

NSFOCUS ADS

User Guide



Version: V4.5R90F06 (2024-12-31)

Confidentiality: RESTRICTED

■ Copyright © 2024 NSFOCUS Technologies, Inc. All rights reserved.

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

■ 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	1
1 Introduction.....	5
1.1 Product Overview.....	5
1.2 Typical Deployment	5
1.2.1 In-Path Deployment	5
1.2.2 Out-of-Path Deployment.....	6
2 Web-based Manager	7
2.1 Login	7
2.2 System Users.....	9
2.3 Web Page Layout.....	10
2.4 Common Icons and Buttons	11
3 System Administration	12
3.1 Local Settings.....	12
3.1.1 Basic Information.....	12
3.1.2 Interface Configuration	16
3.1.3 User Management	18
3.1.4 Management Platform Configuration.....	21
3.1.5 Configuration File Management	24
3.1.6 Bandwidth Overrun Limit Configuration.....	25
3.1.7 Hardware Alert Thresholds	26
3.1.8 Management Interface Access Control	26
3.1.9 HA Configuration.....	29
3.1.10 (Optional) Bypass Configuration	40
3.1.11 Collaboration Configuration	44
3.2 Security Configuration	52
3.2.1 Login Security.....	52
3.2.2 Locked User Management	54
3.2.3 Authentication Configuration.....	54
3.3 Log Services.....	57
3.3.1 Syslog Configuration	57
3.3.2 SNMP Configuration	59
3.3.3 Email Configuration.....	63
3.3.4 SFTP/SSH Configuration.....	65

3.4 Others	66
3.4.1 License	66
3.4.2 System Upgrade	69
3.4.3 Remote Assistance	70
3.4.4 SSL Certificate Import	71
3.4.5 One-Click Inspection	71
3.4.6 System Information	72
3.4.7 Web API File Download	72
4 Real-Time Monitoring	73
4.1 Real-Time System Status	73
4.2 System Information	80
5 Policies	81
5.1 Anti-DDoS Policies	81
5.1.1 Protection Group Management	81
5.1.2 Policy Configuration for Protection Groups	96
5.1.3 Protection Group Policy Templates	127
5.1.4 Carpet Bombing Protection	130
5.1.5 Advanced Global Parameters	132
5.1.6 Response Page Settings	133
5.1.7 SSL Certificate Management	136
5.1.8 Mobile User-Agent Rules	138
5.2 Access Control Policies	139
5.2.1 Allowlist	139
5.2.2 Access Control Rules	145
5.2.3 Reflection Protection Rules	150
5.2.4 GeoIP Rules	152
5.2.5 Blocklist	155
5.2.6 HTTP Keyword Checking	162
5.2.7 SSL/TLS Keyword Checking	164
5.2.8 Connection Exhaustion Protection Rules	167
5.2.9 Regular Expression Rules	169
5.2.10 URL-ACL Protection Rules	171
5.2.11 DNS Keyword Checking	174
5.2.12 DNS Subdomain Allowlist	176
5.2.13 Programmable Rules	180
6 Diversion and Injection	182
6.1 General Settings	182
6.1.1 Running Mode	183
6.1.2 Port Channel Configuration	184
6.1.3 GRE Tunnel Configuration	187
6.1.4 IP Address Configuration	188

6.1.5 Incoming/Outgoing Configuration	191
6.2 Diversion Route	191
6.2.1 BGP Route	192
6.2.2 IP Route Assignment	195
6.3 Traffic Injection	196
6.3.1 Injection Interfaces	196
6.3.2 Injection Routes	198
6.3.3 MAC Address Table	209
6.4 Traffic Diversion	212
6.4.1 Filtering Rules	212
6.4.2 Manual Diversion	213
6.4.3 Group Diversion	219
6.4.4 Diversion Routing Table	220
6.5 Advanced Route Setting	222
6.5.1 MPLS Route	222
6.5.2 Other Routes	224
6.6 Syslog Diversion Configuration	227
6.6.1 Diversion Configuration	227
6.6.2 Diversion Rule List	229
7 Logs	230
7.1 Attack Logs	230
7.1.1 Attack Details	230
7.1.2 Statistical Chart	232
7.2 System Logs	232
7.2.1 System Operation Logs	233
7.2.2 System Login Logs	233
7.2.3 Link Status Logs	234
7.2.4 Traffic Diversion Logs	234
7.2.5 HA Synchronization Logs	235
7.2.6 Syslog Diversion Logs	235
7.2.7 Web API Logs	236
7.2.8 Authorization Configuration Logs	236
7.3 Log Analysis	236
7.4 Protection Logs	239
8 Advanced Applications	241
8.1 Packet Capture Management	241
8.1.1 Configuring Manual Packet Capture	241
8.1.2 Configuring Automatic Packet Capture	253
8.2 Pattern Matching Rules	258
8.2.1 Creating a Pattern Matching Rule	259
8.2.2 Creating Pattern Matching Rules in Batches	262

8.2.3 Enabling/Disabling Pattern Matching Rules	263
8.2.4 Modifying Pattern Matching Rules	264
8.2.5 Deleting Pattern Matching Rules	264
8.2.6 Viewing Pattern Matching Rules.....	264
8.3 Cloud Signaling.....	264
8.4 Collaboration with TI	269
8.4.1 TI Configuration	269
8.4.2 TI Application Effect and Query	270
8.4.3 TI Database Upgrade	271
8.4.4 IP Exceptions	272
9 Operation and Maintenance	273
9.1 Device Protection Status	273
9.1.1 Checking the Trust Status.....	273
9.1.2 Checking the Protection Status	274
9.2 Network Diagnosis.....	274
9.2.1 Ping	274
9.2.2 Port Check.....	275
9.2.3 Tcpdump	276
10 Console-based Management.....	278
10.1 Login to the Console	278
10.2 Details	279
10.2.1 Configuring IPv4 Network Settings	279
10.2.2 Configuring IPv6 Network Settings	280
10.2.3 Configuring DNS Settings	280
10.2.4 Changing the Console Password.....	281
10.2.5 Setting System Time	282
10.2.6 Restoring Network and Web Password to Default Settings	282
10.2.7 Setting Web Login.....	282
10.2.8 Setting the Console Timeout Value	283
10.2.9 Rolling Back the Version	284
10.2.10 Viewing System Information	285
10.2.11 Configuring the Management Interface Access Control Function	285
10.2.12 Configuring the Web Server Control Function	286
10.2.13 Configuring Remote Assistance	286
10.2.14 Resetting the Authentication Mode.....	287
10.2.15 Restarting or Shutting Down the System	287
10.2.16 Changing Internal IP Address	288
10.2.17 Exiting the Console.....	289
11 Initial Configuration	290
11.1 Login to the Console	290
11.2 Network Configuration on the Console.....	291

11.3 Login to Web-based Manager	291
11.4 Importing a License	293
11.5 Network Configuration on the Web-based Manager	294
12 System Maintenance.....	295
12.1 System Upgrade	295
12.2 Common Troubleshooting	296
12.2.1 Web Login Failure.....	296
12.2.2 Device Access Failure	296
12.2.3 License Import Failure	296
12.2.4 MAC Address Learning Failure	297
12.2.5 Ping Failure or Excessive Packet Drop	297
A Acronyms and Abbreviations.....	298
B Default Parameters.....	230
B.1 Default Parameters of the Management Interface	230
B.2 Default Account of the Web Administrator.....	230
B.3 Default Account of the Console Administrator.....	230
B.4 Default Account of the CLI Administrator	230
B.5 Communication Parameters of the Console Port	230
C IPv4/IPv6 Support	232
D NSFOCUS MASTER TERMS AND CONDITIONS	236

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.



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, cloud signaling, and TI.
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 initial 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
V4.5R90F06	<ul style="list-style-type: none"> New functions: DNS subdomain allowlist auto-learning, HTTPS fingerprint protection, and disk status. Optimized functions: carpet bombing protection, protection groups, access control policies, SSL/TLS keyword checking rule, SNMP agent, syslog, BGP mode, and attack-triggered packet capture.
V4.5R90F05SP02	<ul style="list-style-type: none"> New functions: global and group-specific DNS subdomain allowlists. Optimized functions: time server, RADIUS authentication, HA configuration, and DNS CNAME algorithm.
V4.5R90F05SP01	<ul style="list-style-type: none"> New functions: group-specific allowlist, SSL/TLS keyword checking rules, and total traffic control of protection groups. Optimized functions: global allowlist, TI, HA configuration, and user management.
V4.5R90F05	<ul style="list-style-type: none"> 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.

Version	Description
V4.5R90F04SP03	<ul style="list-style-type: none"> New functions: group-specific exception IP, Windows server for LDAP, and device shutdown. Optimized functions: SNMP settings, and log sending by email.
V4.5R90F04	<ul style="list-style-type: none"> New functions: common UDP watermark protection algorithm, group-specific access control rule, group-specific TI, web API log, and license expiration warning. Optimized functions: global TI, global ACL rule, MAC address configurations, and system logs.
V4.5R90F03SP02	<ul style="list-style-type: none"> Updated the structure based on the new template. Added descriptions about the following new functions: UDP session authentication policy, disk usage, password + email 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.
<i>Italic font</i>	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.

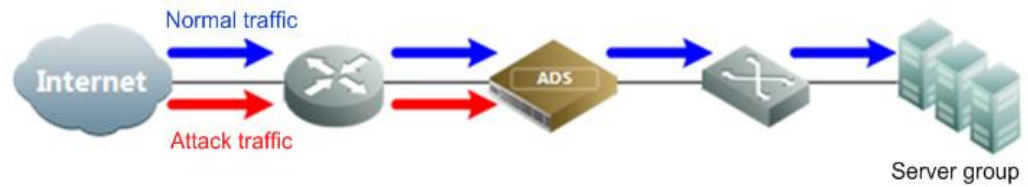


- ADS NX3-2020E, NX3-800E, NX3-HD2500, NX3-HD1000, NX5-HD4500, NX5-4020E, NX5-6025E, NX5-HD5000, NX5-HD6000, NX5-HD6500, NX5-HD8500, and NX5-8000 support both in-path and out-of-path deployment modes, whereas ADS NX5-10000/12000/20000 supports the out-of-path deployment mode only.
- When vADS uses a 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.

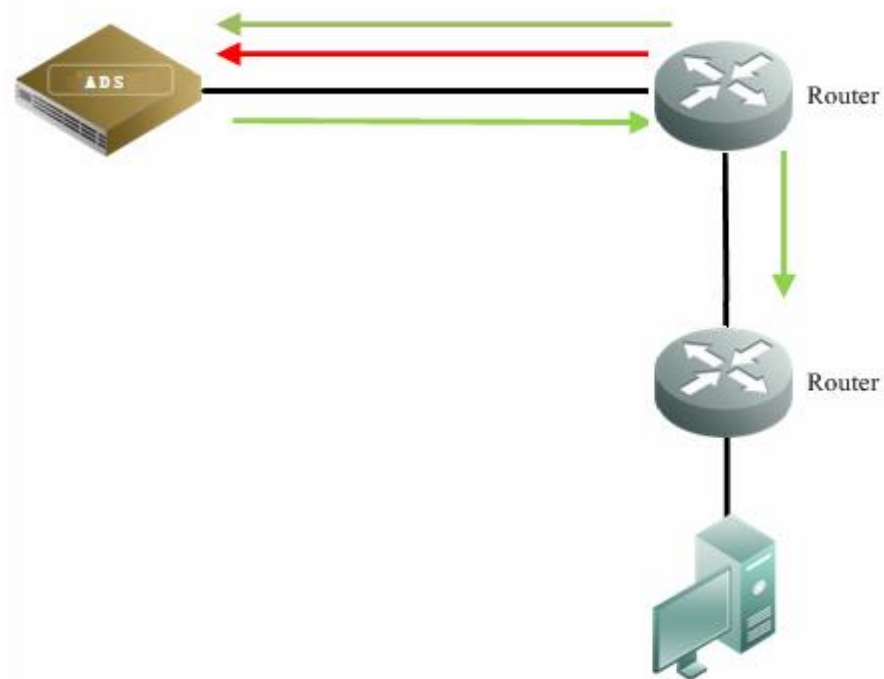
Figure 1-1 In-path deployment of an ADS device



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.

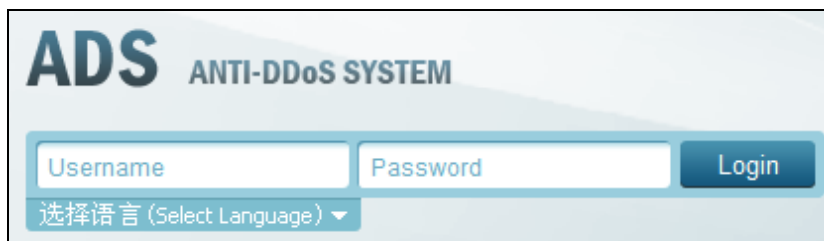
As the ADS device supports both IPv4 and IPv6 protocols, you can type an IPv4 address (for example, **https://192.168.1.100**) or IPv6 address (for example, **https://[2001::107]**).

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](#).

----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 (TI), 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 about 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

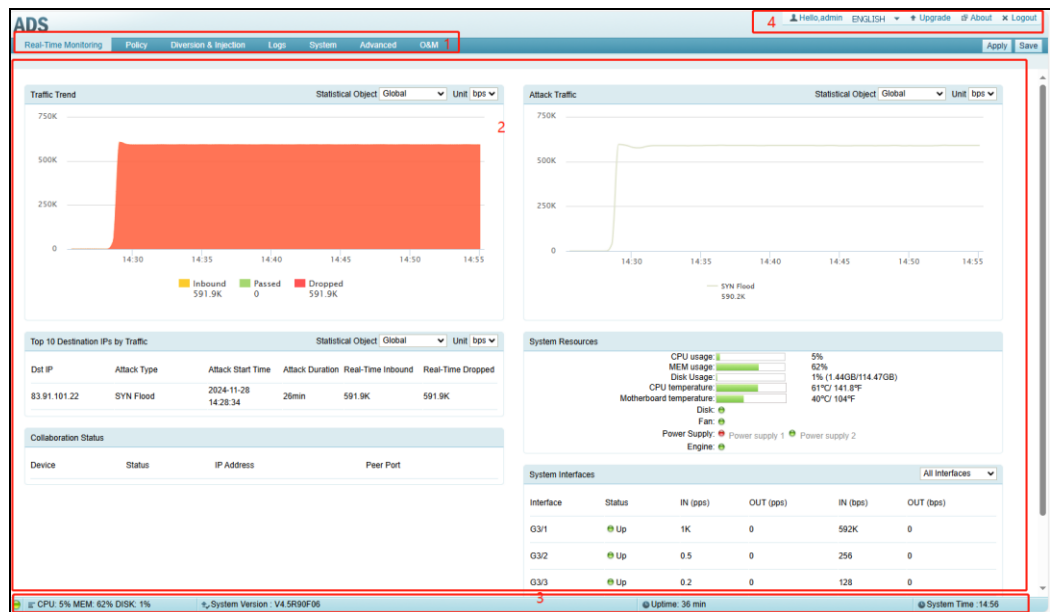






Table 2-2 describes the web page layout.



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
	Switches to another language.
	Switches to the system upgrade window.
	Displays information about the current ADS device.
	Logs you out of the system.

	For the sake of account security, you are advised to click  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.
	Makes the configuration in the active work area take effect immediately.
	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 Platform 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.



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

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

Choose **System > Local Settings > Basic Settings**. The **Basic Settings** page appears, as shown in [Figure 3-1](#).

Figure 3-1 Basic Settings page

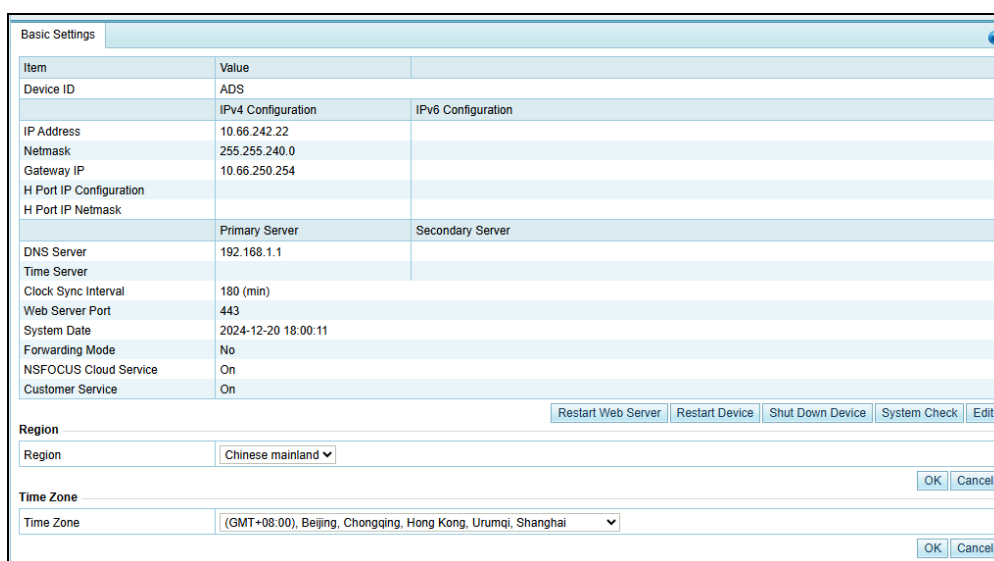





Table 3-1 Basic system settings

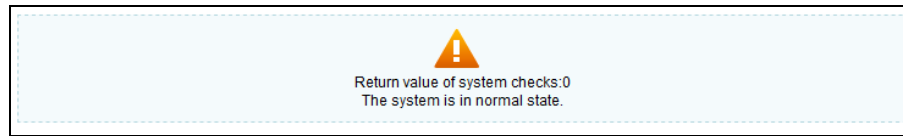
Parameter	Description
Device ID	Device model. It cannot exceed 26 characters.
IP Address/Netmask	<p>IPv4 address/netmask or IPv6 address/prefix length of the management interface of ADS. Note that the IP segment 172.16.1.0/24 is reserved for internal communication.</p> <p> Note</p> <ul style="list-style-type: none"> ADS supports the IPv4/IPv6 dual stack. Therefore, you can configure the IPv4 or IPv6 address for the management interface according to the actual network deployment. The device administrator can use this IP address to exercise remote device management via HTTPS, perform log-related operations, and send emails.
Gateway IP	IPv4/IPv6 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 and out-of-path modes. Therefore, you need to

Parameter	Description
	<p>configure the IPv4 address and related netmask or IPv6 address and related prefix length for this port here.</p> <p> Note</p> <ul style="list-style-type: none"> 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. Only in versions V4.5R90F06 and later can the H port be used as a heartbeat interface in out-of-path mode.
DNS Server	<p>IP addresses of the primary and secondary DNS servers used by the management interface of the current ADS device.</p> <p>Only when the primary DNS server malfunctions can the secondary be used.</p>
Time Server	<p>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 at an interval specified in Clock Sync Interval.</p> <p>A primary and secondary time servers can be configured. Only when the synchronization with the primary time server fails can the time of the secondary server be used.</p> <p> Note</p> <p>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.</p>
Clock Sync Interval	<p>Interval for ADS to automatically synchronize the time with the time server.</p> <p>The value range is 5–180 minutes, with 180 as the default.</p>
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	<p>Unique ID of ADS.</p> <p>It is used for applying for the device license.</p>
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 Service	Controls whether to turn on the NSFOCUS cloud service.

On the **Basic Settings** page shown in [Figure 3-1](#), you can perform the following operations:

- Edit basic system information.
Click **Edit** to open the **Modify Basic Settings** page. Modify parameter settings and click **OK** to commit the changes.
- Check the system status.
Click **System Check** to check whether the system operates properly. Then the system returns check results, as shown in [Figure 3-2](#).

Figure 3-2 System check results



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

- Change the web server port.
 - a. Click **Edit** to open the **Modify Basic Settings** page and modify the web server port.
It can be 443 (default) or an integer ranging from 18000 to 20000. A conflicting port may make the web service inaccessible. If **Web Server Port** is set to another number than 443, management by a third-party device or ADS M may be affected.
For example, change **Web Server Port** to **18000**. Then the accessible address of ADS is changed to **https://*.*.*.18000**.
 - b. Configure parameters and click **OK** to return to the **Basic Settings** page.
 - c. Click **Restart Web Server** on the page shown in [Figure 3-1](#).
- Restart the device remotely.
Click **Restart Device** to restart the current ADS remotely.
- Shut down the device remotely.
Click **Shut Down 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-HD8500.

Figure 3-3 Interface working mode of ADS NX5-HD8500








Interface Working Mode					
Interface	SmartNIC	Mode	MTU	Status	Enable/Disable Interface
G3/1	No	auto	1500	Up/1000/ Full	
G3/2	No	auto	1500	Up/1000/ Full	
G3/3	No	auto	1500	Up/1000/ Full	
G3/4	No	auto	1500	/Down	

Table 3-2 describes interface working mode parameters.

Table 3-2 Interface working mode parameters

Parameter	Description
Interface No.	<p>ADS NX3-800E:</p> <ul style="list-style-type: none"> G3/1–G3/8: 1000M electrical ports F4/1–F4/8: 1000M optical ports <p>ADS NX3-4020E:</p> <ul style="list-style-type: none"> T1/1 and T1/2: 10G optical ports G3/1–G3/8: 1000M electrical ports F4/1–F4/8: 1000M optical ports <p>ADS NX5-10000:</p> <ul style="list-style-type: none"> 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 <p> Note</p> <p>Interface numbers here are provided for illustration only. They may differ from the actual numbers as boards may be inserted into other slots.</p>
SmartNIC	Indicates whether it is a smartNIC. It will be displayed as Yes after a FPGA card that contains 8 x 10G optical ports occupying two slots is inserted.
Mode	<p>The default value is auto, indicating that the interface is working in auto negotiation mode.</p> <ul style="list-style-type: none"> 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.

Parameter	Description
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

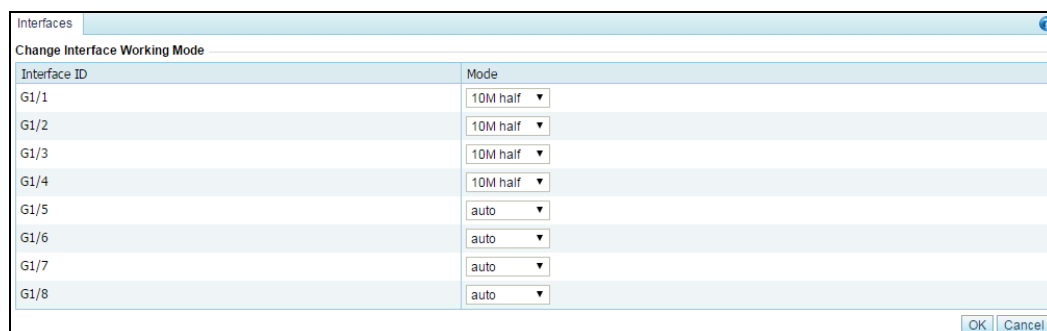
Step 2 To enable or disable an interface, click  or  in the Enable/Disable Interface column.
----End

Changing the Working Mode of 1000M Electrical Ports

ADS NX5-4020E is used as an example here.

On the **Interfaces** 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



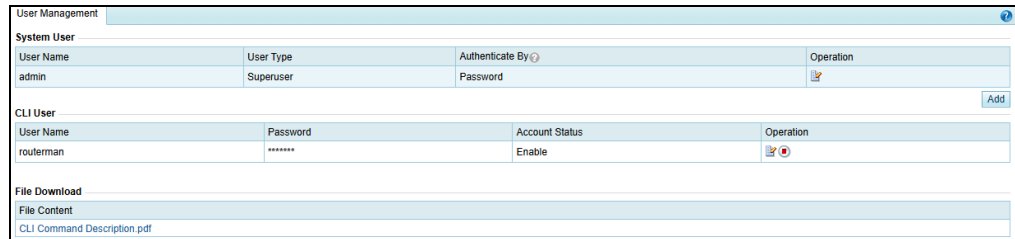
Interface ID	Mode
G1/1	10M half
G1/2	10M half
G1/3	10M half
G1/4	10M half
G1/5	auto
G1/6	auto
G1/7	auto
G1/8	auto

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



The screenshot shows the 'User Management' interface. It has two main sections: 'System User' and 'CLI User'. The 'System User' section contains a table with columns: User Name, User Type, Authenticate By, and Operation. The 'CLI User' section contains a table with columns: User Name, Password, Account Status, and Operation. Below these tables is a 'File Download' section with a link to 'CLI Command Description pdf'.

User Name	User Type	Authenticate By	Operation
admin	Superuser	Password	

User Name	Password	Account Status	Operation
routerman	*****	Enable	

File Download
[CLI Command Description 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](#).

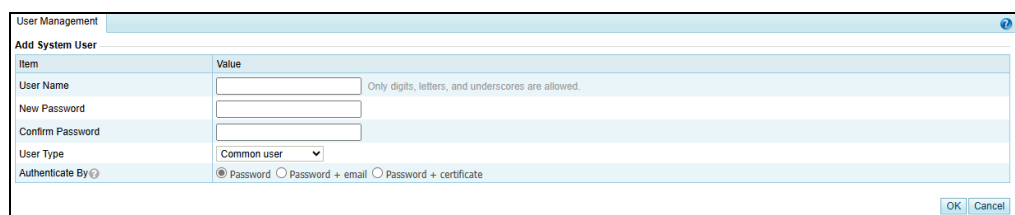
Under **File Download**, you can click the *CLI Command Line Manual* link to download this user guide.

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



The screenshot shows the 'Add System User' form. It has fields for User Name, New Password, Confirm Password, User Type (dropdown), and Authenticate By (radio buttons). The 'User Name' field has a hint: 'Only digits, letters, and underscores are allowed.' The 'User Type' dropdown is set to 'Common user'. The 'Authenticate By' radio buttons are set to 'Password'.

Item	Value
User Name	<input type="text"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
User Type	Common user
Authenticate By	<input checked="" type="radio"/> Password <input type="radio"/> Password + email <input type="radio"/> Password + certificate

OK Cancel

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

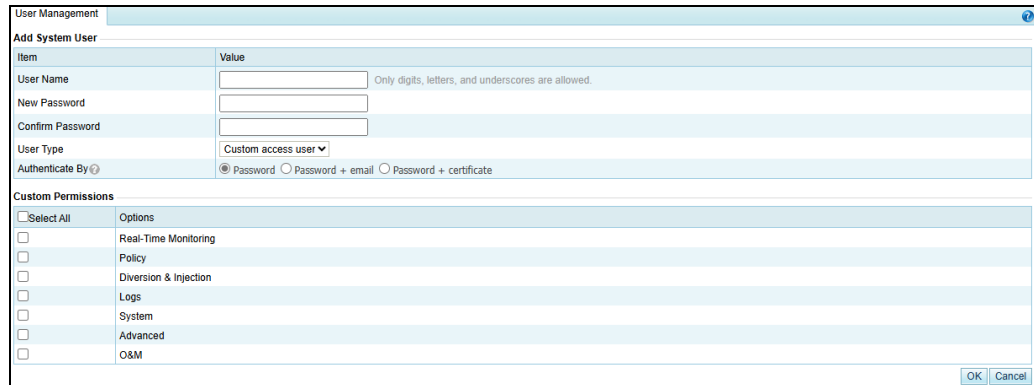





Table 3-3 describes parameters for adding a user.

Table 3-3 Parameters for adding a user

Parameter	Description
User Name	Specifies the user name of the new account, which is unique and cannot be admin. It should contain 4 to 20 characters long. The minimum user name length is determined by the Min User Name Length value specified under System > Security Settings > Login Security . Also, the user name can only consist of letters, digits, and underscores.
New 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 Settings > Login Security .
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 , Auditor , 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 . <ul style="list-style-type: none"> 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. <div>  <p>Note</p> <ul style="list-style-type: none"> 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 email service. To download the UKey program, click Download Application in the lower-left corner of the login page. </div>

Editing a User

You can edit a default user (admin) and custom user.

Click  in the **Operation** column of a user to edit the user's account information. Only **admin** can edit user accounts and other users can only change their own passwords.

Rename the default user (**admin**) with caution. If you forget the new name, you have to restore it along with its password to the default through the console. For details, see section [10.2.7 Setting Web Login](#).


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 Settings > Login Security**. 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 Platform Configuration

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

3.1.4.1 Configuring a Management Platform

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 Platform**.


Figure 3-8 Management Platform page

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

Figure 3-9 Add Management Platform page

Table 3-4 describes management mode parameters.

Table 3-4 Management mode parameters

Parameter	Description
Enable	Controls whether ADS accepts centralized management. <ul style="list-style-type: none"> Yes: indicates that ADS is subject to centralized management. No: indicates that ADS is not subject to centralized management.
IP Address	IP address of ADS M or the third-party device to which ADS submits data. You can type either an IPv4 or IPv6 address. This is required when ADS M or Third-Party Management is selected as the management platform.  Note Currently, ADS can submit data to five management devices simultaneously.
Domain Name/IP Address	Domain name or IP address of ESPC/ESPP to which ADS submits data. You can type either an IPv4 or IPv6 address. This is required when ESPC/ESPP is selected as the management platform.
Management Platform	Type of the device to which ADS submits data. The value can be one of the following: <ul style="list-style-type: none"> ADS M ESPC/ESPP

Parameter	Description
	<ul style="list-style-type: none"> 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.
Access Key	<p>Specifies the access key used for configuring the web API. This parameter is available only when Third-Party Management or ADS M is selected as the management platform.</p> <p>The access key must be a combination of 6 to 15 uppercase letters, lowercase letters, and digits.</p>
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	<p>Specifies the language of messages sent by ADS to ADS M, ESPC/ESPP, or a third-party platform.</p> <p>Generally, after you configure protection policies for ADS via ADS M, ADS returns related messages.</p>

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 Platform** to open the management mode page shown in [Figure 3-8](#).

In the **HTTP Authentication Synchronization** area, the **Synchronization Status and Cause of 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	<p>Controls whether to enable the HTTP authentication synchronization function.</p> <ul style="list-style-type: none"> Yes: enables this function. No: disables this function.
Src IP	<p>Specifies the IP address to which HTTP authentication information is synchronized. Both IPv4 and IPv6 addresses are allowed here.</p> <p> Note</p>

Parameter	Description
	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.

The default file name is **cfgbackup_version_export time_collapsar.conf**, such as **cfgbackup_V4_5R90F06_202411151854_collapsar.conf**.

Figure 3-10 Configuration file management

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



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

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.
User Name	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. Fill in a UNIX absolute path, for example, /tmp/.
Backup Frequency	Specifies how often the configuration file is backed up, which can be Daily , Weekly , or Monthly .
Test FTP Setting	Clicking Test Now sends test file to the specified FTP server to check whether the settings are correct.

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.

Parameter	Description
	<ul style="list-style-type: none"> Yes: enables the function. No: disables the function.
Device Alert Threshold (pps)	Alert triggering threshold for the overall traffic of the device in pps. A bandwidth overrun alert is generated when this threshold is exceeded.
Device Alert Threshold (bps)	Alert triggering threshold for the overall traffic of the device 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 alert thresholds for hardware and virtual devices are different.

Table 3-8 Hardware alert thresholds

Parameter	Description
CPU Usage Threshold	Specifies the percentage of CPU usage that will trigger an alert.
Memory Usage Threshold	Specifies the percentage of memory usage that will trigger an alert.
Disk Usage 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.
Motherboard Temperature Threshold	Specifies the temperature of the motherboard that will trigger an alert.
Fan Alert	Controls whether to turn the fan switch on. If it is turned on, an alert will be triggered when a fan fails.
Power Alert	Controls whether to turn the power switch on. If it is turned on, an alert will be triggered when the power supply fails.
Disk Status Alert	Controls whether to turn the disk switch on. If it is turned on, an alert will be triggered when a disk fails.

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

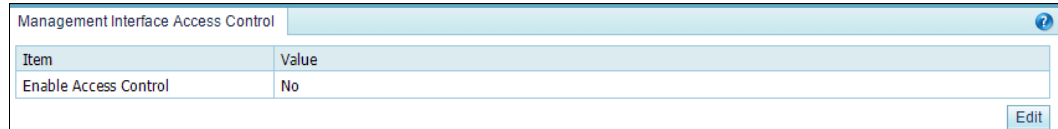
external IP addresses to which ADS connects, such as NSFOCUS Cloud or other collaborative platforms, and allow access from these IP addresses.

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)



Item	Value
Enable Access Control	No

Edit

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. <ul style="list-style-type: none">• Yes: enables the function.• No: disables the function.
Default Rule	Specifies a default rule. <ul style="list-style-type: none">• Permit any: allows any IP addresses other than those denied access in management interface access control rules to access ADS.• Deny 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

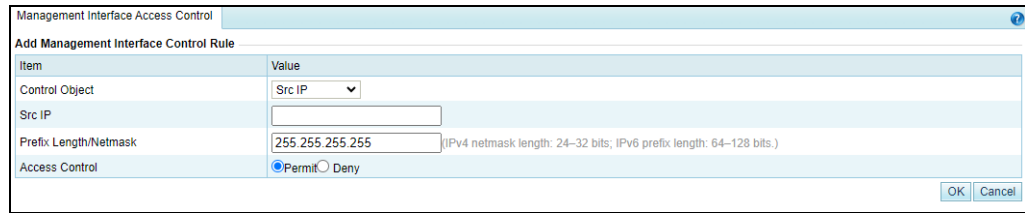



Table 3-10 describes parameters for creating a management interface access control rule.

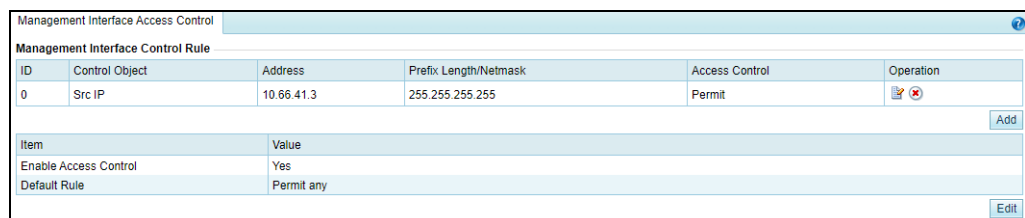
Table 3-10 Parameters for creating a management interface access control rule

Parameter	Description
Control Object	Specifies use of a source IP address or MAC address for access control. <div>  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. </div>
Src IP/Source MAC	Specifies a source IP address/segment or a MAC address that is allowed or forbidden to access ADS.
Prefix Length/Netmask	Specifies the subnet mask of the source IP address/segment. This parameter is available only when Control Object is set to Src IP . <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Permit: allows the specified IP address/segment or MAC address to access ADS. Deny: 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



----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

	<p>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:</p> <ul style="list-style-type: none"> • 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.

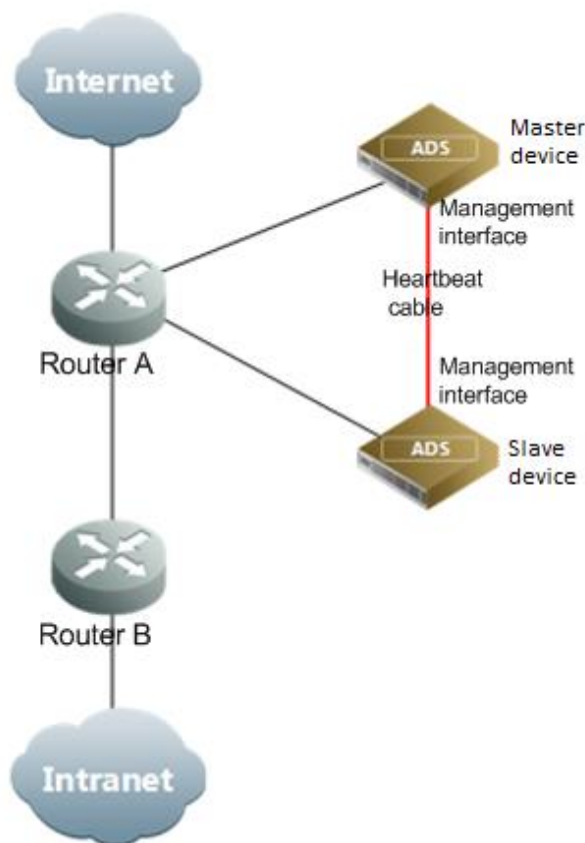
- In active-active mode, one ADS device functions as the primary device, and the other as the secondary device. Both the primary and secondary devices handle services and achieve load balancing. If the primary device fails, the secondary device takes over all work and traffic handled by the former, ensuring 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 or H 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**.

Figure 3-16 HA page

HA

Device Status

HA Status: ● Role: Not enabled Connection Status: ●

Basic Settings

Item	Value
HA Mode	Active/Standby
HA Role	Not enabled
Local IP	
Primary IP	
Secondary IP	

[View Status](#) [Enable](#) [Edit](#) [Advanced Config](#)

Configuration Synchronization

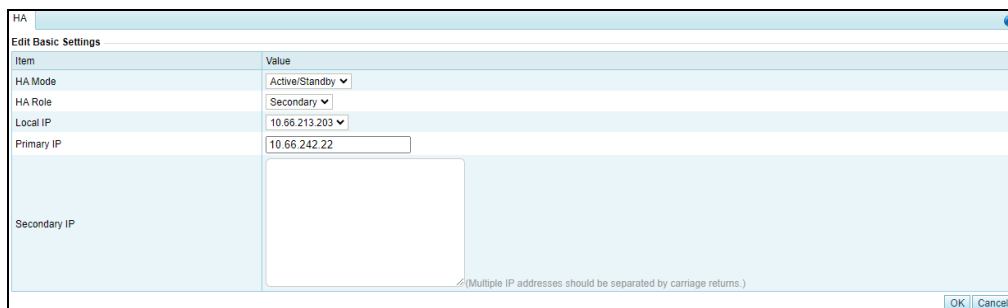
Item	Value
Protection Groups	No
Group Policy Templates	No
Carpet Bombing Protection	No
Advanced Global Parameters	No
Response Page Settings	No
SSL Certificate Mgmt	No
Mobile User-Agent Rules	No
Allowlist	No
Access Control Policy	No
Reflection Protection Rule	No
GeoIP Rules	No
Blocklist	No
HTTP Keyword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

[Edit](#)

Step 2 Modify basic settings of HA.

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

Figure 3-17 Editing basic settings





Item	Value
HA Mode	Active/Standby
HA Role	Secondary
Local IP	10.66.213.203
Primary IP	10.66.242.22
Secondary IP	

(Multiple IP addresses should be separated by carriage returns.)

OK Cancel

Table 3-11 describes parameters of basic HA settings.

Table 3-11 Parameters of basic HA settings

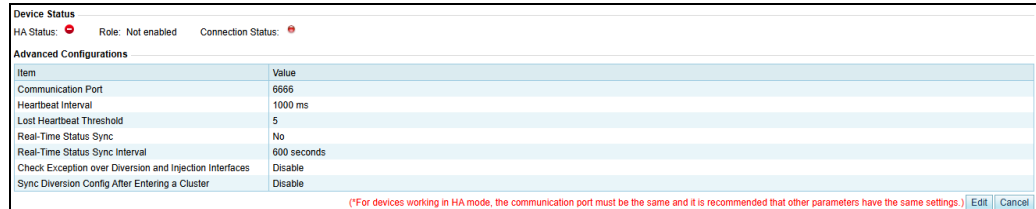
Parameter	Description
HA Mode	HA mode, which can be Active/Active or Active/Standby .
HA Role	<p>Role played by the current device in dual-system hot standby mode.</p> <p>In active/standby mode:</p> <ul style="list-style-type: none"> Primary: indicates that this device works as a primary device. After HA is enabled, it starts handling services until a failure occurs. Secondary: 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. <p>In active/active mode:</p> <ul style="list-style-type: none"> Primary: indicates that this device works as a primary device. After HA is enabled, it starts handling services until a failure occurs. Secondary: 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 the IP address of the management interface or heartbeat interface. You can type an IPv4 or IPv6 address. Note that the IP segment 172.16.1.0/24 is reserved for internal communication.
Primary IP	<p>IP address of the primary device, which can be an IPv4 or IPv6 address.</p> <p> Note</p> <ul style="list-style-type: none"> This parameter needs to be set only when HA Role is set to Secondary. The route between Primary IP and Secondary IP must be reachable.
Secondary IP	<p>IP address of the secondary device, which can be an IPv4 or IPv6 address.</p> <p> Note</p> <ul style="list-style-type: none"> This parameter needs to be set only when HA Role is set to Primary. The route between Primary IP and Secondary 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



- b. Click **Edit**.

Figure 3-19 Editing advanced settings

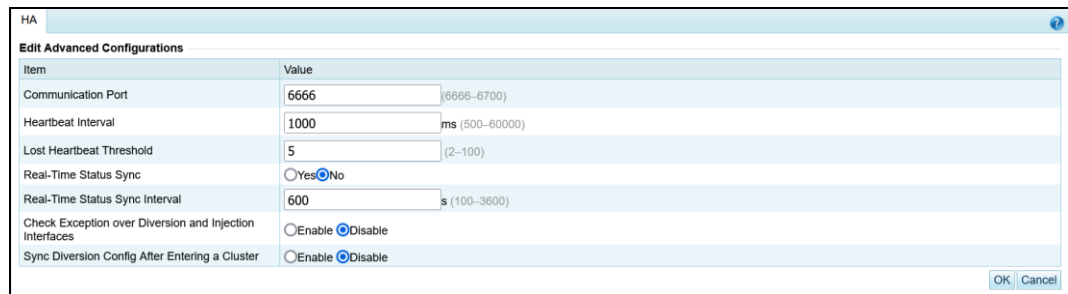





Table 3-12 describes the advanced HA configuration parameters.

Table 3-12 Advanced HA configuration parameters

Parameter	Description
Communication Port	Port for HA communication.
Heartbeat Interval	Interval for the active device to synchronize keepalive information to the standby device, in milliseconds.  Note The Heartbeat Interval values on the primary and secondary devices should be as close as possible to avoid possible HA connection establishment failures.
Lost Heartbeat Threshold	An auxiliary parameter for detecting heartbeat timeouts when an HA connection is established. When the number of lost heartbeats exceeds this value, the heartbeat connection is deemed disconnected.  Note The Lost Heartbeat Threshold values on the primary and secondary devices should be as close as possible to avoid possible HA connection establishment failures.

Parameter	Description
Real-Time Status Sync	Whether to enable real-time status synchronization.  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.
Sync 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**.

The **Policy** tab page is displayed by default in the **Configuration Synchronization** area, as shown in [Figure 3-16](#).

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

Figure 3-20 Policy configurations to be synchronized

HA

Device Status

HA Status: ● Role: Not enabled Connection Status: ●

Basic Settings

Item	Value
HA Mode	Active/Standby
HA Role	Not enabled
Local IP	
Primary IP	
Secondary IP	

View Status

Enable

Edit

Advanced Config

Configuration Synchronization

Policy

Diversion & Injection

System

Advanced

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

Edit


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

The screenshot shows the NSFOCUS ADS configuration interface. At the top, there's a 'Device Status' section with 'HA Status' (red dot), 'Role: Not enabled', and 'Connection Status' (red dot). Below this is the 'Basic Settings' section with a table of configuration items.

Item	Value
HA Mode	Active/Standby
HA Role	Not enabled
Local IP	10.66.213.203
Primary IP	10.66.242.22
Secondary IP	

Below the 'Basic Settings' is the 'Configuration Synchronization' section. It has tabs for 'Policy', 'Diversion & Injection' (selected), 'System', and 'Advanced'. The 'Diversion & Injection' tab shows a table of configuration items.

Item	Value
Running Mode	No
Port Channel	No
GRE Tunnel	No
IP Address	No
BGP Route	No
IP Route Assignment	No
Injection Interfaces	No
Injection Routes	No
MAC Address Table	No
Filtering Rules	No
Manual Diversion	No
Group Diversion	No
Genie Diversion	No
Arbor Diversion	No
MPLS Route	No
Others	No

Buttons for 'View Status', 'Enable', 'Edit', and 'Advanced Config' are visible at the top right of the 'Configuration Synchronization' section. An 'Edit' button is at the bottom right.

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

The screenshot shows the NSFOCUS ADS configuration interface, similar to Figure 3-21. The 'System' tab is selected under 'Configuration Synchronization'. It shows a table of configuration items.

Item	Value
System User	No
Management Mode	No
Collaboration	No
Bandwidth Overrun Limit	No
Syslog Configuration	No
SNMP Trap Setting	No
Email	No
SFTP/SSH	No

Buttons for 'View Status', 'Enable', 'Edit', and 'Advanced Config' are visible at the top right of the 'Configuration Synchronization' section. An 'Edit' button is at the bottom right.

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](#), click the **Advanced** tab.

Figure 3-23 Advanced configurations to be synchronized

The screenshot shows the HA Configuration page on a primary device. The top section, 'Device Status', shows 'HA Status' as 'Not enabled' and 'Connection Status' as 'Not enabled'. Below this is the 'Basic Settings' section with a table of items and values:

Item	Value
HA Mode	Active/Standby
HA Role	Not enabled
Local IP	10.66.213.203
Primary IP	10.66.242.22
Secondary IP	

Buttons for 'View Status', 'Enable', 'Edit', and 'Advanced Config' are visible. Below is the 'Configuration Synchronization' section with tabs for 'Policy', 'Diversion & Injection', 'System', and 'Advanced'. The 'Advanced' tab is selected, showing a table of items and values:

Item	Value
Pattern Matching Rules	No
Automatic Packet Capture	No
Ti Configuration	No

An 'Edit' button is at the bottom right.

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** tab page shown in [Figure 3-16](#).

After HA is enabled, the **HA** 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

The screenshot shows the HA Configuration page on a primary device with HA enabled. The top section, 'Device Status', shows 'HA Status' as 'Enabled' and 'Connection Status' as 'Peer Lists: 10.66.242.13'. Below this is the 'Basic Settings' section with a table of items and values:

Item	Value
HA Mode	Active/Standby
HA Role	Primary
Local IP	10.66.242.242
Primary IP	
Secondary IP	10.66.242.13

Buttons for 'View Status', 'Disable', 'Edit', and 'Advanced Config' are visible. Below is the 'Configuration Synchronization' section with tabs for 'Policy', 'Diversion & Injection', 'System', and 'Advanced'. The 'Advanced' tab is selected, showing a table of items and values:

Item	Value
Protection Groups	No
Group Policy Templates	No
Carpet Bombing Protection	No
Advanced Global Parameters	No
Response Page Settings	No
SSL Certificate Mgmt	No
Mobile User Agent Rules	No
Allowlist	No
Access Control Policy	No
Reflection Protection Rule	No
GeolIP Rules	No
Blocklist	No
HTTP Keyword Checking	No
SSL/TLS Keyword Checking	No
Connection Exhaustion Rules	No
Regular Expression Rules	No
URL ACL Protection Rules	No
DNS Keyword Checking	No

Figure 3-25 HA Configuration page on a secondary device

HA

Device Status

HA Status: ● Role: Secondary Connection Status: ● Peer Lists: 10.66.242.242

Basic Settings

Item	Value
HA Mode	Active/Standby
HA Role	Secondary
Local IP	10.66.242.13
Primary IP	10.66.242.242
Secondary IP	10.66.242.13

Configuration Synchronization

(Disable the HA function before modifying HA Mode, HA Role, Local IP, Primary IP, Secondary IP, Communication Port, or Heartbeat Sync Interval.) View Status Disable Edit Advanced Config

Policy Diversion & Injection System Advanced

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

Disabling HA

After HA is enabled, in the lower-right corner of the **Basic Settings** area on the **HA** 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**, **Primary IP**, **Secondary IP**, and **Heartbeat 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

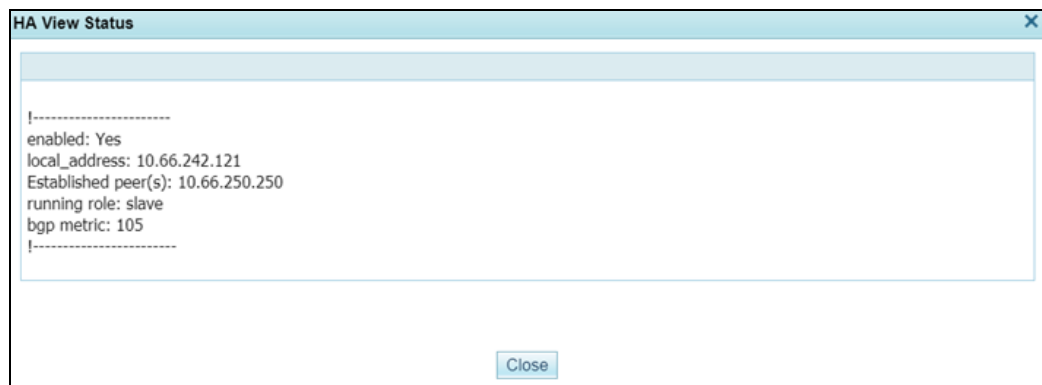
HA View Status

```

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

Close

Figure 3-27 HA status information of a secondary device

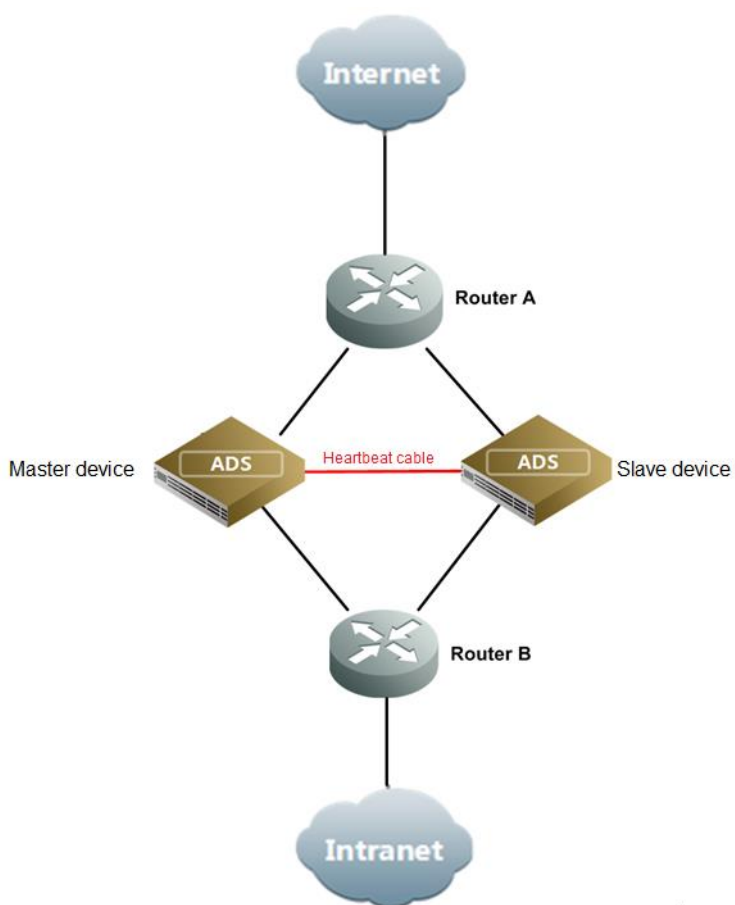


3.1.9.2 HA Configuration on ADS in In-Path Mode

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 on the **HA** page:

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

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



Item	Value
HA Mode	Active/Standby
HA Role	Primary
Local IP	10.66.242.242
Primary IP	10.66.242.13
Secondary IP	10.66.242.13

Item	Value
Protection Groups	No
Group Policy Templates	No
Carpet Bombing Protection	No
Advanced Global Parameters	No
Response Page Settings	No
SSL Certificate Mgmt	No
Mobile User-Agent Rules	No
Allowlist	No
Access Control Policy	No
Reflection Protection Rule	No
GeolIP Rules	No
Blocklist	No
HTTP Keyword Checking	No
SSL/TLS Keyword Checking	No
Connection Exhaustion Rules	No
Regular Expression Rules	No
URL ACL Protection Rules	No
DNS Keyword Checking	No

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.



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

Bypass Configuration

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	*****	 

Add






Enable All

Disable All

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**.

3.1.10.2 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.

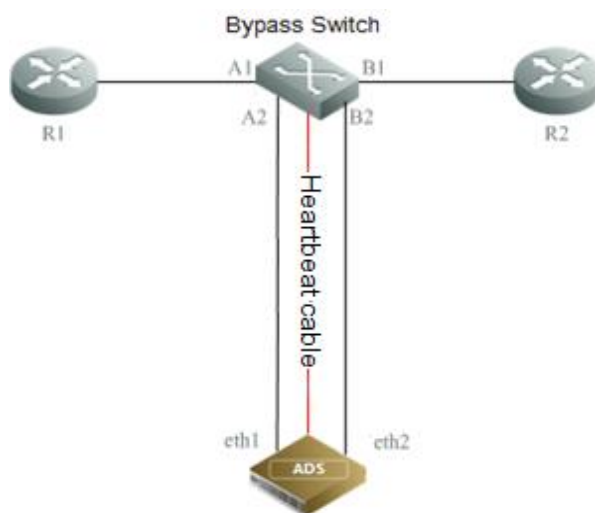
- To enable this function, click  in the **Operation** column. Then the indicator in the **Status** column turns to , indicating that the built-in bypass function is enabled. At the same time, the button in the **Operation** column turns to .
- To disable this function, click  in the **Operation** column.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

3.1.10.3 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.

<div data-bbox="446 1556 502 1646" data-label="Image">  </div> <div data-bbox="446 1612 502 1646" data-label="Text"> <p>Note</p> </div>	<p>If any of the following occurs, the bypass switch automatically switches to the bypass mode:</p> <ul style="list-style-type: none"> • 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. <p>If any of the following occurs, the NSF-BS is automatically switched to the non-bypass mode:</p> <ul style="list-style-type: none"> • 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.
--	---



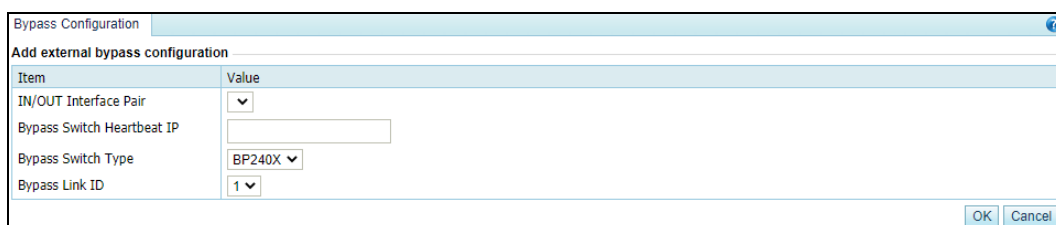
In in-path mode, ADS enters the bypass state by default when started. If you want ADS to implement protection, you must manually disable the external bypass so that ADS can switch to the normal protection state.

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




[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 about 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**. The **Collaboration** page appears, as shown in [Figure 3-33](#).

Figure 3-33 Collaboration configuration page

Collaboration	
Item	Value
Enable	No
Role	Not configured

[Diverged IP Status List](#)
[Lower-Level Device IP List](#)
[Edit](#)

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


Figure 3-34 Configuring an upper-level ADS

Collaboration	
Item	Value
Enable	<input type="radio"/> Yes <input checked="" type="radio"/> No
Role	Upper-level device ▼

[OK](#)
[Cancel](#)

[Table 3-14](#) describes parameters for configuring an upper-level ADS.

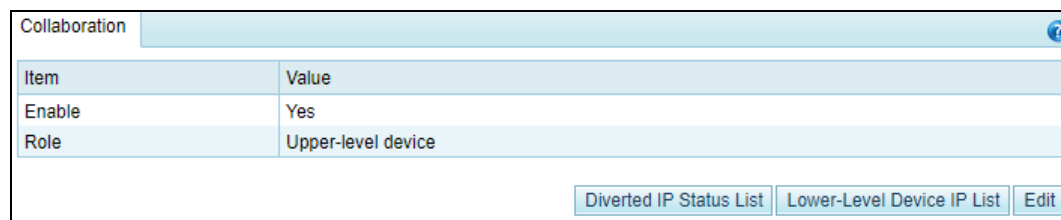
Table 3-14 Parameters for configuring an upper-level ADS

Parameter	Description
Enable	<p>Controls whether to enable collaboration between lower-level and upper-level ADS devices.</p> <ul style="list-style-type: none"> Yes: enables the collaboration function. No: disables the collaboration function. <p> Note</p> <p>To enable collaboration, you need to set Enable to Yes in the Management Platform area (under System > Local Settings > Management Platform). For details, see section 3.1.4 Management Platform Configuration.</p>

Parameter	Description
Role	Role of the device. Here, Upper-level device should be selected.

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

Figure 3-35 Collaboration Configuration page

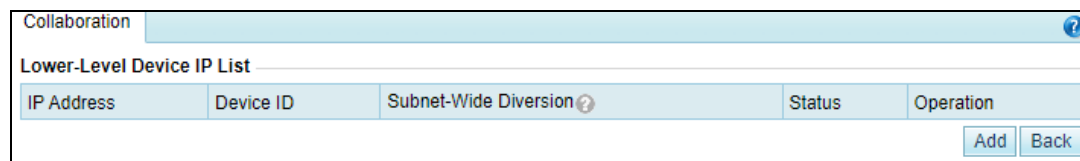


The screenshot shows the 'Collaboration' configuration window. It has a title bar with a question mark icon. Below the title bar is a table with two columns: 'Item' and 'Value'. The table contains two rows: 'Enable' with value 'Yes' and 'Role' with value 'Upper-level device'. At the bottom right of the window, there are three buttons: 'Diverted IP Status List', 'Lower-Level Device IP List', and 'Edit'.

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

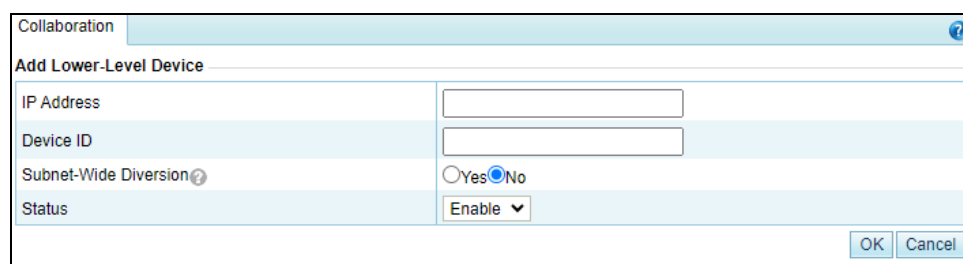


The screenshot shows the 'Collaboration' window with the 'Lower-Level Device IP List' tab selected. It displays a table with five columns: 'IP Address', 'Device ID', 'Subnet-Wide Diversion' (with a question mark icon), 'Status', and 'Operation'. At the bottom right, there are two buttons: 'Add' and 'Back'.

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



The screenshot shows the 'Collaboration' window with the 'Add Lower-Level Device' tab selected. It contains a form with four fields: 'IP Address' (text input), 'Device ID' (text input), 'Subnet-Wide Diversion' (radio buttons for 'Yes' and 'No', with 'No' selected), and 'Status' (a dropdown menu showing 'Enable'). At the bottom right, there are two buttons: 'OK' and 'Cancel'.

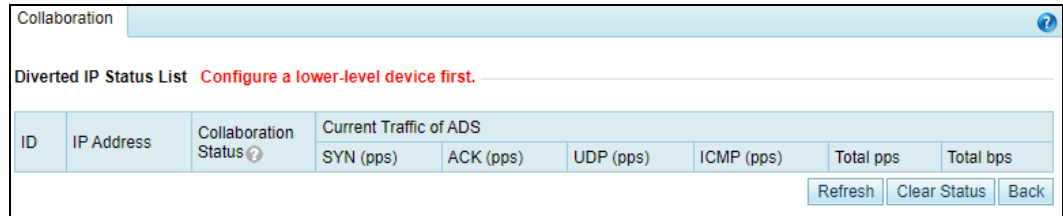
Step 5 Click **OK** to complete the configuration.

----End

Viewing Diverted IP Status List

On the **Collaboration** 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



ID	IP Address	Collaboration Status	Current Traffic of ADS					
			SYN (pps)	ACK (pps)	UDP (pps)	ICMP (pps)	Total pps	Total bps
<div>Refresh Clear Status Back</div>								

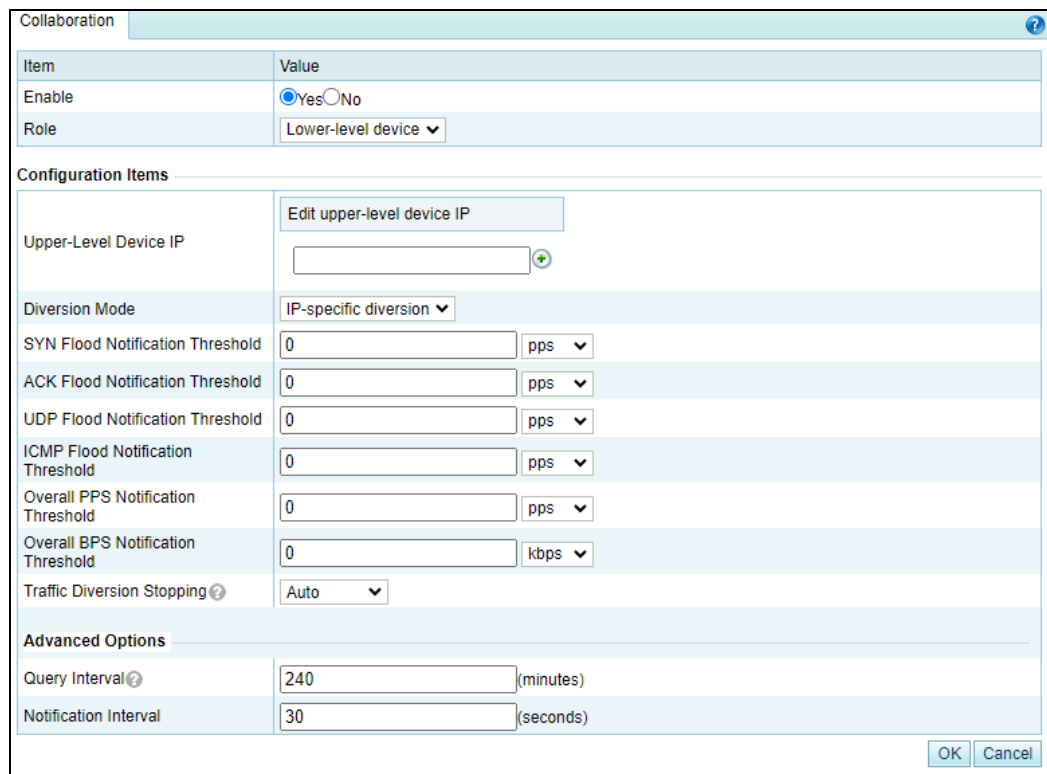
3.1.11.2 Managing Lower-Level ADS Devices

Configuring a Lower-Level ADS

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

- Step 1** On the **Collaboration** 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



Item	Value
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Role	Lower-level device

Configuration Items

Upper-Level Device IP	<input type="text"/> +
Diversion Mode	IP-specific diversion
SYN Flood Notification Threshold	<input type="text"/> pps
ACK Flood Notification Threshold	<input type="text"/> pps
UDP Flood Notification Threshold	<input type="text"/> pps
ICMP Flood Notification Threshold	<input type="text"/> pps
Overall PPS Notification Threshold	<input type="text"/> pps
Overall BPS Notification Threshold	<input type="text"/> kbps
Traffic Diversion Stopping	Auto


Advanced Options


Query Interval	<input type="text"/> (minutes)
Notification Interval	<input type="text"/> (seconds)

OK Cancel

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

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

Parameter		Description
Enable		<p>Controls whether to enable collaboration between lower-level and upper-level ADS devices.</p> <ul style="list-style-type: none"> Yes: enables the collaboration function. No: disables the collaboration function. <p> Note</p> <p>The lower-level device informs the upper-level ADS of diverting traffic when finding that traffic exceeds a notification threshold.</p>
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		<p>Mode of traffic diversion between upper-level and lower-level devices.</p> <ul style="list-style-type: none"> IP-specific diversion: indicates that traffic diversion is triggered when traffic destined for a single IP address exceeds a threshold. Overall diversion: indicates that traffic diversion is triggered for top N IP addresses by traffic when the overall traffic of the lower-level device exceeds a threshold.
IP-specific diversion	When the Diversion Mode is set to IP-specific diversion , you can configure the following parameters.	
	SYN Flood Notification Threshold	A traffic diversion triggering threshold for SYN Flood traffic. The lower-level device informs the upper-level ADS of diverting traffic when this threshold is exceeded.
	ACK Flood Notification Threshold	A traffic diversion triggering threshold for ACK Flood traffic. The lower-level device instructs the upper-level device to divert traffic when this threshold is exceeded.
	UDP Flood Notification Threshold	A traffic diversion triggering threshold for UDP Flood traffic. The lower-level device instructs the upper-level device to divert traffic when this threshold is exceeded.
	ICMP Flood Notification Threshold	A traffic diversion triggering threshold for ICMP Flood traffic. The lower-level device instructs the upper-level device to divert traffic when this threshold is exceeded.
	Overall Notification Threshold PPS	A notification triggering threshold for traffic in pps. The lower-level device instructs the upper-level device to divert traffic when the overall traffic in pps exceeds this threshold.
	Overall Notification Threshold BPS	A notification triggering threshold for traffic in bps. The lower-level device instructs the upper-level device to divert traffic when the overall traffic in bps exceeds this threshold.
Overall diversion	When the Diversion Mode is set to Overall diversion , you can configure the following parameters.	
	Top N	Top N IP addresses by traffic, for which the traffic is diverted. The value range is 1–10, with 3 as the default value.

Parameter		Description
	Device PPS Notification Threshold	A notification triggering threshold for device traffic in pps. The lower-level device instructs the upper-level device to divert traffic of top N IP addresses when the device traffic in pps exceeds this threshold.
	Device BPS Notification Threshold	A notification triggering threshold for device traffic in bps. The lower-level device instructs the upper-level device to divert traffic of top N IP addresses when the device traffic in bps exceeds this threshold.
Traffic Diversion Stopping		<p>Specifies when to stop traffic diversion.</p> <ul style="list-style-type: none"> • Auto: The lower-level ADS automatically determines whether to send a 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. <p> Note</p> <p>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.</p>
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 <input type="button" value="Test"/>
Diversion Mode	IP-specific 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	1000000(kbps)
Traffic Diversion Stopping	Auto

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 on the left of the **Test** button, the connection succeeds.

----End

Viewing Diverted IP Status List


On the **Collaboration** 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

Collaboration

99.99.99.99

Diverted IP Status List Current Upper-Level Device IP: 99.99.99.99 Status: ● DISCONNECTED

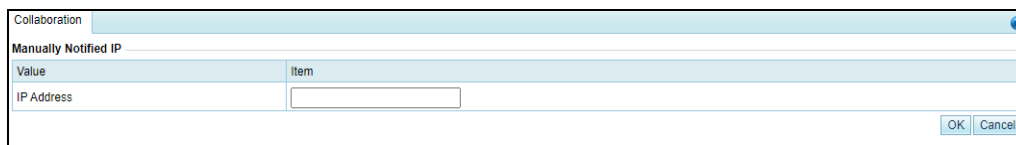
ID	IP Address	Collaboration Status 	Current Traffic of Lower-Level ADS						Current Traffic of Upper-Level ADS						Operation
			SYN (pps)	ACK (pps)	UDP (pps)	ICMP (pps)	Total pps	Total bps	SYN (pps)	ACK (pps)	UDP (pps)	ICMP (pps)	Total pps	Total bps	
<div>RefreshBack</div>															

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** page shown in Figure 3-40, click **Manually Notified IP**.

Figure 3-42 Configuring manually notified IP addresses



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

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

----End

Configuring Notification Filtering Rules

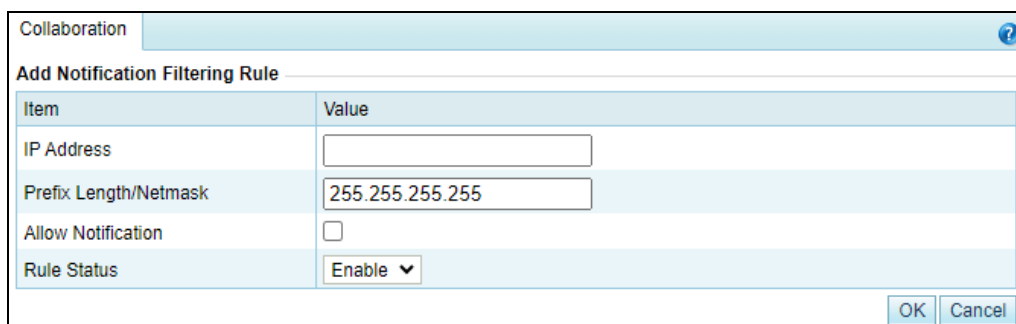
The upper-level ADS can successfully divert traffic destined for the specified IP addresses upon a manual or automatic notification only when notification filtering rules are configured.

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

Step 1 On the **Collaboration** page shown in [Figure 3-40](#), click **Notification Filtering Rule**.

Step 2 Click **Add**.

Figure 3-43 Adding a notification filtering rule



[Table 3-16](#) describes parameters for creating a notification filtering rule.

Table 3-16 Parameters for creating a notification filtering rule

Parameter	Description
IP Address	Destination IP address or segment of traffic to be manually diverted to the upper-level device.
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. <ul style="list-style-type: none"> Enable: enables this rule.

Parameter	Description
	<ul style="list-style-type: none"> 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](#)
- [Locked User Management](#)
- [Authentication Configuration](#)

3.2.1 Login Security

This section describes how to configure login security parameters.

The procedure is as follows:

Step 1 Choose **System > Security Settings > Login Security**, and then click **Edit**. See [Figure 3-44](#).

Figure 3-44 Configuring login security parameters

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	Off
Password Blocklist	<div></div> One password takes up a separate line.
Max Password Age	0 days (0–365) 0 indicates no limit
Max Login Failures	6 (0–10) 0 indicates no limit
Lockout Period	300 seconds (1–1000)
IP Access Control	Unlimited
Idle Timeout	0 minutes (0–1440) 0 indicates no limit
Use Verification Code	Off

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.

Parameter	Description
Password Strength Check	<p>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.</p> <ul style="list-style-type: none"> • On: omits the password strength check. • Off: performs the password strength check. If this is selected, the password complexity and minimum length must be specified. <ul style="list-style-type: none"> – 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 passwords. The value range is 6–30, with 6 as the default.
Password Blocklist	<p>Blocked passwords, with each in a separate line. None of those can be used as the password of a user account.</p>
Max Password Age	<p>Specifies the lifetime of the password that is successfully configured. A password whose lifetime has expired must be changed.</p> <p>The value ranges from 0 to 365 days. The value 0 indicates that this function is disabled.</p>
Max Login Failures	<p>Specifies the maximum number of consecutive failed login attempts in the allowed login interval.</p> <p>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.</p>
Lockout Period	<p>Specifies how long a user will be locked after Max Login Failures is exceeded. During the lockout period, the user is prevented from logging in to the system.</p> <p>The value ranges from 1 to 1000 seconds. You are advised to set it to a value no smaller than 180 seconds.</p>
IP Access Control	<p>Controls whether to control access from certain IP addresses.</p> <ul style="list-style-type: none"> • 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.
Idle Timeout	<p>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.</p> <p>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.</p>
Use Verification Code	<p>Controls whether to allow use of login verification codes.</p> <ul style="list-style-type: none"> • On: allows use of login verification codes, indicating that a user can successfully log in to ADS only after typing a correct verification code. • Off: 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** page to manually unlock the account.



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

Choose **System > Security Settings > Locked User**. Select the IP address to be unlocked and click **Unlock**.

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, 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 Settings > Authentication**.

Figure 3-45 Authentication Configuration page



Authentication	
Authentication	
Item	Value
Authentication Mode	Local
Edit	
Email Authentication Configuration	
Item	Value
Email Verification Code Timeout	15 minutes
Edit	








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


Figure 3-46 Editing authentication parameters

Authentication	
Authentication	
Item	Value
Authentication Mode	<input type="radio"/> Local <input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> LDAP
Authentication Server	<input type="text"/>
Authentication Port	<input type="text" value="389"/> <small>*(0-65535)</small>
Encryption	<input type="button" value="clear"/>
User Property	<input type="text" value="uid"/>
Base DN	<input type="text"/> <small>*Example: cn=xx, dc=xx1, dc=xx2</small>
User Name	<input type="text"/> <small>*Example: uid=xx,cn=xx,dc=xx1,dc=xx2</small>
Password	<input type="password"/> <small>Password should be 1 to 200 characters long.</small>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Table 3-18 Parameters for configuring the authentication mode

Parameter	Description
Authentication Mode	Specifies the authentication mode, which can be Local , RADIUS , TACACS+ , or LDAP .
Authentication Server	<p>Specifies the IP address or domain name of the authentication server. Both IPv4 and IPv6 addresses are supported.</p> <p> Note</p> <p>You can enter a domain name when the Authentication Mode is set to LDAP.</p>
Authentication Port	Specifies the port on which the authentication server listens for authentication requests.
Protocol	<p>Specifies the authentication protocol used to secure a connection to the authentication server.</p> <p>The options vary with the authentication server.</p> <p> Note</p> <p>This parameter is required when the Authentication Mode is set to RADIUS or TACACS+.</p>

Parameter	Description
Shared Key	<p>Specifies a text string used to encrypt the connection to the authentication server.</p> <p>The shared key configured on ADS must be the same as that configured on the authentication server; otherwise, ADS cannot communicate with the server.</p> <p> Note</p> <p>This parameter is required when the Authentication Mode is set to RADIUS or TACACS+.</p>
Authentication Duration	<p>Specifies the authentication duration, after which the authentication server returns the success or failure of the authentication information.</p> <p> Note</p> <p>This parameter is required when the Authentication Mode is set to RADIUS or TACACS+.</p>
Encryption	<p>Specifies the encryption mode of the LDAP network communication. Options include:</p> <ul style="list-style-type: none"> • clear: plaintext communication • ssl: SSL-encrypted communication • tls: TLS-encrypted communication <p> Note</p> <p>This parameter is required when the Authentication Mode is set to LDAP.</p>
User Property	<p>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.</p> <p> Note</p> <p>This parameter is required when the Authentication Mode is set to LDAP.</p>
Base DN	<p>Specifies the top of the LDAP directory tree, namely, the base directory.</p> <p> Note</p> <p>This parameter is required when the Authentication Mode is set to LDAP.</p>
User Name	<p>Specifies the name of the LDAP user.</p> <p> Note</p> <p>This parameter is required when the Authentication Mode is set to LDAP.</p>
Password	<p>Specifies the password of the LDAP user.</p> <p> Note</p> <p>This parameter is required when the Authentication Mode is set to LDAP.</p>
Use Secondary RADIUS Server	<p>Controls whether to enable the secondary RADIUS server for authentication. If it is enabled, the secondary RADIUS server will provide services when the primary server fails to handle authentication requests. You need to configure the</p>

Parameter	Description
	<p>following parameters to make the secondary RADIUS server take effect:</p> <ul style="list-style-type: none"> • Authentication Server: IP address of the secondary RADIUS server. • Authentication Port: port on which the secondary RADIUS server listens for authentication requests. The value range is 0–65535, with 1812 as the default. • Protocol: the authentication protocol used to secure a connection to secondary RADIUS server. This parameter can be set to pap, chap, spap, mschapv1, or mschapv2. • Shared Key: a text string used to encrypt the connection to the secondary RADIUS server. The shared key configured on ADS must be the same as that configured on the secondary RADIUS server; otherwise, ADS cannot communicate with the server. • Authentication Duration: authentication duration, after which the secondary RADIUS server returns the success or failure of the authentication. <p> Note</p> <p>This parameter is optional when the Authentication Mode is set to RADIUS.</p>

Step 2 Click **OK** to save the authentication configuration.

Step 3 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 4 Click **OK**.

----End

3.3 Log Services

This section covers the following topics:

- Syslog Configuration
- SNMP Configuration
- [Email Configuration](#)
- [SFTP/SSH Configuration](#)

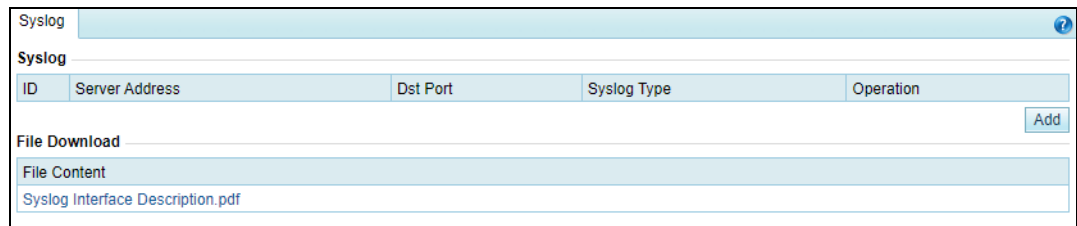
3.3.1 Syslog Configuration

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 3-47](#), you can click the file name in the **File Download** area to download the syslog file to a local disk drive.

Figure 3-47 Configuring syslog



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


Note

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

Figure 3-48 Configuring a syslog server

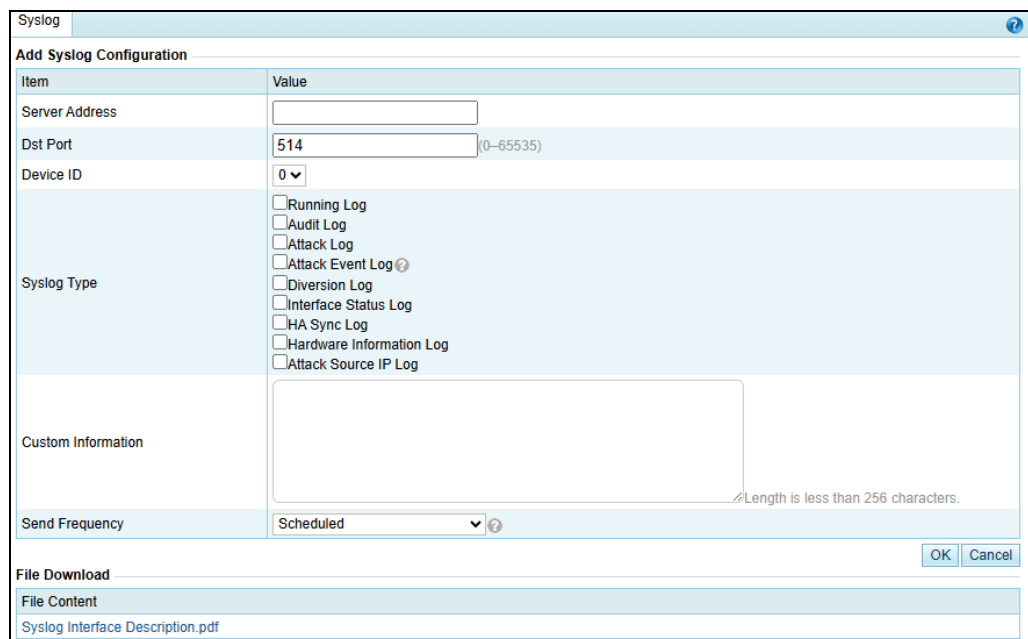



Table 3-19 Parameters for configuring a syslog server

Parameter	Description
Server Address	IPv4 or IPv6 address of the syslog server.
Dst 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.

Parameter	Description
Syslog Type	<p>Specifies the type of log messages that are sent to the syslog server, which can be:</p> <ul style="list-style-type: none"> Running Log Audit Log Attack Log Attack Event Log Diversion Log Interface Status Log HA Sync Log Hardware Information Log Attack Source IP Log <p>By default, the system sends log messages every 30 seconds.</p>
Custom Inforamtion	<p>Specifies the user-defined information that precedes the logs selected and will be sent to the syslog server.</p> <p>You can type less than 256 characters.</p>
Send Frequency	<p>Specifies the type of alerts, which can be either of the following:</p> <ul style="list-style-type: none"> Scheduled: sends alerts every 30 seconds. When a threshold is exceeded: sends alerts when a threshold is exceeded. <p> Note</p> <ul style="list-style-type: none"> This parameter is valid only for the operation log and hardware information log. If When a threshold is exceeded 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 unsolicited manner.

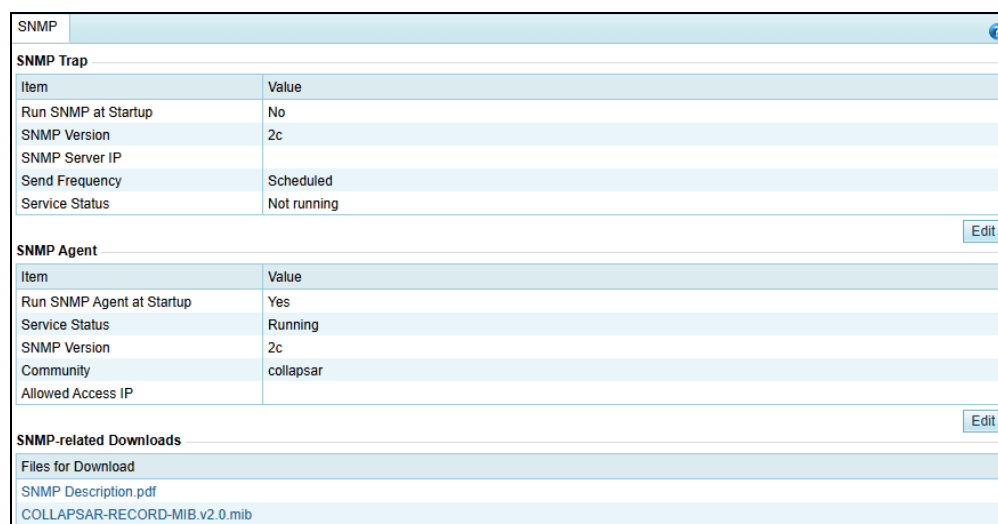
To configure SNMP, perform the following steps:

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

The **SNMP** page appears, as shown in [Figure 3-49](#).

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 3-49 SNMP page



Step 2 Click **Edit** in the **SNMP Trap** 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. <ul style="list-style-type: none"> Yes: launches the SNMP trap service when ADS is started. No: does not launch the SNMP trap service when ADS is started.
SNMP Version	SNMP protocol supported by the SNMP trap, which is set to 2c .
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.
Send Frequency	Specifies the type of alerts, which can be either of the following: <ul style="list-style-type: none"> Scheduled: sends alerts every 30 seconds. When a threshold is exceeded: sends alerts when a threshold is exceeded.



Parameter	Description
	 Note <p>If When a threshold is exceeded is selected, you need to further set hardware alert thresholds. For details, see section 3.1.7 Hardware Alert Thresholds.</p>

Table 3-21 SNMPv3 trap parameters

Parameter	Description
Run SNMP at Startup	<p>Controls whether to launch the SNMP trap service when ADS is started.</p> <ul style="list-style-type: none"> Yes: launches the SNMP trap service when ADS is started. No: does not launch the SNMP trap service when ADS is started.
SNMP Version	SNMP protocol supported by the SNMP trap, which is set to 3 .
Authentication Mode	<p>Specifies the authentication modes for different security levels of the SNMPv3 user. The default value is No identity authentication.</p> <p>Options include the following:</p> <ul style="list-style-type: none"> No authentication: does not authenticate users and provides no privacy or encryption function. In this case, only User Name needs to be set. Account authentication: provides only authentication. In this case, User Name and Password need to be set. Private key authentication: provides both authentication and encryption. In this case User Name, Password, Authentication Protocol, Private Key Protocol, and Private Key Password need to be set.
User Name	Specifies the SNMPv3 server user name.
Password	Specifies the password for the SNMPv3 server user.
Authentication Protocol	<p>Specifies the authentication protocol.</p> <p>Options include MD5 and SHA.</p>
Private Key Protocol	<p>Specifies the cipher algorithm for data transmission.</p> <p>Options include DES and AES.</p>
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.
Send Frequency	<p>Specifies the type of alerts, which can be either of the following:</p> <ul style="list-style-type: none"> Scheduled: sends alerts every 30 seconds. When a threshold is exceeded: sends alerts when a threshold is exceeded.  Note <p>If When a threshold is exceeded is selected, you need to further set hardware alert thresholds. For details, see section 3.1.7 Hardware Alert Thresholds.</p>

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 agent parameters.

Table 3-22 SNMPv2c agent parameters

Parameter	Description
Run SNMP at Startup	Controls whether to launch the SNMP agent when ADS is started. <ul style="list-style-type: none"> Yes: launches the SNMP agent when ADS is started. No: does not launch the SNMP agent when ADS is started.
SNMP 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.
Allowed Access IP	IP addresses that are allowed to access the SNMP agent. At most 10 addresses can be typed, with each in a separate line. Leaving it empty means the SNMP agent is accessible to all IP addresses.

Table 3-23 SNMPv3 agent parameters

Parameter	Description
Run SNMP at Startup	Controls whether to launch the SNMP agent when ADS is started. <ul style="list-style-type: none"> Yes: launches the SNMP agent when ADS is started. No: does not launch the SNMP agent when ADS is started.
SNMP 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: <ul style="list-style-type: none"> No authentication: does not authenticate users and provides no privacy or encryption function. In this case, only User Name needs to be set. Account authentication: provides only authentication. In this case, User Name and Password need to be set. Private key authentication: provides both authentication and encryption. In this case User Name, Password, Authentication Protocol, Private Key Protocol, and Private Key Password need to be set.
User Name	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 .

Parameter	Description
Private Key Password	Specifies the key used for encryption.
Allowed Access IP	IP addresses that are allowed to access the SNMP agent. At most 10 addresses can be typed, with each in a separate line. Leaving it empty means the SNMP agent is accessible to all IP addresses.

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 2 Click **Edit**.

Figure 3-50 Editing log sending parameters

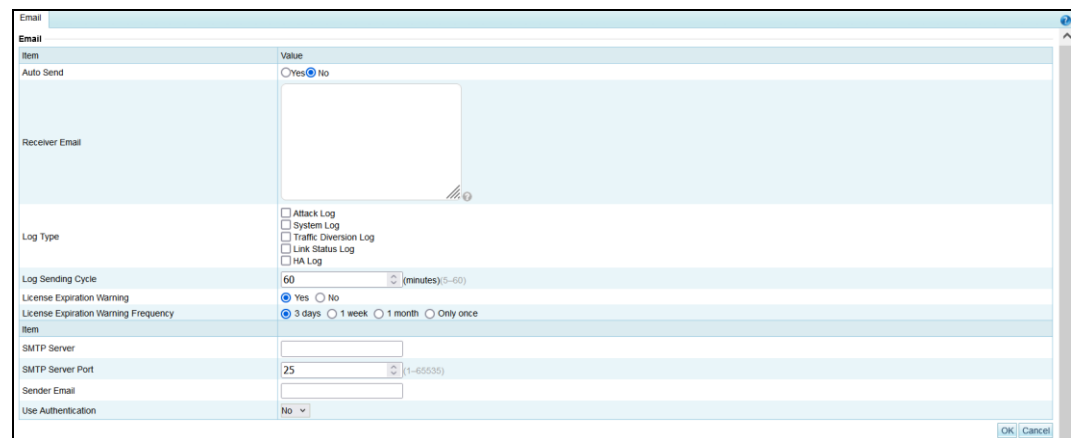


Table 3-24 describes parameters for configuring log sending by email.

Table 3-24 Parameters for configuring log sending by email

Parameter	Description
Auto Send	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 Email and Log Type .
Receiver Email	Email address that receives logs. A maximum of 10 email addresses are allowed, with each in a separate line.
Log Type	Type of logs to be sent, which can be Attack Log , System Log ,

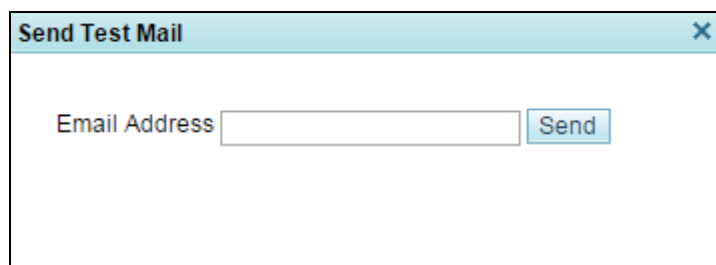
Parameter	Description
	Traffic Diversion Log, Link Status Log, and HA Log. By default, the system sends log messages every 60 minutes.
Log Sending Cycle	Specifies how frequently emails are to be sent. The value range is 5 to 60 minutes.
License Expiration Warning	Controls whether to enable the license 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	Email address that sends logs.
Use Authentication	Specifies whether to authenticate the SMTP user that attempts to send emails. <ul style="list-style-type: none"> 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 User Name/SMTP Password	User name and password for sending emails. The two parameters are available only when you select Yes for Use Authentication .

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

Step 4 Send a test mail.

After email parameters are configured, click **Send Test Mail** to check whether parameters are correctly configured. In the dialog box shown in [Figure 3-51](#), type the email address to receive the test mail.

Figure 3-51 Send Test Mail dialog box



The dialog box titled "Send Test Mail" has a close button (X) in the top right corner. It contains a text input field labeled "Email Address" and a "Send" button.

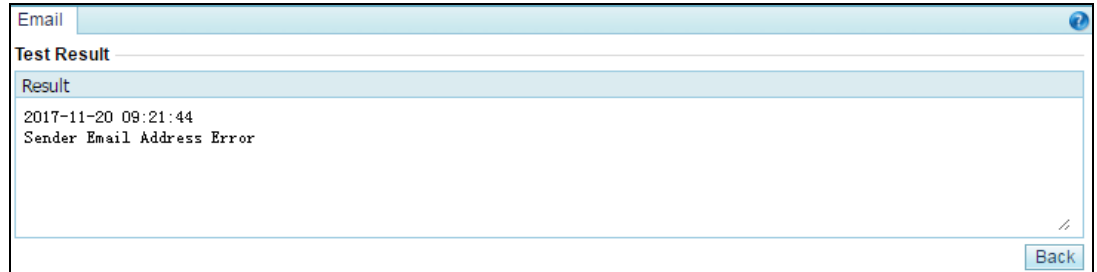
Step 5 Type the receiving address and then click **Send**.


ADS then sends a test mail to the specified address.

Step 6 View the test result.

Click **Test Result**. Then the test result is displayed, as shown in [Figure 3-52](#).

Figure 3-52 Email test result



	<p>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.</p>
---	---

----End

3.3.4 SFTP/SSH Configuration

ADS can be configured to export logs of the protected server to a specified directory via SFTP or SSH.

Choose **System > Log Services > SFTP/SSH**, and then click **Edit** in the **SFTP/SSH Log Server** area. Configure parameters and click **OK** to save the settings.

[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.
User Name	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. Fill in a UNIX absolute path, for example, /tmp/ .
Interval (s)	Interval (unit: second) for exporting logs via SFTP or SSH. The value ranges from 60 to 86400, that is, 1 minute to 1 day.

3.4 Others

This section covers the following topics:

- [License](#)
- [System Upgrade](#)
- [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**. The initial **License** page appears, as shown in [Figure 3-53](#).

Figure 3-53 License Info page before the import of a license

License				
Type	/ ?			
Basic Service Start Date	/			
Basic Service End Date	/			
Processing Capacity (pps)	0			
Processing Capacity (Gbps)	0.00			
Authorized Modules	Module Name	Status	Start Date	End Date
	IPv6	/	/	/
	TI	/	/	/
Holder	/			
Serial No.	/			
License Update <input type="button" value="Browse..."/> No file selected. <input type="button" value="Submit"/> <input type="button" value="Preview"/> <input type="button" value="Export"/>				

After a license is imported, different license information is displayed for hardware and virtual devices, as shown in [Figure 3-54](#) and [Figure 3-55](#).

Figure 3-54 License page on a hardware device after the import of a license

License				
Type	Trial ?			
Basic Service Start Date	2024-10-24			
Basic Service End Date	2025-01-22			
Processing Capacity (pps)	59,520,000			
Processing Capacity (Gbps)	80.00			
Authorized Modules	Module Name	Status	Start Date	End Date
	IPv6	Supported	2024-10-24	2025-01-22
	TI	Supported	2024-10-24	2025-01-22
Holder	1			
Serial No.	6EF4-3913-C59F-5B59			





Figure 3-55 License page on a virtual device after the import of a license

License				
Type	Trial ?			
Basic Service Start Date	2024-10-24			
Basic Service End Date	2025-01-22			
Processing Capacity (pps)	59,520,000			
Processing Capacity (Gbps)	80.00			
Authorized Modules	Module Name	Status	Start Date	End Date
	IPv6	Supported	2024-10-24	2025-01-22
	TI	Supported	2024-10-24	2025-01-22
Holder	1			
Serial No.	6EF4-3913-C59F-5B59			
Authorization Configuration				
Authorization Status	Unknown			
Mode of Authorization	Cloud-based Authentication			
Authorization Center Address	auth.api.nsfocus.com			
Update License	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Submit"/>	<input type="button" value="Preview"/> <input type="button" value="Export"/>
<input type="button" value="Confirm"/>				

[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 .

Parameter		Description
		 Only vADS supports the Subscription license type.
Basic Service Start Date		Date when the current basic service license is produced.  The "current basic service" indicates the service authorized by the current license.
Basic Service End Date		Date when the current basic 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.  The "current basic service" indicates the service authorized by the current license.
Processing Capacity (pps)		Maximum number of packets that ADS can process per second.
Processing Capacity (Gbps)		Maximum bandwidth for traffic cleaning.  If the traffic exceeds the specified maximum bandwidth, ADS will log a system operation alert message.
Authorized Modules		Shows whether the current version supports IPv6 and TI and their respective start date and end date (if supported).
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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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

Parameter		Description
		<p>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.</p> <p>Specifies the server URL of the cloud authorization center:</p> <ul style="list-style-type: none"> 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** page, you can perform the following operations:

- Previewing a license

In the lower-right corner of the **Authorization Configuration** area, 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

In the lower-right corner of the **Authorization Configuration** area, 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.



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


- Exporting a license

In the lower-right corner of the **Authorization Configuration** area, 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 Upgrade

You can manually import the upgrade 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	<ul style="list-style-type: none"> • If the version of the upgrade 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 upgrade package.

Step 3 Click **Upgrade** to start updating the device.

 Note	<p>The update process may take a long time. Wait until an update success message appears.</p> <p>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.</p>
---	--

Step 4 After an upgrade success message appears, restart the system as prompted.

 Note	<p>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.</p>
---	---

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

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

	<p>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.</p>
---	--

----End

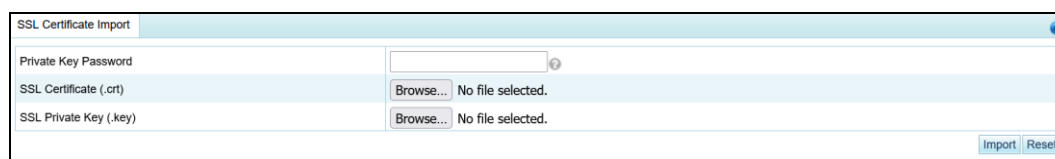
3.4.4 SSL Certificate Import

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 3-56 SSL Certificate Import page



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

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

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

----End

3.4.5 One-Click Inspection

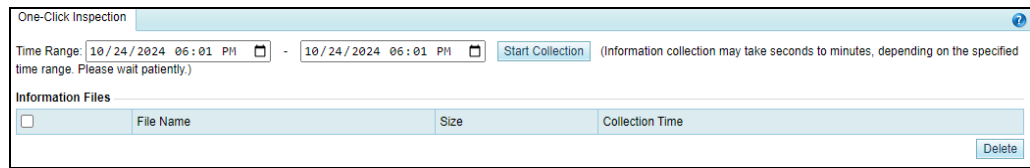
When ADS fails, you can collect device information by using the one-click inspection function, and deliver such information to NSFOCUS technical support, who therefore do not need to log in to ADS for collection of such information.

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**.

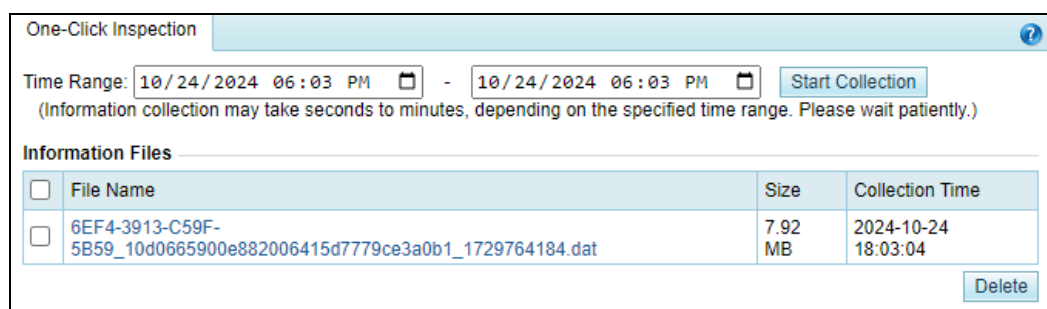
Figure 3-57 One-Click Inspection page



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 **Information Files** list, as shown in [Figure 3-58](#).

Figure 3-58 One-click inspection result



Step 3 Click the file name in the **File Name** 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.

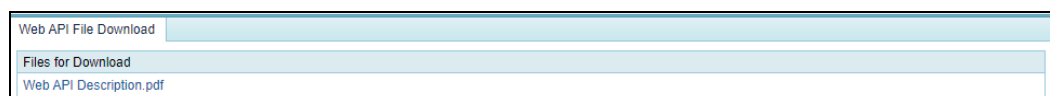
3.4.7 Web API File Download

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 3-59](#), click the file name in the **Files for Download** area to download the file to a local disk drive.

Figure 3-59 Web API File Download page



----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
- Service Board Speed
- Collaboration Status
- System Interfaces

Traffic Trend

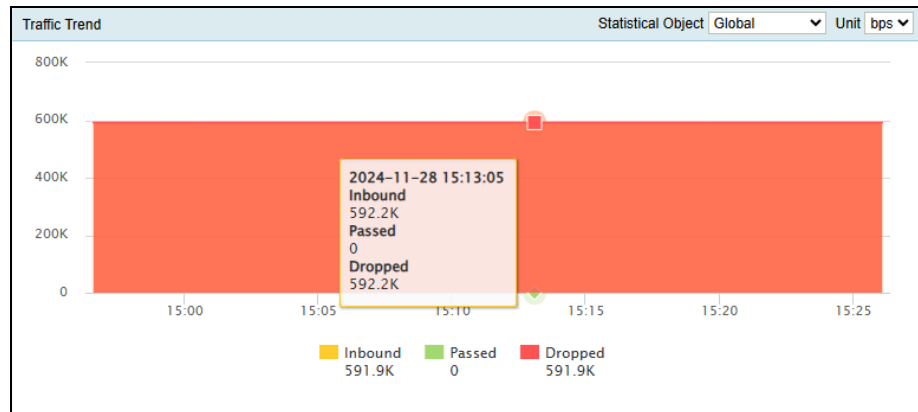
On the **Real-Time Monitoring** page, the **Traffic Trend** area shows traffic received, passed, and dropped by the ADS device in the last 30 minutes, as shown in [Figure 4-1](#). Here, the yellow curve indicates incoming traffic, the green curve outgoing traffic, and the orange curve dropped traffic. 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



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
TCP fragment	— TCP Fragment
ICMP fragment	— ICMP Fragment






















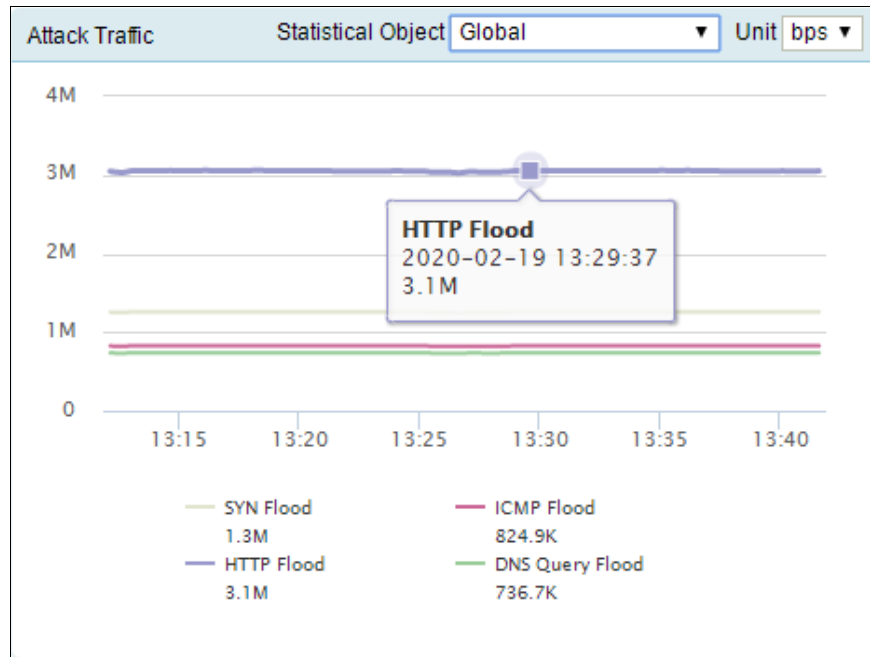
Attack Type	Color Indication
HTTP flood	 HTTP Flood
HTTPS flood	 HTTPS Flood
SIP flood	 SIP Flood
DNS query flood	 DNS Query Flood
DNS amplification	 DNS Amplification
SSDP amplification	 SSDP Amplification
NTP amplification	 NTP Amplification
Chargen amplification	 Chargen Amplification
SNMP amplification	 SNMP Amplification
Memcache amplification	 Memcache Amplification
Manual strategy	 Manual Strategy
Amplification	 Amplification
UDP fragment	 UDP Fragment
DNS flood	 DNS Flood
LAND flood	 LAND Flood
HTTP slow attack	 HTTP Slow Attack
FIN/RST flood	 FIN/RST Flood
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 type, attack start time, attack duration, real-time inbound traffic, and real-time dropped traffic.

If no packet is dropped for a destination IP address, "---" is displayed in **Attack Type**, **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
Dst IP	Attack Type	Attack Start Time	Attack Duration	Real-Time Inbound	Real-Time Dropped
83.91.101.22	SYN Flood	2024-11-28 14:28:34	58min	591.9K	591.9K

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, motherboard temperature, disk status, fan status, power supply status, and engine status. For fan status, power supply status, and engine status,  indicates that the disks, fans, power supply, or engine works properly and  indicates the opposite.


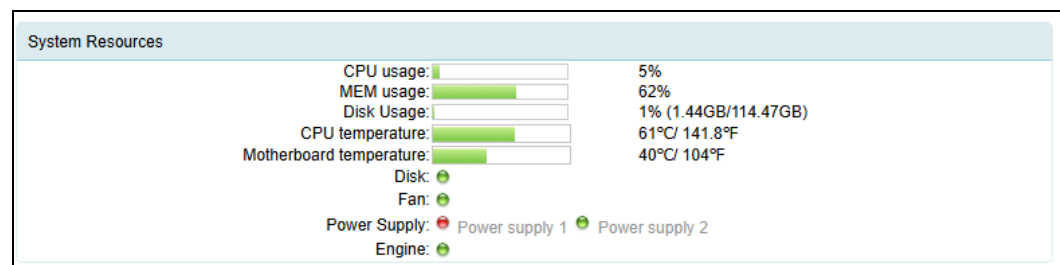
 Note	Only ADS NX3-HD2500, NX5-HD4500, NX5-HD6500, and ADS NX5-HD8500 and some ADS NX5-8000 devices have the power supply status displayed.
--	---

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



System Resources of 6U Devices

The 6U devices refer to ADS NX5-10000, ADS NX5-12000, and ADS NX5-20000.



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, engine status, CPU usage, memory usage, disk usage, CPU temperature, motherboard temperature, and fan status. For fan status, power on status, and engine status,  indicates that the fans, power supply, or engine 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:

2

Power Supply:

Boards

Slot	Power on Status	Engine	Disk	CPU Usage	Memory Usage	Disk Usage	CPU temperature	Motherboard temperature	Fan
1*	<div></div>	<div></div>	<div></div>	5%	60%	35%	66°C/150.8°F	47°C/116.6°F	<div></div>
2	<div></div>	<div></div>	<div></div>	5%	53%	31%	60°C/140°F	43°C/109.4°F	<div></div>
3	<div></div>	<div></div>	<div></div>	0%	0%	0%	0°C/32°F	0°C/32°F	<div></div>
4	<div></div>	<div></div>	<div></div>	0%	0%	0%	0°C/32°F	0°C/32°F	<div></div>
5	<div></div>	<div></div>	<div></div>	0%	0%	0%	0°C/32°F	0°C/32°F	<div></div>
6	<div></div>	<div></div>	<div></div>	0%	0%	0%	0°C/32°F	0°C/32°F	<div></div>

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-HD6000, 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 All Interfaces ▼					
Interface	Status	IN (pps)	OUT (pps)	IN (bps)	OUT (bps)
G3/1	 Up	1K	0.2	592.2K	188
G3/2	 Up	0.5	0	256	0
G3/3	 Up	0.2	0	128	0
G3/4	 Down	0	0	0	0
Total		1K	0.2	592.6K	188

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
- Carpet Bombing Protection
- [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 [5.1.1.7 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 Protection Groups**: 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.
- **Generating a Group Policy Template**: create a group policy template based on the configured protection policies.
- **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

The screenshot shows a web-based configuration window titled 'Protection Groups'. It contains three input fields: 'Group Name', 'Description', and 'Template'. The 'Group Name' and 'Description' fields have red asterisks indicating they are required. The 'Template' field is a dropdown menu currently showing 'test'. At the bottom right, there are 'Next' and 'Cancel' buttons.

[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.

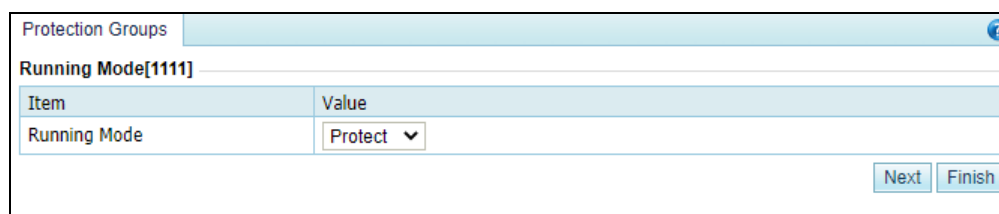
You can select the running mode from three values: **Protect**, **Alert**, and **Forward**.

- **Protect**: After protection policies take effect, ADS starts to protect traffic of the protection group.
- **Alert**: 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.

	<p>All protection policies are constrained by the running mode as follows when an attack is detected:</p> <ul style="list-style-type: none"> • Protect mode: generates an alert and drops attack packets. • Alert mode: generates alerts without dropping attack packets. • Forward mode: does not provide any protection.
---	--

After a 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



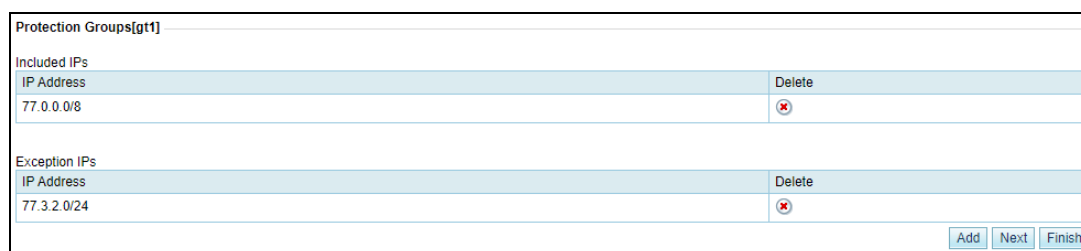
The screenshot shows a window titled "Protection Groups" with a sub-header "Running Mode[1111]". Below this is a table with two columns: "Item" and "Value". The "Item" column contains "Running Mode" and the "Value" column contains a dropdown menu currently set to "Protect". At the bottom right of the window are two buttons: "Next" and "Finish".

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



The screenshot shows a window titled "Protection Groups[gt1]". It has two sections: "Included IPs" and "Exception IPs". Each section has a table with "IP Address" and "Delete" columns. In the "Included IPs" section, there is one entry: "77.0.0.0/8". In the "Exception IPs" section, there is one entry: "77.3.2.0/24". At the bottom right of the window are three buttons: "Add", "Next", and "Finish".



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

Add IP[gtt]

Included IPs


Exception IPs

OK

Cancel


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	<p>You can type IPv4 or IPv6 addresses or segments, with one in each line, in the following formats:</p> <ul style="list-style-type: none"> 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. <div>  <div> <p>Protection IP ranges of different protection groups must not overlap. The exception IP addresses configured will not be protected.</p> <ul style="list-style-type: none"> If one and only one IP address configured here is in use by another protection group, the system will give a prompt. After you click OK in the confirmation dialog box, the system will automatically move the IP address to the exception IP list of that group. Exception IP addresses, if any, will not be protected under the current group. </div> </div>

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

Deleting an IP Address or IP Address Range

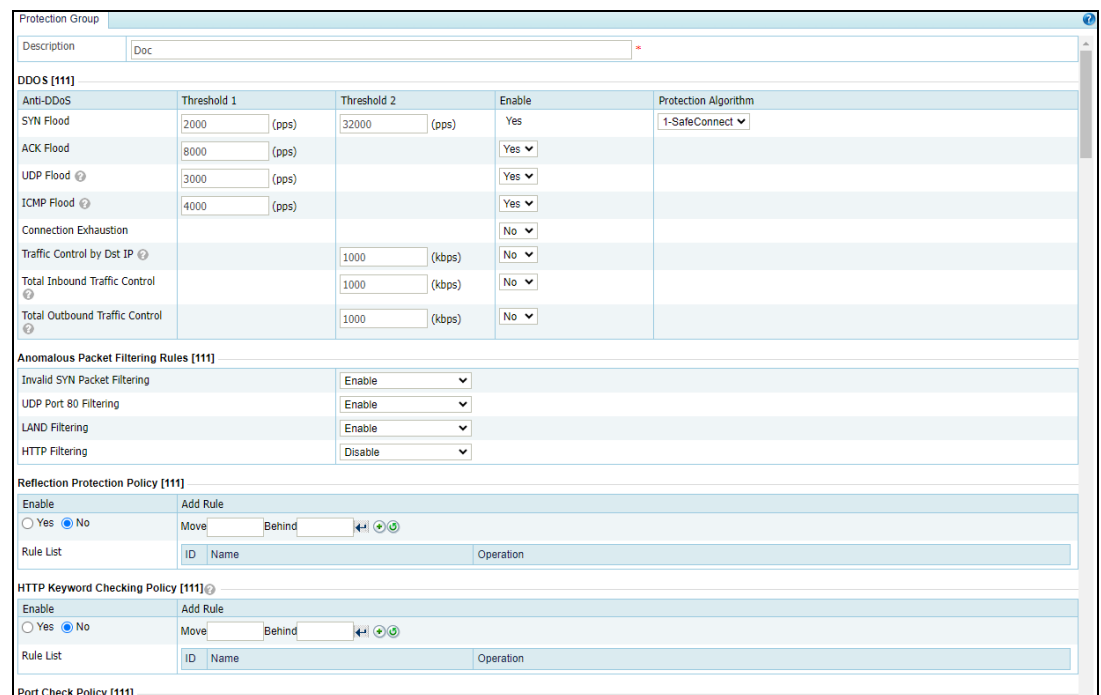
On the IP list shown in [Figure 5-3](#), click  in the **Delete** column of an IP address or IP address range and click **OK** in the confirmation dialog box to delete this IP address or IP address range.

 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



The screenshot displays the 'Protection Group' configuration window. It includes a 'Description' field with the value 'Doc'. Below this, several policy sections are visible:

- DDOS [111]**: A table with columns for policy name, Threshold 1, Threshold 2, Enable, and Protection Algorithm. Policies include SYN Flood, ACK Flood, UDP Flood, ICMP Flood, Connection Exhaustion, Traffic Control by Dst IP, Total Inbound Traffic Control, and Total Outbound Traffic Control.
- Anomalous Packet Filtering Rules [111]**: A table with columns for rule name and Enable status. Rules include Invalid SYN Packet Filtering, UDP Port 80 Filtering, LAND Filtering, and HTTP Filtering.
- Reflection Protection Policy [111]**: Includes an 'Enable' section with radio buttons for 'Yes' and 'No' (selected), and an 'Add Rule' section with a 'Move' dropdown and 'Behind' button.
- HTTP Keyword Checking Policy [111]**: Similar to the Reflection Protection Policy, with 'Enable' radio buttons and an 'Add Rule' section.
- Port Check Policy [111]**: Partially visible at the bottom.

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 Allowlist

Specify whether to enable the allowlist and the proxy monitoring. For details about the allowlist function, see section [5.2.1 Allowlist](#).

Setting a Group-specific DNS Subdomain Allowlist

Specify whether to enable the DNS subdomain allowlist and configure primary domain and action for unmatched DNS requests.

- **Enable:** It is **No** by default. The global DNS subdomain allowlist has a higher priority than the group-specific allowlist of DNS subdomains. If both are enabled, only the global DNS subdomain allowlist takes effect. For details about the global DNS subdomain allowlist, see section [5.2.12 DNS Subdomain Allowlist](#).
- **Primary Domain:** Enter each primary domain name in a separate line. At most three can be configured. Only DNS requests matching a primary domain name are further matched against the subdomain allowlist. Leaving this field empty indicates that all DNS requests are deemed to be a match.
A primary domain name should meet the following requirements:
 - A primary domain name only consists of letters, digits, dots, hyphens, and/or underscores.
 - Each label of the primary domain name ranges from 1 to 63 characters, and the primary domain name cannot exceed 128 characters.
 - The primary domain name should contain at least one label.
 - A label cannot start or end with a hyphen, nor have consecutive hyphens.
- **Action for Unmatched DNS Requests:** controls DNS requests matching the primary domain list but not the subdomain list. Options include **Default**, **Limit rate**, and **Drop**. If the subdomain list is empty, this action does not work. Before setting an action, configure a valid DNS subdomain allowlist for the group. You can add a group-specific allowlist of DNS subdomains when editing the access policy of the protection group. For detailed parameters, see section [5.2.12 DNS Subdomain Allowlist](#).
- **Subdomain Allowlist Auto-Learning:** Configure auto-learning parameters only after the auto-learning function of DNS subdomain allowlist is enabled. For descriptions of the parameters, see Table 5-46.

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

Specify whether to enable the blocklist, lockout period, and whether to enable proxy monitoring. For details about the blocklist function, see section [5.2.5 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 [5.2.4 GeoIP Rules](#).

Setting Group-specific TI

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 TI, see section [8.4 Collaboration with TI](#).



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

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

Protection Group							
URL Rule (applicable to HTTP protection only) [111]							
ID	Domain Name or IP	URL	Dst IP	Dst Port	SYN Cookie URL	Algorithm	Operation
							<input type="button" value="Add"/> <input type="button" value="Finish"/>

Adding a URL Protection Rule

- 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

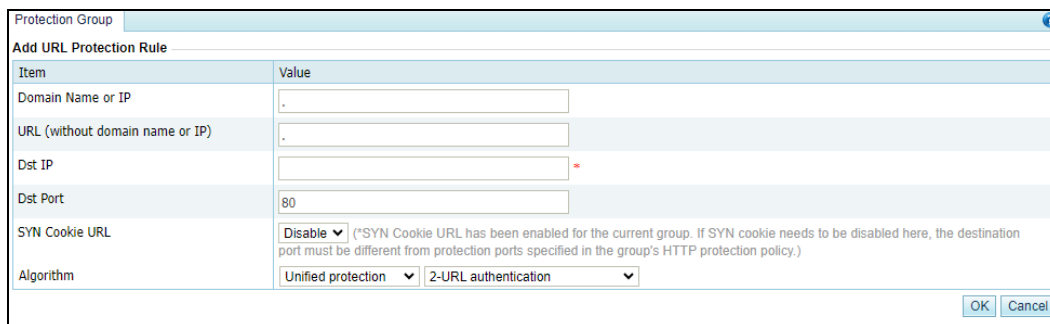


Figure 5-8 Adding a URL protection rule — precision protection

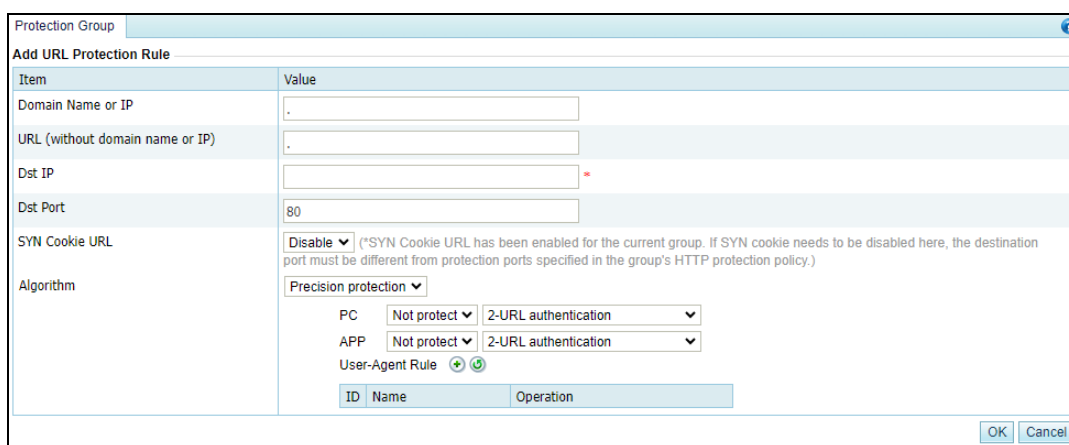




Table 5-3 describes parameters for creating a URL protection rule.


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 (without 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.
Dst 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.
Dst 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 .


Parameter	Description
	The setting of this parameter depends on whether SYN Cookie URL is enabled for HTTP protection.
Algorithm	<p>Protection mode and policy adopted for packets matching URL protection rules. For detailed parameter descriptions, see Table 5-13.</p> <p> Note</p> <p>Protection algorithms are used together with the SYN Cookie URL function.</p> <ul style="list-style-type: none"> 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 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 a group name or IP address. Fuzzy matching is supported.
- Specify a running mode. By default, protection groups of all running modes (**Protect**, **Alert**, 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


Protection Group					
Group [x11]					
Item	Value				
Group Name	p11				
Group Description	th				
Running Mode [x11]					
Protect					
Included IPs [x11]					
67.60.20.0/24					
Exception IPs [x11]					
DDoS [x11]					
Attack Type	Threshold 1	Threshold 2	Enable	Protection Algorithm	
SYN Flood	1 (pps)	32000 (pps)	Yes	1-SafeConnect	
ACK Flood	8000 (pps)		Yes		
UDP Flood (x)	100 (pps)		Yes		
ICMP Flood (x)	4000 (pps)		Yes		
Connection Exhaustion			No		
Traffic Control by Dst IP		1000 (kpps)	No		
Total Inbound Traffic Control		1000 (kpps)	No		
Total Outbound Traffic Control		1000 (kpps)	No		
Anomalous Packet Filtering Rules [x11]					
Invalid SYN Packet Filtering			Enable		
UDP Port 80 Filtering			Enable		
LAND Filtering			Enable		
HTTP Filtering			Disable		
Reflection Protection Policy [x11]					
Enable	Rule	Description	Protocol	Src Port	Action
No					
HTTP Keyword Checking Policy [x11] (x)					

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 running mode, IP list, 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 change the 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 allowlist

On the protection group list, click **Allowlist** in the **Access Policy** column. Click **Edit** to modify the status of the allowlist and proxy monitoring. After the allowlist is enabled, you can view, add, search, import, export, and clear the allowlist. For details, see section [5.2.1 Allowlist](#).
 - 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 [5.2.2 Access Control Rules](#).

- Edit the blocklist

On the protection group list, click **Blocklist** in the **Access Policy** column. Click **Edit** to edit the blocklist. For details, see section [5.2.5 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 [5.2.4 GeoIP Rules](#).


- Edit group-specific TI policies

On the protection group list, click **TI** in the **Access Policy** column to edit the TI policy for the protection group. Click **Edit** to enable TI and specify the protection policy.

- Edit group-specific DNS subdomain allowlist

On the protection group list, click **DNS Subdomain Allowlist** in the **Access Policy** column. Click **Edit** to enable DNS subdomain allowlist and its auto-learning, and specify primary domains, action for unmatched DNS requests, and auto-learning parameters. After the DNS subdomain allowlist is enabled, you can view, add, search, import, export, and clear the DNS domain allowlist. For details, see section [5.2.12 DNS Subdomain Allowlist](#).


- 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), click **Delete** to the lower right of the list, and then click **OK** in the confirmation dialog box to delete them.



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 Generating a Group Policy Template

After creating a protection group and configuring its policies, you can save it as a group policy template for application to protection groups of the same businesses.

Choose **Policy > Anti-DDoS > Protection Groups**, and click  in the **Operation** column. On the **Generate Group Policy Template** page that appears, type a template name and

description, and click **OK**. The policy template will then be displayed and managed on the **Group Policy Template** page. For details, see section [5.1.3 Protection Group Policy Templates](#).



The group policy template references the policies configured (see section [5.1.2 Policy Configuration for Protection Groups](#)), but excludes IP addresses on the blocklist/allowlist, access control rules with other IP addresses than 0.0.0.0:: as destination IP addresses, and URL rules.

5.1.1.7 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

Protection Group									
Group Name or IP		Running Mode	All	Filter	First < Previous Next > Last 1/1 Go to				
<input type="checkbox"/>	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
<input type="checkbox"/>	default_protection_group	Protect			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		-	all_users	
<input type="checkbox"/>	jd1	Protect			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	fh	
<input type="checkbox"/>	test333	Protect			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	fh	
<input type="checkbox"/>	111	Alert			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	Doc	

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** 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

Auto-learning Parameter Configuration

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


Save and Start

Save

Cancel

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 , 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: <ul style="list-style-type: none"> 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 five ports or port ranges separated by the comma like "80,90-92". <div>  <p>Note</p> <p>Ports specified here cannot overlap with those specified for HTTPS protection.</p> </div>

Parameter	Description
HTTP Protection Object	<p>Specifies the object of HTTP protection, which can be either of the following:</p> <ul style="list-style-type: none"> 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

Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
default_protection_group	Protect			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		-	all_users	
js1	Protect			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Ongoing(Automatic) [Manual Stop Icon]	fh	
test333	Protect			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started [Start Icon]	fh	
111	Alert			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started [Start Icon]	Doc	

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

You can also click [Manual Stop Icon] to manually stop the auto-learning process.

For ongoing auto-learning, you can click [Edit Icon] in the **Auto-learning** 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

Item	Value
Learning Duration	1 day
Percentage of Increase	50%
Policy Application Mode	Automatic
Policy Name	<input checked="" type="checkbox"/> SYN Flood Threshold 1 <input checked="" type="checkbox"/> ACK Flood Threshold 1 <input checked="" type="checkbox"/> UDP Flood Threshold 1 <input checked="" type="checkbox"/> ICMP Flood Threshold 1 <input checked="" type="checkbox"/> HTTP GET Flood Threshold 1 <input checked="" type="checkbox"/> HTTP POST Flood Threshold 1
HTTP Protection Port	80 (Port Range) ?
HTTP Protection Object	<input checked="" type="radio"/> Destination IP/Port <input type="radio"/> Destination IP/Port/URL

Save Cancel

----End

Viewing the Auto-learning Status

On the page shown in Figure 5-10, the **Auto-learning** 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


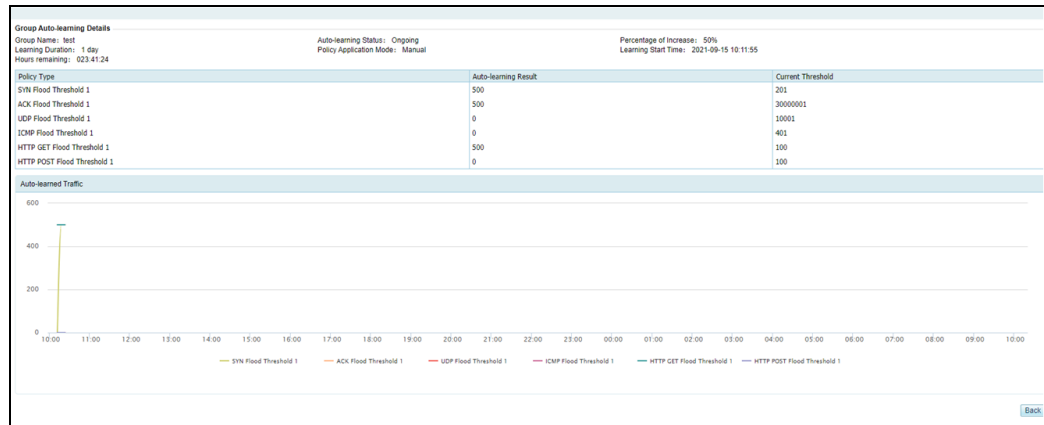
On the page shown in Figure 5-10, you can click  in the **Auto-learning** column of a protection group to view auto-learning details of the group.

Figure 5-14 Auto-learning details



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
- SSL/TLS keyword checking 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

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

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

Figure 5-15 DDoS protection policy

DDoS [default_protection_group]					
Anti-DDoS	Threshold 1	Threshold 2	Enable	Protection Algorithm	
SYN Flood	2000 (pps)	2000 (pps)	Yes	1-SafeConnect ▾	
ACK Flood	8000 (pps)		Yes ▾		
UDP Flood ⓘ	1000 (pps)		Yes ▾		
ICMP Flood ⓘ	4000 (pps)		Yes ▾		
Connection Exhaustion			Yes ▾		
Traffic Control by Dest IP ⓘ		1000 (kbps)	No ▾		
Total Inbound Traffic Control ⓘ		1000 (kbps)	No ▾		
Total Outbound Traffic 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
Anti-DDoS	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.
Enable	Controls whether to enable the protection. <ul style="list-style-type: none"> 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 threshold for the SYN traffic rate. When 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 threshold for the rate (pps) of reverse detection packets in response to SYN packets to a destination, 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.



- 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%.

- **Enable:** 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 the threshold for ACK traffic rate. When 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 the threshold for UDP traffic rate. When 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 threshold for ICMP traffic rate. When 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 [5.2.8 Connection Exhaustion Protection Rules](#).)

Traffic Control by Dst IP

Threshold 2: specifies the maximum traffic, in kbps, allowed to reach a destination IP address in the protection group. Traffic above the specified value will be dropped. The value ranges from 0 to 48000000.

This policy is disabled by default. You can enable it for protection.

Total Inbound Traffic Control

Threshold 2: specifies the maximum traffic, in kbps, allowed to reach all destination IP addresses in the protection group. Traffic above the specified value will be dropped. The value ranges from 0 to 48000000.

This policy is disabled by default. You can enable it for protection.

Total Outbound Traffic Control

- **Threshold 2:** specifies the maximum outbound traffic of the protection group. Traffic above the specified value will be is dropped. The value ranges from 0 to 167772160.
- This policy is disabled by default. You can enable it for protection.



- 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 [default_protection_group]	
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 about reflection protection rules, see section [5.2.3 Reflection Protection Rules](#).

Figure 5-17 shows the reflection protection policy.

















 <p>Note</p>	<ul style="list-style-type: none"> 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

Reflection Protection Policy [default_protection_group]												
Enable <input type="radio"/> Yes <input checked="" type="radio"/> No		Add Rule Move <input type="text"/> Behind <input type="text"/>   										
Rule List		<table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ARMS--</td> <td>   </td> </tr> <tr> <td>2</td> <td>SNMP--</td> <td>   </td> </tr> </tbody> </table>		ID	Name	Operation	1	ARMS--	 	2	SNMP--	 
ID	Name	Operation										
1	ARMS--	 										
2	SNMP--	 										

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






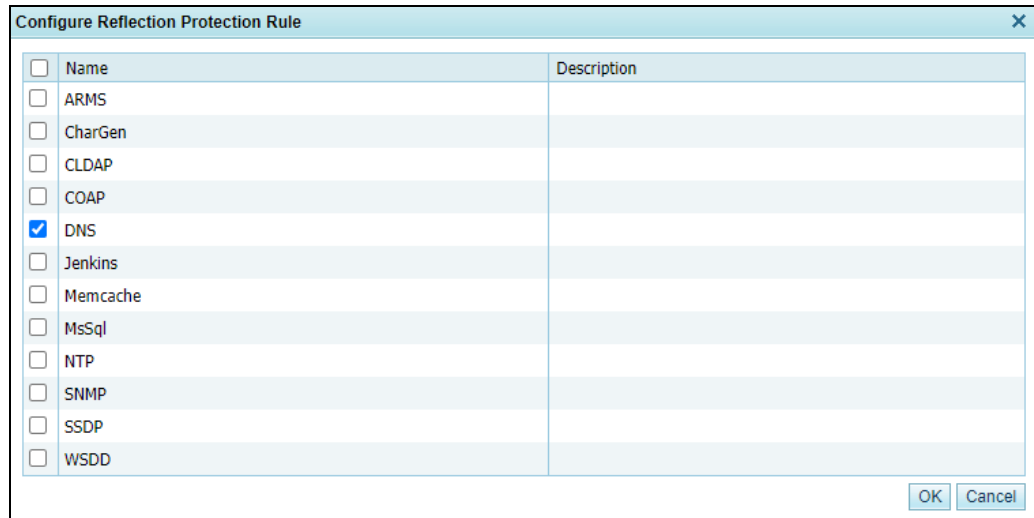
- **Enable:** Select **Yes** or **No** to enable or disable the policy.
- **Rearrange rules:** Click  or  to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3** indicates that the first rule will be put below the 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 [5.2.3.1 Creating a Reflection Protection Rule](#).
- **Delete a rule:** Click  to delete the rule.

Figure 5-18 Adding reflection protection rules



The dialog box titled "Configure Reflection Protection Rule" contains a table with two columns: "Name" and "Description". The "Name" column lists various protocols: ARMS, CharGen, CLDAP, COAP, DNS (checked), Jenkins, Memcache, MsSql, NTP, SNMP, SSDP, and WSDD. Each protocol has a corresponding checkbox. At the bottom right, there are "OK" and "Cancel" buttons.

Name	Description
<input type="checkbox"/> ARMS	
<input type="checkbox"/> CharGen	
<input type="checkbox"/> CLDAP	
<input type="checkbox"/> COAP	
<input checked="" type="checkbox"/> DNS	
<input type="checkbox"/> Jenkins	
<input type="checkbox"/> Memcache	
<input type="checkbox"/> MsSql	
<input type="checkbox"/> NTP	
<input type="checkbox"/> SNMP	
<input type="checkbox"/> SSDP	
<input type="checkbox"/> WSDD	

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.


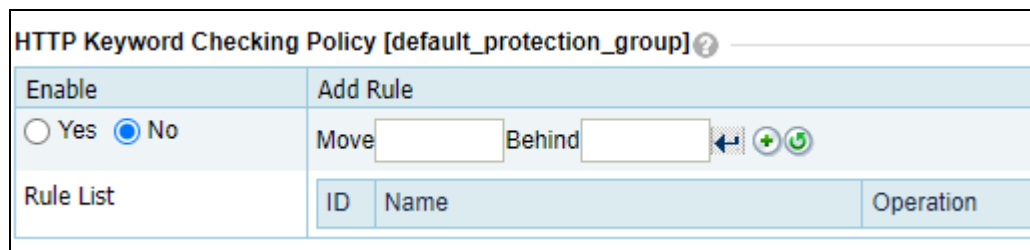
 Note	<ul style="list-style-type: none"> When multiple rules are referenced, the HTTP keyword checking policy matches attack packets with these rules in a top-down manner. In principle, the matching stops once a rule is hit. The administrator may need to adjust the rule sequence as required. When multiple rules are hit, ADS performs protection based on the first rule.
--	--



Figure 5-19 HTTP keyword checking policy





The interface shows the "HTTP Keyword Checking Policy [default_protection_group]" configuration. It includes an "Enable" section with "Yes" and "No" radio buttons (currently "No" is selected). There is an "Add Rule" button and a "Move" section with text boxes for "Move" and "Behind", followed by navigation icons. Below is a "Rule List" table with columns "ID", "Name", and "Operation".

HTTP Keyword Checking Policy [default_protection_group] ?		
Enable <input type="radio"/> Yes <input checked="" type="radio"/> No		
Add Rule Move <input type="text"/> Behind <input type="text"/>		
Rule List		
ID	Name	Operation

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

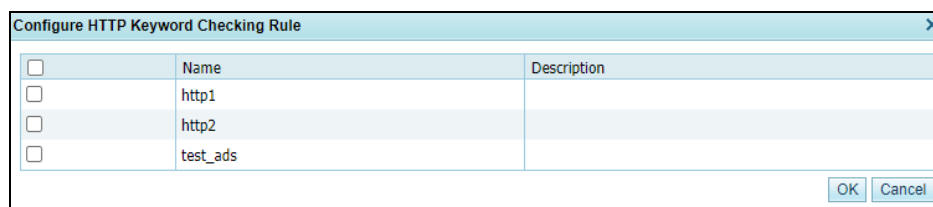
- Enable:** Select **Yes** or **No** to enable or disable the policy.
- Adjust rule sequence: Click  or  in the **Operation** column to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes.

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



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 5-21 shows the port check policy. [Table 5-6](#) describes parameters 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 the rule.

Figure 5-21 Port check policy

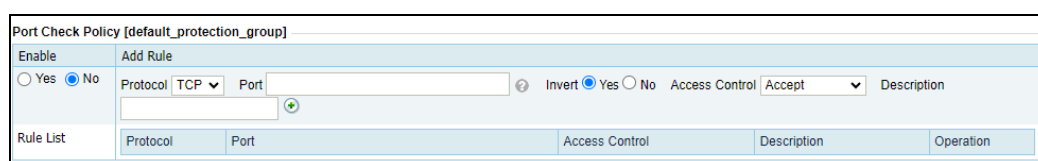



Table 5-6 Parameters of a port check policy

Parameter	Description
Enable	Controls whether to enable this policy. <ul style="list-style-type: none"> • Yes: enables the policy. • No: disables the policy.
Protocol	Specifies the protocol, which can be TCP or UDP .






Parameter	Description
Port	Specifies ports 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. <ul style="list-style-type: none"> Accept: allows packets from the specified port to pass through ADS. Drop: drops such packets. Drop+blocklist: 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 SSL/TLS Keyword Checking Policy

SSL/TLS keyword checking is a process by which ADS parses the TLS-encrypted handshake packets from a source IP address and checks specific fields against keywords. Then, ADS takes the specified action against those packets that match a rule.

 Note	<ul style="list-style-type: none"> A protection policy can reference 10 SSL/TLS keyword checking rules at most. When multiple rules are referenced, the SSL/TLS keyword checking policy matches handshake packets with these rules in a top-down manner. In principle, the matching stops once a rule is hit. You can adjust the rule sequence as required. When multiple rules are matched, ADS performs protection based on the first rule.
--	--

You can perform the following operations on the SSL/TLS keyword checking policy:

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

For how to create an SSL/TLS keyword checking rule, see section [5.2.7 SSL/TLS Keyword Checking](#).

5.1.2.7 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 [5.2.5 Blocklist](#).

HTTPS protection policies are classified into four types:

- **Connection Protection – Renegotiation Protection:** The system checks HTTPS packets from clients. When **Add Abnormal IP to Blocklist** is set to **Yes**, the system adds source IP addresses that match the HTTPS protection algorithm to the blocklist.
- **Connection Protection – Fingerprint Protection:** The system checks HTTPS client hello packets for fingerprints. Those packets identified with abnormal fingerprints will be rate-limited or added to the blocklist, depending on the action configured.
- **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	<p>Specifies the port to protect.</p> <p>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.</p> <p>The port configured for the HTTP protection policy must be different from that for the HTTPS protection policy.</p> <p> Note</p> <p>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.</p>
Protection Threshold	<p>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.</p>

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 Blocklist	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.

Connection Protection – Fingerprint Protection

The fingerprint protection policy checks fingerprints contained in HTTPS client hello packets, and then filters and handles packets that contain abnormal fingerprints, based on the parameters listed in [Table 5-9](#).

Table 5-9 Parameters of the HTTPS fingerprint protection policy

Parameter	Description
Enable	Controls whether to enable the HTTP fingerprint protection policy.
Statistical Period	Period of time when the number and proportion of packets containing a specific fingerprint to a certain destination IP address are counted. Value range: 1–3600, in seconds.
Number of Visits	Number of packets containing a specific fingerprint destined for an IP address. Value range: 1–1000000.
Proportion of Visits	Proportion of client hello packets with the specified fingerprint to the total client hello packets to a destination IP address in a statistical period. Value range: 1%–100%.
Action	<p>Protective measure against packets with the fingerprint that meet both the Number of Visits and Proportion of Visits settings.</p> <ul style="list-style-type: none"> Limit rate: limits the number of packets with matching fingerprint passing through ADS based on the specified threshold. Excessive packets will be dropped. Value range: 0–6000000, in pps. Add to blocklist: adds the source IP address of packets with matching fingerprint to the blocklist. To select this option, you must enable the blocklist function in advance. For details about this function, see section 5.2.5 Blocklist.
Execution Time	<p>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.</p> <p>This parameter must be configured when the action is set to Limit rate.</p>

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 5-10 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 5-10 Application layer protection – non-decrypted traffic protection parameters

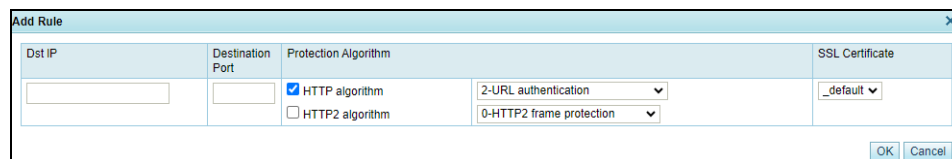
Parameter	Description
Enable	Controls whether to enable the access rate-based protection, resource-specific access protection, and large resource access protection. If you select No , the corresponding protection type of non-decrypted traffic will not take effect.
Large Resource Threshold	Specifies the 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.
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



- b. **Table 5-11** describes parameters for creating an application layer protection – decrypted traffic protection rule.

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

Parameter	Description
Dst 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 5-12 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	<p>Connection control items. New connections, failed connections, and timeout connections only work for destination IP addresses and ports under application layer protection.</p> <ul style="list-style-type: none"> • New Connections: limits the number of new HTTPS connections initiated by a source IP address to the specified destination port. • Failed Connections: 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 Validation Failures: performs RFC authentication on HTTP2 packets from source IP addresses.
Threshold	<p>Threshold of each control item:</p> <ul style="list-style-type: none"> • New Connections: 1–65535 • Failed Connections: 1–256 • Connection Timeout: 1–1000 • HTTP2 RFC Validation Failures: 1–64
Action	<p>Action taken on packets from clients or IP addresses of clients, which can be either of the following:</p> <ul style="list-style-type: none"> • 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.

Parameter	Description
	<ul style="list-style-type: none"> Add to blacklist: If a client fails to be authenticated by an HTTPS protection algorithm, the system identifies its IP address as an abnormal one and adds it to the blacklist to block it. You need to enable the blacklist function before setting this action. For details about the blacklist, see section 5.2.5 Blacklist.

----End

5.1.2.8 HTTP Protection Policy

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

- HTTP Get Flood:** 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:** 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.
- Slow Aattck 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:** If SYN Cookie URL is enabled, this protection mechanism also applies to new connections.

Figure 5-23 shows the HTTP protection policy.


Figure 5-23 HTTP protection policy



HTTP Protection Policy [default_protection_group]				
HTTP Protection	SYN Cookie URL	Protection Target	Protection Port	
Full protection ▼	Enable ▼	Destination IP/Port ○ Destination IP/Port/URL	80 (Port Range) ⓘ	
	Policy	Threshold 1	Threshold 2	Protection Algorithm
	HTTP Get Flood	100 (pps)		Proxy Protection Disable ▼ Custom Field
	HTTP Post Flood	100 (pps)		(Proxy fields "X-Forwarded-For" and "Cdn-Src-Ip" are supported.)
	Slow Attack Protection	1000 (pps)	500 (Bytes)	Unified protection ▼ 2-URL authentication ▼ Template Name -- ▼
				Status Enable ▼
				Status Disable ▼


Table 5-13 describes parameters for configuring the HTTP protection policy.

Table 5-13 Parameters for configuring the HTTP protection policy

Parameter	Description
HTTP Protection	<p>Specifies the HTTP protection mode, which can be one of the following:</p> <ul style="list-style-type: none"> Full protection: Both group protection and URL rule protection are provided. Only for URL rules: 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.

Parameter		Description
		<ul style="list-style-type: none"> 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. 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 for URL rules automatically disables SYN Cookie URL.
Protection Target		<p>Specifies the protection target, which can be either of the following:</p> <ul style="list-style-type: none"> 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.
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	<p>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.</p> <p> Note</p> <p>Enabling proxy protection automatically disables SYN Cookie URL.</p>
	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	<p>Specifies the HTTP GET protection mode, which can be either of the following:</p> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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	<p>Specifies the protection algorithm, which can be one of the following, with 2_URL authentication as the default:</p> <ul style="list-style-type: none"> 0_TAG authentication and 1_HTTPCOOKIES authentication verify the destination IP address by adding authentication information

Parameter		Description
		<p>into HTTP packets.</p> <ul style="list-style-type: none"> • 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 check 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). <p> Note</p> <ul style="list-style-type: none"> • 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 5.1.6 Response Page Settings .
	User-Agent Rule	<p>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.</p> <p>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 5.1.8 Mobile User-Agent Rules.</p>
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	<p>Controls whether to enable or disable HTTP POST flood protection.</p> <ul style="list-style-type: none"> • HTTP Post Flood protection can be enabled only when HTTP Protection is set to Full protection or Only for URL rules. • 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

Parameter	Description
	<p>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.</p> <p> Note</p> <p>Setting HTTP Protection to Not protect or Only for URL rules automatically disables low-and-slow attack protection.</p>

5.1.2.9 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 policy.


 Note	<ul style="list-style-type: none"> 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


DNS Keyword Checking Policy [default_protection_group]								
Enable	Add Rule							
<input type="radio"/> Yes <input checked="" type="radio"/> No	Move <input type="text"/> Behind <input type="text"/> 							
Rule List	<table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>		ID	Name	Operation			
ID	Name	Operation						





Table 5-14 describes parameters of the DNS keyword checking policy.

Table 5-14 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

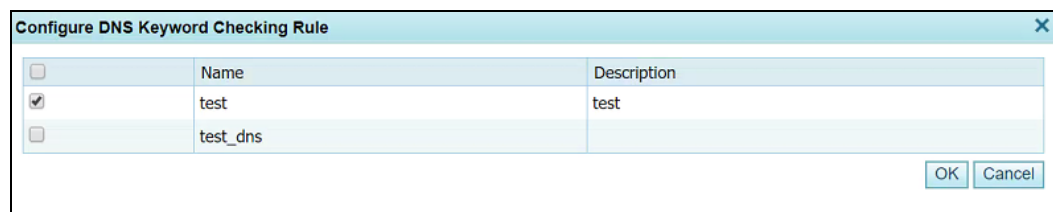
Parameter	Description
	default DNS keyword checking policy.
Action	Specifies the action that ADS will take against the source IP address (host). For details, see section 5.2.11 DNS Keyword Checking .

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 [5.2.11 DNS Keyword Checking](#).

Figure 5-25 Configuring DNS keyword checking rules







5.1.2.10 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

DNS Protection Policy [default_protection_group]			
Protection Type	Enable	Parameter Configuration	
DNS Query	<input checked="" type="radio"/> Yes <input type="radio"/> No	Protection Algorithm 	2-TCP_BIT  Algorithm 2-TCP_BIT is applicable to DNS cache servers.
		Reverse Detection Rate	32000 (pps)
DNS Response	<input type="radio"/> Yes <input checked="" type="radio"/> No	Protection Algorithm	2-DNS retransmission 
		Action	Accept+trust 

[Table 5-15](#) describes parameters of the DNS protection policy.

Table 5-15 Parameters of the DNS protection policy

Parameter		Description
DNS Query	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_NS , 4-DNS retransmission , 5-DNS_CNAME , and 6-DNS_NS&CNAME . Before selecting an algorithm, check the DNS server type. <ul style="list-style-type: none"> Algorithm 1-Default is applicable to authoritative DNS servers and DNS cache servers and can work only with traffic control settings in the UDP protection policy. Algorithm 2-TCP_BIT is applicable to DNS cache servers. Algorithm 3-DNS_NS is applicable to authoritative DNS servers. Algorithm 4-DNS retransmission is applicable to DNS cache servers. Algorithm 5-DNS_CNAME is applicable to authoritative DNS servers. Algorithm 6-DNS_NS&CNAME is applicable to authoritative DNS servers.
	Reverse Detection Rate	Specifies the maximum rate of reverse detection packets. The value ranges from 1 to 240000000.
DNS Response	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: <ul style="list-style-type: none"> Accept: passes through DNS responses authenticated by the protection algorithm Accept+trust: passes through DNS responses authenticated by the protection algorithm and adds the source IP address of these responses to the trust list.



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.

5.1.2.11 TCP Control Parameters Protection Policy

[Figure 5-27](#) shows the TCP control parameters protection policy.

Figure 5-27 TCP control parameters

TCP Control Parameters [default_protection_group]		
Targeting	<input checked="" type="radio"/> Destination IP/Port <input type="radio"/> Dst IP	
SYN Control	SYN Time Sequence Check	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Retransmission Interval	22 (2750 ms) - 28 (3500 ms)
	Source Bandwidth Limit	Disable
	Per Source IP Rate Limit	0 (pps)
SYN-ACK Control	SYN-ACK Learning Mode	<input type="radio"/> Yes <input checked="" type="radio"/> No
	SYN-ACK Protection Algorithm	Drop
	Reverse Detection Rate	<input type="radio"/> Yes <input checked="" type="radio"/> No 32000 (pps)
	ACK Learning Mode	<input type="radio"/> Yes <input checked="" type="radio"/> No
ACK Control	ACK Protection Algorithm	ACK check
	Reverse Detection Rate	<input type="radio"/> Yes <input checked="" type="radio"/> No 32000 (pps)
	Retransmission Interval	8 (1000 ms) - 24 (3000 ms)
	RST Tx Rate	100000 (pps)
Other	TCP Fragment Control	Drop

Table 5-16 describes parameters of the TCP control policy.

Table 5-16 Parameters of the TCP control policy

Control Item	Parameter	Description
SYN Control	Targeting	Specifies how to identify a target server to be protected. <ul style="list-style-type: none"> Destination IP/Port: indicates that the server to be protected is identified by the destination IP address and port. Dst 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.
	Retransmission Interval	Specifies how many milliseconds will elapse between when a SYN packet is discarded and when it is resent.
	Source Bandwidth Limit	Works with Per Source IP Rate Limit to limit the bandwidth used by the source host to send SYN packets. It has the following values: <ul style="list-style-type: none"> Disable: disables this function. Drop+blocklist: 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.
	Per Source IP Rate Limit	Works with 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	SYN-ACK 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. <p>The learning mode works only when neither SYN protection nor ACK protection is available.</p>
	SYN-ACK Protection Algorithm	Specifies the SYN-ACK protection algorithm. Options include Drop , Close , Source authentication , Session check , and Combined protection . <ul style="list-style-type: none"> Drop: drops SYN-ACK packets.

Control Item	Parameter	Description
		<ul style="list-style-type: none"> • 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 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 Drop , Time sequence Check , or ACK check , with Drop as the default value. <ul style="list-style-type: none"> • Drop: drops ACK packets. • Time sequence check: For two identical ACK packets, if their sending interval is in the range of configured for Retransmission Interval, 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. <ul style="list-style-type: none"> • Accept: allows TCP fragments in IPv4 or IPv6 packets to pass through. • Drop: drops TCP fragments in IPv4 or IPv6 packets. • Limit rate: restricts the transmission rate of TCP fragments.

5.1.2.12 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 about regular expression rules, see section [5.2.9 Regular Expression Rules](#).

Figure 5-28 shows the TCP regular expression protection policy.


 <p>Note</p>	<ul style="list-style-type: none"> 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	Add Rule													
<input type="radio"/> Yes <input checked="" type="radio"/> No	Move <input type="text"/> Behind <input type="text"/> <input type="button" value="←"/> <input type="button" value="→"/> <input type="button" value="+"/> <input type="button" value="x"/>													
Rule List	<table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th>Operation</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table>		ID	Name	Operation									
ID	Name	Operation												

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 [5.2.9 Regular Expression Rules](#).
- Delete a rule:** Click  to delete the rule.

Figure 5-29 Adding regular expression rules

Configure Regular Expression Rule		
<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	regex1	
<input type="checkbox"/>	regex2	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

5.1.2.13 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

Botnet & IP Behavior Control Policy [default_protection_group]							
Rule Name	Enable	Access Control	Statistical Period	Traffic Unit	Rate Limit	Blocklist Threshold	Consecutive Abnormal Cycles
SYN Packets	<input type="radio"/> Yes <input checked="" type="radio"/> No	Limit rate	4 (s)	<input checked="" type="radio"/> Packets <input type="radio"/> Bytes	400 Packets	400 Packets	3
GET/POST Packets	<input type="radio"/> Yes <input checked="" type="radio"/> No	Limit rate	4 (s)	<input checked="" type="radio"/> Packets <input type="radio"/> Bytes	200 Packets	200 Packets	3
ACK Packets	<input type="radio"/> Yes <input checked="" type="radio"/> No	Limit rate	4 (s)	<input checked="" type="radio"/> Packets <input type="radio"/> Bytes	400 Packets	400 Packets	3
DNS Query Packets	<input type="radio"/> Yes <input checked="" type="radio"/> No	Limit rate	4 (s)	<input checked="" type="radio"/> Packets <input type="radio"/> Bytes	200 Packets	200 Packets	3
SIP Packets	<input type="radio"/> Yes <input checked="" type="radio"/> No	Limit rate	4 (s)	<input checked="" type="radio"/> Packets <input type="radio"/> Bytes	200 Packets	200 Packets	3
UDP Packets	<input type="radio"/> Yes <input checked="" type="radio"/> No	Limit rate	4 (s)	<input checked="" type="radio"/> Packets <input type="radio"/> Bytes	400 Packets	400 Packets	3
Other Packets	<input type="radio"/> Yes <input checked="" type="radio"/> No	Limit rate	4 (s)	<input checked="" type="radio"/> Packets <input type="radio"/> Bytes	400 Packets	400 Packets	3
Empty Connection Check		Disable					

Table 5-17 describes botnet and IP behavior control parameters.

Table 5-17 Botnet and IP behavior control parameters

Parameter	Description
Enable	Controls whether to enable packet rate control.
Access Control	<p>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:</p> <ul style="list-style-type: none"> Limit rate: limits the traffic rate. Limit rate+blocklist: 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 5.2.5 Blocklist. <p>For the empty connection check, Access Control has the following values:</p> <ul style="list-style-type: none"> Disable: disables the empty connection check function. Drop+blocklist: 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.

Parameter	Description
Statistical Period	Specifies the statistical period for calculating the percentage of packets that match the rule.
Traffic Unit	Specifies how to measure the packet forwarding rate. Options include Packets and Bytes .
Rate Limit	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.
Blocklist 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+blocklist 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 Blocklist Threshold . Value range: 1–10.  Note This parameter can be configured only when Limit rate+blocklist is selected for Access Control .

5.1.2.14 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

SIP Protection Policy[default_protection_group]		
SIP Protection	Port	Protection Algorithm
<input checked="" type="radio"/> Yes <input type="radio"/> No	5061	Protection mode ▼

[Table 5-18](#) describes parameters of the SIP protection policy.

Table 5-18 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

Parameter	Description
	port number of attack packets matches the specified port.
Protection Algorithm	Protection algorithm. <ul style="list-style-type: none"> • 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 <i>sending a register packet first</i>, the system drops the invite packet.

5.1.2.15 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

[Table 5-19](#) describes parameters of the UDP session authentication policy.

Table 5-19 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:

Parameter		Description
		<ul style="list-style-type: none"> 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.

5.1.2.16 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 the UDP payload check policy.

Figure 5-33 UDP payload check policy

UDP Payload Check Policy [default_protection_group]		
Payload Check	Mode Check	Packet Length Threshold
Drop UDP packets with no payload	Disable	80

[Table 5-20](#) describes parameters of the UDP payload check policy.

Table 5-20 Parameters of the UDP payload check policy

Parameter	Description
Payload Check	<p>Specifies whether to check the UDP payload and post-check actions. It has the following values:</p> <ul style="list-style-type: none"> Disable: disables UDP payload inspection. Drop UDP packets with no payload: drops packets whose payload length is 0. Drop UDP packets with no payload while under attack: 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.

5.1.2.17 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 about regular expression rules, see [section 5.2.9 Regular Expression Rules](#).

Figure 5-34 shows the area configuring the UDP regular expression protection policy.










 <p>Note</p>	<ul style="list-style-type: none"> 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							
<input type="radio"/> Yes <input checked="" type="radio"/> No	Move <input type="text"/> Behind <input type="text"/>    							
Rule List	<table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>		ID	Name	Operation			
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. Select one or more rules and then click **OK**.

For how to create a regular expression rule, see section 5.2.9 Regular Expression Rules.

- **Delete a rule:** Click  to delete the rule.

5.1.2.18 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 5-35 shows parameters of the UDP protection policy.

Figure 5-35 UDP protection policy

UDP Protection Policy [default_protection_group] ?			
UDP Fragment Control	Accept ▼		
Min UDP Packet Length	0	(Bytes)	
Max UDP Packet Length	65535	(Bytes)	
Traffic Control by Src IP+Src Port	<input type="radio"/> Yes <input checked="" type="radio"/> No	65535 (0-524280)	<input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Src IP	<input type="radio"/> Yes <input checked="" type="radio"/> No	3000000 (0-24000000)	<input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Dst IP+Dst Port	<input type="radio"/> Yes <input checked="" type="radio"/> No	65535 (0-524280)	<input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Dst IP+Src Port	<input type="radio"/> Yes <input checked="" type="radio"/> No	65535 (0-524280)	<input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Dst IP	<input type="radio"/> Yes <input checked="" type="radio"/> No	3000000 (0-24000000)	<input checked="" type="radio"/> pps <input type="radio"/> bps

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

Table 5-21 Parameters of the UDP protection policy

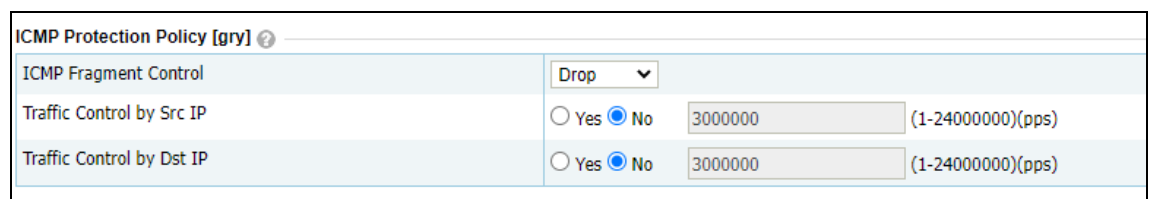
Parameter	Description
UDP Fragment Control	Controls whether to drop detected UDP fragments in IPv4 or IPv6 packets. <ul style="list-style-type: none"> Accept: allows UDP fragments to pass through. Drop: drops UDP fragments. Limit rate: limits the packet transmission rate to a specified threshold when 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. 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

Parameter	Description
	fragments will be dropped. This parameter is disabled by default. The value range is 0–24000000, with 3000000 as the default value.

5.1.2.19 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 5-36 shows parameters of the ICMP protection policy.

Figure 5-36 ICMP Protection Policy area



ICMP Protection Policy [gry] ?	
ICMP Fragment Control	Drop ▼
Traffic Control by Src IP	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="text" value="3000000"/> (1-24000000)(pps)
Traffic Control by Dst IP	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="text" value="3000000"/> (1-24000000)(pps)

Table 5-22 describes parameters of the ICMP protection policy.

Table 5-22 Parameters of the ICMP protection policy

Parameter	Description
ICMP Fragment Control	Controls whether to drop the detected ICMP fragments. <ul style="list-style-type: none"> Accept: allows ICMP fragments to pass through. Drop: drops ICMP fragments. Limit rate: limits the packet transmission rate to a specified 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.

5.1.2.20 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 5-37 shows the watermark protection policy.

Figure 5-37 Watermark protection policy



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

- **Enable:** Select **Yes** or **No** to enable or disable the policy.
- **Add 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 the rule.

Table 5-23 describes parameters for configuring a watermark protection policy.

Table 5-23 Parameters of a watermark protection policy

Parameter	Description
Mode	<p>Mode of the watermark protection policy.</p> <ul style="list-style-type: none"> • 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 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	<p>Specifies the protocol for matching packets. Options include UDP and TCP. Only UDP is supported for the common mode.</p>
Port Range	<p>Specifies the port for matching packets. Value range: 0–65535.</p> <p>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.</p>
Offset	<p>Specifies the offset of packet transmission. Value range: 0–1480.</p>
Hash Key	<p>Specifies the hash key. Value range: 0–4294967295.</p> <p> Note</p> <p>This parameter is only available for the advanced mode.</p>
Character Type	<p>Specifies the character type for matching packets, which can be Ordinary characters or Hexadecimal characters.</p>

Parameter	Description
	 <p>This parameter is only available for the common mode.</p>
Signature	<p>Specifies the specific character for matching packets. You can type up to 16 hexadecimal characters or ordinary characters.</p> <p>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.</p>  <p>This parameter is only available for the common mode.</p>

5.1.2.21 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 about how to configure programmable rules, see section [5.2.13 Programmable Rules](#).

A protection group can only reference one programmable rule.

You can perform the following operations on the programmable rule:



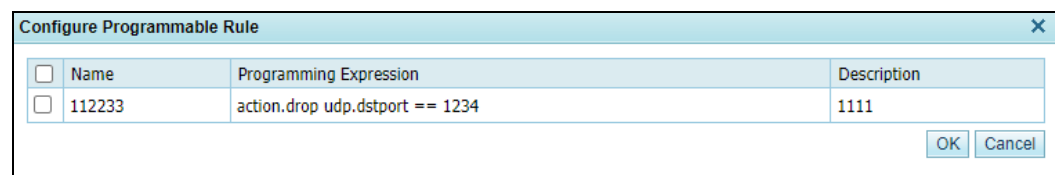
- **Enable:** Select **Yes** or **No** to enable or disable the programmable rule.
- Add a rule: Click  to open the rule configuration page shown in [Figure 5-38](#). Select one programmable rule and then click **OK**.
- Delete a rule: You can click  to delete the rule.

Figure 5-38 Adding a programmable rule



The dialog box titled "Configure Programmable Rule" contains a table with the following data:

<input type="checkbox"/>	Name	Programming Expression	Description
<input type="checkbox"/>	112233	action.drop udp.dstport == 1234	1111

At the bottom right of the dialog box are buttons for **OK** and **Cancel**.

5.1.2.22 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 5-39](#) 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+blocklist**.

Figure 5-39 Protocol ID check policy

Table 5-24 describes parameters of a protocol ID check policy.

Table 5-24 Parameters of a protocol ID check policy

Parameter		Description
Enable		Controls whether to enable this policy. <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Accept: allows packets of this protocol ID to pass through. Drop: drops packets of this protocol ID. Drop+blocklist: 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 Template** to open the built-in protection group policy template list of the system.

Figure 5-40 Protection group policy templates

Group Policy Template				
<input type="checkbox"/>	Name	Description	Time of Creation	Operation
<input type="checkbox"/>	_default	Builtin template for General Server.	2021-03-12 15:25:23	
<input type="checkbox"/>	_dns_auth_server	Builtin template for DNS Auth Server.	2021-03-12 15:25:23	
<input type="checkbox"/>	_dns_cache_server	Builtin template for DNS Cache Server.	2021-03-12 15:25:23	
<input type="checkbox"/>	_web_server	Builtin template for Web Server.	2021-03-12 15:25:23	
<input type="checkbox"/>	test	fh	2024-06-28 10:48:10	
<div>Add Delete</div>				

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 5-41.

Figure 5-41 Basic information of a protection group policy template

Group Policy Template

Template Name

Name:

Description

Template _default

Next Cancel

Table 5-25 describes parameters for creating a protection group policy template.

Table 5-25 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 5-42 Configuring protection policies for a protection group policy template

Group Policy Template				
Description: 111				
DDOS [111]				
Anti-DDoS	Threshold 1	Threshold 2	Enable	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 (kpbs)	No	
Total Inbound Traffic Control		1000 (kpbs)	No	
Total Outbound Traffic Control		1000 (kpbs)	No	
Anomalous Packet Filtering Rules [111]				
Invalid SYN Packet Filtering			Enable	
UDP Port 80 Filtering			Enable	
LAND Filtering			Enable	
HTTP Filtering			Disable	
Reflection Protection Policy [111]				
Enable: <input type="radio"/> Yes <input checked="" type="radio"/> No				
Add Rule: Move Behind				
Rule List: ID Name Operation				
HTTP Keyword Checking Policy [111]				
Enable: <input type="radio"/> Yes <input checked="" type="radio"/> No				
Add Rule: Move Behind				
Rule List: ID Name Operation				

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

- Click **Add** to configure a group-specific access control rule. For details, see [5.2.2 Access Control Rules](#).
- Specify whether to enable the allowlist and proxy monitoring. For details about the allowlist function, see section [5.2.1 Allowlist](#).
- Specify whether to enable the DNS subdomain allowlist and configure parameters. For details about the DNS subdomain allowlist function, see section [5.2.12 DNS Subdomain Allowlist](#).
- Specify whether to enable the blocklist, block period, and whether to enable proxy monitoring. For details about the blocklist function, see section [5.2.5 Blocklist](#).
- 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 [5.2.4 GeoIP Rules](#).
- 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 TI, see section [8.4 Collaboration with TI](#).



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

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

Step 6 After the configuration, click **Apply** in 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 5-40](#), click the name of a template to view its details.

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

5.1.3.3 Editing a Protection Group Policy Template


You can edit the description, protection policies, allowlist, DNS subdomain allowlist, access control rules, blocklist, GeoIP rules, and TI configuration of a protection group policy template.

On the protection group policy template list shown in [Figure 5-40](#), click  in the **Operation** column to reset protection policies and the access policies 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 5-40](#), 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 5-40](#), select several templates (or select check boxes), click **Delete** to the lower right of the list, and then click **OK** in the confirmation dialog box to delete them.

5.1.4 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. ADS provides carpet bombing protection based on the DDoS policy and behavior.

The system provides a default carpet bombing protection rule, which can be viewed, enabled, disabled, and edited, but cannot be deleted. You can also create a carpet bombing protection rule to meet your particular needs.




The IP address range of the default carpet bombing protection rule is **0.0.0.0/0** and **::/0**, indicating all IPv4 and IPv6 addresses, which cannot be edited.

Choose **Policy > Anti-DDoS > Carpet Bombing Protection**. Click **Add** and configure parameters on the page that appears. [Table 5-26](#) describes parameters for configuring a carpet bombing protection rule.

A carpet bombing protection rule, after being created, can be viewed, queried, enabled, disabled, edited, and deleted.

Table 5-26 Parameters of carpet bombing protection

Parameter	Description	
Name	Name of the carpet bombing protection rule, which must be unique.	
Enable	Controls whether to enable the carpet bombing protection function. <ul style="list-style-type: none"> Yes: enables the carpet bombing protection function. No: disables the carpet bombing protection function. 	
IP Range	Destination IP segments. Each IP segment, like 192.168.1.0/24, should be in a separate line. <ul style="list-style-type: none"> For IPv4 addresses, the subnet mask should be 8 to 24 bits. For IPv6 addresses, the prefix length should be 8 to 120 bits. 	
IP Aggregation	Specifies how to aggregate IP addresses using the IPv4 netmask or IPv6 prefix length. The IPv4 Netmask is fixed to 24 and the IPv6 Prefix Length is fixed to 120 . The value here cannot be edited.	
DDoS Policy-based Carpet Bombing Protection	The protection thresholds here work for network segments defined with a subnet mask or prefix length. If the total number of packets of a certain type to a network segment exceeds the related threshold, the network segment will be protected with the related policy, which is the one configured for the protection group to which the destination IP address belongs. For details about the protection policy, see section 5.1.2 Policy Configuration for Protection Groups .	
	Anti-D DoS	Displays different types of packets and the traffic control by destination segment.
	Threshold 1	Threshold for the rate of traffic to a network segment. When the rate (pps) of such traffic exceeds the specified value, the network segment will be protected with the related policy. <ul style="list-style-type: none"> SYN Flood: The value range is 0–48000000. ACK Flood: The value range is 0–240000000. UDP Flood: The value range is 0–48000000. ICMP Flood: The value range is 0–48000000. HTTP Get Flood: The value range is 0–48000000. HTTP Post Flood: The value range is 0–48000000. HTTPS Flood: The value range is 0–48000000. Traffic Control by Dst Segment: The value range is 0–8000000, in kbps.
	Enable	Controls whether to enable the protection of the current type.
Behavior-based Carpet Bombing Protection	Destination IPs here refers to the number of IP addresses to be protected, which is a subset of the IP addresses configured in IP Range . 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 blacklist or limit its rate, or do both.	
	Enable	Controls whether to enable the behavior-based carpet bombing protection.
	Action	Specifies the action taken against a source IP address that triggers the carpet bombing protection rule. Options include Add to blacklist , Limit rate , and Limit rate+blacklist .
	Statistic	Specifies a period of time when the number of visits to destination IP

	al Period	addresses is counted. Value range: 1–600, in seconds.
	Paramet ers of Limit rate policy	<p>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.</p> <ul style="list-style-type: none"> • 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.
	Paramet ers of Add to blocklis t policy	<p>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.</p> <ul style="list-style-type: none"> • 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. <p> Note</p> <ul style="list-style-type: none"> • 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 5.2.5 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.
Description	Brief information about the carpet bombing protection rule, which is less than 256 characters.	
Time	Time when the carpet bombing protection rule was created. The time was automatically generated by the system on the creation of the new rule. It cannot be edited.	

5.1.5 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 5-43](#).

Figure 5-43 Advanced Global Parameters page

Advanced Global Parameters	
Trust Time Control	
Item	Value
Advanced Trust Time (min)	15
Normal Trust Time (min)	30

[Edit](#)

[Table 5-27](#) describes advanced global parameters.

Table 5-27 Advanced global parameters

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

5.1.6 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.

5.1.6.1 Creating a Response Page

To create a response page, perform the following steps:

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

Figure 5-44 Response Page Settings tab page

Response Page Settings					
<input type="checkbox"/> Select All	Template Name	Logo	Prompt Message	Custom Mode	Operation
<input type="checkbox"/>	test1		test1	Close	  
<input type="checkbox"/>	test		test	Close	  
<div> Delete Add </div>					

Step 2 Click Add.

The **Add Response Page Template** page appears, as shown in Figure 5-45.


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 5-45 Add Response Page Template page

Add Response Page Template

Item	Value
Template Name	<input type="text"/>
Logo	<input type="button" value="Choose File"/> No file chosen <small>(*The image size cannot exceed 50 KB. The image format can be JPG, GIF, or JPEG and the recommended pixel size is 150x38.)</small>
Prompt Message	<input type="text"/> <small>(The HTML template content can be modified.) @</small> <small>(To ensure that the CAPTCHA function works, do not change the "keep" label or use "class=verify".)</small> <small>(The template can contain up to 1390 bytes, including 425 reserved for the system. The current length is:) 748 bytes.</small>
	<div> <div>Custom HTML Code</div> <pre> 1 <!DOCTYPE html> 2 <html> 3 <head> 4 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> 5 </head> 6 <body> 7 <p style="font: 12px Arial;">In order to prevent malicious attacks, we need to verify your identity...</p> 8 <small style="font: 12px Arial;">Please enter the characters in the image below</small> 9 <!--Keep--> 10 11 <style> 12 .verify { 13 border: 1px solid #ddd; 14 width: 240px; </pre> </div> <div> <input checked="" type="checkbox"/> Custom Mode </div>
	<div> <div>Preview</div> <div> In order to prevent malicious attacks, we need to verify your identity... Please enter the characters in the image below  <input type="text"/> <input type="button" value="Submit"/> </div> </div>

OK
Cancel

Table 5-28 describes parameters for creating a response page.

Table 5-28 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, gif, or jpeg format and must be within 50 KB. A pixel size of 150*38 is recommended.
Prompt Message	Specifies the prompt message displayed under the logo.

Parameter	Description
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.
--	---


5.1.6.2 Editing a Response Page

On the page shown in [Figure 5-44](#), click  in the row of a response page.

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

5.1.6.3 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 5-44](#), 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 5-44](#), select one or more response pages (or select the check box in the table header 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.

5.1.6.4 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 5-44](#), click  in the row of a response page.

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

Figure 5-46 Response page preview

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

----End

5.1.7 SSL Certificate Management

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

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

5.1.7.1 Adding an SSL Certificate

To add an SSL certificate, perform the following steps:

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

Figure 5-47 SSL certificate management

SSL Certificate Mgmt			
SSL Certificate			
<input type="checkbox"/>	Certificate Name	Description	Operation
<input type="checkbox"/>	nsfocus	Default certificate	--
			<input type="button" value="Delete"/> <input type="button" value="Add"/>

Step 2 Click **Add**.

Figure 5-48 Adding an SSL certificate

Item	Value
Name	<input type="text"/>
SSL Certificate	<input type="button" value="Choose File"/> No file chosen (A file with the .crt extension in the PEM format)
SSL Private Key	<input type="button" value="Choose File"/> No file chosen (A file with the .key extension in the PEM format)
Private Key Password	<input type="text"/> (Leave it empty if no password is available.)
Description	<div><div></div></div> Length is less than 256 characters.

OK Cancel


Table 5-29 describes parameters of an SSL certificate.

Table 5-29 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.
Private Key Password	If a password is set for the private key of the SSL certificate to be imported, type the correct password; otherwise, leave it empty.
Description	Description of the SSL certificate.

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

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

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

----End

5.1.7.2 Editing an SSL Certificate

On the SSL certificate list shown in Figure 5-47, click  in the **Operation** column of a certificate.

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

5.1.7.3 Deleting an SSL Certificate

On the SSL certificate list shown in Figure 5-47, click  in the **Operation** column of a certificate and click **OK** in the displayed confirmation dialog box to delete this certificate.

5.1.8 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 User-Agent Rules**.

Figure 5-49 Mobile user-agent rules

Mobile User-Agent Rules						
<input type="checkbox"/>	Name	User-Agent String	Relationship	Description	Time of Creation	Operation
<input type="checkbox"/>	default_webapi	okhttp CFNetwork Dalvik	OR		2019-09-12 16:18:45	 
<input type="checkbox"/>	default_webview	Linux; Android iPhone iPad	OR		2019-09-10 16:44:13	 
Add Delete						

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

Figure 5-50 Adding a mobile user-agent rule

Add Mobile User-Agent Rule	
Item	Value
Name	<input type="text"/>
User-Agent	1 <input type="text"/> (*At least one expression should be typed.)
	2 <input type="text"/>
	3 <input type="text"/>
	4 <input type="text"/>
	5 <input type="text"/>
Relationship	OR <input type="button" value="v"/>
Description	<input type="text"/>
Time of Creation	2024-10-25 17:07:49
OK Cancel	

Table 5-30 describes parameters for adding a mobile user-agent rule.

Table 5-30 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

Parameter	Description
	can be typed here. Each string can contain a maximum of 100 characters.
Relationship	<p>Specifies the relationship of user-agent strings.</p> <ul style="list-style-type: none"> • 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, allowlist, and other functions to make certain specific applications more easily controlled. The access control policies are described in the sequence of protection provided in the engine.

This section covers the following topics:

- [Allowlist](#)
- [Access Control Rules](#)
- [Reflection Protection Rules](#)
- [GeoIP Rules](#)
- [Blocklist](#)
- [HTTP Keyword Checking](#)
- [SSL/TLS Keyword Checking Policy](#)
- [Connection Exhaustion Protection Rules](#)
- [Regular Expression Rules](#)
- [URL-ACL Protection Rules](#)
- [DNS Keyword Checking](#)
- [DNS Subdomain Allowlist](#)
- [Programmable Rules](#)

5.2.1 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 a match is found, the ADS engine allows these packets to pass through, without executing access control rules or protection algorithms, thereby improving the system performance.



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.

Addresses can be added to the allowlist by either of the following:

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

IP addresses can be automatically added to the allowlist for reasons listed in [Table 5-31](#).

Table 5-31 Reasons for adding a source IP address to the allowlist

Policy/Rule	Reason for Adding a Source IP Address to the Allowlist
HTTP keyword checking rule	When the action of an HTTP keyword checking rule is set to Accept+allowlist , the system adds source IP addresses of matching packets to the allowlist.
DNS keyword checking rule	When the action of a DNS keyword checking rule is set to Accept+allowlist , the system adds source IP addresses of matching packets to the allowlist.
Programmable rule	When the action of a programmable rule is set to accept_white , the system adds source IP addresses of matching packets to the allowlist.
SSL/TLS keyword checking rule	When the action of an SSL/TLS keyword checking rule is set to Accept+allowlist , the system adds source IP addresses of matching packets to the allowlist.

You can perform the following operations regarding the allowlist:

- [Enabling and Disabling the Allowlist Function](#)
- [Enabling Proxy Monitoring](#)
- [Adding an Entry to the Allowlist](#)
- [Importing an Allowlist File](#)
- [Viewing Allowlist Entries](#)
- [Querying the Allowlist](#)
- [Clearing Allowlist Entries](#)
- [Exporting Allowlist Entries](#)

5.2.1.1 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 **Policy > Access Control > Allowlist**.

By default, the allowlist function is disabled.

Figure 5-51 Allowlist configuration page

Allowlist	
Allowlist	
Item	Value
Enable	No
Edit	

Step 2 Click **Edit** and then select **Yes** to enable the allowlist function.

Figure 5-52 Allowlist enabled

Allowlist	
Allowlist	
Item	Value
Enable	Yes
Configuration Items	
Item	Value
Proxy Monitoring	No
Edit Allowed IP List Add Search Import Export Clear	

----End

Disabling the Allowlist Function

If the allowlist function is enabled, you can click **Edit** and then select **No** to disable it.

5.2.1.2 Enabling Proxy Monitoring

On the page shown in [Figure 5-52](#), you can enable or disable the proxy monitoring function of the allowlist. By default, this function is disabled.

- **No:** 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.
- **Yes:** 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.

5.2.1.3 Adding an Entry to the Allowlist

You can manually add a trusted IP address or IP segment to the allowlist.

Choose **Policy > Access Control > Allowlist**. On the page shown in [Figure 5-52](#), click **Add** to type an IPv4 or IPv6 address. For IPv4 addresses, the netmask length should be 12 to 32. For IPv6 addresses, the prefix length should be 64 to 128.


5.2.1.4 Importing an Allowlist File

You can add trusted IPv4 or IPv6 addresses by importing an 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 allowlist file is in format of **.txt** or **.csv**, with one IP address per line. The following uses IPv4 addresses as an example to illustrate the format:

10.10.10.10

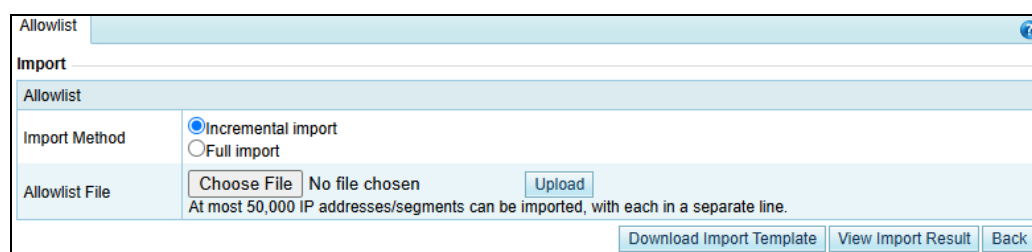
172.16.10.10

 <p>Note</p>	<ul style="list-style-type: none"> • 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. • Enable the allowlist before you import an allowlist file; otherwise, the imported allowlist cannot take effect.
---	---

To import an allowlist file, perform the following steps:

Step 1 On the page shown in [Figure 5-52](#), click **Import**.

Figure 5-53 Importing an allowlist file



Step 2 (Optional) On the page that appears, click **Download Import Template** and save it to a local disk. Type trusted IP addresses or IP segments in the template.

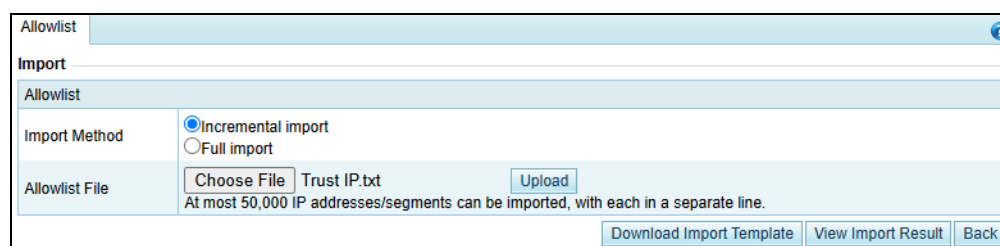
Step 3 Configure the import method.

- **Incremental import:** appends new IP addresses in the file to the allowlist.
- **Full import:** overwrites the allowlist with IP addresses included in the file.

Step 4 Click **Choose File**, select the allowlist file and click **Open**.

The file name is then displayed on the page.

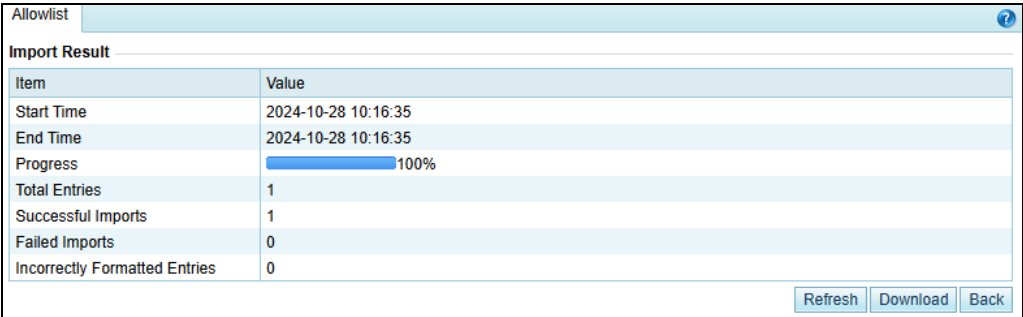
Figure 5-54 Importing the allowlist file



Step 2 Click **Upload**.

After the allowlist file is imported, the system shows the import result.


Figure 5-55 Import result



Step 5 View the number of entries successfully and unsuccessfully imported on the **Import Result** page.

You can also perform the following operations:

- Click **Refresh** to update imports in real time.
- Click **Download** to save the import result file to a local disk.
- Click **Back** to return to the Import Allowlist page.



Note

In addition, you can click **View Import Result** on the **Import** page to view import results.

----End

5.2.1.5 Viewing Allowlist Entries

After the list of trusted IP addresses is loaded to the engine, you can view the allowlist entries on the web-based manager.

Choose **Policy > Access Control > Allowlist**. On the page shown in [Figure 5-52](#), click **Allowed IP List** to view information that is successfully imported to the allowlist. The system displays a maximum of 1000 IP addresses added or imported.

5.2.1.6 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 checking it against access control rules or protection algorithms.

To query the allowlist, perform the following steps:

Step 3 On the page shown in [Figure 5-56](#), click **Search**.

Figure 5-56 Querying the allowlist

Step 4 Type the IP address to be queried in the textbox and click **OK** to check whether the IP address is trusted.

Figure 5-57 Allowlist query result

Step 5 After viewing the result, click **Back** to return to the allowlist configuration page.

----End

5.2.1.7 Clearing Allowlist Entries

By clearing the allowlist, you can delete the trust status of all IP addresses listed in the allowlist on the engine (memory). If an IP address in this allowlist needs to be re-trusted after the allowlist is cleared, you need to manually add it to the allowlist or import an allowlist file.

On the allowlist configuration page shown in [Figure 5-52](#), click **Clear**. On the **Clear** page that appears, select an allowlist type to be cleared, and click **OK**.

- **Manual:** allowlist that is manually added or imported.
- **Auto:** allowlist that is generated by algorithms. [Table 5-31](#) describes algorithms that automatically add IP addresses to the allowlist.

5.2.1.8 Exporting Allowlist Entries

To export an allowlist file, follow these steps:

Step 1 On the page shown in [Figure 5-52](#), click **Export**.


Step 2 Configure allowlist export parameters.


Table 5-32 Parameters for exporting allowlist entries

Parameter	Description
Export Type	Specifies the type of the allowlist for export, which can be Manual or Auto .
Export Method	Specifies the export method, which can be either of: <ul style="list-style-type: none"> • Quick: Only allowed IP addresses are included in the exported file. • Detailed: Allowlist entry details, like the allowed IP addresses and the reason for their addition, are included in the exported file.

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

Figure 5-58 Viewing allowlist export results

Allowlist	
Export	
Item	Value
Start Time	2024-10-28 10:20:45
End Time	2024-10-28 10:20:45
Export Status	Export file generation completed successfully.
Export Progress	<div><div></div></div> 100 %
Operation	
<div>Refresh Back</div>	

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

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

----End

5.2.2 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](#)

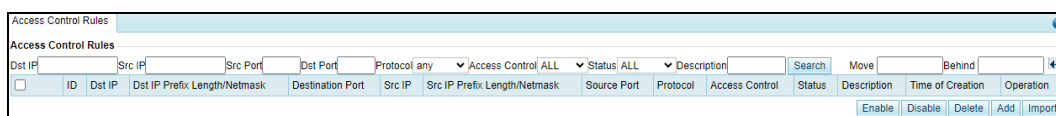
5.2.2.1 Creating an Access Control Rule

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

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

Initially, the rule list is empty.

Figure 5-59 List of access control rules



Step 2 Click **Add**.

Figure 5-60 Creating an access control rule

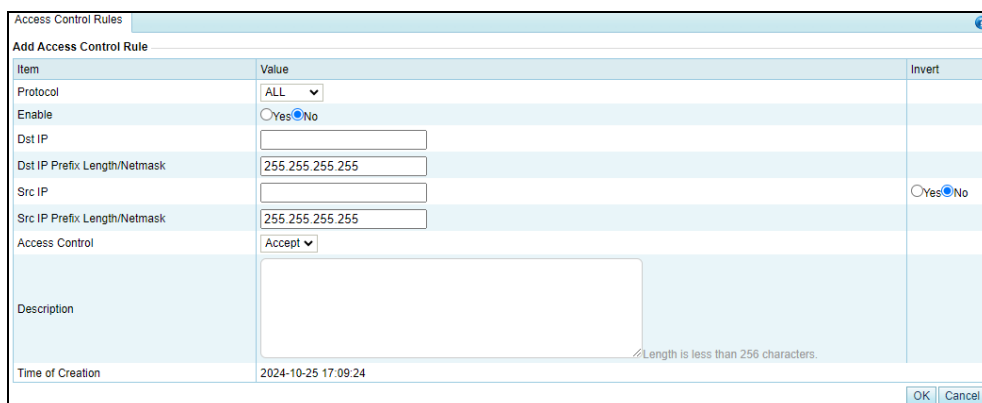


Table 5-33 describes parameters for creating an access control rule.

Table 5-33 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. <ul style="list-style-type: none"> Yes: enables the rule. No: disables the rule.
Dst 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 Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the destination IP address.
Dst 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.
Src 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.
Src 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

Parameter	Description
	control policy for all connections of the source IP address.
Access Control	<p>Action performed by the ADS device on packets with specified signatures. It has the following options:</p> <ul style="list-style-type: none"> • 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, with no 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

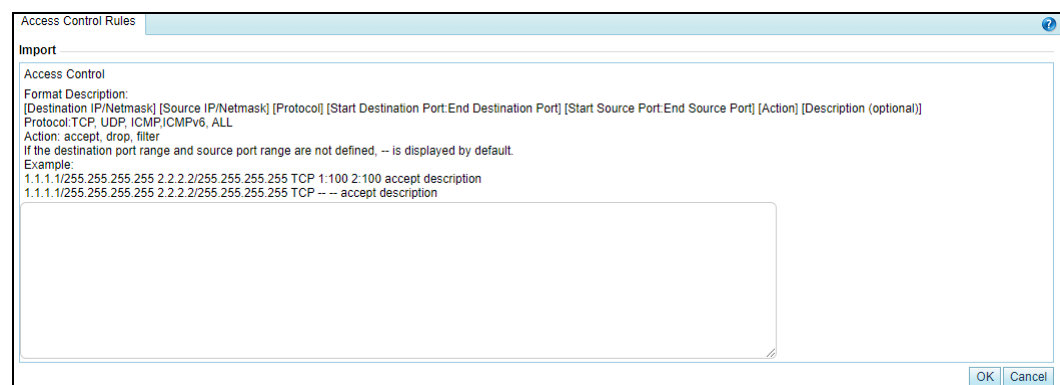
5.2.2.2 Creating Access Control Rules in Batches

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

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

Step 2 Click **Import**.

Figure 5-61 Creating access control rules in batches



Step 3 Type multiple access control rules as prompted.

Pay attention to the following format specifications:

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

- Protocol: **TCP, UDP, ICMP, ICMPv6**, and **ALL**.
- Action: **Allow, Drop**, and **Filter**.
- If the value range of **Destination Port** and **Source Port** is not defined, -- is used to replace their values by default.



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

5.2.2.3 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 **Policy > Access Control > Access Control Rules**.

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

Step 3 Click **OK** in the confirmation box 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 **Policy > Access Control > Access Control Rules**.

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

Step 3 Click **OK** in the confirmation box to disable the selected rules.





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


----End

5.2.2.4 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.

5.2.2.5 Editing an Access Control Rule

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

Step 1 Choose **Policy > 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

5.2.2.6 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 **Policy > 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 **Policy > Access Control > Access Control Rules**. Select one or more access control rules (or select the check box in the table header 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.



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

5.2.2.7 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.

5.2.3 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](#)

























5.2.3.1 Creating a Reflection Protection Rule

Step 1 Choose **Policy > Access Control > Reflection Protection Rules**.

The reflection protection rule list is displayed, as shown in [Figure 5-62](#).

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

Figure 5-62 Reflection protection rules

Reflection Protection Rules							
<input type="checkbox"/>	Name	Protocol	Src Port	Action	Description	Time of Creation	Operation
<input type="checkbox"/>	Memcache	UDP	11211	Drop			 
<input type="checkbox"/>	COAP	UDP	5683	Drop			 
<input type="checkbox"/>	MsSql	UDP	1434	Drop			 
<input type="checkbox"/>	Jenkins	UDP	33848	Drop			 
<input type="checkbox"/>	SSDP	UDP	1900	Drop			 
<input type="checkbox"/>	SNMP	UDP	161	Drop			 
<input type="checkbox"/>	WSDD	UDP	3702	Drop			 
<input type="checkbox"/>	CLDAP	UDP	389	Drop			 
<input type="checkbox"/>	ARMS	UDP	3283	Drop			 
<input type="checkbox"/>	NTP	UDP	123	Drop			 
<input type="checkbox"/>	DNS	UDP	53	Drop			 
<input type="checkbox"/>	CharGen	UDP	19	Drop			 
							<input type="button" value="Add"/> <input type="button" value="Delete"/>

Step 2 Click **Add**.

A dialog box for creating a reflection protection rule appears, as shown in [Figure 5-63](#).

Figure 5-63 Creating a reflection protection rule

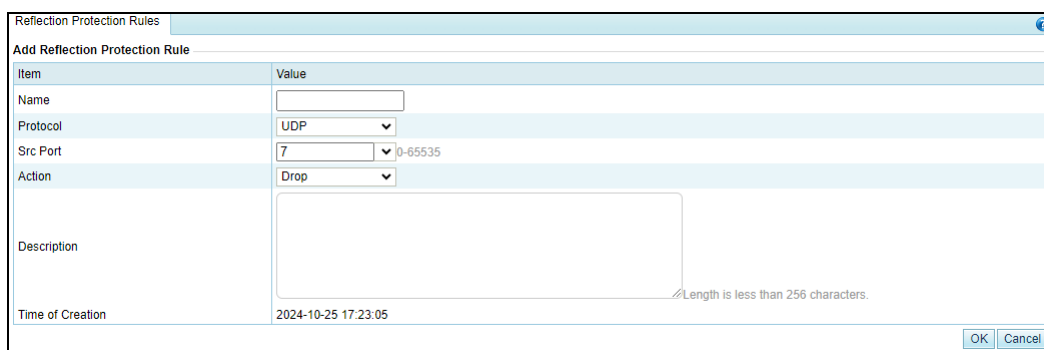


Table 5-34 describes parameters for creating a reflection protection rule.

Table 5-34 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 and TCP.
Src 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: <ul style="list-style-type: none"> Drop: drops such packets. Drop+blocklist: drops such packets and adds their source IP addresses to the blocklist. Before selecting this option, you must enable the blocklist. For details about the blocklist, see section 5.2.5 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 1000pps as the default value.
Description	Presents description of the new rule, which can contain a maximum of 256 characters.
Time of Creation	Indicates the time automatically generated by the system on the creation of the new rule. It cannot be edited.

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

----End

5.2.3.2 Editing a Reflection Protection Rule

All reflection protection rules can be edited.


Step 1 On the page shown in [Figure 5-62](#), 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

5.2.3.3 Deleting Reflection Protection Rules

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

Method 1: On the page shown in [Figure 5-62](#), 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 5-62](#), 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.

5.2.4 GeoIP Rules

The GeoIP database provides mappings between IP addresses and countries. After importing a GeoIP database 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 Database](#)

5.2.4.1 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 [5.2.2 Access Control Rules](#).

To create a GeoIP rule, perform the following steps:

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

The **GeoIP Rules** page appears, as shown in [Figure 5-64](#).

Parameter	Description
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

5.2.4.2 Configuring a GeoIP Database

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

Importing a GeoIP Database

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

To import a GeoIP database, perform the following steps:

Step 1 Choose **Policy > Access Control > GeoIP Rules > GeoIP Database**.

Figure 5-66 Viewing the GeoIP database

Step 2 Import a GeoIP database.

- Select an IP protocol, click **Choose File**, and then select a file to be imported.
- Click **Import** to import the GeoIP database.

After the successful import, the version and update information are displayed in the **GeoIP Database Update** area. The new database, 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 Database

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

On the page shown in [Figure 5-66](#), 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.

5.2.5 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 5-36](#).

Table 5-36 Reason for adding a source IP address to the blocklist

Policy/Rule	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	<p>When URL Protection Mode is set to Drop+blocklist 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.</p> <p>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.</p> <p>When URL Protection Mode is set to Monitor+blocklist 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.</p>
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 rule	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+blocklist , the system adds 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+blocklist , the system adds 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/Rule	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+blocklist , the system adds 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+blocklist , 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+blocklist , 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 Blocklist 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 checking rule with Action set to Drop+Blocklist or Drop+Blocklist+Disconnect 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+Blocklist 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 blocklist, the system adds source IP address that triggers the carpet bombing protection rule to the blocklist.
SSL/TLS keyword checking rule	When the action of an SSL/TLS keyword checking rule is set to Drop+blocklist or Drop+blocklist+disconnect , the system adds source IP addresses of matching packets 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.

	<ul style="list-style-type: none"> 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
- Querying the Blocklist
- Importing a Blocklist File
- Viewing the Import Result
- Exporting a Blocklist File

5.2.5.1 Enabling and Disabling the Blocklist Function

Enabling the Blocklist Function

To enable the blocklist function, perform the following steps:

Step 1 Choose **Policy > Access Control > Blocklist**.

Initially, the blocklist function is disabled.

Figure 5-67 Blocklist status

Item	Value
Enable	No

Step 2 Click **Edit** and then select **Yes** to enable the blocklist function. See Figure 5-68.

Figure 5-68 Enabling the blocklist policy

Item	Value
Enable	Yes

Configuration Items	
Item	Value
Auto Block	Temporary 120 (minutes)
Proxy Monitoring	Yes

Table 5-37 Blocklist parameters

Parameter	Description
Auto Block	<p>Specifies the duration when an IP address is blocked. This parameter has two options:</p> <ul style="list-style-type: none"> • 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

Parameter	Description
	this address are always dropped.
Proxy Monitoring	<p>Controls whether to enable or disable the proxy monitoring function. By default, this function is disabled.</p> <ul style="list-style-type: none"> 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 5-69](#), the blocklist function is enabled and blocklist configuration items are available.

Figure 5-69 Blocklist function enabled

Blocklist	
Blocklist	
Item	Value
Enable	Yes
Configuration Items	
Item	Value
Auto Block	Temporary 120 (minutes)
Proxy Monitoring	Yes

Buttons: Edit, Search, Blocked IP List, Add, Import, Export, Clear

----End

Disabling the Blocklist Function

To disable the blocklist function, perform the following steps:

On the page shown in [Figure 5-68](#), select **No**. Then the value of **Enable** turns to **No**, as shown in [Figure 5-67](#).

5.2.5.2 Adding a Blocklist Entry

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

Step 1 On the page shown in [Figure 5-69](#), click **Add** to add a blocklist entry.

Figure 5-70 Adding a blocklist entry

Step 2 Set parameters.

Table 5-38 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.

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

----End

5.2.5.3 Viewing Blocklist Entries

On the page shown in [Figure 5-69](#), click **Blocked IP List**. The system displays a maximum of 1000 IP addresses blocked recently, as shown in [Figure 5-71](#). You can click **Refresh** to obtain IP addresses blocked most recently.

Figure 5-71 Viewing blocklist entries

For the **Dst 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.

5.2.5.4 Deleting Blocklist Entries

To delete a blocklist entry, perform the following steps:

Step 1 On the page shown in [Figure 5-71](#), select one or more blocklist entries and then click **Delete**.

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

----End

5.2.5.5 Clearing Blocklist Entries

To clear blocklist entries, perform the following steps:

Step 1 On the page shown in [Figure 5-69](#) or [Figure 5-71](#), click **Clear**.

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

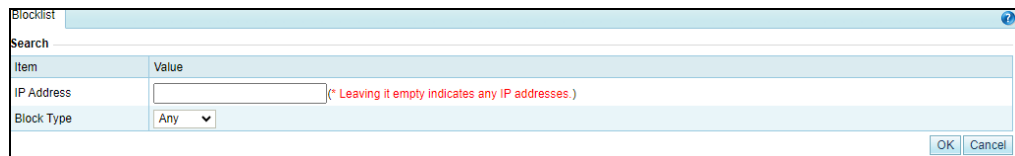
----End

5.2.5.6 Querying the Blocklist

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

Step 1 On the page shown in [Figure 5-72](#), click **Search**.

Figure 5-72 Searching for an IP address



Step 2 On the **Search** page shown in [Figure 5-72](#), type an IP address, and click **OK**.

The blocklist search result is displayed.

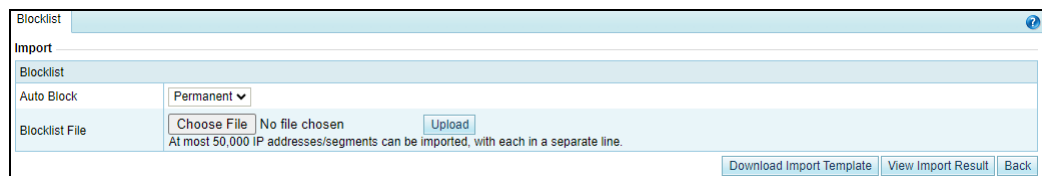
----End

5.2.5.7 Importing a Blocklist File

To import a blocklist file, perform the following steps:

Step 1 On the page shown in [Figure 5-69](#), click **Import**.

Figure 5-73 Importing a blocklist file





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

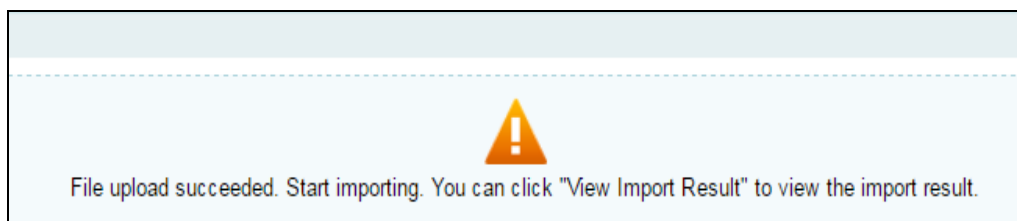
Step 2 On the page shown in [Figure 5-73](#), click **Choose File**.

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

Step 4 Click **Upload**.

After the upload is complete, the system prompts that the file is successfully imported, as shown in [Figure 5-74](#).

Figure 5-74 Import success prompt



After the blacklist file is imported, the system automatically switches to the page shown in [Figure 5-73](#).

----End

5.2.5.8 Viewing the Import Result

To view the import result, perform the following steps:

Step 1 On the page shown in [Figure 5-73](#), 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 5-75](#).

Figure 5-75 Viewing import results

Import Result	
Item	Value
Start Time	2021-09-15 11:04:23
End Time	2021-09-15 11:04:23
Progress	<div><div></div></div> 100%
Total Entries	1000
Successful Imports	1000
Failed Imports	0
Incorrectly Formatted Entries	0
<div>Refresh Download Back</div>	

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

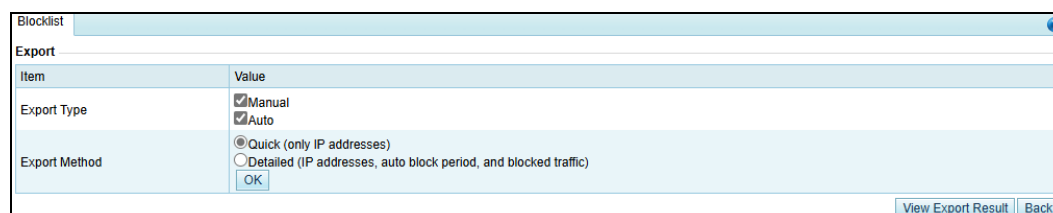
----End

5.2.5.9 Exporting a Blocklist File

To export a blocklist file, perform the following steps:

Step 1 On the page shown in [Figure 5-69](#), click **Export Blocklist**.

Figure 5-76 Exporting a blocklist file




Step 2 Set blocklist export parameters.

Table 5-39 Parameters for blocklist export

Parameter	Description
Export Type	Specifies the type of the blocklist for export, which can be Manual or Automatic.
Export Method	Specifies the export type, which can be either of the following: <ul style="list-style-type: none">• Quick: Only blocked IP addresses are included in the exported file.• Detailed: 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.

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

5.2.6 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.

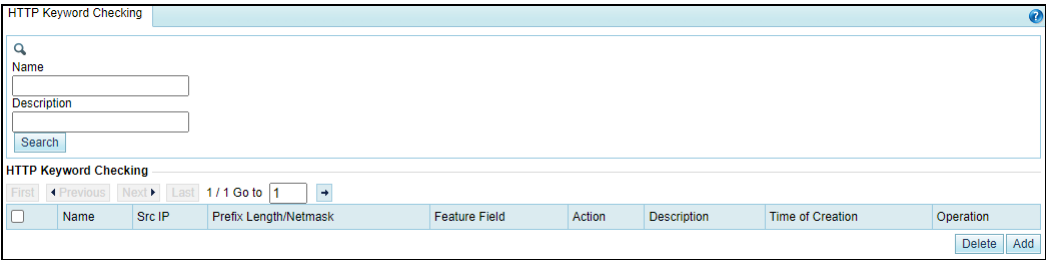
An HTTP keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting HTTP keyword checking rules are the same as those for access control rules.

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

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

Initially, the rule list is empty.

Figure 5-77 List of HTTP keyword checking rules



Step 2 Click **Add**.

Figure 5-78 Creating an HTTP keyword checking rule

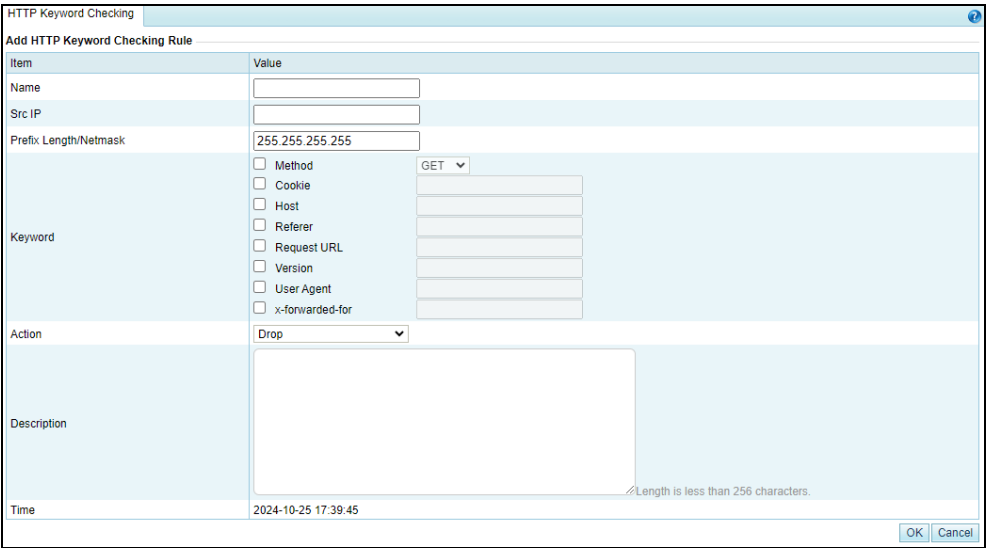


Table 5-40 describes parameters for creating an HTTP keyword checking rule.

Table 5-40 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.
Src IP	Specifies the source IP address. Both IPv4 and IPv6 are supported. The value 0.0.0.0 or :: indicates all source IP addresses.

Parameter	Description
Prefix Length/Netmask	Specifies the prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address.
Keyword	Specifies the type of keywords to be checked. You can select one or more.
Action	<p>Specifies the action to be taken against a packet that matches an HTTP keyword checking rule. It can be any of the following:</p> <ul style="list-style-type: none"> • 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+blocklist: 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 5.2.5 Blocklist. • Drop+disconnect: indicates ADS drops a packet with the specified signature and disconnects the current connection. • Drop+blocklist+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+allowlist: 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 5.2.1 Allowlist. • 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, with no more than 256 characters.
Time	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 SSL/TLS Keyword Checking

An SSL/TLS keyword checking rule analyzes and checks whether SSL/TLS client hello and server hello packets contain matching keywords. For matching packets, ADS will take one of the following actions, depending on your configuration:

- Accept
- Accept+allowlist
- Drop
- Drop+blocklist
- Drop+disconnect
- Drop+blocklist+disconnect
- Limit rate

You can configure up to 1024 SSL/TLS 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 SSL/TLS 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.

Choose **Policy > Access Control > SSL/TLS Keyword Checking** to manage the rule list in the right pane of the page. Initially, the rule list is empty.

Click **Add** and configure parameters on the page that appears. [Table 5-41](#) describes parameters for configuring an SSL/TLS keyword checking rule.

An SSL/TLS keyword checking rule, after being created, can be queried, edited and deleted. However, the rule that has been referenced in a group protection policy cannot be deleted.

Table 5-41 Parameters for adding an SSL/TLS keyword checking rule

Parameter		Description
Name		Name of the SSL/TLS keyword checking rule, containing 1–20 characters of letters, digits, and/or underscores.
Src IP		Specifies the source IP address. Both IPv4 and IPv6 are supported. The value 0.0.0.0 or :: indicates all source IP addresses.
Prefix Length/Netmask		Specifies the prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address. For example, you can type a prefix length of 64 or a netmask of 255.255.255.0. The prefix length of an IPv6 address must be in the range of 0 to 128.
Source or Destination Port		Specifies the source port or destination port of packets to be checked. The value range is 0–65535, with 443 as the default value. For a JA3 template, or a custom template with HandShakeType set to Client hello , the destination port of packets will be checked against this setting. For a JA3S template, or a custom template with HandShakeType set to Server hello , the source port of packets will be checked against this setting.
Keyword Template		Specifies a keyword template. Options include JA3 , JA3S , and Custom . Different templates provide different keywords that you can specify for checking. Click Help to view introduction to JA3/JA3S fingerprinting.
Keyword	Specifies keywords for checking. For a JA3 template, configure the following fields for check of client hello packets.	
	SSLVersion	SSL version of a client hello or server hello packet. It must be a string of four hexadecimal characters.
	Cipher Suites	Cipher suite of a client hello packet. It must be a string of 0–256 hexadecimal characters, in increments of 4.
	SSLExtension	It must be a string of 0–128 hexadecimal characters.
	Elliptic Curves/Supported groups	An extension field, indicating the elliptic curve. It must be a string of 0–128 hexadecimal characters.
	EllipticCurve	An extension field, indicating whether to compress the elliptic curve. It must

Parameter		Description
	PointFormat	be a string of 0–128 hexadecimal characters.
	Full String Import	Populates the foresaid keywords automatically with a full string you type in the text box. You can use a packet capture tool such as Wireshark to obtain the full string.
	Generate JA3 Fingerprint	Calculates the JA3 fingerprint based on keywords you typed to facilitate your configuration checking.
	<p>For a JA3S template, configure the SSLVersion, Cipher Suites, and SSLExtension of a server hello packet.</p> <p>You can also type a full string in the text box and click Full String Import to automatically populate keywords. In addition, you can click Generate JA3S Fingerprint to calculate the JA3S fingerprint for your configuring checking.</p>	
	<p>For a custom template, select the check box before each parameter configured to make the setting take effect.</p>	
	HandShakeType	Handshake type. Valid values include Client hello and Server hello . The default value is Client hello .
	SSLVersion	SSL version of a client hello or server hello packet. It must be a string of four hexadecimal characters.
	Random	Random number generated. It must be a string of four hexadecimal characters.
	Session ID	Session ID of a packet. It must be a string of 0–128 hexadecimal characters.
	Cipher Suites	<p>Cipher suite of a packet. It must be a string of hexadecimal characters.</p> <ul style="list-style-type: none"> When HandShakeType is set to Client hello, it is a string of 0–256 hexadecimal characters, in increments of 4. When HandShakeType is set to Server hello, it is a string of four hexadecimal characters.
	Cipher Suites Numbers	<p>This parameter is available only when HandShakeType is set to Client hello.</p> <p>Specifies the minimum and maximum numbers of cipher suites of a packet. The value range is 0–256.</p> <p>Selecting Yes under Invert inverts the settings.</p>
	Extension Numbers	<p>Specifies the minimum and maximum numbers of extensions of a packet. The value range is 0–256.</p> <p>Selecting Yes under Invert inverts the settings.</p>
	Custom Extension	Custom extensions of a packet. It must be a string of 8–256 hexadecimal characters, in increments of 2.
	Server Name Indication	<p>This parameter is available only when HandShakeType is set to Client hello.</p> <p>Server name indication (SNI for short) is a TLS extension by which a client indicates to the server which host name it is attempting to connect to so that the server can obtain the correct certificate for the domain and return it to the client for verification. Type 1 to 128 characters, including only digits, letters, periods, colons, brackets, hyphens, and underscores, such as 123.com.</p> <p>SNI is case-insensitive.</p>
	Invert	Some parameters including Cipher Suites Numbers , Extension Numbers and Server Name Indication provide Invert settings. Selecting Yes indicates the exclusion of the value configured.

Parameter	Description
Action	<p>Specifies the action to be taken against packets that match this SSL/TLS keyword checking rule. It can be any of the following:</p> <ul style="list-style-type: none"> • Accept: allows matching packets to pass through ADS. • Drop: drops matching packets. • Drop+blocklist: drops matching packets and adds their source IP addresses to the blocklist. To select this option, you must enable the blocklist function in advance. For details about this function, see section 5.2.5 Blocklist. • Drop+disconnect: drops matching packets and disconnects the current connection. • Drop+blocklist+disconnect: drops matching packets, adds their source IP addresses to the blocklist, and then disconnects the current connection. To select this option, you must enable the blocklist function in advance. • Accept+allowlist: allows matching packets to pass through and adds their IP addresses to the allowlist. To select this option, you must enable the allowlist in advance. For details about this function, see section 5.2.1 Allowlist. • Limit rate: limits the number of matching packets passing through ADS based on the specified threshold. Excessive packets will be dropped. The value range is 1–6000000 pps, with 4000 as the default value.
Description	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.

5.2.8 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. If the number of connections from a source IP address exceeds the allowed number of concurrent connections, or that of new connections in a new connection statistic cycle, the source IP address will be automatically added to the blocklist.

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](#)

5.2.8.1 Creating a Connection Exhaustion Protection Rule

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

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

Initially, the rule list is empty.

Figure 5-79 List of connection exhaustion rules

Connection Exhaustion Rules											
<input type="checkbox"/>	Dst IP	Dst IP Prefix Length/Netmask	Dst Port	Src IP	Src IP Prefix Length/Netmask	Concurrent Connections	New Connection Statistical Cycle	New Connections	Description	Time of Creation	Operation
											<input type="button" value="Delete"/> <input type="button" value="Add"/>

Step 2 Click Add.

Figure 5-80 Creating a connection exhaustion rule

Connection Exhaustion Rules

Add Connection Exhaustion Rule

Item	Value
Dst IP	<input type="text"/>
Dst IP Prefix Length/Netmask	<input type="text" value="255.255.255.255"/>
Dst Port	<input type="text" value="0"/>
Src IP	<input type="text" value="0.0.0.0"/> 0.0.0.0 or :: indicates any IP addresses.
Src IP Prefix Length/Netmask	<input type="text" value="0.0.0.0"/>
Concurrent Connections	<input type="text" value="24"/> (1-513) The maximum allowed number is 512. The value 513 indicates no limit.
New Connection Statistical Cycle	<input type="text" value="3"/> (1-300 seconds)
New Connections	<input type="text" value="12"/> (1-10000)
Description	<div></div> Length is less than 256 characters.
Time of Creation	2024-10-25 17:49:34



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

Table 5-42 describes parameters for creating a connection exhaustion rule.

Table 5-42 Parameters for creating a connection exhaustion rule

Parameter	Description
Dst 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.
Dst Port	Server ports to be protected. The port number ranges from 0 to 65535.
Src 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	Threshold of allowed concurrent connections from a source IP address. If this

Parameter	Description
Connections	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.
Description	Presents description of the rule, with no 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 Connection Exhaustion Rule

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

Step 1 Choose **Policy > 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

5.2.8.3 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. However, a rule being referenced in a group protection policy cannot be deleted.

- Method 1: Choose **Policy > Access Control > Connection Exhaustion Rules**. Click  in the **Operation** column of a rule and then click **OK** in the confirmation dialog box to delete the rule.
- Method 2: Choose **Policy > Access Control > Connection Exhaustion Rules**. Select one or more connection exhaustion rules (or select the check box in the table header 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.

5.2.9 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 **Policy > Access Control > Regular Expression Rules**.

Initially, the rule list is empty.

Step 2 Click **Add**.

Figure 5-81 Creating a regular expression rule

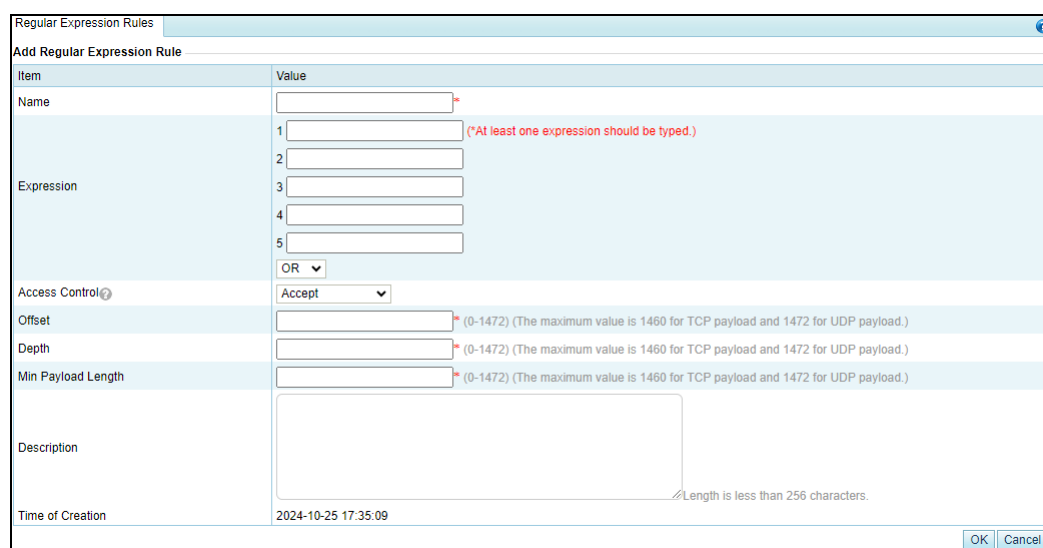


Table 5-43 describes parameters for creating a regular expression rule.

Table 5-43 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 or AND .
Access Control	Specifies the action the ADS device takes for packets with specified signatures. It has the following values: <ul style="list-style-type: none"> Accept: allows such packets to pass through. Drop: drops such packets once they are detected. Drop+blocklist: drops such packets and adds their source IP addresses to the blocklist. Before selecting this option, you must enable the blocklist. For

Parameter	Description
	<p>details about the blocklist, see section 5.2.5 Blocklist.</p> <ul style="list-style-type: none"> • Drop+disconnect: drops such packets and disconnects the connection to 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, with no 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

5.2.10 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](#)

5.2.10.1 Creating a URL-ACL Protection Rule

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

Step 1 Choose **Policy > Access Control > URL-ACL Rules**.

Initially, the rule list is empty.

Figure 5-82 List of URL-ACL rules

URL-ACL Rules									
<input type="checkbox"/>	ID	Domain Name	URL (html/html/jsp/php/asp, without domain name)	Dst IP	Dst Port	URL Protection Mode	Description	Time of Creation	Operation
<div> Move <input type="text"/> Behind <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> </div>									

Step 2 Click **Add**.

Figure 5-83 Creating a URL-ACL rule

Item	Value
Domain Name	.
URL	.*(html html jsp php asp, without domain name)
Dst IP	.
Dst Port	80
URL Protection Mode	Drop+blocklist
Description	
Time	2024-10-25 17:52:17

Table 5-44 describes parameters for creating a URL-ACL rule.

Table 5-44 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.
Dst IP	IP address of the server. You can type an IPv4 or IPv6 address according to the actual network deployment.
Dst 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: <ul style="list-style-type: none"> Drop+blocklist: drops packets and adds the source addresses to the blocklist. Trust: allows packets to pass. Block proxy: blocks the proxy if it is possible to use the proxy to transfer packets. Limit rate by Src IP: limits the rate above which packets from the source IP address are forwarded. Monitor+blocklist: counts the total number of HTTP requests of the 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

Parameter	Description
	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 blacklist.
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, with no more than 256 characters.
Time	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

5.2.10.2 Editing a URL-ACL Protection Rule

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

Step 1 Choose **Policy > Access Control > URL-ACL Rules**.


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

5.2.10.3 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. However, a rule being referenced in a group protection policy cannot be deleted.


- Method 1: Choose **Policy > Access Control > URL-ACL Rules**. Click  in the **Operation** column of a rule and then click **OK** in the confirmation dialog box to delete the rule.
- Method 2: Choose **Policy > Access Control > URL-ACL Rules**. Select one or more URL-ACL rules (or select the check box in the table header 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.

5.2.10.4 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 .

5.2.11 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.

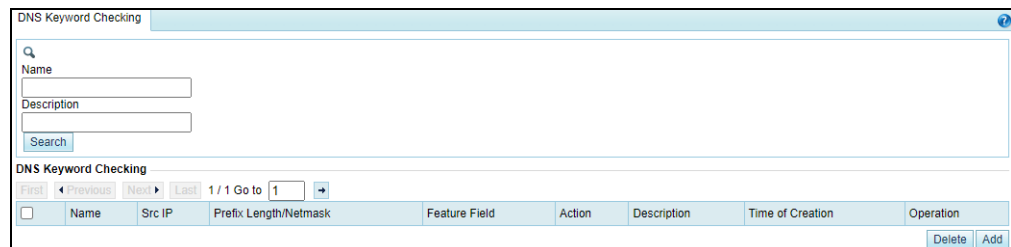
A DNS keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting DNS keyword checking rules are the same as those for access control rules.

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

Step 1 Choose Policy > Access Control > DNS Keyword Checking.

Initially, the rule list is empty.

Figure 5-84 List of DNS keyword checking rules



DNS Keyword Checking

Search

Name

Description

Search

DNS Keyword Checking

First Previous Next Last 1 / 1 Go to 1

	Name	Src IP	Prefix Length/Netmask	Feature Field	Action	Description	Time of Creation	Operation
--	------	--------	-----------------------	---------------	--------	-------------	------------------	-----------

Delete Add

Step 2 Click Add.

Figure 5-85 Creating a DNS keyword checking rule

Table 5-45 describes parameters for creating a DNS keyword checking rule.

Table 5-45 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.
Src IP	Specifies the source IP address. Both IPv4 and IPv6 are supported. The value 0.0.0.0 or :: indicates all source IP addresses.
Prefix Length/Netmask	Specifies the prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the 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: <ul style="list-style-type: none"> • 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+blocklist: 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 5.2.5 Blocklist. • Accept+allowlist: 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 5.2.1 Allowlist. • 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

Parameter	Description
	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, with nomore 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

5.2.12 DNS Subdomain Allowlist

A DNS random subdomain attack, also known as pseudo-random subdomain (PRSD) attack or a water torture attack, floods the authoritative server with thousands of malicious DNS requests. As a result, the authoritative server becomes overloaded with requests and even crashes. Rate limiting can effectively block such attack packets, but it also blocks normal traffic. To ensure normal services, it is advisable to add trusted DNS subdomains to the allowlist and allow related queries to pass through.

You can configure a global or group-specific DNS subdomain allowlist. The former has a higher priority than the latter. This section describes how to configure a global DNS subdomain allowlist.

5.2.12.1 Enabling/Disabling the DNS Subdomain Allowlist Function

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

Enabling the DNS Subdomain Allowlist Function

To enable the DNS subdomain allowlist function, perform the following steps:

Step 1 Choose **Policy > Access Control > DNS Subdomain Allowlist**.

By default, the DNS subdomain allowlist function is disabled.

Step 2 Click **Edit**, select **Yes** for **Enable**, and click **OK** in the confirmation dialog box.


Step 3 Select a value for **Action for Unmatched DNS Requests**.

The action set here applies to all DNS requests that do not match the subdomain list. If the subdomain list is empty, the global allowlist function of subdomains does not work. Leave this parameter at its default settings and modify it after adding valid subdomain names. You can select one of the following options:

- **Default:** indicates that packets of DNS requests that do not match the subdomain list are not handled here, but are submitted for subsequent checks.
- **Limit rate:** limits the number of packets of DNS requests that do not match the subdomain list based on the specified threshold. Excessive packets will be dropped. The value range is 1–24000000 pps, with 2000 as the default value.
- **Drop:** directly drops packets of DNS requests that do not match the subdomain list.

Step 4 Configure the auto-learning parameters of the DNS subdomain allowlist.

Table 5-46 Parameters of DNS subdomain allowlist auto-learning

Parameter		Description
Enable		<p>Controls whether to enable the auto-learning function of the subdomain allowlist.</p> <p>After the DNS subdomain allowlist and its auto-learning function are both enabled, the system can automatically learn and identify requests from normal DNS subdomains, and filters out requests from malicious subdomains. This improves protection effectiveness and reduces false positives.</p>
Auto-learning Type		<p>Packet type on which DNS subdomain auto-learning will be based. Options include DNS query and DNS response.</p> <ul style="list-style-type: none"> • DNS query is applicable to diversion and in-path modes. <ul style="list-style-type: none"> – In diversion mode, ADS will automatically learn subdomain names from DNS queries over all interfaces. – In in-path mode, ADS will automatically learn subdomain names only from DNS queries over the IN interface. • DNS response is applicable to the in-path mode. In this mode, ADS will automatically learn subdomain names from DNS responses received by the OUT interface. For ADS in in-path mode, the preferred option is DNS response. <p> Note</p> <p>If DNS response is selected, Action for Unmatched DNS Requests cannot be set to Drop.</p>
Min Source IPs		<p>This parameter is required when DNS query is selected for Auto-learning Type.</p> <p>Minimum number of source IP addresses that request the same subdomain names. The value range is 2–256, with 3 as the default.</p>
Statistical Period		<p>This parameter is required when DNS query is selected for Auto-learning Type.</p> <p>Period of time when the number of source IP addresses that request the same domain name is counted. The value range is 1–3600 seconds, with 30 as the default.</p> <p>When the number reaches the threshold specified with Min Source IPs in the statistical period, the requested subdomain name is added to the allowlist.</p>
Constraints	Max Domain Levels	<p>Maximum number of levels allowed for domain name. When the number reaches the threshold, the domain name will not be added to the allowlist.</p> <p>The value range is 0–16, with 0 as the default. The value 0 indicates no limit.</p>
	Uppercase Restriction	<p>Controls whether to allow the subdomain name to contain uppercase letters. The value Yes indicates subdomain names containing uppercase letters will not be added to the allowlist.</p>
Auto Allowlist Duration		<p>Validity period of subdomain names in the allowlist. After this period, the subdomain names will be removed from the allowlist.</p> <p>The value range is 0–8000000 minutes, with 120 as the default. The value 0 indicates permanently valid.</p>

Step 5 Click **OK** to enable the DNS subdomain allowlist function.

Figure 5-86 DNS subdomain allowlist

DNS Subdomain Allowlist	
DNS Subdomain Allowlist	
Item	Value
Enable	Yes (The global allowlist of DNS subdomains has a higher priority than the group-specific allowlist of DNS subdomains. If both are enabled, only the global allowlist takes effect.)
Primary Configuration Items	
Item	Value
Action for Unmatched DNS Requests	Default
Subdomain Allowlist Auto-Learning	
Item	Value
Enable	Yes
Auto-learning Type	DNS query
Min Source IPs	3
Statistical Period	30(s)
Constraints	Max Domain Levels: 0
	Uppercase Restriction: Yes
Auto Allowlist Duration	120(min)

[Edit](#) | [Subdomain List](#) | [Add](#) | [Search](#) | [Import](#) | [Export](#) | [Clear](#)

----End

Disabling the DNS Subdomain Allowlist Function

If the DNS subdomain allowlist function is enabled, you can click **Edit** in the DNS **Subdomain Allowlist** area and then select **No** for **Enable** to disable it.

5.2.12.2 Adding Subdomains to the DNS Subdomain Allowlist

You can manually add a trusted subdomain to the DNS subdomain allowlist or import a subdomain allowlist file.

Adding a Subdomain

On the page shown in [Figure 5-86](#), click **Add** to type a domain name. The domain name is case-insensitive, and should meet the following requirements:

- A domain name only consists of letters, digits, dots, hyphens, and/or underscores.
- Each label of the domain name ranges from 1 to 63 characters, and the domain name cannot exceed 128 characters.
- The domain name should contain at least one label.
- A label cannot start or end with a hyphen, nor have consecutive hyphens.

Importing a Subdomain Allowlist File

To import a subdomain allowlist file, perform the following steps:

- Step 1** On the page shown in [Figure 5-86](#), click **Import**.
- Step 2** (Optional) On the page that appears, click **Download Import Template** and save it to a local disk drive. Type allowed subdomains in the template.

At most 10,000 subdomain names can be imported, with each in a separate line.

- Step 3** Click **Choose File**, select the allowlist file (.txt) and click **Open**.

The file name is then displayed on the page.

- Step 4** Click **Upload**.

After the allowlist file is imported, the system shows the import result.


Figure 5-87 Import result

DNS Subdomain Allowlist	
Import Result	
Item	Value
Start Time	2024-10-28 10:24:06
End Time	2024-10-28 10:24:06
Progress	100%
Total Entries	2
Successful Imports	2
Failed Imports	0
Incorrectly Formatted Entries	0
Refresh Download Back	

Step 5 View the number of successful and failed imports on the **Import Result** page.

You can also perform the following operations:

- Click **Refresh** to update import data in real time.
- Click **Download** to save the import result file to a local disk drive.
- Click **Back** to return to the **Import Subdomain Allowlist** page.

 <p>Note</p>	<p>In addition, you can click View Import Result on the Import Subdomain Allowlist page to view import results.</p>
--	---

----End

5.2.12.3 Managing the Subdomain Allowlist

After adding subdomain to the DNS subdomain allowlist, you can view, query, delete, export, and clear it.

Viewing the subdomain allowlist

On the page shown in [Figure 5-86](#), click **Subdomain List** to view allowed subdomains that are manually added or imported. The system displays a maximum of 1000 manually allowed subdomains.

Deleting the subdomain allowlist

On the **Allowed Subdomain List** page, select one or more domain names and then click **Delete**. In the confirmation dialog box, click **OK**.

Querying the subdomain allowlist

On the page shown in [Figure 5-86](#), click **Search**. Type the domain name to query in the textbox and click **OK** to check whether the subdomain name is allowed. Only exact search is supported.

If the domain name is manually allowlisted, the **Allow Type** shows **MANUAL**. If the domain name is automatically allowlisted, the **Allow Type** shows **AUTOMATIC**.

Figure 5-88 Query result


DNS Subdomain Allowlist	
Search Result	
Item	Value
Domain Name	123.www.test.com
Allowlisted	Yes
Allow Type	AUTOMATIC

Exporting the subdomain allowlist

On the page shown in [Figure 5-86](#), click **Export**. On the **Export Subdomain Allowlist** page that appears, configure export parameters, and click **OK**. [Table 5-47](#) describes export parameters.

Table 5-47 Parameters for exporting subdomain names

Parameter	Description
Export Type	Specifies the type of the subdomain allowlist for export, which can be Manual or Auto .
Export Method	Specifies the export method, which can be either of the following: <ul style="list-style-type: none">• Quick: Only allowed domain names are included in the exported file.• Detailed: Allowlist entry details, like the allowed domain names and the reason for their addition, are included in the exported file.

Click  in the **Operation** row to save the exported DNS subdomain allowlist file to a local disk drive.

Clearing the subdomain allowlist

By clearing the DNS subdomain allowlist, you can delete the trust status of all subdomains included in the allowlist on the engine (memory). If a subdomain in this allowlist needs to be re-trusted after the allowlist is cleared, you need to manually add it to the allowlist or import an allowlist file.

On the page shown in [Figure 5-86](#), click **Clear**. On the **Clear Subdomain Allowlist** page that appears, select an allowlist type to be cleared, and click **OK**.

- **Manual**: the subdomain allowlist that is manually added or imported.
- **Auto**: the subdomain allowlist that is generated by auto-learning.

5.2.13 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 Protection Rules**. Click **Add** and configure parameters. [Table 5-48](#) 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 reference a programmable rule in a group protection policy, see section [5.1.2.21 Programmable Rule](#).

Table 5-48 Parameters of a programmable rule

Parameter	Description
Name	Name of the rule, which can contain 20 characters at most.
Programming Expression	<p>Expression of the rule, which can contain 200 characters at most. You can type the following character types:</p> <ul style="list-style-type: none"> • 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 <p>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.</p> <ul style="list-style-type: none"> • 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 most.
Time of Creation	Time when the rule was created. It is automatically generated by the system.

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.



When ADS is in in-path mode, only the **General Settings** menu is available under **Diversion & Injection**, while **Diversion Routes**, **Traffic Injection**, **Traffic Diversion**, **Advanced Route Setting**, and **Syslog Diversion** are unavailable.

6.1 General Settings

This section covers the following topics:

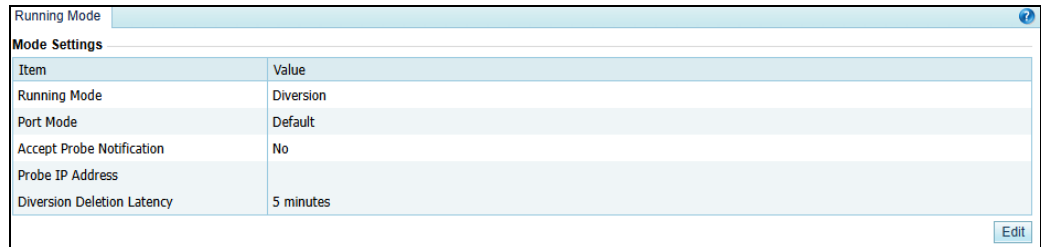
- Running Mode
- Port Channel Configuration
- GRE Tunnel Configuration
- IP Address Configuration
- Incoming/Outgoing Configuration

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**.

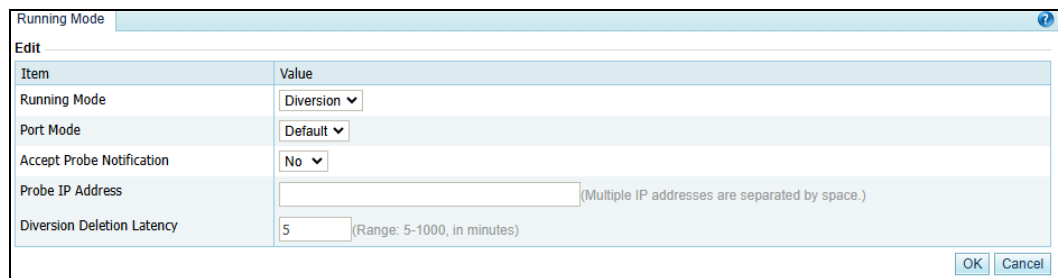
Figure 6-1 Running mode of the ADS device (diversion mode)



Item	Value
Running Mode	Diversion
Port Mode	Default
Accept Probe Notification	No
Probe IP Address	
Diversion Deletion Latency	5 minutes

Step 2 Click **Edit**.


Figure 6-2 Editing the running mode (diversion mode)





Item	Value
Running Mode	Diversion
Port Mode	Default
Accept Probe Notification	No
Probe IP Address	
Diversion Deletion Latency	5

Table 6-1 describes parameters on this page.

Table 6-1 Parameters for setting the running mode

Parameter	Description
Running Mode	<p>Current running mode of the ADS device. It has the following options:</p> <ul style="list-style-type: none"> 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. <p> Note</p> <ul style="list-style-type: none"> 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

Parameter	Description
	<p>the current ADS device to handle attacks that are detected.</p> <p> Note</p> <p>This parameter is required only when Running Mode is set to Diversion.</p>
Probe IP Address	<p>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.</p> <p> Note</p> <p>This parameter is required only when Running Mode is set to Diversion.</p>
Diversion Deletion Latency	<p>After receiving a diversion deletion notification, ADS deletes the diversion after an automatic delay. The value should be in the range of 5–1000 minutes.</p> <p>If ADS receives a diversion deletion notification, and then receives a diversion setup notification before Diversion Deletion Latency expires, ADS automatically ignores the diversion deletion notification and continues to divert traffic.</p>

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	<p>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.</p>
--	---

Choose **Diversion & Injection > General Settings > Port Channels > Port Channels** to open the port channel configuration page. See [Figure 6-3](#).

Figure 6-3 Port Channel page

Port Channels Port Channel Status			
Port Channel Members			
Interface ID	Priority ?	Mode ?	Operation
G3/1	32768	Active	
G3/2	32768	Active	
G3/3	32768	Active	
G3/4	32768	Active	
F4/1	32768	Active	
F4/2	32768	Active	
F4/3	32768	Active	
F4/4	32768	Active	
Port Channels			
Port Channel ID	Physical Port	Aggregation Mode ?	Operation
<div>Add</div>			

Editing a Port Channel Member

In the **Port Channel Members** 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	G3/1
Priority ?	32768 (1-65535)
Mode ?	Active
<div>OK Cancel</div>	

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 changed.
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. <ul style="list-style-type: none"> Passive: The interface does not send, but only receives Link Aggregation Control Protocol Data Unit (LACPDU)s from the peer; Active: The interface sends and receives LACPDU.s.

Parameter	Description
	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** page appears, as shown in Figure 6-5.

Figure 6-5 Creating a port channel for the ADS device

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 95.
Physical Port	Available physical ports on the current ADS device. <div> <p>Note</p> <ul style="list-style-type: none"> 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. </div>
Aggregation Mode	Specifies how member interfaces of the current port channel aggregate, which can be Manual or Dynamic. <ul style="list-style-type: none"> 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.

	<p>A port channel configured with an IP address and injection interface cannot be deleted.</p>
---	--

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 Channels > Port Channel Status** to open the port channel status page. See [Figure 6-6](#).

Figure 6-6 Port Channel Status page

Port Channel

Port Channel Status

LACP Packet Statistics

Port Channel ID	Value							
0	Portchannel0's PDU statistic is :							
	PortName	PortNo	PortMode	LacpDesent	LacpDesRecv	MarkerPduDesent	MarkerPduDesRecv	
	TL1/1	0	0	0	0	0	0	
1	Portchannel1's PDU statistic is :							
	PortName	PortNo	PortMode	LacpDesent	LacpDesRecv	MarkerPduDesent	MarkerPduDesRecv	
	TL1/2	1	1	21461	0	0	0	
30	Portchannel30's PDU statistic is :							
	PortName	PortNo	PortMode	LacpDesent	LacpDesRecv	MarkerPduDesent	MarkerPduDesRecv	
	GE/5	6	6	0	0	0	0	
31	Portchannel31's PDU statistic is :							
	PortName	PortNo	PortMode	LacpDesent	LacpDesRecv	MarkerPduDesent	MarkerPduDesRecv	
	GE/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: 00-30-71-ae-2d-ae
	Max Active-linknumber	24								TimeoutMode: LONG PERSIST
	Prompt 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	00-30-71-ae-2d-ae	11	00-00-00-00-00-00	65536	0	Yes			
	ActorPortName	Status	PortNo	PortMode	PortPri	Speed(Mb/s)	PortKey	PortStat	IS_FSM	TI_FSM
	TL1/1	SELECTED	0	0	32768	10000	11	00110000	DEFAULTED	NO_FKEY1000C
	ActorPortName	PortNo	SysPri	SystemID	PortPri	PortKey	PortStat			
	TL1/1	0	65536	00-00-00-00-00-00	65536	0	00000000			
	[*]MapAggregation Port Stat:									
	ActorPortName	Status	PortNo	PortMode	PortPri	Speed(Mb/s)	PortKey	PortStat	IS_FSM	TI_FSM
	TL1/1	SELECTED	0	0	32768	10000	11	00110000	DEFAULTED	NO_FKEY1000C
	ActorPortName	PortNo	SysPri	SystemID	PortPri	PortKey	PortStat			
	TL1/1	0	65536	00-00-00-00-00-00	65536	0	00000000			

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	<input type="text"/>
GRE Tunnel IP	<input type="text"/>
Local IP	12.19.1.254 ▼
Remote IP	<input type="text"/>

OK Cancel

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

IP Addresses

Interface IP List

IP Address	Prefix Length/Netmask	Interface	VLAN ID	Web Access	SSH Login	Operation
12.19.1.254	255.255.255.0	V4/1	1	No	No	
12:19:1::254	64	V4/1	1	No	No	

Add

Loopback Address

ID	IP Address	Prefix Length/Netmask	Operation
----	------------	-----------------------	-----------

Add



The number of interfaces varies with ADS series, but the procedure for configuring interface IP 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 IP** page appears, as shown in [Figure 6-9](#).

Figure 6-9 Adding an IP address

IP Addresses


Add IP

Item	Value
IP Address	<input type="text"/>
Prefix Length/Netmask	<input type="text" value="255.255.255.0"/>
Interface	<input type="text" value="V4/1"/> (Note: A maximum of 100 VLANs can be added for a single interface)
VLAN ID	<input type="text"/> (Note: The value range is 1–4095. Type 1 in the case of no specific VLAN. 802.1Q encapsulation will be performed when the VLAN ID is greater than 1.)
Web Access	<input type="checkbox"/>
SSH Login	<input type="checkbox"/>

OK Cancel


[Table 6-5](#) describes parameters of an interface.

Table 6-5 Interface parameters

Parameter	Description
IP Address	<p>IP address of a specified interface on the ADS device. You can type an IPv4 or IPv6 address according to the actual network deployment.</p> <p>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.</p> <div>  Note </div> <p>An interface can have multiple IP addresses.</p>
Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the specified port.

Parameter	Description
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.

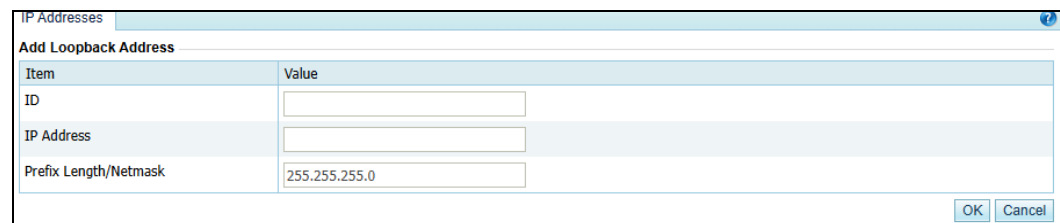
Deleting an IP Address

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** page appears, as shown in [Figure 6-10](#).

Figure 6-10 Adding a loopback address




[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.
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.





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	 
			<input type="button" value="Add"/>

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 ?	<input type="text"/>
Outgoing Interface ID ?	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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 Routes > BGP Routes**. As shown in [Figure 6-13](#), only BGP routes are displayed on the **Local Route** page.

Figure 6-13 Local route parameters

Local Route					
Route Daemon					
	Name	Parameter	Neighbor	Type	Operation
	BGP_v4	BGPV4 /Bind IP 12.19.1.254 /Local AS 65530 /Local Port 179 /Router ID 12.19.1.254 /Metric 100 /Community 600:650		Diversion	
	BGP_v6	BGPV4 /Bind IP 12:19:1::254 /Local AS 65530 /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** 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


Item	Value
Name	<input type="text"/>
Type	Diversion
Local AS	<input type="text"/>
Local Port	<input type="text" value="179"/>
Keepalive	<input type="text" value="60"/>
Holdtime	<input type="text" value="180"/>
Metric	<input type="text" value="100"/>
Bind IP	<input type="text"/>
Router ID	<input type="text" value="127.0.0.1"/>
Management Port (3000-4000)	<input type="text"/>
No-advertise	<input checked="" type="radio"/> Yes <input type="radio"/> No
No-export	<input checked="" type="radio"/> Yes <input type="radio"/> No
Community	<input type="text" value="600:650"/> (*The default value is 600:650.)

[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. <div> Note </div> <p>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.</p>
Local Port	BGP port of the route daemon. Generally, the default port 179 is used.
Bind IP	Local IP address of the route daemon.

Parameter	Description
	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 .


	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.

	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

Neighbor Name	Neighbor IP	Local Daemon	Remote AS	Remote Port	Passive Mode	Auth	eBGP Multihop	Last-Hop IP
		BGP_v4		179	<input type="radio"/> Yes <input checked="" type="radio"/> No			

OK Cancel






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 .
Passive Mode	Controls whether to enable the passive mode for the BGP neighbor.
Auth	Authentication password. This parameter is required only when you encrypt the BGP neighbor.
eBGP Multihop	Maximum number of hops allowed by the External Border Gateway Protocol (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.

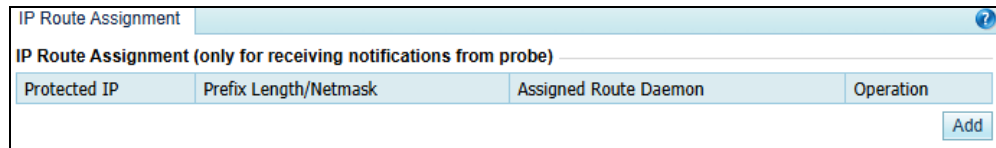


After you click , if the link works properly, the ping output displays the status of only the first five packets.

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

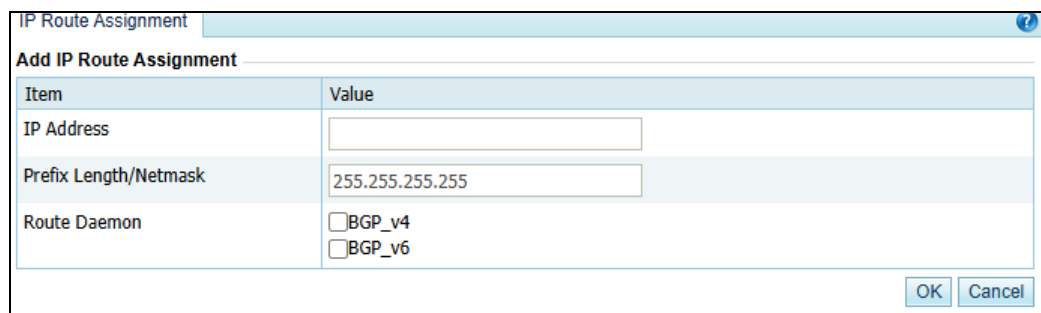


Protected IP	Prefix Length/Netmask	Assigned Route Daemon	Operation
Add			

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



Item	Value
IP Address	<input type="text"/>
Prefix Length/Netmask	<input type="text" value="255.255.255.255"/>
Route Daemon	<input type="checkbox"/> BGP_v4 <input type="checkbox"/> BGP_v6

OK Cancel

[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.
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.


	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

	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 reinjection.

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

Injection Interfaces						
<input type="checkbox"/>	Interface IP	IP Prefix Length/Netmask	VLAN ID	Physical Port	Description	Operation
<input type="checkbox"/>	59.74.2.254	255.255.255.0	0	G4/3		
<input type="checkbox"/>	59:74:2::254	64	0	G4/3		
<input type="checkbox"/>	80:91:77::1	64	77	G4/5		
<input type="checkbox"/>	80.91.77.1	255.255.255.0	77	G4/5		
<input type="checkbox"/>	83.16.55.254	255.255.255.0	0	PortChannel 1		
						<input type="button" value="Add"/> <input type="button" value="Delete"/>

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	<input type="text"/>
Prefix Length/Netmask	<input type="text" value="255.255.255.0"/> (Note: An IPv6 address is valid only when its prefix length ranges from 48 to 128.)
VLAN ID	<input type="text"/> (Type 0 if 802.1Q encapsulation is unnecessary.)
Physical Port	<input type="checkbox"/> V4/1 <input type="checkbox"/> V4/2
Description	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>Length is less than 256 characters.</small>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Table 6-10 describes parameters of an injection interface.

Table 6-10 Parameters of an injection interface

Parameter	Description
Interface IP	<p>IP address of the injection interface. You can type an IPv4 or IPv6 address according to the actual network deployment.</p> <ul style="list-style-type: none"> 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.
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.
Description	Brief information about the injection interface, which is less than 256 characters.

	<p>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.</p> <ul style="list-style-type: none"> 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 check box in the table header 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](#).

Figure 6-20 Injection routes

	Protected 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
<input type="checkbox"/>	0.0.0.0	0.0.0.0	12.19.1.1	0	Invalid	0.0.0.0	0	Invalid	0	Invalid	Enable	⚠ (Primary)	0		
<input type="checkbox"/>	::	0	12:19:1::1	0	Invalid	::	0	Invalid	0	Invalid	Enable	⚠ (Primary)	0		


- Step 2** Click **Add**.

Figure 6-21 Creating an injection route

Item	Value
Protected IP	<input type="text"/>
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 work only if the injection MPLS label learning is enabled on the Advanced Config page.)
Loopback	0.0.0.0
VPN Label	0 (*If no VPN label is configured, fill in 0.)
VPN Learning Mode	Invalid (*Auto learning can work only if the injection MPLS label learning is enabled on the Advanced Config page.)
GRE Tunnel ID	0 Select: ▼
GRE Tunnel Learning Mode	Invalid (*Auto learning can work only if the injection MPLS label learning is enabled on the Advanced Config page.)
Rule Status	Enable ▼
Priority	Primary ▼
IP to Check	0.0.0.0
Gateway of IP to Check	0.0.0.0
Description	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>length is less than 256 characters.</small>

Table 6-11 describes parameters for creating an injection route.

Table 6-11 Parameters for creating an injection route

Parameter	Description
Protected IP	<p>IP address or IPv4 segment of a protected host. You can type an IPv4 or IPv6 address according to the actual network deployment.</p> <p> Note</p> <p>Currently, you can add an injection route for IP addresses in the /16 or /24 subnet, but not for those in the /4 subnet.</p>
Prefix Length/Netmask	<p>Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be protected.</p> <p>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.</p>
Next-Hop IP	<p>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.</p> <p>You can type an IPv4 or IPv6 address according to the actual network deployment.</p>
MPLS Label	MPLS label of the packet forwarded by the injection route. Leave it at the default value 0 if no MPLS label is configured.
MPLS Learning Mode	<p>Specifies how to learn MPLS labels. It has the following values:</p> <ul style="list-style-type: none"> 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.

Parameter	Description
Loopback	Specifies the loopback IP address of the border router in the network where the protected server resides.
VPN Label	VPN label. Leave it at the default value 0 if no VPN label is configured.
VPN Learning Mode	Specifies how to learn the VPN label. It has the following values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Auto-learning: indicates that the ADS system automatically learns GRE 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: <ul style="list-style-type: none"> • Enable: indicates that the system queries the injection rule when forwarding packets. • Disable: indicates that the system does not query the injection rule when forwarding packets.
Priority	Route priority. The default value is Primary . <ul style="list-style-type: none"> • Primary: indicates a higher priority. • Secondary: indicates a lower priority.
IP to Check	IP address to be pinged when the connectivity of the current route is checked. The default value is 0.0.0.0 , indicating that the next-hop IP address is used as the IP to check.
Gateway of IP to Check	The gateway of the IP address to be pinged when the connectivity of the current route is checked. The default value is 0.0.0.0 , indicating that no corresponding static route is configured. If IP to Check and Gateway of IP to Check are set to other values than the default ones, the system automatically adds a static route to IP to Check and with the next hop as Gateway of IP to Check .
Description	Brief information about the route, which is less than 256 characters.



Note

When **Next-Hop IP** 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.

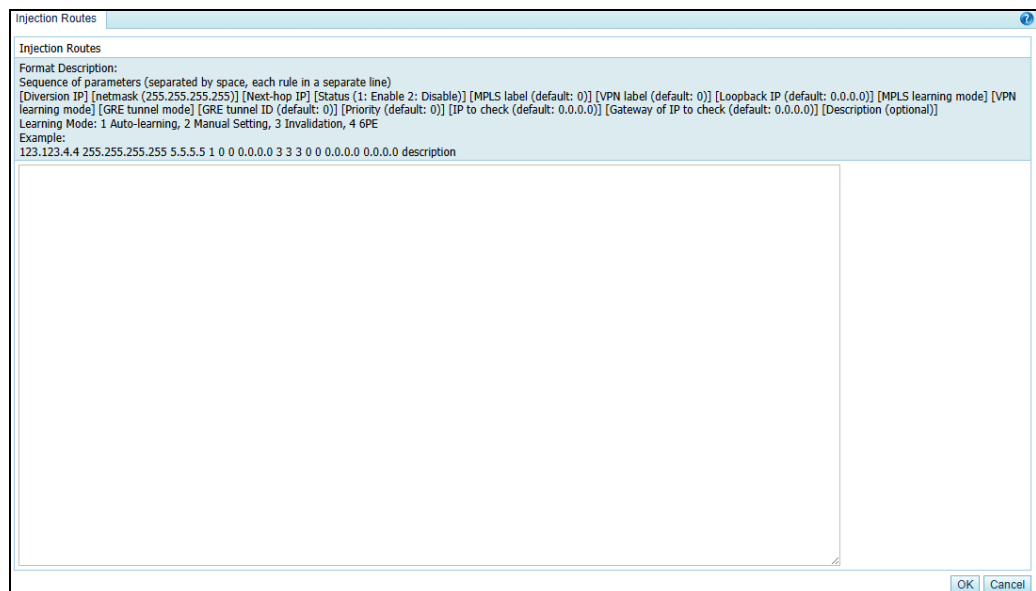
----End

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 **Add Multiple** to the lower right of the injection route list.

Figure 6-22 Creating injection routes in batches



Step 2 Type multiple injection routes as prompted.

Pay attention to the following format specifications:

- An injection route is typed in the following format:[Diversion IP] [netmask (255.255.255.255)] [Next-hop IP] [Status (1: Enable 2: Disable)] [MPLS label (default: 0)] [VPN label (default: 0)] [Loopback IP (default: 0.0.0.0)] [MPLS learning mode] [VPN learning mode] [GRE tunnel mode] [GRE tunnel ID (default: 0)] [Priority (default: 0)] [IP to check (default: 0.0.0.0)] [Gateway of IP to check (default: 0.0.0.0)] [Description (optional)].
- For the learning mode, 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 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:

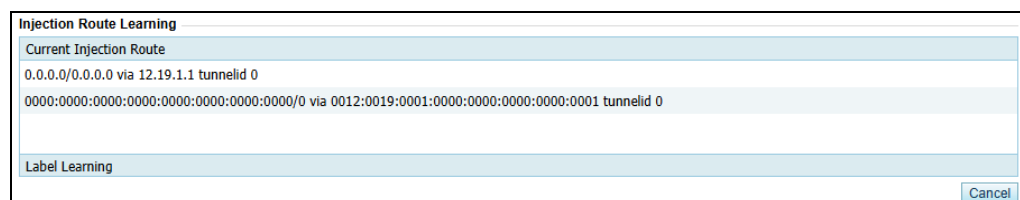
- : The link of this injection route functions properly. That is, ADS can successfully ping the **IP to Check** of the injection route.
- : The link of this injection route is faulty. That is, ADS fails to ping the **IP to Check** of the injection route. In this case, traffic cannot be injected along 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** 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



- **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.


	<p>Injection routes support encapsulation of two layers of labels.</p> <ul style="list-style-type: none"> • 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  on the right of an injection route, as shown in [Figure 6-20](#).



	<ul style="list-style-type: none"> • 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 check box in the table header 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 check box in the table header 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 check box in the table header 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. Click **Edit** to configure parameters.

- 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 6-24.

Figure 6-24 Advanced options

Injection Routes	
Advanced Options	
Item	Value
Enable Injection MPLS Label Learning	No
Enable Longest Route Match	No
Enable Route Cache	No
Diversion-Interface-Preferred Injection	No
VLAN-Preferred Injection	No
Advanced Functions	
Item	Value
Injection Route Redundancy	Disable
Injection Connectivity Check	Disable
LDP Neighbor Status Check	Disable
<input type="button" value="Edit"/> <input type="button" value="Cancel"/>	


Figure 6-25 Advanced options – with the injection route redundancy enabled


Injection Routes	
Edit Advanced Options	
Item	Value
Enable Injection MPLS Label Learning	<input type="radio"/> Yes <input checked="" type="radio"/> No (After this is enabled, injection routes are dispatched only when requested in a diversion notification.)
Enable Longest Route Match	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Route Cache	<input type="radio"/> Yes <input checked="" type="radio"/> No
Diversion-Interface-Preferred Injection	<input type="radio"/> Yes <input checked="" type="radio"/> No
VLAN-Preferred Injection	<input type="radio"/> Yes <input checked="" type="radio"/> No
Edit Advanced Functions	
Item	Value
Injection Route Redundancy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Injection Connectivity Check	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LDP Neighbor Status Check	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Edit Advanced Function Parameters	
Item	Value
Check Interval	60 s (1-600)
Max Retries	3 (1-10)
Max Link Switchovers	5 (0-10)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	


Step 3 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.
		<div>  Note </div> <ul style="list-style-type: none"> If MPLS label learning is enabled while MPLS

Parameter		Description
		<p>injection is disabled, injection routes of other types will be unable to be dispatched.</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p> Note</p> <ul style="list-style-type: none"> 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	<p>Controls whether to enable the injection route redundancy function.</p> <p> Note</p> <p>After injection route redundancy is enabled, neither diversion-interface-preferred injection nor injection MPLS label learning can be enabled.</p>
	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.
	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

Parameter		Description
		injection routes will lose effect and traffic diversion for all MPLS-related IP addresses will stop.
Advanced Function Parameters	Check Interval	Specifies the interval between two link availability checks. The value ranges from 1 to 600, in seconds. The default value is 60 .
	Max Retries	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.
	Max Link Switches	<p>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.</p> <p> Note</p> <p>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.</p>

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:

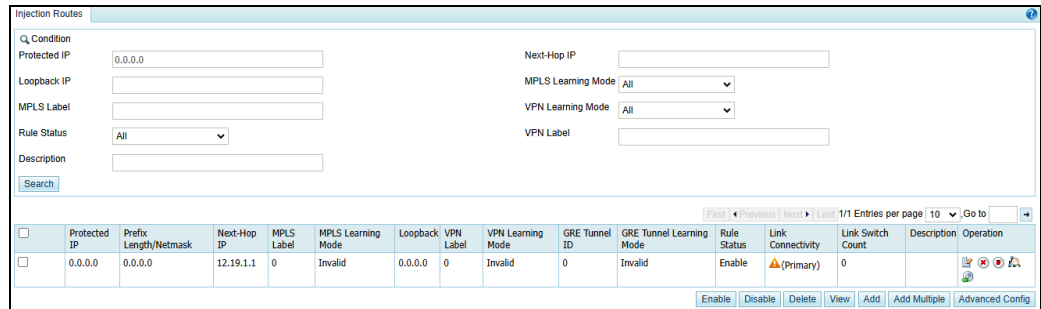
Step 1 Set filtering conditions.

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



----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 about dynamic learning of MAC addresses, see section [6.3.2.6 Learning MAC Address](#). This section covers the following topics:

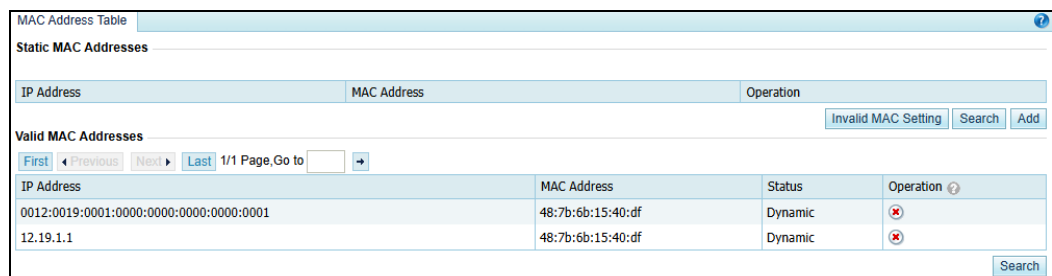
- [Adding a MAC Address Entry](#)
- [Editing a MAC Address Entry](#)
- [Deleting a MAC Address Entry](#)
- [Querying MAC Addresses](#)
- [Configuring Invalid MAC Addresses](#)
- [Configuring Valid MAC Addresses](#)

6.3.3.1 Adding a MAC Address Entry

To add a MAC address entry, perform the following steps:

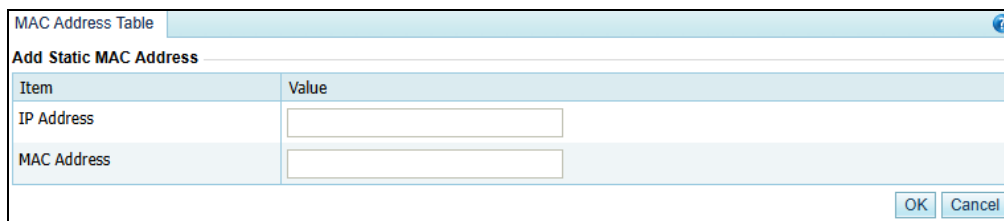
- Step 1** Choose **Diversion & Injection > Traffic Injection > MAC Address Table** to open the configuration page for the MAC address table.

Figure 6-27 MAC address table




- 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




Step 3 Type the IP address and MAC address and click **OK** to save the settings.

 Note	<p>The ADS device supports the IPv4/IPv6 dual stack. Therefore, you can configure IPv4 or IPv6 addresses in the MAC address table.</p>
--	--

----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.

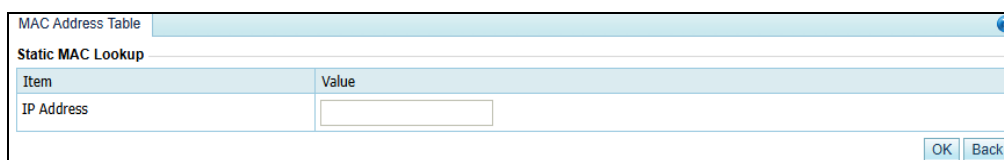
In the MAC address table shown in [Figure 6-27](#), click  in the **Operation** column of a MAC address entry and then click **OK** to delete an entry.

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 **Search** to the lower right of the MAC address table to open the static MAC address lookup page.

Figure 6-29 Querying the MAC address mapped to an IP address



Step 2 Type the IPv4 or IPv6 address and click **OK**.

Then, the MAC address mapped to this IP address is displayed.

Step 3 Click **Back** to return to the MAC address table.

----End

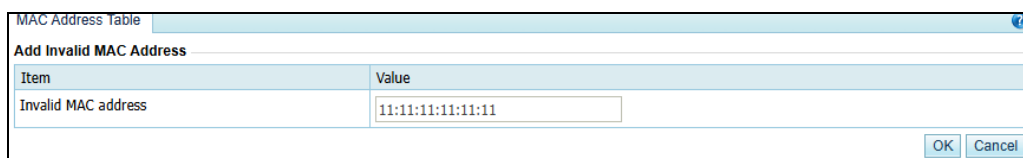
6.3.3.5 Configuring Invalid MAC Addresses

If the MAC address of an IP packet is the same as an invalid MAC address configured on the ADS device, the system drops the packet automatically.

To add an invalid MAC address, perform the following steps:

Step 1 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](#).

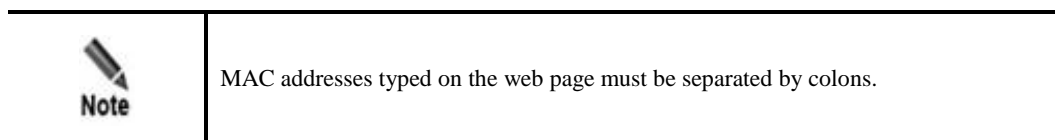
Figure 6-30 Configuring invalid MAC addresses



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.



----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 valid MAC address lookup 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.

A check in the **Allow diversion by default** check box, 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

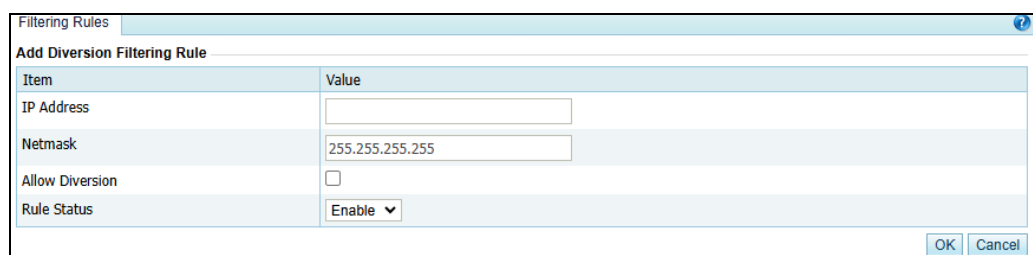


IP Address	Prefix Length/Netmask	Allow Diversion	Rule Status	Operation
Allow diversion by default <input checked="" type="checkbox"/> Add				

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



Item	Value
IP Address	<input type="text"/>
Netmask	<input type="text" value="255.255.255.255"/>
Allow Diversion	<input type="checkbox"/>
Rule Status	Enable ▼

[OK](#) [Cancel](#)

[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.
Netmask	Netmask of the IP address to be protected. This parameter allows you to configure a network segment.
Allow Diversion	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: <ul style="list-style-type: none"> 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 the 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.



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:

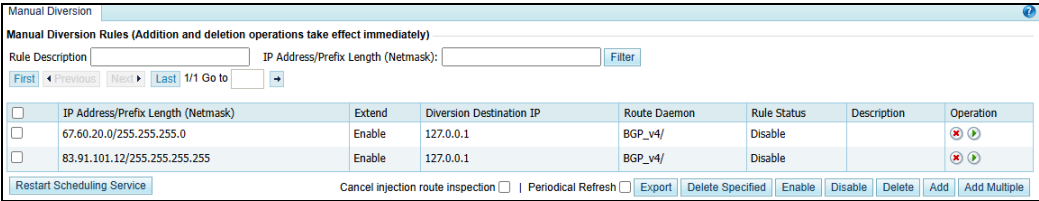
- [Creating a Manual Traffic Diversion Rule](#)
- [Creating Manual Diversion Rules in Batches](#)
- [Enabling and Disabling Manual Diversion Rules](#)
- [Filtering Manual Diversion Rules](#)
- [Deleting Manual Diversion Rules](#)
- [Deleting a Specified Route](#)
- [Refreshing Routes Periodically](#)
- [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



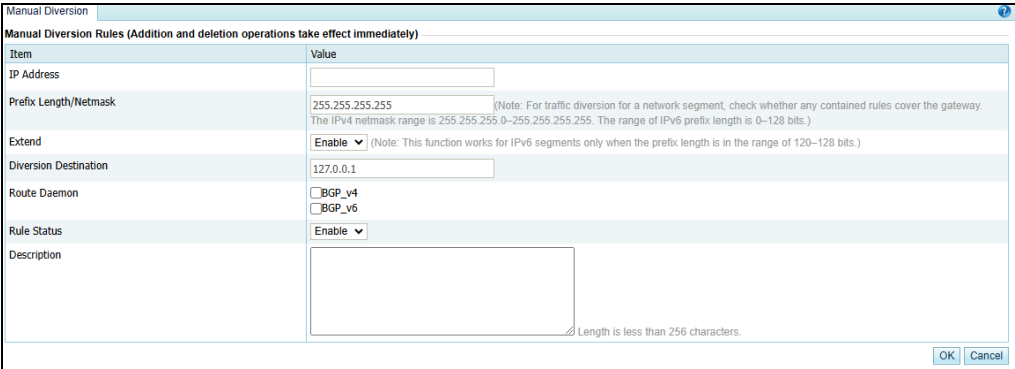
The screenshot shows the 'Manual Diversion' configuration window. At the top, it says 'Manual Diversion Rules (Addition and deletion operations take effect immediately)'. Below this is a search bar with 'Rule Description' and 'IP Address/Prefix Length (Netmask)' fields, and a 'Filter' button. There are navigation buttons: 'First', 'Previous', 'Next', 'Last', and a '1/1 Go to' dropdown. A table lists the current rules:

<input type="checkbox"/>	IP Address/Prefix Length (Netmask)	Extend	Diversion Destination IP	Route Daemon	Rule Status	Description	Operation
<input type="checkbox"/>	67.60.20.0/255.255.255.0	Enable	127.0.0.1	BGP_v4/	Disable		
<input type="checkbox"/>	83.91.101.12/255.255.255.255	Enable	127.0.0.1	BGP_v4/	Disable		

At the bottom, there are buttons: 'Restart Scheduling Service', 'Cancel injection route inspection' (checkbox), 'Periodical Refresh' (checkbox), 'Export', 'Delete Specified', 'Enable', 'Disable', 'Delete', 'Add', and 'Add Multiple'.

- Step 2** Click **Add**.

Figure 6-34 Creating a traffic diversion rule




The screenshot shows the 'Manual Diversion' configuration window with the 'Add' rule form. It has a title bar 'Manual Diversion' and a subtitle 'Manual Diversion Rules (Addition and deletion operations take effect immediately)'. The form is divided into two columns: 'Item' and 'Value'. The fields are:

- IP Address:
- Prefix Length/Netmask: (Note: For traffic diversion for a network segment, 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: This function works for IPv6 segments only when the prefix length is in the range of 120-128 bits.)
- Diversion Destination:
- Route Daemon: ☐ BGP_v4, ☐ BGP_v6
- Rule Status: ☒ Enable
- Description: (Note: Length is less than 256 characters.)


At the bottom right, there are 'OK' and 'Cancel' buttons.

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.
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. <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Enable: enables a diversion filtering rule immediately after it is added. Disable: disables the diversion filtering rule that can be enabled later manually.
Description	Brief information about the diversion rule, which is less than 256 characters.

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

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] [Extend (1: Enable 2: Disable)] [Diversion destination] [Route daemon] [Rule status (1: Enable 2: Disable)] [Description (optional)], for example, 10.10.10.18 255.255.255.255 1 127.0.0.1 nei1/ 1 description. For multiple daemons, a manual diversion rule is as follows: 10.10.10.18 255.255.255.255 1 127.0.0.1 nei1/nei2/ 1 description.
- The list of available daemons is: BGP_v4 and BGP_v6.
- 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 check box in the table header 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.

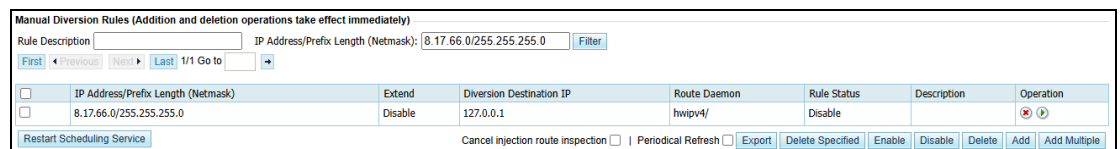
Disabling Manual Diversion Rules

- 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 check box in the table header to select all manual diversion rules) to be disabled, 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 Rules (Addition and deletion operations take effect immediately)

Rule Description: IP Address/Prefix Length (Netmask): **Filter**


First ◀ Previous Next ▶ Last 1/1 Go to

<input type="checkbox"/>	IP Address/Prefix Length (Netmask)	Extend	Diversion Destination IP	Route Daemon	Rule Status	Description	Operation
<input type="checkbox"/>	8.17.66.0/255.255.255.0	Disable	127.0.0.1	hwip4/	Disable		 

Restart Scheduling Service Cancel injection route inspection ☐ Periodical Refresh ☐ **Export** **Delete Specified** **Enable** **Disable** **Delete** **Add** **Add Multiple**

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 about 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 the rule.
- Method 2: On the manual diversion rule list shown in [Figure 6-33](#), select one or more rules (or select the check box in the table header 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.



For details about 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 on the **Delete Specified Route** page.

Figure 6-37 Deleting a specified diversion rule

Delete Specified Route (It takes effect immediately)	
Item	Value
IP Address	<input type="text"/>
Prefix Length/Netmask	255.255.255.255 <small>(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.)</small>
Extend	Enable ▾
Diversion Destination	<input type="text"/>
Route Daemon	<input type="checkbox"/> BGP_v4 <input type="checkbox"/> BGP_v6 <input type="checkbox"/> All <small>(It applies only to rules (in which daemon is all) added for the "routerman" account.)</small> <input type="checkbox"/> ospf <input type="checkbox"/> rip <input type="checkbox"/> 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



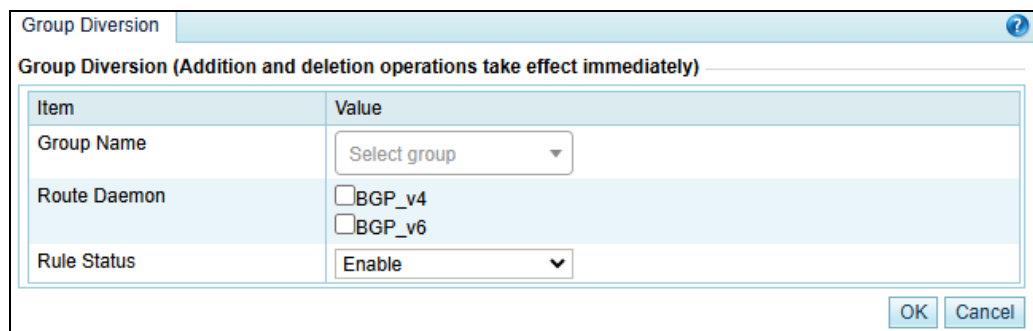
The interface shows a table with columns: Group Name, Route Daemon, Status, and Operation. There are 'Delete' and 'Add' buttons at the bottom right.

Group Name	Route Daemon	Status	Operation

Buttons: Delete, Add

Step 2 Click **Add**.

Figure 6-39 Creating a group diversion rule



The dialog box contains the following fields:

- Group Name: Select group (dropdown)
- Route Daemon: ☐ BGP_v4, ☐ BGP_v6
- Rule Status: Enable (dropdown)

Buttons: OK, Cancel

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. <ul style="list-style-type: none"> 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 check box in the table header 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.

- **IP Address:** specifies the IP address to be protected, namely, the IP address that packets are originally destined for.
- **Dst IP:** specifies the destination IP address to which the traffic is diverted for cleaning.

Figure 6-40 Diversion routing table

Diversion Routing Table					
Diversion Route List (Refresh to view the current diversion route)					
IP Address	Netmask	Dst IP	Route Daemon	Route Source	Operation
67.60.20.0	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.1	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.2	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.3	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.4	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.5	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.6	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.7	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.8	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.9	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.10	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.11	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.12	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.13	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.14	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.15	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.16	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.17	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.18	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.19	255.255.255.255	127.0.0.1	BGP_v4	local	
67.60.20.20	255.255.255.255	127.0.0.1	BGP_v4	local	

Searching for a Diversion Route

Step 1 On the page shown in [Figure 6-40](#), click **Search** to the lower right of the diversion routing table.

The **Search** page appears, as shown in [Figure 6-41](#).

Figure 6-41 Searching for diversion routes

Diversion Routing Table


Search Diversion Route

Item	Value
IP Address	<input type="text"/>
Netmask	<input type="text" value="255.255.255.0"/>

OK Cancel

[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.
Netmask	<div>  Note </div> <p>The netmask of an IPv4 address to be searched for must be 255.255.255.255.</p>

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

Exporting the Diversion Route List

On the page shown in [Figure 6-40](#), click **Export** to the lower right of the diversion routing table.

The diversion route list will be downloaded and saved to a local disk drive in text format.

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.

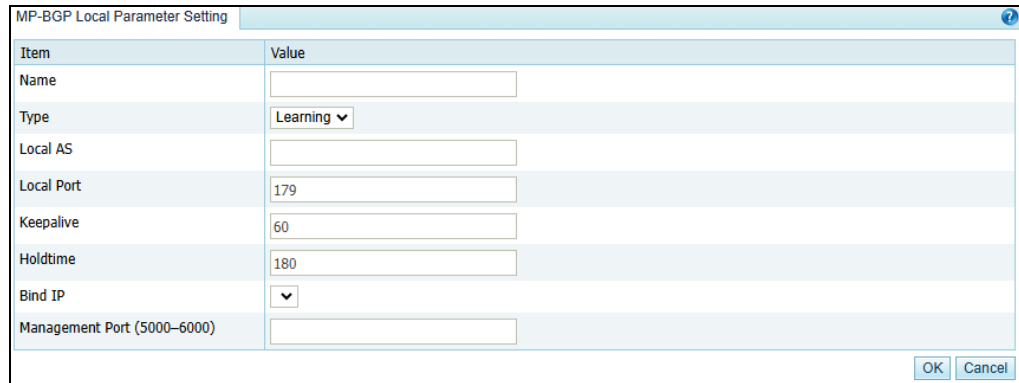
Figure 6-42 List of MPLS routes

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	
<div>Add MP-BGP</div>					

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



The dialog box titled "MP-BGP Local Parameter Setting" contains the following fields:

Item	Value
Name	<input type="text"/>
Type	Learning ▼
Local AS	<input type="text"/>
Local Port	179
Keepalive	60
Holdtime	180
Bind IP	▼
Management Port (5000-6000)	<input type="text"/>

Buttons: OK, Cancel

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.

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
<input type="text"/>	<input type="text"/>	aa	<input type="text"/>	179	<input type="text"/>	<input type="text"/>	<input type="text"/>	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	  
ripng	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 Daemon

Route Service Setting: sldp

Item	Value
Run Service at Startup	<input type="radio"/> Yes <input checked="" type="radio"/> No
Type	Learning
LSR-ID	

Interface Setting

IP Address	Enable MPLS Setting
12.19.1.254	<input type="checkbox"/>
12:19:1::254	<input type="checkbox"/>

OK Cancel Clear Settings

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. <ul style="list-style-type: none"> 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.

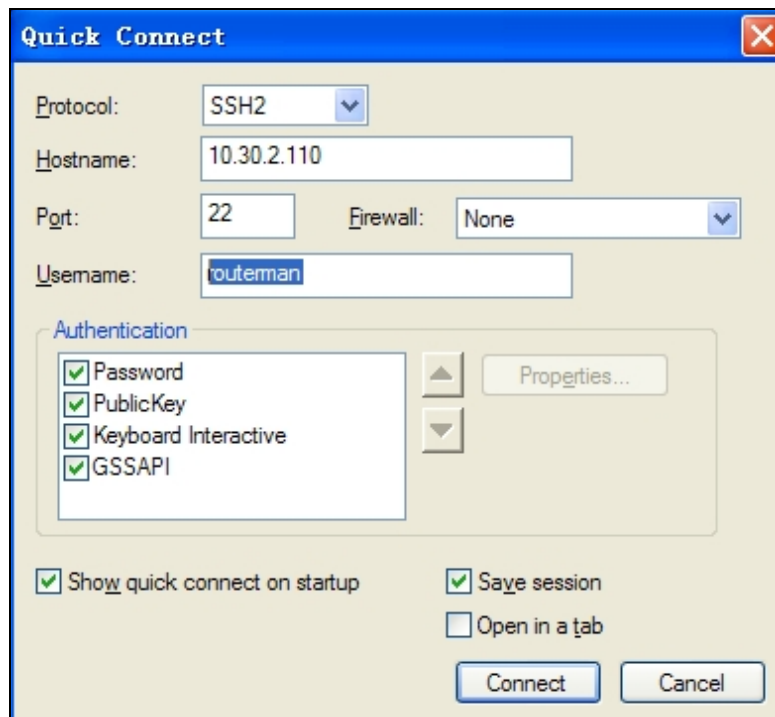
----End

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



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](#).


	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.

	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

Name	IP Address	Port	Operation

Step 2 Click **Add**.

Figure 6-50 Creating a diversion rule

Item	Value
Name	Arbor
Rule Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Address	
Port	
Alert Level	Type
Level 1	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Level 2	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Level 3	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Level 4	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Level 5	<input checked="" type="radio"/> Auto <input type="radio"/> 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	<p>Specifies the alert level that will trigger traffic diversion. This parameter is available only for Genie and Arbor devices.</p> <ul style="list-style-type: none"> 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 a specific date or month. 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

Time	Attack Type	Src IP	Dst IP	Src Port	Dst Port	Policy
2024-11-28 15:54:08	SYN Flood	6.4.4.4	83.91.101.22	876	80	SYN_Time_Sequence_Check
2024-11-28 15:54:08	SYN Flood	6.4.4.4	83.91.101.22	875	80	SYN_Time_Sequence_Check
2024-11-28 15:54:08	SYN Flood	6.4.4.4	83.91.101.22	874	80	SYN_Time_Sequence_Check
2024-11-28 15:53:38	SYN Flood	6.4.4.4	83.91.101.22	876	80	SYN_Time_Sequence_Check
2024-11-28 15:53:38	SYN Flood	6.4.4.4	83.91.101.22	875	80	SYN_Time_Sequence_Check
2024-11-28 15:53:38	SYN Flood	6.4.4.4	83.91.101.22	874	80	SYN_Time_Sequence_Check
2024-11-28 15:53:08	SYN Flood	6.4.4.4	83.91.101.22	34342	80	SYN_Time_Sequence_Check
2024-11-28 15:53:08	SYN Flood	6.4.4.4	83.91.101.22	34341	80	SYN_Time_Sequence_Check
2024-11-28 15:53:08	SYN Flood	6.4.4.4	83.91.101.22	34340	80	SYN_Time_Sequence_Check
2024-11-28 15:52:38	SYN Flood	6.4.4.4	83.91.101.22	5792	80	SYN_Time_Sequence_Check
2024-11-28 15:52:38	SYN Flood	6.4.4.4	83.91.101.22	5791	80	SYN_Time_Sequence_Check
2024-11-28 15:52:38	SYN Flood	6.4.4.4	83.91.101.22	5790	80	SYN_Time_Sequence_Check
2024-11-28 15:52:08	SYN Flood	6.4.4.4	83.91.101.22	25169	80	SYN_Time_Sequence_Check
2024-11-28 15:52:08	SYN Flood	6.4.4.4	83.91.101.22	25167	80	SYN_Time_Sequence_Check
2024-11-28 15:52:08	SYN Flood	6.4.4.4	83.91.101.22	25166	80	SYN_Time_Sequence_Check
2024-11-28 15:51:38	SYN Flood	6.4.4.4	83.91.101.22	58544	80	SYN_Time_Sequence_Check
2024-11-28 15:51:38	SYN Flood	6.4.4.4	83.91.101.22	58543	80	SYN_Time_Sequence_Check
2024-11-28 15:51:38	SYN Flood	6.4.4.4	83.91.101.22	58542	80	SYN_Time_Sequence_Check

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.
Src IP/Port	Source IP address and port of the attack. <div>  <p>Note</p> <p>Src IP is displayed as the real source IP address in the following logs:</p> <ul style="list-style-type: none"> 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. </div>
Dst IP/Port	Destination IP address and port of the attack.
Policy	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** 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 Chart

To the lower left of the **Statistical Chart** 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

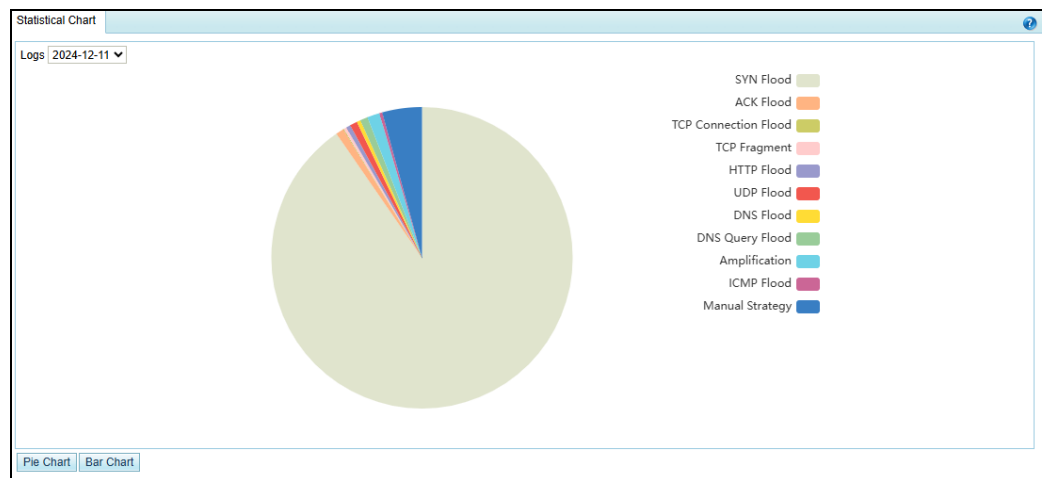
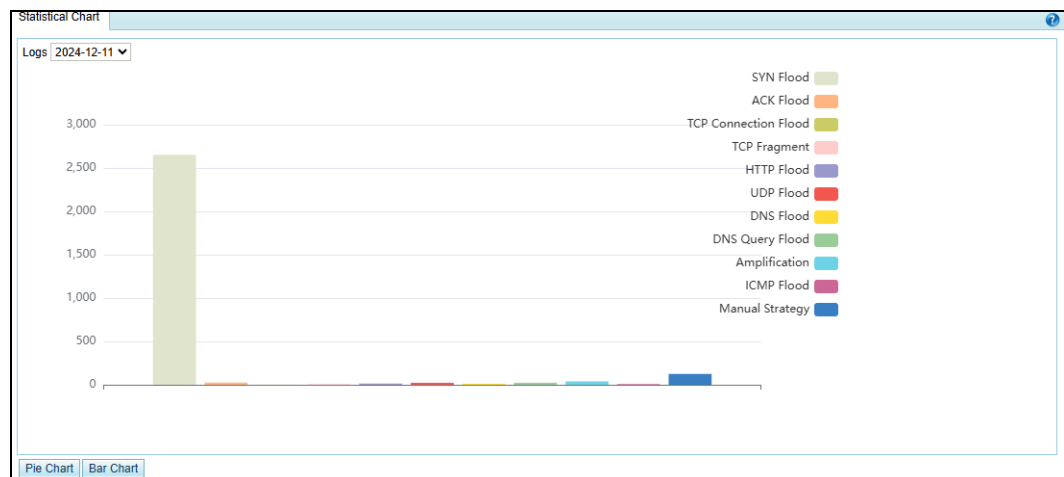


Figure 7-3 Number of attacks of each type



7.2 System Logs

You can search for system logs and download recent 50,000 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
- Authorization 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.
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
Login IP	IP address of a login user
Result	Whether the login succeeded or failed

Parameter	Description
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

Parameter	Description
	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

	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 Log**. The **HA Sync Log** 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.
Description	Log details, including what type of information a log records and operation results.

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.



- 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 involved in the current operation.
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 Authorization Configuration Logs

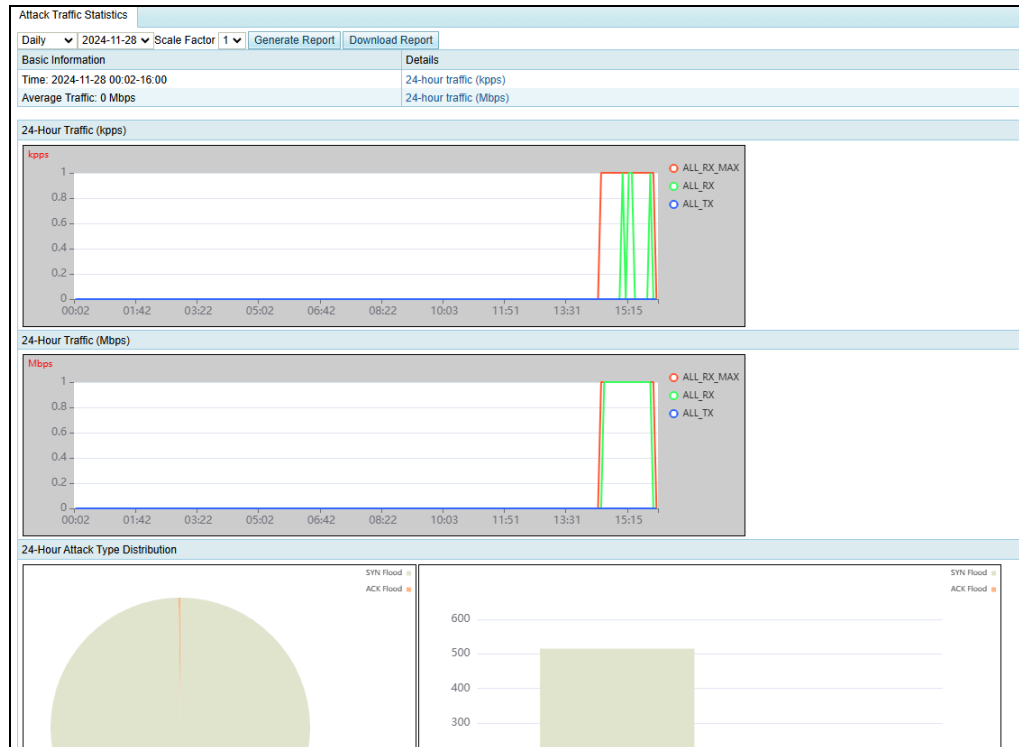
The **Authorization Configuration Log** page is available only when vADS is used. For details about authorization configuration, see section 3.4.1 [License](#).

The authorization configuration log list displays the authorization 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



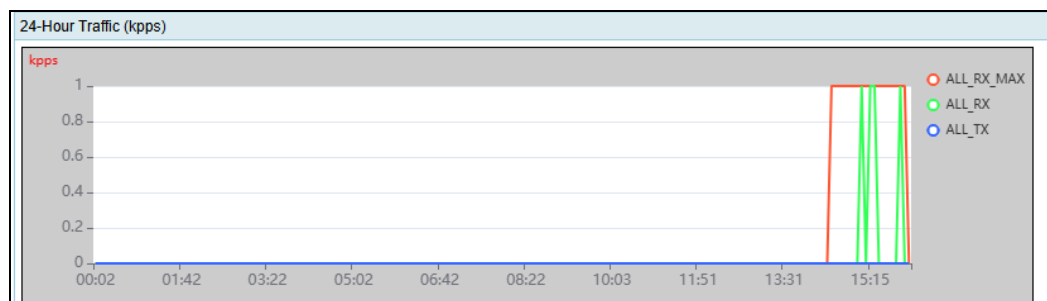
Daily Attack Traffic Report

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.

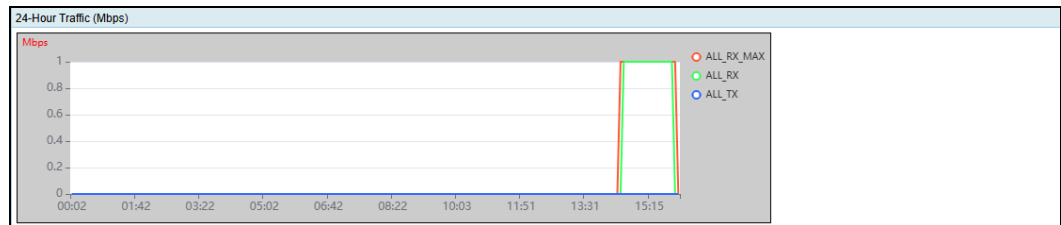
Figure 7-5 24-hour traffic (in kpps)



- 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)

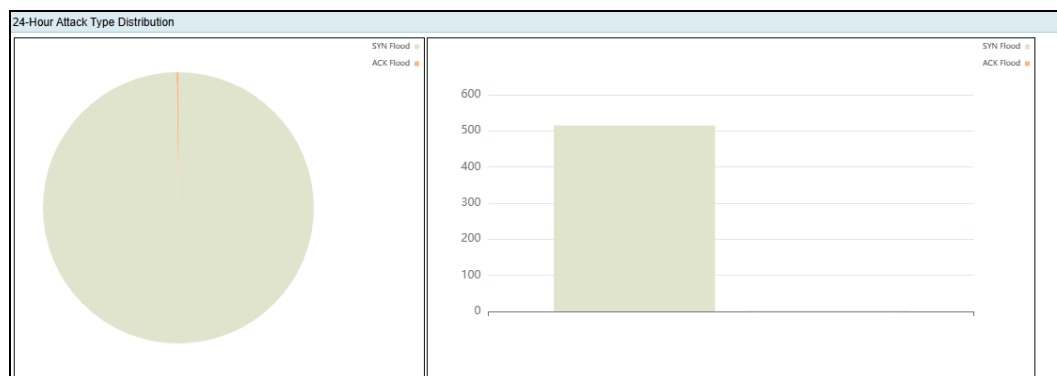


- 24-hour attack type statistics

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 Top 5 Target IPs									
83.91.101.22	SYN Flood	ACK Flood	FIN RST Flood	TCP Misuse	TCP Connection Flood	TCP Fragment	HTTP Flood	HTTP Slow Attack	
	513	0	0	0	0	0	0	0	
	HTTPS Flood	UDP Flood	UDP Fragment	SIP Flood	DNS Flood	DNS Query Flood	DNS Amplification	SSDP Amplification	
	0	0	0	0	0	0	0	0	
	SNMP Amplification	Chargen Amplification	NTP Amplification	Memcache Amplification	Amplification	ICMP Flood	ICMP Fragment	LAND Flood	
	0	0	0	0	0	0	0	0	
	Manual Strategy	CLDAP Amplification	MS SQL Amplification	TI Strategy	Carpet Bombing Attack				
83.91.3.1	SYN Flood	ACK Flood	FIN RST Flood	TCP Misuse	TCP Connection Flood	TCP Fragment	HTTP Flood	HTTP Slow Attack	
	1	1	0	0	0	0	0	0	
	HTTPS Flood	UDP Flood	UDP Fragment	SIP Flood	DNS Flood	DNS Query Flood	DNS Amplification	SSDP Amplification	
	0	0	0	0	0	0	0	0	
	SNMP Amplification	Chargen Amplification	NTP Amplification	Memcache Amplification	Amplification	ICMP Flood	ICMP Fragment	LAND Flood	
	0	0	0	0	0	0	0	0	
	Manual Strategy	CLDAP Amplification	MS SQL Amplification	TI Strategy	Carpet Bombing Attack				
8391:0001:0000:0000:0000:0000:0000:0001	SYN Flood	ACK Flood	FIN RST Flood	TCP Misuse	TCP Connection Flood	TCP Fragment	HTTP Flood	HTTP Slow Attack	
	1	0	0	0	0	0	0	0	
	HTTPS Flood	UDP Flood	UDP Fragment	SIP Flood	DNS Flood	DNS Query Flood	DNS Amplification	SSDP Amplification	
	0	0	0	0	0	0	0	0	
	SNMP Amplification	Chargen Amplification	NTP Amplification	Memcache Amplification	Amplification	ICMP Flood	ICMP Fragment	LAND Flood	
	0	0	0	0	0	0	0	0	
	Manual Strategy	CLDAP Amplification	MS SQL Amplification	TI Strategy	Carpet Bombing Attack				

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.



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						
Protection Event Statistics						
<div> <div>Q</div> <div> Group ALL </div> <div> Dst IP </div> <div> Dst Port </div> <div> Policy ALL </div> <div> Time Today </div> <div>Search</div> </div>						
<div> <div>First</div> <div>Previous</div> <div>Next</div> <div>Last</div> <div>1/450 Go to</div> <div>Download</div> <div>Clear</div> </div>						
Group	Dst IP	Dst Port	Policy	Start Time	End Time	
default_protection_group	30.13.66.8a	111	UDP_Control_By_Dstip	2024-12-16 11:11:44	Ongoing	
default_protection_group	30.13.66.25	8001	SYN_Algorithm	2024-12-16 11:11:44	Ongoing	
default_protection_group	30.13.66.88	8001	SYN_Algorithm	2024-12-16 11:11:44	Ongoing	
default_protection_group	30.13.66.86	111	UDP_Control_By_Dstip	2024-12-16 11:11:44	Ongoing	
default_protection_group	30.13.66.9	80	SYN_Time_Sequence_Check	2024-12-16 11:11:14	Ongoing	
default_protection_group	30.13.66.50	443	HTTPS_FINGERPRINT_Protection	2024-12-16 11:11:14	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 TI	Describes how to configure collaboration between ADS and TI as well as TI upgrade and IP exceptions.

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 Capture**.





In the upper part of the **Manual 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 **Not running**.

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 Capture

Manual Capture Rules

<input type="checkbox"/>	Name	Status	Number of PCAP Files	Operation
<input type="checkbox"/>	in	Not running	1	   

Refresh Add Delete

PCAP Files

<input type="checkbox"/>	File Name	Size (bytes)	Task Details	Operation
<input type="checkbox"/>	colicap_in_1_2024-11-28_15-52-28.cap	86014	Interface: all Protocol: ALL Sampling Ratio: 1 Advanced Options: Received	View Download Analyze

Delete

Step 2 Click **Add** to create a manual packet capture task.

Figure 8-2 Creating a manual packet capture task

Manual Capture

Parameter Settings

Item	Value
Name	<input type="text"/>
Interface	ALL
Protocol	ALL
Max Packets	<input type="text"/> (1–30000)
Max Time	<input type="text"/> (1–3600s) (*If both Max Packets and Max Time are set, the packet capture will stop at whichever limit is reached first.)
Packet Sampling Rate	1 (1–65535) (*Example: 1000, indicating that one in 1000 packets is captured. The value 1 indicates that no sampling is conducted.)
Src IP	<input type="text"/> (Example: 192.168.1.0/24. For IPv4 addresses, the netmask length should be 1 to 32; for IPv6 addresses, the prefix length should be 1 to 128.)
Destination IP/Group	<input checked="" type="radio"/> IP <input type="text"/> <input type="radio"/> Group default_protection_group
Source/Destination IP	<input type="text"/> (*If this field is set, Source IP and Destination IP will lose effect.)
Max Packet Length	<input type="text"/> (64–1518)
Advanced Options	<input checked="" type="checkbox"/> Receive <input type="checkbox"/> Send <input type="checkbox"/> Drop (*If no option is selected, a packet reaching the device will be captured by default.)







Add Back

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.
Max Packets	Number of packets to be captured. The value ranges from 1 to 30000.
Max Time	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 Max Packets or that of Max Time is met.
Packet Sampling Rate	Specifies the ratio of matched packets to captured packets. Value range:

Parameter	Description
	<p>1–65535.</p> <p>For example, the value 1000 indicates that one in 1000 packets are captured. The default value is 1, indicating no packet sampling.</p> <p>When the traffic bursts, the packet sampling rate allows the device to capture packets in a longer period.</p>
Src IP	<p>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.</p> <p> Note</p> <p>The source IP address can be an IPv4 or IPv6 address.</p>
Destination IP/Group	<p>Destination IP address or group of this task. You can select IP or Group.</p> <ul style="list-style-type: none"> • 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	<p>Source or destination IP address of the task. This parameter is optional. If you set this parameter, ignore Src IP and Destination IP/Group.</p> <p> Note</p> <p>Both IPv4 and IPv6 addresses are allowed.</p>
Src Port	<p>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.</p> <p> Note</p> <p>This parameter is available only when Protocol is set to UDP or TCP.</p>
Dst Port	<p>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.</p> <p> Note</p> <p>This parameter is available only when Protocol is set to UDP or TCP.</p>
Source or Destination Port	<p>Source or destination port of the task. This parameter is optional. If this parameter is specified, the system ignores both Src Port and Dst Port.</p> <p> Note</p> <p>This parameter is available only when Protocol is set to UDP or TCP.</p>
Max Packet Length	<p>Maximum length of the packet to be captured. The value ranges from 64 to 1518.</p>
Advanced Options	<p>This parameter is optional. Options are as follows:</p> <ul style="list-style-type: none"> • Receive: indicates that ADS captures received packets. • Send: indicates that ADS captures packets that are sent. • Drop: indicates that ADS captures dropped packets. <p> Note</p>


Parameter	Description
	<ul style="list-style-type: none"> 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 Add.

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 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 **Not running**.

8.1.1.3 Stopping a Manual Packet Capture Task

In the **Manual 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 **Not running**.


8.1.1.4 Viewing a Manual Packet Capture Task

In the **Manual 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 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 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 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 Capture Rules** area shown in [Figure 8-1](#), select one or more manual packet capture tasks (or select the check box in the table header 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.



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 **PCAP 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 Details

Packet Summary: Name:colicap_in_1_2024-11-28_15-52-28.cap Size:86014 Task Details:Interface: all | Protocol: ALL | Sampling Ratio: 1 | Advanced Options: Received

FirstPreviousNextLast

1/1 pages | 1000Go to

No	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Information
1	2024-11-28 15:52:28	6.4.4.4	17060	83.91.101.22	80	tcp	70	SYN
2	2024-11-28 15:52:28	6.4.4.4	17066	83.91.101.22	80	tcp	70	SYN
3	2024-11-28 15:52:28	6.4.4.4	17061	83.91.101.22	80	tcp	70	SYN
4	2024-11-28 15:52:28	6.4.4.4	17062	83.91.101.22	80	tcp	70	SYN
5	2024-11-28 15:52:28	6.4.4.4	17067	83.91.101.22	80	tcp	70	SYN
6	2024-11-28 15:52:28	6.4.4.4	17069	83.91.101.22	80	tcp	70	SYN
7	2024-11-28 15:52:28	6.4.4.4	17068	83.91.101.22	80	tcp	70	SYN
8	2024-11-28 15:52:28	6.4.4.4	17064	83.91.101.22	80	tcp	70	SYN

IP Layer

Src IP	6.4.4.4	Total Length	52
Dst IP	83.91.101.22	IP Header Length	20
TOS	0x0000	TTL	62
IP Flag	0x0002	Offset	--
Protocol	tcp	Checksum	0xc9b8
IP ID	0xb092		

TCP

Source IP Blocking

Src Port	17060	Dst Port	80
TCP Seq Number	0x9e16f35	TCP ACK Number	0xcd044141
TCP Flag	0x0002	Maximum Segment Size	--
Timestamp	--	Window scale	8

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

Parameter	Description
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
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 Details

Packet Summary: Name:colicap_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

Back

First

Previous

Next

Last

1/1 pages,

1000entries

Go to

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:f0fe	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		

Source IP Blocking

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

Application-Layer Fingerprint Extraction

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 5.2.5 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		

Source IP Blocking

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)

OK Back

Step 3 Set the block period. For parameter details, see [Table 5-37](#).

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 **Policy > Access Control > Blocklist** and click **Blocklist List** in the lower-right corner of the **Blocklist** page.

Figure 8-7 Newly created blocklist entry

Blocklist								
Blocklist List								
Manually Blocked IPs: 949567 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
<input type="checkbox"/>	1	9.8.7.6	20 minutes	966 minutes	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	2	10.50.50.1	278 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	3	1.16.65.162	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	4	1.16.65.163	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	5	1.16.65.164	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	6	1.16.65.165	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	7	1.16.65.166	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	8	1.16.65.167	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	9	1.16.65.168	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	10	1.16.65.169	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	11	1.16.65.17	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	12	1.16.65.170	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	13	1.16.65.171	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	14	1.16.65.172	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	15	1.16.65.173	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-
<input type="checkbox"/>	16	1.16.65.174	281 minutes	Permanent	BLOCK_MANUAL	0 (pkts)	0 (bytes)	-

----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 [5.1.2.9 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
Application-Layer Fingerprint Extraction			

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

OK

Cancel

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 **Policy > 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								
<input type="checkbox"/>	Name	Source IP	Netmask	Feature Field	Action	Description	Time of Creation	Operation
<input type="checkbox"/>	test_ads	14.1.1.1	255.255.255.255	DNS Flags:0100	Drop		2021-01-21 14:42:28	 
<div> Delete Add </div>								

----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	--		
<div>Application-Layer Fingerprint Extraction</div>			

Step 2 Click **Application-Layer Fingerprint Extraction**.

Figure 8-12 Extracting HTTP fingerprints

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 **Policy > 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								
<input type="checkbox"/>	Name	Source IP	Netmask	Feature Field	Action	Description	Time of Creation	Operation
<input type="checkbox"/>	test1	::	0	Method:get Host:localhost Request Url:/11 Version:HTTP/1.1	Drop		2020-02-21 14:40:06	 
								<div><div>Delete</div><div>Add</div></div>

----End

Payload Fingerprint Extraction

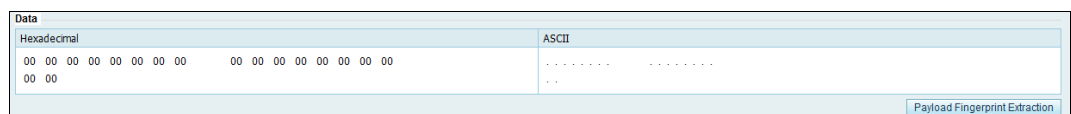
For TCP, UDP, and ICMP packets, you can extract payload fingerprints from the data displayed in the **Data** area by taking consecutive hexadecimal characters to directly create a pattern matching rule. For details about pattern matching rules, see section [8.2 Pattern Matching Rules](#).

To create a pattern matching rule based on fingerprints, perform the following steps:

Step 1 View details about a TCP, UDP, or ICMP packet.

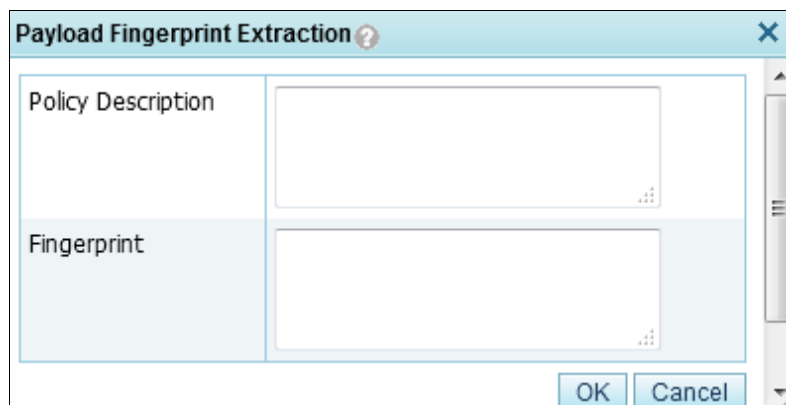
As shown in Figure 8-14, the payload information of the captured TCP, UDP, or ICMP packet is displayed in the **Data** area.

Figure 8-14 Data area



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

Pattern Matching Rules											
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	::	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

PCAP Analysis						
Packet Summary: Name: colcap_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	474554202720485454502f312e31000a486f73743a2034312e38352e34302e	31	0	31	100.00%	Apply
udp	47656386f29204368726f6d652f34372e302e323532362e31303620536166	31	271	302	100.00%	Apply
udp	456e638f84696e673a20677a69702c206465666c5174652c20736463680d0a	31	321	352	100.00%	Apply
udp	4554202720485454502f312e31000a486f73743a2034312e38352e34302e31	31	1	32	100.00%	Apply
udp	43616388652436f6e74726f6c3a206d51782d5167653d300d0a4163636570	31	58	89	100.00%	Apply
udp	4368726f6d652f34372e302e323532362e31303620536166172692f353337	31	278	309	100.00%	Apply
udp	4854444c2c206c696e6520476563686f29204368726f6d652f34372e302e32	31	260	291	100.00%	Apply
udp	496626406f6469666965642d53696e63653a205765642c203231204637420	31	425	456	100.00%	Apply
udp	4c2c206c696e6520476563686f29204368726f6d652f34372e302e32353236	31	263	294	100.00%	Apply
udp	4d4c2c206c696e6520476563686f29204368726f6d652f34372e302e323532	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 **PCAP 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 Capture Rules** area shown in [Figure 8-1](#), select one or more packet capture files (or select the check box in the table header to select all files) and click **Delete**.

Step 2 Click **OK** in the confirmation dialog box.

	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).

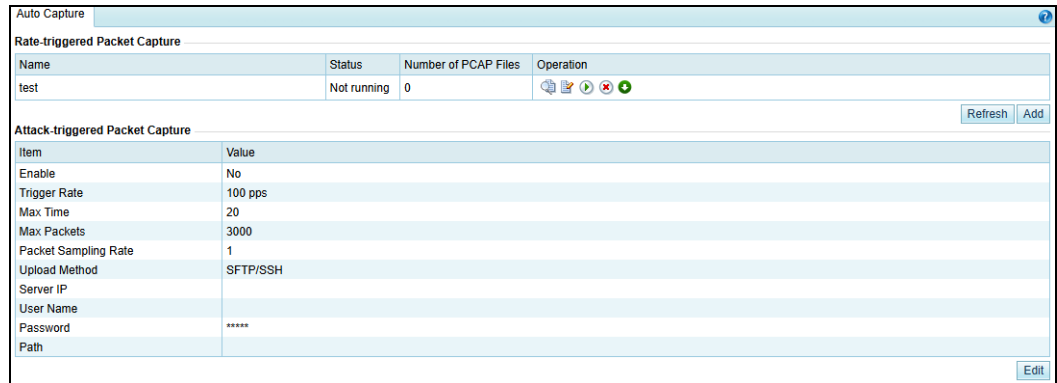
Creating a Rate-triggered Automatic Packet Capture Task

To configure a rate-triggered packet capture task, perform the following steps:

Step 1 Choose **Advanced > Packet Capture > Auto 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 **Not running**.

Figure 8-18 Auto Capture page



The screenshot shows the 'Auto Capture' page. It has two main sections: 'Rate-triggered Packet Capture' and 'Attack-triggered Packet Capture'.

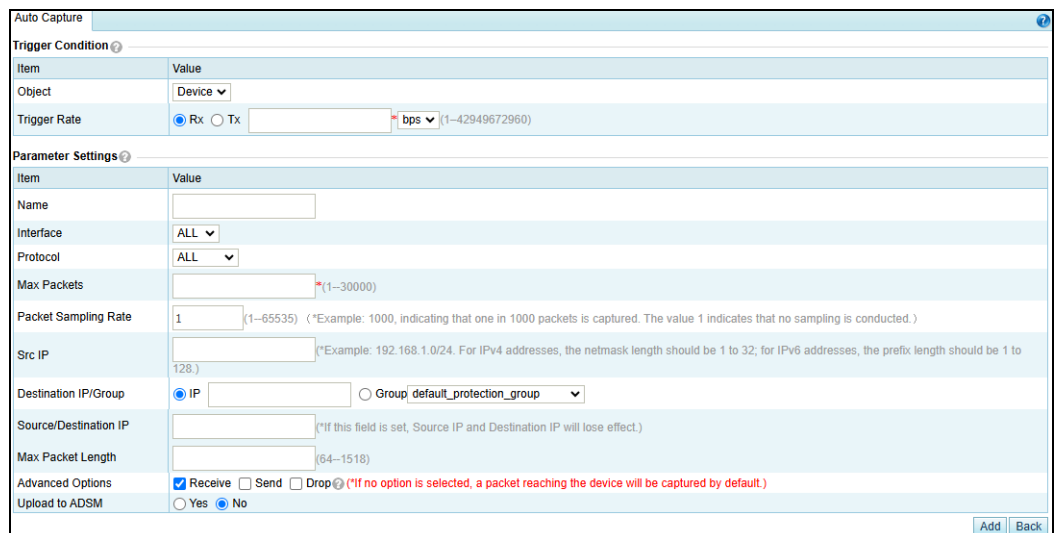
Rate-triggered Packet Capture: A table with columns: Name, Status, Number of PCAP Files, and Operation. It shows one entry named 'test' with status 'Not running' and 0 files. There are icons for refresh, add, delete, and edit.

Attack-triggered Packet Capture: A form with fields: Item, Value, Enable, Trigger Rate, Max Time, Max Packets, Packet Sampling Rate, Upload Method, Server IP, User Name, Password, and Path. The 'Enable' field is set to 'No'. The 'Trigger Rate' is '100 pps'. The 'Max Packets' is '3000'. The 'Packet Sampling Rate' is '1'. The 'Upload Method' is 'SFTP/SSH'. The 'Server IP' is empty. The 'User Name' is empty. The 'Password' is masked with '*****'. The 'Path' is empty. There are 'Refresh' and 'Add' buttons.

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



The screenshot shows the configuration page for an automatic packet capture task. It has two main sections: 'Trigger Condition' and 'Parameter Settings'.





Trigger Condition: A form with fields: Item, Value, Object, Trigger Rate, and Tx. The 'Object' is set to 'Device'. The 'Trigger Rate' is set to 'Rx' and 'bps'. The 'Tx' field is empty.




Parameter Settings: A form with fields: Item, Value, Name, Interface, Protocol, Max Packets, Packet Sampling Rate, Src IP, Destination IP/Group, Source/Destination IP, Max Packet Length, Advanced Options, and Upload to ADSM. The 'Interface' is set to 'ALL'. The 'Protocol' is set to 'ALL'. The 'Max Packets' is set to '30000'. The 'Packet Sampling Rate' is set to '1'. The 'Src IP' is set to '128.'. The 'Destination IP/Group' is set to 'IP'. The 'Source/Destination IP' is empty. The 'Max Packet Length' is set to '1518'. The 'Advanced Options' are set to 'Receive', 'Send', and 'Drop'. The 'Upload to ADSM' is set to 'No'.

Table 8-4 describes 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.
Trigger Rate	Specifies the traffic threshold of the specified object that will trigger automatic packet capture. <ul style="list-style-type: none"> The traffic rate direction can be Rx or Tx.

Parameter	Description
	<ul style="list-style-type: none"> 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	<p>Protocol used by packets to be captured. Values can be ALL, TCP, UDP, and ICMP, ICMPV6, and Custom, with ALL as the default value.</p> <p>When Protocol is set to Custom, you can set a protocol port number, which must be in the range of 0–255.</p>
Max Packets	Number of packets to be captured. The value ranges from 1 to 30000.
Max Time	<p>Specifies how long a capture task can last at most. The value range is 1–3600 in seconds.</p> <p>The system stops capturing packets when either the setting of Max Packets or that of Max Time is met.</p>
Packet Sampling Rate	<p>Specifies the ratio of matched packets to captured packets. Value range: 1–65535.</p> <p>For example, the value 1000 indicates that one in 1000 packets are captured. The default value is 1, indicating no packet sampling.</p> <p>When the traffic bursts, the packet sampling rate allows the device to capture packets in a longer period.</p>
Src IP	<p>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.</p> <p> Note</p> <p>The source IP address can be an IPv4 or IPv6 address.</p>
Destination IP/Group	<p>Destination IP address or group of this task. You can select IP or Group.</p> <ul style="list-style-type: none"> 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	<p>Source or destination IP address of the task. This parameter is optional. If you set this parameter, ignore Src IP and Destination IP/Group.</p> <p> Note</p> <p>Both IPv4 and IPv6 addresses are allowed.</p>
Src Port	<p>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.</p> <p> Note</p> <p>This parameter is available only when Protocol is set to UDP or TCP.</p>
Dst Port	<p>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.</p> <p> Note</p>

Parameter	Description
	This parameter is available only when Protocol is set to UDP or TCP .
Source or Destination Port	Source or destination port of the task. This parameter is optional. If this parameter is specified, the system ignores both Src Port and Dst 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: <ul style="list-style-type: none"> • Receive: indicates that ADS captures received packets. • Send: indicates that ADS captures packets that are sent. • Drop: indicates that ADS captures dropped packets.  Note <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 a Management Platform.


Step 4 Click **OK** to complete the configuration.

The automatic packet capture task starts only when specified conditions are triggered.

----End

Managing Rate-triggered Auto Capture Tasks

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 Auto Capture Files


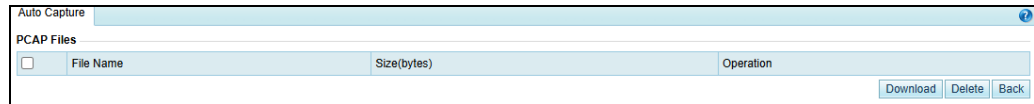
On the page shown in [Figure 8-18](#), click  in the **Operation** column of an automatic packet capture task to open the packet capture file list, as shown in [Figure 8-20](#).

Figure 8-20 Automatic packet capture file list



File Name	Size(bytes)	Operation
		Download Delete Back

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

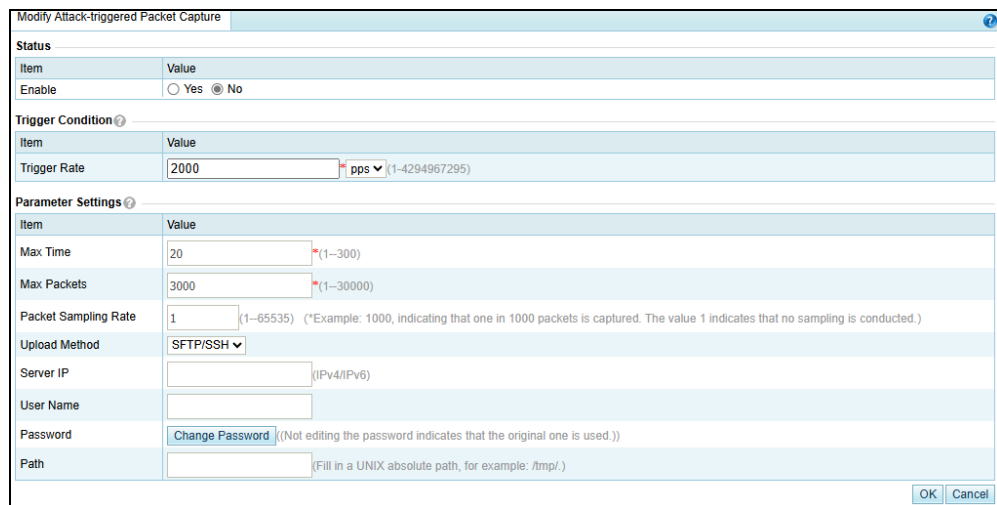
When an attack happens, causing ADS to drop packets at a rate greater than the specified value, automatic packet capture starts.

To configure an attack-triggered packet capture task, perform the following steps:

Step 1 Choose **Advanced > Packet Capture > Auto Capture**.

Step 2 Click **Edit** in the **Attack-triggered Packet Capture** area to edit parameters.

Figure 8-21 Attack-triggered packet capture



Item	Value
Enable	<input type="radio"/> Yes <input checked="" type="radio"/> No
Trigger Rate	2000 pps (1-4294967295)
Max Time	20 (1-300)
Max Packets	3000 (1-30000)
Packet Sampling Rate	1 (1-65535) (*Example: 1000, indicating that one in 1000 packets is captured. The value 1 indicates that no sampling is conducted.)
Upload Method	SFTP/SSH
Server IP	(IPv4/IPv6)
User Name	
Password	Change Password (Not editing the password indicates that the original one is used.)
Path	(Fill in a UNIX absolute path, for example: /tmp/.)

[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

Parameter		Description
		1–4294967295 pps or 1–42949672960 bps.
Max Time		Length of time the packet capture task lasts. The value range is 1–300, in seconds.
Max Packets		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 capture duration reaches the respective threshold, the system stops capturing more packets.
Packet Sampling Rate		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 rate allows the device to capture packets in a longer period.
Upload Method		Specifies how packet capture files are uploaded to the specified server. <ul style="list-style-type: none"> SFTP/SSH: uploads automatic packet capture data to the specified SFTP/SSH server. ADSM: uploads automatic packet capture data to ADS M.
SFTP/SSH	Server IP	Specifies the IPv4 or IPv6 address of the SFTP/SSH server that receives attack-triggered packet capture files from ADS.
	User Name	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 Change 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_attact type_packet sampling rate_capture time.
ADSM	ADSM	IP address of ADS M that receives attack-triggered packet capture files from ADS. At most two servers can be selected. If none is selected, the IP address of the first ADS M configured under System > Local Settings > Management Platform will be used by default.

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 8-22 Pattern Matching Rules page

Pattern Matching Rules												
<input type="checkbox"/>	Dst IP	Dst IP Prefix Length/Netmask	Destination Port	Src IP	Src IP Prefix Length/Netmask	Source Port	Protocol	Access Control	Status	Description	Time of Creation	Operation
<input type="checkbox"/>	2.1.1.0	255.255.255.0		1.1.1.0	255.255.255.0		TCP	Drop	Enable		2024-06-18 16:12:39	  
<input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input type="button" value="Add"/> <input type="button" value="Import"/>												

Step 2 Click **Add**.


Figure 8-23 Creating a pattern matching rule (TCP)

Item	Value	Invert
Dst IP	<input type="text"/>	<input type="checkbox"/>
Dst IP Prefix Length/Netmask	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/>
Dst Port	From <input type="text"/> To <input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Src IP	<input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Src IP Prefix Length/Netmask	<input type="text" value="255.255.255.0"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Src Port	From <input type="text"/> To <input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Protocol	TCP	<input type="radio"/> Yes <input checked="" type="radio"/> No
Access Control	Drop	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No
Interface	From <input type="text"/> To <input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Packet Length	From <input type="text"/> To <input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
IP ID	From <input type="text"/> To <input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
TOS	<input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
TTL/Hop Limit	<input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
UDP Checksum	<input type="text"/> (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.)	<input type="radio"/> Yes <input checked="" type="radio"/> No
ICMP Type	<input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
ICMPv6 Type	<input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
TCP Seq Number	From <input type="text"/> To <input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
TCP ACK Number	From <input type="text"/> To <input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
TCP Option	<input type="text"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Check TCP Flag	<input type="checkbox"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
TCP Flag	<input type="text" value="SYN,ACK,FIN,RST,URG,PSH"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Signature Offset	0 Bytes (0-1400)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Signature Depth	1400 Bytes (0-1400)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Match Case	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No
Signature	<input type="text"/> Ordinary characters	<input type="radio"/> Yes <input checked="" type="radio"/> No

Table 8-6 describes parameters for creating a pattern matching rule.


Table 8-6 Automatic packet capture parameters

Parameter	Description
Dst 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.

Parameter	Description
Dst 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.
Src 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.
Src Port	Source port range. This is required only when Protocol is set to TCP or UDP . For example, 1049–5094 indicates packets with the source port in the range from 1049 to 5094. If only 1049 is filled, it indicates that only packets with the source port 1049 will be deemed to match this rule.
Protocol	Values are TCP , UDP , ICMP , and ICMPv6 .
Access Control	<p>Action performed by ADS on packets matching this rule.</p> <ul style="list-style-type: none"> • Filter indicates that ADS allows packets matching this rule to pass through. • Drop indicates that ADS drops packets matching this rule. • Drop+blocklist indicates that ADS drops packets matching this rule and adds their source IP addresses to the blocklist. • Drop+disconnect indicates that ADS drops packets matching this rule and sends an RST packet to the server to interrupt the connections. • Drop+blocklist+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. • 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. Excessive packets will be dropped. The value range is 1–6000000 pps, with 4000 as the default value. <p> Note</p> <p>If Access Control is set to Drop+blocklist or Drop+blocklist+disconnect, you also need to enable the global blocklist function. Otherwise, the blocklist is invalid. For details, see section 5.2.5 Blocklist.</p>
Enable	Controls whether to enable this rule. The value Yes indicates this rule is enabled.
Interface	Range of the interfaces through which packets are transmitted. The value range is 0–95.
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 Checksum	Checksum of UDP packets. This is available only when Protocol is set to

Parameter	Description
	UDP.
ICMP Type	Type of the ICMP packet header. This is available only when Protocol is set to ICMP .
ICMPv6 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.
TCP Option	Three options are available: Maximum Segment Size , 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	<p>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).</p> <p>You can also leave this field empty. In this case, Offset and Depth are both 0, which cannot be changed.</p> <p>Requirements for typing ordinary characters are as follows:</p> <ul style="list-style-type: none"> • 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. <p>Requirements for typing hexadecimal characters are as follows:</p> <ul style="list-style-type: none"> • 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. <p>You can select Ordinary characters or Hexadecimal characters for</p>

Parameter	Description
	<p>Signature.</p> <p>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.</p> <p>The following shows how to copy signature characters from Wireshark:</p> <p>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.</p>
Description	Brief description of this rule.
Time of Creation	Time when the rule is created, which is automatically generated by the system.

	<p>The Invert column is available for some parameters. Suppose that you specify 202.114.1.242 as the source IP address and 255.255.255.0 as the netmask. If you select Yes for Invert, packets with a source IP address beyond the range 202.114.1.1–202.114.1.254 are deemed to match the configured rule.</p>
---	--

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 8-22](#), click **Import** below the table to create pattern matching rules in batches.

Figure 8-24 Creating pattern matching rules in batches

Pattern Matching Rules

Import

Format: [DIP/Netmask] [SIP/Netmask] [Protocol] [Start DPort:End DPort] [Start SPort:End SPort] [Start interface:End interface] [Start packet length:End packet length] [Access Control type] [Signature Offset:Signature Depth:Invert Match Case] [Signature type] [Signature] [Check TCP Flag] [Description (optional)]

Protocol: TCP/UDP/ICMP/ICMPv6

Access control types:

TCP: filter (protect) drop (drop) black (drop+blocklist) reset (drop+disconnect) blockrst (drop+blocklist+disconnect) limit (rate-limiting)

UDP/ICMP/ICMPv6: filter (protect) drop (drop) black (drop+blocklist) limit (rate-limiting)

Invert: 1 indicates using the logical negation operator to reverse the meaning of the operand. 0 indicates not using the logical negation operator.

Match Case: 1 indicates case insensitivity; 0 indicates case sensitivity.

Signature type: 1 indicates hexadecimal characters and 0 indicates ordinary characters.

Signature: For the signature, you can type either hexadecimal characters like "abab" or "\xab\xab" or ordinary characters. The latter should not contain the following characters: ! \$ " \\.

If no range (such as DPort range, SPort range, interface range, and packet length range) is set, fill in a colon (:).

CHECK indicates checking TCP flags, followed by specific TCP flags such as SYN (or NONE if no flags are checked); NOTCHECK indicates not checking TCP flags.

Each rule should be in a separate line. 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\vb 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

OK

Cancel

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 8-22](#), select one or more pattern matching rules (or select the check box in the table header 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 8-22](#), select one or more pattern matching rules (or select the check box in the table header 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 8-22](#), click  in the **Operation** column to edit parameters of a rule, as shown in [Figure 8-23](#).

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 8-22](#), click  in the **Operation** column and then click **OK** in the confirmation dialog box to delete the rule.
- On the Pattern Matching Rules page shown in [Figure 8-22](#), select one or more pattern matching rules (or select the check box in the table header 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

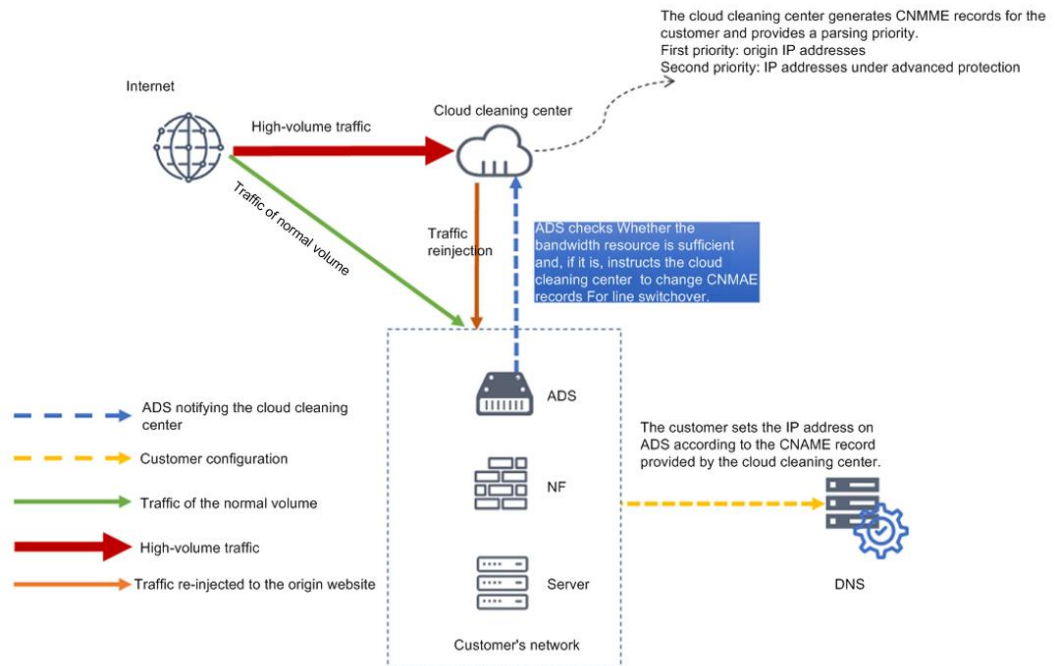
On the **Pattern Matching Rules** page shown in [Figure 8-22](#), click  in the **Operation** column of a pattern matching rule to view its information.

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 8-25](#) 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 8-25 Topology of the cloud signaling scenario



To configure cloud signaling, perform the following steps:

Step 1 Choose **Advanced > Cloud Signaling > Configuration and Status**.

Figure 8-26 Configuration and Status page

Configuration and Status			
Configuration and Status			
Cloud Signaling Status: Off		Cloud connection status: @	
<div>Enable</div>			
Configuration			
Item	Value		
Local Link Bandwidth	10000 Mbps		
To-Cloud Bandwidth Threshold	80%		
Off-Cloud Bandwidth Threshold	40%		
Cloud Signaling IP and CNAME List		Origin IP	Status
CNAME			
<div>Edit</div>			

Step 3 Configure parameters.

a. Click **Edit**.


Figure 8-27 Configuring cloud signaling parameters

Configuration and Status

Modify Cloud Signaling Configuration

Item	Value
Local Link Bandwidth	<input type="text" value="10000"/> Mbps 1–10000000
To-Cloud Bandwidth Threshold	<input type="text" value="80"/> % 1–100
Off-Cloud Bandwidth Threshold	<input type="text" value="40"/> % 1–95


Cloud Signaling IP and CNAME List

CNAME	<input type="text"/>	Origin IP	<input type="text"/>	
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 Threshold	Bandwidth	When the incoming traffic exceeds the to-cloud bandwidth 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.
Off-Cloud Threshold	Bandwidth	When the total traffic falls below the off-cloud bandwidth 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. <div>  <div>Note</div> </div> <p>The from-cloud bandwidth usage threshold must be smaller than or equal to the to-cloud bandwidth usage threshold minus 5.</p>

c. Configure origin IP addresses and CNAME records.


You can click  to add multiple entries.

Figure 8-28 Configuring the cloud signaling IP address and CNAME list

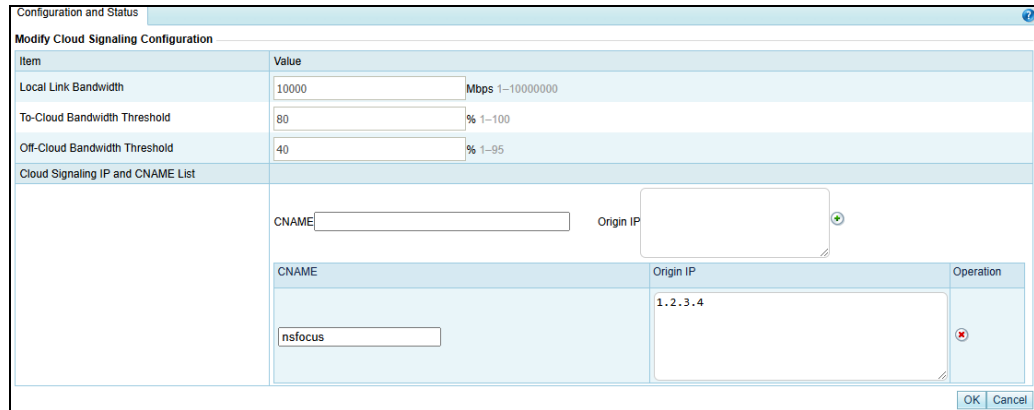


Table 8-8 Parameters for configuring origin IP addresses and CNAME records

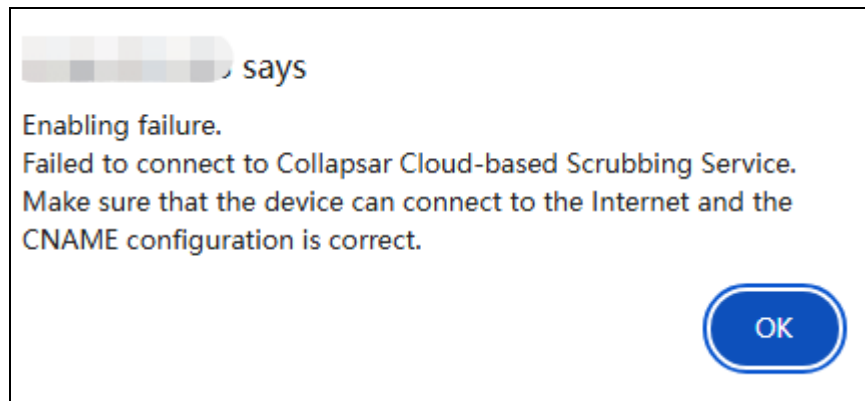
Parameter	Description
CNAME	CNAME is a Canonical Name Record or Alias Record that maps one domain name, for example, M, to another, for example, M'. Therefore, changing the IP address that maps domain name M' also changes the IP address translated for domain name M. Here, you should type the CNAME string 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 4 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 8-28 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 8-29 Message displayed in the case that cloud signaling cannot be enabled




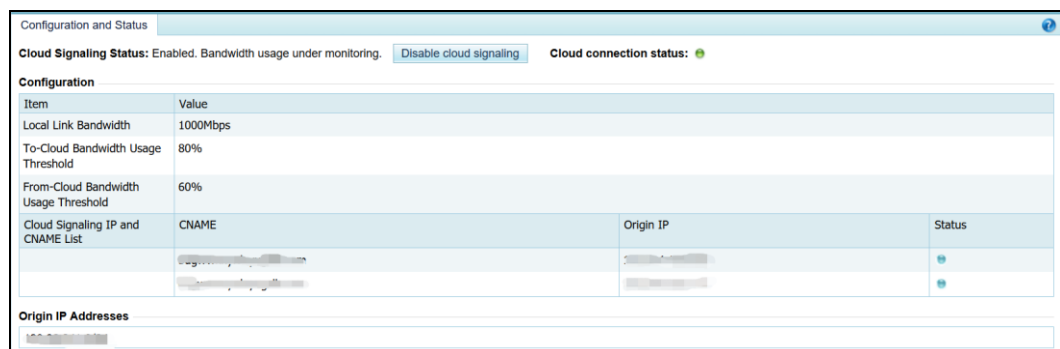
 <p>Note</p>	<ul style="list-style-type: none"> You are advised to add the source IP address to the allowlist on ADS, the firewall, and WAF. After cloud signaling is enabled, no settings can be edited.
---	--




Figure 8-30 Page displayed after cloud signaling is enabled





Step 5 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 8-30.

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	Status is displayed as

Traffic	Status Description
for scrubbing.	 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 TI

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.



To use this function, you need to buy an additional license. For details, contact NSFOCUS technical support.

ADS can collaborate with TI. Specifically, ADS uploads blocked source IP addresses to TI, which sends the latest threat intelligence data to ADS. The TI module allows ADS to filter traffic based on the TI database and users to query IP reputation. In addition, ADS analyzes the effectiveness of TI protection and provides related statistics. 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 TI-based protection algorithms.

8.4.1 TI Configuration

Choose **Advanced > TI > TI Configuration**. On the **TI Configuration** page, click **Edit** to configure the collaboration between ADS and TI.

Table 8-10 TI configuration parameters

Parameter	Description
Enable	Controls whether to enable collaboration with TI. Selecting No will disable all related functions. After this function is enabled, ADS immediately downloads data from TI 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.

Parameter	Description
Share Threat Intelligence	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 TI.
Cloud Intelligence Server	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 TI.
Synchronization Status	<ul style="list-style-type: none"> Last Synchronization Record: provides information about the last synchronization from TI. This information is automatically updated on a daily basis. Last Share Record: provides information about the last upload of data to TI. This information is automatically updated on an hourly basis.
Test Connectivity	Tests whether ADS is properly connected to TI. After you click this button, if Connected is displayed, ADS can properly communicate with TI; if another word is displayed, you must check the network status to ensure the proper communication between ADS and TI.

8.4.2 TI 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 TI Application Effect

Choose **Advanced > TI > TI Application Effect and Query > TI Application Effect**. The **TI 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 TI from ADS.

Choose **Advanced > TI > TI Application Effect and Query > TI Query** 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 Mode	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 TI database.
- Click **Cloud details** in the **Search** column to further view detailed intelligence information of the IP address in the cloud-side TI database.



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 TI Database Upgrade

The TI database can be upgraded automatically or manually.

8.4.3.1 Automatic Synchronization

Choose **Advanced > TI > TI Database Upgrade**. In the **Auto Sync** area of the **TI Database 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 TI database to the latest version at the specified upgrade time.

Clicking **Upgrade Now** immediately triggers upgrade of the TI database.

8.4.3.2 Local Upgrade

The TI database can be upgraded offline.

In the **Local Upgrade** area of the **TI Database 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**.

	The intelligence package is available at https://update.nsfocusglobal.com/ .
---	--

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 > TI > IP Exceptions**. Click **Edit** in the **IP Exceptions** 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.

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**.

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 9-1 Viewing the trust information of a source IP address

The screenshot shows a web interface titled 'Trusted IP'. At the top, there is a search bar labeled 'Src IP' containing the text '10.66.242.1'. To the right of the search bar are three buttons: 'Search', 'Clear Trust', and 'Clear Trust for All'. Below the search bar is a table with two columns: 'Item' and 'Value'. The table is currently empty, and a message 'No data.' with a warning icon is displayed below the table.

- Click **Clear Trust** to clear the information about specific trusted IP addresses.
- Click **Clear Trust for All** to clear the information about all 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 9-2 Protection Status page

Step 2 Configure query parameters.

Table 9-1 Parameters for querying the protection status of a destination IP address

Parameter	Description
Dst IP	Destination IP address to be queried. You can type an IPv4 or IPv6 address according to the actual network deployment scenario.
Policy	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 .
Dst Port	Destination port. This is required only when Policy 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.

----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

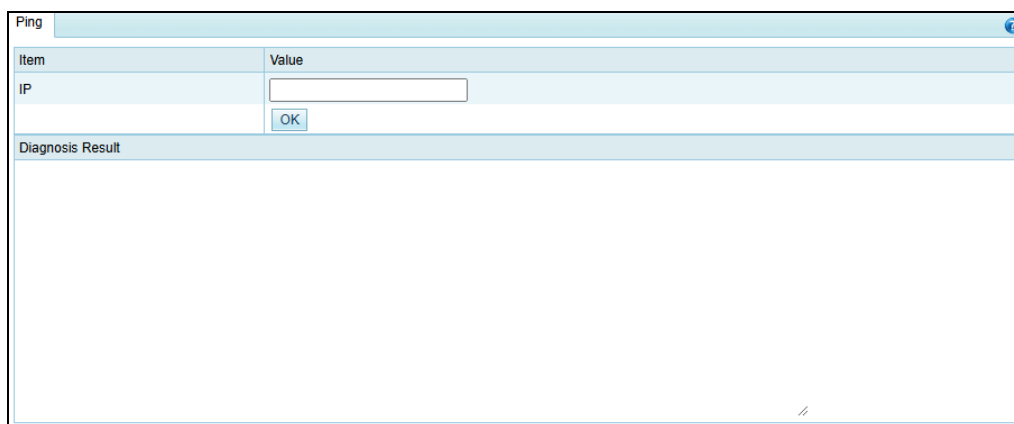
Ping is used to check whether a host is alive or connects to the network.

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 9-3](#).

Figure 9-3 Network diagnosis – ping



The screenshot shows a window titled "Ping". It contains a table with two columns: "Item" and "Value". The "Item" column has a row for "IP" with an empty text input field next to it. Below the input field is an "OK" button. Below the table is a section titled "Diagnosis Result" with a large empty text area for displaying the results.

Step 2 Type an IP address and click **OK**.

The ping result will then be displayed in the text box below.

----End

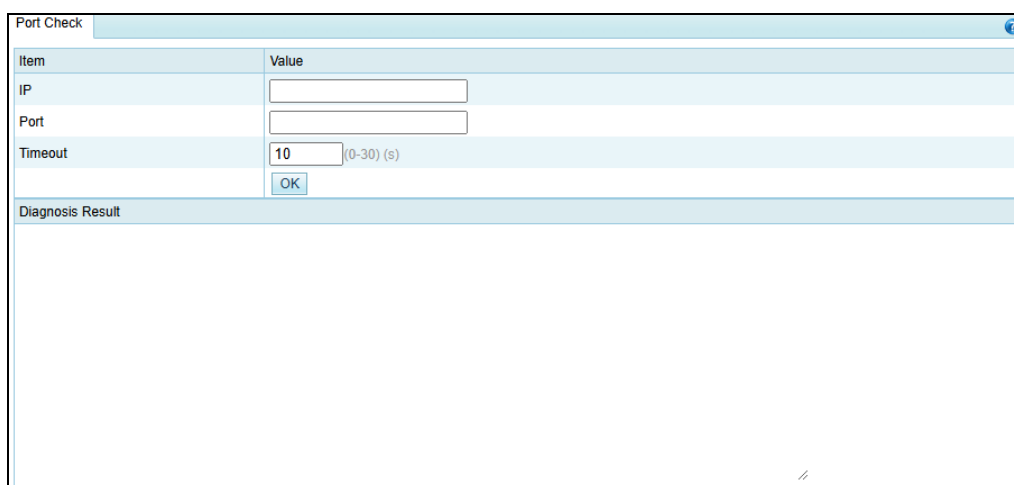
9.2.2 Port Check

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 3 Choose **O&M > Network Diagnosis > Port Check**.

Figure 9-4 Network diagnosis – port check



The screenshot shows a window titled "Port Check". It contains a table with two columns: "Item" and "Value". The "Item" column has rows for "IP", "Port", and "Timeout". The "Value" column has corresponding text input fields. The "Timeout" field has a value of "10" and a unit "(0-30) (s)". Below the input fields is an "OK" button. Below the table is a section titled "Diagnosis Result" with a large empty text area for displaying the results.

Step 4 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 5 Click **OK**.

The port check result will then be displayed in the text box below.

----End

9.2.3 Tcpdump

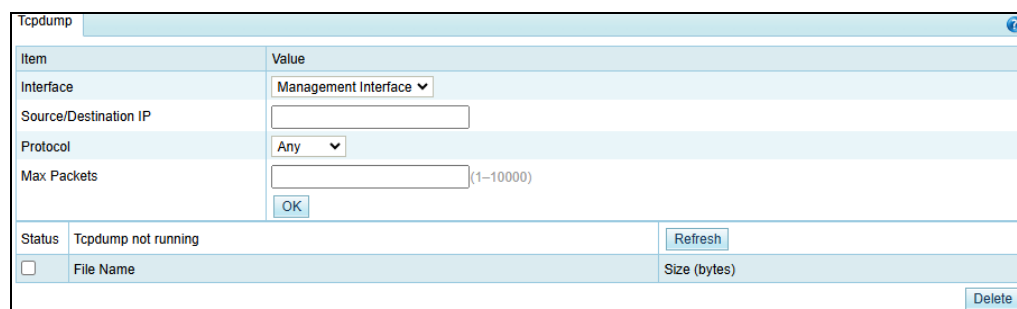
Tcpdump is used to intercept and analyze packets being transmitted or received over a network as defined by a user. The user can check the status of and troubleshoot network interface cards (NICs) based on such analysis.

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 9-5 Network diagnosis – tcpdump



Step 2 Configure tcpdump parameters.

Table 9-3 Tcpdump parameters

Parameter	Description
Interface	Specifies a working interface or the management interface for capturing packets.
Source/Destination IP	Specifies the source or destination IP address of packets to be captured. No value indicates all IP addresses.
Protocol	Specifies a protocol so that packets transmitted by using this protocol will be captured. You can select Any , TCP , UDP , ICMP , or ICMPv6 .
Max Packets	Specifies the maximum number of packets to be captured. The value ranges from

Parameter	Description
	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 9-5](#).

----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 about 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 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 about 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
 17. Logout
=====
Your password is the initial password.
Please choose "Console Password Change" to customize a new one.
Input your selection:
```

10.2.1 Configuring IPv4 Network Settings

On the main menu, type **1** and press **Enter** to open the IPv4 address configuration 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:█
```



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:█
```



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 10-8](#).

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 access 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



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
17. Logout
=====
Your password is the initial password.
Please choose "Console Password Change" to customize a new one.
Input your selection:9
This operation will rollback system to last available 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

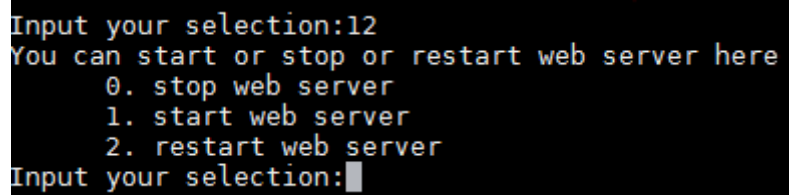
```
The management interface ACL function has been enabled.
The default ACL action is permit
Management interface ACL list:
Do you want to disable management interface ACL function?[yes/no]
```

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



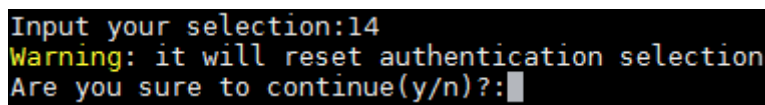
In the window shown in [Figure 10-18](#), you can perform the following operations:

- 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



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.



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.

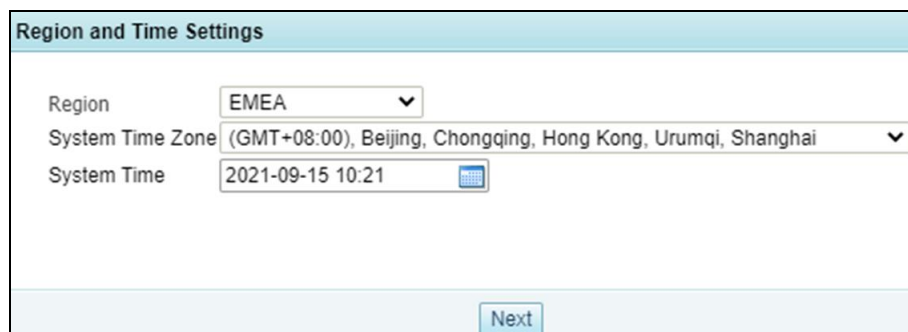
Figure 11-1 Login page

The login page for the ADS Anti-DDoS System. It features a light blue background with a subtle wave pattern. At the top, the text "ADS ANTI-DDoS SYSTEM" is displayed. Below this, there is a login form with a username field containing "admin", a password field with masked characters, and a "Login" button. A language selection dropdown menu labeled "选择语言 (Select Language)" is positioned below the username field.

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

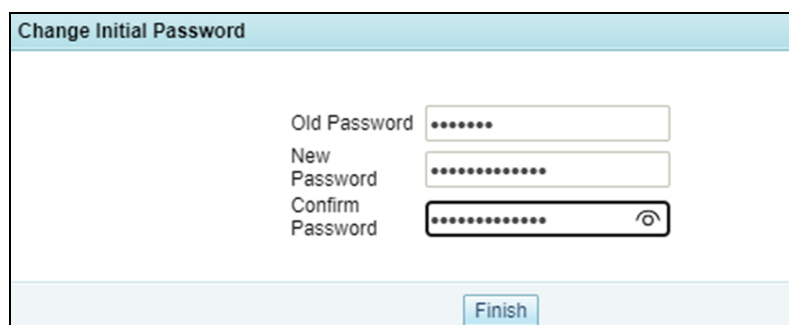
The "Region and Time Settings" page. It has a light blue header with the title "Region and Time Settings". Below the header, there are three settings: "Region" set to "EMEA", "System Time Zone" set to "(GMT+08:00), Beijing, Chongqing, Hong Kong, Urumqi, Shanghai", and "System Time" set to "2021-09-15 10:21". A "Next" button is located at the bottom right of the page.

Step 6 Click **Next**.

The page for changing the initial password appears.

The new password must be a string of no less than eight characters and contain at least two of the following character types: English letters, digits, and special characters.

Figure 11-3 Changing the initial password

The "Change Initial Password" page. It has a light blue header with the title "Change Initial Password". Below the header, there are three password fields: "Old Password", "New Password", and "Confirm Password". The "New Password" and "Confirm Password" fields have a strength indicator icon on the right. A "Finish" button is located at the bottom right of the page.

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 Logout. 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.

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**.

Figure 11-4 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 /
	T1 /
Holder	/
Serial No.	/

License Update Choose File No file chosen Submit Preview Export

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 11-5](#).

Figure 11-5 Importing the license successfully

License				
Type	Trial			
Basic Service Start Date	2024-10-24			
Basic Service End Date	2025-01-22			
Processing Capacity (pps)	59,520,000			
Processing Capacity (Gbps)	80.00			
Authorized Modules	Module Name	Status	Start Date	End Date
	IPv6	Supported	2024-10-24	2025-01-22
	TI	Supported	2024-10-24	2025-01-22
Holder	1			
Serial No.	6EF4-3913-C59F-5B59			

----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** in 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	<p>Warning:</p> <p>1. After the upgrade completes, a system restart is required to make the changes take effect. The system restart may cause service interruption. Therefore, before upgrading the system, disable the device from receiving service traffic.</p> <p>2. If configuration changes are made, save them before the upgrade. Otherwise, they will be lost after the upgrade.</p> <p>Update path:</p> <p>Go to https://update.nsfocus.com/update/upLic and download the latest update for installation. You can do so only after uploading the license of the current device. Alternatively, you can contact the vendor for help.</p> <p><input type="button" value="Choose File"/> No file chosen</p> <p><input type="button" value="Upgrade"/></p>

Upgrade History

First ◀ Previous Next ▶ Last 1 / 2 Go to 1 ➡

ID	Time	Source Version	Source Version Build Date	Target Version	Target Version Build Date	Operation	Release Notes
1	2024-10-11 17:41:06	V4.5R90F05.sp02	20240627	V4.5R90F06	20241011	Normal upgrade.	View
2	2024-10-11 17:31:26	V4.5R90F06	20241011	V4.5R90F05.sp02	20240627	Version Rollback	
3	2024-10-11 17:06:45	V4.5R90F05.sp02	20240627	V4.5R90F06	20241011	Normal upgrade.	
4	2024-06-28 09:49:01	V4.5R90F05.sp01	20240408	V4.5R90F05.sp02	20240627	Normal upgrade.	
5	2024-06-28 09:44:50	V4.5R90F05.sp02	20240627	V4.5R90F05.sp01	20240408	Version Rollback	
6	2024-06-27 16:12:25	V4.5R90F05.sp01	20240408	V4.5R90F05.sp02	20240627	Normal upgrade.	
7	2024-06-27 15:31:37	V4.5R90F05.sp02	20240625	V4.5R90F05.sp01	20240408	Version Rollback	
8	2024-06-25 17:58:43	V4.5R90F05.sp01	20240408	V4.5R90F05.sp02	20240625	Normal upgrade.	
9	2024-06-19 16:48:08	V4.5R90F05.sp02	20240618	V4.5R90F05.sp01	20240408	Version Rollback	
10	2024-06-19 10:26:47	V4.5R90F05.sp01	20240408	V4.5R90F05.sp02	20240618	Normal upgrade.	

Step 2 Click **Choose File**, select an upgrade package, and then click **Upgrade**.



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 > System 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

The web-based manager cannot be accessed after the device 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 the attack traffic has not reached its processing capacity.

Troubleshooting

- Check whether the device that is directly connected with ADS has a hub. 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 any access control rule restricts access from the IP address in question.

12.2.3 License Import Failure

Symptom

The import of a license file failed.

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 a license file 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 ADS connects to a router, neither can learn the MAC address of the other device.

Troubleshooting

Check the following:

- Check whether IP addresses of the two devices are in the same network segment, whether the IP configuration is correct, and whether the connected interface is 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 the optical module resolved 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 Packet Drop

Symptom

Two devices cannot not ping each other or too many packets are dropped on a network where ADS is installed.

Troubleshooting

Check the following step by step:

- 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 software operates properly.
- Remove the device and detect packet loss on uplink and downlink devices to determine whether the hardware 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	√	√
	DNS protection algorithms 5 and 6	√	√
	TCP control parameters	√	√
	TCP control parameters – TCP fragment control	√	√
	Botnet & 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	√	√

Module	Function	IPv4	IPv6
	UDP protection – traffic control by Dst IP + Dst port	√	√
	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	√	×
	Programmable rules	√	√
	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	√	√
	Carpet bombing protection rule	√	√
	Connection exhaustion rules	√	√
	URL-ACL protection rules	√	√
	Blocklist	√	√
	Allowlist	√	√
	HTTP keyword checking	√	√
	DNS keyword checking	√	√
	SSL/TLS keyword checking	√	√
	DNS subdomain allowlist	√	√
Diversion & Injection	Running mode	√	√
	Port channel configuration	√	√
	IP address configuration	√	√
	Working interface access control (web and SSH)	√	√

Module	Function	IPv4	IPv6
	BGP diversion	√	√
	OSPF diversion	√	√
	ISIS	√	√
	RIP	√	√
	LDP	√	×
	IP route assignment	√	√
	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 Kuangang 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	√	√

Module	Function	IPv4	IPv6
	HA synchronization logs	√	√
	Syslog diversion logs	√	√
System	Basic settings	√	√
	Interface link configuration	—	—
	System user management	√	√
	Management mode configuration	√	√
	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	√	√
TI	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 Primary 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 Primary 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 Licensee'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.