is automatically executed to dispatch updated thresholds to the related protection group.
Policy Name	Specifies policies whose thresholds will be adapted to auto-learning results.
HTTP Protection Port	Specifies ports under HTTP protection within the range of 0–65535. You can type a maximum of 5 ports or port ranges separated by the comma like "80,90-92". Note Ports specified here cannot overlap with those specified for HTTPS protection.
HTTP Protection Object	Specifies the object of HTTP protection, which can be either of the following: • **Destination IP/Port/URL**: The IP address, port, and URL should all be matched. • **Destination IP/Port**: Only the IP address and port should be matched.

Step 3 Click **Save** to commit the settings.

If you click **Save and Start**, the system will collect traffic flowing over the network. In this case, the auto-learning status of the protection group changes to Ongoing(⚠Manual), as shown in Figure 5-12.

Figure 5-12 Auto-learning configured and started



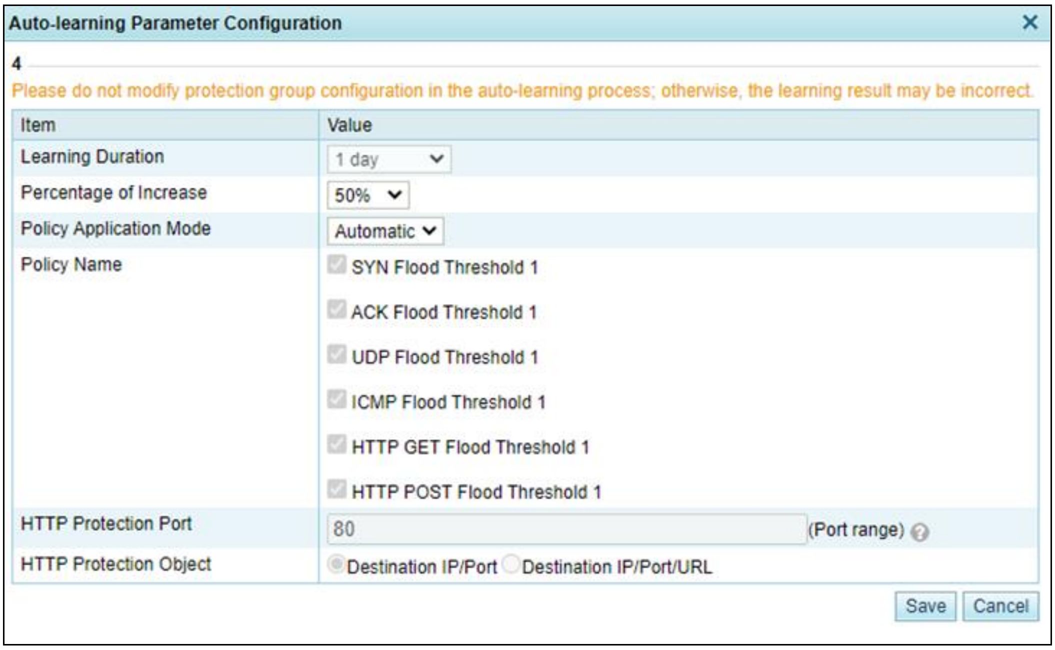
□ Select All	Group Name	Running Mode	Edit IP List	Edit Policy	Access Policy	Edit URL Rule	Auto-learning	Description	Delete
	default_protection_group	Protect			Blacklist		-	all_users	
□	test	Protect			Blacklist		Ongoing(Manual)	aa	⊗
□	111	Protect			Blacklist		Not started	111	⊗
□	fff@5239888D34	Protect			Blacklist		Not started	sa	⊗
□	test_blacklist	Protect			Blacklist		Ongoing(Automatic)	111	⊗
□	test_aaa	Protect			Blacklist		Not started	aaa	⊗

When the specified auto-learning duration expires, auto-learning automatically stops.

You can also click ● to manually stop the auto-learning process.

For ongoing auto-learning, you can click in the **Auto-learning Operation** column of a protection group to edit related parameters, including the percentage of increase in thresholds and policy application mode, as shown in Figure 5-13.

Figure 5-13 Editing auto-learning parameters



Auto-learning Parameter Configuration

4

Please do not modify protection group configuration in the auto-learning process; otherwise, the learning result may be incorrect.

Item	Value
Learning Duration	1 day
Percentage of Increase	50%
Policy Application Mode	Automatic
Policy Name	☑ SYN Flood Threshold 1 ☑ ACK Flood Threshold 1 ☑ UDP Flood Threshold 1 ☑ ICMP Flood Threshold 1 ☑ HTTP GET Flood Threshold 1 ☑ HTTP POST Flood Threshold 1
HTTP Protection Port	80 (Port range)
HTTP Protection Object	● Destination IP/Port ○ Destination IP/Port/URL

----End

Viewing the Auto-learning Status

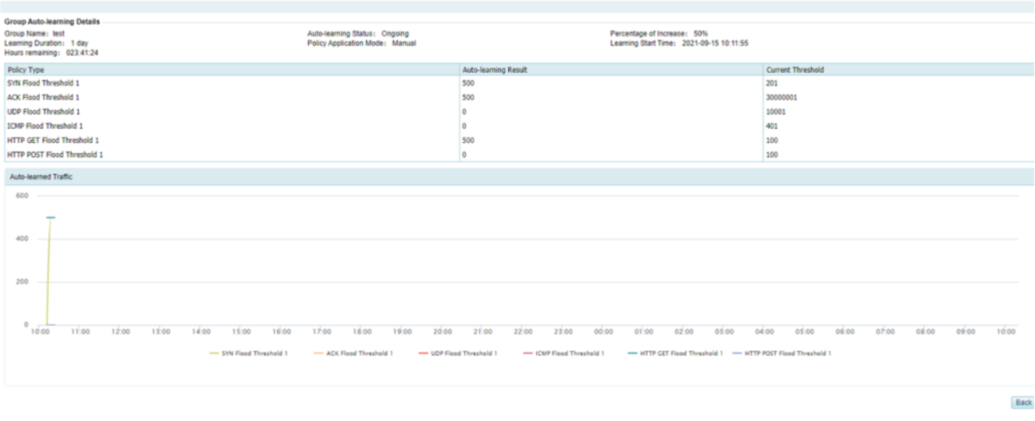
On the page shown in Figure 5-10, the **Auto-learning Status** column shows the auto-learning status of protection groups. The auto-learning status of a protection group can be any of the following:

- **Not started**: The auto-learning function is not enabled.
- **Ongoing**: Auto-learning is enabled and in progress.
- **Complete**: Auto-learning is complete.
- **Abnormal**: Auto-learning failed because of some external factors, such as a device restart during auto-learning.

Viewing Auto-learning Details

On the page shown in Figure 5-10, you can click in the **Auto-learning Operation** column of a protection group to view auto-learning details of the group.

Figure 5-14 Auto-learning details



Group Auto-learning Details

Group Name: test
Learning Duration: 1 day
Hours remaining: 023:41:24

Auto-learning Status: Ongoing
Policy Application Mode: Manual

Percentage of Increase: 50%
Learning Start Time: 2021-09-15 10:11:55

Policy Type	Auto-learning Result	Current Threshold
SYN Flood Threshold 1	500	201
ACK Flood Threshold 1	500	30000001
UDP Flood Threshold 1	0	10001
ICMP Flood Threshold 1	0	401
HTTP GET Flood Threshold 1	500	100
HTTP POST Flood Threshold 1	0	100

Auto-learned Traffic

When the policy application mode is **Manual** and the learning status is **Complete**, you can edit dispatched thresholds.

After the edit is complete, click **Update Thresholds** to dispatch the new thresholds to the related protection group.

5.1.2 Policy Configuration for Protection Groups

ADS provides the following anti-DDoS policies and rules:

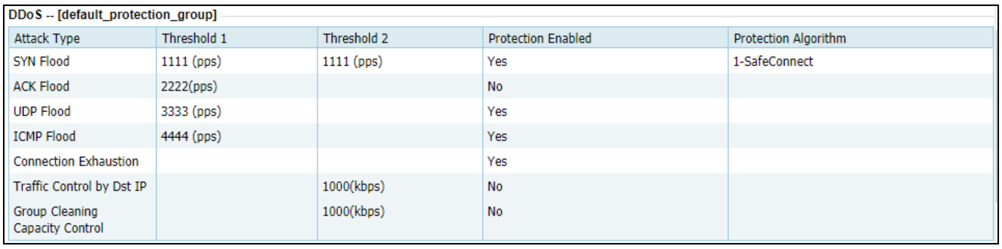
- DDoS protection policies
- Anomalous packet filtering rules
- Reflection protection policy
- HTTP keyword checking policy
- Port check policy
- HTTPS protection policy
- HTTP protection policy
- DNS keyword checking policy
- DNS protection policy
- TCP control parameters protection policy
- TCP regular expression protection policy
- Botnet & IP behavior control policy
- SIP protection policy
- UDP session authentication policy
- UDP payload check policy
- UDP regular expression protection policy
- UDP protection policy
- ICMP protection policy
- Watermark protection policy
- Programmable rule
- Protocol ID check policy

5.1.2.1 DDoS Protection Policy

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

Figure 5-15 shows parameters of the default DDoS protection policy.

Figure 5-15 DDoS protection policy area



DDoS -- [default_protection_group]

Attack Type	Threshold 1	Threshold 2	Protection Enabled	Protection Algorithm
SYN Flood	1111 (pps)	1111 (pps)	Yes	1-SafeConnect
ACK Flood	2222(pps)		No	
UDP Flood	3333 (pps)		Yes	
ICMP Flood	4444 (pps)		Yes	
Connection Exhaustion			Yes	
Traffic Control by Dst IP		1000(kbps)	No	
Group Cleaning Capacity Control		1000(kbps)	No	

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

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

Parameter	Description
Attack Type	Types of DDoS attacks that can be blocked.
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.
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.
- **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.

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.
- **Protection Algorithm**
  - **0-SynCheck** applies to symmetrical networks only.
  - **1-SafeConnect**, **2-DynaCheck**, and **3-SeqCheck** apply to both symmetrical and asymmetrical networks. When ADS is deployed in out-of-path mode, you can only select one of the three algorithms.

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.

This policy is enabled by 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.

This policy is enabled by default. After this policy is enabled, related protection will be implemented through the UDP Protection Policy.

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.

This policy is enabled by default. After this policy is enabled, related protection will be implemented through the ICMP Protection Policy.

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 Protection Rules.)

Carpet Bombing

Carpet bombing protection can work only when carpet bombing protection rules are configured. You can only select **Yes** or **No** for it. The carpet bombing protection takes effect only when **Group** is selected for **Scope of Validity** under **Advanced > Carpet Bombing Protection > Configuration**. (For how to configure carpet bombing protection rules, see section 8.5 Carpet Bombing Protection.Carpet Bombing Protection

) and you select **Yes** here. If the actions of the carpet bombing protection rule include "add to blacklist", you need to first enable the group-specific blocklist. For detailed configuration, see section 8.5 Carpet Bombing Protection.

Group-Specific Cleaning Capacity Control

Threshold 2: specifies the maximum traffic allowed to arrive at the protection group, above which the excess traffic is dropped. The value ranges from 0 to 48000000.

This policy is enabled by default.

Note	
Note	• Generally, the system adopts default DDoS protection settings. If you want to edit settings of threshold 1 or 2, contact NSFOCUS technical support. • You should apply protection algorithms to the DDoS protection policies according to the actual network environment and the deployment mode. Otherwise, network interruption may occur.

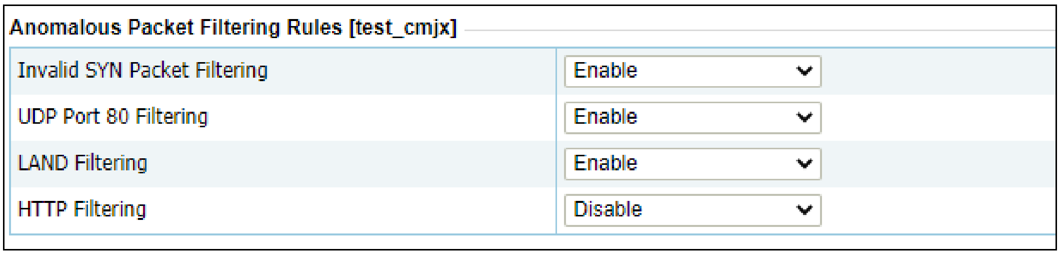
5.1.2.2 Anomalous Packet Filtering Rules

Anomalous packet filtering rules include rules for filtering SYN packets, UDP packets destined for port 80, LAND packets, and HTTP packets. ADS can handle traffic according to these rules only when they are enabled.

Figure 5-16 shows the area for configuration of anomalous packet filtering rules. You can perform the following operations on the rules:

- **Enable**: enable a rule. ADS filters traffic once anomalous packets with certain signatures are detected.
- **Disable**: disable a rule.
- **Enable only in protection state**: ADS filters out anomalous packets with certain signatures only when in the protection state.

Figure 5-16 Anomalous packet filtering rules



Anomalous Packet Filtering Rules [test_cmjx]

Invalid SYN Packet Filtering	Enable
UDP Port 80 Filtering	Enable
LAND Filtering	Enable
HTTP Filtering	Disable

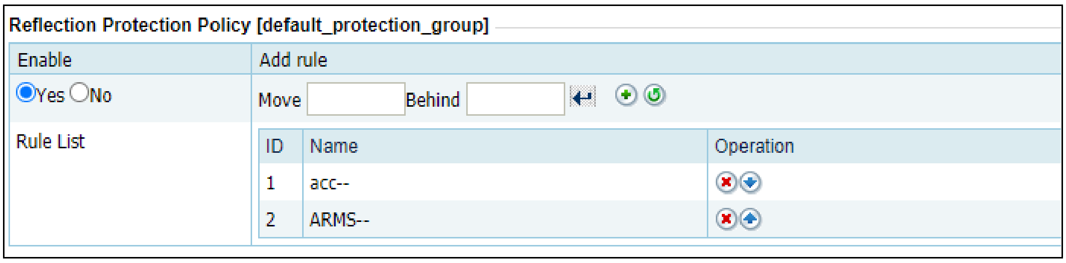
5.1.2.3 Reflection Protection Policy

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 Reflection Protection Rules.

Figure 5-17 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 5-17 Reflection protection policy of a protection group



Reflection Protection Policy [default_protection_group]

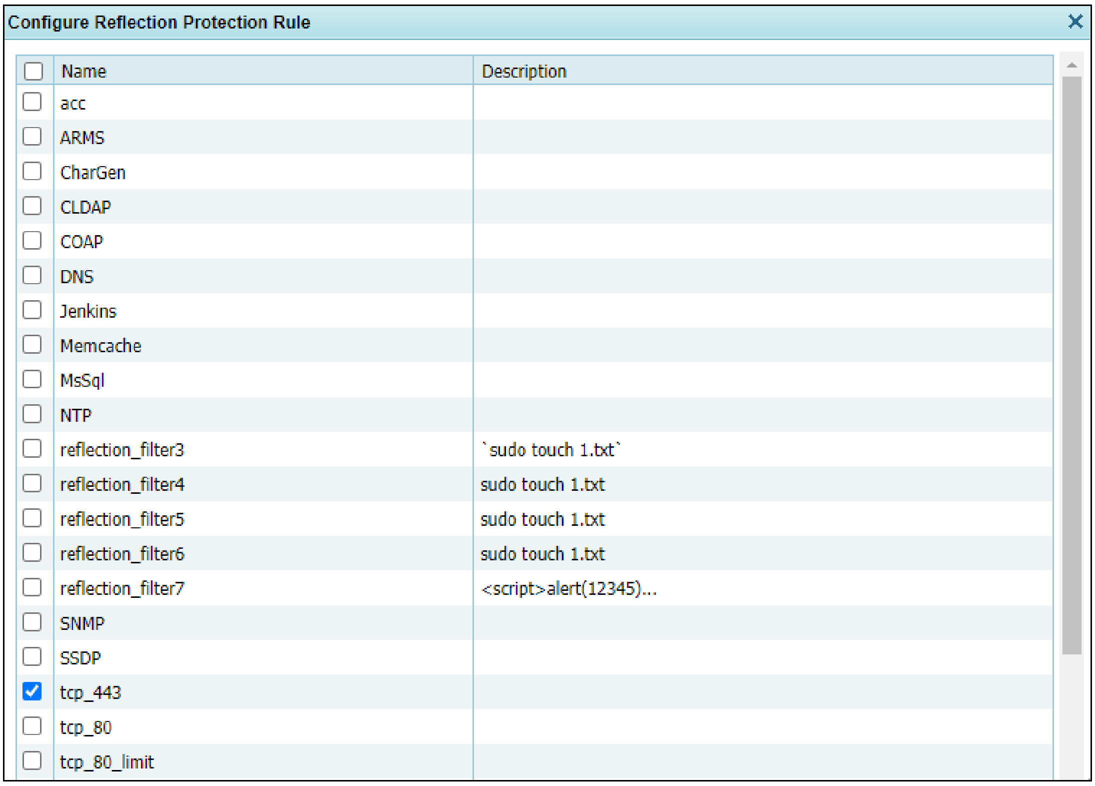
Enable	Add rule		
● Yes ○ No	Move ____ Behind ____ ↵ ⊕ ↻		
Rule List	ID	Name	Operation
	1	acc--	✖ ⬇
	2	ARMS--	✖ ⬆

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 5-18. 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 5-18 Adding reflection protection rules



Configure Reflection Protection Rule ×

□	Name	Description
□	acc	
□	ARMS	
□	CharGen	
□	CLDAP	
□	COAP	
□	DNS	
□	Jenkins	
□	Memcache	
□	MsSql	
□	NTP	
□	reflection_filter3	`sudo touch 1.txt`
□	reflection_filter4	sudo touch 1.txt
□	reflection_filter5	sudo touch 1.txt
□	reflection_filter6	sudo touch 1.txt
□	reflection_filter7	<script>alert(12345)...
□	SNMP	
□	SSDP	
☑	tcp_443	
□	tcp_80	
□	tcp_80_limit	

5.1.2.4 HTTP Keyword Checking Policy

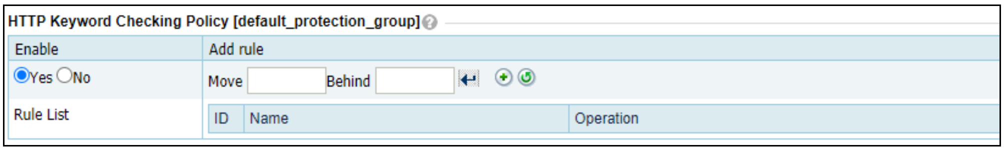
HTTP keyword checking is a process by which ADS checks specific fields in HTTP attack traffic against keywords and then takes the specified action against those packets that match a rule.

Figure 5-19 shows the current HTTP keyword checking rules.

Note

- 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. The administrator may need to adjust the rule sequence as required.
- When multiple rules are hit, ADS performs protection based on the first rule.

Figure 5-19 HTTP Keyword Checking Policy area



HTTP Keyword Checking Policy [default_protection_group]

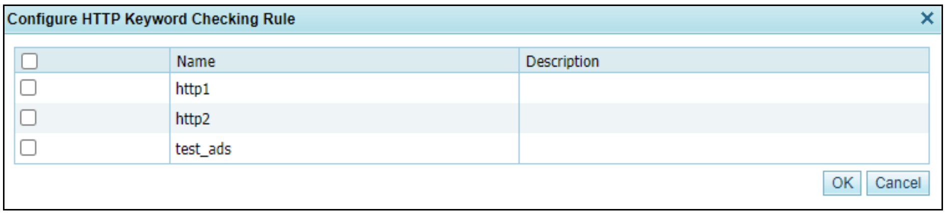
Enable	Add rule
● Yes ○ No	Move [ ] Behind [ ]
Rule List	ID | Name | Operation

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 ⬇ in the **Operation** column 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 5-20 Configuring HTTP keyword checking rules



Configure HTTP Keyword Checking Rule ✕

□	Name	Description
□	http1	
□	http2	
□	test_ads	

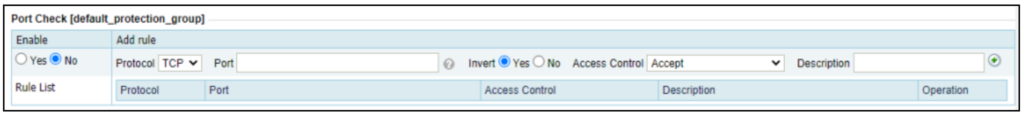
5.1.2.5 Port Check Policy

The port check policy indicates that after the port check function is enabled, the system checks the data arriving at the specified port according to the configured policy but handles the data to other ports based on the group algorithm.

Figure 5-34 shows the port check policy settings. Table 5-6 describes of a port check policy.

- ADS detects traffic by matching port check rules in a top-down manner. If a hit is found, ADS performs access control for the port according to the matching rule and stop matching other rules.
- Rearrange rules: You can click ⬆ or ⬇ to move a rule one level up or down.
- Add a rule: You can click ⊕ to add a rule.
- Delete a rule: You can click ✖ to delete a rule.

Figure 5-21 Port check policy of a protection group



Port Check [default_protection_group]

Enable: ○ Yes ● No

Add rule: Protocol TCP; Port; Invert ● Yes ○ No; Access Control Accept; Description

Rule List

Protocol	Port	Access Control	Description	Operation

Table 5-6 Parameters of a port check policy

Parameter	Description
Enable	Controls whether to enable this policy. • **Yes**: indicates that the policy is enabled. • **No**: indicates that the policy is disabled.

Parameter	Description
Protocol	Specifies the protocol, which can be **TCP** or **UDP**.
Port	Specifies the number of port to be checked. You can add a maximum of 10 rules, each of which can include 48 ports. Ports must be separated by the comma.
Invert	Controls whether to invert the port setting. **Yes**: indicates that other ports than the ones specified will be matched and **No** indicates the opposite. For example, if **Port** is set to **80** and **Invert** is set **Yes**, ADS checks ports other than port 80.
Access Control	Specifies how to handle packets matching the rule. • **Accept**: allows packets from the specified port to pass through ADS. • **Drop**: drops such packets. • **Drop and add to blacklist**: drops such packets and adds them to the blocklist.
Description	Brief description of the policy, which can contain a maximum of 15 characters.

5.1.2.6 **HTTPS Protection Policy**

HTTPS protection policies provide protection for HTTPS connections. The HTTPS protection policy empowers the system to check HTTPS packets from clients. By recording and counting HTTPS sessions from a source IP address, the system determines whether the source IP address is abnormal and marks it as abnormal if the abnormal access exists. You need to enable the blocklist function before configuring an HTTPS protection policy. For how to enable the blocklist, see section 5.2.10 Blocklist.

HTTPS protection policies are classified into three types:

- Connection Protection – Renegotiation Protection: 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 blocklist.
- Application Layer Protection – Non-decrypted Traffic Protection: In the case of no certificate, the system detects whether a source IP address is abnormal by checking HTTPS sessions from it, and automatically adds detected abnormal IP addresses to the blocklist. This type of protection includes access rate-based protection, resource-specific access protection, and large resource access protection to defend against HTTPS traffic attacks.
- Application Layer Protection – Decrypted Traffic Protection: The system configures an SSL certificate for specified destination IP addresses and ports and then authenticates clients with HTTPS protection algorithms, including HTTP2 RFC authentication, and controls SSL connections. Packets that fail the check will be dropped or their source IP addresses will be added to the blocklist.

When all protection algorithms are enabled for HTTPS protection, the matching IP addresses and ports of application layer protection – decrypted traffic protection are protected according to the decrypted traffic protection configurations, other IP addresses are protected according to the connection protection configurations, and all subsequent HTTPS packets are subject to the application layer protection – non-decrypted traffic protection configurations.

The following describes the HTTPS protection process:

- In a normal trust scenario, for example, only SYN algorithm authentication is passed, an IP address configured with application layer protection – decrypted traffic protection is protected according to the decrypted traffic protection configurations. If it is not included in any such rules, the IP address will be protected by connection protection configurations, and then the application layer protection – non-decrypted traffic protection configurations (the **Protection Port** setting works in this case).
- In an advanced trust scenario, for example, decryption algorithms authentication is passed, all packets are subject to the application layer protection – non-decrypted traffic protection configurations.
  - If the destination IP address is subject to application layer protection – decrypted traffic protection, ADS takes the specified action against those packets whose destination port is the same as the one configured in the decrypted traffic protection rule or as the protection port.
  - ADS takes the specified action against those packets whose destination port is the same as the protection port.

Table 5-7 describes the common parameters for configuring an HTTPS protection policy.

Table 5-7 HTTPS protection parameters

Parameter	Description
Protection Port	Specifies the port to protect. The value range is 0–65535, 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. Note By default, this port works for connection protection – renegotiation protection and application layer protection – non-decrypted traffic protection. If a certificate is configured for the destination IP address and destination port in an application layer protection – decrypted traffic protection rule, when finding traffic destined for this IP address, ADS further checks its destination port and will implement application layer protection – non-decrypted traffic protection for the matching traffic.
Protection Threshold	Specifies the threshold for the number of HTTPS packets (in pps) arriving at a specific port of the destination IP address. If the value is exceeded, the HTTPS protection mechanism will be triggered.

Connection Protection – Renegotiation Protection

The connection protection – renegotiation protection checks HTTPS packets from clients. Table 5-8 describes parameters for configuring a connection protection policy.

Table 5-8 Connection protection parameters

Parameter	Description
Enable	Control whether to enable the connection protection policy.
Per Source IP Renegotiation Rate Limit	Specifies the rate of new SSL connections (in pps) 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 blocklist. 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 blocklist. You need to enable the Blocklist before configuring this parameter.

Application Layer Protection – Non-decrypted Traffic Protection

This policy automatically adds detected abnormal IP addresses to the blocklist. Therefore, make sure that the blocklist function is enabled.

This type of protection includes the following three rules:

- Access Rate-based Protection: The system counts the HTTPS requests from a source IP address. The IP address will be deemed to be abnormal and added to the group-specific blocklist if its number of visits to HTTPS resources exceeds the threshold in a statistical period.
- Resource-specific Access Protection: The system counts the access from an IP address to a specific resource. If both of its number and proportion of visits to the source exceed the respective threshold in a statistical period, the source IP address is deemed to be abnormal. If the source IP address keeps abnormal in consecutive statistical periods (when **Consecutive Abnormal Cycles** is met), it will be added to the group-specific blocklist.
- Large Resource Access Protection: The system counts the access from an IP address to large resources. If both of its number and proportion of visits to large resources exceed the respective threshold in a statistical period, the source IP address is deemed to be abnormal. If the source IP address keeps abnormal in consecutive statistical periods (when **Consecutive Abnormal Cycles** is met), it will be added to the group-specific blocklist.

Table 5-9 describes the parameters for configuring an application layer protection – non-decrypted traffic protection policy. Note that the configuration parameters vary with the protection type.

Table 5-9 Application layer protection – non-decrypted traffic protection parameters

Parameter	Description
Enable	Controls whether to enable the application layer protection – non-decrypted traffic protection policy. If you select **No**, none of non-decrypted traffic protection policies take effect.
Large Resource Threshold	Specifies the minimum size of resources to be identified as large resources. Value range: 1–10485760, in KB.
Number of Visits	Specifies the maximum number of visits allowed for a source IP address in a statistical period. Value range: 1–10000.

Parameter	Description
Proportion of Visits	Specifies proportion of visits to the current HTTP resource (a specific resource or a large resource) to total visits to all resources in a statistical period. Value range: 1%–100%.
Statistical Period	Specifies the period of time in which the number of visits is counted. Value range: 1–3600, in seconds.
Consecutive Abnormal Cycles	Specifies the maximum allowed number of consecutive statistical periods during which the source IP address is deemed to be abnormal. Value range: 1–10.

Application Layer Protection – Decrypted Traffic Protection

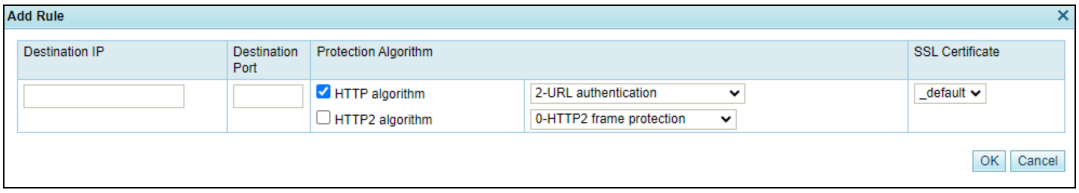
To configure an application layer protection – decrypted traffic protection policy, follow these steps:

Step 1 Select **Yes** or **No** under **Enable** to enable or disable the application layer protection – decrypted traffic protection policy.

Step 2 Create an application layer protection – decrypted traffic protection rule.

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

Figure 5-22 Creating an application layer protection – decrypted traffic protection rule



Add Rule

Destination IP	Destination Port	Protection Algorithm		SSL Certificate
		☑ HTTP algorithm	2-URL authentication	_default
		☐ HTTP2 algorithm	0-HTTP2 frame protection	

b. Table 5-10 describes parameters for creating an application layer protection – decrypted traffic protection rule.

Table 5-10 Parameters of an application layer protection – decrypted traffic protection rule

Parameter	Description
Destination IP	Specifies the destination IP address to protect. Such an IP address should be within the IP address range covered by the protection group.
Destination Port	Specifies the port number of the destination IP address to protect. Value range: 0–65535.
Protection Algorithm	Specifies the algorithm used in the rule.
SSL Certificate	Specifies the SSL certificate used in the rule. You can select the default certificate or import others as required. For how to import an SSL certificate, see section 3.4.4 SSL Certificate Import.

Step 3 After the configuration is complete, click **OK** to return to the HTTPS protection policy page.

Step 4 Configure control items for the application layer protection – decrypted traffic protection rule.

Table 5-11 Control items of an application layer protection – decrypted traffic protection rule

Parameter	Description
Enable	Controls whether to enable control of the number of new connections, failed connections, timeout connections, and HTTP2 RFC authentication of the destination port to protect.
Connection Type	Connection control items. New connections, failed connections, and timeout connections 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. • **Connection timeout**: 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. • **HTTP2 RFC authentication**: performs RFC authentication on HTTP2 packets from source IP addresses.
Threshold	Threshold of each control item: • New connections: 1–65535 • Failed connections: 1–256 • Connection timeout: 1–1000 • HTTP2 RFC authentication: 1–64
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 blocklist to block it. You need to enable the blocklist function before setting this action. For details on the blocklist, see section 5.2.10 Blocklist.

----End

5.1.2.7 HTTP Protection Policy

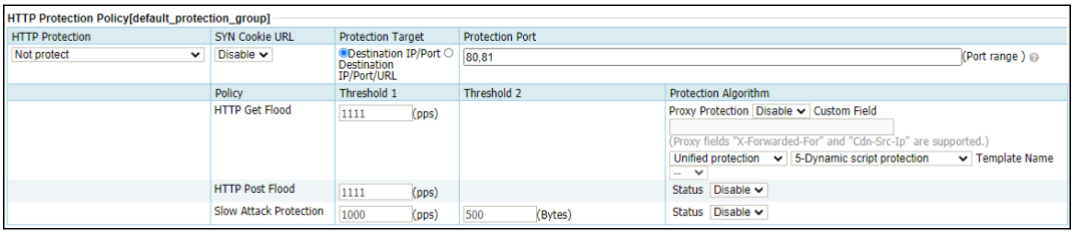
The HTTP protection policy for a protection group covers the following items:

- HTTP GET flood protection: This protection mechanism is triggered if the number of HTTP GET packets transmitted to a destination IP address per second (unit: pps) exceeds the specified value.

- HTTP POST flood protection: This protection mechanism is triggered if the number of HTTP POST packets transmitted to a destination IP address per second (unit: pps) exceeds the specified value.
- Low-and-slow attack protection: This protection mechanism is triggered if the number of HTTP packets to a destination IP address exceeds threshold 1 and the payload size of such packets is smaller than threshold 2.
- SYN cookie URL protection: If SYN Cookie URL is enabled, this protection mechanism also applies to new connections.

Figure 5-23 shows the HTTPS protection policy configuration for a protection group.

Figure 5-23 HTTP protection policy



HTTP Protection Policy[default_protection_group]

HTTP Protection	SYN Cookie URL	Protection Target	Protection Port
Not protect	Disable	● Destination IP/Port ○ Destination IP/Port/URL	80,81 (Port range)

Policy	Threshold 1	Threshold 2	Protection Algorithm
HTTP Get Flood	1111 (pps)		Proxy Protection Disable Custom Field (Proxy fields "X-Forwarded-For" and "Cdn-Src-Ip" are supported.) Unified protection 5-Dynamic script protection Template Name --
HTTP Post Flood	1111 (pps)		Status Disable
Slow Attack Protection	1000 (pps)	500 (Bytes)	Status Disable

Table 5-12 describes parameters for configuring the HTTP protection policy.

Table 5-12 Parameters for configuring the HTTP protection policy

Parameter	Description
HTTP Protection	Specifies the HTTP protection mode, which can be one of the following: • **Full protection**: Both group protection and URL rule protection are provided. • **Only on the rules of URL protection**: The protection group is protected only by URL rules. In this case, SYN Cookie URL cannot be enabled. • **Not protect**
SYN Cookie URL	Controls whether to enable or disable SYN Cookie URL. • **Enable**: SYN Cookie URL protection can be enabled only when the following conditions are met: 1. **Full protection** is selected for **HTTP Protection**. 2. **Status** is set to **Enable** for HTTP POST flood protection. After SYN Cookie URL is enabled, proxy protection will be disabled automatically. • **Disable**: 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** automatically disables SYN Cookie URL.
Protection Target	Specifies the protection target, which can be either of the following: • **Destination IP/Port**: indicates that ADS determines whether to enter the protection state based on the destination IP address and port. • **Destination IP/Port/URL**: indicates that ADS determines whether to enter the protection state based on the destination IP address, port, and URL.

Parameter		Description
Protection Port		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, like 80,90-92. The value range is 0–65535. Also, HTTPS port numbers must be excluded.
HTTP Get Flood	**Threshold 1**	Specifies the HTTP GET traffic rate (pps), above which HTTP GET flood protection is triggered. If the rate of HTTP GET traffic to a destination IP address exceeds the specified value, HTTP GET flood protection is triggered. The value range is 0–48000000.
	Proxy Protection	Controls whether to enable proxy protection. After HTTP GET flood protection is enabled, you can enable proxy protection. You are advised to enable this function if a proxy server exists in your network. Note Enabling proxy protection automatically disables SYN Cookie URL.
	Custom Field	After proxy protection is enabled, you can configure this parameter to allow ADS to accurately identify the actual proxied IP address.
	Protection mode	Specifies the HTTP GET protection mode, which can be either of the following: • **Unified protection**: ADS provides HTTP GET protection in a unified way, without distinguishing between traffic from PCs and mobile applications. • **Precision protection**: ADS applies different protection policies for traffic from PCs and mobile applications based on the setting of the user-agent field. ➢ For PC protection, you can choose whether to enable precision protection and configure an HTTP GET protection algorithm. ➢ For mobile application protection, you can choose whether to enable precision protection, reference user-agent rules for mobile devices, and configure an HTTP GET protection algorithm.
	Protection algorithm	Specifies the protection algorithm, which can be one of the following, with **2_URL authentication** as the default: • **0_TAG authentication** and **1_HTTPCOOKIES authentication** verify the destination IP address by adding authentication information into HTTP packets. • **2_URL authentication** verifies the destination IP address by adding information similar to cookies into URL requests. • **3_ASCII image authentication** and **4_BMP image authentication** verify the destination IP address by adding an image. • **5_Dynamic script protection** verifies the destination IP address by executing dynamic scripts on the client. • **6_Legend game authentication** and **7_FCS** verify the destination IP address by checking the packets of the "Legend" game and the flash server. • **8_Pattern matching check** verify the destination IP address by matching a signature string that is defined under **Advanced** > **Pattern Matching** (see section 8.2 Pattern Matching Rules for the configuration of pattern matching).

Parameter		Description
		Note • **6_Legend authentication**, **7_FCS check** and **8_Pattern matching check** are specific to protection groups and available only when SYN Cookie URL is enabled. • Enabling SYN Cookie URL disables the **0_TAG authentication** and **1_HTTPCOOKIES authentication** algorithms.
	Template Name	Specifies the template name. This parameter is required only when **4_BMP image authentication** is selected for **Protection Algorithm**. It is used to select the response page that contains a CAPTCHA code image. The default value is **--**. For response page settings, see section 5.1.5 Response Page Settings.
	User-Agent Rule	Indicates user-agent rules. These rules are required only for precision protection. Packets that match a user-agent rule referenced here are deemed traffic of a mobile device, or regarded as traffic of a PC. You can click ⊕ and select one or more existing user-agent rules. At least one rule should be selected and at most five can be configured. For details about user-agent rules for mobile devices, see section 5.1.7 Mobile User-Agent Rules.
HTTP Post Flood	**Threshold 1**	Specifies the HTTP POST traffic rate (pps) above which HTTP POST flood protection is triggered. If the rate of HTTP POST traffic to a destination IP address exceeds the specified value, HTTP POST flood protection is triggered. The value range is 0–48000000.
	Status	Controls whether to enable or disable HTTP POST flood protection. • **HTTP POST flood** protection can be enabled only when **HTTP Protection** is set to **Full protection** or **Only on the rules of URL protection**. • If **HTTP Protection** is set to **Not protect**, the setting of **Status** changes to **Disable** automatically.
Slow Attack Protection	**Threshold 1**	Specifies the number of HTTP packets arriving at the destination IP address per second, above which low-and-slow protection is triggered.
	Threshold 2	Specifies length of HTTP packets arriving at the destination IP address, below which low-and-slow protection is triggered.
	Status	Controls whether to enable low-and-slow attack protection. This type of protection can be enabled only when HTTP protection is enabled and **Full protection** is selected for **HTTP Protection**. Low-and-slow attack protection is triggered if the number of HTTP packets to a destination IP address per second exceeds threshold 1 and the payload size of such packets is smaller than threshold 2. Note Setting **HTTP Protection** to **Not protect** or **Only on the rules of URL protection** automatically disables low-and-slow attack protection.

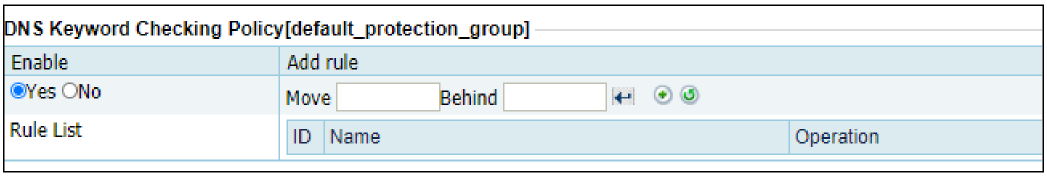
5.1.2.8 DNS Keyword Checking Policy

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 5-24 shows 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 5-24 DNS Keyword Checking Policy area



DNS Keyword Checking Policy[default_protection_group]

Enable	Add rule
● Yes ○ No	Move Behind
Rule List	ID | Name | Operation

Table 5-13 describes parameters of the default DNS keyword checking policy.

Table 5-13 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.

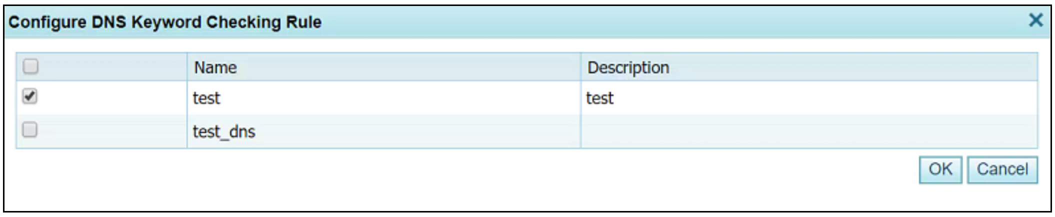
On this page, you can edit the DNS keyword checking policy as follows:

- **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 5-25 Configuring DNS keyword checking rules



Configure DNS Keyword Checking Rule

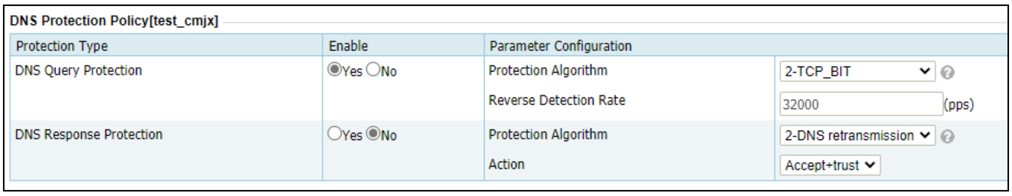
□	Name	Description
☑	test	test
□	test_dns	

5.1.2.9 DNS Protection Policy

DNS protection is a policy against DNS attacks and spoofing targeting DNS servers. Figure 5-26 shows the current DNS protection policy.

The DNS retransmission algorithm for DNS response protection applies to common servers (such as web servers), instead of recursive DNS servers and authoritative DNS servers.

Figure 5-26 DNS Protection Policy area



DNS Protection Policy[test_cmjx]

Protection Type	Enable	Parameter Configuration	
DNS Query Protection	● Yes ○ No	Protection Algorithm	2-TCP_BIT
		Reverse Detection Rate	32000 (pps)
DNS Response Protection	○ Yes ● No	Protection Algorithm	2-DNS retransmission
		Action	Accept+trust

Table 5-14 describes parameters of the DNS protection policy.

Table 5-14 Parameters of the DNS protection policy

Parameter		Description
DNS Query Protection	Enable	Controls whether to enable DNS query protection. **Yes** indicates that ADS provides DNS query protection.
	Protection Algorithm	Specifies an algorithm for DNS query protection. Options include **1-Default**, **2-TCP_BIT**, **3-DNS_CNAME,** and **4-DNS retransmission.**
	Reverse Detecti on Rate	Specifies the maximum rate of reverse detection packets. The value ranges from 1 to 240000000.
DNS Response Protection	Enable	Controls whether to enable DNS response protection. **Yes** indicates that ADS provides DNS response protection.
	Protection Algorithm	Specifies an algorithm for DNS query protection. Options include **1-Default** and **2-DNS retransmission**.
	Action	Specifies how to handle DNS responses: • **Accept**: passes through DNS responses authenticated by the protection algorithm

Parameter		Description
		- **Accept+trust**: passes through DNS responses authenticated by the protection algorithm and adds the source IP address of these responses to the trust list.

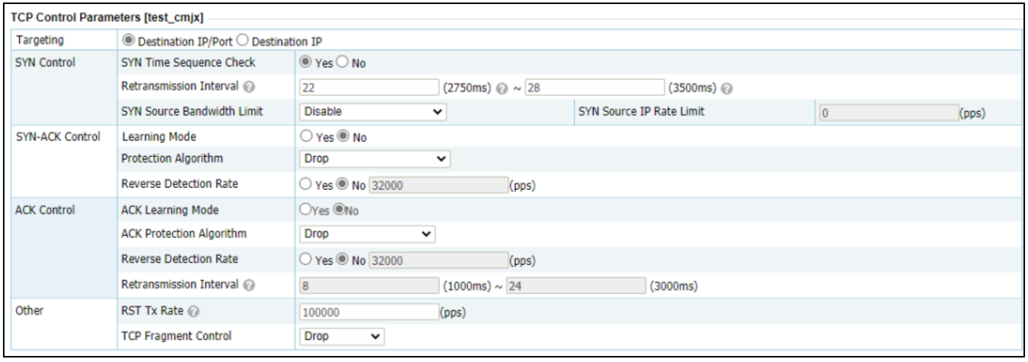
Note	DNS protection is triggered when the number of UDP packets transmitted per second exceeds the specified threshold. For the setting of UDP flood thresholds, see section 5.1.2.1 DDoS Protection Policy.

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

5.1.2.10 TCP Control Parameters Protection Policy

Figure 5-27 shows parameters of the TCP control parameters protection policy.

Figure 5-27 TCP Control Parameters Protection Policy area



TCP Control Parameters [test_cmjx]

Targeting	● Destination IP/Port ○ Destination IP			
SYN Control	SYN Time Sequence Check	● Yes ○ No		
	Retransmission Interval	22 (2750ms) ~ 28 (3500ms)		
	SYN Source Bandwidth Limit	Disable	SYN Source IP Rate Limit	0 (pps)
SYN-ACK Control	Learning Mode	○ Yes ● No		
	Protection Algorithm	Drop		
	Reverse Detection Rate	○ Yes ● No 32000 (pps)		
ACK Control	ACK Learning Mode	○Yes ●No		
	ACK Protection Algorithm	Drop		
	Reverse Detection Rate	○ Yes ● No 32000 (pps)		
	Retransmission Interval	8 (1000ms) ~ 24 (3000ms)		
Other	RST Tx Rate	100000 (pps)		
	TCP Fragment Control	Drop		

Table 5-15 describes parameters of the TCP control policy.

Table 5-15 Parameters of the TCP control policy

Control Item	Parameter	Description
SYN Control	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:

Control Item	Parameter	Description
		• **Disable**: disables this function. • **Drop and add to blacklist**: adds the IP address of the source host to the blocklist 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.
SYN-ACK Control	Learning Mode	Controls whether to enable the SYN-ACK learning mode. This learning mode works only in non-protection state. 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 learning mode works only when neither SYN protection nor ACK protection is available.
	Protection Algorithm	Specifies the SYN-ACK protection algorithm. Options include **Drop**, **Close**, **Source authentication**, **Session check**, and **Combined ACK protection**. • **Drop**: drops SYN-ACK packets. • **Close**: allows SYN-ACK packets to pass through the authentication by the algorithm and checks them in subsequent protection processes. • **Source authentication**: checks resent SYN-ACK packets and passes them through if requirements for authentication by this algorithm are met; otherwise, these packets are dropped. • **Session check**: This check is done on SYN-ACK packets that pass through source authentication. If session check requirements are met, packets are allowed to pass through, or will be dropped. • **Combined ACK protection**: This check is done on SYN-ACK packets that pass through source authentication. The check must be coupled with the ACK protection algorithm. Packets that meet check requirements are allowed to pass through, or will be dropped.
	Reverse Detection Rate	Specifies the maximum rate at which ADS sends SYN-ACK packets for reverse detection. The value range is 1–240000000.
ACK Control	ACK Learning Mode	Controls whether to enable the ACK learning mode. This learning mode works only in non-protection state. 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 learning mode works only when neither ACK protection is available.
	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.

Control Item	Parameter	Description
		• **Drop**: drops ACK packets. • **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. • **ACK Check**: indicates that packets from source IP addresses that meet check requirements will be allowed to pass through, or will be dropped.
	Reverse Detection Rate	Specifies the maximum rate at which ADS sends ACK packets for reverse detection. The value range is 1–240000000.
	Retransmission Interval	Specifies how many milliseconds will elapse between when the ACK packet is discarded for the first time and when it is resent.
Other	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. • **Accept**: allows TCP fragments in IPv4 or IPv6 packets to pass through. • **Drop**: drops TCP fragments in IPv4 or IPv6 packets. • **Rate-limiting**: restricts the transmission rate of TCP fragments.

5.1.2.11 TCP Regular Expression Protection Policy

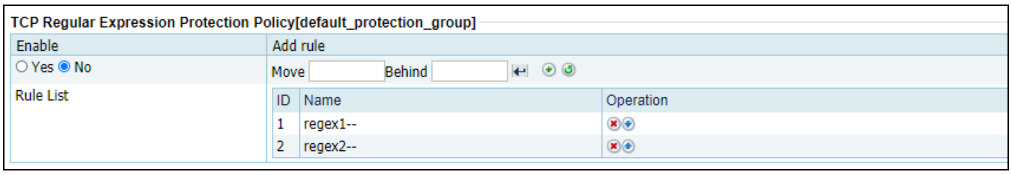
After configuring regular expression rules, you can enable the TCP regular expression protection and reference created regular expression rules. For details on regular expression rules, see section 5.2.4 Regular Expression Rules.

Figure 5-28 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 5-28 TCP regular expression protection policy



TCP Regular Expression Protection Policy[default_protection_group]

Enable

○ Yes ● No

Rule List

Add rule

Move Behind

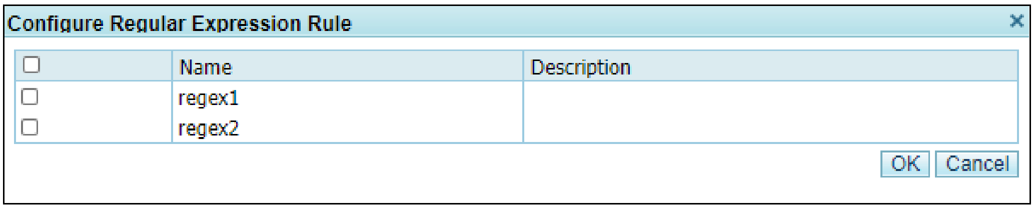
ID	Name	Operation
1	regex1--	✖ ⬇
2	regex2--	✖ ⬆

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 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 addition dialog box shown in Figure 5-29. 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 5-29 Adding regular expression rules



Configure Regular Expression Rule ✕

□	Name	Description
□	regex1	
□	regex2	

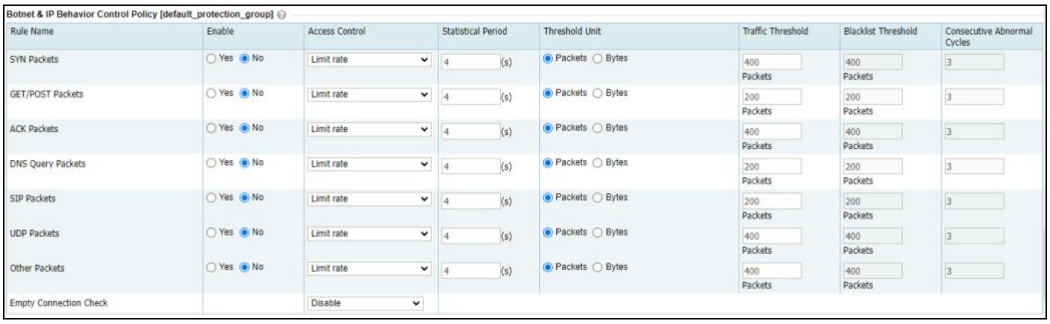
5.1.2.12 Botnet & IP Behavior Control Policy

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 blocklist and limiting its TX rate, the system can effectively defend against botnet attacks.

Supporting more protocols, the botnet and IP behavior control policy implements more granular protection against packet attacks from botnet hosts to further improve ADS's protection capability.

Figure 5-30 shows botnet and IP behavior control parameters.

Figure 5-30 Botnet & IP Behavior Control Policy area



Botnet & IP Behavior Control Policy [default_protection_group]

Rule Name	Enable	Access Control	Statistical Period	Threshold Unit	Traffic Threshold	Blacklist Threshold	Consecutive Abnormal Cycles
SYN Packets	○ Yes ● No	Limit rate	4 (s)	● Packets ○ Bytes	400 Packets	400 Packets	3
GET/POST Packets	○ Yes ● No	Limit rate	4 (s)	● Packets ○ Bytes	200 Packets	200 Packets	3
ACK Packets	○ Yes ● No	Limit rate	4 (s)	● Packets ○ Bytes	400 Packets	400 Packets	3
DNS Query Packets	○ Yes ● No	Limit rate	4 (s)	● Packets ○ Bytes	200 Packets	200 Packets	3
SIP Packets	○ Yes ● No	Limit rate	4 (s)	● Packets ○ Bytes	200 Packets	200 Packets	3
UDP Packets	○ Yes ● No	Limit rate	4 (s)	● Packets ○ Bytes	400 Packets	400 Packets	3
Other Packets	○ Yes ● No	Limit rate	4 (s)	● Packets ○ Bytes	400 Packets	400 Packets	3
Empty Connection Check		Disable					

Table 5-16 describes botnet and IP behavior control parameters.

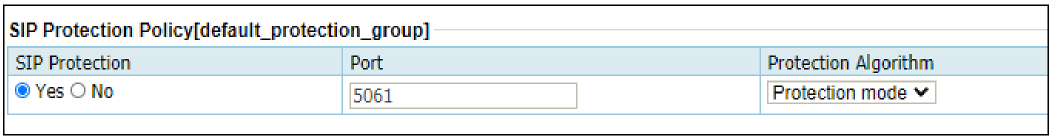
Table 5-16 Botnet and IP behavior control parameters

Parameter	Description
Enable	Controls whether to enable packet rate control.
Access Control	Specifies the action the system takes to exert access control for trusted IP addresses whose packet forwarding rate (pps or bps) exceeds the threshold. It has the following values: • **Limit rate**: limits the traffic rate. • **Limit rate & add to blacklist**: adds an IP address to the blocklist and limits the traffic rate from this IP address when its traffic exceeds the specified value. To select this value, you must enable the blocklist function first. For details, see section 5.2.10 Blocklist. **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 blocklist 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.
Statistical Period	Specifies the statistical period for calculating the percentage of packets that match the rule.
Threshold Unit	Specifies how to measure the packet forwarding rate. Options include **Packets** and **Bytes**.
Traffic Threshold	Specifies the maximum number of packets that a trusted IP address can send within the statistical period. More packets than allowed will be dropped and an attack event will be logged. Value range: 1–11840000 in packets or 1–1000000000 in bytes.
Blacklist Threshold	Specifies the maximum number of packets that a trusted IP address can send within the statistical period. When the actual traffic exceeds the threshold, the source IP address will be added to the blocklist and an attack event will be logged. Value range: 1–11840000 in packets or 1–1000000000 in bytes. Note This parameter can be configured only when **Limit rate & add to blacklist** is selected for **Access Control**.
Consecutive Abnormal Cycles	Specifies the number of consecutive statistical periods during which a trusted IP address send more packets than the **Blacklist Threshold**. Value range: 1–10. Note This parameter can be configured only when **Limit rate & add to blacklist** is selected for **Access Control**.

5.1.2.13 SIP Protection Policy

With the SIP protection policy, the system provides protection against packets using the Session Initiation Protocol (SIP). Figure 5-31 shows parameters of the SIP protection policy.

Figure 5-31 SIP Protection Policy area



SIP Protection Policy[default_protection_group]

SIP Protection	Port	Protection Algorithm
● Yes ○ No	5061	Protection mode

Table 5-17 describes parameters of the SIP protection policy.

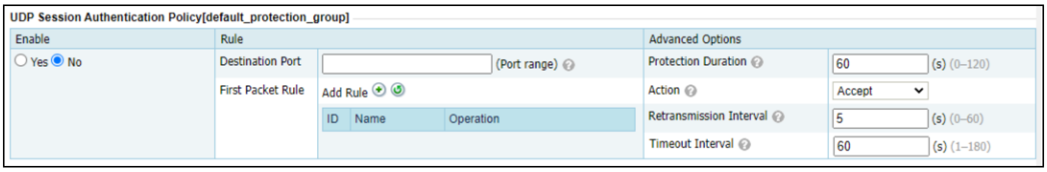
Table 5-17 Parameters of the SIP protection policy

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. • **Protection mode**: The system performs protection against register attacks and invite attacks, and identifies attack packets via interaction with register and invite packets. • **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.

5.1.2.14 UDP Session Authentication Policy

The UDP session authentication policy uses a regular expression to check the first packets for signature matches. For matching packets, ADS checks whether they are retransmitted within the configured retransmission interval, and if yes, allows subsequent packets to go through.Figure 5-32 shows parameters of the UDP session authentication policy.

Figure 5-32 UDP session authentication policy



UDP Session Authentication Policy[default_protection_group]

Enable: ○ Yes ● No

Rule

Destination Port: (Port range)

First Packet Rule: Add Rule

ID	Name	Operation

Advanced Options

Protection Duration: 60 (s) (0–120)

Action: Accept

Retransmission Interval: 5 (s) (0–60)

Timeout Interval: 60 (s) (1–180)

Table 5-18 describes parameters of the UDP session authentication policy.

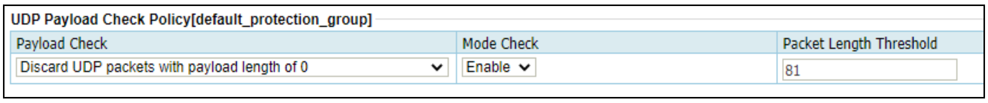
Table 5-18 Parameters of the UDP session authentication policy

Parameter		Description
Enable		Controls whether to enable UDP session authentication.
Rule	Destination Port	Specifies ports in the range of 0–65535, with 53 and the destination port specified in the SIP protection policy excluded. A single port, port ranges, or multiple ports can be typed. Multiple values should be separated by the comma (,). UDP session authentication is triggered only when the destination port number of UDP packets matches the configured one.
	First Packet Rule	Click ⊕ to select an existing UDP regular expression in the list and click **OK**. Note that only its regular expression is referenced here and its action setting does not work.
Advanced Options	Protection Duration	When a destination IP address is under protection, some sessions may be recorded because of the first packet being sent already. In this case, checking the first packet would interrupt the session. Therefore, the protection duration is introduced to prevent this from happening. If a UDP packet, whose quadruple contains a matching destination port, does not match the first packet rule, it is recorded as part of a new session and subsequent packets will be handled as per the configured action. The value is an integer in the range of 0–120, in seconds. The value **0** indicates that the protection is disabled.
	Action	Specifies how subsequent packets of a session recorded in the protection duration are protected. Options include: • **Accept**: directly forwards packets. • **Default**: checks packets against subsequent policies.
	Retransmission Interval	Specifies the period of time allowed for retransmission of the first packet. The value is an integer in the range of 0–60, in seconds. The value **0** indicates that no retransmission required for the authentication purpose.
	Timeout Interval	Specifies the timeout interval for a recorded session. If no packet is transmitted within the timeout interval, ADS stops recording the session. Subsequently, the session needs to be reauthenticated. The value is an integer in the range of 1–180, in seconds.

5.1.2.15 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 5-33 shows UDP payload check policy.

Figure 5-33 UDP Payload Check Policy area



UDP Payload Check Policy[default_protection_group]

Payload Check	Mode Check	Packet Length Threshold
Discard UDP packets with payload length of 0	Enable	81

Table 5-19 describes parameters of the UDP payload check policy.

Table 5-19 Parameters of the UDP payload check policy

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	Controls 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.

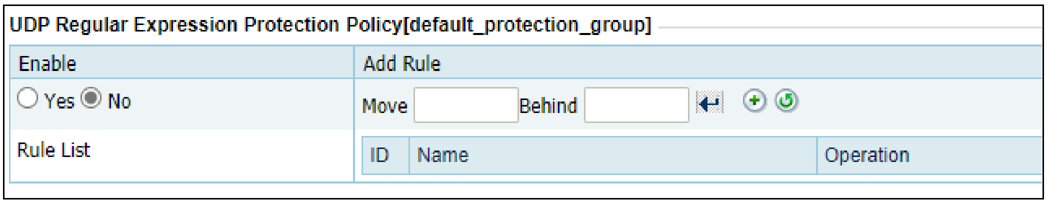
5.1.2.16 UDP Regular Expression Protection Policy

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.

0 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 5-34 UDP regular expression protection policy



UDP Regular Expression Protection Policy[default_protection_group]

Enable	Add Rule
○ Yes ● No	Move ▭ Behind ▭ ↵ ⊕ ↻
Rule List	ID | Name | Operation

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

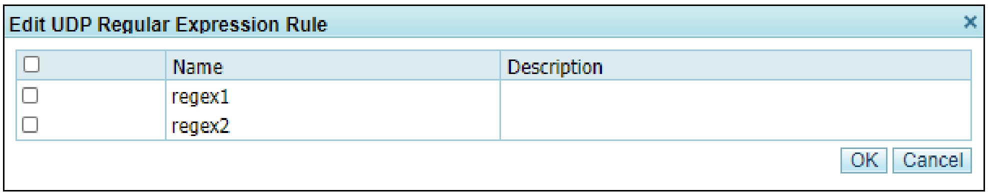
- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- Rearrange rules: Click ⬆ or ⬇ to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3** indicates that the first rule will be put below the third rule. Click ↵ to commit the change.

- **Add rule**: Click ⊕ to open the rule configuration dialog box shown in Figure 5-35. 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 5-35 Adding UDP regular expression rules



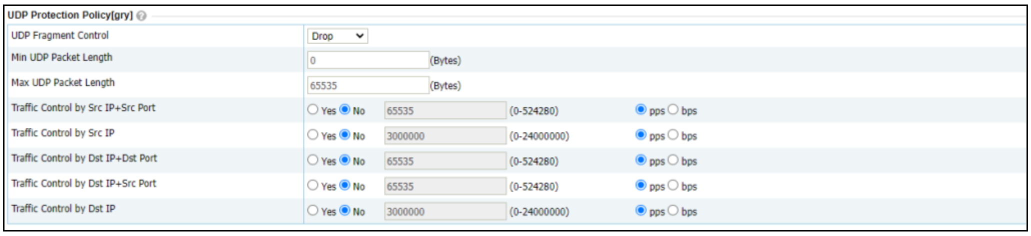
Edit UDP Regular Expression Rule ×

□	Name	Description
□	regex1	
□	regex2	

5.1.2.17 UDP Protection Policy

With the UDP protection policy, the system checks UDP requests from clients, and drops requests that do not meet specified conditions. Figure 5-36 shows parameters of the UDP protection policy.

Figure 5-36 UDP Protection Policy area



UDP Protection Policy[gry]

UDP Fragment Control	Drop			
Min UDP Packet Length	0 (Bytes)			
Max UDP Packet Length	65535 (Bytes)			
Traffic Control by Src IP+Src Port	○ Yes ● No	65535	(0-524280)	● pps ○ bps
Traffic Control by Src IP	○ Yes ● No	3000000	(0-24000000)	● pps ○ bps
Traffic Control by Dst IP+Dst Port	○ Yes ● No	65535	(0-524280)	● pps ○ bps
Traffic Control by Dst IP+Src Port	○ Yes ● No	65535	(0-524280)	● pps ○ bps
Traffic Control by Dst IP	○ Yes ● No	3000000	(0-24000000)	● pps ○ bps

Table 5-20 describes parameters of the UDP protection policy.

Table 5-20 Parameters of the UDP protection policy

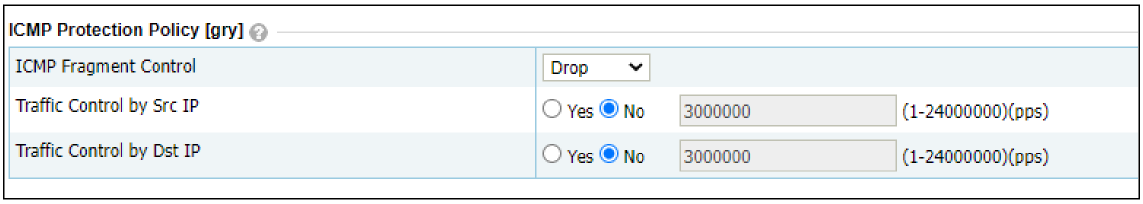
Parameter	Description
UDP Fragment Control	Controls whether to drop detected UDP fragments in IPv4 or IPv6 packets. • **Accept**: allows UDP fragments to pass through. • **Drop**: drops UDP fragments. • **Limit rate**: limits the packet transmission rate to a specified threshold when UDP fragments are detected.
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.

Parameter	Description
	This parameter is disabled by default. The value range is 1–524280, with **65535** as the default value.
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 0–24000000, 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 0–524280, 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 0–524280, 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 0–24000000, with **3000000** as the default value.

5.1.2.18 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 5-37 shows parameters of the ICMP protection policy.

Figure 5-37 ICMP Protection Policy area



ICMP Protection Policy [gry]

ICMP Fragment Control	Drop		
Traffic Control by Src IP	○ Yes ● No	3000000	(1-24000000)(pps)
Traffic Control by Dst IP	○ Yes ● No	3000000	(1-24000000)(pps)

Table 5-21 describes parameters of the ICMP protection policy.

Table 5-21 Parameters of the ICMP protection policy

Parameter	Description
ICMP Fragment Control	Controls whether to drop the detected ICMP fragments. • **Accept**: allows ICMP fragments to pass through. • **Drop**: drops ICMP fragments. • **Limit rate:** limits the packet transmission rate to a specified

Parameter	Description
	threshold when ICMP fragments are detected.
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.

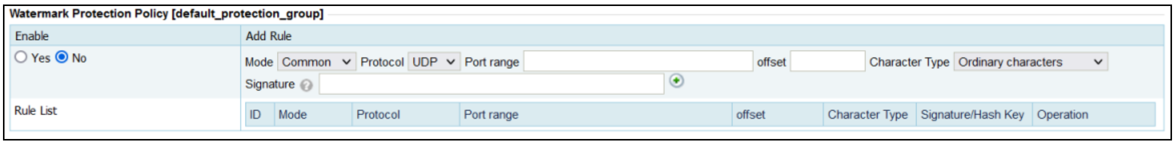
5.1.2.19 Watermark Protection Policy

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. 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.

Figure 5-38 shows the watermark protection policy.

Figure 5-38 Watermark protection policy



Watermark Protection Policy [default_protection_group]

Enable

○ Yes ● No

Add Rule

Mode: Common Protocol: UDP Port range: offset: Character Type: Ordinary characters

Signature:

Rule List

ID	Mode	Protocol	Port range	offset	Character Type	Signature/Hash Key	Operation

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

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- **Add a rule**: Create a common rule or advanced rule by setting **Mode** to **Common** or **Advanced**. After the configuration is complete, click ⊕. Then the watermark protection policy is displayed in the rule list.
- Delete a rule: Click ✖ to delete a rule.

Table 5-22 describes parameters for configuring a watermark protection policy.

Table 5-22 Parameters of a watermark protection policy

Parameter	Description
Mode	Mode of the watermark protection policy. • **Advanced**: When a data packet hits a specified rule, if the original payload length is smaller than "offset + 4", the XOR operation is performed on the hash key and the four bytes from the start position (followed by 0 if there are less than four bytes). The packet will be allowed to pass through if the XOR

Parameter	Description
	operation result is the same as the last four bytes; otherwise, it will be dropped. • **Common**: When a data packet hits a specified rule, if the original payload matches the signature from the offset position, it is allowed to pass through. Otherwise, the packet will be dropped. This mode is applicable to businesses with distinct features.
Protocol	Specifies the protocol for matching packets. Options include **UDP** and **TCP**. Only UDP is supported for the common mode.
Port range	Specifies the port for matching packets. Value range: 0–65535. You can type up to 5 ports or port ranges, separated by the comma (,), such as 1-20,21-100. Ports in the port range cannot overlap.
Offset	Specifies the offset of packet transmission. Value range: 0–1480.
hashKey	Specifies the hash key. Value range: 0–4294967295. Note This parameter is only available for the advanced mode.
Character Type	Specifies the character type for matching packets, which can be **Ordinary characters** or **Hexadecimal characters**. Note This parameter is only available for the common mode.
Signature	Specifies the specific character for matching packets. You can type up to 16 hexadecimal characters or ordinary characters. In the former case, \x may not be contained like \"ababab\" or "\xab\xab\". In the latter case, the string should not contain the following characters: ! $ \ " \x. For specific requirements, see Signature. Note This parameter is only available for the common mode.

5.1.2.20 Programmable Rule

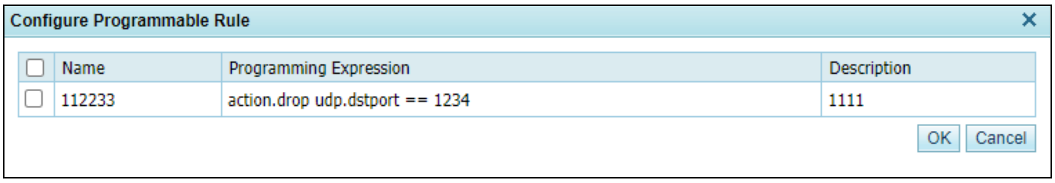
If you have configured programmable rules, you can enable the programmable rule for a protection group and reference the created programmable rule. For details on how to configure programmable rules, see section 5.2.9 Programmable Rules.Programmable Rules

A protection group can only reference one programmable rule.

You can perform the following operations on the programmable rule:

- **Enable**: Select **Yes** or **No** to enable or disable the programmable rule.
- Add a rule: Click ⊕ to open the rule configuration page shown in Figure 5-39. Select one programmable rule and then click **OK**.
- Delete a rule: You can click ⊗ to delete a rule.

Figure 5-39 Adding a programmable rule



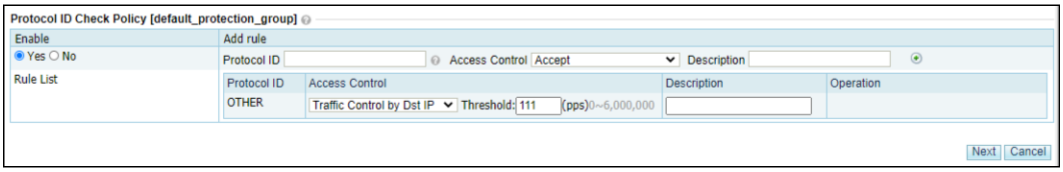
Configure Programmable Rule

□	Name	Programming Expression	Description
□	112233	action.drop udp.dstport == 1234	1111

5.1.2.21 Protocol ID Check Policy

The protocol ID check policy allows users to define different protection actions for other protocols than TCP, UDP, ICMP, and ICMPv6. Figure 5-40 shows protocol ID check parameters. The check 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 **Accept**, **Drop**, or **Drop and add to blacklist**.

Figure 5-40 Protocol ID check policy



Protocol ID Check Policy [default_protection_group]

Enable: ● Yes ○ No

Add rule: Protocol ID | Access Control: Accept | Description

Rule List

Protocol ID	Access Control	Description	Operation
OTHER	Traffic Control by Dst IP Threshold: 111 (pps)0~6,000,000		

Table 5-23 describes parameters of a protocol ID check policy.

Table 5-23 Parameters of a protocol ID check policy

Parameter		Description
Enable		Controls whether to enable this policy. • **Yes**: enables this policy • **No**: disables this policy.
Add rule	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: • **Accept**: 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 blocklist. 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.

5.1.3 Protection Group Policy Templates

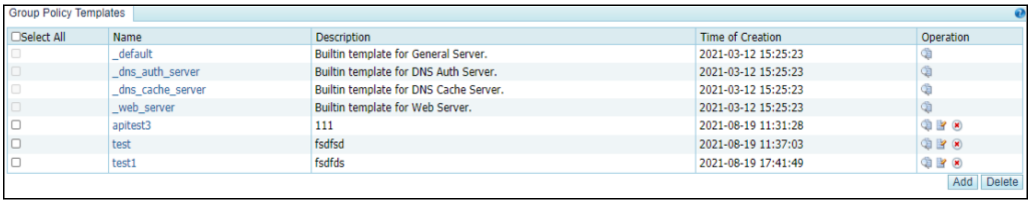
You can create and configure a protection group policy template and apply it to a newly created protection group.

5.1.3.1 Creating a Protection Group Policy Template

To create a protection group policy template, perform the following steps:

Step 1 Choose **Policy** > **Anti-DDoS** > **Group Policy Templates** to open the built-in protection group policy template list of the system.

Figure 5-41 Protection group policy templates



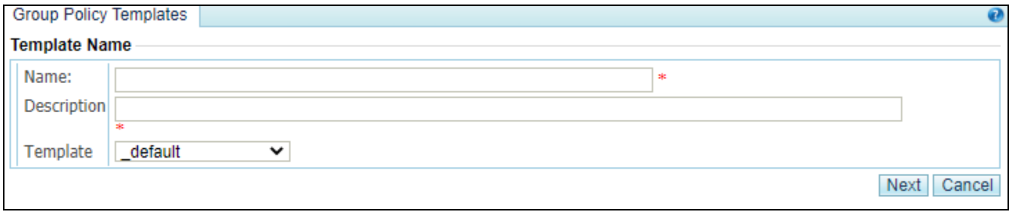
Group Policy Templates

□Select All	Name	Description	Time of Creation	Operation
□	_default	Builtin template for General Server.	2021-03-12 15:25:23	
□	_dns_auth_server	Builtin template for DNS Auth Server.	2021-03-12 15:25:23	
□	_dns_cache_server	Builtin template for DNS Cache Server.	2021-03-12 15:25:23	
□	_web_server	Builtin template for Web Server.	2021-03-12 15:25:23	
□	apitest3	111	2021-08-19 11:31:28	
□	test	fsdfsd	2021-08-19 11:37:03	
□	test1	fsdfds	2021-08-19 17:41:49	

Step 2 Configure basic information of a protection group policy template.

To the lower right of the list, click **Add** to create a protection group policy template, as shown in Figure 5-42.

Figure 5-42 Basic information of a protection group policy template



Group Policy Templates

Template Name

Name: *

Description *

Template _default

Table 5-24 describes parameters for creating a protection group policy template.

Table 5-24 Parameters for creating a protection group policy template

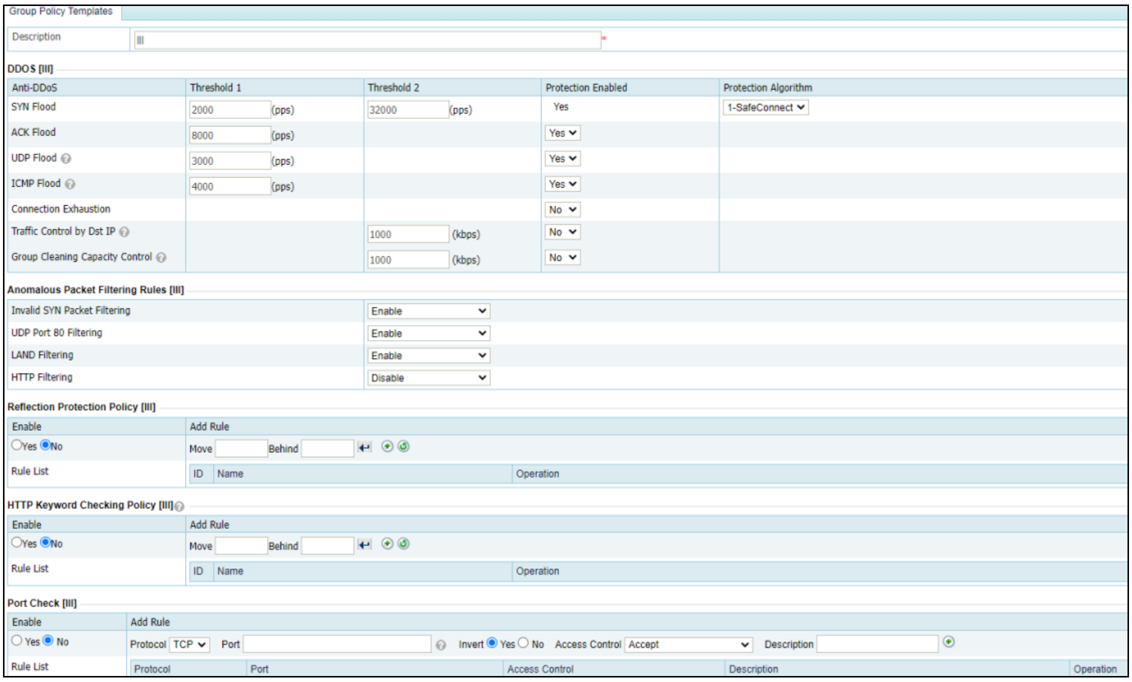
Parameter	Description
Name	Name of the new protection group policy template. The name must be unique and must be a string of no more than 32 characters that can only be letters, digits, or underscores. For a custom template, the name cannot begin with an underscore (_).
Description	Description of a protection group policy template. It supports a maximum of 64 characters and cannot contain carriage returns or line breaks.
Template	Existing template out of which this new template is created. Either a default template or a custom one can be selected here.

Step 3 Configure various protection policies for the protection group policy template.

Click **Next** to configure protection policies for this template.

For details about protection policies, see section 5.1.2 Policy Configuration for Protection Groups.

Figure 5-43 Configuring protection policies for a protection group policy template



Group Policy Templates

Description: |||

DDOS [III]

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

Anomalous Packet Filtering Rules [III]

Invalid SYN Packet Filtering	Enable
UDP Port 80 Filtering	Enable
LAND Filtering	Enable
HTTP Filtering	Disable

Reflection Protection Policy [III]

Enable: ○ Yes ● No

Add Rule: Move ___ Behind ___

Rule List:

ID	Name	Operation

HTTP Keyword Checking Policy [III]

Enable: ○ Yes ● No

Add Rule: Move ___ Behind ___

Rule List:

ID	Name	Operation

Port Check [III]

Enable: ○ Yes ● No

Add Rule: Protocol TCP Port ___ Invert ● Yes ○ No Access Control Accept Description ___

Rule List:

Protocol	Port	Access Control	Description	Operation

Step 4 Click **Next** to configure the access policy.

a. Click **Add** to configure a group-specific access control rule. For details, see 5.2.1 Access Control Rules.

b. You need to specify whether to enable the blocklist, block period, and whether to enable proxy monitoring. For details about the blocklist function, see section 5.2.10 Blocklist.

c. Click **Add** to configure a group-specific GeoIP rule. You need to choose whether to enable the group-specific rule, and specify the source location, access control, and description. For details about the GeoIP rules, see 5.2.3 GeoIP Rules.

d. Specify whether to enable the threat intelligence-based protection for the group and specify the action taken against traffic whose source/destination IP address has a match in the intelligence database. Options include **Block** and **Traffic Control by Dst IP**. For details about NTI, see section 8.4 Collaboration with NTI.

Note	The group-specific NTI protection takes effect only when the **Protection Scope is set** to **Group** under **Advanced** > **NTI** > **NTI Configuration.**

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

Step 6 After the configuration, click **Apply** at the upper-right corner to commit the settings.

----End

5.1.3.2 Viewing a Protection Group Policy Template

On the protection group policy template list shown in Figure 5-41, click the name of a template to view its details.

After viewing template details, click **Back** to return to the **Group Policy Templates** page.

5.1.3.3 Editing a Protection Group Policy Template

You can edit the description and protection policies of a protection group policy template.

On the protection group policy template list shown in Figure 5-41, click 📝 in the **Operation** column to reset protection policies and the blocklist of a protection group.

Edit protection policies on the new page, and click **Complete** to save the settings.

5.1.3.4 Deleting a Protection Group Policy Template

You can delete protection group policy templates one by one or in bulk on ADS.

- Method 1: On the protection group policy template list shown in Figure 5-41, click ⊗ in the **Operation** column of a template and click **OK** in the confirmation dialog box to delete it.
- Method 2: On the protection group policy template list shown in Figure 5-41, select several templates (or select check boxes in the **Select All** column), click **Delete** to the lower right of the list, and then click **OK** in the confirmation dialog box to delete them.

5.1.4 Advanced Global Parameters

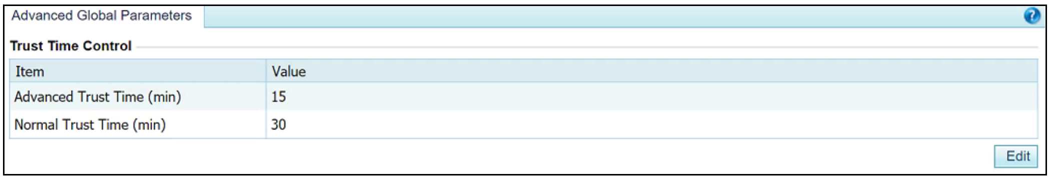
You can configure trust control parameters.

The procedure is as follows:

Step 1 Choose **Policy > 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 5-44.

Figure 5-44 Advanced Global Parameters page



Advanced Global Parameters

Trust Time Control

Item	Value
Advanced Trust Time (min)	15
Normal Trust Time (min)	30

Table 5-25 describes advanced global parameters.

Table 5-25 Advanced global parameters

Parameter	Description
Advanced Trust Time (min)	Specifies the time during which a source IP address authenticated with the

Parameter	Description
	advanced algorithm stays in the trust list. The value ranges from 1 to 3600, with **5** as the default.
Normal Trust Time (min)	Specifies the 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

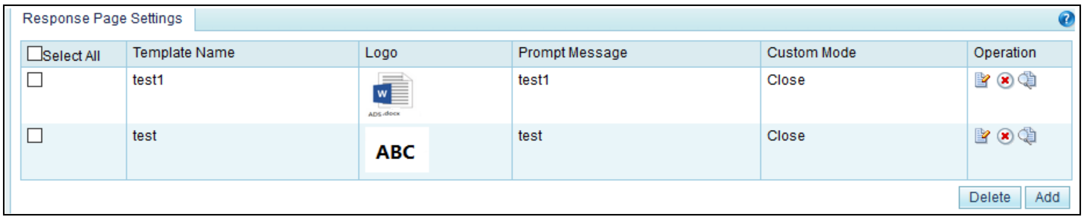
If **4-BMP image authentication** is specified as the algorithm for the HTTP protection policy and a template is specified, a client attempting to access a server through ADS needs to input a code for authentication in the automatically displayed response page. The client can access the server only after 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 **Policy** > **Anti-DDoS** > **Response Page Settings**.

Figure 5-45 Response Page Settings tab page



Response Page Settings

□Select All	Template Name	Logo	Prompt Message	Custom Mode	Operation
□	test1		test1	Close	
□	test	ABC	test	Close	

Step 2 Click **Add**.

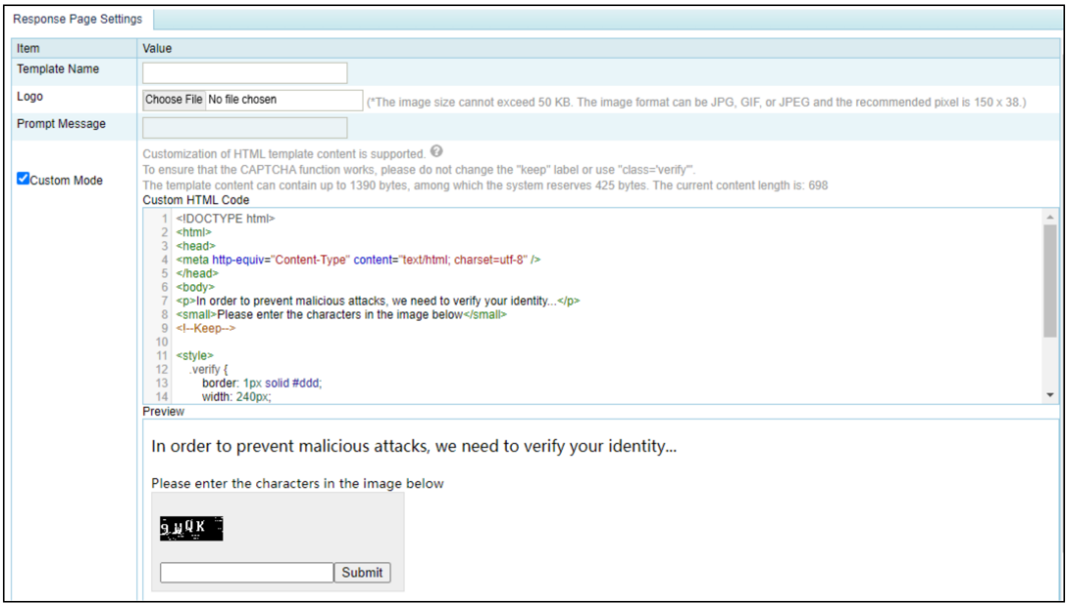
The **Response Page Settings** page appears, as shown in Figure 5-46.

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 5-46 Response Page Settings page



Response Page Settings

Item	Value
Template Name	
Logo	Choose File No file chosen (*The image size cannot exceed 50 KB. The image format can be JPG, GIF, or JPEG and the recommended pixel is 150 x 38.)
Prompt Message	
☑Custom Mode	Customization of HTML template content is supported. To ensure that the CAPTCHA function works, please do not change the "keep" label or use "class='verify'". The template content can contain up to 1390 bytes, among which the system reserves 425 bytes. The current content length is: 698 Custom HTML Code

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<p>In order to prevent malicious attacks, we need to verify your identity...</p>
<small>Please enter the characters in the image below</small>
<!--Keep-->

<style>
   .verify {
       border: 1px solid #ddd;
       width: 240px;
```

Preview

In order to prevent malicious attacks, we need to verify your identity...

Please enter the characters in the image below

Table 5-26 describes parameters for creating a response page.

Table 5-26 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 5-45, 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 5-45, 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 5-45, 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.

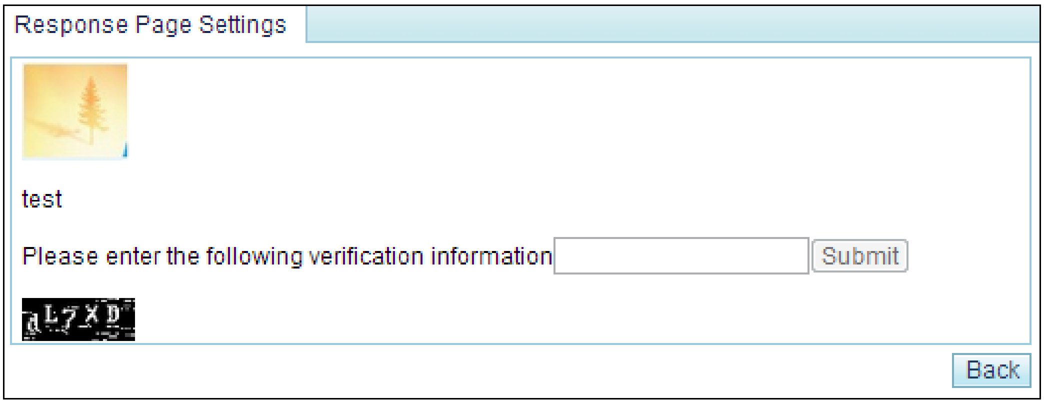
5.1.5.4 Previewing a Response Page

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

Step 1 On the page shown in Figure 5-45, click 🔍 in the row of a response page.

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

Figure 5-47 Response page preview



Response Page Settings

test

Please enter the following verification information [ ] Submit

Back

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

----End

5.1.6 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.

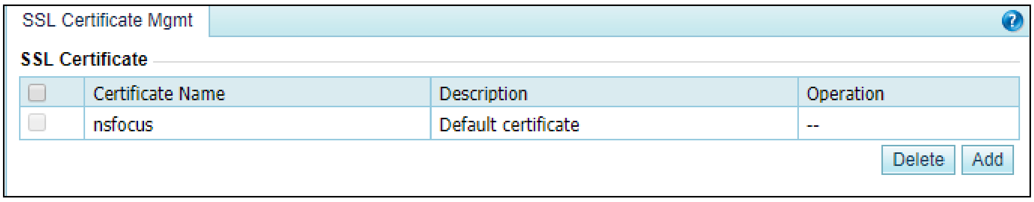
ADS provides the **nsfocus** certificate upon delivery. This certificate cannot be edited or deleted. You can add other certificates as required.

5.1.6.1 Adding an SSL Certificate

To add an SSL certificate, perform the following steps:

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

Figure 5-48 SSL certificate management



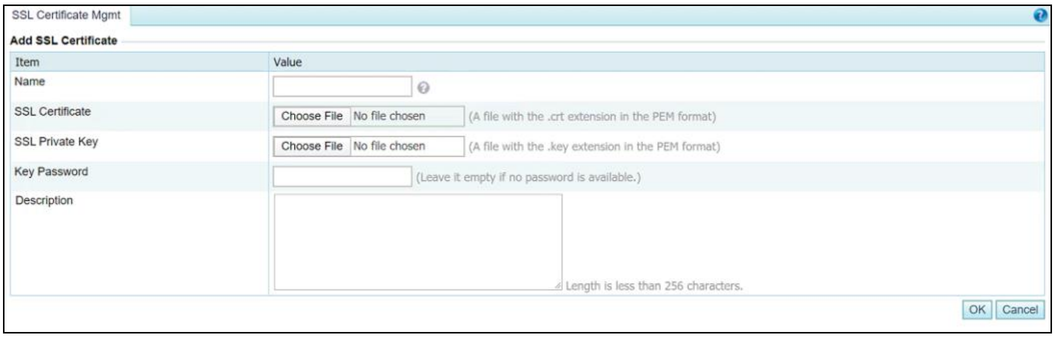
SSL Certificate Mgmt

SSL Certificate

□	Certificate Name	Description	Operation
□	nsfocus	Default certificate	--

Step 2 Click **Add**.

Figure 5-49 Adding an SSL certificate



SSL Certificate Mgmt

Add SSL Certificate

Item	Value
Name	
SSL Certificate	Choose File No file chosen (A file with the .crt extension in the PEM format)
SSL Private Key	Choose File No file chosen (A file with the .key extension in the PEM format)
Key Password	(Leave it empty if no password is available.)
Description	Length is less than 256 characters.

Table 5-27 describes parameters of an SSL certificate.

Table 5-27 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 **Choose File** to select an SSL certificate file.
SSL Private Key	Click **Choose 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.

Parameter	Description
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

5.1.6.2 Editing an SSL Certificate

To edit an SSL certificate, perform the following steps:

Step 1 On the SSL certificate list shown in Figure 5-48, 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

5.1.6.3 Deleting an SSL Certificate

On the SSL certificate list shown in Figure 5-48, click ⊗ in the **Operation** column of a certificate and click **OK** in the displayed confirmation dialog box to delete this certificate.

5.1.7 Mobile User-Agent Rules

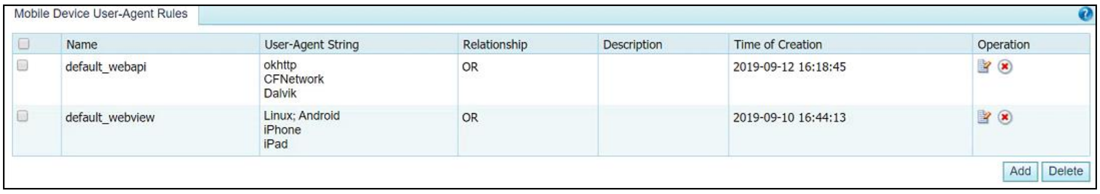
Mobile user-agent rules are used to filter traffic of mobile applications. Packets that match such a user-agent rule are deemed as mobile traffic, or will be regarded as traffic of a PC.

You can create, modify, and delete mobile user-agent rules, but cannot delete rules that are being referenced. A maximum of 32 rules can be created. Two default built-in rules (default_webapi and default_webview) cannot be deleted. This section describes how to create a mobile user-agent rule.

To create a mobile user-agent rule, perform the following steps:

Step 1 Choose **Policy** > **Anti-DDoS** > **Mobile Device User-Agent Rules**.

Figure 5-50 Mobile user-agent rules

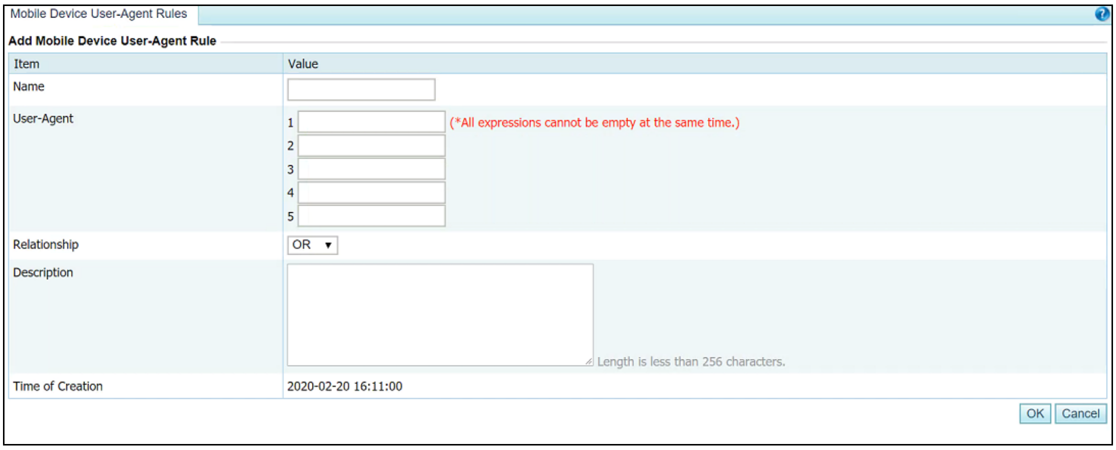


Mobile Device User-Agent Rules

□	Name	User-Agent String	Relationship	Description	Time of Creation	Operation
□	default_webapi	okhttp CFNetwork Dalvik	OR		2019-09-12 16:18:45	
□	default_webview	Linux; Android iPhone iPad	OR		2019-09-10 16:44:13	

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

Figure 5-51 Adding a mobile user-agent rule



Mobile Device User-Agent Rules

Add Mobile Device User-Agent Rule

Item	Value
Name	
User-Agent	1 (*All expressions cannot be empty at the same time.) 2 3 4 5
Relationship	OR
Description	Length is less than 256 characters.
Time of Creation	2020-02-20 16:11:00

Table 5-28 describes parameters for adding a mobile user-agent rule.

Table 5-28 Parameters for adding a mobile user-agent rule

Parameter	Description
Name	Specifies the name of the mobile user-agent rule. It can contain a maximum of 20 characters.
User-Agent	Specifies one or more user-agent strings that need to be matched against the **User-Agent** field of packets. Packets that contain the **User-Agent** field matching a string specified here are regarded as mobile traffic, or will be deemed as traffic of PCs. For each rule, at least one user-agent string should be configured and at most five can be typed here. Each string can contain a maximum of 100 characters.
Relationship	Specifies the relationship of user-agent strings. • **OR**: Packets that contain the **User-Agent** field matching one string specified here are regarded as mobile traffic. • **AND**: Packets that contain the **User-Agent** field matching all strings specified here are regarded as mobile traffic.
Description	Indicates the description of the new rule. It can contain a maximum of 256 characters.

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

----End

5.2 Access Control Policies

The system provides the access control list (ACL), blocklist, and allowlist 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
- HTTP Keyword Checking
- Connection Exhaustion Protection Rules
- URL-ACL Protection Rules
- Programmable Rules
- Blocklist
- Allowlist

5.2.1 Access Control Rules

Access control rule allows ADS to control the traffic passing through it and determine how (accept, filter, limit rate, 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
- Querying Access Control Rules

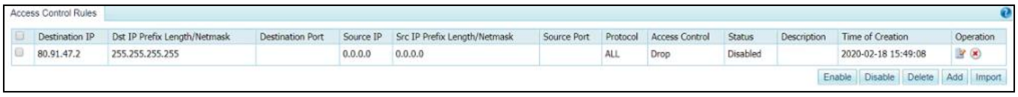
5.2.1.1 Creating an Access Control Rule

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 5-52 List of access control rules

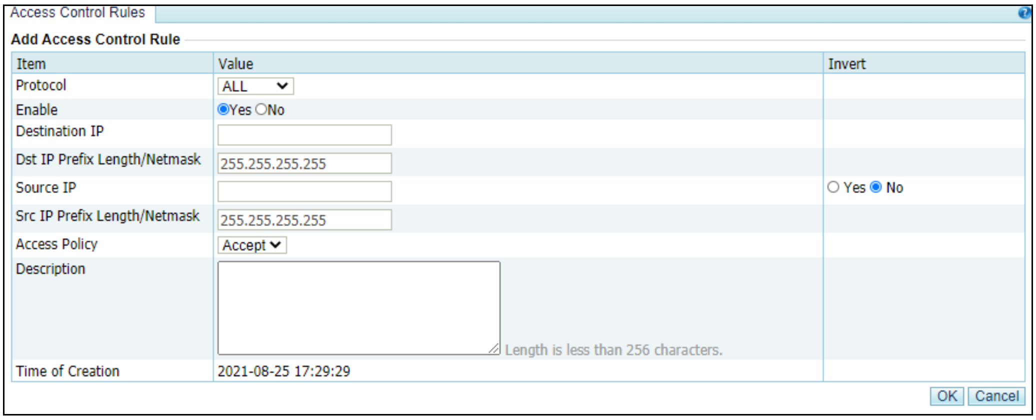


Access Control Rules

□	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
□	80.91.47.2	255.255.255.255		0.0.0.0	0.0.0.0		ALL	Drop	Disabled		2020-02-18 15:49:08	

Step 2 Click **Add**.

Figure 5-53 Creating an access control rule



Access Control Rules

Add Access Control Rule

Item	Value	Invert
Protocol	ALL	
Enable	● Yes ○ No	
Destination IP		
Dst IP Prefix Length/Netmask	255.255.255.255	
Source IP		○ Yes ● No
Src IP Prefix Length/Netmask	255.255.255.255	
Access Policy	Accept	
Description	Length is less than 256 characters.	
Time of Creation	2021-08-25 17:29:29	

Table 5-29 describes parameters for creating an access control rule.

Table 5-29 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.

Parameter	Description
Access Policy	Action performed by the ADS device on packets with specified signatures. It has the following options: • **Accept:** allows such packets to pass through. • **Drop**: drops the packets once they are detected. • **Filter**: 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

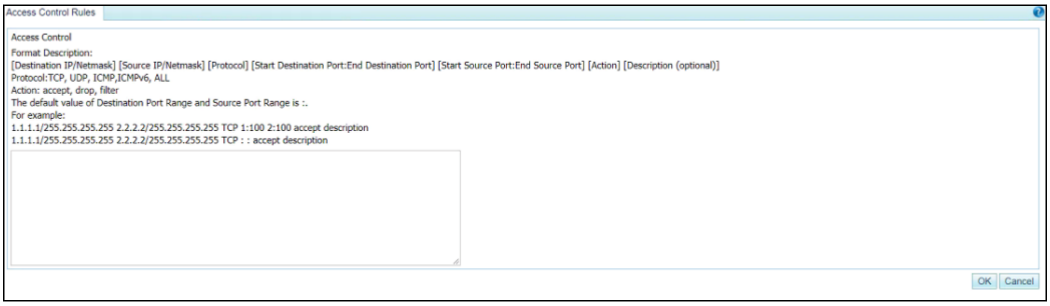
5.2.1.2 Creating Access Control Rules in Batches

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 5-54 Creating access control rules in batches



Access Control Rules

Access Control

Format Description:

[Destination IP/Netmask] [Source IP/Netmask] [Protocol] [Start Destination Port:End Destination Port] [Start Source Port:End Source Port] [Action] [Description (optional)]

Protocol:TCP, UDP, ICMP,ICMPv6, ALL

Action: accept, drop, filter

The default value of Destination Port Range and Source Port Range is :.

For example:

1.1.1.1/255.255.255.255 2.2.2.2/255.255.255.255 TCP 1:100 2:100 accept description

1.1.1.1/255.255.255.255 2.2.2.2/255.255.255.255 TCP : : accept description

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

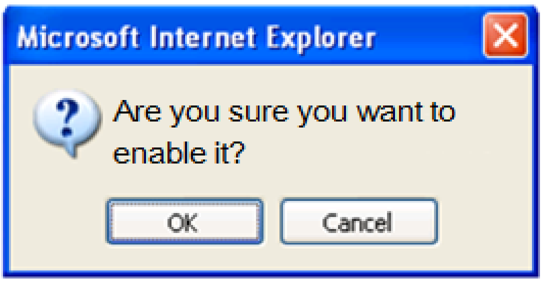
To enable access control rules, perform the following steps:

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 5-55.

Figure 5-55 Enabling access control rules



Microsoft Internet Explorer

Are you sure you want to enable it?

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

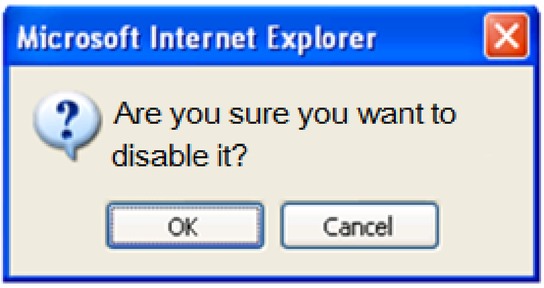
To disable access control rules, perform the following steps:

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 5-56.

Figure 5-56 Confirmation dialog box



Microsoft Internet Explorer

Are you sure you want to disable it?

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.

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.

You can also type the rule IDs in the **Move** and **Behind** text boxes above the access control rule list. For example, **Move 1 Behind 3** indicates that the first rule will be put below the third rule. Click ↵ to commit the change.

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.

5.2.1.7 Querying Access Control Rules

You can filter access control rules by destination IP, source IP, source port, destination port, protocol, access control, status, and description. After specifying the query conditions, click **Search**. Then the page lists only access control rules meeting the query conditions.

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.

You can create a maximum of 32 reflection protection rules.

This section covers the following topics:

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

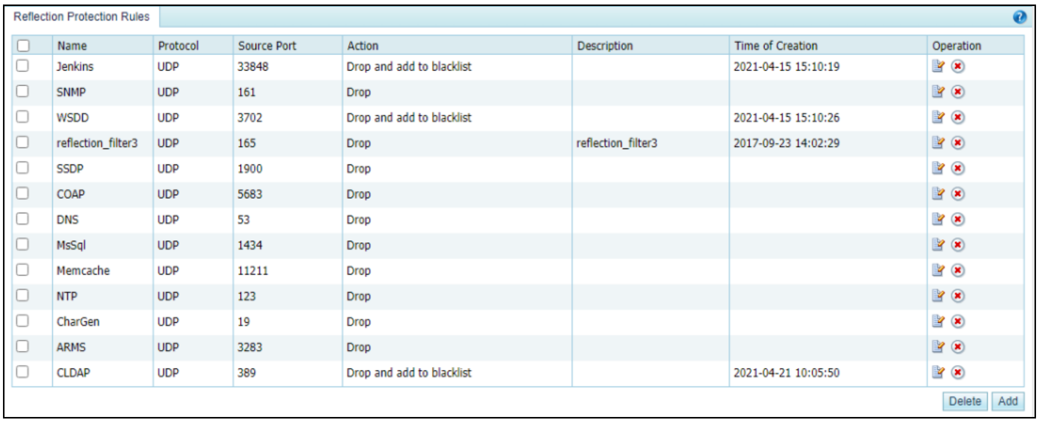
5.2.2.1 Creating a Reflection Protection Rule

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

The reflection protection rule list is displayed, as shown in Figure 5-57.

Initially, the list provides six predefined rules: Jenkins, WSDD, COAP, ARMS, CHARGEN, SSDP, NTP, DNS, SNMP, MS SQL, Memcache, and CLDAP.

Figure 5-57 Reflection protection rules



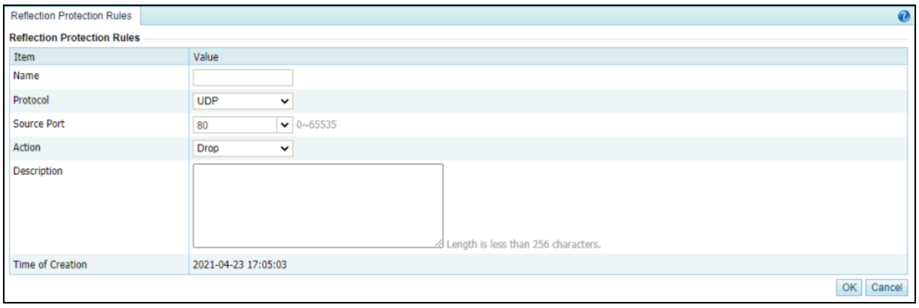
Reflection Protection Rules

□	Name	Protocol	Source Port	Action	Description	Time of Creation	Operation
□	Jenkins	UDP	33848	Drop and add to blacklist		2021-04-15 15:10:19	
□	SNMP	UDP	161	Drop			
□	WSDD	UDP	3702	Drop and add to blacklist		2021-04-15 15:10:26	
□	reflection_filter3	UDP	165	Drop	reflection_filter3	2017-09-23 14:02:29	
□	SSDP	UDP	1900	Drop			
□	COAP	UDP	5683	Drop			
□	DNS	UDP	53	Drop			
□	MsSql	UDP	1434	Drop			
□	Memcache	UDP	11211	Drop			
□	NTP	UDP	123	Drop			
□	CharGen	UDP	19	Drop			
□	ARMS	UDP	3283	Drop			
□	CLDAP	UDP	389	Drop and add to blacklist		2021-04-21 10:05:50	

Step 2 Click **Add**.

A dialog box for creating a reflection protection rule appears, as shown in Figure 5-58.

Figure 5-58 Creating a reflection protection rule



Reflection Protection Rules

Reflection Protection Rules

Item	Value
Name	
Protocol	UDP
Source Port	80 0~65535
Action	Drop
Description	Length is less than 256 characters.
Time of Creation	2021-04-23 17:05:03

Table 5-30 describes parameters for creating a reflection protection rule.

Table 5-30 Parameters of a reflection protection rule

Parameter	Description
Name	Name of the reflection protection rule. The name must be unique.
Protocol	Protection type. The options include **UDP** amd **TCP**.
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 blocklist. Before selecting this option, you must enable the blocklist. For details on the blocklist, see section 5.2.10 Blocklist • **Limit rate**: 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.

Parameter	Description
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 5-57, 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 5-57, 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 5-57, 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 (**Accept**, **Filter**, **Drop** or **Limit rate**) against packets that are found to match the rule based on the destination IP address and source location.

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 destination 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 of the destination IP address less than 120 bits are high-priority rules.

You can create a maximum of 128 GeoIP rules.

This section covers the following topics:

- Creating a GeoIP Rule
- Configuring a GeoIP Library

5.2.3.1 Creating a GeoIP Rule

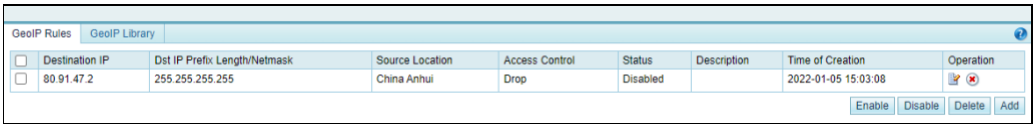
Initially, the GeoIP rule list is empty. You can create, enable, disable, edit, or delete a GeoIP rule. The procedures are the same as those for access control rules. For details, see related descriptions in section 5.2.1 Access Control Rules.

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 5-59.

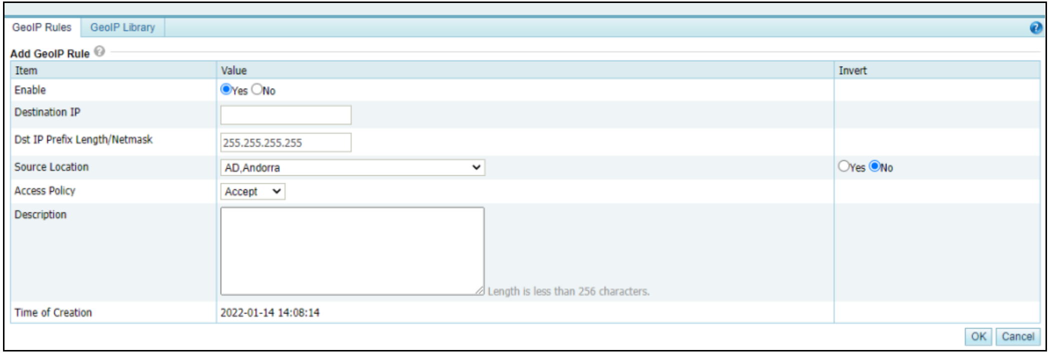
Figure 5-59 List of GeoIP rules



□	Destination IP	Dst IP Prefix Length/Netmask	Source Location	Access Control	Status	Description	Time of Creation	Operation
□	80.91.47.2	255.255.255.255	China Anhui	Drop	Disabled		2022-01-05 15:03:08	

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

Figure 5-60 Creating a GeoIP rule



Add GeoIP Rule

Item	Value	Invert
Enable	● Yes ○ No	
Destination IP		
Dst IP Prefix Length/Netmask	255.255.255.255	
Source Location	AD,Andorra	○ Yes ● No
Access Policy	Accept	
Description	Length is less than 256 characters.	
Time of Creation	2022-01-14 14:08:14	

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

Table 5-31 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

Parameter	Description
	address) of the destination IP address.
Source Location	Specifies the country or region to which source IP addresses belong. When **CN,China** is selected, the second drop-down box appears, providing **Mainland** and provincial-level regions for you to choose.
Access Policy	Specifies the action to be taken against packets that match this rule. It can be any of the following: • **Accept**: allows such packets to pass through ADS. • **Drop**: drops such packets. • **Filter**: does not take any action against such packets at this step, but will still check them against other protection rules. • **Limit rate**: specifies the maximum rate allowed for an IP address in the country/region specified with **Source Location** to transmit traffic to the destination IP address.
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 negate the setting of **Source Location**. For example, if **US,United States** is selected for **Source Location** and **Yes** is selected for **Invert**, all countries except the USA will be taken as source locations.

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

----End

5.2.3.2 Configuring a GeoIP Library

You can update the GeoIP library by importing a new one, or type an IP address and check the country to which it belongs.

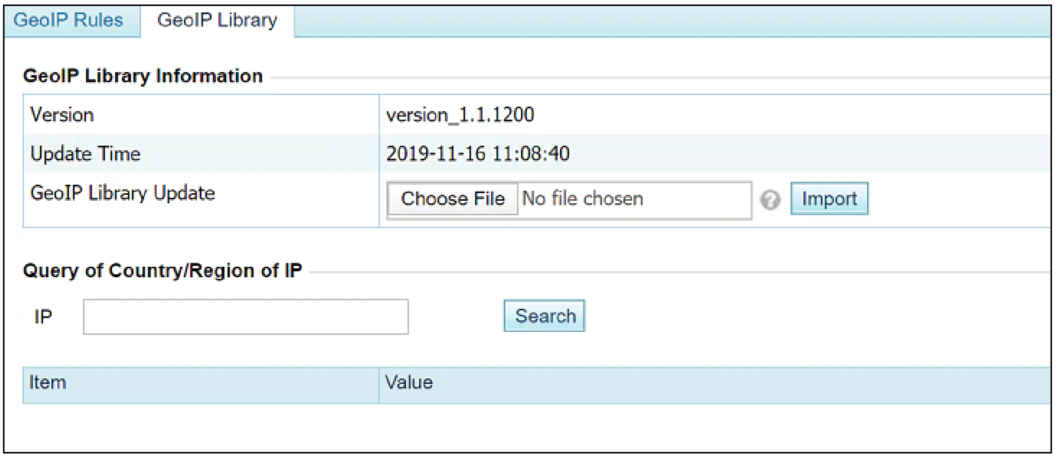
Importing a GeoIP Library

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

To import a GeoIP library, perform the following steps:

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

Figure 5-61 Viewing the GeoIP library



Version	version_1.1.1200
Update Time	2019-11-16 11:08:40
GeoIP Library Update	Choose File No file chosen

IP

Item	Value

Step 2 Import a GeoIP library.

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

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

After the successful import, the version and update information 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.

----End

Querying the GeoIP Library

From the GeoIP library, you can query the country to which an IP address belongs.

On the page shown in Figure 5-61, you can type an IP address (IPv4 or IPv6) in the **IP** text box and then click **Search** to query the country or region where it is located.

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 blocklist, 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 1024 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.

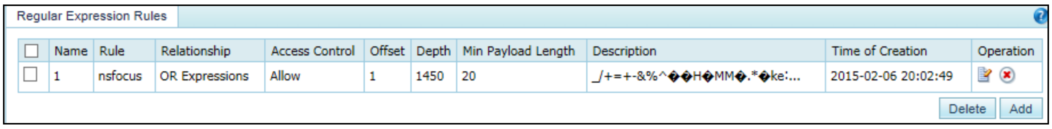
A regular expression rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting a regular expression rule are the same as those for access control rules.

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 5-62 List of regular expression rules

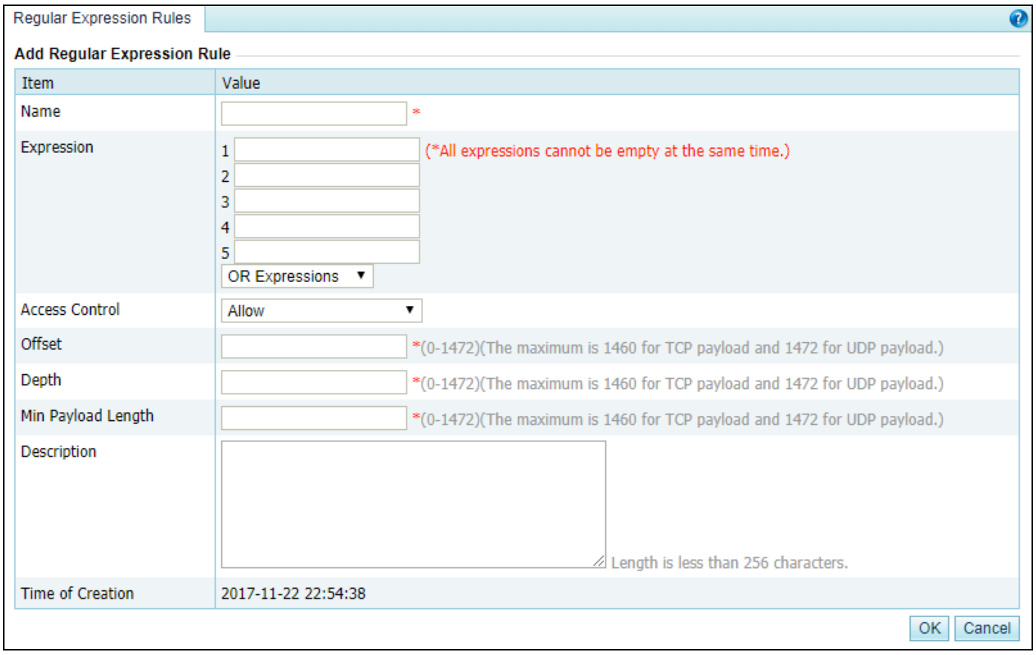


Regular Expression Rules

□	Name	Rule	Relationship	Access Control	Offset	Depth	Min Payload Length	Description	Time of Creation	Operation
□	1	nsfocus	OR Expressions	Allow	1	1450	20	_/+=+-&%^��H�MM�.*�ke:...	2015-02-06 20:02:49	

Step 2 Click **Add**.

Figure 5-63 Creating a regular expression rule



Regular Expression Rules

Add Regular Expression Rule

Item	Value
Name	*
Expression	1 (*All expressions cannot be empty at the same time.) 2 3 4 5 OR Expressions ▼
Access Control	Allow ▼
Offset	*(0-1472)(The maximum is 1460 for TCP payload and 1472 for UDP payload.)
Depth	*(0-1472)(The maximum is 1460 for TCP payload and 1472 for UDP payload.)
Min Payload Length	*(0-1472)(The maximum is 1460 for TCP payload and 1472 for UDP payload.)
Description	Length is less than 256 characters.
Time of Creation	2017-11-22 22:54:38

Table 5-32 describes parameters for creating a regular expression rule.

Table 5-32 Parameters for creating a regular expression rule

Parameter	Description
Name	Unique name of the regular expression rule.
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: • **Accept**: 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 blocklist. Before selecting this option, you must enable the blocklist. For details on the blocklist, see section 5.2.10 Blocklist. • **Drop and disconnect**: drops such packets and disconnects the connection to

Parameter	Description
	their destination IP addresses. • **Limit rate**: 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 blocklist, add to allowlist, 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 1024 DNS keyword checking rules, which can take effect only after being referenced in a group 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.

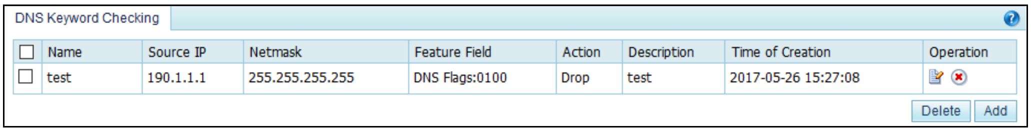
A DNS keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting DNS keyword checking rules are the same as those for access control rules.

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 5-64 List of DNS keyword checking rules

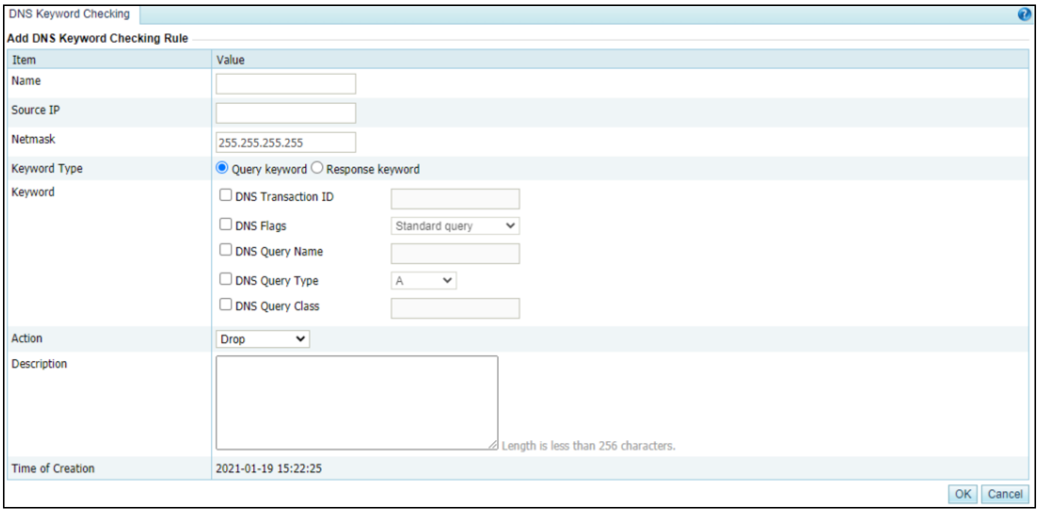


DNS Keyword Checking

□	Name	Source IP	Netmask	Feature Field	Action	Description	Time of Creation	Operation
□	test	190.1.1.1	255.255.255.255	DNS Flags:0100	Drop	test	2017-05-26 15:27:08	

Step 2 Click **Add**.

Figure 5-65 Creating a DNS keyword checking rule



DNS Keyword Checking

Add DNS Keyword Checking Rule

Item	Value
Name	
Source IP	
Netmask	255.255.255.255
Keyword Type	● Query keyword ○ Response keyword
Keyword	□ DNS Transaction ID □ DNS Flags: Standard query □ DNS Query Name □ DNS Query Type: A □ DNS Query Class
Action	Drop
Description	Length is less than 256 characters.
Time of Creation	2021-01-19 15:22:25

Table 5-33 describes parameters for creating a DNS keyword checking rule.

Table 5-33 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. Both IPv4 and IPv6 are supported. The value **0.0.0.0** or **::** 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.
Action	Specifies the action to be taken against a packet that matches a DNS keyword checking rule. It can be any of the following: • **Accept**: 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 blocklist. To select this option, you must enable the blocklist function in advance. For details about this function, see section 5.2.10 Blocklist. • **Accept+Whitelist**: indicates that ADS allows a packet with the specified signature to pass through and adds its IP address to the allowlist. To select this option, you must enable the allowlist function in advance. For details about this function, see section 5.2.11 Allowlist. • **Limit rate**: indicates that the maximum number of packets matching this rule

Parameter	Description
	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 blocklist, add to allowlist, 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 1024 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.

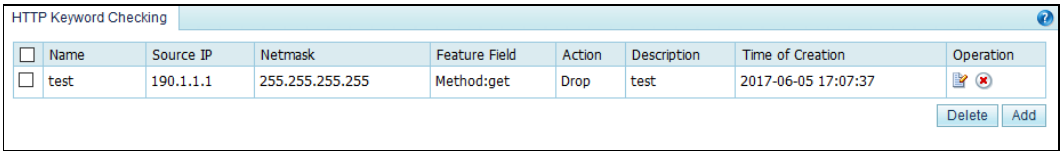
An HTTP keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting HTTP keyword checking rules are the same as those for access control rules.

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 5-66 List of HTTP keyword checking rules

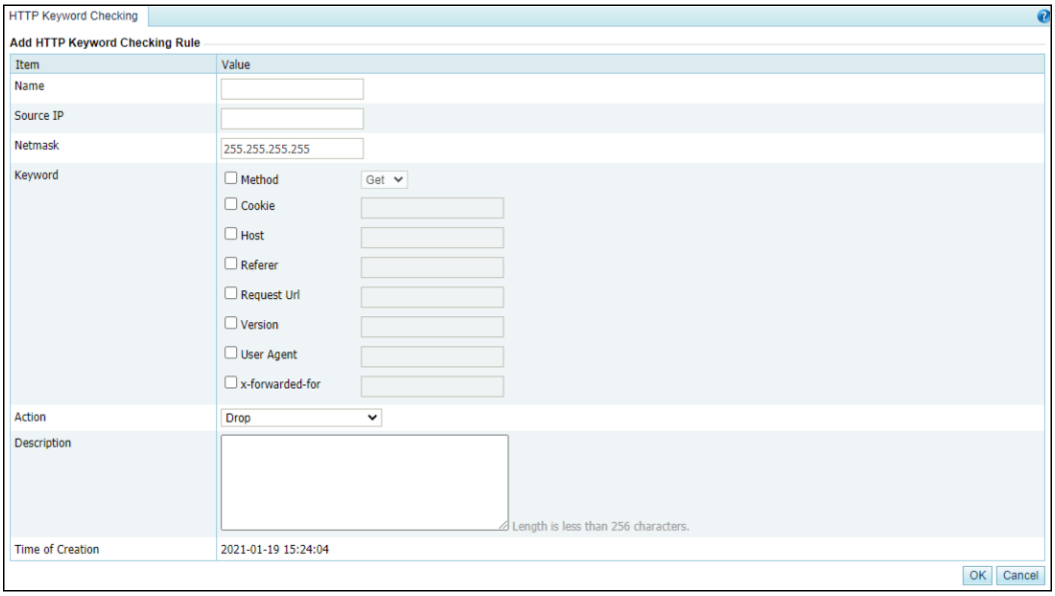


HTTP Keyword Checking

□	Name	Source IP	Netmask	Feature Field	Action	Description	Time of Creation	Operation
□	test	190.1.1.1	255.255.255.255	Method:get	Drop	test	2017-06-05 17:07:37	

Step 2 Click **Add**.

Figure 5-67 Creating an HTTP keyword checking rule



HTTP Keyword Checking

Add HTTP Keyword Checking Rule

Item	Value
Name	
Source IP	
Netmask	255.255.255.255
Keyword	□ Method Get □ Cookie □ Host □ Referer □ Request Url □ Version □ User Agent □ x-forwarded-for
Action	Drop
Description	Length is less than 256 characters.
Time of Creation	2021-01-19 15:24:04

Table 5-34 describes parameters for creating an HTTP keyword checking rule.

Table 5-34 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. Both IPv4 and IPv6 are supported. The value **0.0.0.0** or **::** 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: • **Accept**: 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 blocklist. To select this option, you must enable the blocklist function in advance. For details about this function, see section 5.2.10 Blocklist. • **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 blocklist. To select this option, you must enable the blocklist function in advance. • **Accept+Whitelist**: indicates that ADS allows a packet with the specified signature to pass through and adds its source IP address to the allowlist. To select this option, you must enable the allowlist function in advance. For details about this function, see section 5.2.11 Allowlist.

Parameter	Description
	- **Limit rate**: 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 Protection Rules

A connection exhaustion protection rule protects against connection exhaustion attacks by restricting the number of IP connections in a specified network segment. You can create a maximum of 128 connection exhaustion protection rules.

This section covers the following topics:

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

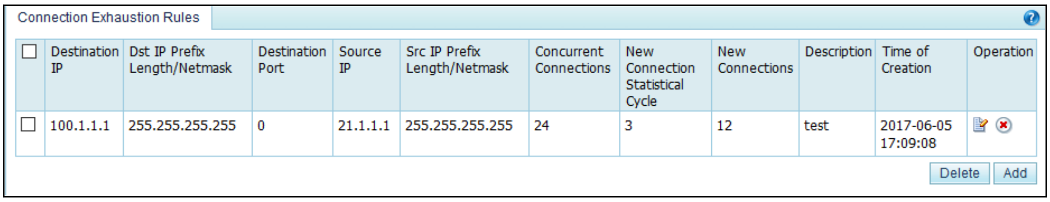
5.2.7.1 Creating a Connection Exhaustion Protection Rule

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

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

Initially, the rule list is empty.

Figure 5-68 List of connection exhaustion rules

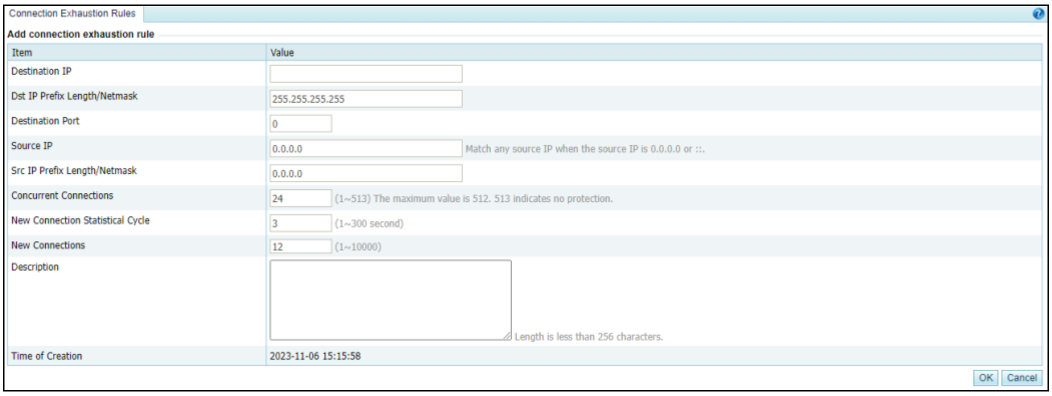


Connection Exhaustion Rules

□	Destination IP	Dst IP Prefix Length/Netmask	Destination Port	Source IP	Src IP Prefix Length/Netmask	Concurrent Connections	New Connection Statistical Cycle	New Connections	Description	Time of Creation	Operation
□	100.1.1.1	255.255.255.255	0	21.1.1.1	255.255.255.255	24	3	12	test	2017-06-05 17:09:08	

Step 2 Click **Add**.

Figure 5-69 Creating a connection exhaustion rule



Connection Exhaustion Rules

Add connection exhaustion rule

Item	Value
Destination IP	
Dst IP Prefix Length/Netmask	255.255.255.255
Destination Port	0
Source IP	0.0.0.0 Match any source IP when the source IP is 0.0.0.0 or ::.
Src IP Prefix Length/Netmask	0.0.0.0
Concurrent Connections	24 (1~513) The maximum value is 512. 513 indicates no protection.
New Connection Statistical Cycle	3 (1~300 second)
New Connections	12 (1~10000)
Description	Length is less than 256 characters.
Time of Creation	2023-11-06 15:15:58

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 blocklist function must be enabled for the use of connection exhaustion rules.

Table 5-35 describes parameters for creating a connection exhaustion rule.

Table 5-35 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 the actual network deployment. The value **0.0.0.0** or **::** indicates that this rule matches packets with any source IP addresses.
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 blocklist. The value ranges from 1 to 513. The value **513** 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 blocklist. 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.

Parameter	Description
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

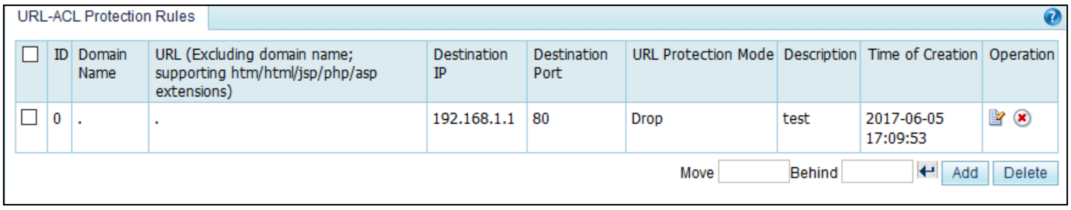
5.2.8.1 Creating a URL-ACL Protection Rule

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 5-70 List of URL-ACL rules

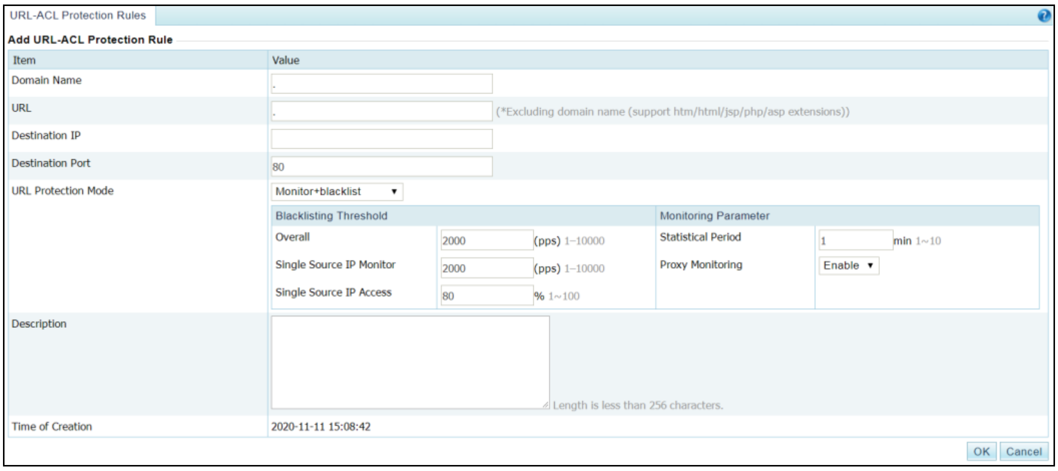


URL-ACL Protection Rules

□	ID	Domain Name	URL (Excluding domain name; supporting htm/html/jsp/php/asp extensions)	Destination IP	Destination Port	URL Protection Mode	Description	Time of Creation	Operation
□	0	.	.	192.168.1.1	80	Drop	test	2017-06-05 17:09:53	

Step 2 Click **Add**.

Figure 5-71 Creating a URL-ACL rule



URL-ACL Protection Rules

Add URL-ACL Protection Rule

Item	Value
Domain Name	.
URL	. (*Excluding domain name (support htm/html/jsp/php/asp extensions))
Destination IP	
Destination Port	80
URL Protection Mode	Monitor+blacklist
Description	Length is less than 256 characters.
Time of Creation	2020-11-11 15:08:42

Blacklisting Threshold		Monitoring Parameter	
Overall	2000 (pps) 1~10000	Statistical Period	1 min 1~10
Single Source IP Monitor	2000 (pps) 1~10000	Proxy Monitoring	Enable
Single Source IP Access	80 % 1~100		

Table 5-36 describes parameters for creating a URL-ACL rule.

Table 5-36 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. • **Monitor+blacklist**: counts the total number of HTTP requests of the

Parameter	Description
	source IP address matching this rule and adds this address to the blocklist if the value specified with **Single Source IP Access** is exceeded.
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**.
Overall	Specifies the threshold for the number of packets that hit this rule. If the specified value is exceeded, ADS checks whether traffic of each source IP address exceeds the value specified with **Single Source IP Monitor**. The value ranges from 1 to 10000.
Single Source IP Monitor	Specifies the threshold for the number of packets from a source IP address that match this rule. If the specified value is exceeded during a statistical period, the percentage of packets matching the rule is calculated. The value ranges from 1 to 10000.
Single Source IP Access	Specifies the threshold for the percentage of packets from a source IP address that match the rule during a statistical period. If the specified value is exceeded, the source IP address will be added to the blocklist.
Statistical Period	Specifies the statistical period for calculating the percentage of packets that match the rule. The value ranges from 1 to 10 minutes.
Proxy Monitoring	If proxy monitoring is enabled, for packets that are sent via a proxy, their real source IP addresses will be parsed for calculations.
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 Programmable Rules

A programmable rule is a user-defined protection rule that provides flexible protection performance. By matching packets at the binary or bit level for any byte content, programmable rules can meet the changing requirements in the attack and defense scenarios and defend against complex attacks.

Choose **Policy > Access Control > Programmable Rules**. Click **Add** and configure parameters. Table 5-37 describes parameters for creating a programmable rule.

- A programmable rule, after being added, can be edited and deleted. However, the programmable rule referenced by a protection group cannot be deleted.
- You can configure up to 64 programable rules, which can take effect only after being referenced in a group protection policy. For details about how to refence a programmable rule in a group protection policy, see section 5.1.2.20 Programmable Rule.Programmable Rule

Table 5-37 Parameters of a programmable rule

Parameter	Description
Name	Name of the rule, which can contain 20 characters at most.
Programming Expression	Expression of the rule, which can contain 200 characters at most. You can type the following character types: • Keywords, such as tcp, ip, udp. • Operational rules, including relational operators (==, !=, >, <, >=), logical operators (and, or, not), arithmetic operators (+, -, *, /), and bitwise operators (&, |) • Actions, including **drop**, **accept**, **drop_black**, **accept_white**, **accept_trust_low**, and **accept_trust_high** After you type a text, the system automatically displays associated characters for you to select. For example, the expression **action.drop tcp.port==137** means that the packets to TCP port 137 will be dropped. • Click **Verify** to check whether the expressions typed are correct. The verification result is shown below. • Click **Help** to view the supported character types and detailed filed description.
Description	Descriptive information about the rule, which can contain 256 characters at

Parameter	Description
	most.
Time of Creation	Time when the rule was created. It is automatically generated by the system.

5.2.10 Blocklist

The blocklist policy is used to filter source IP addresses of packets. Once a source IP address matches an address on the blocklist, 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 blocklist using either of the following methods:

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

IP addresses can be automatically added to the blocklist in several ways, as listed in Table 5-38.

Table 5-38 Reason for adding a source IP address to the blocklist

Policy	Reason for Adding a Source IP Address to the Blocklist
Pattern matching rule	Once attack packets are filtered out through pattern matching, the source IP address of such packets is automatically added to the blocklist. For description of pattern matching, see section 8.2 Pattern Matching Rules.
URL-ACL protection rule	When **URL Protection Mode** is set to **Drop** for URL-ACL rules, ADS adds the source IP address to the global blocklist once detecting that an HTTP request amid IP packets matches such a URL-ACL rule. When **URL Protection Mode** is set to **Block proxy** for URL-ACL rules, ADS adds the IP address of a proxy server to the global blocklist once detecting that an HTTP request from the proxy server amid packets matches such a URL-ACL rule. When **URL Protection Mode** is set to **Monitor+blacklist** for URL-ACL rules, ADS adds source IP addresses to the global blocklist once detecting that the proportion of matching packets from those IP addresses exceeds the value specified with **Single Source IP Access**.
Low-and-slow attack protection	Once low-and-slow attack protection is triggered, if the blocklist is enabled for the protection group involving the destination IP address, the system adds source IP addresses of matching packets to the blocklist.
Reflection protection policy	Once the reflection protection policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address and the rule's action is set to **Drop and add to blacklist**, the system will add source IP addresses of matching packets to the blocklist.
Port check policy	Once the port check policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address and **Access Control** is set to **Drop and add to blacklist**, the system will add source IP addresses of matching packets to the blocklist.
UDP regular expression protection policy	Once the UDP regular expression protection policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address, the system will add source IP addresses of matching packets to the blocklist.

Policy	Reason for Adding a Source IP Address to the Blocklist
Protocol ID check policy	Once the protocol ID check policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address and **Access Control** is set to **Drop and add to blacklist**, the system will add source IP addresses of matching packets to the blocklist.
TCP control parameters protection policy	Once the TCP control parameters protection policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address and **SYN Source Bandwidth Limit** is set to **Drop and add to blacklist**, the system adds the source IP address of matching packets to the blocklist.
IP behavior control policy	Once the IP behavior control policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address and **Access Control** or **Empty Connection Check** is set to **Drop and add to blacklist**, the system adds the source IP address of matching packets to the blocklist.
HTTPS protection policy	Once an HTTPS protection policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address and **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 blocklist.
TCP regular expression protection policy	Once the TCP regular expression policy is triggered, if the blocklist is enabled for the protection group involving the destination IP address, the system adds the source IP address that matches such a rule to the blocklist.
HTTP keyword checking rule	Once an HTTP keyword check rule with **Action** set to **Drop+Blacklist** is triggered, the system adds source IP addresses that fail the HTTP keyword check to the blocklist.
DNS keyword checking rule	Once a DNS keyword checking rule with **Action** set to **Drop+Blacklist** is triggered, the system adds source IP addresses that fail the DNS keyword check to the blocklist.
Connection exhaustion rule	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 blocklist.
Programmable rule	When the action of a programmable rule is set to **drop_black**, the system adds source or destination IP addresses that match the programmable rule to the blocklist.
Carpet bombing protection	When the carpet bombing protection is configured to be globally effective and its action includes blacklist, the system adds source IP address that triggers the carpet bombing protection rule to the blocklist.

This section describes how to enable or disable a blocklist, add a blocked item manually, delete a blocked item, and clear a blocklist.

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

You can perform the following operations regarding the blocklist:

- Enabling and Disabling the Blocklist Function

- Adding a Blocklist Entry
- Viewing Blocklist Entries
- Deleting Blocklist Entries
- Clearing Blocklist Entries
- Searching the Blocklist
- Importing a Blocklist File
- Viewing the Import Result
- Exporting a Blocklist File

5.2.10.1 Enabling and Disabling the Blocklist Function

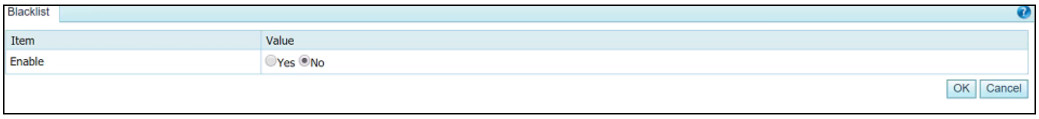
Enabling the Blocklist Function

To enable the blocklist function, perform the following steps:

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

Initially, the blocklist function is disabled.

Figure 5-72 Blocklist status

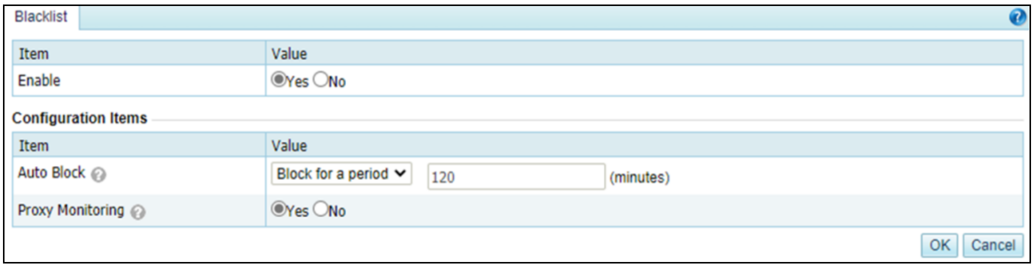


Blacklist

Item	Value
Enable	○Yes ●No

Step 2 Click **Edit** and then select **Yes** to enable the blocklist function. See Figure 5-73.

Figure 5-73 Enabling the blocklist policy



Blacklist

Item	Value
Enable	●Yes ○No

Configuration Items

Item	Value
Auto Block	Block for a period 120 (minutes)
Proxy Monitoring	●Yes ○No

Table 5-39 Blocklist parameters

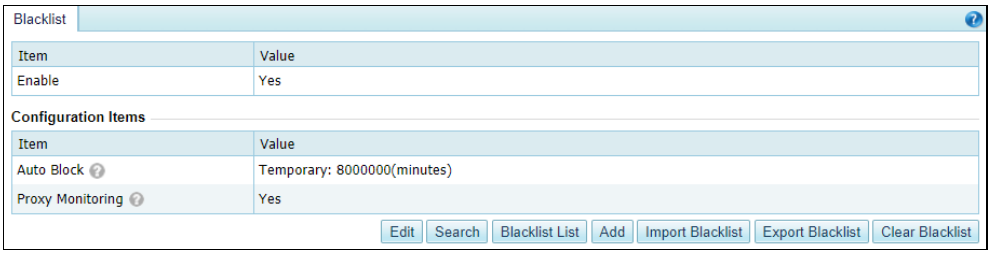
Parameter	Description
Auto Block	Specifies the duration when an IP address is blocked. This parameter has two options: • **Temporary**: The IP address is blocked and packets from this address are dropped in the specified period. • **Permanent**: The IP address is permanently blocked and packets from this address are always dropped.

Parameter	Description
Proxy Monitoring	Controls whether to enable or disable the proxy monitoring function. By default, this function is disabled. • **No**: disables proxy monitoring. In this case, ADS filters source IP addresses of HTTP packets by matching blocklist entries, without checking the real source IP addresses of those packets. • **Yes**: enables proxy monitoring. In this case, ADS first matches source IP addresses of HTTP packets against blocklist entries. If no match is found, ADS will continue to use this blocklist to filter the real source IP addresses extracted from the payloads of those packets. In attack logs generated in this situation, the **Source IP** field indicates the real source IP address.

Step 3 Set parameters and click **OK** to return to the previous page.

As shown in Figure 5-74, the blocklist function is enabled and blocklist configuration items are available.

Figure 5-74 Blocklist function enabled



Blacklist

Item	Value
Enable	Yes

Configuration Items

Item	Value
Auto Block	Temporary: 8000000(minutes)
Proxy Monitoring	Yes

----End

Disabling the Blocklist Function

To disable the blocklist function, perform the following steps:

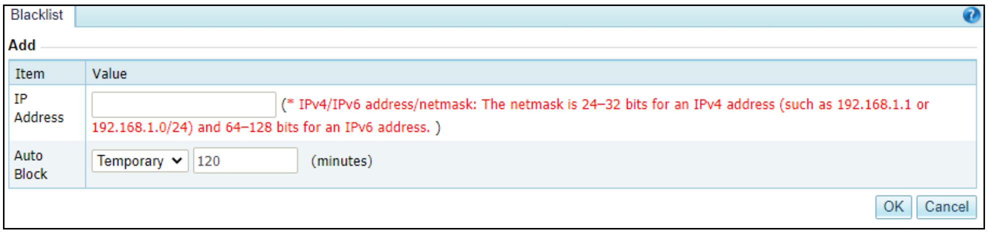
On the page shown in Figure 5-73, select **No**. Then the value of **Enable** turns to **No**, as shown in Figure 5-72.

5.2.10.2 Adding a Blocklist Entry

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

Step 1 On the page shown in Figure 5-74, click **Add** to add a blocklist entry.

Figure 5-75 Adding a blocklist entry



Item	Value
IP Address	(* IPv4/IPv6 address/netmask: The netmask is 24–32 bits for an IPv4 address (such as 192.168.1.1 or 192.168.1.0/24) and 64–128 bits for an IPv6 address.)
Auto Block	Temporary 120 (minutes)

Step 2 Set parameters.

Table 5-40 Blocklist parameters

Parameter	Description
IP Address	Specifies the source IP address to be blocked. Either an IPv4 or IPv6 address is allowed. Formats are as follows: • IPv4 address/netmask of 24 to 32 bits, such as 192.168.1.0/24. • IPv6 address/prefix length of 64 to 128 bits.
Auto Block	Specifies the duration when an IP address is blocked. Two options are available: • Regular: The IP address is blocked and packets from this address are dropped in the specified period. • Permanent: The IP address is permanently blocked and packets from this address are always dropped.

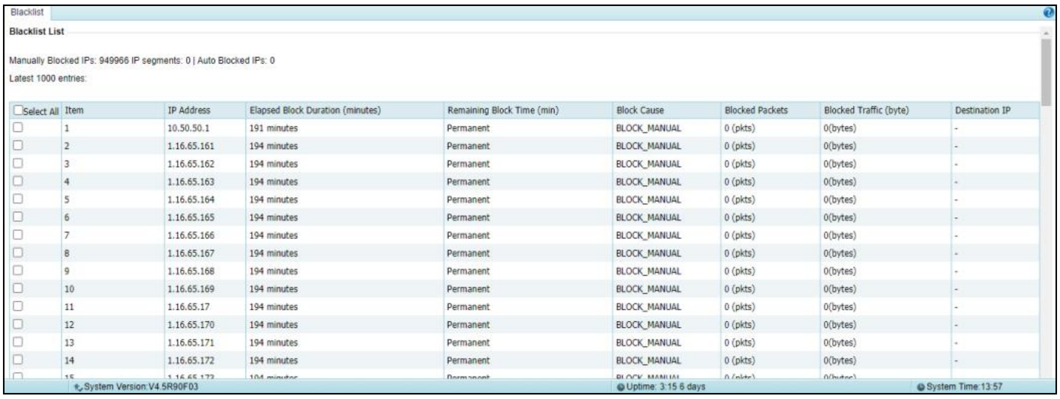
Step 3 Click **OK** to complete the configuration.

----End

5.2.10.3 Viewing Blocklist Entries

On the page shown in Figure 5-74, click **Blacklist List**. The system displays a maximum of 1000 IP addresses blocked recently, as shown in Figure 5-76. You can cick **Refresh** to obtain IP addresses blocked most recently.

Figure 5-76 Viewing blocklist entries



Blacklist

Blacklist List

Manually Blocked IPs: 949966 IP segments: 0 | Auto Blocked IPs: 0

Latest 1000 entries:

□Select All	Item	IP Address	Elapsed Block Duration (minutes)	Remaining Block Time (min)	Block Cause	Blocked Packets	Blocked Traffic (byte)	Destination IP
□	1	10.50.50.1	191 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	2	1.16.65.161	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	3	1.16.65.162	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	4	1.16.65.163	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	5	1.16.65.164	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	6	1.16.65.165	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	7	1.16.65.166	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	8	1.16.65.167	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	9	1.16.65.168	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	10	1.16.65.169	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	11	1.16.65.17	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	12	1.16.65.170	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	13	1.16.65.171	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	14	1.16.65.172	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	15	1.16.65.173	194 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	

System Version:V4.5R90F03

Uptime: 3:15 6 days

System Time:13:57

For the **Destination IP** column:

- If the source IP address is added to the blocklist automatically, the destination IP address is displayed.
- If the source IP address is added to the blocklist manually, the destination IP address is not displayed. Instead, a hyphen (-) is displayed in this column.

5.2.10.4 Deleting Blocklist Entries

To delete a blocklist entry, perform the following steps:

Step 1 On the page shown in Figure 5-76, select one or more blocklist entries and then click **Delete**.

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

----End

5.2.10.5 Clearing Blocklist Entries

To clear blocklist entries, perform the following steps:

Step 1 On the page shown in Figure 5-74 or Figure 5-76, click **Clear Blacklist**.

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

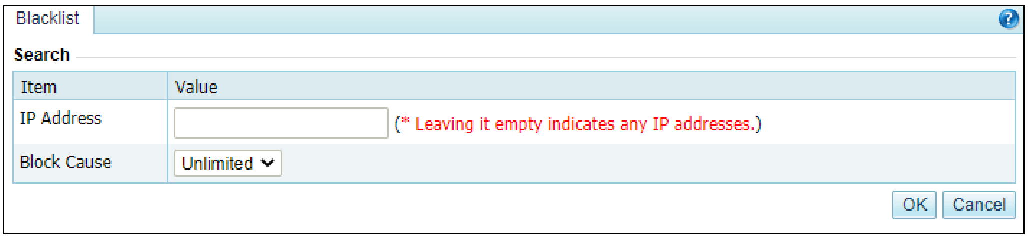
----End

5.2.10.6 Searching the Blocklist

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

Step 1 On the page shown in Figure 5-77, click **Search**.

Figure 5-77 Searching for an IP address



Blacklist

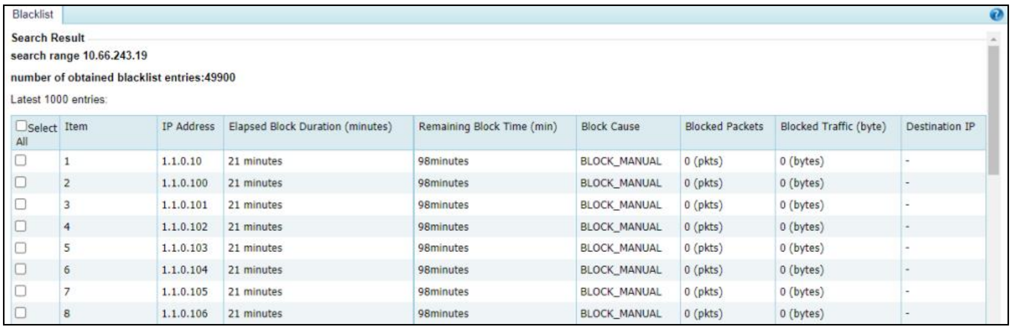
Search

Item	Value
IP Address	(* Leaving it empty indicates any IP addresses.)
Block Cause	Unlimited

Step 2 On the **Search** page shown in Figure 5-77, type an IP address, and click **OK**.

The blocklist search result is displayed, as shown in Figure 5-78.

Figure 5-78 Blocklist search result



Blacklist

Search Result

search range 10.66.243.19

number of obtained blacklist entries:49900

Latest 1000 entries:

□Select All	Item	IP Address	Elapsed Block Duration (minutes)	Remaining Block Time (min)	Block Cause	Blocked Packets	Blocked Traffic (byte)	Destination IP
□	1	1.1.0.10	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
□	2	1.1.0.100	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
□	3	1.1.0.101	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
□	4	1.1.0.102	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
□	5	1.1.0.103	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
□	6	1.1.0.104	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
□	7	1.1.0.105	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
□	8	1.1.0.106	21 minutes	98minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-

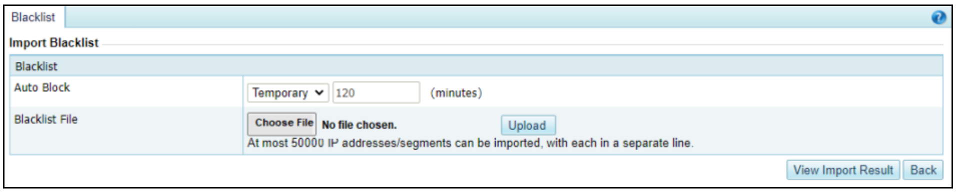
----End

5.2.10.7 Importing a Blocklist File

To import a blocklist file, perform the following steps:

Step 1 On the page shown in Figure 5-74, click **Import Blacklist**.

Figure 5-79 Importing a blocklist file



Blacklist

Import Blacklist

Blacklist	
Auto Block	Temporary 120 (minutes)
Blacklist File	Choose File No file chosen. Upload At most 50000 IP addresses/segments can be imported, with each in a separate line.

Note

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

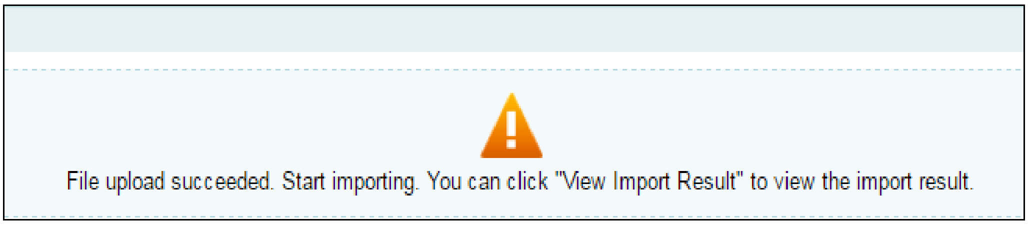
Step 2 On the page shown in Figure 5-79, click **Choose File**.

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

Step 4 Click **Upload**.

After the upload is complete, the system prompts that the file is successfully imported, as shown in Figure 5-80.

Figure 5-80 Import success prompt



File upload succeeded. Start importing. You can click "View Import Result" to view the import result.

After the blocklist file is imported, the system automatically switches to the page shown in Figure 5-79.

----End

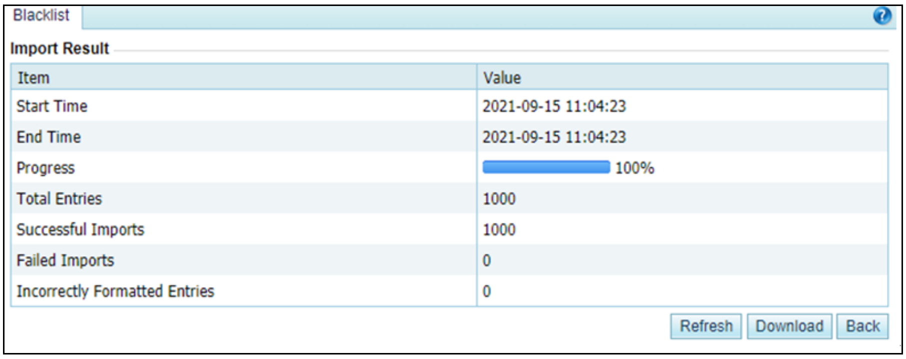
5.2.10.8 Viewing the Import Result

To view the import result, perform the following steps:

Step 1 On the page shown in Figure 5-79, 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 5-81.

Figure 5-81 Viewing import results



Item	Value
Start Time	2021-09-15 11:04:23
End Time	2021-09-15 11:04:23
Progress	100%
Total Entries	1000
Successful Imports	1000
Failed Imports	0
Incorrectly Formatted Entries	0

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

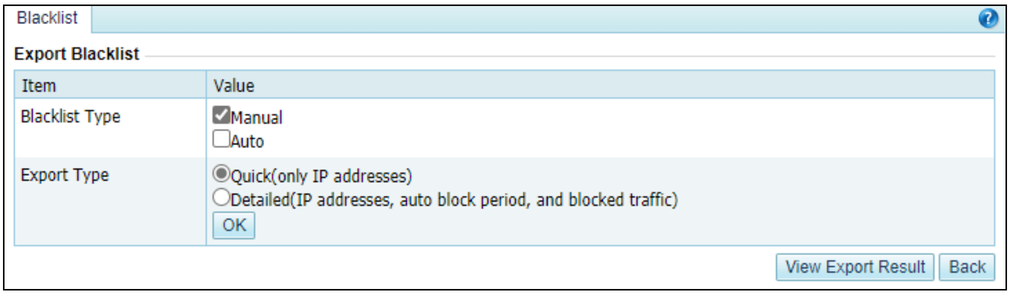
----End

5.2.10.9 Exporting a Blocklist File

To export a blocklist file, perform the following steps:

Step 1 On the page shown in Figure 5-74, click **Export Blacklist**.

Figure 5-82 Exporting a blocklist file



Blacklist

Export Blacklist

Item	Value
Blacklist Type	☑Manual □Auto
Export Type	●Quick(only IP addresses) ○Detailed(IP addresses, auto block period, and blocked traffic) OK

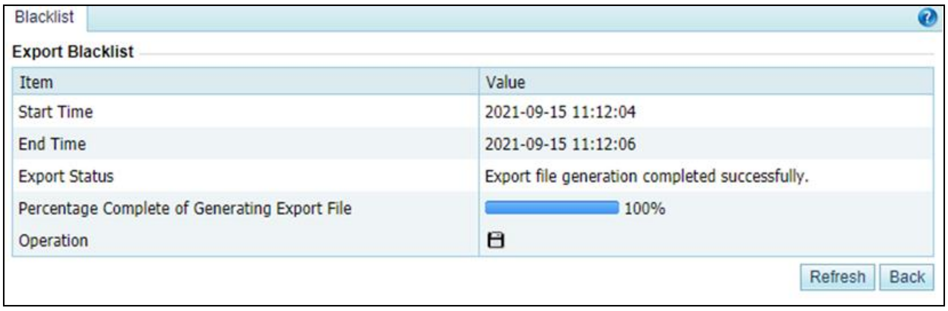
Step 2 Set blocklist export parameters.

Table 5-41 Parameters for blocklist export

Parameter	Description
Blacklist Type	Specifies the type of the blocklist for export, which can be Manual or Automatic.
Export Type	Specifies the export type, which can be either of the following: • **Quick export**: Only blocked IP addresses are included in the exported file. • **Detailed export**: Blocklist entry details, like the blocked IP addresses, auto block period, and blocked traffic are in the exported file.

Step 3 Click **OK** to return to the blocklist export result page.

Figure 5-83 Viewing blocklist export results



Blacklist

Export Blacklist

Item	Value
Start Time	2021-09-15 11:12:04
End Time	2021-09-15 11:12:06
Export Status	Export file generation completed successfully.
Percentage Complete of Generating Export File	100%
Operation	💾

Step 4 Click 💾 in the **Operation** row to save to exported blocklist file to a local disk drive.

Step 5 Click **Back** to return to the blocklist configuration page.

----End

5.2.11 Allowlist

After the allowlist function is enabled, ADS checks whether the source IP address of packets matches any address (an IPv4 address or IPv6 address) in the allowlist. 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 allowlist has a higher priority than the blocklist. Therefore, if the source IP address of packets is included in both the blocklist and allowlist, the ADS device allows such packets to pass through.

You can perform the following operations regarding the allowlist:

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

5.2.11.1 Enabling and Disabling the Allowlist Function

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

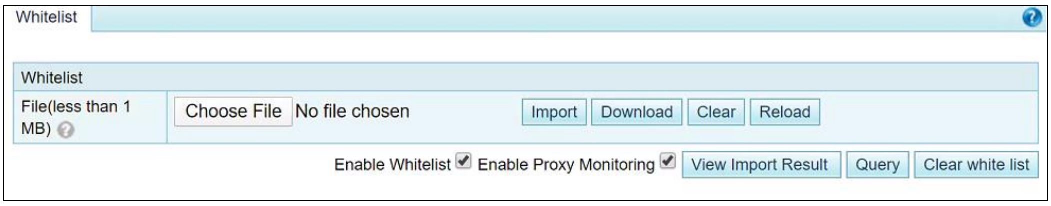
Enabling the Allowlist Function

To enable the allowlist function, perform the following steps:

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

By default, the allowlist function is disabled.

Figure 5-84 Allowlist configuration page



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

----End

Disabling the Allowlist Function

If the allowlist function is enabled, deselect **Enable Whitelist** to disable the allowlist, as shown in Figure 5-84.

5.2.11.2 Enabling Proxy Monitoring

On the page shown in Figure 5-84, you can enable or disable the proxy monitoring function of the allowlist. By default, this function is disabled.

- Deselecting the **Enable Proxy Monitoring** check box disables proxy monitoring. After this function is disabled, ADS filters source IP addresses of HTTP packets by matching the allowlist entries, without checking real source IP addresses of those packets.
- Selecting the **Enable Proxy Monitoring** check box enables proxy monitoring. After this function is enabled, ADS first matches source IP addresses of HTTP packets against allowlist entries. If no match is found, ADS will continue to use this allowlist to filter the real source IP addresses extracted from the payloads of those packets.

5.2.11.3 Importing a Allowlist File

You can add trusted IPv4 or IPv6 addresses by importing a allowlist file on the ADS device. After the allowlist 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 allowlist file will overwrite the existing file saved on the device.

The allowlist 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

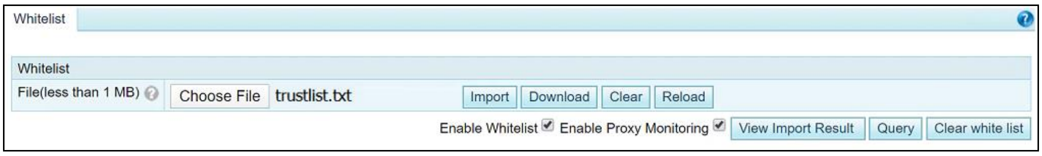
- Since the ADS device supports the IPv4/IPv6 dual-stack, you can configure IPv4 or IPv6 addresses in the allowlist file according to the actual network deployment.
- The allowlist file name supports English letters and digits. The file must be within 1 MB. It is recommended that the file contain a maximum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

To import a allowlist file, perform the following steps:

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

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

Figure 5-85 Importing the allowlist file



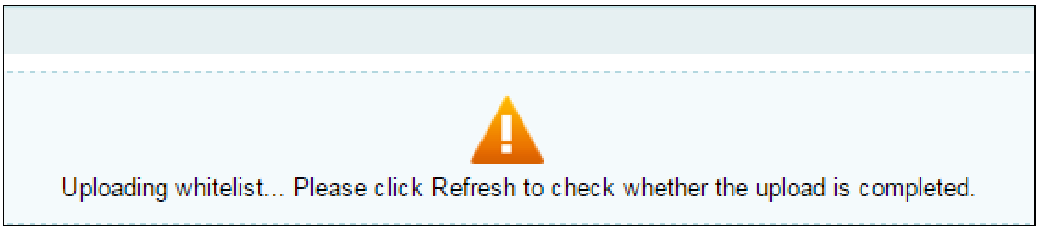
File(less than 1 MB) trustlist.txt

Enable Whitelist ☑ Enable Proxy Monitoring ☑

Step 3 Click **Import**.

A message is displayed, prompting that the import is in progress, as shown in Figure 5-86.

Figure 5-86 Import progress message



Uploading whitelist... Please click Refresh to check whether the upload is completed.

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

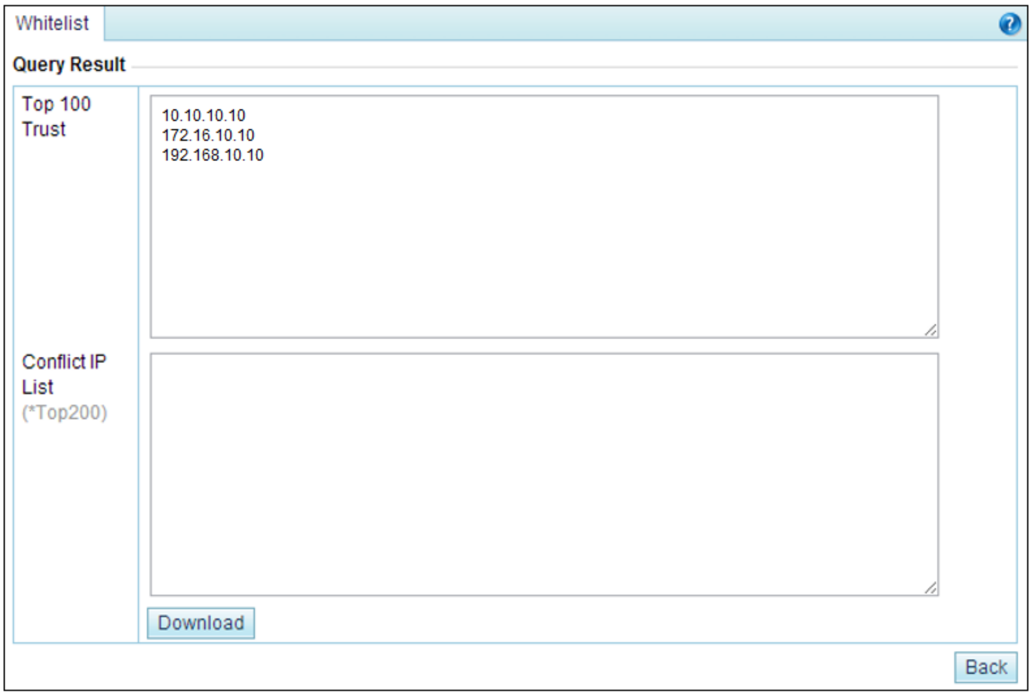
----End

5.2.11.4 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 allowlist configuration page shown in Figure 5-84 to view information that is successfully imported to the allowlist. See Figure 5-87.

Figure 5-87 Viewing the import result



Whitelist

Query Result

Top 100 Trust

```
10.10.10.10
172.16.10.10
192.168.10.10
```

Conflict IP List (*Top200)

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 allowlist configuration page.

----End

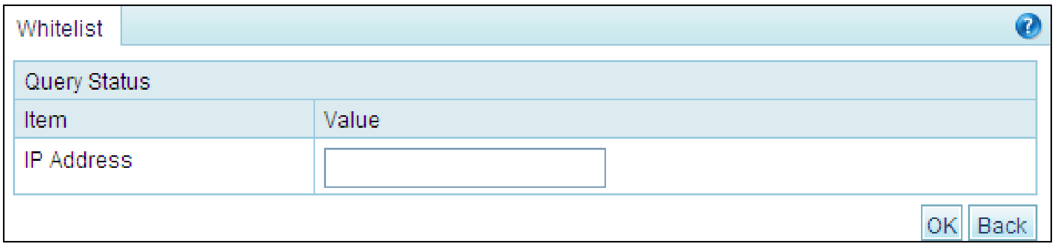
5.2.11.5 Querying the Allowlist

Querying the allowlist, 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 allowlist, perform the following steps:

Step 1 On the allowlist configuration page shown in Figure 5-84, click **Query** to open the **Query Status** page.

Figure 5-88 Querying the allowlist

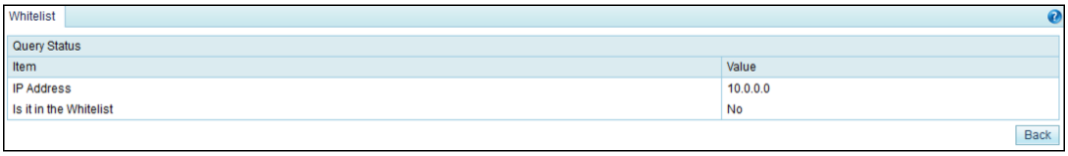


Query Status

Item	Value
IP Address	

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

Figure 5-89 Allowlist query result



Query Status

Item	Value
IP Address	10.0.0.0
Is it in the Whitelist	No

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

----End

5.2.11.6 Clearing the Allowlist

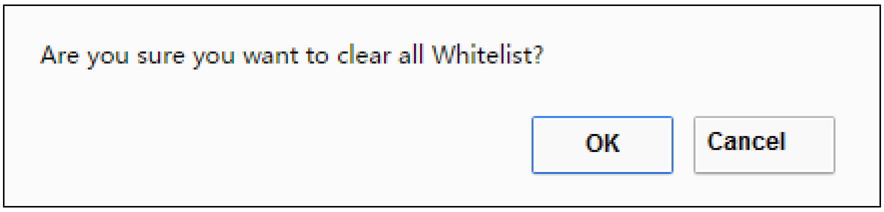
By clearing the allowlist, you can only delete the trust status of all IP addresses listed in the allowlist on the engine, but cannot delete the allowlist file. If IP addresses in this allowlist need to be re-trusted after the allowlist is cleared, you need to reload the allowlist file. For details,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

To clear the allowlist, perform the following steps:

Step 1 Click **Clear white list** on the allowlist configuration page shown in Figure 5-84.

Then, a dialog box appears, asking you whether to clear the allowlist, as shown in Figure 5-90.

Figure 5-90 Clearing trust relationships



Are you sure you want to clear all Whitelist?

Step 2 Click **OK** to save the settings.

----End

5.2.11.7 Clearing the Configuration

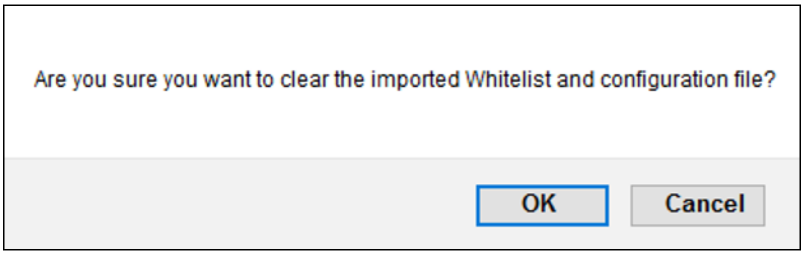
By clearing the configuration, you can delete the allowlist file and trust relationships of IP addresses on the engine. You are advised to back up the allowlist file before clearing the configuration. For details, see Downloading the Configuration.

To clear the configuration, perform the following steps:

Step 1 Click **Clear** on the allowlist configuration page shown in Figure 5-84.

Then, a dialog box appears, asking you whether to delete the allowlist file and all trusted entries, as shown in Figure 5-91.

Figure 5-91 Clearing the configuration



Are you sure you want to clear the imported Whitelist and configuration file?

Step 2 Click **OK** to save the settings.

----End

5.2.11.8 Downloading the Configuration

You can download the allowlist file to a local disk drive for backup.

To download the configuration, perform the following steps:

Step 1 Click **Download** on the allowlist configuration page shown in Figure 5-84.

Step 2 Click **Save** and select a file path to save the allowlist file in the related directory.

----End

5.2.11.9 Reloading the Allowlist 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 allowlist, click **Reload** on the allowlist configuration page shown in Figure 5-84.

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 ADS in out-of-path mode. These rules can be configured only when the current running mode is **Diversion**.

Note

When ADS is 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:

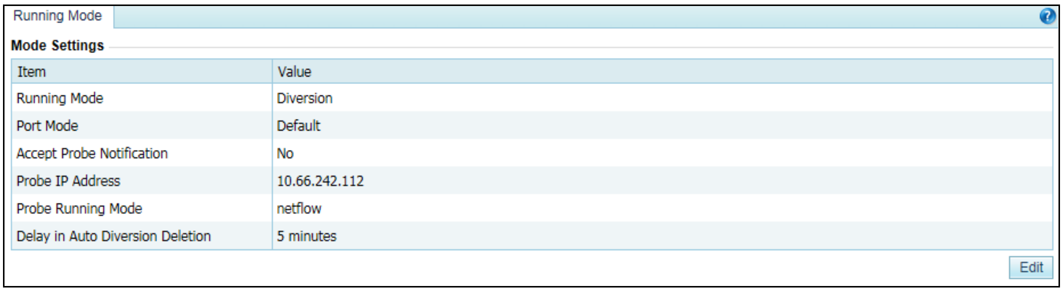
- Running Mode
- Port Channel Configuration
- GRE Tunnel Configuration
- IP Address Configuration

6.1.1 Running Mode

To configure the running mode on ADS, perform the following steps:

Step 1 Choose **Diversion & Injection** > **General Settings** > **Running Mode**.

Figure 6-1 Running mode of the ADS device (diversion mode)



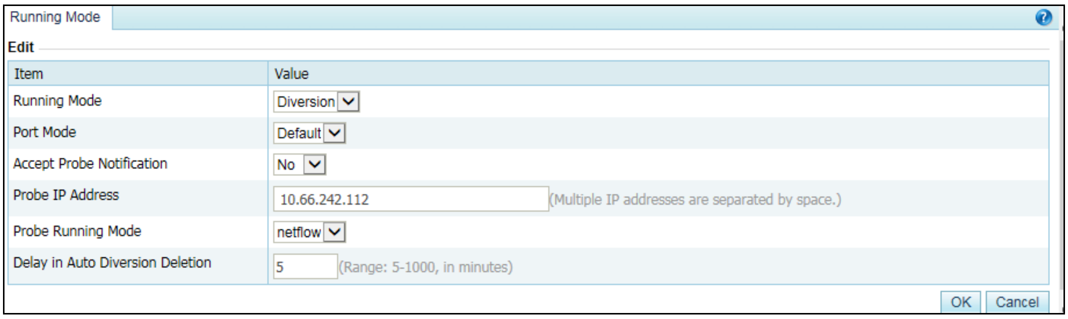
Running Mode

Mode Settings

Item	Value
Running Mode	Diversion
Port Mode	Default
Accept Probe Notification	No
Probe IP Address	10.66.242.112
Probe Running Mode	netflow
Delay in Auto Diversion Deletion	5 minutes

Step 2 Click **Edit**.

Figure 6-2 Editing the running mode (diversion mode)



Running Mode

Edit

Item	Value
Running Mode	Diversion
Port Mode	Default
Accept Probe Notification	No
Probe IP Address	10.66.242.112 (Multiple IP addresses are separated by space.)
Probe Running Mode	netflow
Delay in Auto Diversion Deletion	5 (Range: 5-1000, in minutes)

Table 6-1 describes parameters on this page.

Table 6-1 Parameters for setting the running 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. Note - ADS NX5-10000 does 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.

Parameter	Description
	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**.
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 module allows you to manually or dynamically aggregate several interfaces into a port channel and view the port channel status.

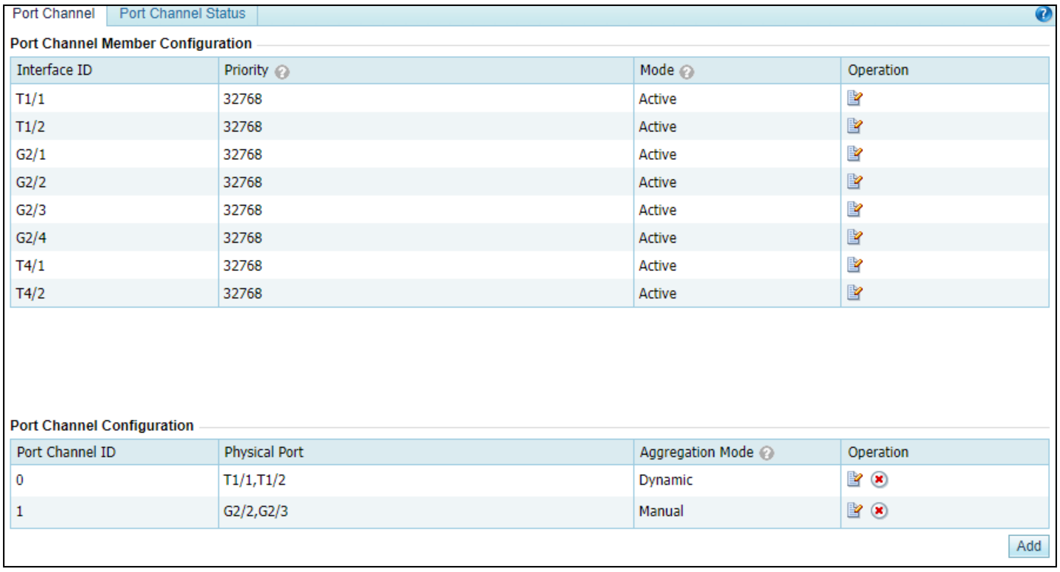
6.1.2.1 Configuring a Port Channel

Port channel configuration allows you to configure ports for data exchange between ADS and other products. You can use any combinations of available ports on the current 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 NX5-4020E 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 NX5-4020E as an example to describe how to configure the port channel.

Choose **Diversion & Injection** > **General Settings** > **Port Channel** > **Port Channel** to open the port channel configuration page. See Figure 6-3.

Figure 6-3 Port Channel page



Port Channel | Port Channel Status

Port Channel Member Configuration

Interface ID	Priority	Mode	Operation
T1/1	32768	Active	✎
T1/2	32768	Active	✎
G2/1	32768	Active	✎
G2/2	32768	Active	✎
G2/3	32768	Active	✎
G2/4	32768	Active	✎
T4/1	32768	Active	✎
T4/2	32768	Active	✎

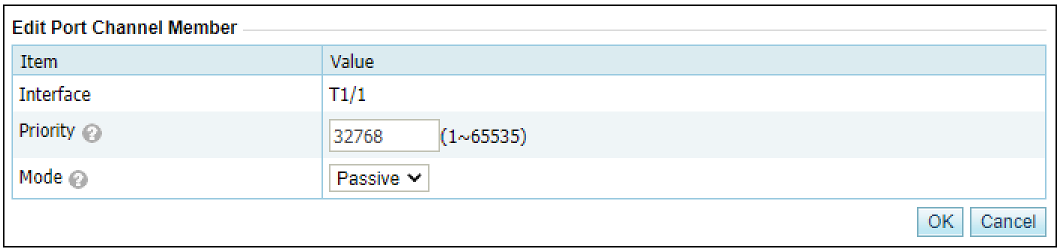
Port Channel Configuration

Port Channel ID	Physical Port	Aggregation Mode	Operation
0	T1/1,T1/2	Dynamic	✎ ⊗
1	G2/2,G2/3	Manual	✎ ⊗

Editing a Port Channel Member

In the **Port Channel Member Configuration** area shown in Figure 6-3, click ✎. The **Edit Port Channel Member** page appears, as shown in Figure 6-4.

Figure 6-4 Edit Port Channel Member page



Edit Port Channel Member

Item	Value
Interface	T1/1
Priority	32768 (1~65535)
Mode	Passive

Table 6-2 describes parameters for editing a port channel member.

Table 6-2 Parameters for editing a port channel member

Parameter	Description
Interface	Serial number of the port, which cannot be modified.
Priority	Specifies the priority level of the interface. The parameter is effective only for dynamic aggregation, in which interfaces are selected based on their priorities. A smaller value indicates a higher priority. If two interfaces have the same priority, the selection is based on their IDs, which are sorted by the sequence number in ascending order. A smaller ID indicates a higher priority
Mode	Specifies the LACP working mode of the interface, which can be **Active** or **Passive**. • **Passive**: The interface does not send, but only receives Link Aggregation

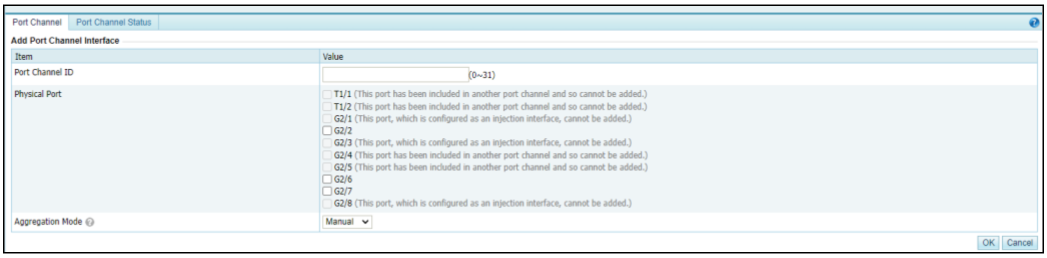
Parameter	Description
	Control Protocol Data Unit (LACPDUs) from the peer; - **Active**: The interface sends and receives LACPDUs. The parameter is effective only for dynamic aggregation.

Adding a Port Channel Interface

Currently, a port can only be included in one port channel.

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 6-5.

Figure 6-5 Creating a port channel for the ADS device



Add Port Channel Interface

Item	Value
Port Channel ID	(0~31)
Physical Port	□ T1/1 (This port has been included in another port channel and so cannot be added.) □ T1/2 (This port has been included in another port channel and so cannot be added.) □ G2/1 (This port, which is configured as an injection interface, cannot be added.) □ G2/2 □ G2/3 (This port, which is configured as an injection interface, cannot be added.) □ G2/4 (This port has been included in another port channel and so cannot be added.) □ G2/5 (This port has been included in another port channel and so cannot be added.) □ G2/6 □ G2/7 □ G2/8 (This port, which is configured as an injection interface, cannot be added.)
Aggregation Mode	Manual

Table 6-3 describes parameters for creating a port channel.

Table 6-3 Parameters for creating 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 can have one or several ports, but each port can be included in only one port channel. - A port configured with an IP address and configured as an injection interface cannot be added to a port channel.
Aggregation Mode	Specifies how member interfaces of the current port channel aggregate, which can be **Manual** or **Dynamic**. - **Manual**: The port channel does not run any protocol and its members remain unchanged; - **Dynamic**: The aggregation and selection of the port channel members totally depend on the LACP protocol.

Editing a Port Channel

On the port channel list in Figure 6-3, click 📝 in the **Operation** column to edit a 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.

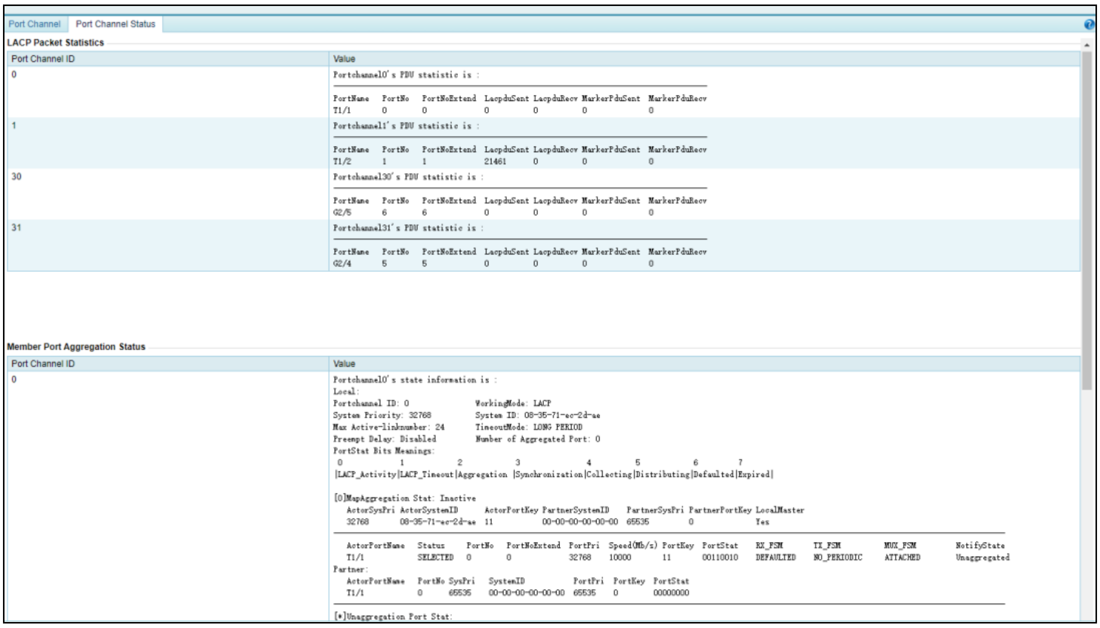
Note	A port channel configured with an IP address and injection interface cannot be deleted.

6.1.2.2 Port Channel Status

This page shows the statistics about LACP packets sent and received through port channels (**0** is displayed for a port channel in manual aggregation mode) and the member aggregation status.

Choose **Diversion & Injection** > **General Settings** > **Port Channel** > **Port Status** to open the port channel status page. See Figure 6-6.

Figure 6-6 Port Channel Status page



LACP Packet Statistics

Port Channel ID | Value

0
```
Portchannel0's PDU statistic is :
------------------------------------------------------------------------------------------
PortName   PortNo   PortNoExtend  LacpduSent LacpduRecv MarkerPduSent  MarkerPduRecv
T1/1       0        0             0          0          0              0
```

1
```
Portchannel1's PDU statistic is :
------------------------------------------------------------------------------------------
PortName   PortNo   PortNoExtend  LacpduSent LacpduRecv MarkerPduSent  MarkerPduRecv
T1/2       1        1             21461      0          0              0
```

30
```
Portchannel30's PDU statistic is :
------------------------------------------------------------------------------------------
PortName   PortNo   PortNoExtend  LacpduSent LacpduRecv MarkerPduSent  MarkerPduRecv
G2/5       6        6             0          0          0              0
```

31
```
Portchannel31's PDU statistic is :
------------------------------------------------------------------------------------------
PortName   PortNo   PortNoExtend  LacpduSent LacpduRecv MarkerPduSent  MarkerPduRecv
G2/4       5        5             0          0          0              0
```

Member Port Aggregation Status

Port Channel ID | Value

0
```
Portchannel0's state information is :
Local:
Portchannel ID: 0              WorkingMode: LACP
System Priority: 32768         System ID: 08-35-71-ec-2d-ae
Max Active-linknumber: 24      TimeoutMode: LONG PERIOD
Preempt Delay: Disabled        Number of Aggregated Port: 0
PortStat Bits Meanings:
 0            1           2           3               4          5            6         7
|LACP_Activity|LACP_Timeout|Aggregation |Synchronization|Collecting|Distributing|Defaulted|Expired|

[0]MapAggregation Stat: Inactive
   ActorSysPri ActorSystemID     ActorPortKey PartnerSystemID   PartnerSysPri PartnerPortKey LocalMaster
   32768       08-35-71-ec-2d-ae 11           00-00-00-00-00-00 65535         0              Yes
------------------------------------------------------------------------------------------------------------------
   ActorPortName  Status    PortNo   PortNoExtend  PortPri  Speed(Mb/s) PortKey  PortStat  RX_FSM    TX_FSM       MUX_FSM     NotifyState
   T1/1           SELECTED  0        0             32768    10000       11       00110010  DEFAULTED NO_PERIODIC  ATTACHED    Unaggregated
Partner:
   ActorPortName  PortNo SysPri  SystemID           PortPri  PortKey  PortStat
   T1/1           0      65535   00-00-00-00-00-00  65535    0        00000000
------------------------------------------------------------------------------------------------------------------
[*]Unaggregation Port Stat:
```

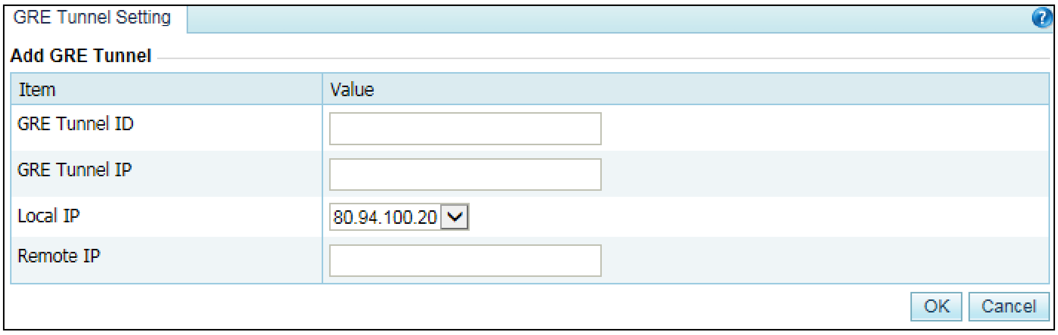
6.1.3 GRE Tunnel Configuration

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.

Creating a GRE Tunnel

Step 1 To the lower right of the GRE tunnel list, click **Add**.

Figure 6-7 Creating a GRE tunnel



Item	Value
GRE Tunnel ID	
GRE Tunnel IP	
Local IP	80.94.100.20
Remote IP	

Step 2 On the **Add GRE Tunnel** page, configure parameters.

Table 6-4 describes parameters for creating a GRE tunnel.

Table 6-4 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 or IPv6 address.
Remote IP	Destination IP address of the GRE tunnel. This parameter can be set to an IPv4 or IPv6 address.

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

----End

Modifying a GRE Tunnel

On the GRE tunnel list, click 📝 in the **Operation** column to edit GRE tunnel configuration. The configuration of GRE tunnels in use cannot be edited.

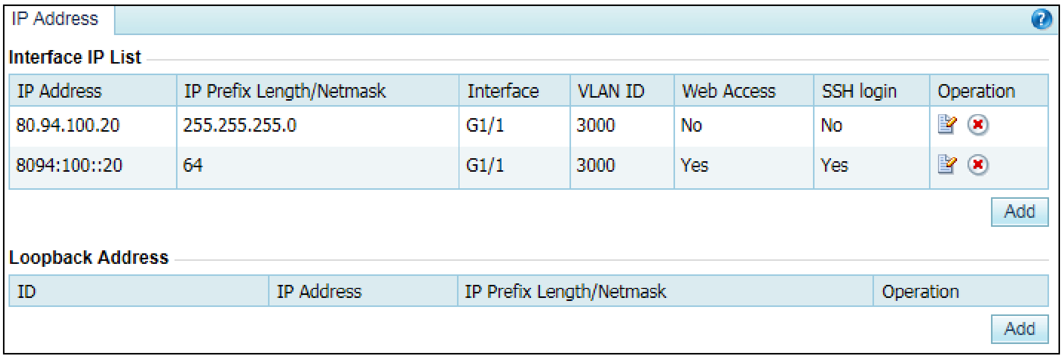
Deleting a GRE Tunnel

On the GRE tunnel list, click ✖ in the **Operation** column to delete a GRE tunnel. GRE tunnels in use cannot be deleted.

6.1.4 IP Address Configuration

For ADS running in diversion mode, you can configure the IP addresses and loopback addresses for two interfaces that are used by ADS on the page shown in Figure 6-8.

Figure 6-8 IP address list in diversion mode



Interface IP List

IP Address	IP Prefix Length/Netmask	Interface	VLAN ID	Web Access	SSH login	Operation
80.94.100.20	255.255.255.0	G1/1	3000	No	No	✎ ✖
8094:100::20	64	G1/1	3000	Yes	Yes	✎ ✖

Loopback Address

ID	IP Address	IP Prefix Length/Netmask	Operation

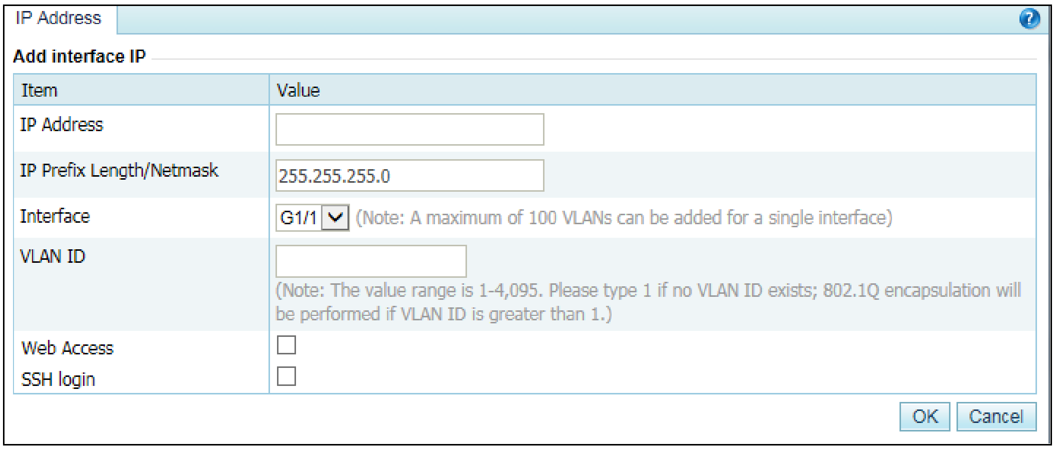
Note

The number of interfaces varies with ADS series, but the procedure for configuring interfaceIP addresses is the same. This section uses ADS NX5-4020E 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 6-9.

Figure 6-9 Adding an IP address



Add interface IP

Item	Value
IP Address	
IP Prefix Length/Netmask	255.255.255.0
Interface	G1/1 (Note: A maximum of 100 VLANs can be added for a single interface)
VLAN ID	(Note: The value range is 1-4,095. Please type 1 if no VLAN ID exists; 802.1Q encapsulation will be performed if VLAN ID is greater than 1.)
Web Access	□
SSH login	□

Table 6-5 describes parameters of an interface.

Table 6-5 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 based on an IPv4 address is not recommended. 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.

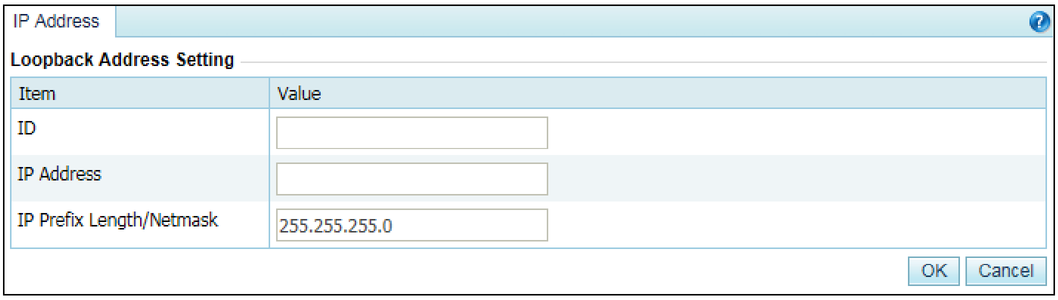
Deleting an IP Address

On the page shown in Figure 6-8, 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 Setting** page appears, as shown in Figure 6-10.

Figure 6-10 Adding a loopback address



IP Address

Loopback Address Setting

Item	Value
ID	
IP Address	
IP Prefix Length/Netmask	255.255.255.0

Table 6-6 describes parameters of a loopback address.

Table 6-6 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

On the page shown in Figure 6-8, click ⊗ in the **Operation** column to delete a loopback address. Loopback addresses in use cannot be deleted.

6.1.5 Incoming/Outgoing Configuration

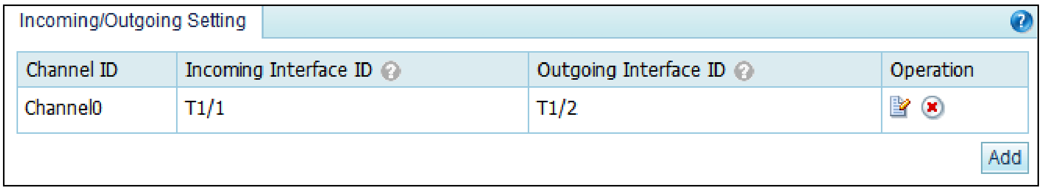
This section describes how to configure a pair of incoming and outgoing interfaces for connecting to an external bypass switch.

Note	The incoming/outgoing configuration is available only when ADS is deployed in in-path mode.

You can add, edit, and delete incoming/outgoing interface pairs. For how to add a pair of incoming/outgoing interfaces, perform the following steps:

Step 1 Choose **Diversion & Injection** > **General Settings** > **Incoming/Outgoing Setting**.

Figure 6-11 Incoming/Outgoing Setting page

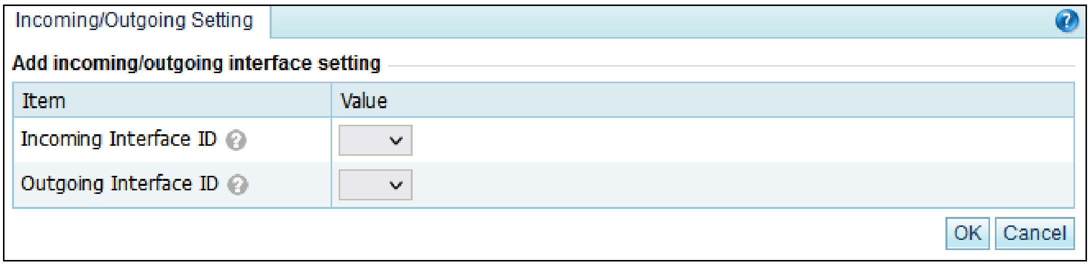


Incoming/Outgoing Setting

Channel ID	Incoming Interface ID	Outgoing Interface ID	Operation
Channel0	T1/1	T1/2	✎ ⊗

Step 2 Click **Add**.

Figure 6-12 Adding a pair of incoming/outgoing interfaces



Incoming/Outgoing Setting

Add incoming/outgoing interface setting

Item	Value
Incoming Interface ID	
Outgoing Interface ID	

Step 3 Specify **Incoming Interface ID** and **Outgoing Interface ID**.

Step 4 Click **OK** to complete the configuration.

----End

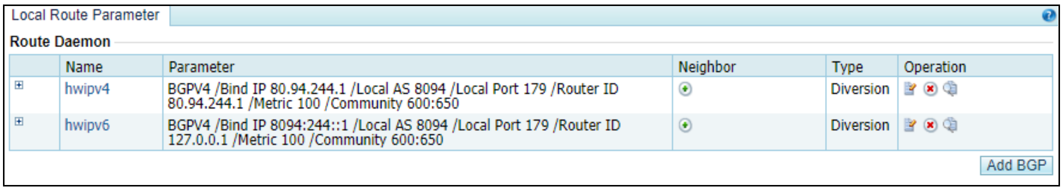
6.2 Diversion Route

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

Choose **Diversion & Injection** > **Diversion Route** > **BGP Route**. As shown in Figure 6-13, only BGP routes are displayed on the **Local Route Parameter** page.

Figure 6-13 Local route parameters



Local Route Parameter

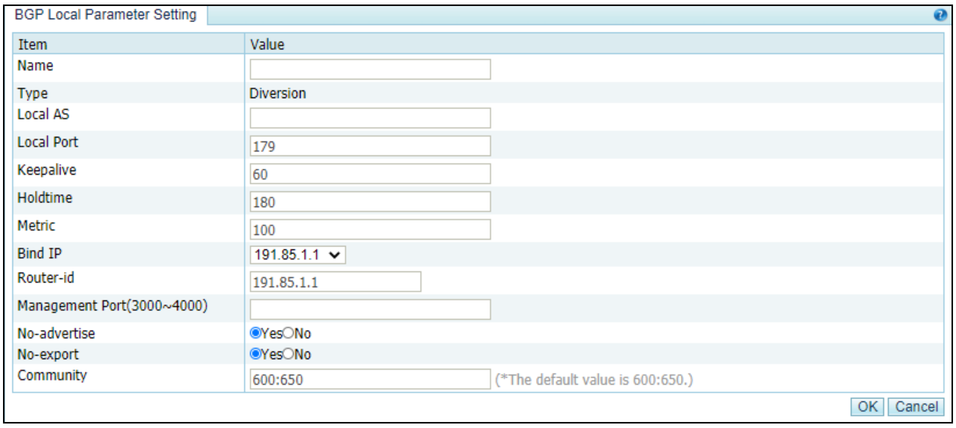
Route Daemon

	Name	Parameter	Neighbor	Type	Operation
⊞	hwipv4	BGPV4 /Bind IP 80.94.244.1 /Local AS 8094 /Local Port 179 /Router ID 80.94.244.1 /Metric 100 /Community 600:650	⊕	Diversion	
⊞	hwipv6	BGPV4 /Bind IP 8094:244::1 /Local AS 8094 /Local Port 179 /Router ID 127.0.0.1 /Metric 100 /Community 600:650	⊕	Diversion	

Creating a BGP Route

On the page shown in Figure 6-13, click **Add BGP** to the lower right of the route daemon list to configure local BGP parameters. See Figure 6-14.

Figure 6-14 Creating a BGP route



BGP Local Parameter Setting

Item	Value
Name	
Type	Diversion
Local AS	
Local Port	179
Keepalive	60
Holdtime	180
Metric	100
Bind IP	191.85.1.1
Router-id	191.85.1.1
Management Port(3000~4000)	
No-advertise	●Yes○No
No-export	●Yes○No
Community	600:650 (*The default value is 600:650.)

OK Cancel

Table 6-7 describes parameters for creating a BGP route.

Table 6-7 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.
Router-id	Router ID included in the BGP route.
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**.

Note	Other parameters including **Keepalive**, **Holdtime**, **Metric**, **No-advertise**, and **No-export** are directly taken from the BGPv4 protocol.

Editing a BGP Route

On the route daemon list shown in Figure 6-13, 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 6-13, click ✖ in the **Operation** column to delete a route.

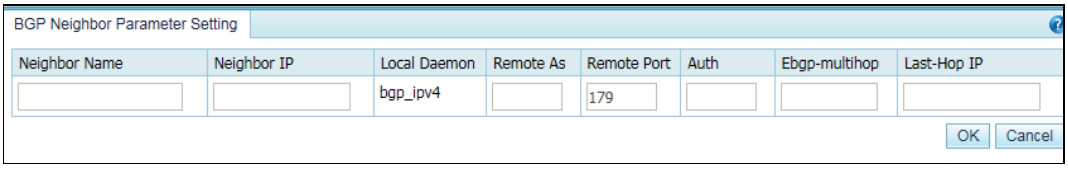
Viewing the Route Status

On the route daemon list shown in Figure 6-13, 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 6-13, click ⊕ in the **Neighbor** column to add a BGP neighbor. See Figure 6-15.

Figure 6-15 Adding a BGP neighbor



BGP Neighbor Parameter Setting

Neighbor Name	Neighbor IP	Local Daemon	Remote As	Remote Port	Auth	Ebgp-multihop	Last-Hop IP
		bgp_ipv4		179			

Note	After a neighbor is added, click ▶ to check whether it is connected.

Table 6-8 describes parameters of a BGP neighbor.

Table 6-8 Parameters for creating 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.

Parameter	Description
Ebgp-multihop	Maximum number of hops allowed by the External Border Gateway Protocol (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

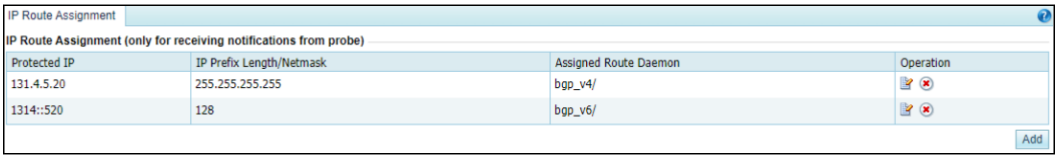
After all BGP neighbors are displayed, you can click ✎ to modify information of a neighbor, click ⊗ to delete a neighbor, click ▶ to check whether a neighbor can be pinged, or click 🔍 to view the connection status of a neighbor.

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's anti-DDoS detection device and to decide which route daemon sends notifications. See Figure 6-16.

Figure 6-16 IP route assignment



IP Route Assignment

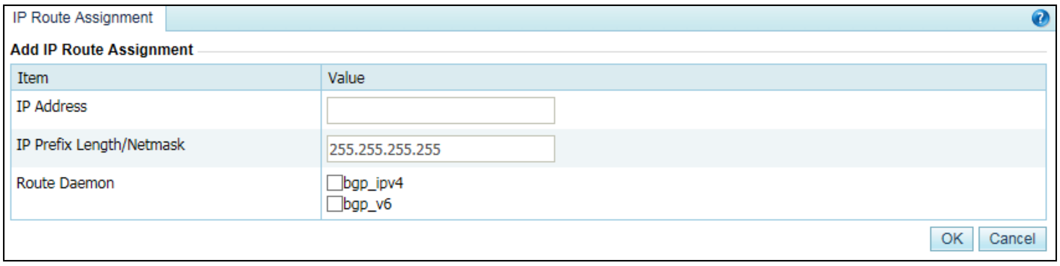
IP Route Assignment (only for receiving notifications from probe)

Protected IP	IP Prefix Length/Netmask	Assigned Route Daemon	Operation
131.4.5.20	255.255.255.255	bgp_v4/	✎ ⊗
1314::520	128	bgp_v6/	✎ ⊗

Creating an IP Route

On the page shown in Figure 6-16, 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 6-17 Creating an IP route



Add IP Route Assignment

Item	Value
IP Address	
IP Prefix Length/Netmask	255.255.255.255
Route Daemon	□bgp_ipv4 □bgp_v6

Table 6-9 describes parameters for creating an IP route.

Table 6-9 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 6-16, click ✎ in the **Operation** column to edit an IP route.

Deleting an IP Route

On the IP route assignment list shown in Figure 6-16, 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 NX5-4020E 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:

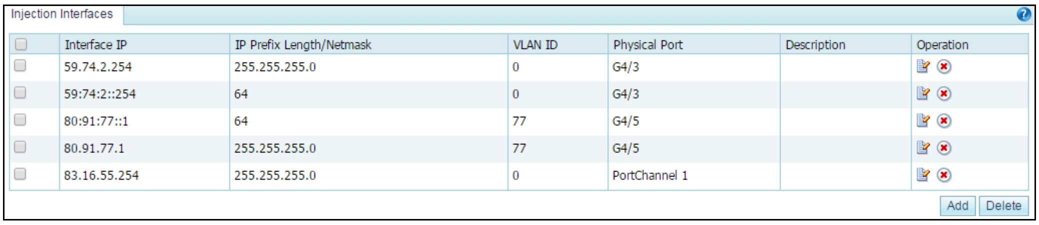
- Adding an Injection Interface
- Editing an Injection Interface
- Deleting Injection Interfaces

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**.

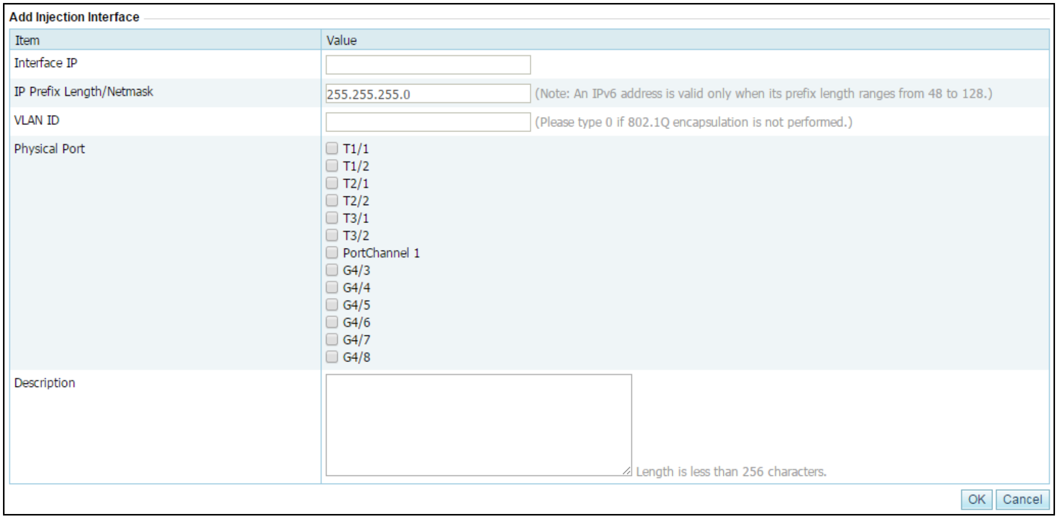
Figure 6-18 Injection interface list



□	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		

Step 2 Click **Add** to open the page for adding an injection interface.

Figure 6-19 Adding an injection interface



Add Injection Interface

Item	Value
Interface IP	
IP Prefix Length/Netmask	255.255.255.0 (Note: An IPv6 address is valid only when its prefix length ranges from 48 to 128.)
VLAN ID	(Please type 0 if 802.1Q encapsulation is not performed.)
Physical Port	□ T1/1 □ T1/2 □ T2/1 □ T2/2 □ T3/1 □ T3/2 □ PortChannel 1 □ G4/3 □ G4/4 □ G4/5 □ G4/6 □ G4/7 □ G4/8
Description	Length is less than 256 characters.

Table 6-10 describes parameters of an injection interface.

Table 6-10 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 6-18, 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 6-18, 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

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 primary-secondary mechanism among routes achieves high availability.

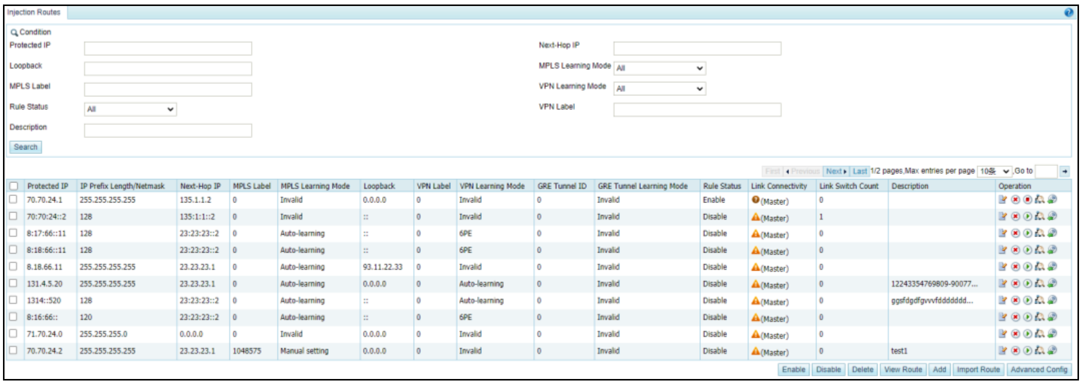
This section covers the following topics:

- 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
-
- Searching for Injection Routes

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 6-20.



Injection Routes

Condition

Protected IP		Next-Hop IP	
Loopback		MPLS Learning Mode	All
MPLS Label		VPN Learning Mode	All
Rule Status	All	VPN Label	
Description			

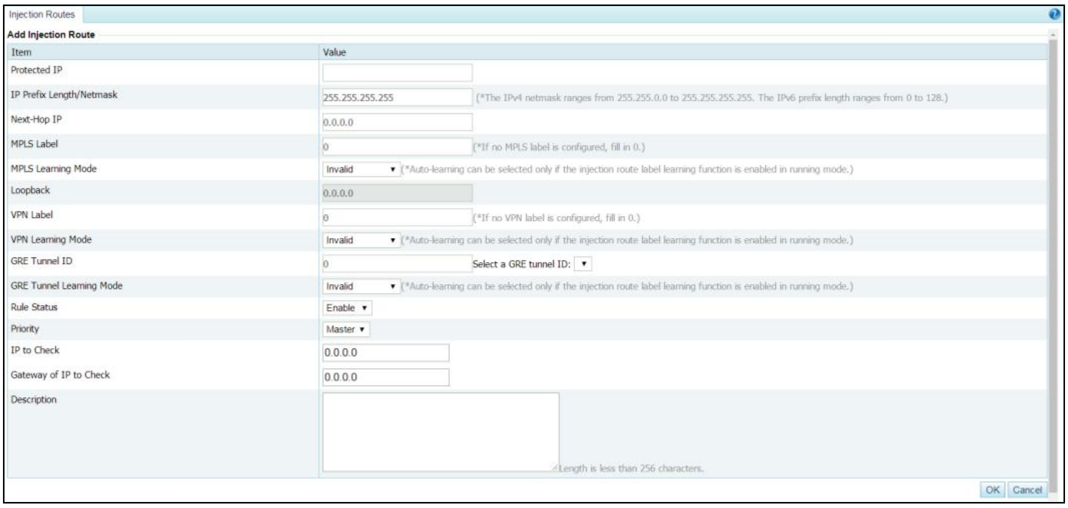
Search

First | Previous | Next | Last 1/2 pages,Max entries per page 10条 ,Go to

□	Protected IP	IP Prefix Length/Netmask	Next-Hop IP	MPLS Label	MPLS Learning Mode	Loopback	VPN Label	VPN Learning Mode	GRE Tunnel ID	GRE Tunnel Learning Mode	Rule Status	Link Connectivity	Link Switch Count	Description	Operation
□	70.70.24.1	255.255.255.255	135.1.1.2	0	Invalid	0.0.0.0	0	Invalid	0	Invalid	Enable	●(Master)	0		
□	70:70:24::2	128	135:1:1::2	0	Invalid	::	0	Invalid	0	Invalid	Disable	⚠(Master)	1		
□	8:17:66::11	128	23:23:23::2	0	Auto-learning	::	0	6PE	0	Invalid	Disable	⚠(Master)	0		
□	8:18:66::11	128	23:23:23::2	0	Auto-learning	::	0	6PE	0	Invalid	Disable	⚠(Master)	0		
□	8.18.66.11	255.255.255.255	23.23.23.1	0	Auto-learning	93.11.22.33	0	Invalid	0	Invalid	Disable	⚠(Master)	0		
□	131.4.5.20	255.255.255.255	23.23.23.1	0	Auto-learning	0.0.0.0	0	Auto-learning	0	Invalid	Disable	⚠(Master)	0	12243354769809-90077...	
□	1314::520	128	23:23:23::2	0	Auto-learning	::	0	Auto-learning	0	Invalid	Disable	⚠(Master)	0	ggsfdgdfgvvvfddddddd...	
□	8:16:66::	120	23:23:23::2	0	Auto-learning	::	0	6PE	0	Invalid	Disable	⚠(Master)	0		
□	71.70.24.0	255.255.255.0	0.0.0.0	0	Invalid	0.0.0.0	0	Invalid	0	Invalid	Disable	⚠(Master)	0		
□	70.70.24.2	255.255.255.255	23.23.23.1	1048575	Manual setting	0.0.0.0	0	Invalid	0	Invalid	Disable	⚠(Master)	0	test1	

Figure 6-20 Injection routes

Step 2 Click **Add**.



Injection Routes

Add Injection Route

Item	Value
Protected IP	
IP Prefix Length/Netmask	255.255.255.255 (*The IPv4 netmask ranges from 255.255.0.0 to 255.255.255.255. The IPv6 prefix length ranges from 0 to 128.)
Next-Hop IP	0.0.0.0
MPLS Label	0 (*If no MPLS label is configured, fill in 0.)
MPLS Learning Mode	Invalid (*Auto-learning can be selected only if the injection route label learning function is enabled in running mode.)
Loopback	0.0.0.0
VPN Label	0 (*If no VPN label is configured, fill in 0.)
VPN Learning Mode	Invalid (*Auto-learning can be selected only if the injection route label learning function is enabled in running mode.)
GRE Tunnel ID	0 Select a GRE tunnel ID:
GRE Tunnel Learning Mode	Invalid (*Auto-learning can be selected only if the injection route label learning function is enabled in running mode.)
Rule Status	Enable
Priority	Master
IP to Check	0.0.0.0
Gateway of IP to Check	0.0.0.0
Description	Length is less than 256 characters.

Figure 6-21 Creating an injection route

Table 6-11 describes parameters for creating an injection route.

Table 6-11 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. Note

Parameter	Description
	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.
Loopback	Specifies the loopback IP address of the border router in the network where the protected server resides.
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. In this mode, the loopback interface uses the IP address of the MP-BGP neighbor by default. • **Invalid**: indicates that no VPN label is configured. • **6PE**: indicates that the injection route uses the 6PE mode. In this mode, the loopback interface uses the IP address of the MP-BGP neighbor by default.
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

Parameter	Description
	forwarding packets. • **Disable**: indicates that the system does not query the injection rule when forwarding packets.
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 IPto 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**.
Description	Brief information about the route.

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.

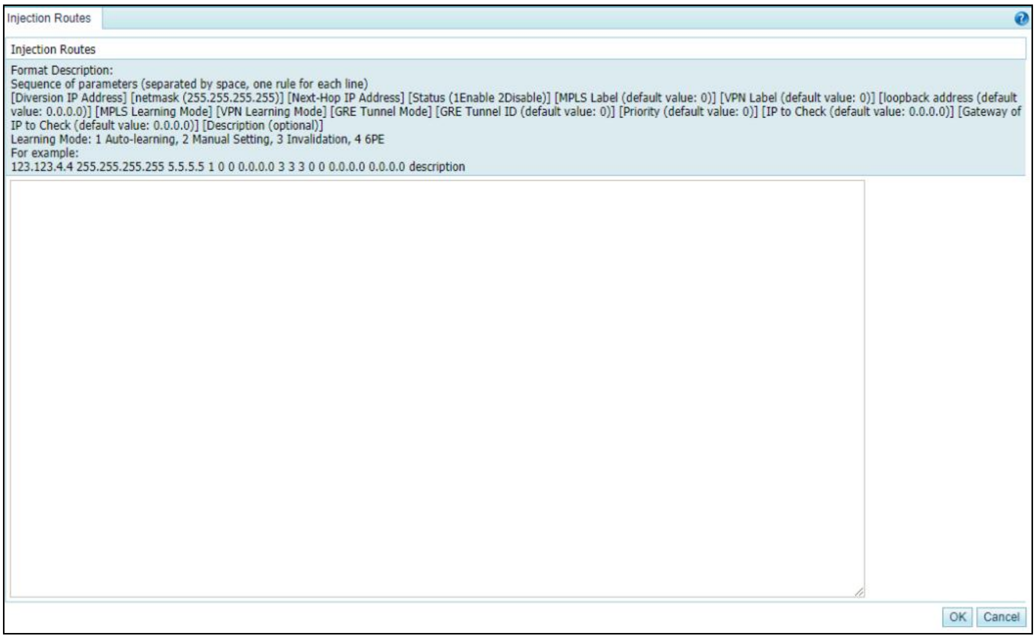
----End

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.

Figure 6-22 Creating injection routes in batches



Injection Routes

Injection Routes

Format Description:
Sequence of parameters (separated by space, one rule for each line)
[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)] [Priority (default value: 0)] [IP to Check (default value: 0.0.0.0)] [Gateway of IP to Check (default value: 0.0.0.0)] [Description (optional)]
Learning Mode: 1 Auto-learning, 2 Manual Setting, 3 Invalidation, 4 6PE
For example:
123.123.4.4 255.255.255.255 5.5.5.5 1 0 0 0.0.0.0 3 3 3 0 0 0.0.0.0 0.0.0.0 description

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 auto-learning, the value **2** indicates manual setting, the value **3** indicates invalid, and the value **4** indicates 6PE.
- 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 6-20. 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 6-20. The link connectivity could be one of the following:

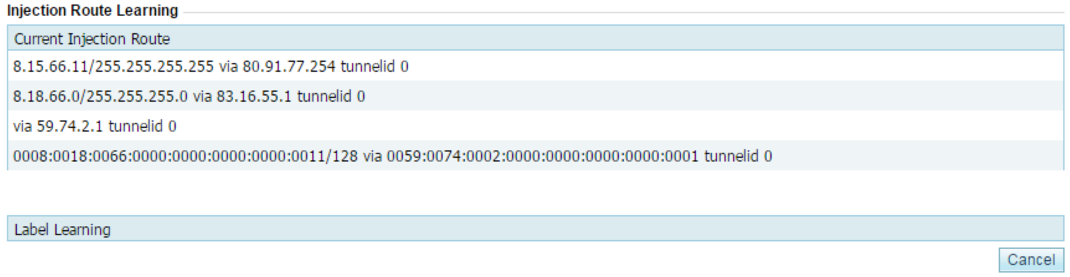
- ✓: The link of this injection route functions properly. That is, ADS can successfully ping the **IP to Check** of the injection route.
- ✖: The link of this injection route is faulty. That is, ADS fails to ping the **IP to Check** of the injection route. In this case, traffic cannot be injected along 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 6-23 Viewing injection routes and learned labels



Injection Route Learning

Current Injection Route

```
8.15.66.11/255.255.255.255 via 80.91.77.254 tunnelid 0
8.18.66.0/255.255.255.0 via 83.16.55.1 tunnelid 0
via 59.74.2.1 tunnelid 0
0008:0018:0066:0000:0000:0000:0000:0011/128 via 0059:0074:0002:0000:0000:0000:0000:0001 tunnelid 0
```

Label Learning

- **Current Injection Route** lists current injection routes that are taking effect on the device engine.
- **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

Injection routes support encapsulation of two layers of labels.

- Upper labels: MPLS labels that are learned via the MPLS protocol. To enable MPLS label learning support on the device, you need to first enable the Label Distribution Protocol (LDP), then configure an MPLS label and the MPLS learning mode for injection routes, and enable injection route label learning.
- Lower labels: 6PE labels or VPN labels that are learned via MP-BGP. To enable support of 6PE or VPN labels on the device, you need to first configure MP-BGP and then configure the VPN label and VPN learning mode for injection routes.

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 auto-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 6-20.

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 6-20, 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 6-20, 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 6-20, 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 6-20, 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 6-20.

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 6-20, 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 6-20, 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.

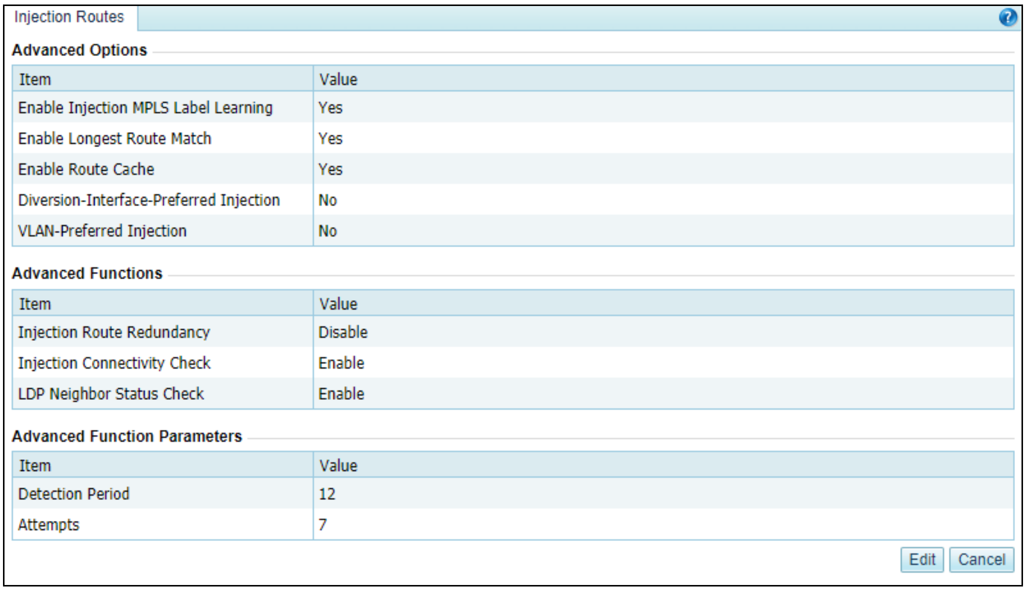
6.3.2.11 Editing Advanced Configurations

You can edit advanced configurations that apply to all injection routes.

Click **Advanced Config** to the lower right of the injection route list shown in Figure 6-20. The page for editing advanced configurations appears.

- By default, no function is enabled. See Figure 6-23.
- After **Injection Route Redundancy** is set to **Enable**, advanced options are as shown in Figure 6-25.

Figure 6-24 Advanced options



Advanced Options

Item	Value
Enable Injection MPLS Label Learning	Yes
Enable Longest Route Match	Yes
Enable Route Cache	Yes
Diversion-Interface-Preferred Injection	No
VLAN-Preferred Injection	No

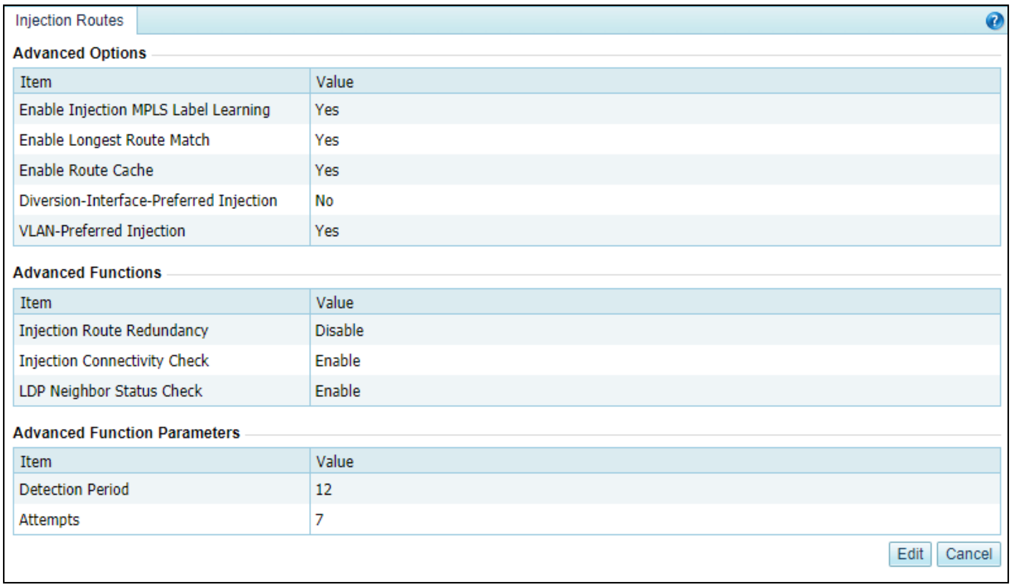
Advanced Functions

Item	Value
Injection Route Redundancy	Disable
Injection Connectivity Check	Enable
LDP Neighbor Status Check	Enable

Advanced Function Parameters

Item	Value
Detection Period	12
Attempts	7

Figure 6-25 Advanced options – with the injection route redundancy enabled



Advanced Options

Item	Value
Enable Injection MPLS Label Learning	Yes
Enable Longest Route Match	Yes
Enable Route Cache	Yes
Diversion-Interface-Preferred Injection	No
VLAN-Preferred Injection	Yes

Advanced Functions

Item	Value
Injection Route Redundancy	Disable
Injection Connectivity Check	Enable
LDP Neighbor Status Check	Enable

Advanced Function Parameters

Item	Value
Detection Period	12
Attempts	7

Step 2 After configuring parameters, click **OK**.

Table 6-12 describes advanced options of injection routes.

Table 6-12 Parameters for advanced options of injection routers

Parameter		Description
Advanced Options	Enable Injection MPLS Label Learning	Controls whether to enable MPLS label learning for injection routes. The default value is **No**. This needs to be enabled only when MPLS injection is enabled.

Parameter		Description
		Note • If MPLS label learning is enabled while MPLS injection is disabled, injection routes of other types will be unable to be dispatched. • MPLS label learning for injection routes 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 IP address, the system selects one based on their netmask values. The route with the largest netmask value will be selected.
	Enable Route Cache	Controls whether to enable route cache. The default value is **No**. The route cache needs to be enabled only when longest route match is enabled. The route cache is like a fast forwarding table. With this enabled, the system does not need to check the entire injection routing table every time.
	Diversion-Interface-Preferred Injection	Controls whether to enable diversion-interface-preferred injection. The default value is **No**. After this 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 should first enable longest route match. • Diversion-interface-preferred injection and injection route redundancy cannot be enabled simultaneously. To enable diversion-interface-preferred injection, you should ensure that the injection route over the diversion interface has the highest priority or all injection routes have the same priority.
	VLA-Preferred Injection	Control whether to inject traffic preferentially from VLAN. The default value is **No**. If this function is enabled, the traffic will be preferentially injected from VLAN.
Advanced Functions	Injection Route Redundancy	Controls whether to enable the injection route redundancy function. Note After injection route redundancy is enabled, neither diversion-interface-preferred injection nor injection MPLS label learning can be enabled.
	Injection Connectivity Check	Controls whether to enable injection connectivity checking. After this is enabled, ADS periodically checks whether the link is available, that is, whether **IP to Check** specified in the injection route rule is reachable. If not, the injection route will be unable to take effect. When **IP to Check** is **0.0.0.0** (default), the system checks whether the next-hop IP address is reachable.

Parameter		Description
	LDP Neighbor Status Check	Controls whether to enable the LDP neighbor status check. After this is enabled, ADS periodically checks whether its LDP neighbor is reachable if MPLS label learning is also enabled for injection routes. If not, all MPLS-related injection routes will lose effect and traffic diversion for all MPLS-related IP addresses will stop.
Advanced Function Parameters	Detection Period	Specifies the interval between two link availability checks. The value ranges from 1 to 600, in seconds. The default value is **60**.
	Attempts	Specifies 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 and a link switch is triggered.
	Link Switch Limit	Specifies the maximum number of link status switches before an injection link is considered invalid. The value ranges from 0 to 10, and the default value is **5**. The value **0** indicates no limit on the number of link status switches. Note A link status switch is counted when the status of a link changes from up to down, but not when the status changes from down to up. After the number of link status switches exceeds the specified maximum number, the system automatically adjusts the priority of the injection link.

6.3.2.12 Searching for Injection Routes

The injection route table shown in Figure 6-20 lists all existing injection routes in the ascending order of creation time by default. By default, each page lists 10 entries. You can also change the number to **20**, **50**, or **100**.

You can set filtering conditions in the upper part of the page to list only injection routes meeting the specified conditions. The procedure is as follows:

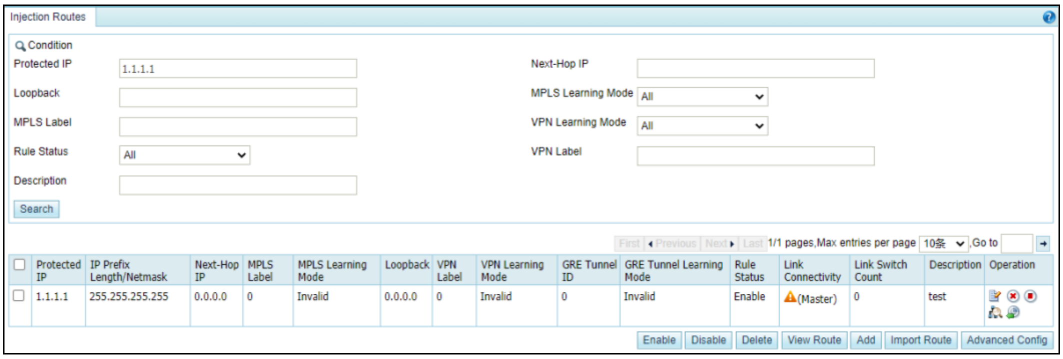
Step 1 Set filtering conditions.

For the description of parameters, see Table 6-11.

Step 2 Click **Search**.

Then only injection routes meeting the conditions are listed below, as shown in Figure 6-26.

Figure 6-26 Searching for injection routes



Protected IP: 1.1.1.1

Loopback:

MPLS Label:

Rule Status: All

Description:

Next-Hop IP:

MPLS Learning Mode: All

VPN Learning Mode: All

VPN Label:

1/1 pages,Max entries per page 10条 ,Go to

□	Protected IP	IP Prefix Length/Netmask	Next-Hop IP	MPLS Label	MPLS Learning Mode	Loopback	VPN Label	VPN Learning Mode	GRE Tunnel ID	GRE Tunnel Learning Mode	Rule Status	Link Connectivity	Link Switch Count	Description	Operation
□	1.1.1.1	255.255.255.255	0.0.0.0	0	Invalid	0.0.0.0	0	Invalid	0	Invalid	Enable	⚠(Master)	0	test	

----End

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:

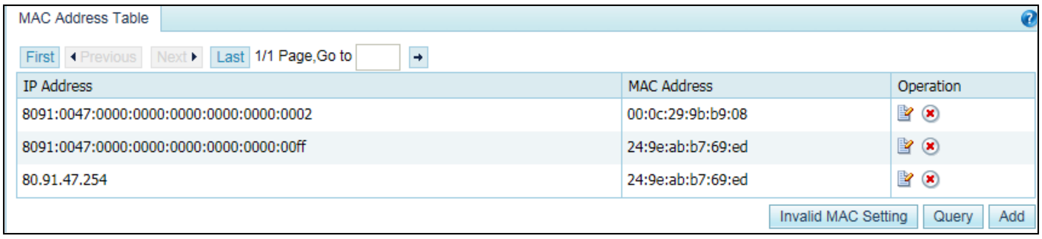
- Adding a MAC Address Entry
- Editing a MAC Address Entry
- Deleting a MAC Address Entry
- Querying MAC Addresses
- Configuring Invalid MAC Addresses
- Configuring Valid MAC Addresses

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 6-27 MAC address table

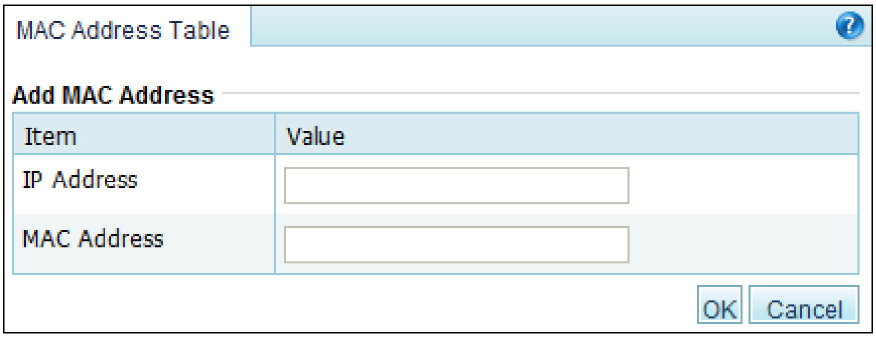


1/1 Page,Go to

IP Address	MAC Address	Operation
8091:0047:0000:0000:0000:0000:0000:0002	00:0c:29:9b:b9:08	
8091:0047:0000:0000:0000:0000:0000:00ff	24:9e:ab:b7:69:ed	
80.91.47.254	24:9e:ab:b7:69:ed	

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 6-28 Adding the mapping between an IP address and a MAC address



MAC Address Table

Add MAC Address

Item	Value
IP Address	
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 6-27, 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.

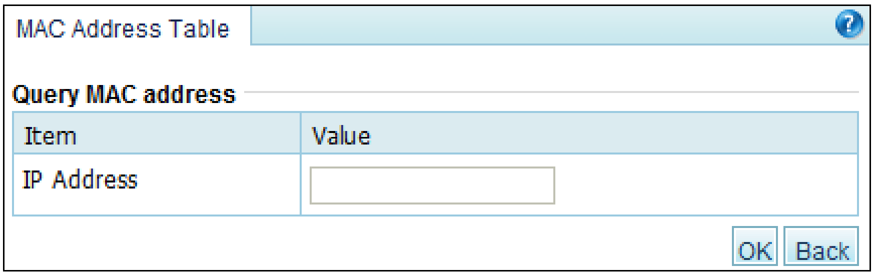
In the MAC address table shown in Figure 6-27, click ✖ in the **Operation** column of a MAC address entry and then click **OK** to delete an entry.

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 On the page shown in Figure 6-27, click **Query** to the lower right of the MAC address table to open the MAC address query page.

Figure 6-29 Querying the MAC address mapped to an IP address



Item	Value
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

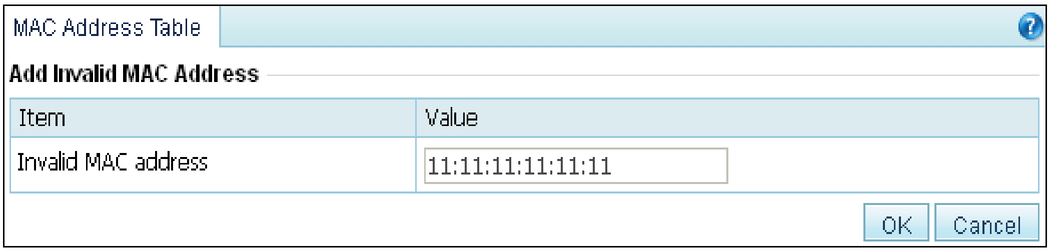
6.3.3.5 Configuring Invalid MAC Addresses

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 On the page shown in Figure 6-27, click **Invalid MAC Setting** to the lower right of the MAC address table to open the page for configuring invalid MAC addresses. See Figure 6-30.

Figure 6-30 Configuring invalid MAC addresses



Item	Value
Invalid MAC address	11:11:11:11:11:11

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

6.3.3.6 Configuring Valid MAC Addresses

The valid MAC addresses can be dynamically learned or statically configured, as shown in the **Status** column. You can operate on valid MAC addresses as follows:

- Querying a valid MAC address

  Click **Search** to the lower right of the valid MAC address list to open the MAC address query page. Type the IPv4 or IPv6 address and click **OK**. Then, the valid MAC address mapped to this IP address is displayed.

- Deleting a valid MAC address

  Click ✖ in the **Operation** column of a valid MAC address and then click **OK** to delete it. Make sure deleting this valid MAC address will not affect the current service traffic. To delete a static MAC address, see section 6.3.3.3 **Deleting a MAC Address Entry**.

6.4 Traffic Diversion

This section covers the following topics:

- Filtering Rules
- Manual Diversion
- Group Diversion
- Diversion Routing Table

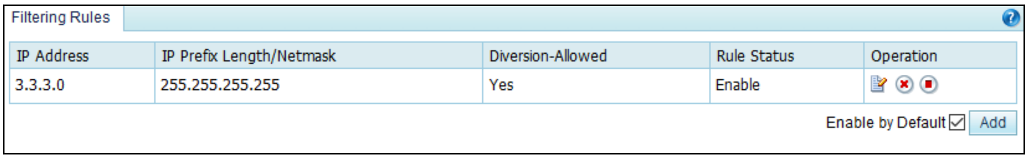
6.4.1 Filtering Rules

A diversion filtering rule informs the current ADS device whether to advertise route information for automatic traffic diversion when receiving attack information from NSFOCUS's anti-DDoS detection devices.

As shown in Figure 6-31, 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.

Enable by Default indicates that ADS, by default, diverts the traffic of the protected IP address included in the routing notification from NSFOCUS Probe.

Figure 6-31 Filtering rules



Filtering Rules

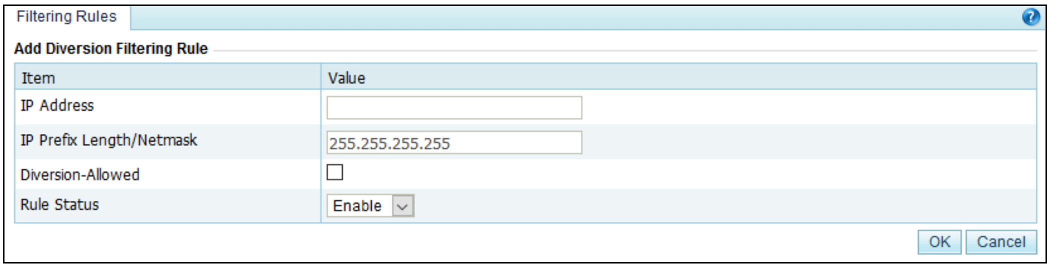
IP Address	IP Prefix Length/Netmask	Diversion-Allowed	Rule Status	Operation
3.3.3.0	255.255.255.255	Yes	Enable	✎ ✖ ●

Enable by Default ☑ Add

Creating a Diversion Filtering Rule

On the page shown in Figure 6-31, click **Add** to the lower right of the list. On the **Add Diversion Filtering Rule** page, configure parameters and click **OK**.

Figure 6-32 Creating a diversion filtering rule



Add Diversion Filtering Rule

Item	Value
IP Address	
IP Prefix Length/Netmask	255.255.255.255
Diversion-Allowed	□
Rule Status	Enable

Table 6-13 describes parameters for creating a diversion filtering rule.

Table 6-13 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.
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 6-31, click ✎ in the **Operation** column to edit a rule.

Deleting a Diversion Filtering Rule

On the diversion filtering rule list shown in Figure 6-31, 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 6-31, 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 6-31, 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:

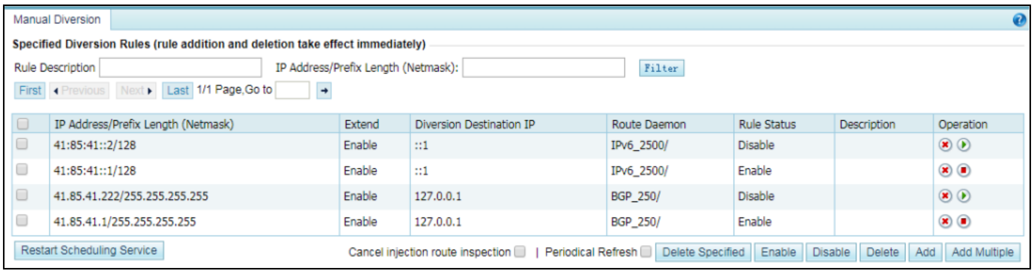
- Creating a Manual Traffic Diversion Rule
- Creating Manual Diversion Rules in Batches
- Enabling and Disabling Manual Diversion Rules
- Filtering Manual Diversion Rules
- Deleting Manual Diversion Rules
- Deleting a Specified Route
- Refreshing Routes Periodically
- Canceling Injection Route Inspection
- 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** > **TrafficDiversion** > **Manual Diversion** to open the diversion rule configuration page.

Figure 6-33 Traffic diversion rules



Manual Diversion

Specified Diversion Rules (rule addition and deletion take effect immediately)

Rule Description: 　IP Address/Prefix Length (Netmask): 　[Filter]

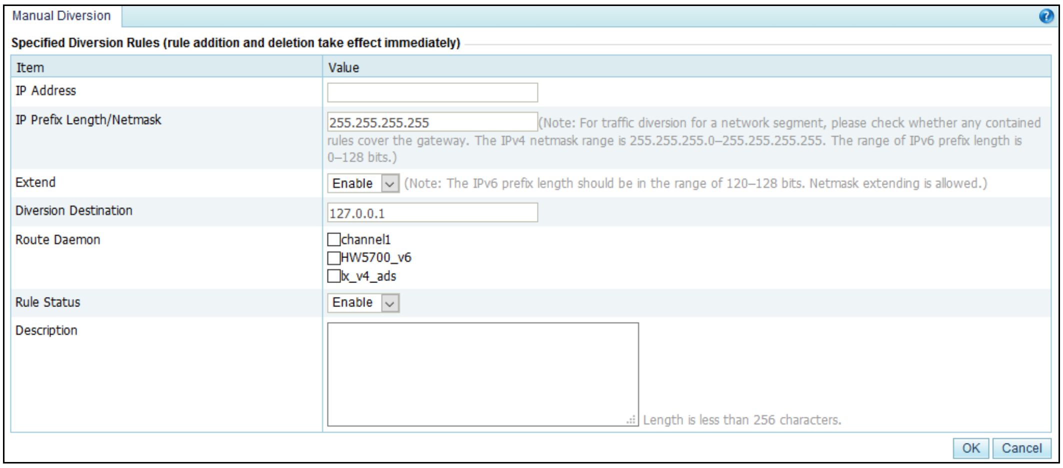
[First] [◂ Previous] [Next ▸] [Last] 1/1 Page,Go to [ ] [→]

□	IP Address/Prefix Length (Netmask)	Extend	Diversion Destination IP	Route Daemon	Rule Status	Description	Operation
□	41:85:41::2/128	Enable	::1	IPv6_2500/	Disable		☒ ▶
□	41:85:41::1/128	Enable	::1	IPv6_2500/	Enable		☒ ■
□	41.85.41.222/255.255.255.255	Enable	127.0.0.1	BGP_250/	Disable		☒ ▶
□	41.85.41.1/255.255.255.255	Enable	127.0.0.1	BGP_250/	Enable		☒ ■

[Restart Scheduling Service] 　Cancel injection route inspection □ | Periodical Refresh □ [Delete Specified] [Enable] [Disable] [Delete] [Add] [Add Multiple]

Step 2 Click **Add**.

Figure 6-34 Creating a traffic diversion rule



Specified Diversion Rules (rule addition and deletion take effect immediately)

Item	Value
IP Address	
IP Prefix Length/Netmask	255.255.255.255 (Note: For traffic diversion for a network segment, please check whether any contained rules cover the gateway. The IPv4 netmask range is 255.255.255.0–255.255.255.255. The range of IPv6 prefix length is 0–128 bits.)
Extend	Enable (Note: The IPv6 prefix length should be in the range of 120–128 bits. Netmask extending is allowed.)
Diversion Destination	127.0.0.1
Route Daemon	□channel1 □HW5700_v6 □lx_v4_ads
Rule Status	Enable
Description	Length is less than 256 characters.

Table 6-14 describes parameters for creating a diversion rule.

Table 6-14 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.

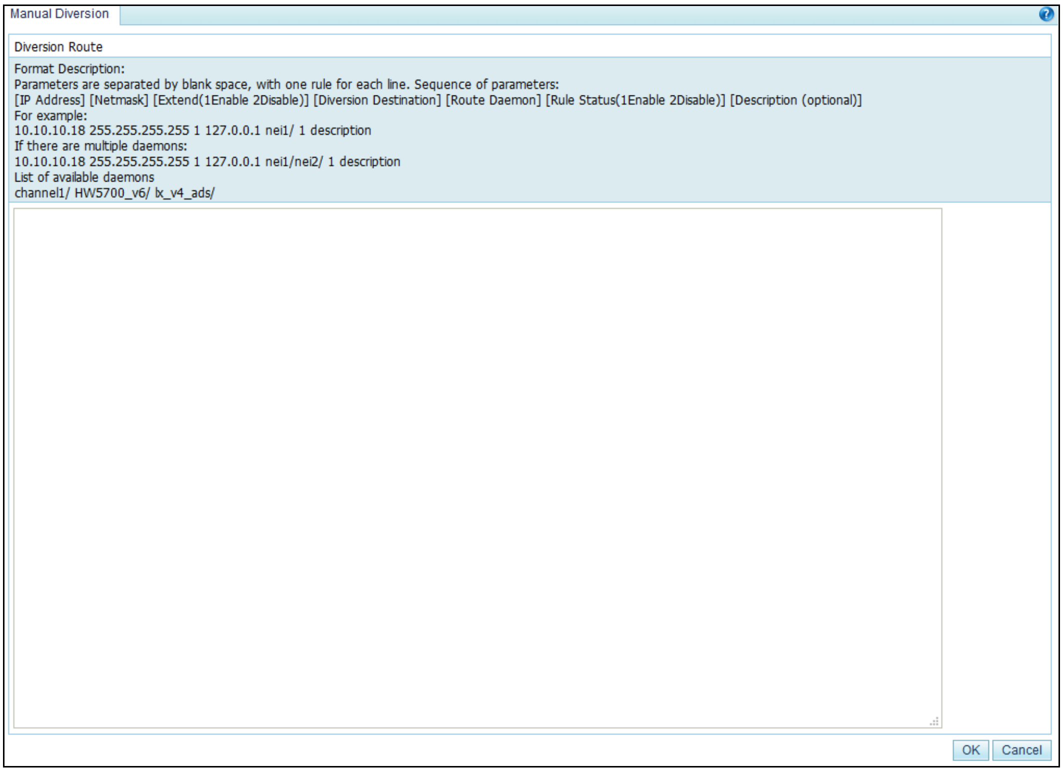
----End

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 6-33.

Figure 6-35 Creating traffic diversion rules in batches



Manual Diversion

Diversion Route

Format Description:
Parameters are separated by blank space, with one rule for each line. Sequence of parameters:
[IP Address] [Netmask] [Extend(1Enable 2Disable)] [Diversion Destination] [Route Daemon] [Rule Status(1Enable 2Disable)] [Description (optional)]
For example:
10.10.10.18 255.255.255.255 1 127.0.0.1 nei1/ 1 description
If there are multiple daemons:
10.10.10.18 255.255.255.255 1 127.0.0.1 nei1/nei2/ 1 description
List of available daemons
channel1/ HW5700_v6/ lx_v4_ads/

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 6-33, 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 6-33, 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.

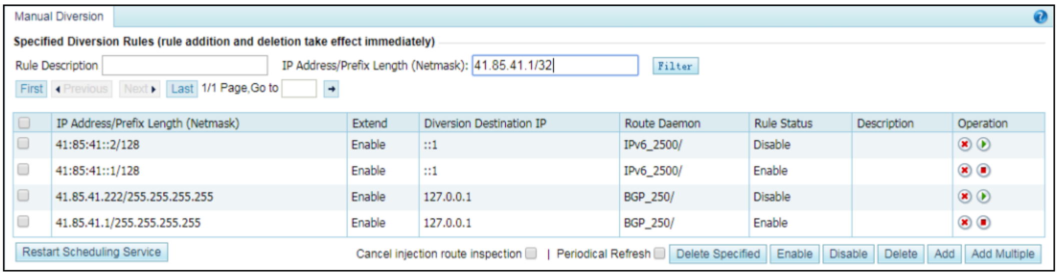
Disabling Manual Diversion Rules

- Method 1: On the manual diversion rule list shown in Figure 6-33, 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 6-33, 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 6-33, 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 6-36.

Figure 6-36 Filtering manual diversion rules



Manual Diversion

Specified Diversion Rules (rule addition and deletion take effect immediately)

Rule Description:

IP Address/Prefix Length (Netmask): 41.85.41.1/32

□	IP Address/Prefix Length (Netmask)	Extend	Diversion Destination IP	Route Daemon	Rule Status	Description	Operation
□	41:85:41::2/128	Enable	::1	IPv6_2500/	Disable		✖ ▶
□	41:85:41::1/128	Enable	::1	IPv6_2500/	Enable		✖ ■
□	41.85.41.222/255.255.255.255	Enable	127.0.0.1	BGP_250/	Disable		✖ ▶
□	41.85.41.1/255.255.255.255	Enable	127.0.0.1	BGP_250/	Enable		✖ ■

Cancel injection route inspection □ | Periodical Refresh □

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 6-33, 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 6-33, 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.

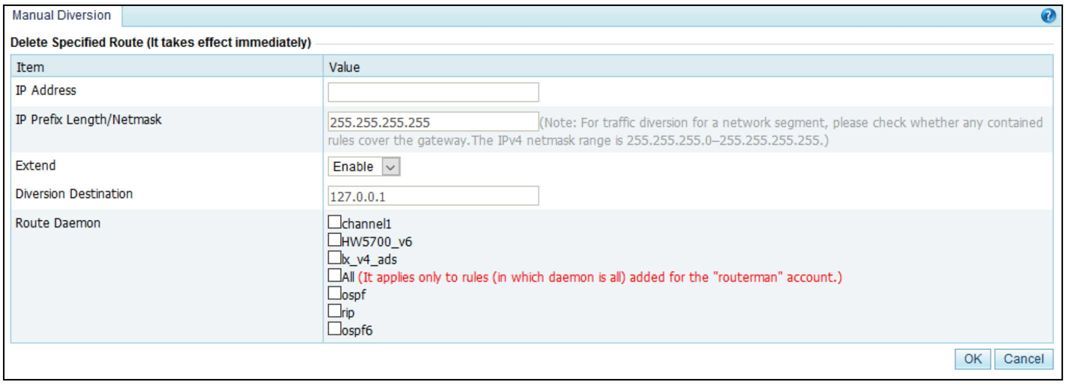
6.4.2.6 Deleting a Specified Route

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 6-33, click **Delete Specified** to open the diversion rule deletion page.

See Table 6-14 for descriptions of parameters in the **Delete Specified Route** dialog box.

Figure 6-37 Deleting a specified diversion rule



Manual Diversion

Delete Specified Route (It takes effect immediately)

Item	Value
IP Address	
IP Prefix Length/Netmask	255.255.255.255 (Note: For traffic diversion for a network segment, please check whether any contained rules cover the gateway.The IPv4 netmask range is 255.255.255.0–255.255.255.255.)
Extend	Enable
Diversion Destination	127.0.0.1
Route Daemon	□channel1 □HW5700_v6 □lx_v4_ads □All (It applies only to rules (in which daemon is all) added for the "routerman" account.) □ospf □rip □ospf6

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 6-33, 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 6-33, you can select the **Cancel injection route inspection** check box to disable injection route inspection, or clear the check box 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 6-33, 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

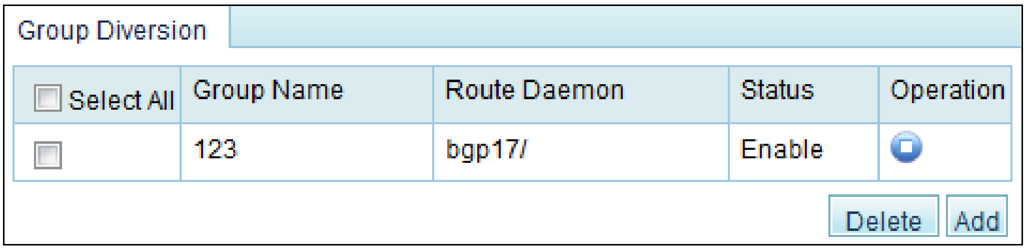
Group diversion rules are used to divert the traffic destined for a protection group to the diversion interface on the ADS device. This section describes how to add, delete, enable, and disable group diversion rules.

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 6-38 Group diversion rules

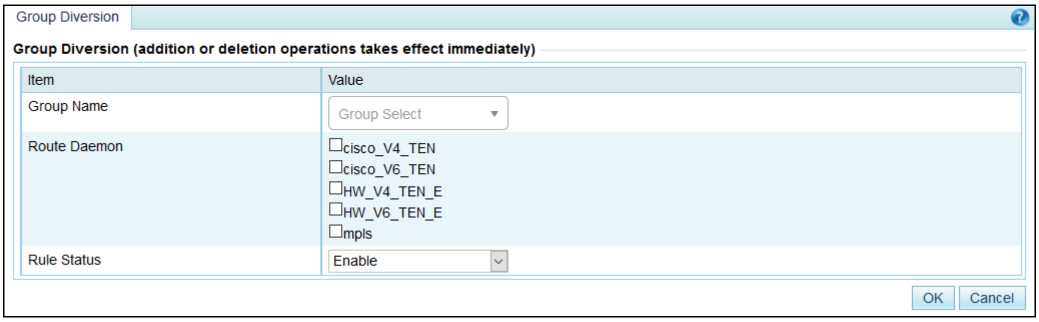


Group Diversion

□ Select All	Group Name	Route Daemon	Status	Operation
□	123	bgp17/	Enable	●

Step 2 Click **Add**.

Figure 6-39 Creating a group diversion rule



Group Diversion

Group Diversion (addition or deletion operations takes effect immediately)

Item	Value
Group Name	Group Select ▾
Route Daemon	□cisco_V4_TEN □cisco_V6_TEN □HW_V4_TEN_E □HW_V6_TEN_E □mpls
Rule Status	Enable

Table 6-15 describes parameters for creating a group diversion rule.

Table 6-15 Parameters for creating a group diversion rule

Parameter	Description
Group Name	Protection group whose traffic is to be diverted. Fuzzy search is supported.
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 6-38, 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 6-38, click ▶ in the **Operation** column of a group diversion rule to enable it.

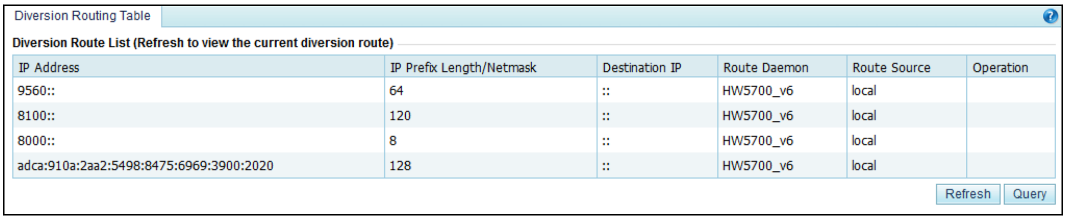
- To disable a group diversion rule, perform the following steps:

  On the group diversion rule list shown in Figure 6-38, click ■ in the **Operation** column of a group diversion rule to disable it.

6.4.4 Diversion Routing Table

As shown in Figure 6-40, 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's anti-DDoS detection devices. Click **Refresh** to view the latest diversion routes of the system.

Figure 6-40 Diversion routing table



Diversion Route List (Refresh to view the current diversion route)

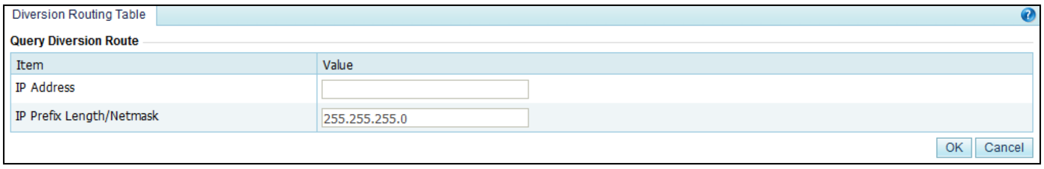
IP Address	IP Prefix Length/Netmask	Destination IP	Route Daemon	Route Source	Operation
9560::	64	::	HW5700_v6	local	
8100::	120	::	HW5700_v6	local	
8000::	8	::	HW5700_v6	local	
adca:910a:2aa2:5498:8475:6969:3900:2020	128	::	HW5700_v6	local	

Searching for a Diversion Route

Step 1 On the page shown in Figure 6-40, click **Query** to the lower right of the diversion routing table.

The **Query Diversion Route** page appears, as shown in Figure 6-41.

Figure 6-41 Searching for diversion routes



Query Diversion Route

Item	Value
IP Address	
IP Prefix Length/Netmask	255.255.255.0

Table 6-16 describes parameters of a diversion route.

Table 6-16 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

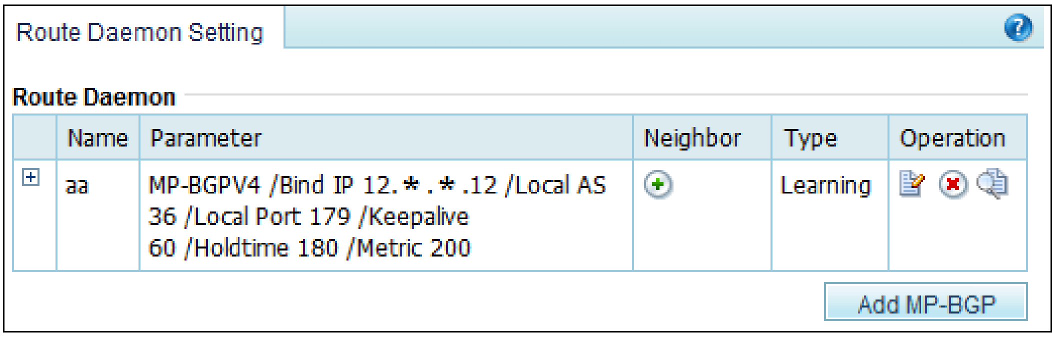
This section covers the following topics:

- MPLS Route
- Other Routes

6.5.1 MPLS Route

On the page shown in Figure 6-42, you can configure MPLS routes to accomplish layer 2 label learning between VPNs.

Figure 6-42 List of MPLS routes



Route Daemon Setting

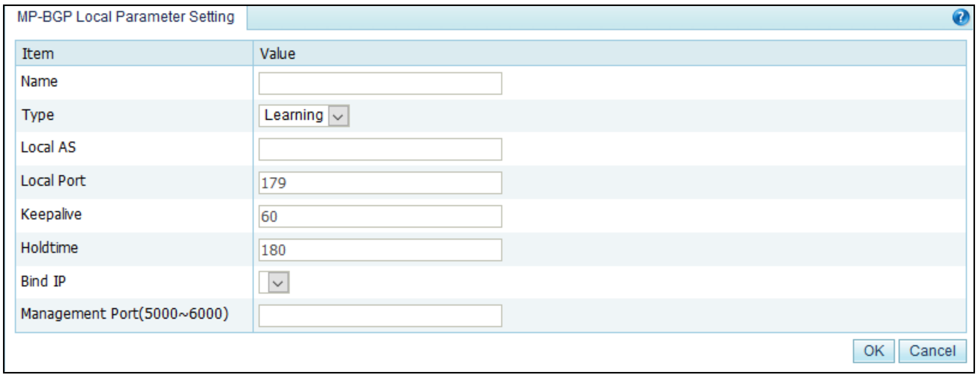
Route Daemon

	Name	Parameter	Neighbor	Type	Operation
⊞	aa	MP-BGPV4 /Bind IP 12.*.*.12 /Local AS 36 /Local Port 179 /Keepalive 60 /Holdtime 180 /Metric 200	⊕	Learning	

Creating an MPLS Route

On the page shown in Figure 6-42, 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 6-43 Creating an MPLS route



MP-BGP Local Parameter Setting

Item	Value
Name	
Type	Learning
Local AS	
Local Port	179
Keepalive	60
Holdtime	180
Bind IP	
Management Port(5000~6000)	

Table 6-17 describes parameters for creating an MPLS route.

Table 6-17 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.
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** are directly taken from the BGPv4 protocol.

Editing a Route

In the list of MPLS routes shown in Figure 6-42, click ✎ in the **Operation** column of a route to edit this route.

Deleting a Route

In the list of MPLS routes shown in Figure 6-42, click ✖ in the **Operation** column of a route to delete this route.

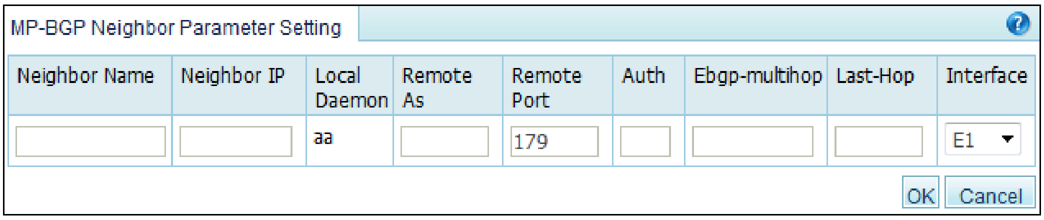
Viewing Route Status

In the list of MPLS routes shown in Figure 6-42, click 🔍 in the **Operation** column of a route to view the status of this route.

Adding a Neighbor

In the list of local routes shown in Figure 6-42, click ⊕ in the **Neighbor** column of a route to add a neighbor for this route. See Figure 6-44.

Figure 6-44 Adding a neighbor for MPLS route



MP-BGP Neighbor Parameter Setting

Neighbor Name	Neighbor IP	Local Daemon	Remote As	Remote Port	Auth	Ebgp-multihop	Last-Hop	Interface
		aa		179				E1

Note

After adding a neighbor, click ▶ to check whether the neighbor is connected.

Viewing the Neighbor Status

In the list of local routes, click 🔍 in the **Operation** column of a route to view the connection status of its 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

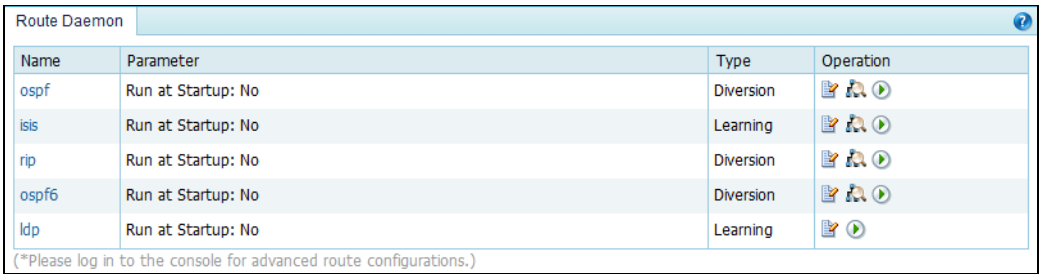
In addition to routing protocols described above, ADS supports such advanced routing protocols as OSPF, ISIS, RIP, OSPF6, LDP, and RIPng.

Currently, the web administrator, **admin**, can configure LDP routes or view, enable, or disable OSPF, ISIS, RIP, OSPF6, LDP, and RIPng routes on the web-based manager, while the CLI administrator, **routerman**, can configure OSPF, ISIS, RIP, RIPng, 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 6-45 List of other routes



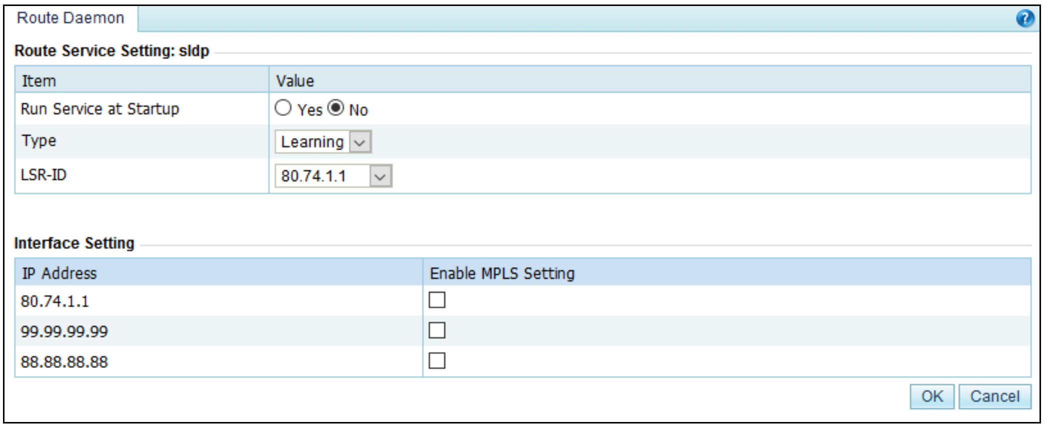
Route Daemon

Name	Parameter	Type	Operation
ospf	Run at Startup: No	Diversion	✎ 🔍 ▶
isis	Run at Startup: No	Learning	✎ 🔍 ▶
rip	Run at Startup: No	Diversion	✎ 🔍 ▶
ospf6	Run at Startup: No	Diversion	✎ 🔍 ▶
ldp	Run at Startup: No	Learning	✎ ▶

(*Please log in to the console for advanced route configurations.)

Step 2 Click ✎ in the **Operation** column to edit LDP route parameters.

Figure 6-46 Editing LDP route parameters



Route Service Setting: sldp

Item	Value
Run Service at Startup	○ Yes ● No
Type	Learning
LSR-ID	80.74.1.1

Interface Setting

IP Address	Enable MPLS Setting
80.74.1.1	□
99.99.99.99	□
88.88.88.88	□

Table 6-18 describes LDP route parameters.

Table 6-18 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.

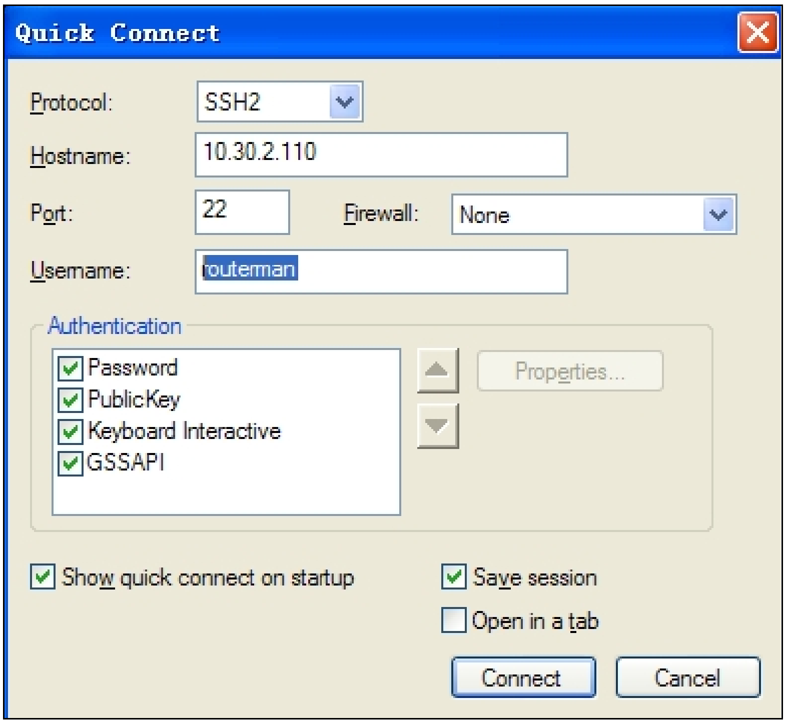
----End

Configuring OSPF, ISIS, RIP, RIPng, 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 6-47 ADS login in SSH mode



Quick Connect

Protocol: SSH2

Hostname: 10.30.2.110

Port: 22 Firewall: None

Username: routerman

Authentication

☑ Password
☑ PublicKey
☑ Keyboard Interactive
☑ GSSAPI

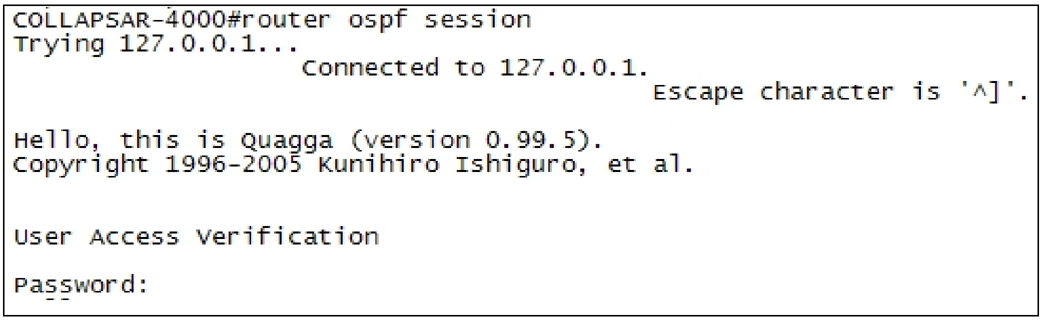
☑ Show quick connect on startup

☑ Save session

□ Open in a tab

Step 2 Enable OSPF on the interface via the CLI.

Figure 6-48 Editing OSPF route parameters



```
COLLAPSAR-4000#router ospf session
Trying 127.0.0.1...
                     Connected to 127.0.0.1.
                                              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 routing protocol list shown in Figure 6-45.

Enabling/Disabling the Routing 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 routing protocol list shown in Figure 6-45.

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 alert level 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 alert level is set to **Manual**, it notifies ADS, which, in turn, notifies the O&M personnel, who will then decide whether to divert the traffic.

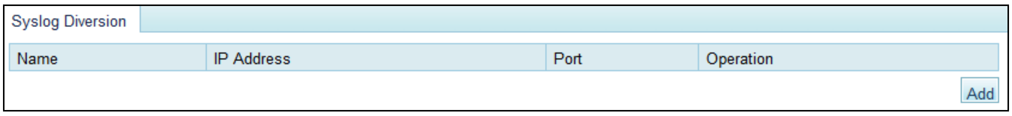
Note	For Genie and Arbor devices, the diversion type can be either **Auto** or **Manual**. For Samurai and Kuanguang devices, the diversion type can only be **Auto**.

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 6-49 Syslog-based diversion rule list

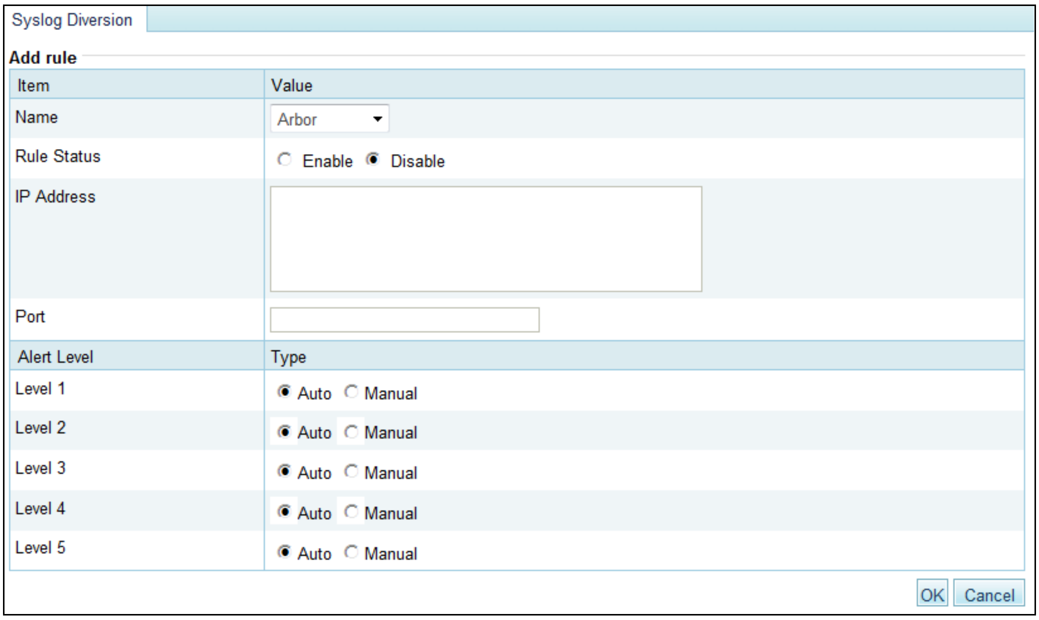


Syslog Diversion

Name	IP Address	Port	Operation

Step 2 Click **Add**.

Figure 6-50 Creating a diversion rule



Syslog Diversion

Add rule

Item	Value
Name	Arbor
Rule Status	○ Enable ● Disable
IP Address	
Port	
Alert Level	**Type**
Level 1	● Auto ○ Manual
Level 2	● Auto ○ Manual
Level 3	● Auto ○ Manual
Level 4	● Auto ○ Manual
Level 5	● Auto ○ Manual

Table 6-19 describes parameters for creating a syslog-based diversion rule.

Table 6-19 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**.
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.

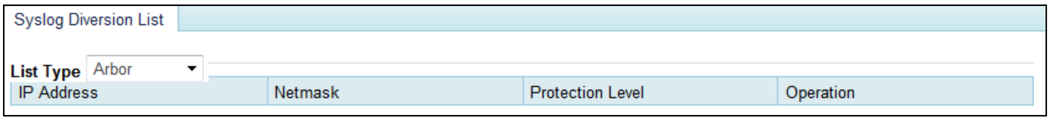
----End

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 6-51 Syslog diversion list



Syslog Diversion List

List Type: Arbor

IP Address	Netmask	Protection Level	Operation

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.
Protection Logs	Describes how to view attack logs from the perspective of protection policies.

7.1 Attack Logs

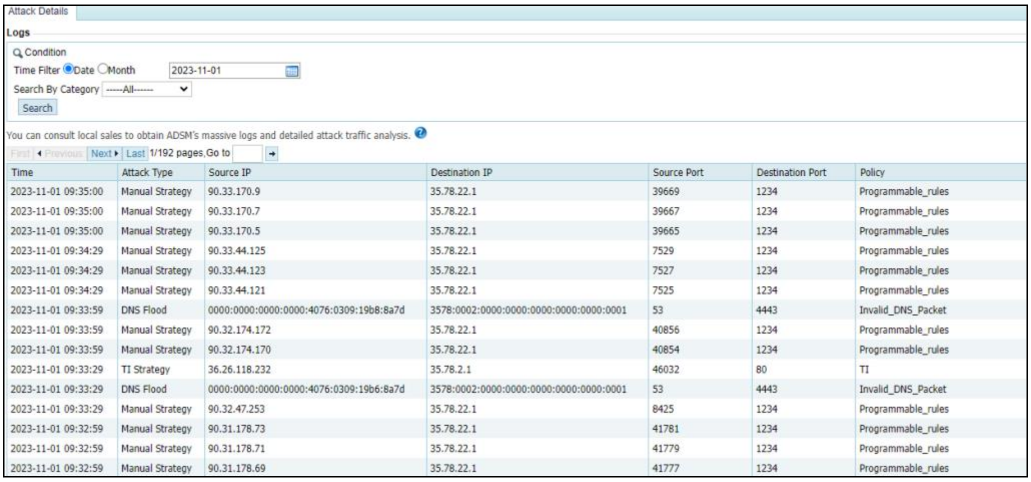
All attack logs are displayed in two ways for easier viewing: statistical graph and data table.

7.1.1 Attack Details

You can view attack logs of the last 15 days. By default, attack logs of the current day are listed, as shown in Figure 7-1.

You can select a 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 policy. If you select **All** from this drop-down box, all logs are searched.

Figure 7-1 Attack logs



Logs

Condition

Time Filter ● Date ○ Month 2023-11-01

Search By Category -----All------

You can consult local sales to obtain ADSM's massive logs and detailed attack traffic analysis.

1/192 pages,Go to

Time	Attack Type	Source IP	Destination IP	Source Port	Destination Port	Policy
2023-11-01 09:35:00	Manual Strategy	90.33.170.9	35.78.22.1	39669	1234	Programmable_rules
2023-11-01 09:35:00	Manual Strategy	90.33.170.7	35.78.22.1	39667	1234	Programmable_rules
2023-11-01 09:35:00	Manual Strategy	90.33.170.5	35.78.22.1	39665	1234	Programmable_rules
2023-11-01 09:34:29	Manual Strategy	90.33.44.125	35.78.22.1	7529	1234	Programmable_rules
2023-11-01 09:34:29	Manual Strategy	90.33.44.123	35.78.22.1	7527	1234	Programmable_rules
2023-11-01 09:34:29	Manual Strategy	90.33.44.121	35.78.22.1	7525	1234	Programmable_rules
2023-11-01 09:33:59	DNS Flood	0000:0000:0000:0000:4076:0309:19b8:8a7d	3578:0002:0000:0000:0000:0000:0000:0001	53	4443	Invalid_DNS_Packet
2023-11-01 09:33:59	Manual Strategy	90.32.174.172	35.78.22.1	40856	1234	Programmable_rules
2023-11-01 09:33:59	Manual Strategy	90.32.174.170	35.78.22.1	40854	1234	Programmable_rules
2023-11-01 09:33:29	TI Strategy	36.26.118.232	35.78.2.1	46032	80	TI
2023-11-01 09:33:29	DNS Flood	0000:0000:0000:0000:4076:0309:19b6:8a7d	3578:0002:0000:0000:0000:0000:0000:0001	53	4443	Invalid_DNS_Packet
2023-11-01 09:33:29	Manual Strategy	90.32.47.253	35.78.22.1	8425	1234	Programmable_rules
2023-11-01 09:32:59	Manual Strategy	90.31.178.73	35.78.22.1	41781	1234	Programmable_rules
2023-11-01 09:32:59	Manual Strategy	90.31.178.71	35.78.22.1	41779	1234	Programmable_rules
2023-11-01 09:32:59	Manual Strategy	90.31.178.69	35.78.22.1	41777	1234	Programmable_rules

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. Note **Source IP** is displayed as the real source IP address in the following logs: • Attack message logged for ADS's dropping packets according to the HTTP proxy protection policy. • Attack message logged for rate limiting against real source IP addresses according to an HTTP GET packet filtering rule in the Botnet & IP behavior control policy configured for a group.
Destination IP/Port	Destination IP address and port of the attack.
Policies	Protection policy triggered for the attack. For details about protection policies, you can click ? in the upper-right corner of the page and choose **Logs** > **Attack Logs** > **Attack Details** to view the description.

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

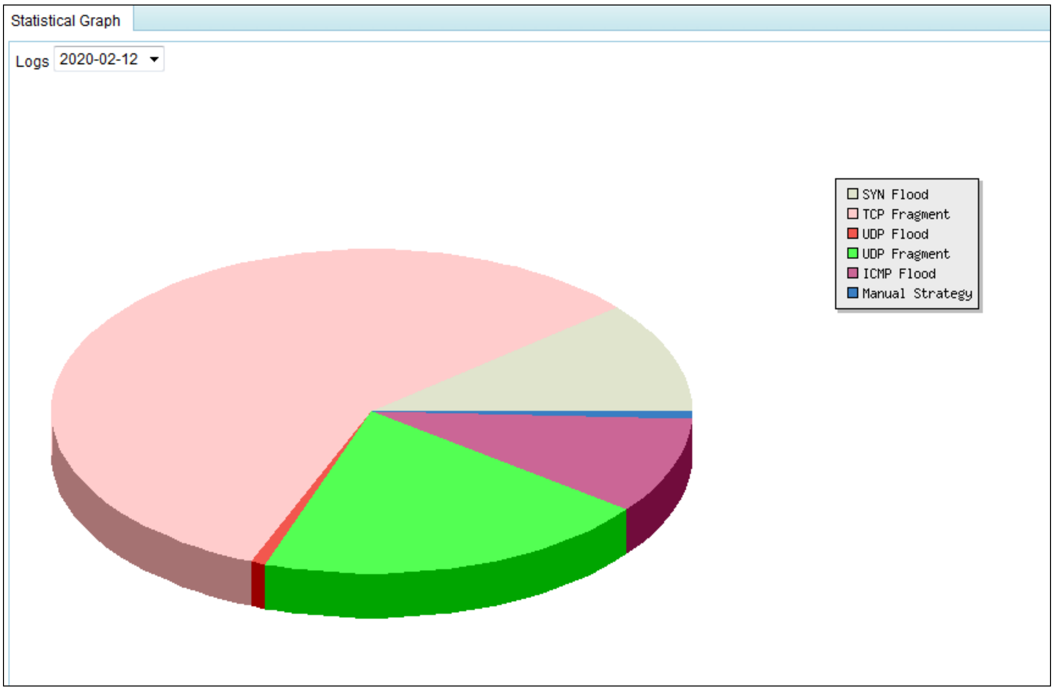
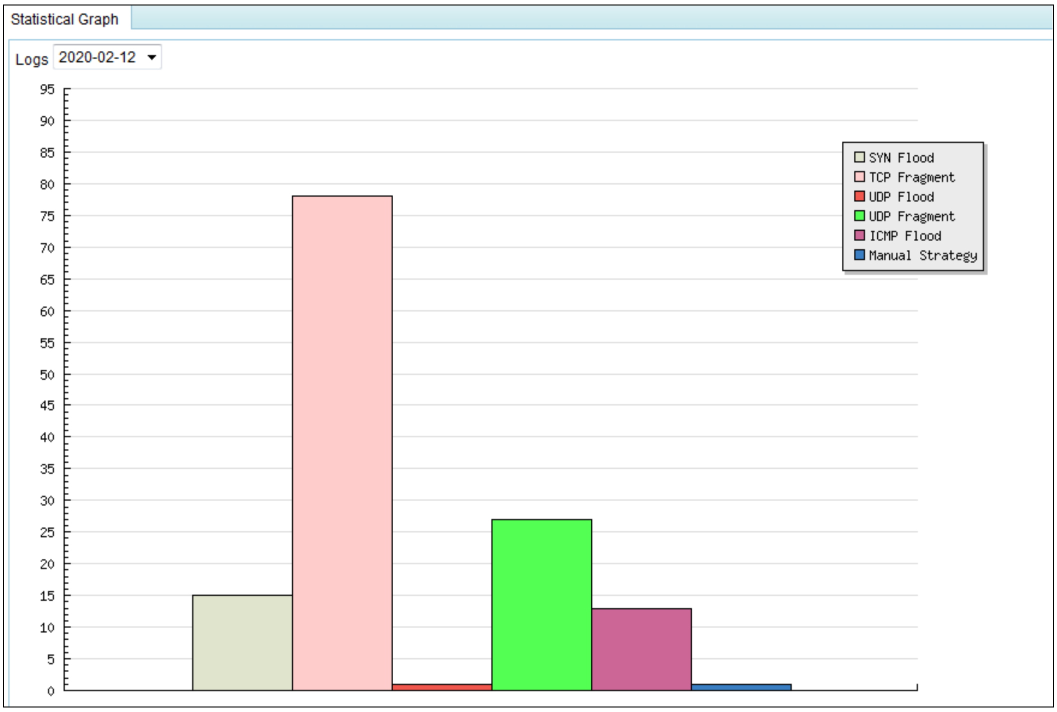


Figure 7-3 Number of attacks of each type



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
- Web API Logs
- Authentication Configuration Logs

7.2.1 System Operation Logs

The system operation log table displays main operations of users in the system as well as NTP synchronization information.

You can filter system operation logs by time, IP address, and account.

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.

Parameter	Description
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 click **Download** to download operation logs to a local disk drive in text format.

7.2.2 System Login Logs

The system login log table displays system login details.

You can filter system login logs by time, login IP address, and operation result.

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
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 click **Download** to download login logs to a local disk drive in text format.

7.2.3 Link Status Logs

The link status log table displays the interface connection status (UP to DOWN or DOWN to UP) of ADS.

You can filter link status logs by time.

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 click **Download** to download link status logs to a local disk drive in text format.

7.2.4 Traffic Diversion Logs

The traffic diversion log table displays the route operations performed by ADS upon receiving alerts from NSFOCUS's anti-DDoS detection devices, as well as manual diversion routing operations performed on the web-based manager. Logs can be retained for 10 days at most.

You can filter traffic diversion logs by time, IP address, and account.

Note

Traffic diversion logs can be viewed only in diversion modes.

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 click **Download** to download traffic diversion logs to a local disk drive in text format.

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.

You can filter HA synchronization logs by time.

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. • **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 click **Download** to download HA synchronization logs to a local disk drive in text format.

7.2.6 Syslog Diversion Logs

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.

7.2.7 Web API Logs

The web API log table displays logs generated by third-party management platforms calling ADS's web APIs.

Table 7-7 describes parameters of web API logs.

Table 7-7 Parameters of web API logs

Parameter	Description
Time	Time when the web API is called.
Account	Account name used to log in to the third-party platform that calls the web API.
IP Address	Source IP address that calls the web API.
Operation	Module that is invovled in the current operation.

Parameter	Description
Description	Specific operation performed.

To the upper right of the log table, you can click **Download** to download web API logs to a local disk drive in text format.

7.2.8 Authentication Configuration Logs

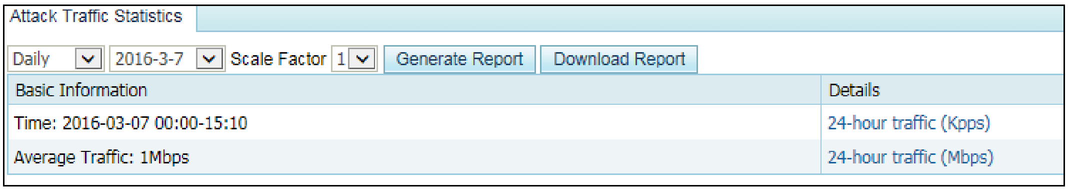
The **Authentication Configuration Log** page is available only when vADS is used. For details about authorization configuration, see *section 3.4.1 License*.

The authentication configuration log list displays the authentication time and status of vADS.

7.3 Log Analysis

As shown in Figure 7-4, 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 7-4 Attack traffic statistics



Attack Traffic Statistics

Daily 2016-3-7 Scale Factor 1

Basic Information	Details
Time: 2016-03-07 00:00-15:10	24-hour traffic (Kpps)
Average Traffic: 1Mbps	24-hour traffic (Mbps)

Daily Attack Traffic Report

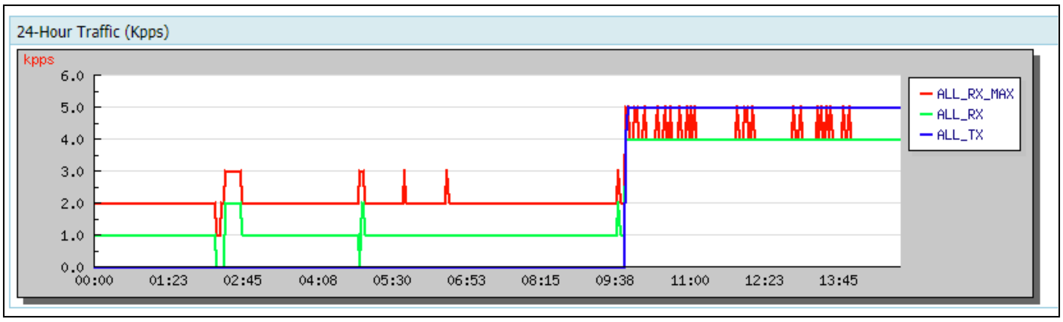
The **Basic Information** column includes statistical time, average incoming traffic, average normal incoming traffic, and average outgoing traffic (unit:Mbps) about attacks on a specific day.

The **Details** column contains the following information:

- 24-hour traffic (in kpps)

  As shown in Figure 7-5, incoming/outgoing traffic (unit: kpps) of a specific day is displayed.

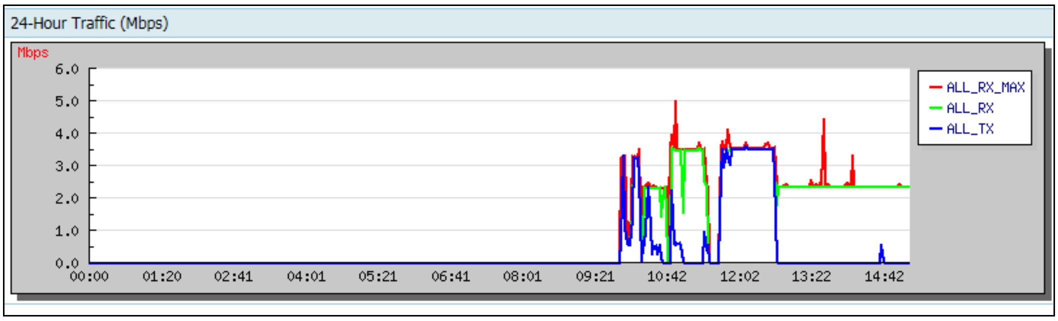
Figure 7-5 24-hour traffic (in kpps)



- 24-hour traffic (in Mbps)

  As shown in Figure 7-6, incoming/outgoing traffic (unit:Mbps) of a specific day is displayed.

Figure 7-6 24-hour traffic (in Mbps)

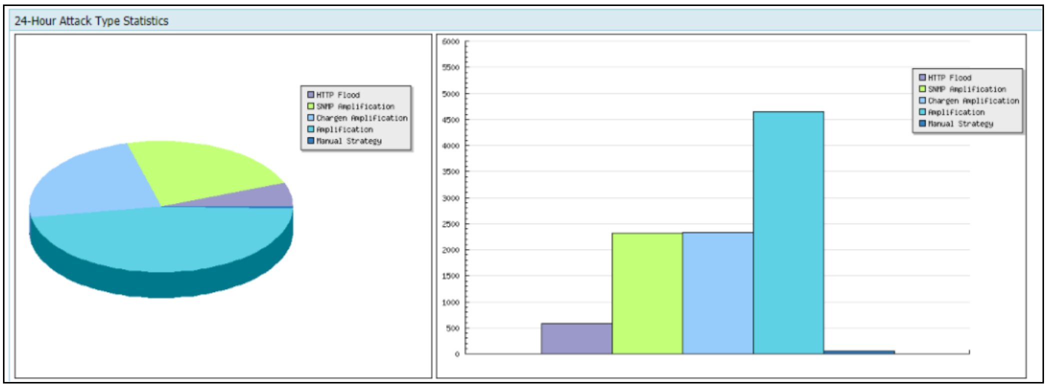


- 24-hour attack type statistics

  As shown in Figure 7-7, 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

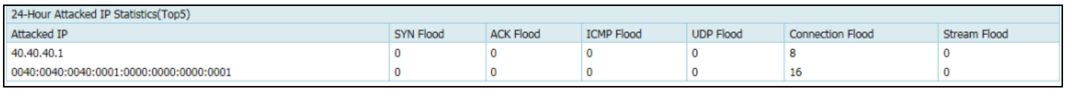
Figure 7-7 24-hour attack type statistics



- 24-hour attacked IP statistics

  As shown in Figure 7-8, attacked IP addresses and attack traffic on a specific day are displayed in the list.

Figure 7-8 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.

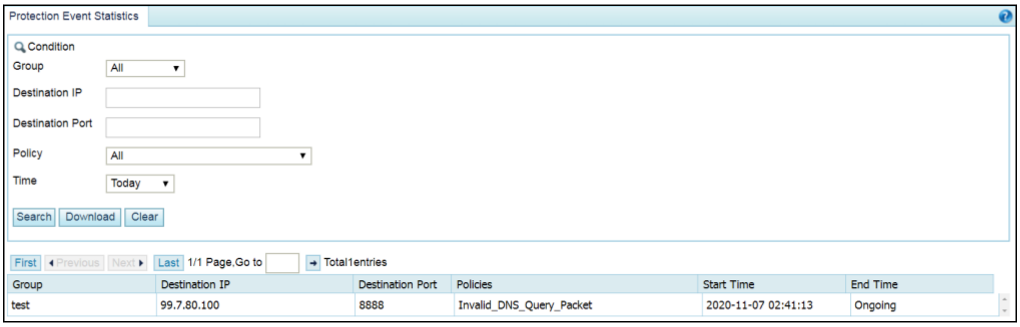
7.4 Protection Logs

To make it easier for users to view the information about attack logs, ADS provides the function of protection event statistics. Users can view the details about attack logs from the perspective of protection policies and adjust protection policies accordingly.

Choose **Logs** > **Protection Logs** > **Protection Event Statistics** to view an attack log by specifying the protection group, destination IP, destination port, policy, and time.

- If the attacked destination IP does not belong to any of the custom protection groups, the value of **Group** is displayed as **default_protection_group**.
- If the attack remains inactive for 5 minutes, the attack is deemed to end. Otherwise, the attack is always "ongoing".

Figure 7-9 Protection event statistics



Protection Event Statistics

Condition

Group	All
Destination IP	
Destination Port	
Policy	All
Time	Today

1/1 Page,Go to Total1entries

Group	Destination IP	Destination Port	Policies	Start Time	End Time
test	99.7.80.100	8888	Invalid_DNS_Query_Packet	2020-11-07 02:41:13	Ongoing

Click **Download** above the log list to download the presented logs to a local disk drive, allowing you to check and process the logs.

Click **Clear** above the log list and click **OK** in the dialog box that appears to delete all logs for protection events that are completed.

8 Advanced Applications

This chapter dwells upon four 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.
Cloud Signaling	Describes how to configure collaboration between ADS and the cloud cleaning center.
Collaboration with NTI	Describes how to configure collaboration between ADS and NTI as well as NTI upgrade and IP exceptions.
Carpet Bombing Protection	Describes how to configure a carpet bombing protection policy.

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

- 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

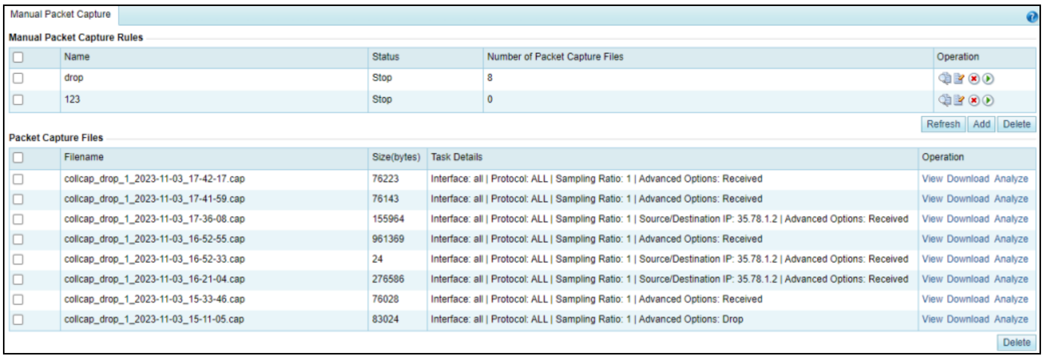
To configure a manual packet capture task, perform the following steps:

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 in the **Status** column. 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. Packet capture parameters are displayed in the **Task Details** column.

Figure 8-1 Manual Packet Capture page



Manual Packet Capture Rules

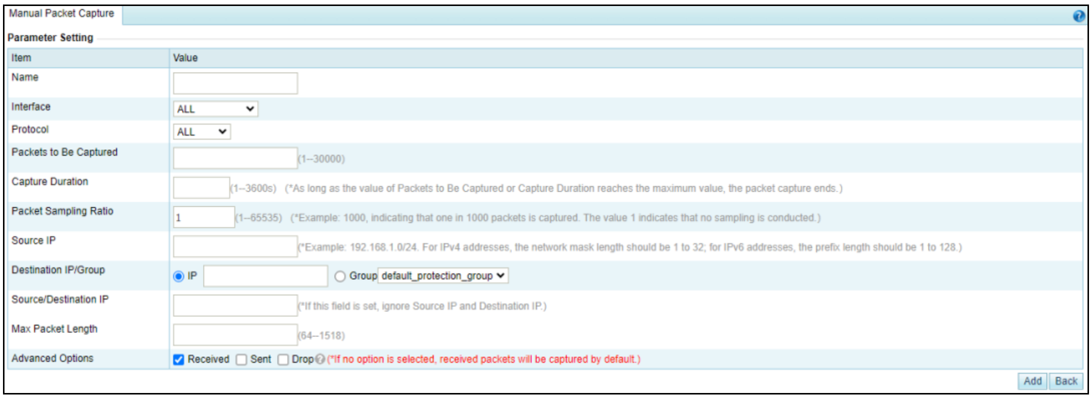
□	Name	Status	Number of Packet Capture Files	Operation
□	drop	Stop	8	
□	123	Stop	0	

Packet Capture Files

□	Filename	Size(bytes)	Task Details	Operation
□	collcap_drop_1_2023-11-03_17-42-17.cap	76223	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Advanced Options: Received	View Download Analyze
□	collcap_drop_1_2023-11-03_17-41-59.cap	76143	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Advanced Options: Received	View Download Analyze
□	collcap_drop_1_2023-11-03_17-36-08.cap	155964	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Source/Destination IP: 35.78.1.2 | Advanced Options: Received	View Download Analyze
□	collcap_drop_1_2023-11-03_16-52-55.cap	961369	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Advanced Options: Received	View Download Analyze
□	collcap_drop_1_2023-11-03_16-52-33.cap	24	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Source/Destination IP: 35.78.1.2 | Advanced Options: Received	View Download Analyze
□	collcap_drop_1_2023-11-03_16-21-04.cap	276586	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Source/Destination IP: 35.78.1.2 | Advanced Options: Received	View Download Analyze
□	collcap_drop_1_2023-11-03_15-33-46.cap	76028	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Advanced Options: Received	View Download Analyze
□	collcap_drop_1_2023-11-03_15-11-05.cap	83024	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Advanced Options: Drop	View Download Analyze

Step 2 Click **Add** to create a manual packet capture task.

Figure 8-2 Creating a manual packet capture task



Parameter Setting

Item	Value
Name	
Interface	ALL
Protocol	ALL
Packets to Be Captured	(1--30000)
Capture Duration	(1--3600s) (*As long as the value of Packets to Be Captured or Capture Duration reaches the maximum value, the packet capture ends.)
Packet Sampling Ratio	1 (1--65535) (*Example: 1000, indicating that one in 1000 packets is captured. The value 1 indicates that no sampling is conducted.)
Source IP	(*Example: 192.168.1.0/24. For IPv4 addresses, the network mask length should be 1 to 32; for IPv6 addresses, the prefix length should be 1 to 128.)
Destination IP/Group	● IP ○ Group default_protection_group
Source/Destination IP	(*If this field is set, ignore Source IP and Destination IP.)
Max Packet Length	(64--1518)
Advanced Options	☑ Received □ Sent □ Drop (*If no option is selected, received packets will be captured by default.)

Step 3 Configure parameters.

Table 8-1 describes parameters for creating a manual packet capture task.

Table 8-1 Parameters for creating a manual packet capture task

Parameter	Description
Name	The name is unique and should be a string of 1 to 15 characters, including letters, digits, and underscores (_).
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 be in the range of 0–255.
Packets to Be Captured	Number of packets to be captured. The value ranges from 1 to 30000.

Parameter	Description
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.
Packet Sampling Ratio	Specifies the ratio of matched packets to captured packets. Value range: 1–65535. For example, the value **1000** indicates that one in 1000 packets are captured. The default value is **1**, indicating no packet sampling. When the traffic bursts, the packet sampling ratio allows the device to capture packets in a longer period.
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.
Destination IP/Group	Destination IP address or group of this task. You can select **IP** or **Group**. • **IP**: When this is selected, you can further specify an IP address in the input box next to it. Leaving the box empty indicates no restriction on the destination of packets. Both IPv4 and IPv6 are supported. • **Group**: When this is selected, you need to select a protection group from the drop-down list.
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. Note This parameter is available only when **Protocol** is set to **UDP** or **TCP**.
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. Note This parameter is available only when **Protocol** is set to **UDP** or **TCP**.
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**.

Parameter	Description
	Note This parameter is available only when **Protocol** is set to **UDP** or **TCP**.
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. **Note** • If none is selected, received packets will be captured by default. • If **Drop** is selected and when the group to which the destination IP address belongs is in alert mode, this packet actually is not dropped.

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.

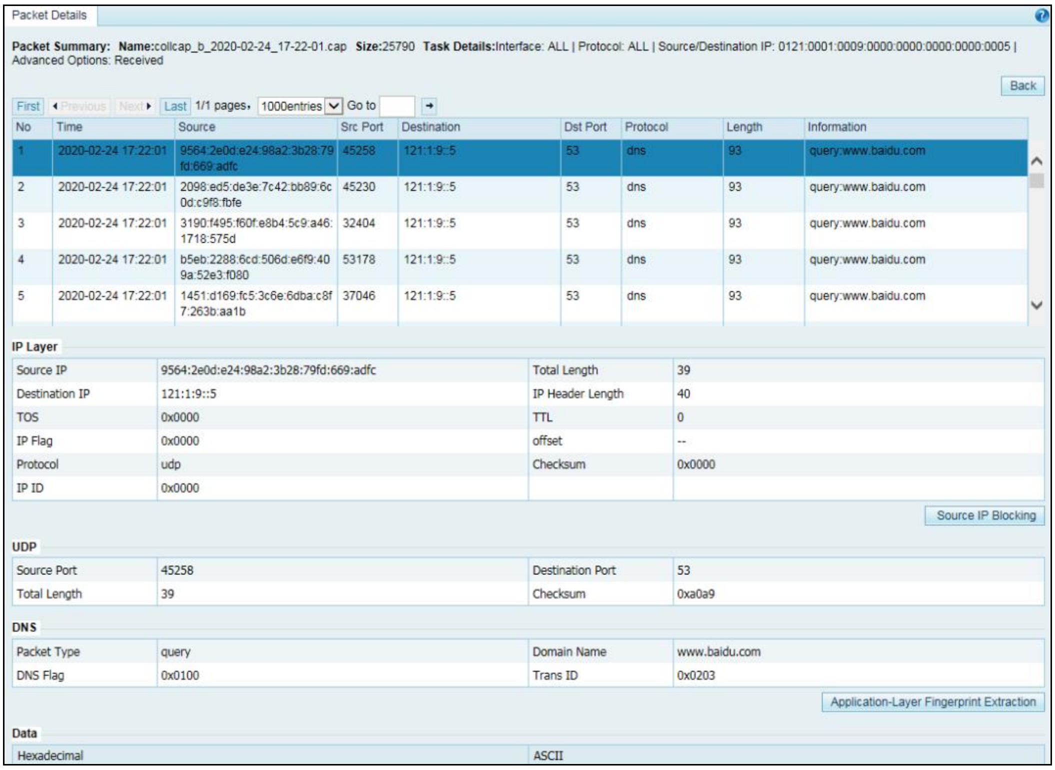
Note	Ongoing packet capture tasks cannot be deleted.

8.1.1.7 Viewing 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 **View** in the **Operation** column of a packet capture file to view its details.

Figure 8-3 Viewing details of a packet capture file



Packet Summary: **Name:**collcap_b_2020-02-24_17-22-01.cap **Size:**25790 **Task Details:**Interface: ALL | Protocol: ALL | Source/Destination IP: 0121:0001:0009:0000:0000:0000:0000:0005 | Advanced Options: Received

No	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Information
1	2020-02-24 17:22:01	9564:2e0d:e24:98a2:3b28:79fd:669:adfc	45258	121:1:9::5	53	dns	93	query:www.baidu.com
2	2020-02-24 17:22:01	2098:ed5:de3e:7c42:bb89:6c0d:c9f8:fbfe	45230	121:1:9::5	53	dns	93	query:www.baidu.com
3	2020-02-24 17:22:01	3190:f495:f60f:e8b4:5c9:a46:1718:575d	32404	121:1:9::5	53	dns	93	query:www.baidu.com
4	2020-02-24 17:22:01	b5eb:2288:6cd:506d:e6f9:409a:52e3:f080	53178	121:1:9::5	53	dns	93	query:www.baidu.com
5	2020-02-24 17:22:01	1451:d169:fc5:3c6e:6dba:c8f7:263b:aa1b	37046	121:1:9::5	53	dns	93	query:www.baidu.com

IP Layer

Source IP	9564:2e0d:e24:98a2:3b28:79fd:669:adfc	Total Length	39
Destination IP	121:1:9::5	IP Header Length	40
TOS	0x0000	TTL	0
IP Flag	0x0000	offset	--
Protocol	udp	Checksum	0x0000
IP ID	0x0000		

UDP

Source Port	45258	Destination Port	53
Total Length	39	Checksum	0xa0a9

DNS

Packet Type	query	Domain Name	www.baidu.com
DNS Flag	0x0100	Trans ID	0x0203

Data

Hexadecimal	ASCII

Viewing the Summary of the Packet Capture File

As shown in Figure 8-3, in the upper part of the page, **Packet Summary** displays the abstract of the packet capture file, including the file name, size, and task details.

Viewing the Packet Abstract

On the **Packet Details** page, abstract information of all captured packets contained in the packet capture file is displayed. Table 8-2 describes parameters of a packet capture file.

Table 8-2 Parameters of a packet capture file

Parameter	Description
No	Sequence number of the packet in the packet capture file
Time	System time when the packet was captured
Source	Source IP address of the packet
Src Port	Source port of the packet
Destination	Destination IP address of the packet
Dst Port	Destination port of the packet
Protocol	Protocol used by the packet, such as ICMP
Length	Packet length

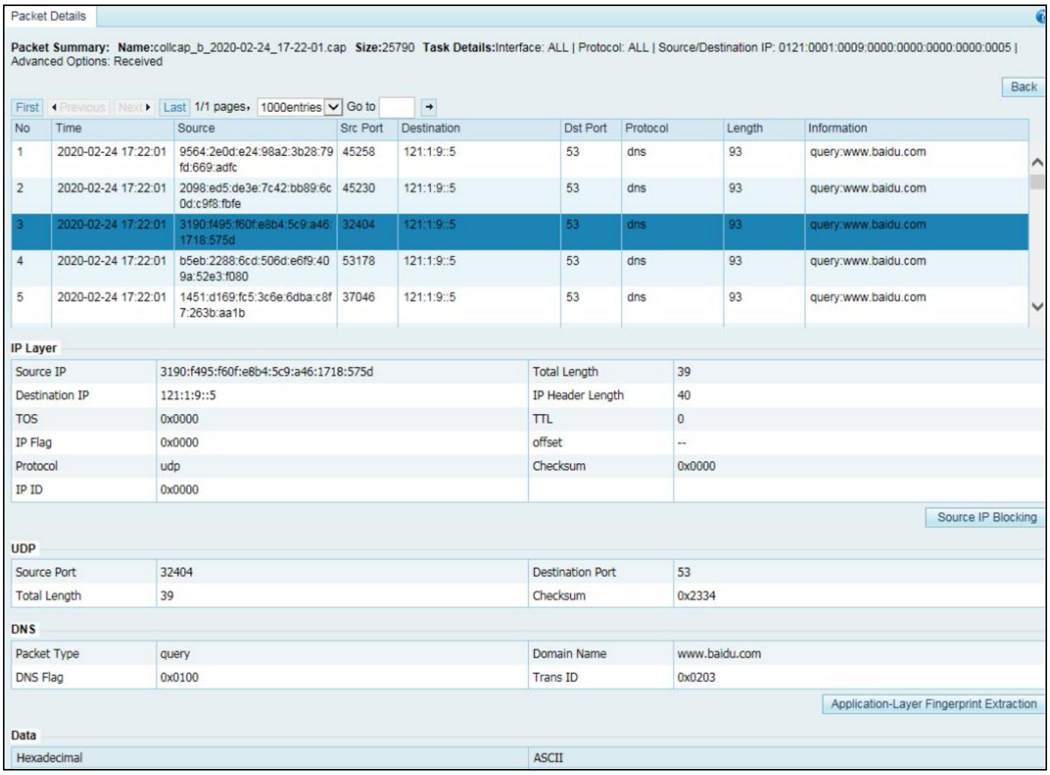
Parameter	Description
Information	Packet information

Viewing Details About a Captured Packet

On the page shown in Figure 8-3, details about the first packet are displayed by default.

You can click a packet to view its details. The displayed information varies with packets. See Figure 8-4.

Figure 8-4 Viewing details about a captured packet



Packet Summary: **Name:**collcap_b_2020-02-24_17-22-01.cap **Size:**25790 **Task Details:**Interface: ALL | Protocol: ALL | Source/Destination IP: 0121:0001:0009:0000:0000:0000:0000:0005 | Advanced Options: Received

No	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Information
1	2020-02-24 17:22:01	9564:2e0d:e24:98a2:3b28:79fd:669:adfc	45258	121:1:9::5	53	dns	93	query:www.baidu.com
2	2020-02-24 17:22:01	2098:ed5:de3e:7c42:bb89:6c0d:c9f8:fbfe	45230	121:1:9::5	53	dns	93	query:www.baidu.com
3	2020-02-24 17:22:01	3190:f495:f60f:e8b4:5c9:a46:1718:575d	32404	121:1:9::5	53	dns	93	query:www.baidu.com
4	2020-02-24 17:22:01	b5eb:2288:6cd:506d:e6f9:409a:52e3:f080	53178	121:1:9::5	53	dns	93	query:www.baidu.com
5	2020-02-24 17:22:01	1451:d169:fc5:3c6e:6dba:c8f7:263b:aa1b	37046	121:1:9::5	53	dns	93	query:www.baidu.com

IP Layer

Source IP	3190:f495:f60f:e8b4:5c9:a46:1718:575d	Total Length	39
Destination IP	121:1:9::5	IP Header Length	40
TOS	0x0000	TTL	0
IP Flag	0x0000	offset	--
Protocol	udp	Checksum	0x0000
IP ID	0x0000		

UDP

Source Port	32404	Destination Port	53
Total Length	39	Checksum	0x2334

DNS

Packet Type	query	Domain Name	www.baidu.com
DNS Flag	0x0100	Trans ID	0x0203

Data

Hexadecimal	ASCII

Source IP Blocking

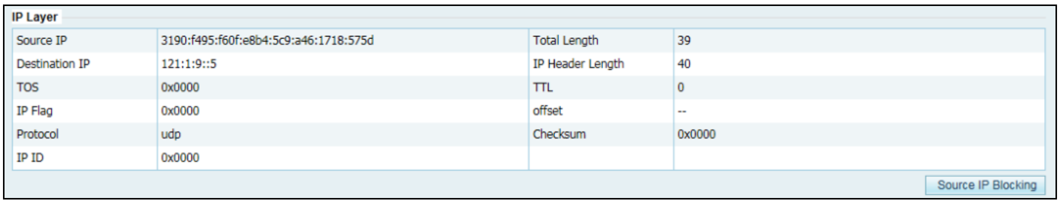
On the **Packet Details** page, you can directly click **Source IP Blocking** to add a source IP address to the global blocklist. For details, see section 5.2.10 Blocklist.

To add a source IP address to the blocklist, perform the following steps:

Step 1 View IP layer information.

As shown in Figure 8-4, network layer information of the captured packet is displayed in the **IP Layer** area.

Figure 8-5 IP Layer area

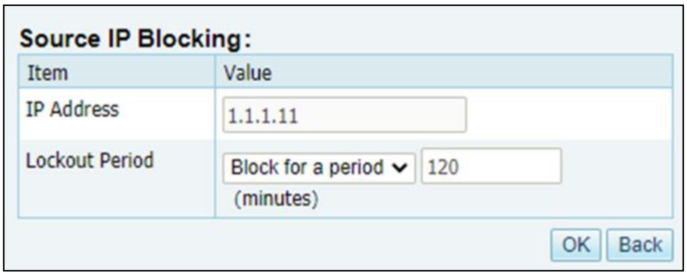


IP Layer

Source IP	3190:f495:f60f:e8b4:5c9:a46:1718:575d	Total Length	39
Destination IP	121:1:9::5	IP Header Length	40
TOS	0x0000	TTL	0
IP Flag	0x0000	offset	--
Protocol	udp	Checksum	0x0000
IP ID	0x0000		

Step 2 Click **Source IP Blocking**.

Figure 8-6 Confirmation dialog box



Source IP Blocking:

Item	Value
IP Address	1.1.1.11
Lockout Period	Block for a period 120 (minutes)

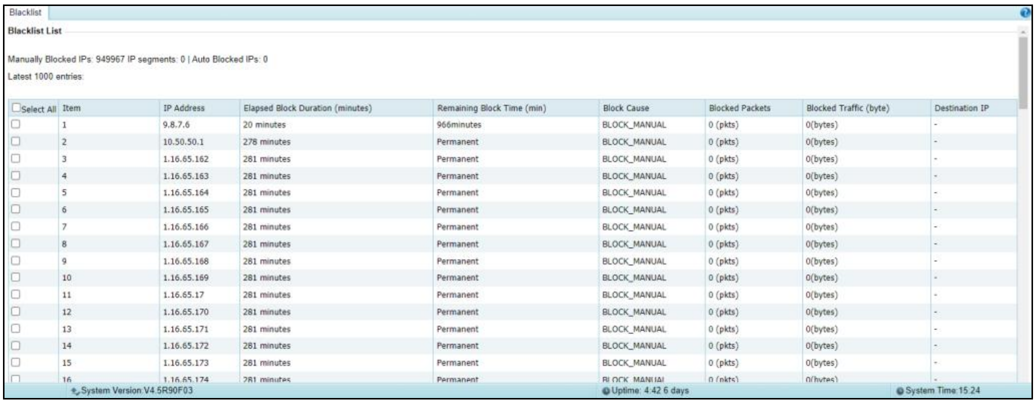
Step 3 Set the block period. For parameter details, see Table 5-39.

Step 4 Click **OK** in the confirmation dialog box to add the source IP address to the blocklist.

Step 5 View the newly created blocklist entry.

Choose **Policies** > **Access Control** > **Blacklist** and click **Blacklist List** in the lower-right corner of the **Blacklist** page.

Figure 8-7 Newly created blocklist entry



Blacklist List

Manually Blocked IPs: 949967 IP segments: 0 | Auto Blocked IPs: 0

Latest 1000 entries:

□Select All	Item	IP Address	Elapsed Block Duration (minutes)	Remaining Block Time (min)	Block Cause	Blocked Packets	Blocked Traffic (byte)	Destination IP
□	1	9.8.7.6	20 minutes	966minutes	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	2	10.50.50.1	278 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	3	1.16.65.162	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	4	1.16.65.163	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	5	1.16.65.164	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	6	1.16.65.165	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	7	1.16.65.166	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	8	1.16.65.167	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	9	1.16.65.168	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	10	1.16.65.169	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	11	1.16.65.17	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	12	1.16.65.170	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	13	1.16.65.171	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	14	1.16.65.172	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	15	1.16.65.173	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-
□	16	1.16.65.174	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0(bytes)	-

System Version:V4.5R90F03

Uptime: 4:42 6 days

System Time:15:24

----End

DNS Fingerprint Extraction

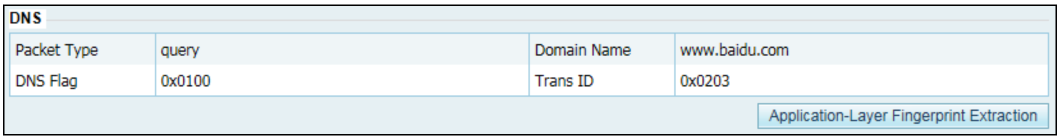
For DNS packets, you can extract DNS fingerprints from their detailed information to directly generate a DNS keyword checking rule. For details about DNS keyword checking rules, see section 5.1.2.8 DNS Keyword Checking Policy.

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

Step 1 View details about a DNS packet.

On the **Packet Details** page, application-layer information of the captured DNS packet is displayed in the **DNS** area, as shown in Figure 8-8.

Figure 8-8 DNS packet information

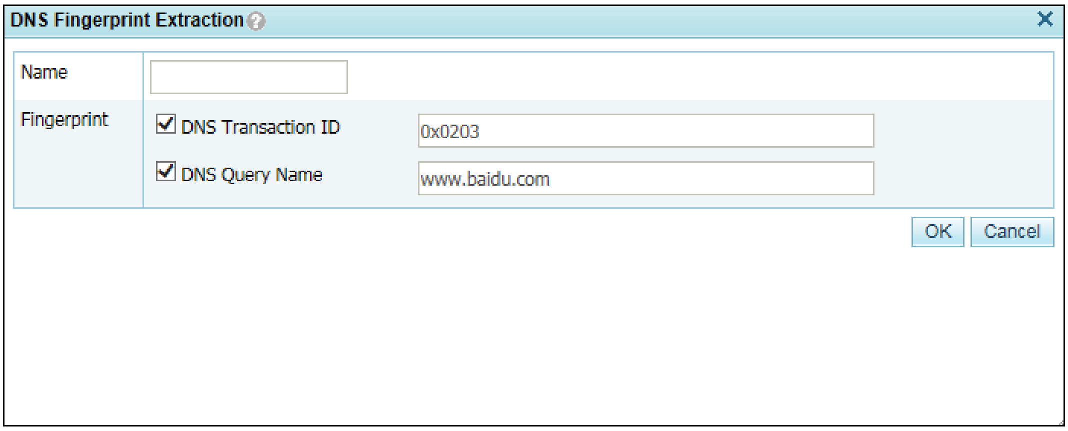


DNS

Packet Type	query	Domain Name	www.baidu.com
DNS Flag	0x0100	Trans ID	0x0203

Step 2 Click **Application-Layer Fingerprint Extraction**.

Figure 8-9 Extracting DNS fingerprints



DNS Fingerprint Extraction

Name		
Fingerprint	☑ DNS Transaction ID	0x0203
	☑ DNS Query Name	www.baidu.com

Step 3 Set **Name** and **Fingerprint**.

Step 4 Click **OK**.

The system automatically generates a DNS keyword checking rule according to the settings.

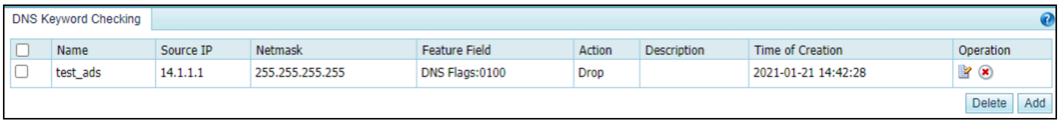
Step 5 View the newly created DNS keyword checking rule.

Choose **Policies** > **Access Control** > **DNS Keyword Checking** to view the newly created DNS keyword checking rule. Parameters of a DNS keyword checking rule are as follows:

- **Name**: policy name you have typed.
- **Source IP**: source IP address of the packet, which is **0.0.0.0(::)**.
- **Netmask**: subnet mask of the packet, which is **0.0.0.0(0)**.

- **Keyword**: The system generates checking rules according to the fingerprint(s) selected in Step 2. For unselected fingerprints, their settings are left empty.
- **Action**: action to be taken for matched packets, with **Drop** as the default value.

Figure 8-10 Newly created DNS keyword checking rule



DNS Keyword Checking

□	Name	Source IP	Netmask	Feature Field	Action	Description	Time of Creation	Operation
□	test_ads	14.1.1.1	255.255.255.255	DNS Flags:0100	Drop		2021-01-21 14:42:28	

----End

HTTP Fingerprint Extraction

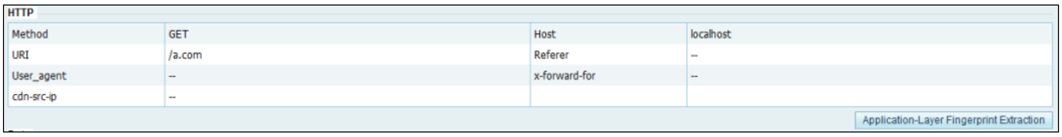
For HTTP packets, you can extract HTTP fingerprints from their detailed information to directly generate a HTTP keyword checking rule. For details about HTTP keyword checking rules, see section 5.2.6 HTTP Keyword Checking.

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

Step 1 View details about an HTTP packet.

As shown in Figure 8-4, the information about the captured HTTP packet is displayed in the **HTTP** area.

Figure 8-11 HTTP area

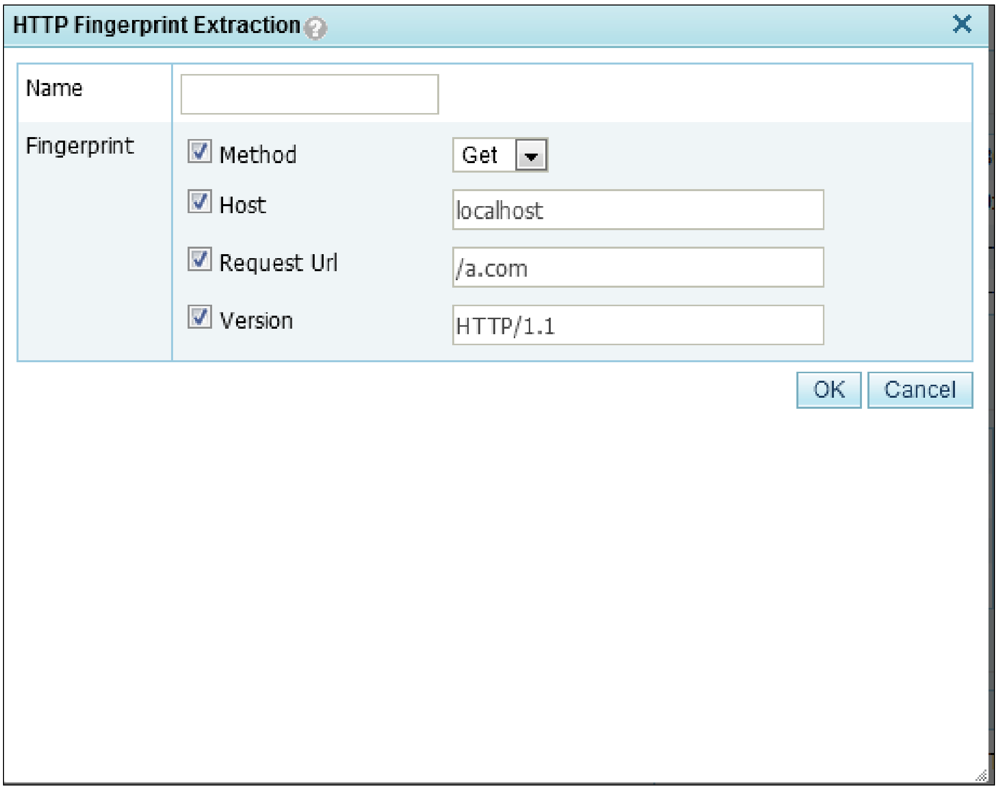


HTTP

Method	GET	Host	localhost
URI	/a.com	Referer	--
User_agent	--	x-forward-for	--
cdn-src-ip	--		

Step 2 Click **Application-Layer Fingerprint Extraction**.

Figure 8-12 Extracting HTTP fingerprints



HTTP Fingerprint Extraction

Name:

Fingerprint:

☑ Method: Get

☑ Host: localhost

☑ Request Url: /a.com

☑ Version: HTTP/1.1

Step 3 Set **Name** and select one or multiple domains for **Fingerprint**.

Step 4 Click **OK**.

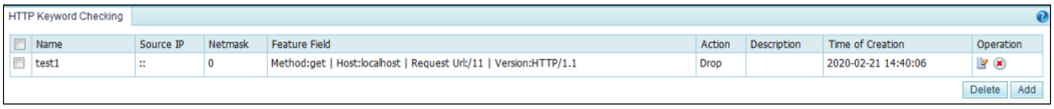
The system automatically generates an HTTP keyword checking rule according to the settings.

Step 5 View the newly created HTTP keyword checking rule.

Choose **Policies** > **Access Control** > **HTTP Keyword Checking**. Parameters of an HTTP keyword checking rule is as follows:

- **Name**: policy name you have typed.
- **Source IP**: source IP address of the packet, which is **0.0.0.0(::)**.
- **Netmask**: subnet mask of the packet, which is **0.0.0.0(0)**.
- **Keyword**: The keyword value depends on the setting of **Fingerprint**.
- **Action**: action to be taken for matched packets, with **Drop** as the default value.

Figure 8-13 Newly created HTTP keyword checking rule



HTTP Keyword Checking

□	Name	Source IP	Netmask	Feature Field	Action	Description	Time of Creation	Operation
□	test1	::	0	Method:get | Host:localhost | Request Url:/11 | Version:HTTP/1.1	Drop		2020-02-21 14:40:06	

----End

Payload Fingerprint Extraction

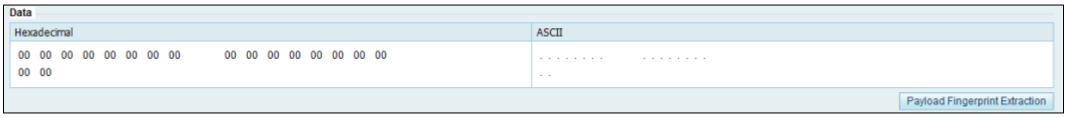
For TCP, UDP, and ICMP packets, you can extract payload fingerprints from the data displayed in the **Data** area by taking consecutive hexadecimal characters to directly create a pattern matching rule. For details about pattern matching rules, see section 8.2 **Pattern Matching Rules**.

To create a pattern matching rule based on fingerprints, perform the following steps:

Step 1 View details about a TCP, UDP, or ICMP packet.

As shown in Figure 8-4, the payload information of the captured TCP, UDP, or ICMP packet is displayed in the **Data** area.

Figure 8-14 Data area

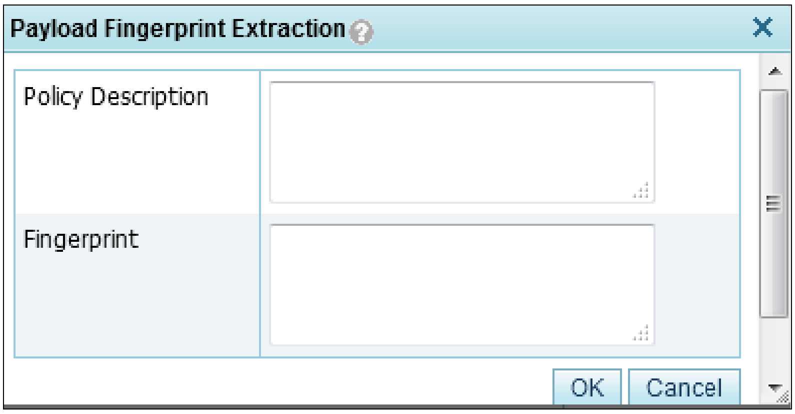


```
00  00  00  00  00  00  00  00        00  00  00  00  00  00  00  00
00  00
```

```
. . . . . . . .       . . . . . . . .
. .
```

Step 2 Click **Payload Fingerprint Extraction**.

Figure 8-15 Extracting payload fingerprints



Step 3 Set **Policy Description** and type one or more hexadecimal values in the **Fingerprint** text box.

Step 4 Click **OK**.

The system automatically generates a pattern matching rule.

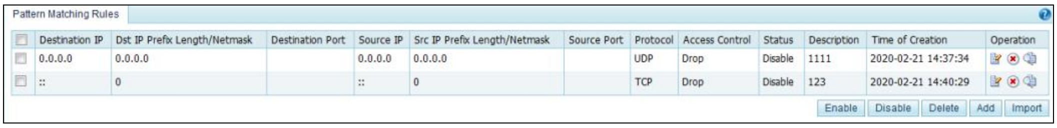
Step 5 View the newly created pattern matching rule.

Choose **Advanced** > **Pattern Matching** > **Pattern Matching Rules** to view the newly created pattern matching rule. As shown in Figure 8-16, parameters of a pattern matching rule are as follows:

- **Status**: indicate the status of the rule, which is **Disable**.
- **Source IP/Destination IP**: indicate the source/destination IP address of the packet, which are both **0.0.0.0(::)**.

- **Protocol**: indicates the protocol of the packet. This parameter is automatically filled according to the protocol you selected for the packet capture task. If **ALL** is selected, **TCP** is displayed by default.
- **Feature Field**: The feature field value depends on the setting of **Fingerprint**.
- **Description**: description of the rule, which is the same as the content of **Policy Description**.

Figure 8-16 Newly created pattern matching rule



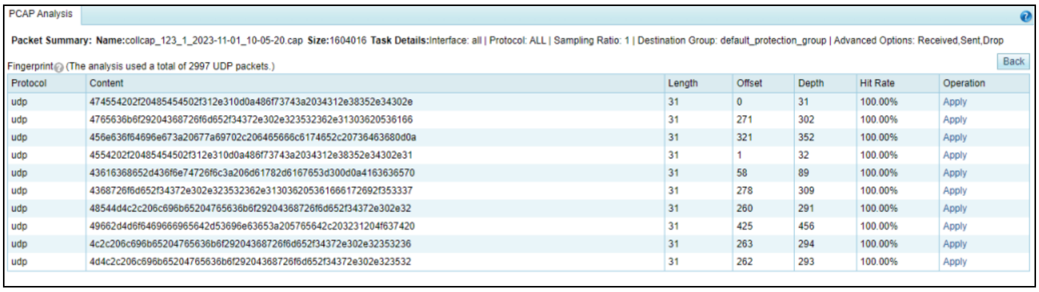
□	Destination IP	Dst IP Prefix Length/Netmask	Destination Port	Source IP	Src IP Prefix Length/Netmask	Source Port	Protocol	Access Control	Status	Description	Time of Creation	Operation
□	0.0.0.0	0.0.0.0		0.0.0.0	0.0.0.0		UDP	Drop	Disable	1111	2020-02-21 14:37:34	
□	::	0		::	0		TCP	Drop	Disable	123	2020-02-21 14:40:29	

----End

8.1.1.8 Analyzing a Manual Packet Capture File

Click **Analyze** in the **Operation** column of a packet capture file. The **PCAP Analysis** page appears, as shown in Figure 8-17.The **PCAP Analysis** page displays related information about the fingerprint found in the packet capture file, including the fingerprint protocol, content, length, offset, depth, and hit rate.

Figure 8-17 PCAP Analysis page



Packet Summary: **Name:**collcap_123_1_2023-11-01_10-05-20.cap **Size:**1604016 **Task Details:**Interface: all | Protocol: ALL | Sampling Ratio: 1 | Destination Group: default_protection_group | Advanced Options: Received,Sent,Drop

Fingerprint (The analysis used a total of 2997 UDP packets.)

Protocol	Content	Length	Offset	Depth	Hit Rate	Operation
udp	474554202f20485454502f312e310d0a486f73743a2034312e38352e34302e	31	0	31	100.00%	Apply
udp	4765636b6f29204368726f6d652f34372e302e323532362e31303620536166	31	271	302	100.00%	Apply
udp	456e636f64696e673a20677a69702c206465666c6174652c20736463680d0a	31	321	352	100.00%	Apply
udp	4554202f20485454502f312e310d0a486f73743a2034312e38352e34302e31	31	1	32	100.00%	Apply
udp	43616368652d436f6e74726f6c3a206d61782d6167653d300d0a4163636570	31	58	89	100.00%	Apply
udp	4368726f6d652f34372e302e323532362e313036205361666172692f353337	31	278	309	100.00%	Apply
udp	48544d4c2c206c696b65204765636b6f29204368726f6d652f34372e302e32	31	260	291	100.00%	Apply
udp	49662d4d6f6469666965642d53696e63653a205765642c203231204f637420	31	425	456	100.00%	Apply
udp	4c2c206c696b65204765636b6f29204368726f6d652f34372e302e32353236	31	263	294	100.00%	Apply
udp	4d4c2c206c696b65204765636b6f29204368726f6d652f34372e302e323532	31	262	293	100.00%	Apply

Click **Apply** in the **Operation** column to extract the fingerprint and generate a pattern matching rule for IPv4 and IPv6 respectively. The pattern matching rules are disabled by default. For detailed operations on pattern matching rules, see section 8.2 Pattern Matching Rules.

Table 8-3 describes parameters of fingerprint extraction.

Table 8-3 Parameters of fingerprint extraction

Parameter	Description
Policy Description	Description of the pattern matching rule to generate. It can contain 256 characters at most.
Action	Access control action of the pattern matching rule to generate, which can be **Filter** or **Drop**.

8.1.1.9 Downloading a Manual Packet Capture File

After a manual packet capture task ends, the manual packet capture file is displayed on the file list, as shown in the **Packet Capture Files** area in Figure 8-1. You can click **Download** in the **Operation** column of a manual packet capture file to download it to a local disk drive.

8.1.1.10 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 Configuring Automatic Packet Capture

Automatic packet capture can be rate-triggered or attack-triggered.

8.1.2.1 Rate-triggered Packet Capture

When the number of packets received by the destination IP address per second exceeds the specified value, automatic packet capture starts.

- 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).

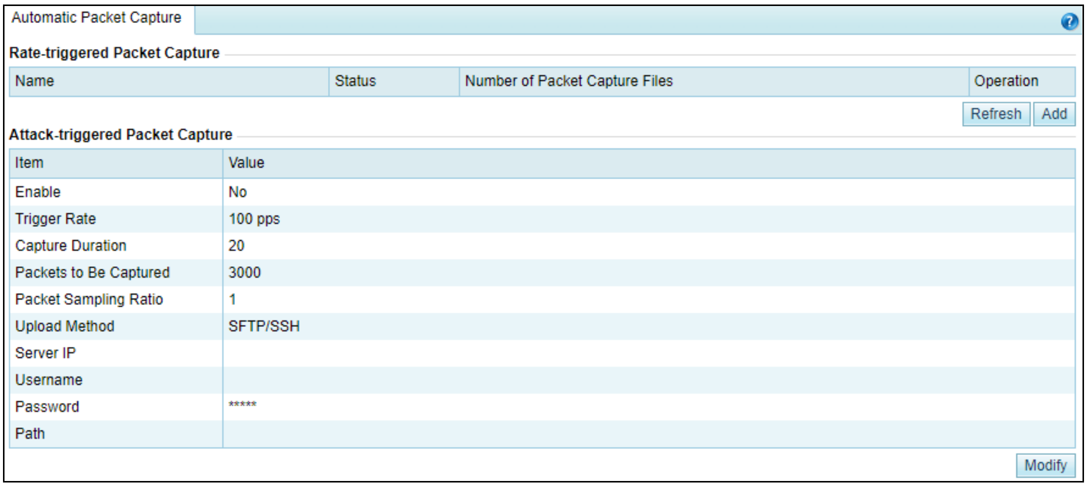
Creating a Rate-triggered Automatic Packet Capture Task

To configure a rate-triggered 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 8-18 Automatic Packet Capture page



Automatic Packet Capture

Rate-triggered Packet Capture

Name	Status	Number of Packet Capture Files	Operation

Refresh Add

Attack-triggered Packet Capture

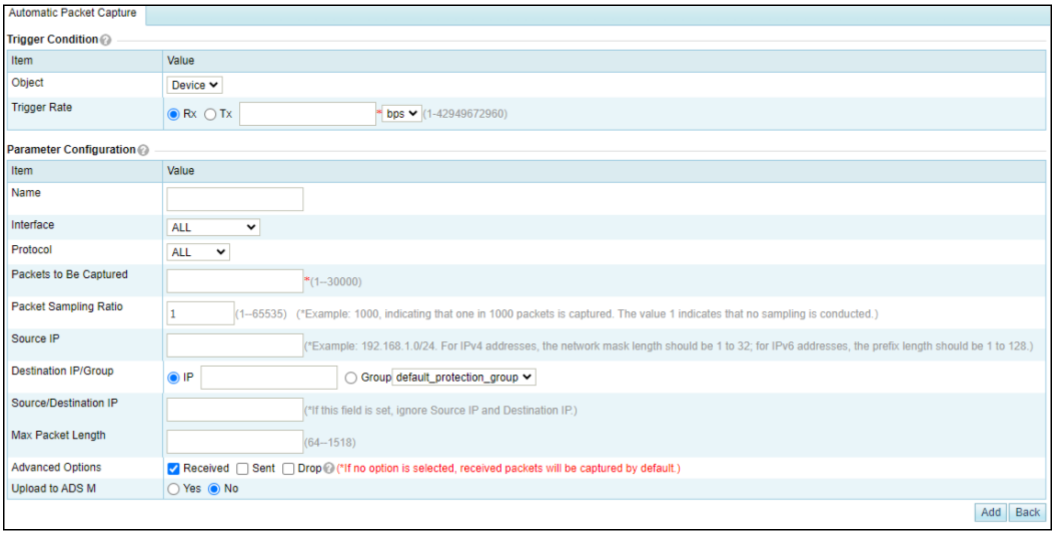
Item	Value
Enable	No
Trigger Rate	100 pps
Capture Duration	20
Packets to Be Captured	3000
Packet Sampling Ratio	1
Upload Method	SFTP/SSH
Server IP	
Username	
Password	*****
Path	

Modify

Step 2 Click **Add in the Rate-triggered Packet Capture** area to create an automatic packet capture task.

Step 3 Configure parameters.

Figure 8-19 Configuring an automatic packet capture task



Automatic Packet Capture

Trigger Condition

Item	Value
Object	Device
Trigger Rate	● Rx ○ Tx * bps (1-42949672960)

Parameter Configuration

Item	Value
Name	
Interface	ALL
Protocol	ALL
Packets to Be Captured	*(1--30000)
Packet Sampling Ratio	1 (1--65535) (*Example: 1000, indicating that one in 1000 packets is captured. The value 1 indicates that no sampling is conducted.)
Source IP	(*Example: 192.168.1.0/24. For IPv4 addresses, the network mask length should be 1 to 32; for IPv6 addresses, the prefix length should be 1 to 128.)
Destination IP/Group	● IP ○ Group default_protection_group
Source/Destination IP	(*If this field is set, ignore Source IP and Destination IP.)
Max Packet Length	(64--1518)
Advanced Options	☑ Received □ Sent □ Drop (*If no option is selected, received packets will be captured by default.)
Upload to ADS M	○ Yes ● No

Add Back

Table 8-4 describes some parameters for rate-triggered packet capture.

Table 8-4 Parameters of rate-triggered packet capture

Parameter	Description
Object	Specifies an object whose traffic will trigger an automatic packet capture task. Options include **Device**, **Group**, and **IP**. ADS will automatically start capturing packets when the traffic reaches the trigger rate.

Parameter	Description
Trigger Rate	Specifies the traffic threshold of the specified object that will trigger automatic packet capture. • The traffic rate direction can be **Rx** or **Tx**. • The traffic rate size can be 1–4294967295 pps or 1–42949672960 bps.
Name	The name is unique and should be a string of 1 to 15 characters, including letters, digits, and underscores (_).
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 be in the range of 0–255.
Packets to Be Captured	Number of packets to be captured. The value ranges from 1 to 30000.
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.
Packet Sampling Ratio	Specifies the ratio of matched packets to captured packets. Value range: 1–65535. For example, the value **1000** indicates that one in 1000 packets are captured. The default value is **1**, indicating no packet sampling. When the traffic bursts, the packet sampling ratio allows the device to capture packets in a longer period.
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.
Destination IP/Group	Destination IP address or group of this task. You can select **IP** or **Group**. • **IP**: When this is selected, you can further specify an IP address in the input box next to it. Leaving the box empty indicates no restriction on the destination of packets. Both IPv4 and IPv6 are supported. • **Group**: When this is selected, you need to select a protection group from the drop-down list.
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

Parameter	Description
	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. Note This parameter is available only when **Protocol** is set to **UDP** or **TCP**.
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. Note This parameter is available only when **Protocol** is set to **UDP** or **TCP**.
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**. Note This parameter is available only when **Protocol** is set to **UDP** or **TCP**.
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. Note • If none is selected, received packets will be captured by default. • If **Drop** is selected and when the group to which the destination IP address belongs is in alert mode, this packet actually is not dropped.
Upload to ADS M	Controls whether to upload automatic packet capture data to ADS M. Note • You can configure up to three automatic packet capture tasks, but can enable this for only one task. • For the implementation of this function, you should configure the IP address of ADS M during management mode configuration. For details, see section 3.1.4.1 Configuring the Management Mode.

Step 4 Click **OK** to complete the configuration.

The automatic packet capture task starts only when specified conditions are triggered.

----End

Managing a Rate-triggered Automatic Packet Capture Task

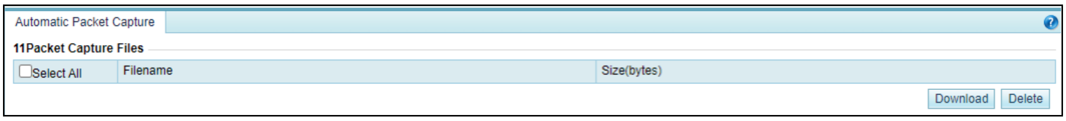
After automatic packet capture tasks are configured, you can manually start or stop them. In addition, you can refresh, view, edit and delete such tasks in the same way as manual packet capture tasks.

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.

Managing Rate-triggered Automatic Packet Capture Files

On the page shown in Figure 8-18, click ⬇ in the **Operation** column of an automatic packet capture task to open the packet capture file list, as shown in Figure 8-20.

Figure 8-20 Automatic packet capture file list



Automatic Packet Capture

11Packet Capture Files

□Select All	Filename	Size(bytes)

You can download, view, and delete automatic packet capture files in the same way as manual packet capture files.

8.1.2.2 Attack-triggered Packet Capture

When an attack happens, causing ADS to drop packets at a rate greater than the specified value, automatic packet capture starts.

To configure an attack-triggered packet capture task, perform the following steps:

Step 1 Choose **Advanced** > **Packet Capture** > **Automatic Packet Capture**.

Step 2 Click **Modify** in the **Attack-triggered Packet Capture** area to edit parameters.

Table 8-5 describes parameters of attack-triggered packet capture.

Table 8-5 Parameters of attack-triggered packet capture

Parameter	**Description**
Enable	Controls whether to enable attack-triggered packet capture.
Trigger Rate	When an attack happens, causing ADS to drop packets at a rate greater than the value specified here, automatic packet capture starts. The value range is 1–4294967295 pps or 1–42949672960 bps.
Capture Duration	Length of time the packet capture task lasts. The value range is 1–300, in seconds.
Packets to be Captured	Number of packets to be captured. The value ranges from 1 to 30000. After this is configured, when either the number of packets captured or the

Parameter	Description
	capture duration reaches the respective threshold, the system stops capturing more packets.
Packet Sampling Ratio	Specifies the ratio of matched packets to captured packets. Value range: 1–65535. For example, the value **1000** indicates that one in 1000 packets are captured. The default value is **1**, indicating no packet sampling. When the traffic bursts, the packet sampling ratio allows the device to capture packets in a longer period.
Upload Method	Specifies how packet capture files are uploaded to the specified server. The default value is **SFTP/SSH**, which cannot be modified.
Server IP	Specifies the IPv4 or IPv6 address of the SFTP/SSH server that receives attack-triggered packet capture files from ADS.
Username	User name used for login to the SFTP/SSH server.
Password	Password used for login to the SFTP/SSH server. You can modify the password by clicking **Edit Password**.
Path	Directory of packet capture files on the SFTP/SSH server. The naming convention for packet capture files is: device IP_protection target IP_attack event ID_attack type_capture time.

Step 3 Click **OK** to complete the configuration.

The automatic packet capture task starts only when the **Trigger Rate** is met.

----End

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:

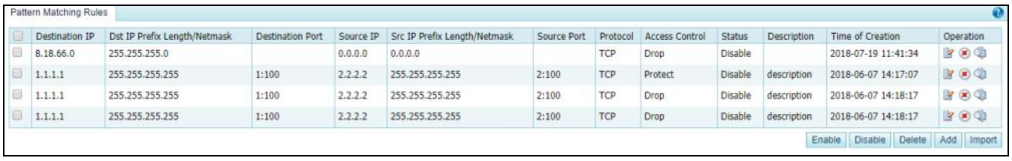
- Creating a Pattern Matching Rule
- Creating Pattern Matching Rules in Batches
- Enabling/Disabling Pattern Matching Rules
- Modifying Pattern Matching Rules
- Deleting Pattern Matching Rules
- Viewing Pattern Matching Rules

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 8-21 Pattern Matching Rules page

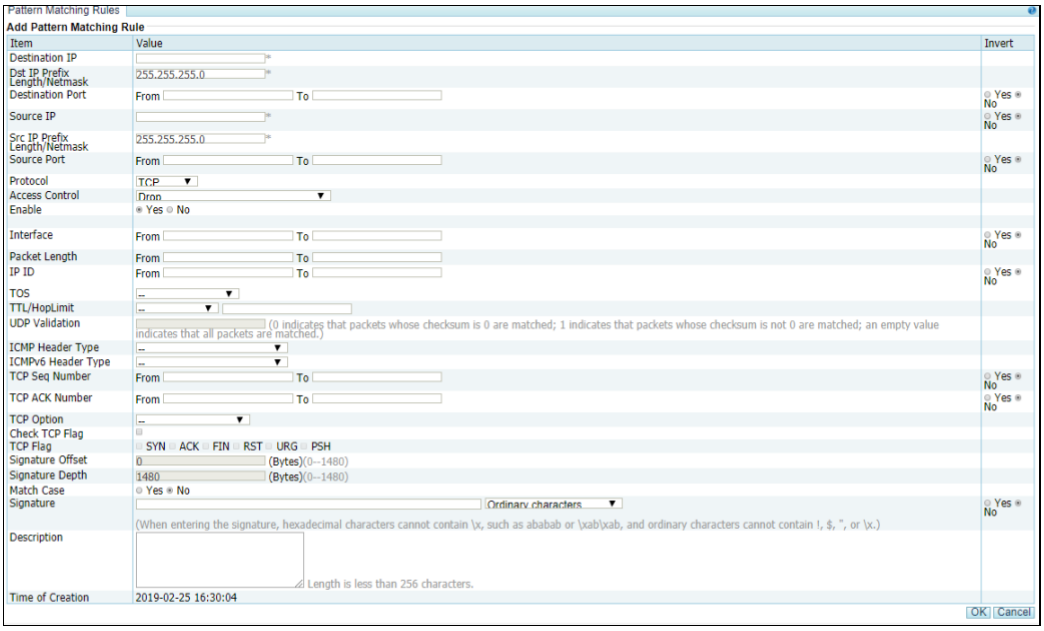


Pattern Matching Rules

☐	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
☐	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 8-22 Creating a pattern matching rule (TCP)



Pattern Matching Rules

Add Pattern Matching Rule

Item	Value	Invert
Destination IP	*	
Dst IP Prefix Length/Netmask	255.255.255.0 *	
Destination Port	From To	○ Yes ● No
Source IP	*	○ Yes ● No
Src IP Prefix Length/Netmask	255.255.255.0 *	
Source Port	From To	○ Yes ● No
Protocol	TCP	
Access Control	Drop	
Enable	● Yes ○ No	
Interface	From To	○ Yes ● No
Packet Length	From To	
IP ID	From To	○ Yes ● No
TOS	--	
TTL/HopLimit	--	
UDP Validation	(0 indicates that packets whose checksum is 0 are matched; 1 indicates that packets whose checksum is not 0 are matched; an empty value indicates that all packets are matched.)	
ICMP Header Type	--	
ICMPv6 Header Type	--	
TCP Seq Number	From To	○ Yes ● No
TCP ACK Number	From To	○ Yes ● No
TCP Option	--	
Check TCP Flag	☐	
TCP Flag	☐ SYN ☐ ACK ☐ FIN ☐ RST ☐ URG ☐ PSH	
Signature Offset	0 (Bytes)(0--1480)	
Signature Depth	1480 (Bytes)(0--1480)	
Match Case	○ Yes ● No	
Signature	Ordinary characters (When entering the signature, hexadecimal characters cannot contain \x, such as ababab or \xab\xab, and ordinary characters cannot contain !, $, ", or \x.)	○ Yes ● No
Description	Length is less than 256 characters.	
Time of Creation	2019-02-25 16:30:04	

Table 8-6 describes parameters for creating a pattern matching rule.

Table 8-6 Automatic packet capture parameters

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.
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

Parameter	Description
	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. • **Filter** 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 blocklist. • **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 blocklist, 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 global blocklist function. Otherwise, the blocklist is invalid. For details, see section *5.2.10* Blocklist.
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.
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.

Parameter	Description
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**.
Signature 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.
Signature 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.
Time of Creation	Time when the rule is created, which is automatically generated by the

Parameter	Description
	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 range202.114.1.1–202.114.1.254 are deemed to match the configured rule.

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

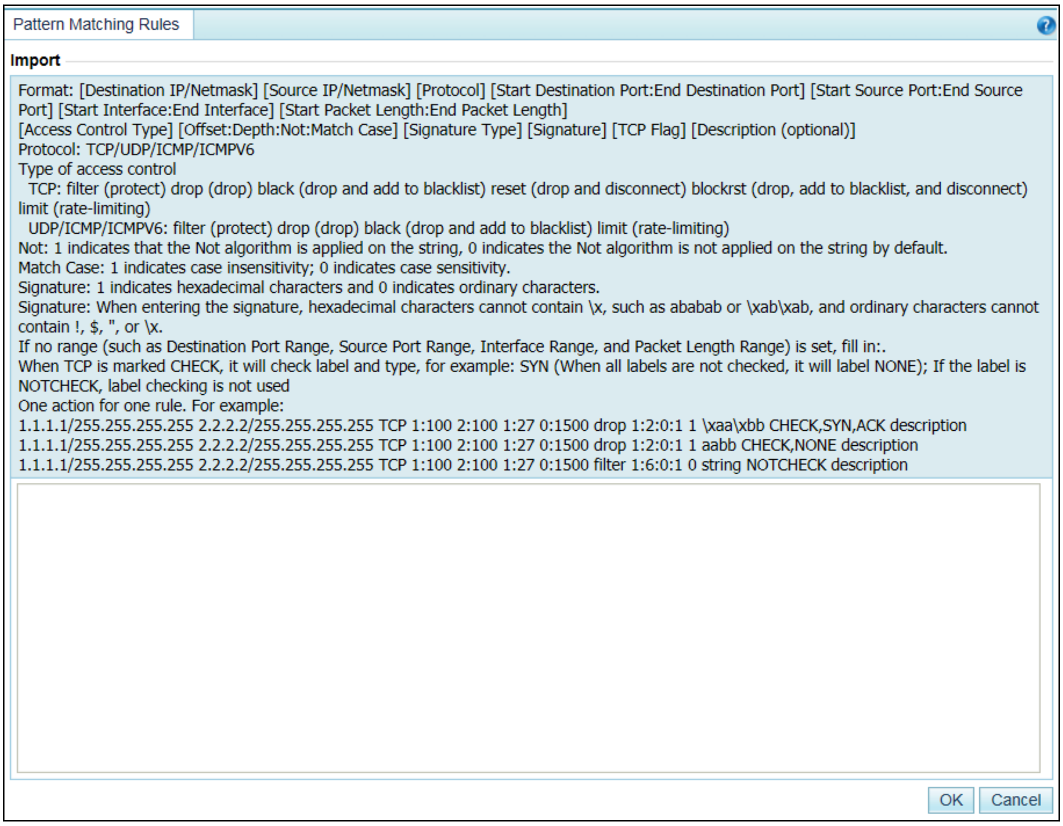
----End

8.2.2 Creating Pattern Matching Rules in Batches

To create pattern matching rules in batches, perform the following steps:

Step 1 On the **Pattern Matching Rules** page shown in Figure 8-21, click **Import** below the table to create pattern matching rules in batches.

Figure 8-23 Creating pattern matching rules in batches



```
Format: [Destination IP/Netmask] [Source IP/Netmask] [Protocol] [Start Destination Port:End Destination Port] [Start Source Port:End Source
Port] [Start Interface:End Interface] [Start Packet Length:End Packet Length]
[Access Control Type] [Offset:Depth:Not:Match Case] [Signature Type] [Signature] [TCP Flag] [Description (optional)]
Protocol: TCP/UDP/ICMP/ICMPV6
Type of access control
  TCP: filter (protect) drop (drop) black (drop and add to blacklist) reset (drop and disconnect) blockrst (drop, add to blacklist, and disconnect)
limit (rate-limiting)
  UDP/ICMP/ICMPV6: filter (protect) drop (drop) black (drop and add to blacklist) limit (rate-limiting)
Not: 1 indicates that the Not algorithm is applied on the string, 0 indicates the Not algorithm is not applied on the string by default.
Match Case: 1 indicates case insensitivity; 0 indicates case sensitivity.
Signature: 1 indicates hexadecimal characters and 0 indicates ordinary characters.
Signature: When entering the signature, hexadecimal characters cannot contain \x, such as ababab or \xab\xab, and ordinary characters cannot
contain !, $, ", or \x.
If no range (such as Destination Port Range, Source Port Range, Interface Range, and Packet Length Range) is set, fill in:.
When TCP is marked CHECK, it will check label and type, for example: SYN (When all labels are not checked, it will label NONE); If the label is
NOTCHECK, label checking is not used
One action for one rule. For example:
1.1.1.1/255.255.255.255 2.2.2.2/255.255.255.255 TCP 1:100 2:100 1:27 0:1500 drop 1:2:0:1 1 \xaa\xbb CHECK,SYN,ACK description
1.1.1.1/255.255.255.255 2.2.2.2/255.255.255.255 TCP 1:100 2:100 1:27 0:1500 drop 1:2:0:1 1 aabb CHECK,NONE description
1.1.1.1/255.255.255.255 2.2.2.2/255.255.255.255 TCP 1:100 2:100 1:27 0:1500 filter 1:6:0:1 0 string NOTCHECK description
```

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/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 8-21, 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 8-21, 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 8-21, click 📝 in the **Operation** column to edit parameters of a rule, as shown in Figure 8-22.

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 either of the following ways:

- On the **Pattern Matching Rules** page shown in Figure 8-21, 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 8-21, select one or more pattern matching rules (or select the **Select All** check box to select all rules in 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

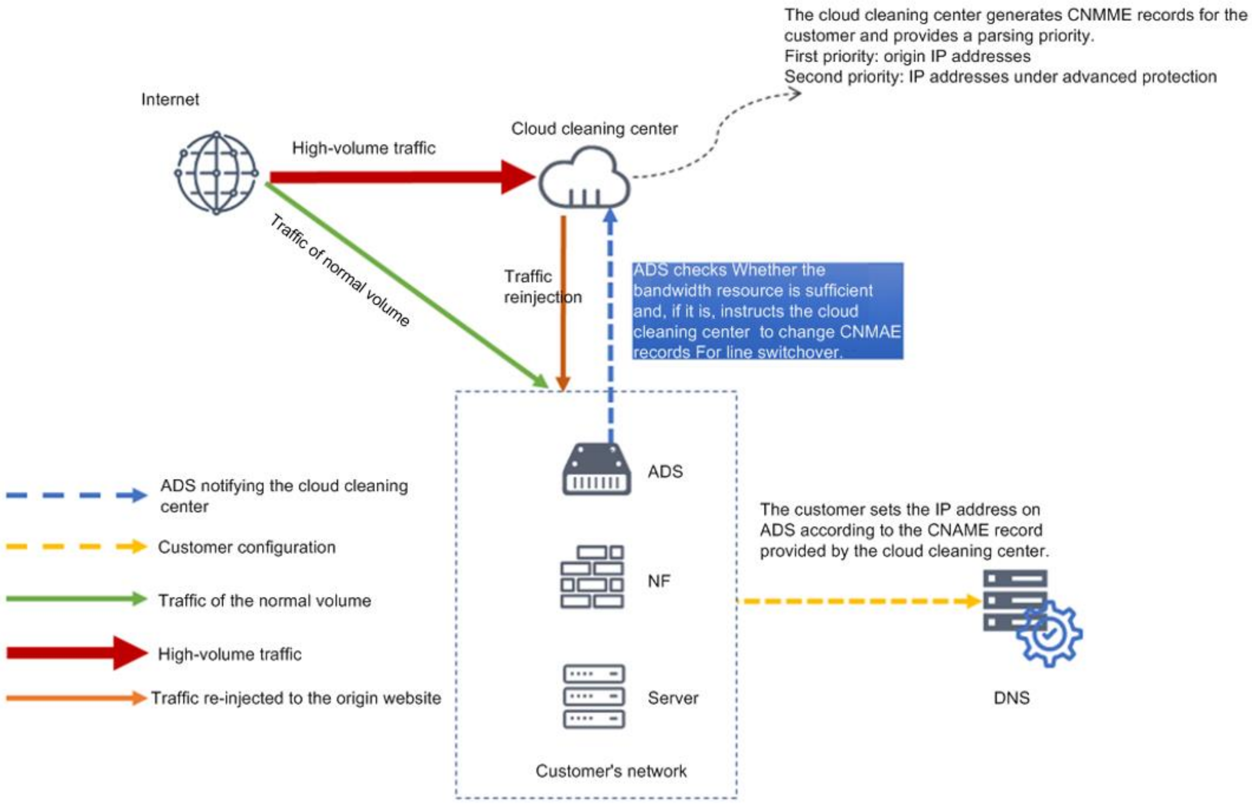
On the **Pattern Matching Rules** page shown in Figure 8-21, click in the **Operation** column of a pattern matching rule to view its information.

After viewing rules, click **Back** to return to the **Pattern Matching Rules** page.

8.3 Cloud Signaling

The cloud signaling function is available only after you purchase the cloud cleaning service. Figure 8-24 shows the topology of the application scenario. Via cloud signaling, ADS, in the case of volumetric attacks, can divert traffic to the cloud cleaning center for cleaning. Then the traffic is injected back to the origin website after being cleaned.

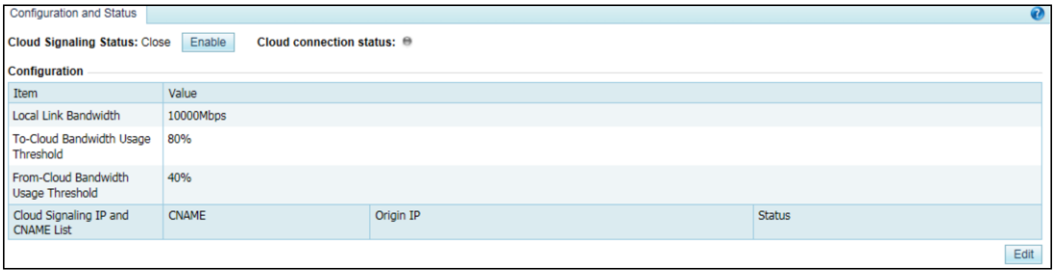
Figure 8-24 Topology of the cloud signaling scenario


The cloud cleaning center generates CNMME records for the customer and provides a parsing priority.
First priority: origin IP addresses
Second priority: IP addresses under advanced protection
Internet
High-volume traffic
Cloud cleaning center
Traffic of normal volume
Traffic reinjection
ADS checks Whether the bandwidth resource is sufficient and, if it is, instructs the cloud cleaning center to change CNMAE records For line switchover.
ADS
NF
Server
Customer's network
ADS notifying the cloud cleaning center
Customer configuration
Traffic of the normal volume
High-volume traffic
Traffic re-injected to the origin website
The customer sets the IP address on ADS according to the CNAME record provided by the cloud cleaning center.
DNS

To configure cloud signaling, perform the following steps:

Step 1 Choose **Advanced** > **Cloud Signaling** > **Configuration and Status**.

Figure 8-25 Configuration and Status page



Configuration and Status

Cloud Signaling Status: Close Enable **Cloud connection status:** ●

Configuration

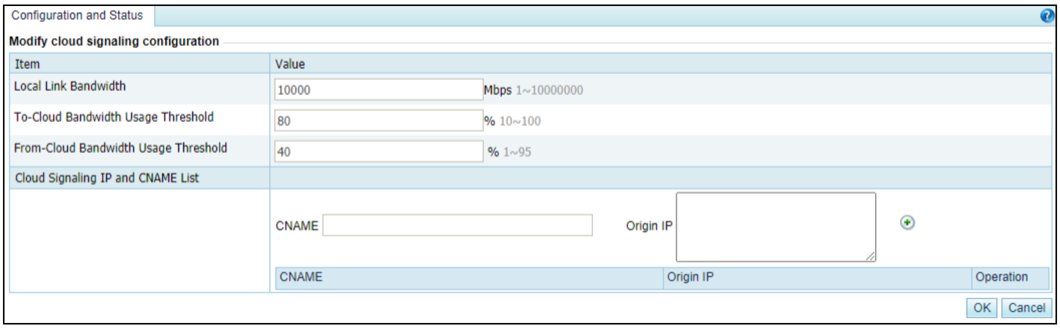
Item	Value		
Local Link Bandwidth	10000Mbps		
To-Cloud Bandwidth Usage Threshold	80%		
From-Cloud Bandwidth Usage Threshold	40%		
Cloud Signaling IP and CNAME List	CNAME	Origin IP	Status

Edit

Step 2 Configure parameters.

a. Click **Edit**.

Figure 8-26 Configuring cloud signaling parameters



Configuration and Status

Modify cloud signaling configuration

Item	Value
Local Link Bandwidth	10000 Mbps 1~10000000
To-Cloud Bandwidth Usage Threshold	80 % 10~100
From-Cloud Bandwidth Usage Threshold	40 % 1~95
Cloud Signaling IP and CNAME List	
	CNAME Origin IP

CNAME	Origin IP	Operation

OK Cancel

b. (Optional) Modify default parameters.

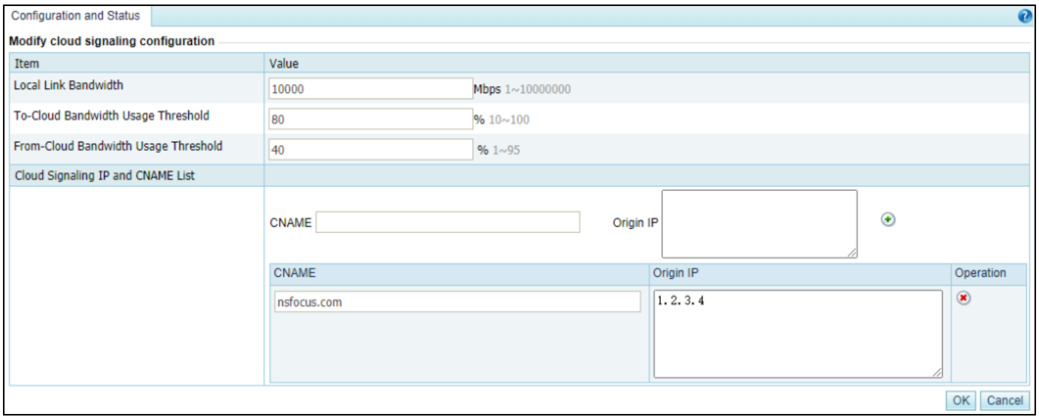
Table 8-7 Parameters for configuring cloud signaling

Parameter	Description
Local Link Bandwidth	Specifies the bandwidth of the link on which ADS resides. The unit is Mbps. The value range is 1–10000000, with **10000** as the default value.
To-Cloud Bandwidth Usage Threshold	When the incoming traffic exceeds the to-cloud bandwidth usage threshold, the traffic will be automatically switched to the cloud cleaning center for cleaning. The value range is 10–100, with **80** as the default value.
From-Cloud Bandwidth Usage Threshold	When the total traffic falls below the from-cloud bandwidth usage threshold, the traffic will be automatically switched to the local ADS for cleaning. The value range is 1–95, with **40** as the default value. **Note** *The from-cloud bandwidth usage threshold must be smaller than or equal to the to-cloud bandwidth usage threshold minus 5.*

c. Configure origin IP addresses and CNAME records.

You can click ⊕ to add multiple entries.

Figure 8-27 Configuring the cloud signaling IP address and CNAME list



Modify cloud signaling configuration

Item	Value
Local Link Bandwidth	10000 Mbps 1~10000000
To-Cloud Bandwidth Usage Threshold	80 % 10~100
From-Cloud Bandwidth Usage Threshold	40 % 1~95
Cloud Signaling IP and CNAME List	

CNAME   Origin IP ⊕

CNAME	Origin IP	Operation
nsfocus.com	1.2.3.4	☒

Table 8-8 Parameters for configuring origin IP addresses and CNAME records

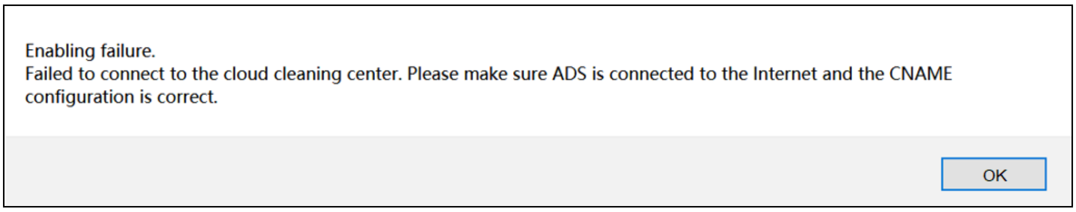
Parameter	Description
CNAME	CNAME is a Canonical Name Record or Alias Record that maps one domain name, for example, M, to another, for example, M'. Therefore, changing the IP address that maps domain name M' also changes the IP address translated for domain name M. Here, you should type the CNAME string provided by NSFOCUS operations personnel. The CNAME string contains a maximum of 256 characters.
Origin IP	Specifies the origin IP address of the website whose traffic requires cloud cleaning. It is usually the public IPv4 address of the local server mapping the domain name used for providing services. One CNAME record supports a maximum of four origin IP addresses and all origin IP addresses, no matter to which CNAME record they belong, must be unique.

Step 3 Enable cloud signaling.

After you click **Enable**, ADS automatically checks its connection to the cloud cleaning center. Then different information will be returned, depending on whether the connection is successfully established.

- If the connection cannot be established, a dialog box shown in Figure 8-27 is displayed.
- If the connection is successfully established, the **Origin IP Addresses** area is displayed, indicating the source IP address of legitimate traffic, which is injected back to the customer's server by the cloud cleaning center.

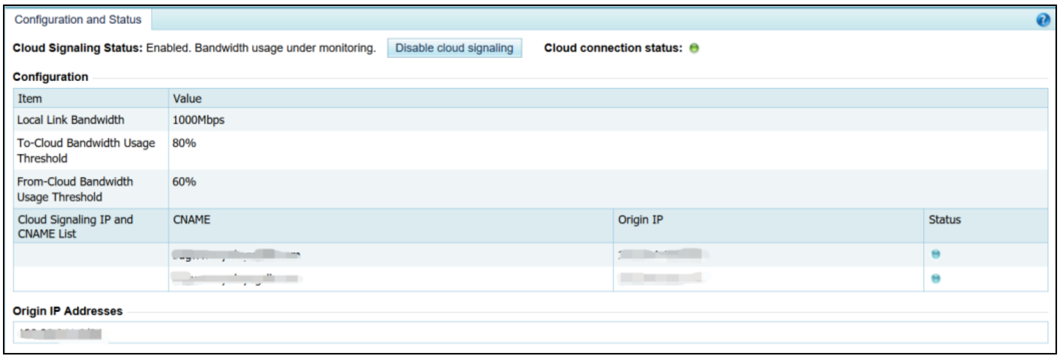
Figure 8-28 Message displayed in the case that cloud signaling cannot be enabled



Enabling failure.
Failed to connect to the cloud cleaning center. Please make sure ADS is connected to the Internet and the CNAME configuration is correct.

Note	
Note	- You are advised to add the source IP address to the allowlist on ADS, the firewall, and WAF. - After cloud signaling is enabled, no settings can be edited.

Figure 8-29 Page displayed after cloud signaling is enabled



Configuration and Status

Cloud Signaling Status: Enabled. Bandwidth usage under monitoring. Disable cloud signaling **Cloud connection status:** ●

Configuration

Item	Value		
Local Link Bandwidth	1000Mbps		
To-Cloud Bandwidth Usage Threshold	80%		
From-Cloud Bandwidth Usage Threshold	60%		
Cloud Signaling IP and CNAME List	CNAME	Origin IP	Status
	[redacted]	[redacted]	●
	[redacted]	[redacted]	●

Origin IP Addresses

[redacted]

Step 4 Check the interaction status between ADS and the cloud cleaning center.

After cloud signaling is enabled, the status of the interaction between ADS and the cloud cleaning center is displayed in the **Status** column shown in Figure 8-28.

Table 8-9 Status description

Traffic	Status Description
When there is no volumetric attack or attack traffic is smaller than the to-cloud bandwidth usage threshold, the traffic destined for the origin IP address will not be directed to the cloud cleaning center, but will be cleaned locally.	**Status** is displayed as ●.
When the attack traffic exceeds the to-cloud bandwidth usage threshold, cloud signaling will be triggered and attack traffic will be diverted to the cloud cleaning center for scrubbing.	**Status** is displayed as ● To-cloud lines updating ... ? .
The attack traffic is successfully diverted to the cloud cleaning center for scrubbing.	**Status** is displayed as ● Traffic already diverted to cloud. .
When the attack traffic falls below the from-cloud bandwidth usage threshold, attack traffic will be switched back from the cloud cleaning center to ADS for local cleaning.	**Status** is displayed as ● From-cloud lines updating ... ? .

----End

8.4 Collaboration with NTI

Threat intelligence, in its narrow sense, refers to indicators of compromise (IoCs) that can be used to identify and detect threats, including file hashes, IP addresses, and URLs. The system supports threat intelligence-based security checks, helping users better identify and detect various cyber threats.

Note	To use this function, you need to buy an additional license. For details, contact NSFOCUS technical support.

ADS can collaborate with NTI. Specifically, ADS uploads blocked source IP addresses to NTI, which sends the latest threat intelligence data to ADS. For high-risk IP addresses, ADS automatically lists them on the blocklist and blocks packets from these addresses. If an blocked IP address is demmed to be benign, you can add it to the exception list, which will not be checked by ADS's NTI-based protection algorithms.

8.4.1 NTI Configuration

Choose **Advanced > NTI > NTI Configuration**. On the **NTI Configuration** page, click **Edit** to configure the collaboration between ADS and NTI.

Table 8-10 NTI configuration parameters

Parameter	Description
Enable	Controls whether to enable collaboration with NTI. Selecting **No** will disable all related functions. After this function is enabled, ADS immediately downloads data from NTI and refreshes the current blocklist. For high-risk IP addresses, ADS will block packets from them.
Protection Scope	Specifies whether the function is valid globally or for specific groups. The options include **Global** and **Group**. A packet whose source IP address has a match in the intelligence database will be dropped in the case of global protection, or handled according to the threat intelligence rule set for the related group in the case of group protection.
Threat Intelligence Sharing	Controls whether to share the local threat intelligence to the cloud. After this function is enabled, ADS reports the discovered high-risk IP addresses to NTI.
Cloud Query Server Address	Specifies a domain in China (nti.nsfocus.com) or outside of China (nti.nsfocusglobal.com) for query of intelligence data of an IP address. 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	Tests 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.

8.4.2 NTI Application Effect and Query

This function allows you to query the blocked IP address, and query the local or cloud-side database to see whether an IP address is dangerous.

8.4.2.1 NTI Application Effect

Choose **Advanced** > **NTI** > **NTI Application Effect and Query** > **NTI Application Effect**. The **NTI Application Effect** page displays information about a top 1000 list of matching IP addresses by byte count, including the total number of matching IP addresses detected, total blocked packets, and total blocked traffic. These IP addresses have been blocked because of having a match in the intelligence database. Click **Refresh to obtain the latest top 1000 matching IP addresses.**

Type an IP address in the text box above the list, and click Search to check whether the IP address is blocked.

For blocked IP addresses, you can operate on them as follows:

- Add an IP address to the exception list

  Click **Add to exception** in the **Operation** column to add a matching IP address, which is deemed to be benign, to the IP exception list. After that, this IP address will not be checked again against the intelligence database.

- Local query

  Click **Local** to query the local database for the intelligence of an IP address.

- Cloud query

  Click **Cloud** to query the cloud-side database for the intelligence of an IP address.

8.4.2.2 Threat Intelligence Search

You can also query the threat intelligence in NTI from ADS.

Choose **Advanced** > **NTI** > **NTI Application Effect and Query** > **Threat Intelligence Search to query whether an IP address is** dangerous**.**

Table 8-11 describes the conditions for query of threat intelligence.

Table 8-11 Threat intelligence query parameters

Parameter	Description
Query Means	Controls whether to query the local or cloud-side database. The default option is **Local**.
IP Address	Specifies the IP addresses to be queried. Multiple IP addresses should be separated by commas (,).

The matched IP addresses are displayed in the lower part of the page together with the credit level and update time.

- Click **Local details** in the **Search** column to further view detailed intelligence information of the IP address in the local NTI database.
- Click **Cloud details** in the **Search** column to further view detailed intelligence information of the IP address in the cloud-side NTI database.

Caution	The **Cloud details** function is only supported by the license of V4.5R90F04 or a later version. If ADS is upgraded by using an earlier license, this function is unavailable.

8.4.3 NTI Upgrade

The NTI database can be upgraded automatically or manually.

8.4.3.1 Automatic Synchronization

Choose **Advanced > NTI > NTI Upgrade**. In the **Auto Sync** area of the **NTI Upgrade** page, click **Edit** to configure parameters for automatic synchronization.

Table 8-12 Parameters for automatic synchronization

Parameter	Description
Server Address	Specifies a domain in China (update.nsfocus.com) or outside of China (update.nsfocusglobal.com) for downloading of threat intelligence data.
Enable	Controls whether to enable automatic synchronization of the threat intelligence database.
Upgrade Time	Specifies how frequently the threat intelligence database is upgraded after automatic synchronization is enabled. Then ADS will upgrade the NTI database to the latest version at the specified upgrade time.

Clicking **Upgrade Now** immediately triggers upgrade of the NTI database.

8.4.3.2 Local Upgrade

The NTI database can be upgraded offline.

In the **Local Upgrade** area of the **NTI Upgrade** page, specify the period of time when an offline threat intelligence package that can be imported remains effective, choose a local threat intelligence package, and then click **Upload**.

8.4.3.3 Upgrade History

The upgrade history records upgrade information of the intelligence database. Click **Refresh** to display the recent upgrade records.

8.4.4 IP Exceptions

After adding a matching or custom IP address to the exception list, the IP address will not be checked or blocked again against the threat intelligence database.

Choose **Advanced > NTI > IP Exceptions**. Click **Edit** in the **IP Exception Configuration** area to enable the IP address exception function.

The IP addresses included in the exception list can be added, deleted, cleared, and queried.

- Search the exception list for an IP address

  Type an IPv4 or IPv6 address in the text box above the exception list and click **Search** to check whether the IP address is included in the exception list.

- Add an IP address to the exception list

  Type an IPv4 or IPv6 address in the text box above the exception list and click **Add** to add the IP address to the exception list. For IPv4 addresses, the netmask is in the range of 24–32; for IPv6 addresses, the netmask is in the range of 120–128.

- Delete IP addresses from the exception list

  Click ✖ in the **Operation** column to remove the selected IP address from the exception list.

  Select several IP addresses and click **Delete** to remove them from the exception list in batch.

- Clear the IP exception list

  Click **Clear** to remove all IP addresses from the exception list.

8.5 Carpet Bombing Protection

Carpet bombing is a kind of DDoS attack that targets a large number of IP addresses by using common attack methods. It generates massive attack traffic in a short time, which easily paralyzes the entire equipment room. The traffic of such an attack destined for a single IP address may not be large enough to trigger protection, leading to false negatives. Through the carpet combing protection, the system counts the number of visits of a source IP address to destination IP addresses and determines whether the source IP address is abnormal. For the identified attack source, the system can add it to the blocklist or limit its rate, or do both. The carpet combing protection can be globally effective or work for protection groups.

Choose **Advanced** > **Carpet Bombing Protection** > **Configuration** and configure parameters. Table 8-13 describes parameters for configuring a carpet bombing protection policy.

Table 8-13 Parameters of carpet bombing protection

Parameter	**Description**
Enable	Controls whether to enable the carpet bombing protection function. • **Yes**: enables the carpet bombing protection function. • **No**: disables the carpet bombing protection function.
Scope of Validity	Specifies the application scope of the carpet bombing protection. Options include **Global** or **Group**. • **Global**: The carpet bombing protection works for all destination IP addresses from a device. • **Group**: The carpet bombing protection works only for IP addresses in protection groups. If **Group** is selected, you should also enable carpet bombing protection in policies configured for the group you want to protect from this type of attacks. For details, see Carpet Bombing.
Action	Specifies the action taken for carpet bombing protection. Options include **Add to blacklist**, **Limit rate**, and **Limit rate & add to blacklist**.

Parameter	Description
Statistical Period	Specifies a period of time when the number of visits to destination IP addresses is counted. Value range: 1–600, in seconds.
Parameters of **Limit rate** policy	When a source IP address accesses more IP addresses than the value of **Destination IPs** within the statistical period and this anomaly persists for the specified number of **Consecutive Abnormal Cycles**, the device limits its traffic. • **Destination IPs**: maximum allowed number of destination IP addresses accessed by a single source IP address in the statistical period. Value range: 1–10000. • **Consecutive Abnormal Cycles**: number of consecutive cycles where a source IP address accesses the specified number of destination IP addresses. The device deems such a source IP address to be abnormal. Value range: 1–10. • **Per Source IP Rate Limit**: maximum traffic rate allowed for a source IP address. Excess packets will be dropped. Value range: 0–524280 in pps or 0–1073741824 in bps. • **Rate Limit Duration**: specifies how long rate limiting is implemented against a source IP address. When the duration expires, rate limiting stops. Value range: 1–3600, in minutes.
Parameters of **Add to blacklist** policy	When a source IP address accesses more IP addresses than the value of **Destination IPs** within the statistical period and this anomaly persists for the specified number of **Consecutive Abnormal Cycles**, the device adds it to the blocklist. • **Destination IPs**: maximum allowed number of destination IP addresses accessed by a single source IP address in the statistical period. Value range: 1–10000. • **Consecutive Abnormal Cycles**: number of consecutive cycles where a source IP address accesses the specified number of destination IP addresses. The device deems such a source IP address to be abnormal. Value range: 1–10. Note • When **Scope of Validity** is set to **Global**, you need to first enable the global blocklist. The system adds the source IP address to the global blocklist. For details about the blocklist function, see section 5.2.10 Blocklist. • When **Scope of Validity** is set to **Group**, you need to firstly enable the group-specific blocklist. The system adds the source IP address to the blocklist of the group you want to protect from this type of attacks. For details about the group-specific blocklist function, see Setting a Group-specific Blocklist.

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:

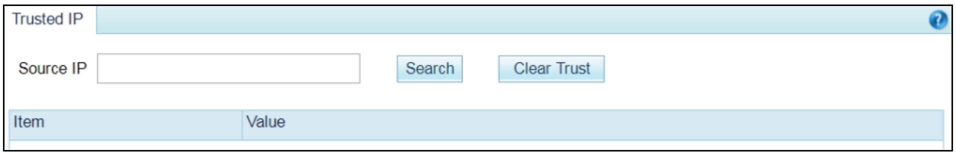
- Device Protection Status
- Network Diagnosis

9.1.1 Checking the Trust Status

To check the trust status of source IP addresses, perform the following steps:

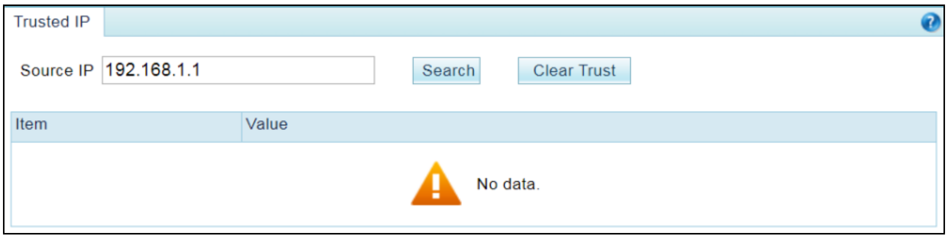
Step 1 Choose **O&M** > **Device Protection Status** > **Trusted IP**.

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


Trusted IP

Source IP: 192.168.1.1

Click **Clear Trust** to clear the information about existing trusted IP addresses.

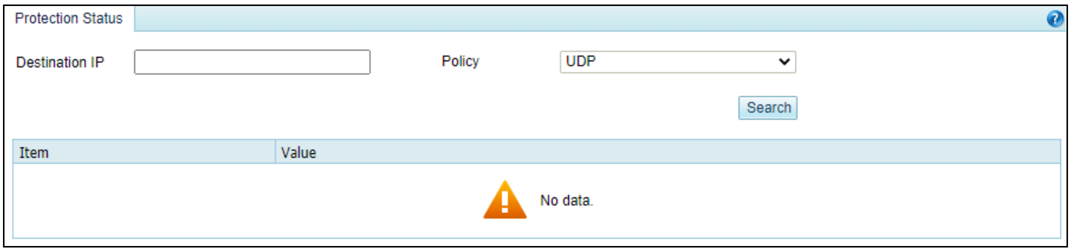
----End

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


Protection Status

Destination IP:

Policy: UDP

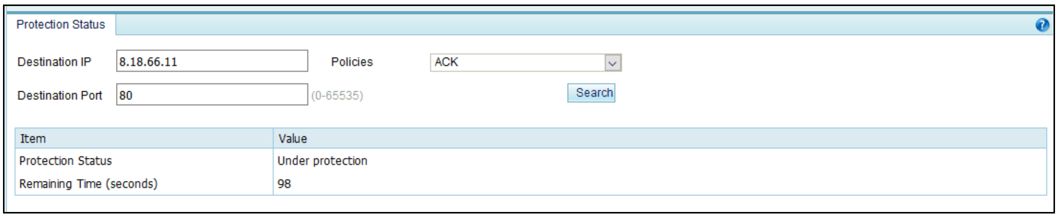
Step 2 Configure query parameters.

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.
URL	URL under protection. This parameter is available only when **HTTP_GET** or **HTTP_POST** is selected for **Policy**.
Destination Port	Destination port. This is required only when **Protocol** is set to other protocols than **UDP**, **ICMP, or DNS_REPLY.**

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



Protection Status

Destination IP: 8.18.66.11

Policies: ACK

Destination Port: 80 (0-65535)

Item	Value
Protection Status	Under protection
Remaining Time (seconds)	98

----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

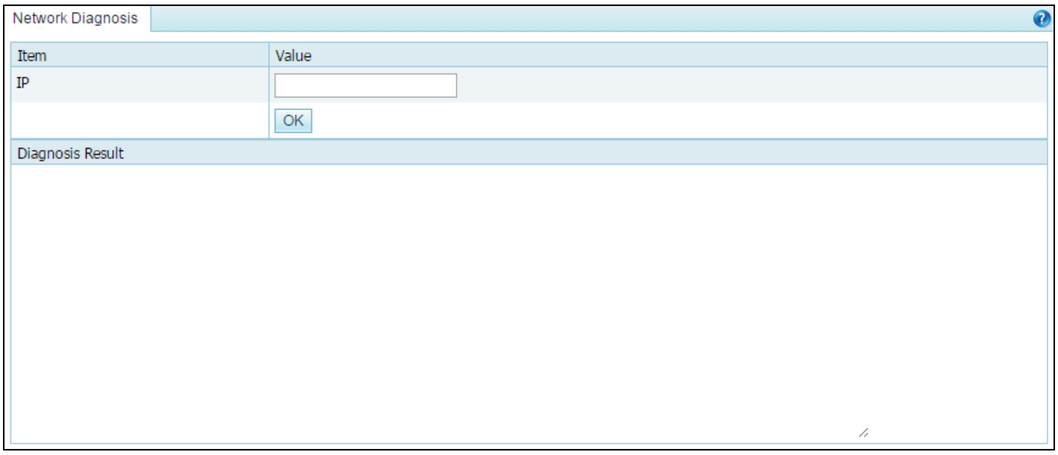
Ping is used to check whether a host is alive or connects to the network.

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



Network Diagnosis

Item	Value
IP	
	OK

Diagnosis Result

Step 2 Type an IP address and click **OK**.

The ping result will then be displayed in the text box below.

----End

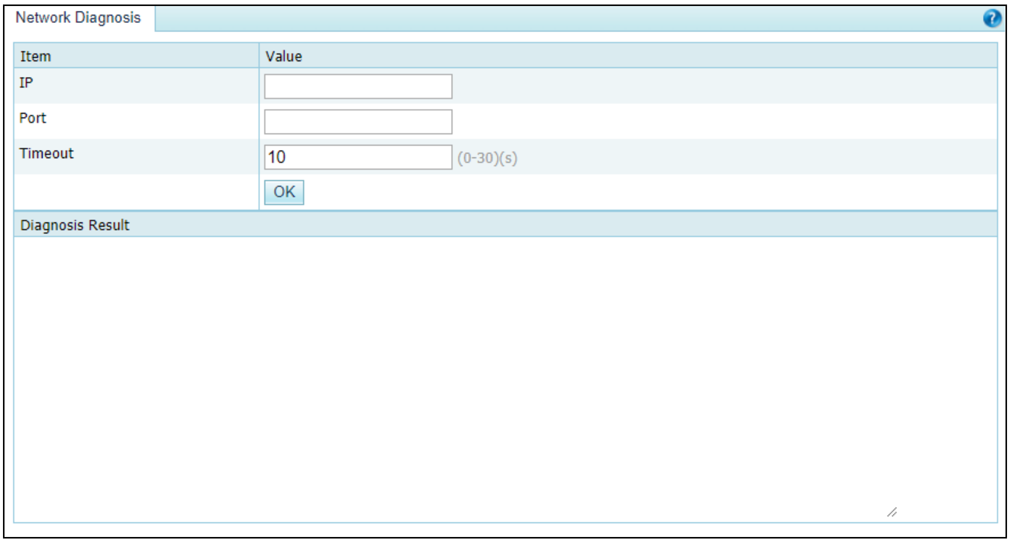
9.2.2 Port Check

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

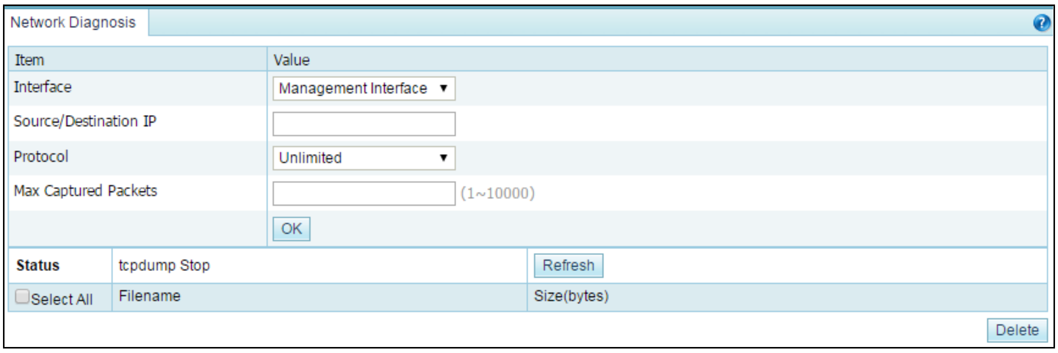
Tcpdump is used to intercept and analyze packets being transmitted or received over a network as defined by a user. The user can check the status of and troubleshoot network interface cards (NICs) based on such analysis.

Generating a Packet Capture File

To generate a packet capture file with tcpdump, perform the following steps:

Step 1 Choose **O&M** > **Network Diagnosis** > **Tcpdump**.

Figure 9-7 Network diagnosis – tcpdump



Network Diagnosis

Item	Value
Interface	Management Interface ▾
Source/Destination IP	
Protocol	Unlimited ▾
Max Captured Packets	(1~10000)
	OK

Status	tcpdump Stop	Refresh
□Select All	Filename	Size(bytes)

Delete

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.

----End

Downloading 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.

Deleting 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.

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 communication parameters of the console port, 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.*

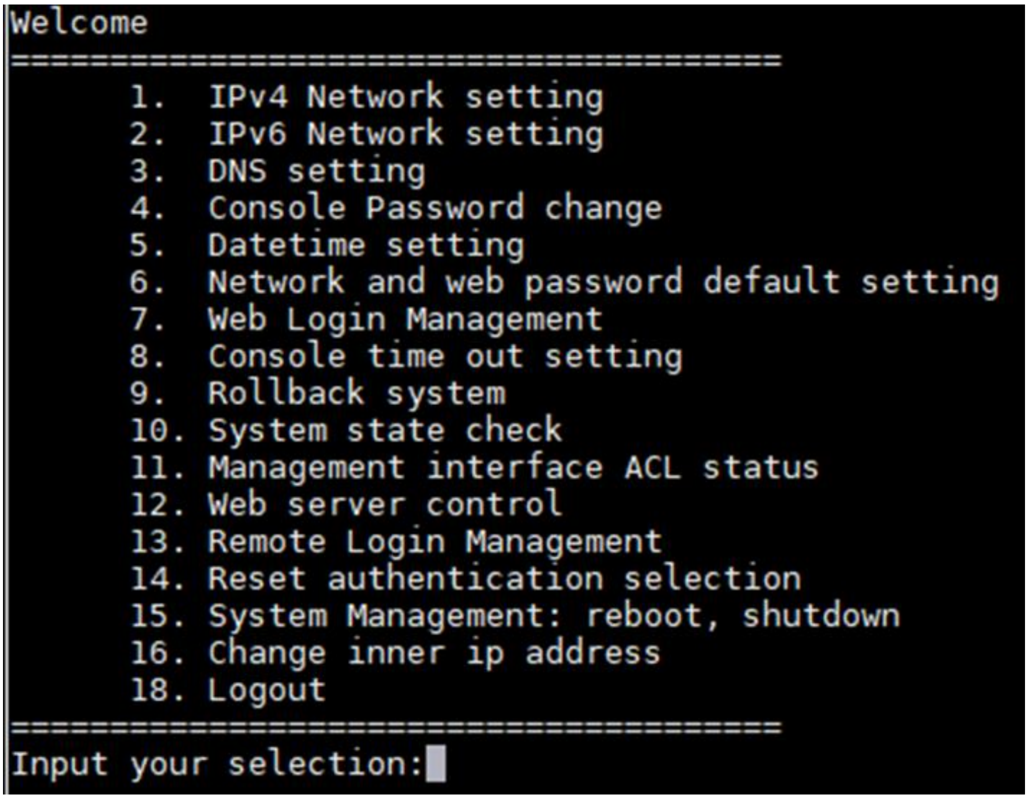
----End

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



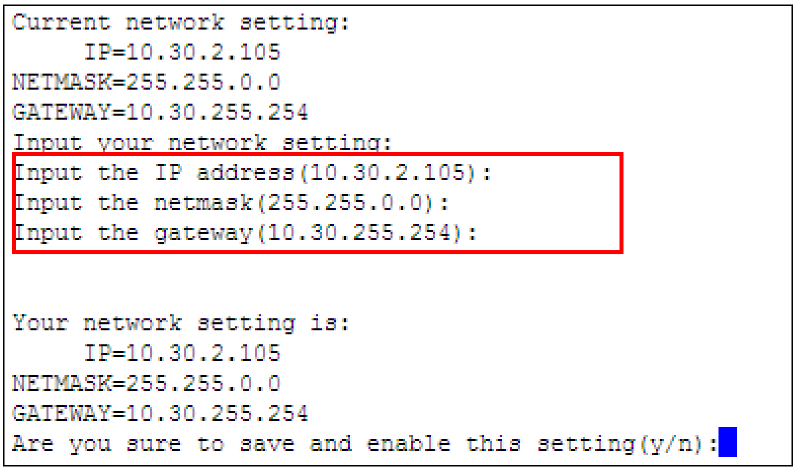
```
Welcome
=======================================
      1.  IPv4 Network setting
      2.  IPv6 Network setting
      3.  DNS setting
      4.  Console Password change
      5.  Datetime setting
      6.  Network and web password default setting
      7.  Web Login Management
      8.  Console time out setting
      9.  Rollback system
      10. System state check
      11. Management interface ACL status
      12. Web server control
      13. Remote Login Management
      14. Reset authentication selection
      15. System Management: reboot, shutdown
      16. Change inner ip address
      18. Logout
=======================================
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 window. 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



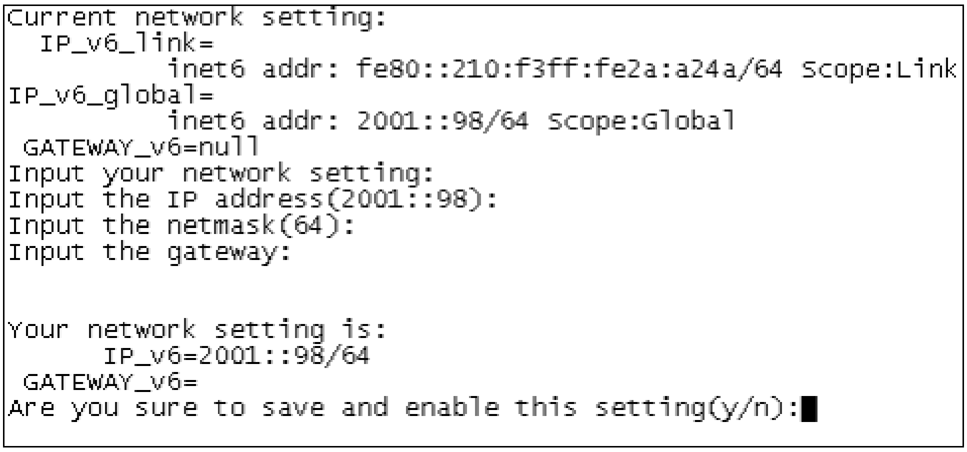
```
Current network setting:
     IP=10.30.2.105
NETMASK=255.255.0.0
GATEWAY=10.30.255.254
Input your network setting:
Input the IP address(10.30.2.105):
Input the netmask(255.255.0.0):
Input the gateway(10.30.255.254):


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 window. 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



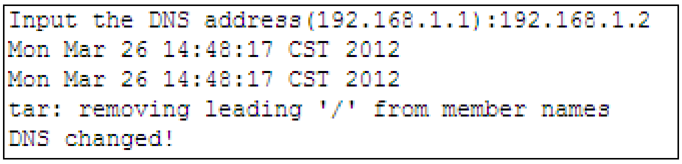
```
Current network setting:
  IP_v6_link=
          inet6 addr: fe80::210:f3ff:fe2a:a24a/64 Scope:Link
IP_v6_global=
          inet6 addr: 2001::98/64 Scope:Global
 GATEWAY_v6=null
Input your network setting:
Input the IP address(2001::98):
Input the netmask(64):
Input the gateway:


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 window.

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!
```

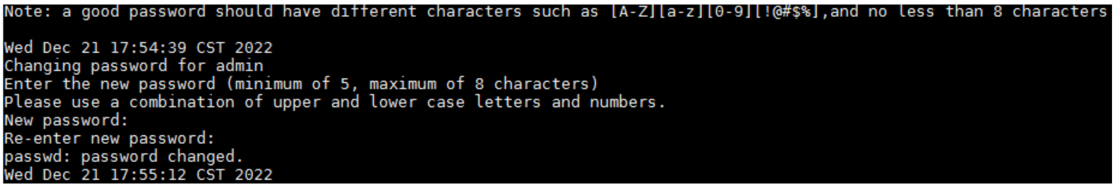
10.2.4 Changing the Console Password

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.

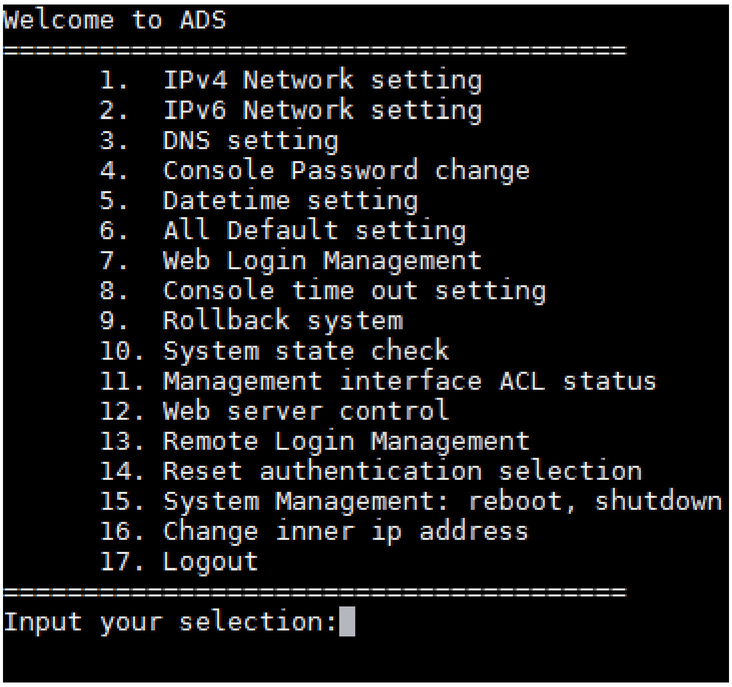
After the password is changed, the main menu is changed, as shown in Figure 10-6.

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

Wed Dec 21 17:54:39 CST 2022
Changing password for admin
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
passwd: password changed.
Wed Dec 21 17:55:12 CST 2022
```

Figure 10-6 Main menu after the password is changed



```
Welcome to 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 Login Management
      8.  Console time out setting
      9.  Rollback system
      10. System state check
      11. Management interface ACL status
      12. Web server control
      13. Remote Login Management
      14. Reset authentication selection
      15. System Management: reboot, shutdown
      16. Change inner ip address
      17. Logout
=======================================
Input your selection:
```

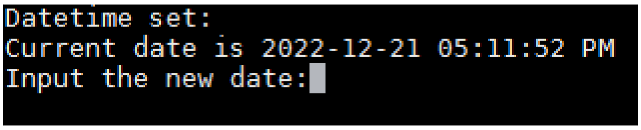
Note	Please set the login password of the console as prompted. See appendix *B* Default Parameters for the initial account of the console.

10.2.5 Setting System Time

On the main menu, type **5** and press **Enter** to set system time, as shown in Figure 10-7.

Type the new system date and time (format: 2022-12-21 05:12:52), and then press **Enter** to save the settings and return to the main menu.

Figure 10-7 Setting system time



```
Datetime set:
Current date is 2022-12-21 05:11:52 PM
Input the new date:
```

Caution	Changing system time may interrupt BGP routes and suspend traffic diversion. Please handle with caution.

10.2.6 Restoring Network and Web Password to Default Settings

On the main menu, type **6** and press **Enter** to restore the network settings and password of the web administrator to default settings. This operation takes effect immediately.

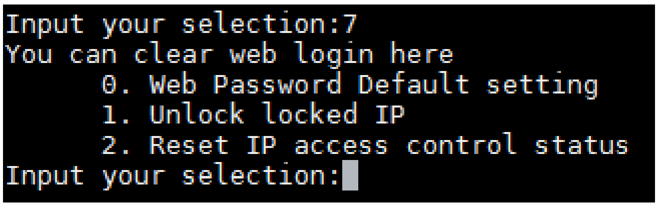
Note that the IP address of the management interface is restored as follows:

- If the management interface is configured with an IPv6 address, the IPv6 address is cleared.
- If the management interface has been configured with a new IPv4 address, this address will be cleared and the factory default is restored.

10.2.7 Setting Web Login

On the main menu, type **7** and press **Enter** to clear web login settings, as shown in Figure 10-9.

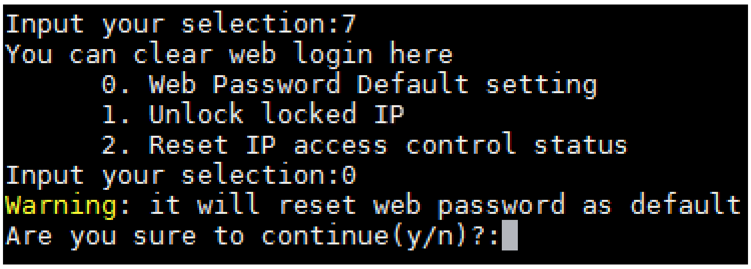
Figure 10-8 Web login management



```
Input your selection:7
You can clear web login here
      0. Web Password Default setting
      1. Unlock locked IP
      2. Reset IP access control status
Input your selection:
```

- Type **0**, type **y** as prompted, and press **Enter** to restore the initial password, **nsfocus**.

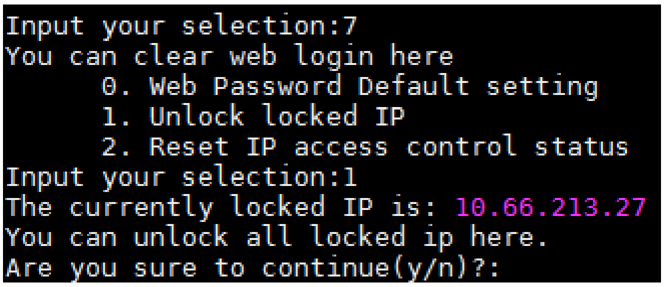
Figure 10-9 Restoring the initial password of the web administrator



```
Input your selection:7
You can clear web login here
      0. Web Password Default setting
      1. Unlock locked IP
      2. Reset IP access control status
Input your selection:0
Warning: it will reset web password as default
Are you sure to continue(y/n)?:
```

- Type **1**, type **y** as prompted, and press **Enter** to unlock the locked IP addresses.

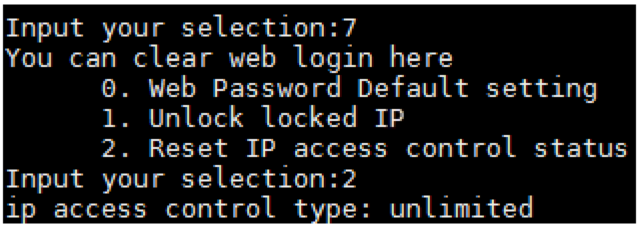
Figure 10-10 Unlocking the locked IP addresses



```
Input your selection:7
You can clear web login here
      0. Web Password Default setting
      1. Unlock locked IP
      2. Reset IP access control status
Input your selection:1
The currently locked IP is: 10.66.213.27
You can unlock all locked ip here.
Are you sure to continue(y/n)?:
```

- Type **2**, type **y** as prompted, and press **Enter** to reset the IP access control status to "unlimited".

Figure 10-11 Resetting IP acccess control status

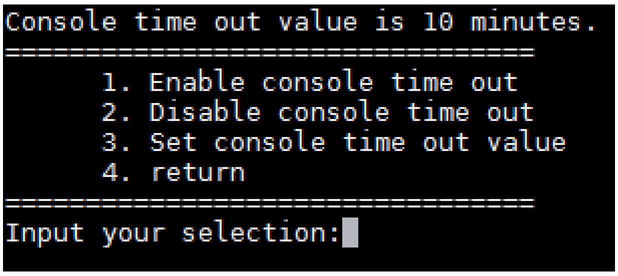


```
Input your selection:7
You can clear web login here
      0. Web Password Default setting
      1. Unlock locked IP
      2. Reset IP access control status
Input your selection:2
ip access control type: unlimited
```

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 10-12 Setting the console timeout value



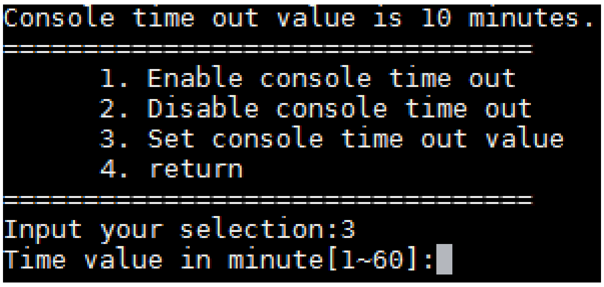
```
Console time out value is 10 minutes.
=================================
      1. Enable console time out
      2. Disable console time out
      3. Set console time out value
      4. return
=================================
Input your selection:
```

In the window shown in Figure 10-13, 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 10-13 Setting the 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:3
Time value in minute[1~60]:
```

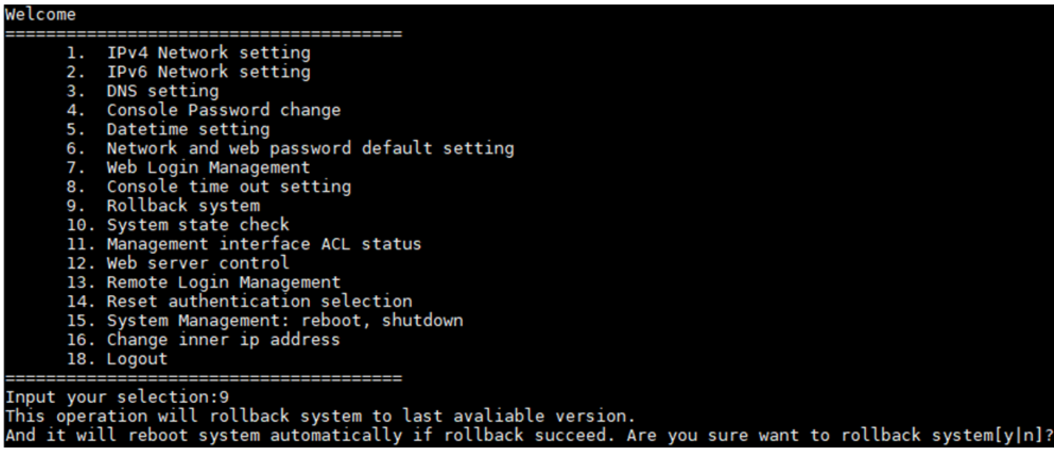
- Type **4** and press **Enter** to return to the main menu.

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 10-14 Rolling back the version



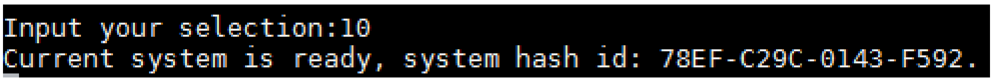
```
Welcome
======================================
      1.  IPv4 Network setting
      2.  IPv6 Network setting
      3.  DNS setting
      4.  Console Password change
      5.  Datetime setting
      6.  Network and web password default setting
      7.  Web Login Management
      8.  Console time out setting
      9.  Rollback system
      10. System state check
      11. Management interface ACL status
      12. Web server control
      13. Remote Login Management
      14. Reset authentication selection
      15. System Management: reboot, shutdown
      16. Change inner ip address
      18. Logout
======================================
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]?
```

In the window shown in Figure 10-14, 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 10-15, the system information shows that the system is normally started. This function is used to check the startup status of the device.

Figure 10-15 Viewing system information

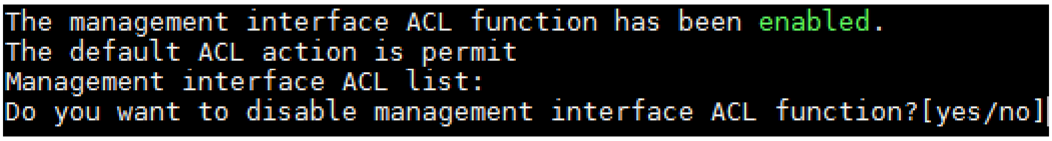


```
Input your selection:10
Current system is ready, system hash id: 78EF-C29C-0143-F592.
```

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 10-16 Configuring the management interface access control function



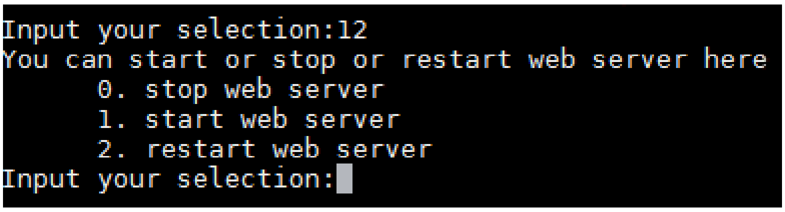
```
The management interface ACL function has been enabled.
The default ACL action is permit
Management interface ACL list:
Do you want to disable management interface ACL function?[yes/no]
```

In the window shown in Figure 10-16, 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 Configuring the Web Server Control Function

On the main menu, type **12** and press **Enter** to open the web server control window.

Figure 10-17 Managing the web server



```
Input your selection:12
You can start or stop or restart web server here
      0. stop web server
      1. start web server
      2. restart web server
Input your selection:
```

In the window shown in Figure 10-17, you can perform the following operations:

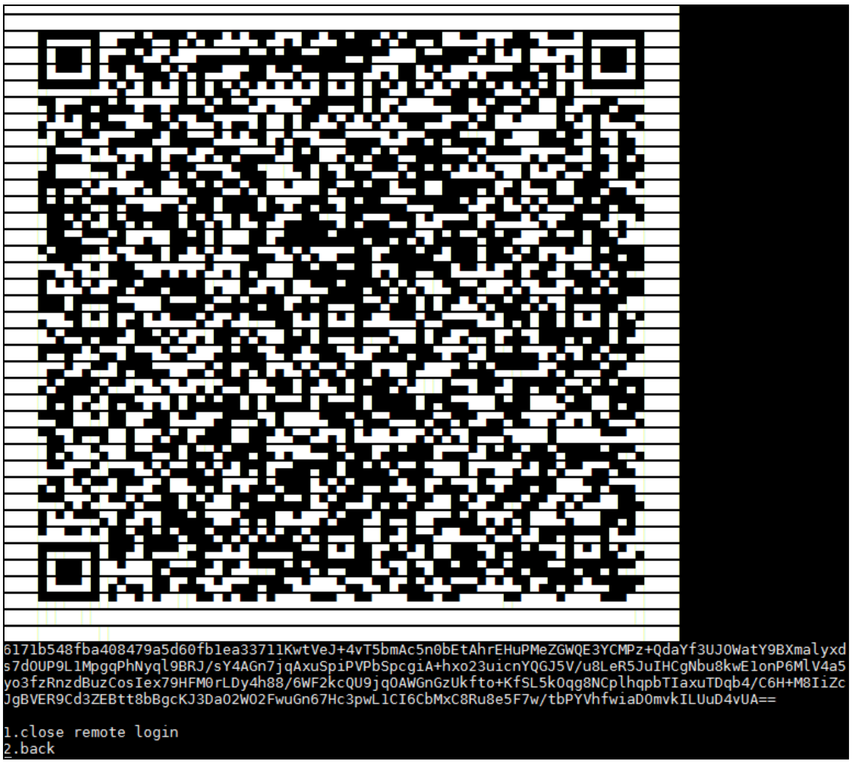
- Type **0** and press **Enter** to stop the web server.
- Type **1** and press **Enter** to start the web server.
- Type **2** and press **Enter** to restart the web server.

10.2.13 Configuring Remote Assistance

On the main menu, type **13** and press **Enter** to open the remote assistance configuration window. Type at most three allowed IP addresses.

As shown in Figure 10-18, this window shows the key for remote login and QR code of the key.

Figure 10-18 Configuring remote assistance



```
6171b548fba408479a5d60fb1ea33711KwtVeJ+4vT5bmAc5n0bEtAhrEHuPMeZGWQE3YCMPz+QdaYf3UJOWatY9BXmalyxd
s7dOUP9L1MpgqPhNyql9BRJ/sY4AGn7jqAxuSpiPVPbSpcgiA+hxo23uicnYQGJ5V/u8LeR5JuIHCgNbu8kwE1onP6MlV4a5
yo3fzRnzdBuzCosIex79HFM0rLDy4h88/6WF2kcQU9jqOAWGnGzUkfto+KfSL5kOqg8NCplhqpbTIaxuTDqb4/C6H+M8IiZc
JgBVER9Cd3ZEBtt8bBgcKJ3DaO2WO2FwuGn67Hc3pwL1CI6CbMxC8Ru8e5F7w/tbPYVhfwiaDOmvkILUuD4vUA==

1.close remote login
2.back
```

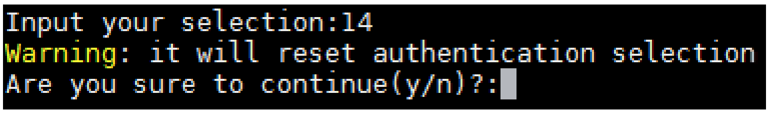
In the window shown in Figure 10-18, you can perform the following operations:

- Type **1** and press **Enter** to disable remote assistance.
- Type **2** and press **Enter** to return to the main menu.

10.2.14 Resetting the Authentication Mode

On the main menu, type **14** and press **Enter** to open the vADS authentication resetting window, as shown in Figure 10-19.

Figure 10-19 Resetting the vADS authentication mode



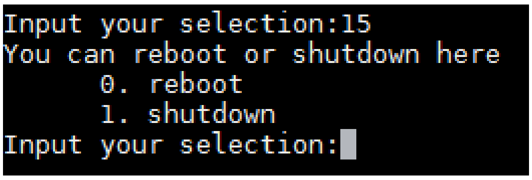
```
Input your selection:14
Warning: it will reset authentication selection
Are you sure to continue(y/n)?:
```

In the window shown in Figure 10-19, type **y** and press **Enter** to reset the vADS authentication mode or type **n** and press **Enter** to return to the previous menu, with the current configuration unchanged.

10.2.15 Restarting or Shutting Down the System

On the main menu, type **15** and press **Enter** to open the system management window.

Figure 10-20 Managing the system

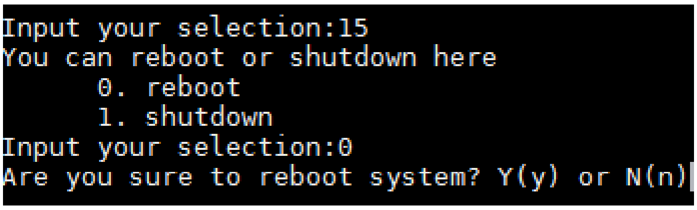


```
Input your selection:15
You can reboot or shutdown here
      0. reboot
      1. shutdown
Input your selection:
```

Restarting the System

In the window shown in Figure 10-20, type **0 and press Enter to open the system restart setting window.**

Figure 10-21 System restart setting window



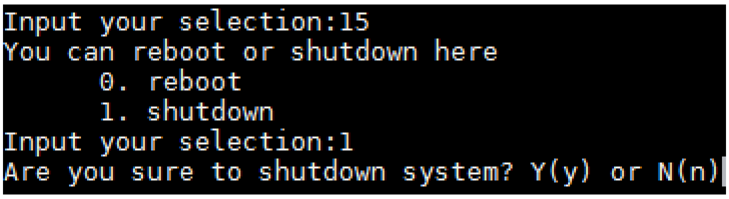
```
Input your selection:15
You can reboot or shutdown here
      0. reboot
      1. shutdown
Input your selection:0
Are you sure to reboot system? Y(y) or N(n)
```

In the window shown in Figure 10-21, type **y as prompted, and press Enter to restart the system.**

Shutting Down the System

In the window shown in Figure 10-20, type **1 and press Enter to open the system shutdown setting window.**

Figure 10-22 System shutdown setting window



```
Input your selection:15
You can reboot or shutdown here
      0. reboot
      1. shutdown
Input your selection:1
Are you sure to shutdown system? Y(y) or N(n)
```

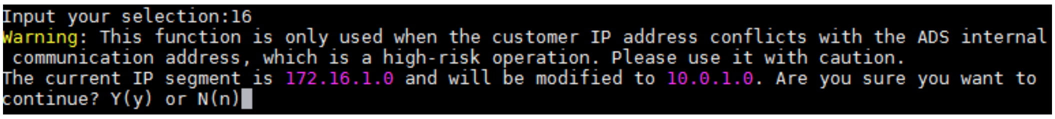
In the window shown in Figure 10-22, type **y as prompted, and press Enter to shut down the system.**

10.2.16 Changing Internal IP Address

This is a high-risk operation, which should be performed with caution. It is applicable only when the customer's IP address conflicts with vADS's IP address reserved for internal communication.

On the main menu, type **16** and press **Enter** to open the internal IP address change window.

Figure 10-23 Changing internal IP address



```
Input your selection:16
Warning: This function is only used when the customer IP address conflicts with the ADS internal
 communication address, which is a high-risk operation. Please use it with caution.
The current IP segment is 172.16.1.0 and will be modified to 10.0.1.0. Are you sure you want to
continue? Y(y) or N(n)
```

In the window shown in Figure 10-23, type **y** and press **Enter** to change vADS's internal IP address or type **n** and press **Enter** to return to the previous menu, with the current configuration unchanged.

10.2.17 Exiting the Console

On the main menu, type **17** and press **Enter** to log out of the console-based manager.

11 Initial Configuration

The device can operate properly after you complete simple network configuration and import a valid certificate. Network configuration involves the following:

- IP address
- Subnet mask
- Gateway
- DNS Server

Network configuration can be conducted on the console or the web-based manager. Both approaches require a computer and accessories (included in the accessory box). Choose an approach as required.

To perform configurations on the console, you need to connect the device to a computer with a console port cable. The console port rate of ADS devices is 115200 bps. After login, you can perform configurations by selecting menus. For details, see section 11.2 Network Configuration on the Console.

To perform configurations on the web-based manager, do as follows:

Step 1 Use a crossover cable (included in the accessory box) to connect the working interface on the device to the network interface on the computer.

Step 2 Configure computer-related parameters to make it in the same network segment as the device.

Step 3 Log in to the Web management interface through HTTPS and configure the device. For details, see sections 11.3 Login to Web-based Manager and 11.5 Network Configuration on the Web-based Manager.

----End

The certificate file can be imported only on the web-based manager. You are recommended to import a certificate file the first time you log in to the Web management interface.

11.1 Login to the Console

Before logging in to the console, the administrator needs 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

- Connect the ADS device and the computer by using a console cable.

Here, the terminal software included in a Microsoft Windows XP operating system is used as an example to detail the connection process:

If the user name and password are correct, the administrator will successfully log in to the console. An optimal display effect will be achieved for terminal ID VT100.

Note	After logging in to the console, you can only operate on the keyboard. Type a sequence number as prompted and press **Enter** to open the corresponding console management menu.

11.2 Network Configuration on the Console

After successful login, configure network parameters of the device as required.

Step 1 Configure the IP address. Since ADS devices support IPv4/IPv6 dual-stack, you can configure the IP address/subnet mask and IPv6 address/prefix length for the management interface.

- IPv4 address: On the main menu, type **1** and press **Enter** to configure the IPv4 address, subnet mask and gateway address as prompted. After confirming the settings, type **y** and press **Enter** to save the settings and return to the main menu.
- IPv6 address: On the main menu, type **2** and press **Enter** to configure the IPv6 address, prefix length and gateway address as prompted. After confirming the settings, type **y** and press **Enter** to save the settings and return to the main menu.

Step 2 On the main menu, type **3** and press **Enter** to configure the DNS server.

Step 3 After the configuration is complete, type **14** on the main menu and press **Enter** to log out of the console.

----End

11.3 Login to Web-based Manager

To log in to the web-based manager of the ADS device (here, an ADS NX5-4020 product is used as an example), perform the following steps:

Step 1 Verify that the client is connected to the Internet.

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

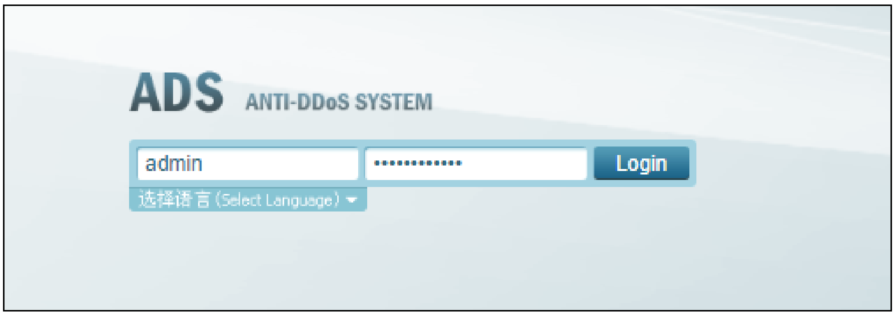
As the ADS device supports both IPv4 and IPv6 protocols, you can type an IPv4 address (for example, **https://192.168.1.100**) or IPv6 address (for example, **https://[2001::107]**).

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

Step 3 Click **Advanced** and then **Proceed to xxxx (unsafe)**.

Step 4 On the login page shown in Figure 11-1, select a language, type a correct user name and password, and click **Login** to log in to the web-based manager.

Figure 11-1 Login page



ADS ANTI-DDoS SYSTEM

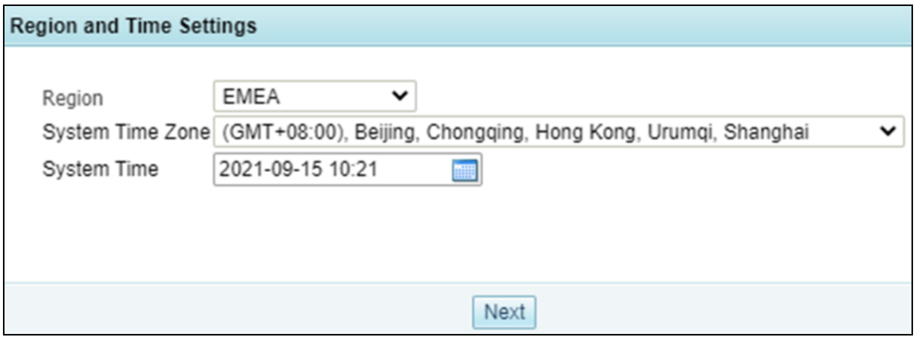
admin

••••••••••••

After a successful login, the web-based manager appears.

Step 5 On the homepage, set the user locality, system time zone, and system time.

Figure 11-2 Setting the country/region and time zone



Region and Time Settings

Region: EMEA

System Time Zone: (GMT+08:00), Beijing, Chongqing, Hong Kong, Urumqi, Shanghai

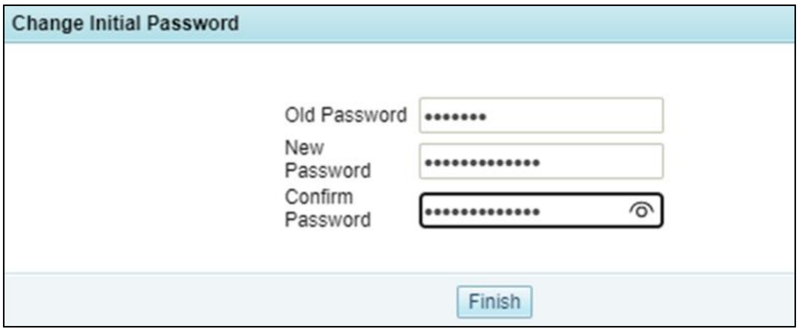
System Time: 2021-09-15 10:21

Step 6 Click **Next**.

The page for changing the initial password appears.

The new password must be a string of no less than 8 characters and contain at least two of the following character types: English letters, digits, and special characters.

Figure 11-3 Changing the initial password



Change Initial Password

Old Password: •••••••

New Password: ••••••••••••••

Confirm Password: ••••••••••••••

Step 7 After changing the initial password, click **Finish** to make the settings take effect. The web-based manager appears.

----End

Note	
	- You are advised to use Chrome, with the 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 IE core (such as Opera), pages may be displayed improperly. - Before login, check whether **Block all pop-ups** is selected. 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 of the user name or password. - During your first login, the system prompts a dialog box of changing the password. You can proceed only after successfully changing the password. The new password cannot be the same as the default password. - The system will return to the login page if a user is idle for the period specified by **Auto Idle Logou**t. After that, the user needs to log in again if the user wants to perform operations. - You need to import the license after the first login. For details, refer to the NSFOCUS ADS User Guide.

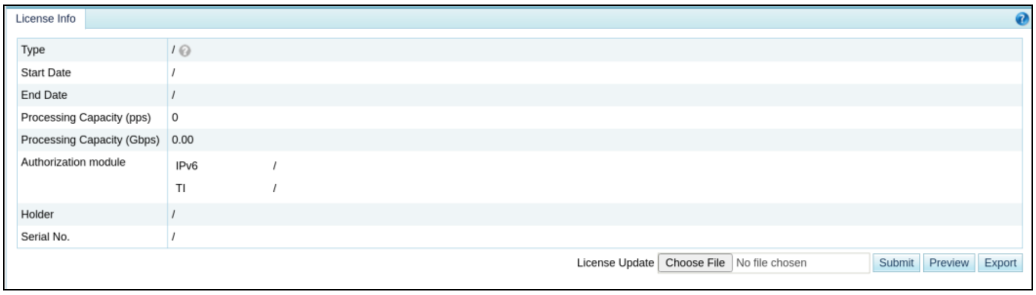
11.4 Importing a License

After logging in to an ADS device, you must import a license before using it.
To import a license, perform the following steps:

Step 1 Choose **System** > **Others** > **License Info**.

Figure 11-5 shows the license page.

Figure 11-4 License page before the import of a license



License Info

Type	/
Start Date	/
End Date	/
Processing Capacity (pps)	0
Processing Capacity (Gbps)	0.00
Authorization module	IPv6 / TI /
Holder	/
Serial No.	/

Step 2 Click **Choose File** to browse to an ADS license file.

Note	
	To get an ADS license file, please contact technical support personnel of NSFOCUS.

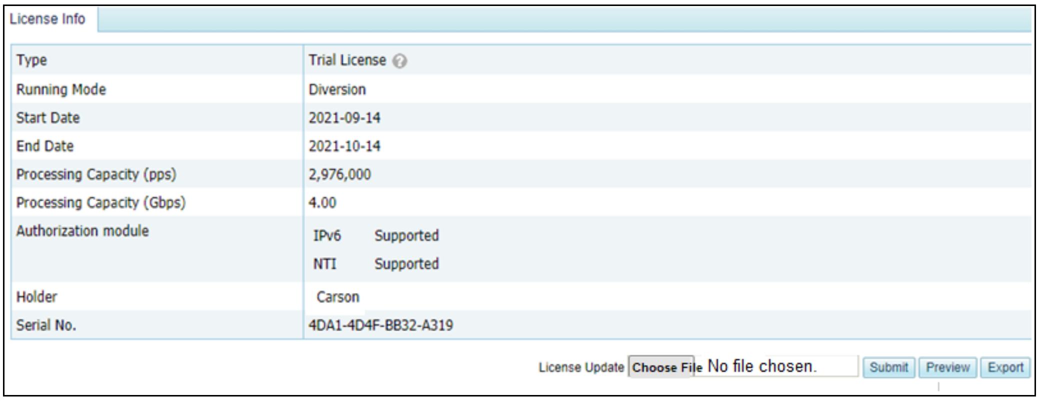
Step 3 Click **Submit** to import the license file.

A dialog box appears, asking you to confirm the terms and conditions for use of NSFOCUS products.

Step 4 Click **OK** in the dialog box to continue the license import.

The page after an import success is as shown in Figure 11-7.

Figure 11-5 Importing the license successfully



License Info

Type	Trial License
Running Mode	Diversion
Start Date	2021-09-14
End Date	2021-10-14
Processing Capacity (pps)	2,976,000
Processing Capacity (Gbps)	4.00
Authorization module	IPv6 Supported NTI Supported
Holder	Carson
Serial No.	4DA1-4D4F-BB32-A319

----End

11.5 Network Configuration on the Web-based Manager

The web-based manager enables you to configure network parameters as required.

Choose **System** > **Local Settings** > **Basic Settings**, and click **Edit** to configure network parameters. Then click **Save** at the upper-right corner of the page to make the configuration take effect.

After the configuration is complete, the device is ready for use.

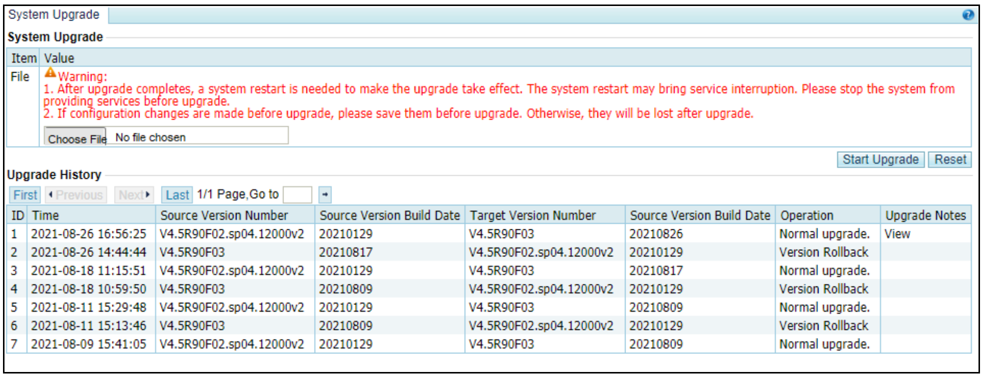
12 System Maintenance

12.1 System Upgrade

Timely system upgrade will increase the anti-attack capability. The system procedure is as follows:

Step 1 Choose **System** > **Others** > **System Upgrade** to open the system upgrade page, as shown in Figure 12-1.

Figure 12-1 System upgrade



System Upgrade

System Upgrade

Item	Value
File	⚠Warning: 1. After upgrade completes, a system restart is needed to make the upgrade take effect. The system restart may bring service interruption. Please stop the system from providing services before upgrade. 2. If configuration changes are made before upgrade, please save them before upgrade. Otherwise, they will be lost after upgrade. Choose File No file chosen

Upgrade History

ID	Time	Source Version Number	Source Version Build Date	Target Version Number	Source Version Build Date	Operation	Upgrade Notes
1	2021-08-26 16:56:25	V4.5R90F02.sp04.12000v2	20210129	V4.5R90F03	20210826	Normal upgrade.	View
2	2021-08-26 14:44:44	V4.5R90F03	20210817	V4.5R90F02.sp04.12000v2	20210129	Version Rollback	
3	2021-08-18 11:15:51	V4.5R90F02.sp04.12000v2	20210129	V4.5R90F03	20210817	Normal upgrade.	
4	2021-08-18 10:59:50	V4.5R90F03	20210809	V4.5R90F02.sp04.12000v2	20210129	Version Rollback	
5	2021-08-11 15:29:48	V4.5R90F02.sp04.12000v2	20210129	V4.5R90F03	20210809	Normal upgrade.	
6	2021-08-11 15:13:46	V4.5R90F03	20210809	V4.5R90F02.sp04.12000v2	20210129	Version Rollback	
7	2021-08-09 15:41:05	V4.5R90F02.sp04.12000v2	20210129	V4.5R90F03	20210809	Normal upgrade.	

Step 2 Click **Choose File**, select an upgrade package, and then click **Start Upgrade**.

Note

During the upgrade, you need to wait patiently until a message indicating successful upgrade appears.

Step 3 On receiving a successful upgrade message, restart the system without clicking **Save**.

Step 4 View version information to confirm upgrade success.

Re-log in to the system, choose **System** > **Others** >**Version Info**, and view the version number; or you can view the current version information in the **Upgrade History** table in the **System Upgrade** page shown in Figure 12-1.

Note	If problems emerge after upgrade and version rollback is needed, the version can only be rolled back to the source version. For detailed rollback operations, please contact technical support personnel of NSFOCUS.

----End

12.2 Common Troubleshooting

12.2.1 Web Login Failure

Symptom

Fail to access the web-based manager after the manager is installed.

Troubleshooting

Check whether the network connection between the client and the device management port is restricted by a firewall. If so, make sure that port 443 of the ADS device is accessible.

12.2.2 Device Access Failure

Symptom

The device is not accessible though its threshold is not triggered yet.

Troubleshooting

- Check whether the device that is directly connected with the ADS has a hub or not. A hub could degrade performance and should be replaced by a switch.
- Check whether the parameters about attack protection rules are too strictly configured.
- Check whether the IP protection rules have restrictions on the IP address.

12.2.3 License Import Failure

Symptom

Fail to import a license.

Troubleshooting

If the license complies with the device model, check the following:

- The production date of the new license must be later than the original one.
- The expiry date of the new license must be later than the original one.

You can import license successfully only when both the preceding conditions are satisfied.

Once a new license is imported, you are barred from importing old licenses. To use such old ones, you need to reapply them.

12.2.4 MAC Address Learning Failure

Symptom

When connected with a router, neither the router nor the device can learn the MAC address.

Troubleshooting

Check the following:

- Check whether IP addresses of the two devices are in the same network segment, whether the IP configuration is incorrect, or whether the interface is not shut down.
- If the connected interface is an optical port, change the optical module or the optical fiber. There once was a MAC learning problem caused by the optical module with too high power. Changing an optical module addressed the problem.
- If the connected interface is an electrical port, set the two ends to the same negotiation mode and speed.
- If the problem persists, contact NSFOCUS technical support engineers.

12.2.5 Ping Failure or Excessive Packets Drop

Symptom

The device does not answer pinging or too many packets are dropped.

Troubleshooting

Check the following from lower layers to high layers:

- Check the working mode and current state of the NIC to determine whether connections are proper.
- Set the operating mode of the device to packet forwarding mode to determine whether the device software operates properly.

Remove the device and detect packet loss on uplink and downlink devices to determine whether the device operates properly.

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 Parameters of the Management Interface

Management IP Address	192.168.1.100
Netmask	255.255.255.0
Default Gateway	192.168.1.1
Reserved IP Segment for Internal Communication	172.16.1.0/24

B.2 Default Account of the Web Administrator

User Name	admin
Password	nsfocus

B.3 Default Account of the Console Administrator

User Name	admin
Password	nsfocus

B.4 Default Account of the CLI Administrator

User Name	routerman

B.5 Communication Parameters of the Console Port

Baud Rate	115200

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	√	√

Module	Function	IPv4	IPv6
	UDP protection – traffic control by Src IP	√	√
	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	√	√
	Blocklist	√	√
	Allowlist	√	√
	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	√	√
	RIP	√	√
	LDP	√	×
	IP route assignment	√	√

Module	Function	IPv4	IPv6
	Injection interface	√	√
	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	√	√

Module	Function	IPv4	IPv6
	Configuration file management	√	√
	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 inspection	—	—
	Version information	—	—
Advanced	Packet capture management	√	√
	Pattern matching rules	√	√
NTI	Upload	√	√
	Synchronization	√	×
	Query	√	×

D NSFOCUS MASTER TERMS AND CONDITIONS

NOTE: IF LICENSEE HAS SIGNED A SEPARATE AGREEMENT WITH NSFOCUS FOR THE PRODUCTS AND SERVICES COVERED BY THIS AGREEMENT, THE TERMS OF SUCH SIGNED AGREEMENT SHALL GOVERN.

YOU SHOULD CAREFULLY READ THE FOLLOWING MASTER TERMS AND CONDITIONS ("**TERMS**") BEFORE INSTALLING AND/OR USING THE PRODUCTS OR SERVICES, THE USE OF WHICH ARE LICENSED BY NSFOCUS (AS DEFINED IN SECTION 11.7) AND ITS AFFILIATES ("**NSFOCUS**") FOR USE ONLY AS SET FORTH BELOW. INSTALLING OR OTHERWISE USING ANY PART OF THE PRODUCTS OR RECEIVING SERVICES INDICATES THAT YOU, ON BEHALF OF YOURSELF AND ANY ENTITY BY WHOM YOU ARE EMPLOYED OR FOR WHOM YOU ARE USING THESE PRODUCTS OR SERVICES ("**LICENSEE**") ACCEPTS THE TERMS OF THE AGREEMENT. YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THE AGREEMENT AND THAT "YOU" AND "YOUR" WILL REFER TO THAT COMPANY OR ORGANIZATION. IF YOU DO NOT AGREE TO THE TERMS OF THE AGREEMENT OR DO NOT HAVE THE AUTHORITY SPECIFIED ABOVE, DO NOT INSTALL OR OTHERWISE USE THE PRODUCTS OR SERVICES AND RETURN THE UNUSED PRODUCTS TO NSFOCUS OR THE RESELLER WHERE YOU OBTAINED THEM.

1. DEFINITIONS

1.1 "*Agreement*" means these Master Terms, the Order, the Cloud Services Terms of Use (if applicable), any Statement of Work (if applicable), and any other document referenced therein.

1.2 "*Appliance(s)*" means the hardware device containing the Software as specified in the Order.

1.3 "*Confidential Information*" means all confidential and proprietary information of a party ("**Disclosing Party**") disclosed to the other party ("**Receiving Party**"), whether orally or in writing, that is identified as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including but not limited to the terms of this Agreement and any pricing. The Software, Documentation, Deliverables, and all proprietary information embedded in the Appliance, is the Confidential Information of NSFOCUS, regardless of marking.

1.4 "*Deliverables*" means all training materials and results of Professional Services provided by NSFOCUS to Licensee pursuant to a Statement of Work (excluding any Licensee Confidential Information).

1.5 "*Documentation*" means the description of the Software and Appliance provided by NSFOCUS to Licensee and the user manuals relating to their use that are provided on-line at the time of Licensee's purchase or license, embedded in the Software, or delivered with the Software or Appliance.

1.6 "*Open Source Software*" or "*OSS*" means software components that are licensed under a license approved by the Open Source Initiative ("OSI") or similar open source or freeware license and are embedded in or provided with the Products.

1.7 "*Order*" means an order that includes a description of Products and Services to be licensed or purchased by Licensee.

1.8 "*Products*" means the Software, Documentation, and Appliance specified in the Order and any Updates thereto.

1.9 "*Professional Services*" means those training and implementation services which may be provided by NSFOCUS as described in a SOW.

1.10 "*Reseller*" means a third-party authorized by NSFOCUS to resell or sublicense Products and Services directly to Licensee.

1.11 "*Services*" means Support and Professional Services.

1.12 "*Software*" means NSFOCUS's proprietary software program(s) described in the Order, in binary or object code form, and any Updates thereto.

1.13 "*Statement of Work*" or "*SOW*" means a mutually agreed upon description of the Professional Services to be provided by NSFOCUS which is attached to an Order.

1.14 "*Support*" means NSFOCUS's standard support services which are available for the Products as specified by NSFOCUS from time to time.

1.15 "*Updates*" means releases and error corrections to the Products that are generally provided by NSFOCUS to customers receiving Support at no additional charge. Updates do not include releases, improvements, or enhancements for which NSFOCUS charges separately or extra as determined by NSFOCUS in its sole discretion.

2.LICENSES

2.1 *License Grant*. Subject to Licensee's compliance with these Master Terms, NSFOCUS hereby grants Licensee a personal, non-exclusive, non-transferable license during the term specified in the Order, without the right of sublicense, to use the Software and Appliance in accordance with the Documentation in the quantities specified in the Order, for Licensee's own internal business purposes.

2.2. *Restrictions*. Except for the limited license rights expressly granted in Section 2.1, NSFOCUS reserves all rights in and to the Products. Except as expressly permitted herein, Licensee shall not: (a) reproduce, modify, translate or create any derivative work of all or any portion of the Products, (b) sell, rent, lease, loan, provide, distribute or otherwise transfer all or any portion of the Product to a third party, (c) reverse engineer, reverse assemble or otherwise attempt to gain access to the source code of all or any portion of the Product (other than the Open Source Software) except to the extent expressly permitted by law, (d) remove, alter, cover, or obfuscate any copyright, trademark or other proprietary rights notices placed or embedded on or in the Products, (e) unbundle any components of the Software, (f) access a Product for the purpose of building a competitive product or service or copying its features or user interface, (g) use the Products to scan unauthorized computer systems or exploit the vulnerability scanned by the Products to intrude into unauthorized computer systems, or grant access to the vulnerability information scanned by the Products to any third party, or (h) cause or permit any third party to do any of the foregoing. In addition, Licensee shall not use the Products for the benefit of any third party, including but not limited to as an application service provider, for third-party training, or time-sharing or service bureau use. Notwithstanding the foregoing, Licensee may make a reasonable number of copies of the Software and Documentation for backup purposes, provided that such copies include all copyright and other intellectual property rights notices that appear on the original. If Licensee is a European Union ("**EU**") resident, information necessary to achieve interoperability of the Products with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available from NSFOCUS upon written request. If Licensee sells, leases, lends, rents, transfers, or otherwise distributes an Appliance to a third party, Licensee will ensure that it erases all copies of the Software from such Appliance.

2.3 *Open Source Software*. Notwithstanding anything herein to the contrary, Open Source Software is licensed to Licensee under such OSS's own applicable license terms, which can be found (a) in the open_source_licenses.txt file, (b) in the Documentation, (c) in the corresponding source files for the Software, or (d) on NSFOCUS's website. These OSS license terms are consistent with the license granted in Section **2**, and may contain additional rights benefiting Licensee. The OSS license terms shall take precedence over this Agreement to the extent that this Agreement imposes greater restrictions on Licensee than the applicable OSS license terms.

2.4 *Audit*. NSFOCUS reserves the right, upon reasonable prior notice to Licensee and during Licensee's normal business hours, to audit Licensee's use of the Products to verify compliance with this Agreement. Any such audit shall be performed by NSFOCUS or its authorized representative, shall not take place more than once per calendar year, and shall be done in a manner to minimize disruption to Licensee's business. In the event that any audit reveals noncompliance with this Agreement, including but not limited to use of the Products other than as specified herein, Licensee shall promptly pay NSFOCUS any shortfall plus accrued interest at NSFOCUS's current rates and shall reimburse NSFOCUS for the reasonable cost of such audit. This does not limit any other remedies that NSFOCUS may have under this Agreement or otherwise.

3. SERVICES

3.1 *Support*. Support may be purchased for one (1) year periods. Provided that Licensee has purchased Support, NSFOCUS will provide the Support specified in the applicable Order during the Support term.

3.2 *Professional Services*. Licensee may purchase Professional Services by executing a SOW with NSFOCUS for such Professional Services. Changes to a SOW are not binding unless and until an amendment to such SOW is executed by both parties.

3.2.1 NSFOCUS hereby provides Customer with a limited, non-exclusive, non-transferable and terminable license to use the Deliverables solely for Customer's internal operations in connection with its authorized use of the applicable Product. Training Deliverables may be used solely for Licensee's internal training purposes. Licensee is prohibited from: (a) modifying the training Deliverables, unless otherwise authorized in writing by NSFOCUS or set forth in the applicable SOW; (b) reselling or sublicensing any Deliverables; and (c) utilizing the training Deliverables to replicate or attempt to perform the training itself, unless otherwise authorized in writing by NSFOCUS or set forth in the applicable SOW; and (d) developing or attempting to develop any of the products described in the Deliverables.

3.2.2 Where access to software licensed by third parties is required in order to allow NSFOCUS to perform the Professional Services, Licensee shall be responsible for ensuring that it has appropriate licenses from its vendors sufficient to allow NSFOCUS to perform such Professional Services. NSFOCUS shall only use such third party software in connection with its performance of Professional Services for Licensee.

4.LIMITED WARRANTIES AND DISCLAIMER

4.1. *Limited Warranty*. NSFOCUS warrants that the Appliance and Software (excluding OSS), as delivered, will perform substantially in accordance with the Documentation for a period of ninety (90) days from the date of delivery to Licensee. NSFOCUS makes no warranty that the operation of the Products will be uninterrupted or error-free, that the Products will meet Licensee's requirements, or that the Products will operate in combination with hardware or software not provided by NSFOCUS. In the event that the Software does not conform to the above warranty, NSFOCUS's entire liability and Licensee's sole remedy shall be for NSFOCUS to: (a) use its reasonable efforts to correct any reproducible error confirmed by NSFOCUS; or (b) at NSFOCUS's option, to accept return of the non-conforming Software and refund to Licensee the fees paid for such Software. In the event the Appliance does not conform to the above warranty, NSFOCUS's entire liability and Licensee's sole remedy shall be for NSFOCUS to provide a repaired or replacement Appliance to Licensee pursuant to NSFOCUS's then current RMA process. NSFOCUS's warranty shall not extend to errors that result from: (i) Licensee's failure to implement any Updates that are provided by NSFOCUS; (ii) use of the Products other than in accordance with the Documentation; (iii) any alterations of or additions or modifications to the Products performed by parties other than NSFOCUS or as authorized by NSFOCUS; (iv) use of the Products in a manner for which they were not designed or outside of the scope of this Agreement; (v) accident, negligence, or misuse of the Products by any party other than NSFOCUS; or (vi) combination of the Products with other products not supplied by NSFOCUS.

4.2 *Services Warranty*. NSFOCUS warrants that Services shall be performed in a professional manner in accordance with industry standards. NSFOCUS's ability to successfully perform hereunder is dependent upon Licensee's provision of timely information, access to resources, and participation. If through no fault or delay of Licensee the Services do not conform to the foregoing warranty, and Licensee notifies NSFOCUS within thirty (30) days of NSFOCUS's delivery of the Services, Licensee may require NSFOCUS to re-perform the non-conforming portions of the Services.

4.3 *Authority*. NSFOCUS warrants that it has full power and authority to enter into this Agreement without the consent of any other person or entity.

4.4 *Harmful Code*. For purposes of this warranty, "Harmful Code" shall include without limitation, any code containing viruses, Trojan horses, time bombs, worms or like destructive code or code that self-replicates or computer instructions, circuitry or other technological means designed to disrupt, damage or interfere with Licensee's authorized use of the Products or License's computers and communications facilities or equipment. NSFOCUS represents and warrants that it: (a) incorporates commercially reasonable measures to screen for Harmful Code, (b) has used commercially reasonable efforts, including the installation of industry standard anti-virus software, to ensure that the Products and Deliverables contain no Harmful Code at delivery and (c) uses commercially reasonable efforts to prevent the introduction of such Harmful Code into the Products and Deliverables. The following shall not be deemed Harmful Code: (i) a feature through the user interface that permits a user to access NSFOCUS's Web site through a browser over the Internet to access Support and/or to register the Products, or (ii) keys that de-activate evaluation copies of the Products after a period of time, making the Products unusable, or (iii) keys which limit the bandwidth for the use of the Products or Deliverables or otherwise prevent the Products or Deliverables from being used other than as specified in the Order.

4.5 *Open Source*. NSFOCUS represents and warrants that Licensee's use and operation of the Open Source Software in binary format, as delivered and when used solely for internal use as described in the Documentation, will not require the disclosure, licensing or assignment of Licensee's proprietary or third-party licensed software under any open source license(s).

4.6 ***Disclaimer of Warranties*.** EXCEPT AS EXPRESSLY SPECIFIED IN THIS SECTION 4, NSFOCUS AND ITS LICENSORS PROVIDE THE PRODUCTS, DELIVERABLES AND SERVICES "AS IS" AND EXPRESSLY DISCLAIM ANY WARRANTIES, TERMS OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO THE PRODUCTS, DELIVERABLES, OR ANY PART THEREOF OR ANY SERVICES PROVIDED HEREUNDER, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THOSE ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE.

4.7 *Licensee Warranties.* Licensee warrants that (a) it has the authority to enter into this Agreement and to comply with its obligations hereunder, and (b) it shall at all times fully comply with all laws and regulations applicable with respect to the use of the Products, Deliverables, and Services. Licensee remains responsible for (i) any data and the content Licensee makes available to NSFOCUS in connection with this Agreement, (ii) the selection and implementation of procedures and controls regarding access, security, encryption, use, and transmission of data, and (iii) backup and recovery of any database and any stored data. Licensee will not send or provide NSFOCUS with access to any personally-identifiable information, whether in data or any other form, and will indemnify and hold NSFOCUS harmless from any claims regarding personally-identifiable data.

5. LIMITATION OF LIABILITY

NSFOCUS AND ITS SUPPLIERS SHALL NOT BE LIABLE TO LICENSEE OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF USE, LOSS OF REVENUE OR ANTICIPATED PROFITS, BUSINESS DISRUPTION, LOST BUSINESS, OR DAMAGE TO SYSTEMS, DATA, OR PROGRAMS ARISING OUT OF THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE LIABILITY OF NSFOCUS AND ITS SUPPLIERS HEREUNDER SHALL IN NO EVENT EXCEED THE FEES PAID OR PAYABLE BY LICENSEE FOR THE PRODUCTS AND SERVICES. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE. THIS DISCLAIMER OF LIABILITY WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN FAILS OF ITS ESSENTIAL PURPOSE AND SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY LAW. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE FOREGOING LIMITATION MAY NOT APPLY TO LICENSEE.

6.PROPRIETARY RIGHTS

The Software, Documentation and Deliverables are licensed, not sold. All right, title and interest in and to the Software, Documentation, and Deliverables (excluding any Licensee Confidential Information), and in any ideas, know-how, and programs that may be developed by NSFOCUS in the course of providing Services, including any enhancements or modifications and all intellectual property rights embodied therein (other than Licensee's Confidential Information), will at all times remain the property of NSFOCUS or its licensors. Licensee hereby acknowledges that the Products, Deliverables, and Services are protected by laws pertaining to intellectual property and proprietary rights in the United States and other countries. Licensee is aware that this Agreement confers only the right to use the Products, Deliverables and Services during the applicable license term specified in the Order. It does not convey any rights of ownership in or to the Software, Documentation or Deliverables.

7.CONFIDENTIALITY

7.1. *Treatment of Confidential Information.* By virtue of this Agreement, either party may have access to the other party's Confidential Information. Receiving Party will protect Disclosing Party's Confidential Information with the same degree of care as it uses to protect its own Confidential Information of like kind, but in no event with less than a reasonable degree of care. Receiving Party will not use or disclose Disclosing Party's Confidential Information except as permitted in this Section or for the purpose of performing its obligations under this Agreement. Confidential Information may be disclosed only to employees or contractors of Receiving Party with a "need to know" and who are instructed and agree not to disclose the Confidential Information and not to use the Confidential Information for any purpose, except as set forth herein. Receiving Party shall have appropriate written agreements with any such employees or contractors sufficient to ensure compliance with the provisions of this Agreement. Receiving Party may disclose the Disclosing Party's Confidential Information to the extent such disclosure is required by order or requirement of a court, administrative agency, or other governmental body, provided that the Receiving Party provides prompt written notice thereof to the Disclosing Party (to the extent legally permitted) and assistance to enable the Disclosing Party to seek a protective order or otherwise prevent or restrict such disclosure. The confidentiality obligations of each party will survive expiration or termination of this Agreement for a period of three (3) years.

7.2. *Exclusions.* Confidential Information does not include information that: (a) is or becomes publicly available through no act or omission of the Receiving Party; (b) the Disclosing Party discloses to third parties without restriction on disclosure; (c) is disclosed to the Receiving Party by a third party without restriction on disclosure and without breach of a nondisclosure obligation; (d) is independently developed by the Receiving Party without use of or access to the Confidential Information of the Disclosing Party; or (e) is previously known to the Receiving Party without a nondisclosure obligation as evidenced by written records.

7.3. *Injunctive Relief*. It is understood and agreed that notwithstanding any other provision of this Agreement, a breach by either party of Section 7 may cause the other party irreparable damage for which recovery of money damages might be inadequate, and that the other party shall therefore be entitled to seek timely injunctive relief, without posting bond, to protect such party's rights under this Agreement in addition to any and all remedies available at law.

7.4 *Return of Confidential Information.* On Disclosing Party's written request or upon expiration or termination of this Agreement for any reason, the Receiving Party will promptly return or destroy, at Disclosing Party's option, all Confidential Information of Disclosing Party, in any form or media, and provide a written statement to Disclosing Party certifying the return or destruction of such Confidential Information. Notwithstanding the foregoing, in no event shall NSFOCUS be permitted to request the return of Products or Deliverables, except in connection with the termination or expiration of this Agreement or the applicable license.

8.INTELLECTUAL PROPERTY RIGHT INDEMNITY

8.1 *Indemnity*. NSFOCUS shall indemnify, hold harmless, and defend Licensee and its officers, directors, and employees from and against all claims, demands, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) to the extent arising from a claim brought by a third party that the Products, as delivered to Licensee and used as licensed hereunder infringes any (a) copyright, trademark or trade secret of a third party or (b) patent enforceable within the United States, Canada, United Kingdom, Germany, Japan or Singapore. Licensee shall provide NSFOCUS with (i) prompt written notice of any such claim or action, (ii) sole control and authority over the defense or settlement of such claim or action, and (iii) reasonable information and assistance to settle and/or defend any such claim or action at NSFOCUS's expense. Should the Products become, or in NSFOCUS's opinion be likely to become, the subject of such a claim, or in the event NSFOCUS wishes to minimize its potential liability hereunder, NSFOCUS shall, at its option and expense: (i) procure for Licensee the right to continue to use the Products as provided herein, (ii) replace the Products with non-infringing, functionally equivalent products; or (iii) suitably modify the Product so that it is not infringing. In the event that none of the foregoing can be achieved using reasonable efforts, then NSFOCUS, at its option, may terminate the licenses for the affected Product (or portion thereof) and refund the fees paid for such Product (or portion thereof) to Licensee, amortized over a three (3) year period on a straight-line basis.

8.2 *Exclusions*. NSFOCUS shall have no obligation with respect to any claim, action or proceeding to the extent arising from: (a) modification of the Products by anyone other than NSFOCUS or its Resellers, (b) use of the Products in combination or conjunction with any equipment, data, devices or software not provided by NSFOCUS wherein the absence of such combination the applicable Product would not have been infringing, (c) use of a Product in a manner other than for which it was intended or outside the scope of this Agreement, or (d) use of other than the then-most current release of the Software if such infringement or claim would have been prevented by the use of such current release.

THE PROVISIONS OF THIS SECTION 8 SET FORTH NSFOCUS'S SOLE AND EXCLUSIVE OBLIGATIONS, AND LICENSEE'S SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF ANY KIND.

9.TERM AND TERMINATION.

9.1. *Term*. This Agreement shall continue in effect until terminated.

9.2. *Termination for Cause*. Either party will have the right to terminate this Agreement if the other party (a) fails to perform any material obligation and fails to cure such breach within thirty (30) days after notice of breach is given, (b) ceases to function as a going concern or to conduct operations in the normal course of business or (c) has a petition filed by or against it under any state, federal or national bankruptcy or insolvency law, which petition has not been dismissed or set aside within sixty (60) days of its filing.

9.3. *Effect of Termination or Expiration*. Upon termination or expiration of this Agreement or applicable license term, Licensee shall immediately cease using the Confidential Information, Products and Deliverables provided under this Agreement and/or the applicable Order and within thirty (30) days thereafter, return to NSFOCUS or destroy all copies of the Confidential Information, Products and Deliverables (including copies in any storage media), and provide written confirmation thereof. This requirement applies to all copies in any form, partial or complete, and whether or not merged into other materials.

9.4. *Survival*. The obligations contained in the following Sections will survive termination of this Agreement for any reason: Sections 2.2, 2.3, 2.4, 4.6, 5, 6, 7, 8, 9 and 11.

10. PUBLICITY.

Licensee agrees that NSFOCUS may identify Licensee as a customer of NSFOCUS in NSFOCUS's marketing materials and on NSFOCUS's website. NSFOCUS may not issue any press release using Licensee's name or logo without Licensee’s prior written consent, such consent not to be unreasonably withheld.

11. GENERAL

11.1. *Assignment*. This Agreement may not be assigned by Licensee, by operation of law or otherwise, without the prior written consent of NSFOCUS, such consent not to be unreasonably withheld.

11.2. *Legal Expenses*. In any action to enforce this Agreement, the prevailing party shall be entitled to seek recovery of all court costs and reasonable attorneys' fees incurred, including such costs and attorneys' fees incurred in enforcing and collecting any judgment.

11.3. *Severability.* If any provision of this Agreement is held to be invalid by a court of competent jurisdiction, then the remaining provisions shall nevertheless remain in full force and effect. The parties further agree to negotiate in good faith a valid and enforceable provision that most nearly effects the parties' intent and to be bound by the mutually agreed substitute provision.

11.4. *Force Majeure*. Except for the obligation to make payments, neither party shall be responsible for any delay in its performance due to causes beyond its reasonable control.

11.5. *Amendment and Waiver*. Any provision of this Agreement may be amended or modified and the observance of any provision of this Agreement may be waived (either generally or any particular instance either retroactively or prospectively) only with the written consent of both parties. In no event will the parties' execution of an Order be deemed an amendment, modification, or waiver of this Agreement. The failure of either party to enforce, or the delay by either party in enforcing, at any time any of the provisions of this Agreement shall not be deemed to be a waiver of the right of such party thereafter to enforce any such provisions.

11.6. *Parties, Governing Law and Jurisdiction*. The "NSFOCUS" entity that Licensee is contracting with under this Agreement, the law that will apply in any claim arising out of or in connection with this Agreement, and the exclusive venue to adjudicate any such claim, shall depend on where Licensee is domiciled as follows:

Licensee domiciled in:	**NSFOCUS Entity**	**Governing Law**	**Exclusive Venue**
Hong Kong or Macau	NSFOCUS Incorporated	Hong Kong	Final and binding arbitration conducted in English in Singapore at Singapore International Arbitration Centre ("SIAC") under its rules as may be modified by this Agreement.

Japan	NSFOCUS Incorporated	United States	Final and binding arbitration conducted in English in Singapore at Singapore International Arbitration Centre ("SIAC") under its rules as may be modified by this Agreement.
Asia/Pacific (excluding Japan, Hong Kong and Macau)	NSFOCUS Technologies (S) Pte. Ltd.	Singapore	Final and binding arbitration conducted in English in Singapore at Singapore International Arbitration Centre ("SIAC") under its rules as may be modified by this Agreement.
Americas	NSFOCUS Incorporated	California	Final and binding arbitration conducted in Santa Clara, California under the Rules of the International Chamber of Commerce such rules may be modified by this Agreement
EMEA	NSFOCUS Technologies UK Limited	England and Wales	Final and binding arbitration conducted in London, England under the Rules of the International Chamber of Commerce as such rules may be modified by this Agreement

The United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer Information Transactions Act (UCITA) are specifically excluded.

11.7. *Notices*. Any notice required or permitted to be given under this Agreement shall be in writing and shall be delivered as follows with notice deemed given as indicated: (a) by personal delivery when delivered by hand, (b) by registered or certified mail, postage prepaid, return receipt requested, five (5) days after deposit in the mail, (c) by overnight courier upon written verification of receipt, or (d) by confirmed fax upon receipt. All notices must be sent to the address set forth in the applicable Order, with a copy sent to NSFOCUS at 690 N. McCarthy Blvd, Suite 170 Milpitas, CA 95035, Attn: VP, Finance and International Business.

11.8. *Relationship of the Parties*. The parties agree and acknowledge that the relationship of the parties is in the nature of an independent contractor. This Agreement shall not be deemed to create a partnership or joint venture and neither party is the other's agent, partner, employee, or representative. Neither party shall have the right to obligate or bind the other party in any manner whatsoever and nothing herein shall give or is intended to give any rights of any kind to third persons.

11.9. *Government Rights.* The Software and Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying, or disclosing of the Software or Documentation by the U.S. Government or other government entity shall be governed solely by the terms of this Agreement.

11.10. *Export Compliance.* Licensee acknowledges and agrees that the Products, Deliverables and related technology subject to this Agreement are subject to the export control laws and regulations of the United States, the European Union and other countries including U.S. embargo and sanctions regulations and prohibitions on export for certain end uses or to certain users. Licensee agrees to comply with all such laws and regulations. Licensee shall promptly advise NSFOCUS in writing of any known or suspected sale, transfer, or diversion in violation of the foregoing.

11.11. *Language*. The original of this Agreement is in English and Licensee waives any right to have it written in any other language.

11.12. *Entire Agreement*. This Agreement constitutes the entire, final, exclusive agreement between the parties and supersedes all previous agreements or representations, oral or written, relating to the subject matter of this Agreement.