NSFOCUS ADS
User Guide

Version: V4.5R89F00 (2016-03-05)

© 2016 NSFOCUS

■ Copyright © 2016 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.**

Contents

Preface **1**
Scope 1
Audience 1
Organization 2
Conventions 2
Customer Support 3
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 User 10
2.3 Web Page Layout 11
2.4 System Modules 12
2.5 Common Icons and Buttons 13
3 Real-Time Monitoring **14**
3.1 System Status 14
3.2 Service Status 17
3.3 System Information 17
4 Policies **18**
4.1 Anti-DDoS Policies 18
4.1.1 Default Anti-DDoS Parameters 18
4.1.2 Protection Groups 33
4.1.3 Advanced Global Parameters 41
4.1.4 Response Page Settings 42
4.1.5 Policy Auto-Learning 44
4.2 Access Control Policies 46
4.2.1 Access Control Rules 47
4.2.2 GeoIP Rules 52
4.2.3 Regular Expression Rules 54

4.2.4 DNS Keyword Checking 56
4.2.5 HTTP Keyword Checking 58
4.2.6 Connection Exhaustion Rules 60
4.2.7 URL-ACL Protection Rules 62
4.2.8 Blacklist 64
4.2.9 Whitelist 71

5 Diversion and Injection 77

5.1 General Settings 77
5.1.1 Running Mode 78
5.1.2 Port Channel Configuration 79
5.1.3 GRE Tunnel Configuration 81
5.1.4 IP Address Configuration 82
5.2 Diversion Route 85
5.2.1 BGP Route 85
5.2.2 IP Route Assignment 88
5.3 Traffic Injection 89
5.3.1 Injection Interfaces 90
5.3.2 Injection Routes 92
5.3.3 MAC Address Table 101
5.4 Traffic Diversion 104
5.4.1 Filtering Rules 104
5.4.2 Manual Diversion 106
5.4.3 Group Diversion 111
5.4.4 Diversion Routing Table 112
5.5 Advanced Route Setting 113
5.5.1 MPLS Route 114
5.5.2 Other Routes 116
5.6 Syslog Diversion Configuration 119
5.6.1 Diversion Configuration 119
5.6.2 Diversion Rule List 121

6 Logs 122

6.1 Attack Logs 122
6.1.1 Attack Details 122
6.1.2 Statistical Graph 123
6.2 System Logs 124
6.2.1 System Operation Logs 125
6.2.2 System Login Logs 125
6.2.3 Link Status Logs 126
6.2.4 Traffic Diversion Logs 127
6.2.5 HA Synchronization Logs 128
6.2.6 Syslog Diversion Logs 129

6.3 Log Analysis 130

7 System Administration 133

7.1 Local Settings 133

7.1.1 Basic Information 133

7.1.2 Interface Configuration 136

7.1.3 User Management 138

7.1.4 Management Mode Configuration 141

7.1.5 Configuration File Import and Export 142

7.1.6 HA Configuration 143

7.1.7 (Optional) Bypass Configuration 154

7.1.8 Collaboration Configuration 157

7.1.9 Bandwidth Overrun Limit Configuration 165

7.2 Security Configuration 166

7.2.1 Login Security Settings 167

7.2.2 Locked User Management 168

7.2.3 Authentication Configuration 168

7.3 Log Services 170

7.3.1 Syslog Settings 170

7.3.2 SNMP Settings 172

7.3.3 Email Settings 173

7.3.4 SFTP/SSH Settings 174

7.4 Others 175

7.4.1 License 175

7.4.2 System Upgrade 177

7.4.3 Remote Assistance 178

7.4.4 SSL Certificate Import 178

7.4.5 One-Click Info Collection 179

7.4.6 Version Information 180

7.4.7 Web API File Download 180

8 Advanced Applications 182

8.1 Packet Capture Management 182

8.1.1 Configuring a Maunal Packet Capture Task 182

8.1.2 Configuring an Automatic Packet Capture Task 184

8.1.3 Managing the Status of Packet Capture Tasks 186

8.1.4 Managing Manual Packet Capture Files 186

8.1.5 Managing Automatic Packet Capture Files 188

8.2 Pattern Matching Rules 189

8.2.1 Adding a Pattern Matching Rule 189

8.2.2 Adding Pattern Matching Rules in Batches 194

8.2.3 Enabling and Disabling Pattern Matching Rules 195

8.2.4 Modifying Pattern Matching Rules 195

8.2.5 Deleting Pattern Matching Rules 195
8.2.6 Viewing Pattern Matching Rules 196
8.3 IP Reputation 196
9 Console-based Management 198
9.1 Login to the Console 198
9.2 Details 201
9.2.1 Configuring IPv4 Network Settings 202
9.2.2 Configuring IPv6 Network Settings 202
9.2.3 Configuring DNS Settings 203
9.2.4 Changing the Console Password 203
9.2.5 Setting System Time 204
9.2.6 Restoring Default Settings 204
9.2.7 Restoring Initial Password of Web Administrator 204
9.2.8 Setting the Console Timeout Value 205
9.2.9 Rolling Back the Version 205
9.2.10 Exiting the Console 206
A Abbreviations 207
B Default Parameters 205
B.1 Default Console Parameters 205
B.2 Default Web Administrator Account 205
B.3 Default Console Administrator Account 205
B.4 Default CLI Administrator Account 205
B.5 Console Specification 205
C IPv4/IPv6 Support 206

Figures

Figure 1-1 In-path deployment of an ADS device 6
Figure 1-2 Out-of-path deployment of an ADS device 6
Figure 2-1 Alert page 8
Figure 2-2 Login page of the ADS device 8
Figure 2-3 Window displayed after successful login 9
Figure 2-4 Web page layout 11
Figure 3-1 Traffic curves 15
Figure 3-2 Interface status of ADS NX5-4020 15
Figure 3-3 System resource 16
Figure 3-4 Attack events in the last 15 minutes 16
Figure 3-5 Latest attack events 17
Figure 3-6 Service status 17
Figure 3-7 System information 17
Figure 4-1 Default Anti-DDoS Settings page 19
Figure 4-2 DDoS Protection Policy area 19
Figure 4-3 HTTP Keyword Checking Policy area 22
Figure 4-4 Editing the default HTTP keyword checking policy 22
Figure 4-5 Configuring HTTP keyword checking rules 23
Figure 4-6 HTTP Protection Policy area 23
Figure 4-7 HTTPS Protection Policy area 24
Figure 4-8 DNS Keyword Checking Policy area 25
Figure 4-9 Editing the default DNS keyword checking policy 26
Figure 4-10 Configuring DNS keyword checking rules 26
Figure 4-11 DNS Protection Policy area 27
Figure 4-12 TCP Control Policy area 27
Figure 4-13 IP Behavior Control Policy area 29
Figure 4-14 SIP Protection Policy area 30

Figure 4-15 UDP Payload Check Policy area 31
Figure 4-16 UDP Protection Policy area 31
Figure 4-17 ICMP Protection Policy area 32
Figure 4-18 Protection groups 33
Figure 4-19 Basic information about a protection group 34
Figure 4-20 IP List page 34
Figure 4-21 Adding an IP segment 35
Figure 4-22 Configuring policies 36
Figure 4-23 List of URL rules 38
Figure 4-24 Configuring a URL rule 38
Figure 4-25 Viewing details of a protection group 40
Figure 4-26 Advanced Global Parameters page 41
Figure 4-27 Response Page Settings tab page 42
Figure 4-28 Response Page Settings page 43
Figure 4-29 Response page preview 44
Figure 4-30 Policy Auto-Learning page 45
Figure 4-31 Starting learning 45
Figure 4-32 Auto-learning record 45
Figure 4-33 Viewing automatically generated protection groups 46
Figure 4-34 List of access control rules 47
Figure 4-35 Creating an access control rule 48
Figure 4-36 Creating access control rules in batches 49
Figure 4-37 Enabling access control rules 50
Figure 4-38 Disabling access control rules 51
Figure 4-39 List of GeoIP rules 52
Figure 4-40 Creating a GeoIP rule 52
Figure 4-41 Viewing the GeoIP library 53
Figure 4-42 List of regular expression rules 55
Figure 4-43 Creating a regular expression rule 55
Figure 4-44 List of DNS keyword checking rules 56
Figure 4-45 Creating a DNS keyword checking rule 57
Figure 4-46 List of HTTP keyword checking rules 58
Figure 4-47 Creating an HTTP keyword checking rule 59

Figure 4-48 List of connection exhaustion rules 60
Figure 4-49 Creating a connection exhaustion rule 61
Figure 4-50 List of URL-ACL rules 63
Figure 4-51 Adding a URL-ACL rule 63
Figure 4-52 Blacklist status 66
Figure 4-53 Enabling the blacklist policy 66
Figure 4-54 Blacklist function enabled 67
Figure 4-55 Adding a blacklist entry 67
Figure 4-56 Viewing blacklist entries 68
Figure 4-57 Searching for an IP address 68
Figure 4-58 Blacklist search result 69
Figure 4-59 Importing a blacklist file 69
Figure 4-60 Import success prompt 69
Figure 4-61 Viewing import results 70
Figure 4-62 Exporting a blacklist file 70
Figure 4-63 Whitelist configuration page 71
Figure 4-64 Importing the whitelist file 72
Figure 4-65 Import progress message 73
Figure 4-66 Viewing the import result 73
Figure 4-67 Querying the trust relationship 74
Figure 4-68 Query result of the trust relationship 74
Figure 4-69 Clearing trust relationships 75
Figure 4-70 Clearing the configuration 75
Figure 5-1 Running mode of the ADS device (diversion mode) 78
Figure 5-2 Editing the running mode of the ADS device (diversion mode) 78
Figure 5-3 Port channel configuration 80
Figure 5-4 Adding a port channel for the ADS device 80
Figure 5-5 GRE tunnel configuration 81
Figure 5-6 Creating a GRE tunnel 82
Figure 5-7 IP address list in diversion mode 83
Figure 5-8 Adding an IP address 83
Figure 5-9 Adding a loopback address 84
Figure 5-10 Local route parameters 85

Figure 5-11 Creating a BGP route 86
Figure 5-12 Adding a BGP neighbor 87
Figure 5-13 IP route assignment 88
Figure 5-14 Creating an IP route 89
Figure 5-15 Injection interface list 90
Figure 5-16 Adding an injection interface 91
Figure 5-17 Injection routes 93
Figure 5-18 Creating an injection route 93
Figure 5-19 Creating injection routes in batches 96
Figure 5-20 Viewing injection routes and learned labels 97
Figure 5-21 Editing advanced configurations. 99
Figure 5-22 MAC address table 101
Figure 5-23 Adding the mapping between an IP address and an MAC address 102
Figure 5-24 Querying the MAC address mapping an IP address 103
Figure 5-25 Query result 103
Figure 5-26 Configuring invalid MAC addresses 103
Figure 5-27 Filtering rules 104
Figure 5-28 Creating a diversion filtering rule 105
Figure 5-29 Traffic diversion rules 106
Figure 5-30 Creating a traffic diversion rule 107
Figure 5-31 Creating traffic diversion rules in batches 108
Figure 5-32 Deleting a specified diversion rule 110
Figure 5-33 Group diversion rules 111
Figure 5-34 Creating a group diversion rule 111
Figure 5-35 Diversion routing table 112
Figure 5-36 Search for diversion routes 113
Figure 5-37 List of MPLS routes 114
Figure 5-38 Creating an MPLS route 114
Figure 5-39 Adding a neighbor for MPLS route 115
Figure 5-40 List of other routes 116
Figure 5-41 Editing LDP route parameters 117
Figure 5-42 ADS login in SSH mode 118
Figure 5-43 Editing OSPF route parameters 118

Figure 5-44 Syslog-based diversion rule list 119
Figure 5-45 Creating a diversion rule 120
Figure 5-46 Syslog Diversion list 121
Figure 6-1 Attack logs 122
Figure 6-2 Attack proportion 124
Figure 6-3 Number of attacks of each type 124
Figure 6-4 System operation logs 125
Figure 6-5 System login logs 126
Figure 6-6 Link status logs 127
Figure 6-7 Traffic diversion logs 128
Figure 6-8 HA synchronization logs 129
Figure 6-9 Syslog diversion logs 130
Figure 6-10 Attack traffic statistics 130
Figure 6-11 24-hour traffic (kpps) 130
Figure 6-12 24-hour traffic (Mbps) 131
Figure 6-13 24-hour attack type statistics 131
Figure 6-14 24-hour attacked IP statistics 131
Figure 7-1 Basic Settings page 134
Figure 7-2 System check results 135
Figure 7-3 Modify basic settings page 136
Figure 7-4 Interface working mode of ADS NX5-4020 137
Figure 7-5 Changing the working mode of 1000M electrical ports 138
Figure 7-6 System users 139
Figure 7-7 Adding a system user 139
Figure 7-8 Configuring the password of a CLI user 140
Figure 7-9 Editing CLI user 140
Figure 7-10 Add Mgmt Mode Config page 141
Figure 7-11 Import/Export page 142
Figure 7-12 HA topology 144
Figure 7-13 HA Configuration page 145
Figure 7-14 Edit Basic Settings area 145
Figure 7-15 Advanced Configurations area 146
Figure 7-16 Edit Advanced Configurations area 147

Figure 7-17 Policy configurations to be synchronized 148
Figure 7-18 Diversion and injection configurations to be synchronized 149
Figure 7-19 System configurations to be synchronized 150
Figure 7-20 Advanced configurations to be synchronized 150
Figure 7-21 HA Configuration tab page on a master device 151
Figure 7-22 HA Configuration tab page on a slave device 152
Figure 7-23 Status viewing result on a master device 153
Figure 7-24 Status viewing result on a slave device 153
Figure 7-25 Bypass Configuration page 154
Figure 7-26 Topology for the interaction between ADS and the bypass switch 155
Figure 7-27 Adding an external bypass group 156
Figure 7-28 Collaboration Configuration page 157
Figure 7-29 Configuring an upper-level ADS 158
Figure 1-1 Collaboration Configuration page 159
Figure 7-30 List of IP addresses of lower-level devices 159
Figure 7-31 Adding a lower-level ADS 159
Figure 7-32 Viewing diverted traffic 160
Figure 7-33 Configuring a lower-level ADS 160
Figure 7-34 Lower-level ADS configuration 163
Figure 7-35 Status of diverted traffic 164
Figure 7-36 Configuring manually notified IP addresses 164
Figure 7-37 Notification filtering rule page 165
Figure 7-38 Adding a notification filtering rule 165
Figure 7-39 Bandwidth Overrun Limit page 166
Figure 7-40 Editing bandwidth overrun thresholds 166
Figure 7-41 Configuring login security parameters 167
Figure 7-42 Locked User Management page 168
Figure 7-43 Authentication Configuration page 169
Figure 7-44 Configuring the authentication configuration. 169
Figure 7-45 Configuring syslog 170
Figure 7-46 Configuring a syslog server 171
Figure 7-47 SNMP Trap Setting page 172
Figure 7-48 Log sending by email 173

Figure 7-49 Exporting logs via SFTP or SSH 174
Figure 7-50 Modifying the SFTP SSH service settings 175
Figure 7-51 License information of ADS 176
Figure 7-52 System Upgrade page 177
Figure 7-53 Remote assistance 178
Figure 7-54 SSL Certificate Import page 179
Figure 7-55 One-Click Info Collection page 179
Figure 7-56 One-click information collection result 180
Figure 7-57 Version information 180
Figure 7-58 Web API File Download page 181
Figure 8-1 Manual packet capture 183
Figure 8-2 Automatic packet capture 184
Figure 8-3 Automatic Packet Capture page 185
Figure 8-4 List of packet capture files 186
Figure 8-5 Viewing a packet capture file 187
Figure 8-6 Details of a packet capture file 187
Figure 8-7 List of packet capture files 188
Figure 8-8 Pattern Matching Rules page 190
Figure 8-9 Adding a pattern matching rule (TCP) 191
Figure 8-10 Adding pattern matching rules in batches 194
Figure 8-11 Cloud IP Reputation page 196
Figure 8-12 IP Reputation Query area 197
Figure 9-1 Location Information dialog box 199
Figure 9-2 Connection Description dialog box 199
Figure 9-3 Port connected to HyperTerminal 200
Figure 9-4 Configuring port attributes 201
Figure 9-5 Login to the console 201
Figure 9-6 Main menu of the console 202
Figure 9-7 IPv4 network settings 202
Figure 9-8 IPv6 network settings 203
Figure 9-9 Configuring the DNS server 203
Figure 9-10 Changing the console password 203
Figure 9-11 Setting system time 204

Figure 9-12 Restoring the initial password of the web administrator 204
Figure 9-13 Setting the console timeout value 205
Figure 9-14 Setting the timeout value 205
Figure 9-15 Rolling back the version 206

Tables

Table 2-1 User permissions 10
Table 2-2 Web page layout 11
Table 2-3 Common buttons 12
Table 2-4 System functions 12
Table 2-5 Buttons and icons 13
Table 4-1 Parameters of the default anti-DDoS policy 19
Table 4-2 Parameters of the default HTTP keyword checking policy 22
Table 4-3 Parameters of the HTTPS protection policy 25
Table 4-4 Parameters of the default DNS keyword checking policy 25
Table 4-5 Parameters of the default DNS protection policy 27
Table 4-6 Parameters of the TCP control policy 27
Table 4-7 IP behavior control parameters 29
Table 4-8 Parameters of the default SIP protection policy 30
Table 4-9 UDP payload inspection parameters 31
Table 4-10 Parameters of the default UDP protection policy 31
Table 4-11 Parameters of the ICMP protection policy 33
Table 4-12 Parameters for creating a protection group 34
Table 4-13 Parameters of an IP segment 35
Table 4-14 Parameters of a URL rule 38
Table 4-15 Advanced global parameters 41
Table 4-16 Parameters for creating a response page 43
Table 4-17 Parameters for creating an access control rule 48
Table 4-18 Parameters for creating a GeoIP rule 53
Table 4-19 Parameters for creating a regular expression rule 55
Table 4-20 Parameters for creating a DNS keyword checking rule 57
Table 4-21 Parameters for creating an HTTP keyword checking rule 59
Table 4-22 Parameters for creating a connection exhaustion rule 61

Table 4-23 Parameters for creating a URL-ACL rule 63
Table 5-1 Parameters in out-of-path mode 78
Table 5-2 Parameters of a port channel 80
Table 5-3 Parameters for creating a GRE tunnel 82
Table 5-4 Interface parameters 83
Table 5-5 Parameters of a loopback address 84
Table 5-6 Parameters for creating a BGP route 86
Table 5-7 Parameters of a BGP neighbor 87
Table 5-8 Parameters for creating an IP route 89
Table 5-9 Parameters of an injection interface 91
Table 5-10 Parameters for creating an injection route 93
Table 5-11 Parameters for editing advanced configurations 99
Table 5-12 Parameters for creating a diversion filtering rule 105
Table 5-13 Parameters for creating a diversion rule 107
Table 5-14 Parameters for creating a group diversion rule 111
Table 5-15 Parameters of a diversion route 113
Table 5-16 Parameters for creating an MPLS route 115
Table 5-17 LDP route parameters 117
Table 5-18 Parameters for creating a syslog-based diversion rule 120
Table 6-1 Attack log parameters 123
Table 6-2 Parameters of system operation logs 125
Table 6-3 Parameters of system login logs 126
Table 6-4 Parameters of link status logs 127
Table 6-5 Parameters of traffic diversion logs 128
Table 6-6 Parameters of HA synchronization logs 129
Table 7-1 Basic system settings 134
Table 7-2 describes interface working mode parameters. 137
Table 7-2 Interface working mode parameters 137
Table 7-3 Management mode parameters 141
Table 7-4 Parameters of basic HA settings 145
Table 7-5 Parameters of advanced HA configurations 147
Table 7-6 Parameters of the external bypass group 156
Table 7-7 Parameters for configuring an upper-level ADS 158

Table 7-8 Parameters for configuring a lower-level ADS 161
Table 7-9 Parameters for creating a notification filtering rule 165
Table 7-10 Bandwidth overflow threshold parameters 166
Table 7-11 Login security parameters 167
Table 7-12 Parameters for configuring the authentication mode 169
Table 7-13 Parameters for configuring a Syslog server 171
Table 7-14 SNMP Trap parameters 172
Table 7-15 Parameters of sending logs by email 173
Table 7-16 Parameters for exporting logs via SFTP or SSH 175
Table 7-17 ADS device license parameters 176
Table 8-1 Parameters for manual packet capture 183
Table 8-2 Automatic packet capture parameters 185
Table 8-3 Parameters of a pattern matching rule 192
Table 8-4 IP reputation configuration parameters 196

Preface

Scope

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

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

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

Currently, two types of model naming methods exist for ADS products, as shown in the following table.

Old Model	New Model	Comparison
ADS 2010	ADS NX3-2010	The functions remain the same. The manuals of one can be used for the other.
ADS 2020	ADS NX3-2020	The functions remain the same. The manuals of one can be used for the other.
ADS 4020	ADS NX5-4020	The functions remain the same. The manuals of one can be used for the other.
ADS 6025	ADS NX5-6025	The functions remain the same. The manuals of one can be used for the other.

Audience

This document is intended for the following users:

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

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

- Linux and Windows operating systems
- TCP/IP protocol

Organization

Chapter	Description
1 Introduction	Describes features of ADS devices.
2 Web-based Manager	Describes basic information about the web-based manager.
3 Real-Time Monitoring	Describes details about security events monitored in real time.
4 Policies	Describes information and configuration about protection policies.
5 Diversion and Injection	Describes detailed information and configuration about the diversion and injection process.
6 Logs	Describes methods and options for viewing various types of logs.
7 System Administration	Describes common operations and methods for system administration and maintenance.
8 Advanced Applications	Describes advanced functions that include packet capturing and pattern matching.
9 Console-based Management	Describes methods for logging in and managing the console of ADS devices.
A Abbreviations	Describes explanation of abbreviations that appear in this article.
B Default Parameters	Describes default parameters of the ADS devices.
C IPv4/IPv6 Support	Describes ADS modules' support for IPv4 and IPv6.

Conventions

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

Convention	Description
Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Customer Support

To obtain materials about network security, visit NSFOCUS website at:

http://www.nsfocus.com/en/index.html

To obtain professional service information and business information about NSFOCUS network security, contact us at:

Global Support

To obtain materials about network security, visit NSFOCUS website at:

http://www.nsfocus.com/en/index.html

To obtain professional service information and business information about NSFOCUS network security, contact us at:

Global Support

24/7 service hotline:

+86-13321167330

+86-400-818-6868

Email: global_support@nsfocus.com

NSFOCUS US

Tel: +1 408-907-6638

Email: mailto:info-us@nsfocus.com

NSFOCUS Japan

Tel: +81-3-6206-8156

Email: info-jp@nsfocus.com

NSFOCUS Malaysia

Tel: +603-2169 6389

Fax: +603-2169 6396

NSFOCUS APAC

Email: info-apac@nsfocus.com

NSFOCUS Australia & New Zealand

Email: info-anz@nsfocus.com

NSFOCUS EU

Email: info-eu@nsfocus.com

NSFOCUS MENA

Email: info-mena@nsfocus.com

1 Introduction

1.1 Product Overview

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

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

1.2 Typical Deployment

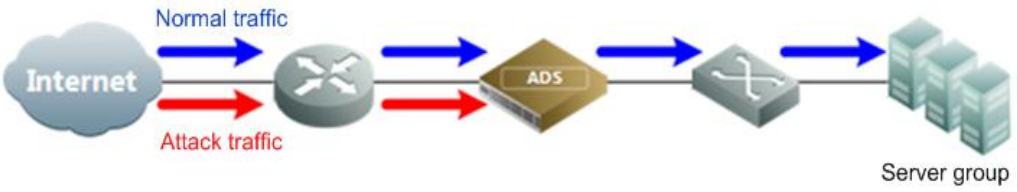
Currently, ADS devices can be deployed in in-path mode or out-of-path mode based on different network environments. The following sections detail the two modes.

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

1.2.1 In-Path Deployment

ADS devices are deployed in in-path mode in network environments with 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.

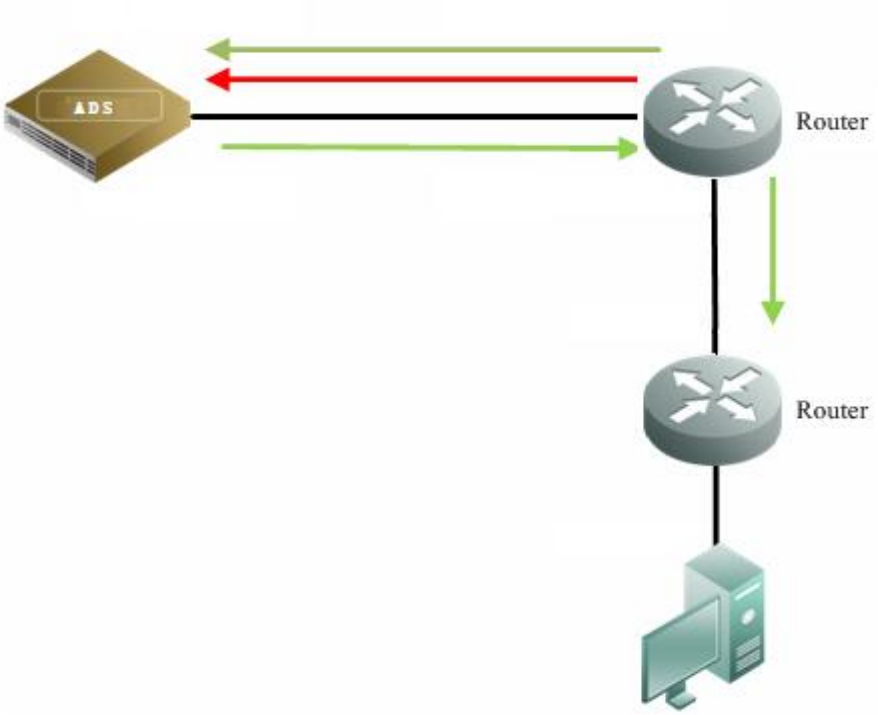
Figure 1-1 In-path deployment of an ADS device



1.2.2 Out-of-Path Deployment

ADS devices can be deployed in out-of-path mode and collaborate with other routers, performing traffic diversion and injection on one or two lines to protect servers in 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 about the web-based manager, as shown in the following table.

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

2.1 Login

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

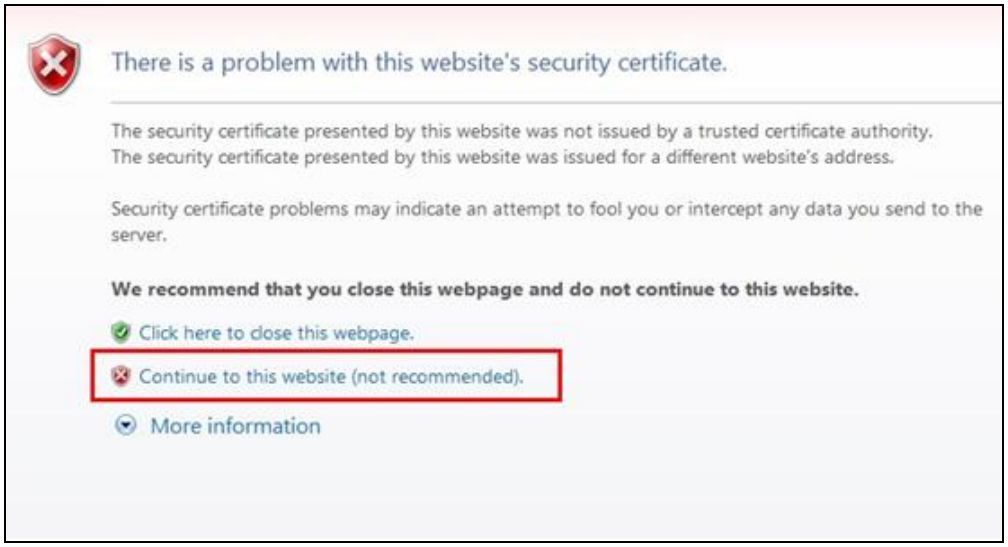
Step 1 Verify that the client host communicates properly with an ADS device (open port 443 if the traffic passes through a firewall).

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

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

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

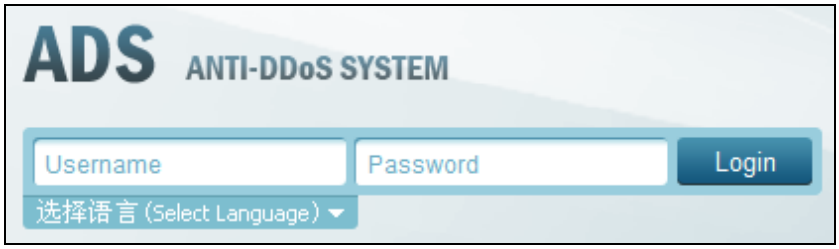
Figure 2-1 Alert page



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

The login page shown in Figure 2-2 appears.

Figure 2-2 Login page of the ADS device



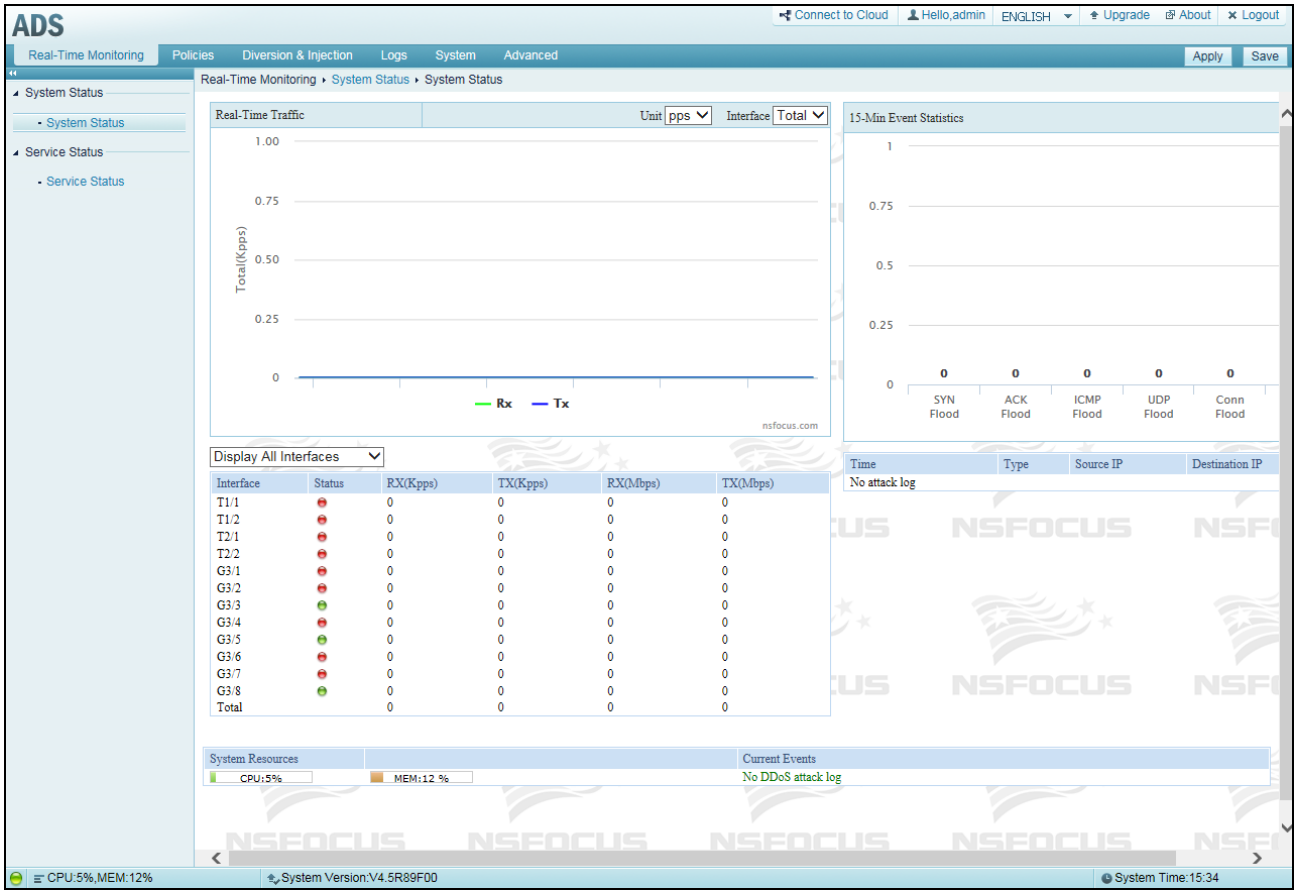
Step 4 Select the language, type the default user name and password (see appendix B Default Parameters), and click **Login** or press **Enter**.

Your selection of a language from the **Select Language** drop-down list has no impact on access of other users.

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

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

Figure 2-3 Window displayed after successful login



Note	Note the following during login: • You are advised to use an IE browser of 8.0 through 10.0 or a Chrome browser with the resolution greater than 1024x768. 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. • During the first login, after you type the default user name and password, the system displays a dialog box, asking you to change the password. Only after you change the default password to a different one, can you successfully log in to the system. • You must import the license after the first login. For details, see section 7.4.1 License. • The system will return to the login page if you remain inactive for a period specified by **Auto Idle Logout**. In the case, you need to log in again to continue using the system. For details, see section 7.2.1 Login Security Settings.

----End

2.2 System User

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

Table 2-1 User permissions

User Role	Configuration Permission	Viewing Permission
Super user	Default system user **admin**, who has all permissions in the web-based manager. It is not allowed to add or delete the super user.	
CLI user	Logs in to the console and performs management.	
Custom user	Configures traffic diversion and injection rules (manual mode), packet capture rules, and IP reputation rules, and performs system management (modification of his or her own account information).	Views monitoring information in real time, information about traffic diversion and injection, logs (detailed information and statistical graphs of attack log details and traffic diversion logs), system management information (basic system configuration and interface configuration), statistical graphs of attack traffic, and BGP neighbor status.
Common user	Performs system management (modification of his or her own account information).	Views monitoring information in real time and system management information (basic system configuration and interface configuration).
Administrator	Configures protection policies and traffic diversion and injection rules and conducts log management (detailed information and statistical graphs of attack logs and traffic diversion logs), and system management (basic configuration, interface configuration, and modification of his or her own account information).	Views monitoring information in real time, protection policy configuration, diversion and injection configuration, log management information (detailed information and statistical graphs of attack logs, statistical graphs of attack traffic, and traffic diversion logs), and system management information (basic configuration and interface configuration).
Audit user	Performs system management (modification of his or her own account information).	Views real-time monitoring data, login logs, and operation logs.

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

2.3 Web Page Layout

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

Users with different privileges 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 privileges in the status bar and shortcut operation area.

Figure 2-4 Web page layout

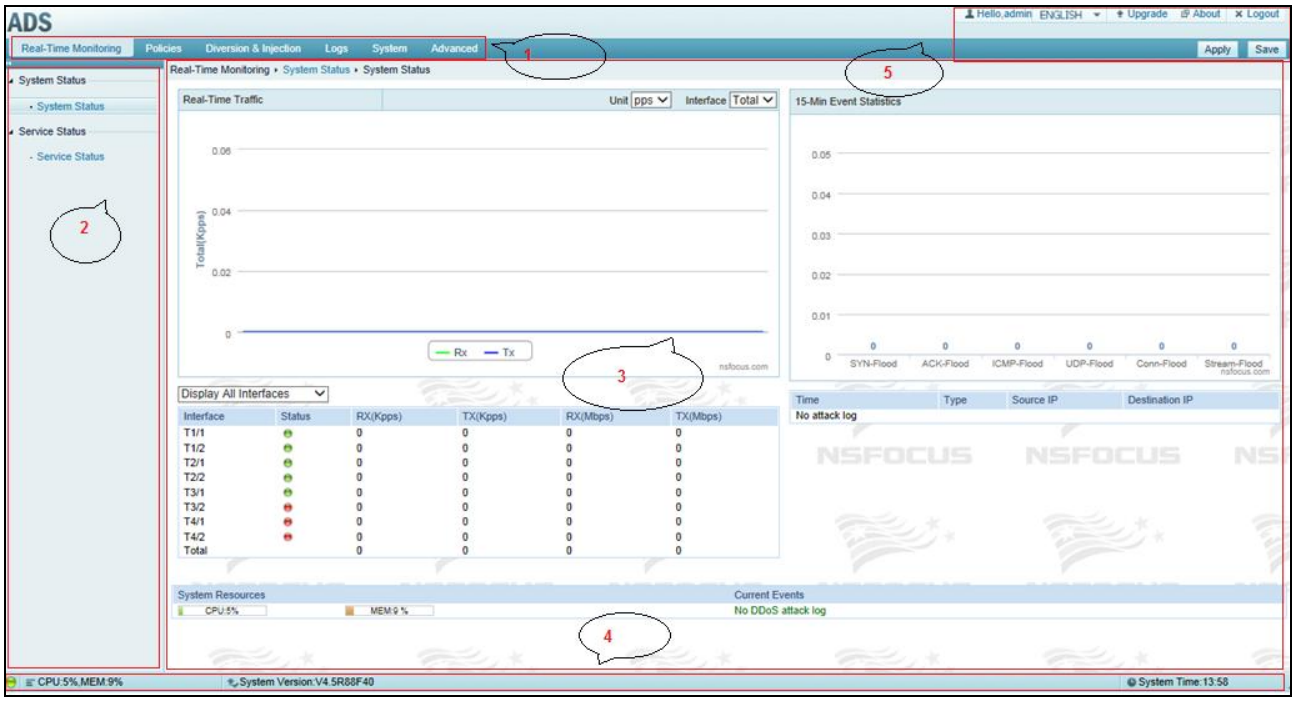


Table 2-2 describes the web page layout.

Table 2-2 Web page layout

SN	Area	Description
1	Menu bar	Main menus of the system.
2	Navigation tree	Involving menus and related sub-menus to help you locate system functions.
3	Work area	Area where you can perform configurations and operations and view data.
4	Status bar	Displaying current device information, software version and system time. For details, see section 3.3 System Information.
5	Quick access bar	Involving common buttons of the system. See Table 2-3 for details.

Table 2-3 lists common buttons.

Table 2-3 Common buttons

Button	Function
admin	Displays information of the current user.
ENGLISH	Switches to another language.
Upgrade	Switches to the system upgrade window.
About	Displays product information about the ADS devices.
Logout	Allows you to log out of the system.
Connect to Cloud	Allows you to download NSFOCUS mobile software. After ADS connects to the cloud, you can monitor the ADS status on a mobile phone.
Apply	Makes the configuration in the work area take effect immediately.
Save	Makes the configuration in the work area take effect the next time you start the system.

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

2.4 System Modules

The web-based manager provides function modules, including real-time monitoring, policies, diversion and injection, logs, system administration and advanced applications. Table 2-4 lists more details.

Table 2-4 System functions

Menu		Function
Real-Time Monitoring	System Status	Displays real-time traffic, interface status, and detailed information and statistical graphs of attack events.
	Service Status	Displays status of the communication between ADS devices and other NSFOCUS devices.
Policies	Anti-DDoS	Allows you to configure anti-DDoS policies.
	Access Control	Allows you to configure access control rules, connection exhaustion rules, URL-ACL rules, and whitelists.
Diversion & Injection	General Settings	Allows you to configure the system running mode and the interface IP address.
	Diversion Route	Allows you to configure diversion routes.
	Traffic Injection	Allows you to configure injection rules.
	Traffic Diversion	Allows you to configure traffic diversion settings.
	Advanced Route	Allows you to configure advanced route settings.

Menu		Function
	Setting	
	Syslog Diversion Configuration	Allows you to configure syslog-based diversion settings.
Logs	Attack Logs	Allows you to query attack logs.
	System Logs	Displays various system running logs.
	Log Analysis	Displays detailed log statistics.
System	Local Settings	Allows you to configure basic information, interface connection, configuration files, and user accounts.
	Security Configuration	Allows you to configure login security settings and unlock an IP address.
	Log Services	Allows you to configure log services and export SFTP/SSH logs.
	Others	Allows you to upgrade the system, manage the license, enable remote assistance, and view version information.
Advanced	Packet Capture	Provides you with common tools used to analyze packets transmitted over the network.
	Pattern Matching	Allows you to configure protection rules based on pattern matching.
	IP Reputation	Allows you to configure collaboration between ADS and the cloud-side IP reputation library.

2.5 Common Icons and Buttons

Table 2-5 describes functions of the common icons and buttons on the web-based manager.

Table 2-5 Buttons and icons

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

3 Real-Time Monitoring

The real-time monitoring module provides real-time traffic information, system resources, attacks of the last 15 minutes, and the latest service status 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
System Status	Describes real-time traffic, interface status, attack events being suffered by the network, and statistical graphs of attack events.
Service Status	Describes the running status of communications between the current device and other NSFOCUS devices.
System Information	Describes basic information of the current system.

3.1 System Status

The system monitors incoming and outgoing traffic, interface status, and device status of the current ADS device and displays the monitoring information in real time.

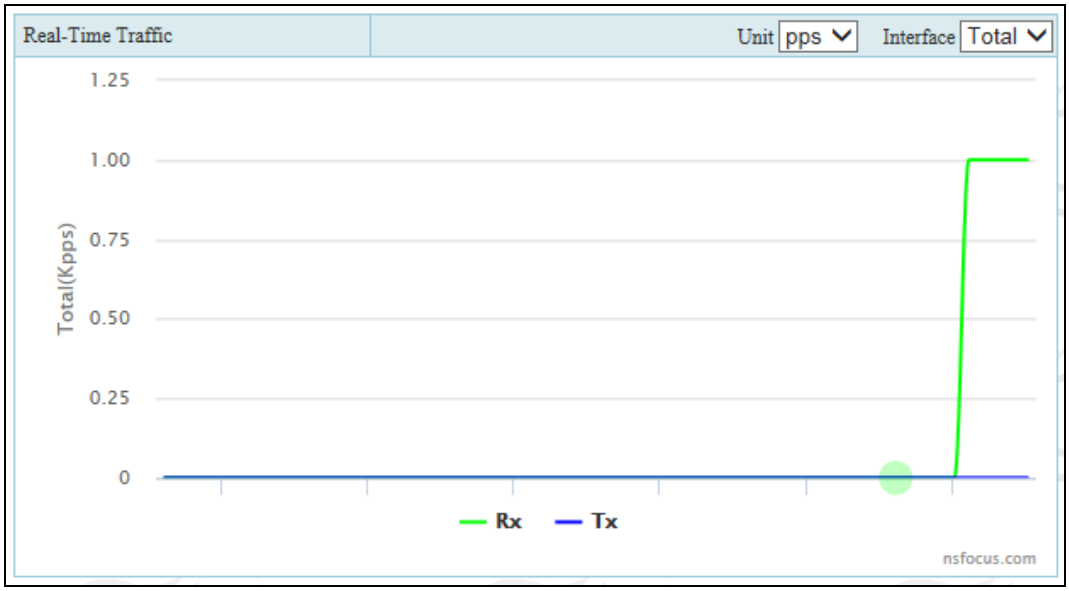
This section covers the following topics:

- Real-time Traffic Curves
- Interface Status
- System Resources
- Attack Events in the Last 15 Minutes
- Latest Attack Events

Real-time Traffic Curves

As shown in Figure 3-1, the **System Status** page shows the incoming and outgoing traffic (unit: kpps) of the ADS device in last 10 minutes. Here, the blue curve indicates the trend of traffic transmitted at a specific interface, and the green curve indicates the trend of traffic received at the interface. The traffic curves are automatically updated every 10 seconds.

Figure 3-1 Traffic curves



Note	You can view traffic trends from different angles by selecting different values from the **Unit** and **Interface** drop-down lists in the upper-right corner of Figure 3-1.

Interface Status

As shown in Figure 3-2, the **System Status** page shows the connection status of interfaces on ADS NX5-4020 (means "connected"; means "disconnected"), and real-time traffic of each interface. **Total** indicates total traffic of all interfaces. The information is automatically updated every 10 seconds.

By default, the information about all interfaces is displayed. As shown in Figure 3-2, clicking **Display online interface** from the drop-down list in the upper-left corner displays the information only about online interfaces.

Figure 3-2 Interface status of ADS NX5-4020

Display All Interfaces

Interface	Status	RX(Kpps)	TX(Kpps)	RX(Mbps)	TX(Mbps)
T1/1		0	0	0	0
T1/2		0	0	0	0
T2/1		0	0	0	0
T2/2		0	0	0	0
G3/1		0	0	0	0
G3/2		0	0	0	0
G3/3		1	0	2	0
G3/4		0	0	0	0
G3/5		0	0	0	0

The number and type of interfaces vary with device models. ADS devices provide the following working interfaces:

- Eight 1000M electrical ports
- Eight 1000M optical ports
- Four 10G optical ports

System Resources

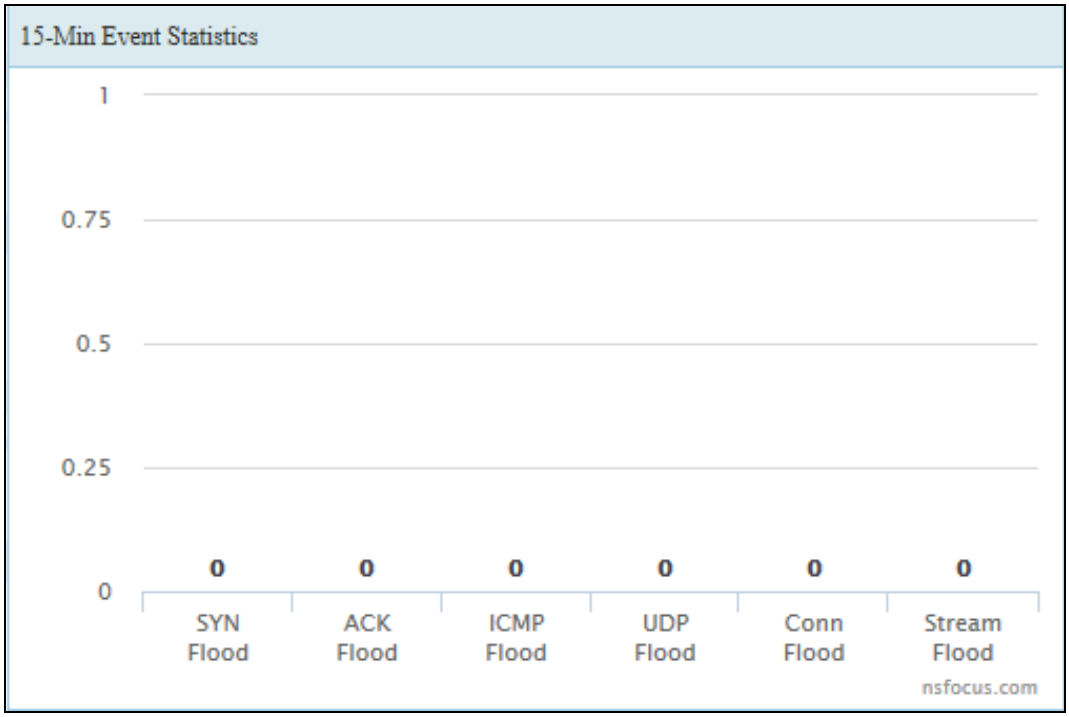
As shown in Figure 3-3, the **System Status** page shows the operating status of the ADS device, including system resource (CPU and memory) utilization and current attack logs. The information is automatically updated every 10 seconds.

Figure 3-3 System resource

Attack Events in the Last 15 Minutes

As shown in Figure 3-4, the **System Status** page shows the statistical graph of attack events in the last 15 minutes on the ADS device. The X-axis indicates the event type and the Y-axis indicates event count. The information is automatically updated every 25 seconds.

Figure 3-4 Attack events in the last 15 minutes



Latest Attack Events

As shown in Figure 3-5, the **System Status** page shows latest attack events (a maximum of five events) on the ADS device, including the attack time, attack type, source and destination IP addresses of attacks.

Figure 3-5 Latest attack events

Time	Type	Source IP	Destination IP
12:03:23	SYN-Flood	10.237.248.36	8.*.*.1
12:03:23	SYN-Flood	10.237.248.36	8.*.*.1
12:03:23	SYN-Flood	10.237.248.36	8.*.*.1
12:02:23	SYN-Flood	16.*.*.76	8.*.*.1
12:02:23	SYN-Flood	16.*.*.76	8.*.*.1

3.2 Service Status

Service status gives a clue to system diagnosis. As shown in Figure 3-6, the **Service Status** page shows the communication status between the ADS device and other NSFOCUS devices.

Figure 3-6 Service status

Service Status

Service Status

Type	Status	IP Address	Port
Communication with Probe	ESTABLISHED	10.30.2.205	Peer Port:54677

The service status **Communication with Probe** indicates the communication between ADS and Probe. **Status** is displayed as **ESTABLISHED** after the connection is established.

Note	Some other statuses may also be displayed in the **Status** column during service connection, for example, **CLOSE_WAIT**, indicating that the service is being disabled. The service status will not be displayed after the service is disabled.

3.3 System Information

All users can view system information. The status bar displays basic system information, including hardware CPU and memory usage, system version, and system time, as shown in Figure 3-7.

The green indicator indicates that the device works properly and the red indicator indicates that the device is abnormal.

Figure 3-7 System information

CPU:5%,MEM:12% | System Version:V4.5R89F00 | System Time:15:36

4 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.

4.1 Anti-DDoS Policies

This section covers the following topics:

- DDoS Protection Policy
- Protection Groups
- Advanced Global Parameters
- Response Page Settings
- Policy Auto-Learning

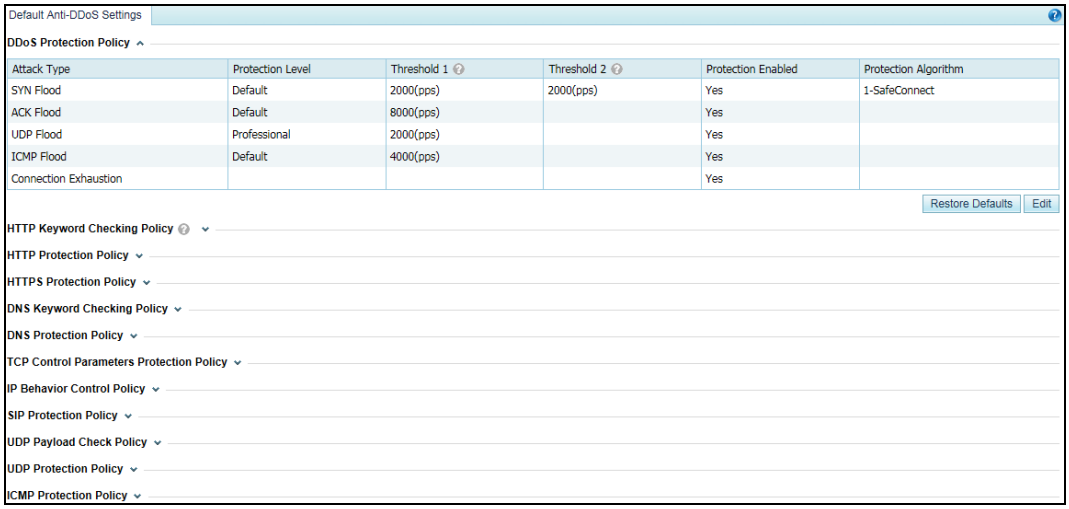
4.1.1 Default Anti-DDoS Parameters

Default Anti-DDoS policies include the following:

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

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

Figure 4-1 Default Anti-DDoS Settings page



4.1.1.1 DDoS Protection Policy

Figure 4-2 shows the parameters of the default anti-DDoS policy. You can click **Edit** in the lower-right corner of the list to edit the parameters, or click **Restore Defaults** to restore default settings.

Figure 4-2 DDoS Protection Policy area

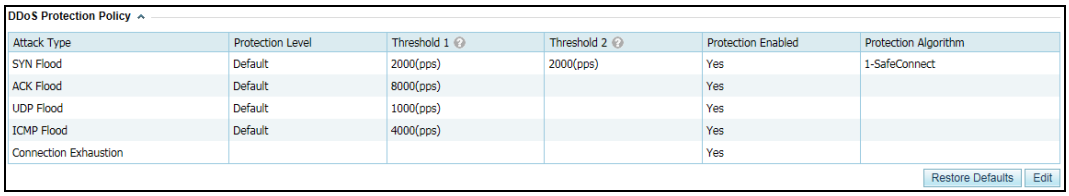


Table 4-1 describes parameters of the DDoS protection policy.

Table 4-1 Parameters of the default anti-DDoS policy

Parameter	Description
Attack Type	Types of DDoS attacks that can be blocked.
Protection Level	Priority for blocking attacks. Two values are available: **Default** and **Professional**. Thresholds in **Default** mode are predefined by the system and thus cannot be changed, while thresholds in **Professional** mode can be changed as required.
Threshold 1	The value varies with DDoS attack type. See the following descriptions.
Threshold 2	The value varies with DDoS attack type. See the following descriptions.

Parameter	Description
Protection Enabled	Controls whether to enable the protection. • **Yes** indicates that the ADS device protects devices hit by DDoS attacks of this type. • **No** indicates that the ADS device does not protect devices hit by DDoS attacks of this type.
Algorithm	Different algorithms are adopted to defend against different types of DDoS attacks. See the following descriptions.

SYN Flood

- **Threshold 1**: specifies the SYN traffic rate at which SYN flood protection is triggered. If the rate (pps) of SYN traffic to a destination exceeds the specified value, SYN flood protection is triggered. The value ranges from 0 to 6000000 for NX3-2010/2020, NX3-600E, ADS NX5-4020/6025, and ADS NX5-8000. You can configure this parameter only when the protection level is set to **Professional**, while leaving it at the default value for the **Default** protection level.
- **Threshold 2**: specifies the rate at which ADS sends reverse detection packets in response to SYN packets, after SYN flood protection is triggered. The value ranges from 1 to 30000000 for ADS NX3-2010/2020, NX3-600E, NX5-4020/6025, and NX5-8000 and. A greater value means a better protection effect but a higher load on the ADS device. You can configure this parameter only when the protection level is set to **Professional**, while leaving it at the default value for the **Default** protection level.

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

- **Algorithm**
  - **0-SynCheck** applies to symmetrical networks only.
  - **1-SafeConnect** and **2-DynaCheck** apply to both symmetrical and non-symmetrical networks. Only **1-SafeConnect** and **2-DynaCheck** are available under out-of-path deployment mode.
- **Protection Enabled**: SYN Flood protection is available only when **Enable** is set to **Yes**.

ACK Flood

Threshold 1: specifies the ACK traffic rate at which ACK flood protection is triggered. If the rate (pps) of ACK traffic to a destination exceeds the specified value, ACK flood protection is triggered. The value ranges from 0 to 30000000 for ADS NX3-2010/2020, NX5-4020/6025, and NX5-8000. You can configure this parameter only when the protection level is set to **Professional**, while leaving it at the default value for the **Default** protection level.

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

UDP Flood

Threshold 1: specifies the UDP traffic rate at which UDP flood protection is triggered. If the rate (pps) of UDP traffic to a destination exceeds the specified value, UDP flood protection is triggered. The value ranges from 0 to 6000000 for ADS NX3-2010/2020, NX5-4020/6025, and NX5-8000.

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

ICMP Flood

Threshold 1: specifies the ICMP traffic rate at which ICMP flood protection is triggered. If the rate (pps) of ICMP traffic to a destination exceeds the specified value, ICMP flood protection is triggered. The value ranges from 0 to 6000000 for ADS NX3-2010/2020, NX5-4020/6025, and NX5-8000.

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

Connection Exhaustion

Connection exhaustion protection cooperates with connection exhaustion rules. You can only select **Yes** or **No** for it. (For how to configure connection exhaustion rules, see section 4.2.6 Connection Exhaustion Rules.)

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

4.1.1.2 HTTP Keyword Checking Policy

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

Figure 4-3 shows the current HTTP keyword checking rules.

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

Figure 4-3 HTTP Keyword Checking Policy area

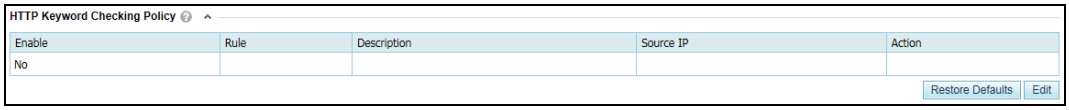


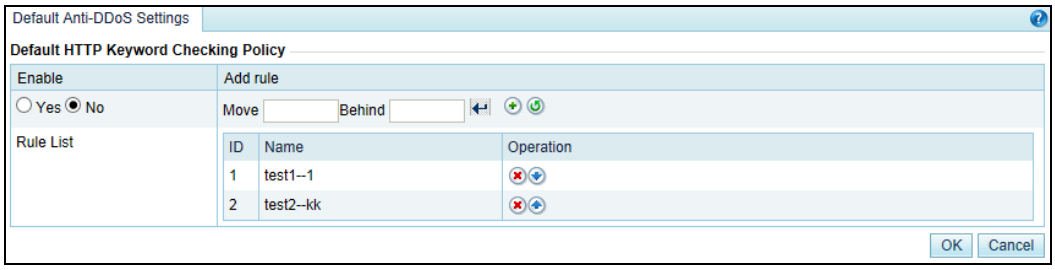
Table 4-2 describes parameters of the HTTP keyword checking policy.

Table 4-2 Parameters of the default HTTP keyword checking policy

Parameter	Description
Enable	Controls whether to enable the default HTTP keyword checking policy.
Rule	Name of each rule included in the policy.
Description	Brief description of each rule.
Source IP	Specifies the source IP address traffic from which will be checked against the default HTTP keyword checking policy.
Action	Specifies the action that ADS will take against the source IP address (host). For details, see section 4.2.5 HTTP Keyword Checking.

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

Figure 4-4 Editing the default HTTP keyword checking policy

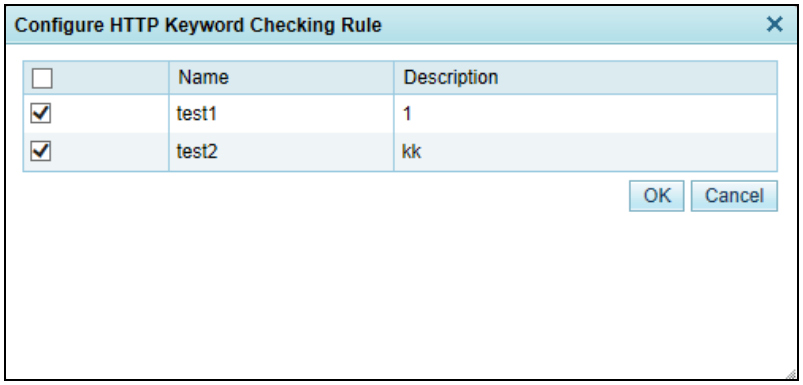


On this page, you can edit the HTTP keyword checking policy as follows:

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

  For the creation of an HTTP keyword checking rule, see section 4.2.5 HTTP Keyword Checking.

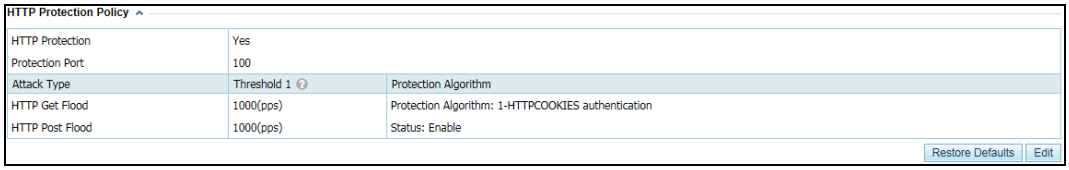
Figure 4-5 Configuring HTTP keyword checking rules



4.1.1.3 HTTP Protection Policy

With the default HTTP Protection Policy, the system checks HTTP packets from clients and drops data that do not meet conditions specified in the policy. Figure 4-6 shows parameters of the default HTTP protection policy. You can click **Edit** in the lower-right corner of the list to edit the parameters, or click **Restore Defaults** to restore default settings.

Figure 4-6 HTTP Protection Policy area



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

Protection Port

This specifies the port number of the destination IP address of HTTP packets. You can configure multiple ports or port ranges. The value range is 0–65535. Multiple ports must be separated by commas. The ports configured for the HTTP protection policy must be different from those for the HTTPS protection policy.

HTTP GET Flood

- **Threshold 1**: specifies the HTTP GET traffic rate at which HTTP GET flood protection is triggered. If the rate (pps) of HTTP GET traffic to a destination exceeds the specified value, HTTP GET flood protection is triggered. The value ranges from 0 to 6000000 for ADS NX3-2010/2020, NX5-4020/6025, and NX5-8000.
-
- **Algorithm**:
  - **0_TAG authentication** and **1_HTTPCOOKIES authentication** verify the destination IP address by adding authentication information into HTTP packets.
  - **2_URL authentication** adds information similar to Cookies into the URL request.

- **3_ASCII image authentication** and **4_BMP image authentication** add a verification code.
- **5_Dynamic script protection** performs verification by adding key values to URLs.
- **6_Legend authentication** and **7_FCS check** checks the packets of game "Legend" and Flash Server.
- **8_Pattern matching check** matches a signature string that is defined during the pattern matching of advanced applications (see section 8.2 Pattern Matching Rules for the configuration of pattern matching).

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

Note	**6_Legend authentication**, **7_FCS check** and **8_Pattern matching check** are available only when **SYN Cookie URL** is enabled during protection group configuration.

HTTP POST Flood

Threshold 1: specifies the HTTP POST traffic rate at which HTTP POST flood protection is triggered. If the rate (pps) of HTTP POST traffic to a destination exceeds the specified value, HTTP POST flood protection is triggered. The value ranges from 0 to 6000000 for ADS NX3-2010/2010, NX5-4020/6025, and NX5-8000.

4.1.1.4 HTTPS Protection Policy

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

With the default HTTPS protection policy, the system checks HTTPS packets from clients. When **Add Abnormal IP to Blacklist** is set to **Yes**, the system adds source IP addresses that match the HTTPS protection algorithm to the blacklist. Figure 4-7 shows parameters of the HTTPS protection policy.

Figure 4-7 HTTPS Protection Policy area

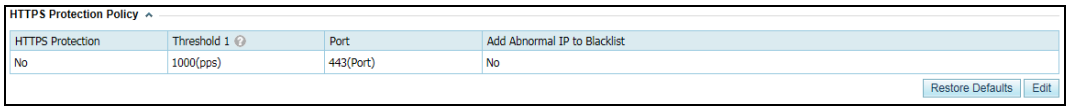


Table 4-3 describes parameters of the HTTPS protection policy.

Table 4-3 Parameters of the HTTPS protection policy

Parameter	Description
HTTPS Protection	Controls whether to enable HTTPS protection.
Threshold 1	Specifies the HTTPS traffic rate at which HTTPS protection is triggered. If the rate (pps) of HTTPS traffic to a destination exceeds the specified value, HTTPS protection is triggered. The value ranges from 0 to 6000000 for ADS NX3-2010/2020, NX5-4020/6025, and NX5-8000.
Threshold 2	Specifies the port corresponding to the destination IP address. The value ranges from 0 to 65535, with **443** as the default. HTTPS protection is triggered only when the destination port number of attack packets matches the specified port. The ports configured for the HTTP protection policy should be different from those for the HTTPS protection policy.
Add Abnormal IP to Blacklist	Controls whether to add abnormal IP addresses to the blacklist. The value **Yes** indicates that, when the IP address of a client fails the check with the HTTPS protection algorithm, the system will add this IP address to the blacklist.

4.1.1.5 DNS Keyword Checking Policy

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

Figure 4-8 shows about the current DNS keyword checking rules.

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

Figure 4-8 DNS Keyword Checking Policy area

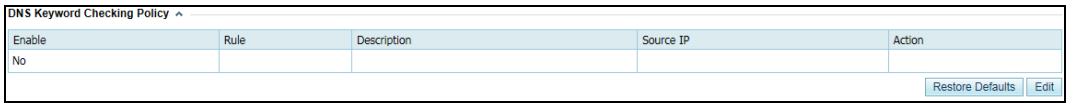


Table 4-4 describes parameters of the DNS keyword checking policy.

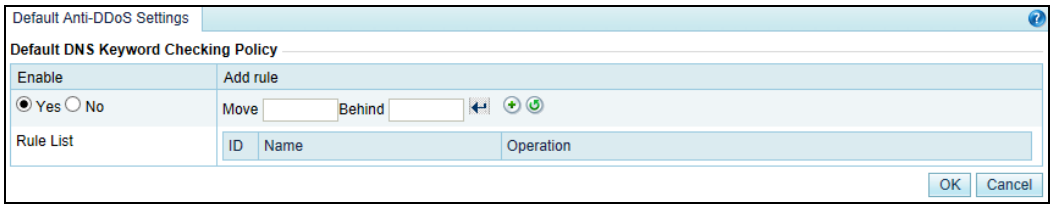
Table 4-4 Parameters of the default DNS keyword checking policy

Parameter	Description
Enable	Controls whether to enable the default DNS keyword checking policy.

Parameter	Description
Rule	Name of each rule included in the policy.
Description	Brief description of each rule.
Source IP	Specifies the source IP address traffic from which will be checked against the default DNS keyword checking policy.
Action	Specifies the action that ADS will take against the source IP address (host). For details, see section 4.2.4 DNS Keyword Checking.

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

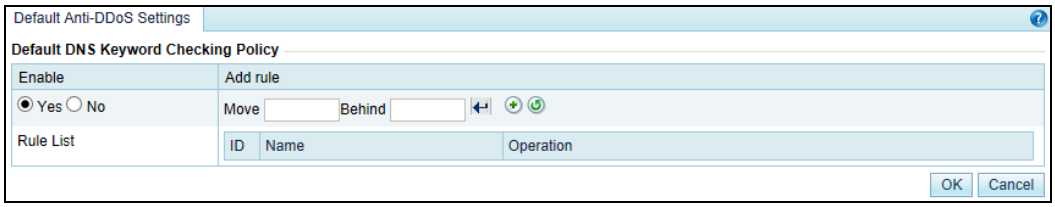
Figure 4-9 Editing the default DNS keyword checking policy



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

- **Enable**: Select **Yes** or **No** to enable or disable the policy.
- Adjust rule sequence: Click or to move a rule one place up or down. You can also type the rule IDs in the **Move** and **Behind** text boxes. For example, **Move 1 Behind 3** indicates that the first rule will be put under the third rule. Click to commit the change.
- **Add rule**: Click to open the policy configuration page. Select one or more rules and then click **OK**.
  - For the creation of a DNS keyword checking rule, see 4.2.4 DNS Keyword Checking.

Figure 4-10 Configuring DNS keyword checking rules



4.1.1.6 DNS Protection Policy

DNS protection is a policy against DNS attacks and spoofing. Figure 4-11 shows the current DNS protection policy.

Figure 4-11 DNS Protection Policy area

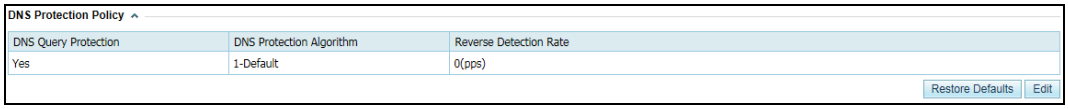


Table 4-5 describes parameters of the DNS protection policy.

Table 4-5 Parameters of the default DNS protection policy

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

Note	DNS protection is triggered when the number of UDP packets transmitted per second exceeds the specified threshold. For the setting of UDP flood thresholds, see section 4.1.1.1 DDoS Protection Policy.

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

4.1.1.7 TCP Control Policy

Figure 4-12 shows parameters of the TCP control policy.

Figure 4-12 TCP Control Policy area

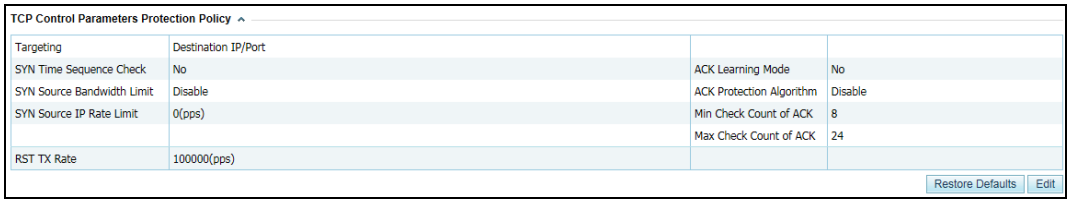


Table 4-6 describes parameters of the TCP control policy.

Table 4-6 Parameters of the TCP control policy

Parameter	Description
Targeting	Specifies how to identify a target server to be protected.

Parameter	Description
	• **Destination IP/Port**: indicates that the server to be protected is identified by the destination IP address and port. • **Destination IP**: indicates that the server to be protected is identified by only the destination IP address.
SYN Time Sequence Check	Controls whether to check the SYN time sequence.
SYN Source Bandwidth Limit	Works with **Threshold Triggering SYN Source Bandwidth Limit** to limit the bandwidth used by the source host to send SYN packets. It has the following values: • **Disable**: disables the function of limiting the bandwidth used by the source host to send SYN packets. • **Drop and add to blacklist**: adds the IP address of the source host to the blacklist when the SYN packet forwarding rate of the source host exceeds the specified value. • **Drop**: drops subsequent packets when the SYN packet forwarding rate of the source host exceeds the specified value.
SYN Source IP Rate Limit	Works with **Bandwidth Limit of SYN Source IP** to specify the maximum rate for the source host to forward SYN packets (pps).
ACK Learning Mode	Controls whether to enable the ACK learning mode. The ACK learning mode can be enabled only when **Protection Enabled** is set to **No**. After the ACK learning mode is enabled, the system learns the packets sent by the client and adds the source IP addresses meeting the specified conditions to the trust list. The ACK learning mode takes effect only when **Protection Enabled** is set to **Yes** for both SYN flood attacks and ACK flood attacks.
ACK Protection Algorithm	When ACK flood protection is enabled, you can configure the ACK protection algorithm, which can be **Disable**, **Time Sequence Check**, or **ACK Check**, with **Disable** as the default value. • **Disable**: indicates that the default algorithm will be used for ACK protection. • **ACK Check**: indicates that the packets properly responding to the ACK check will be allowed through. Otherwise, these packets will be dropped. • **Time Sequence Check**: For two identical ACK packets, if their sending interval is between **Min Check Count of ACK** and **Max Check Count of ACK**, they will be allowed through. Otherwise, they will be dropped.
Min Check Count of ACK	This parameter is used with **Max Check Count of ACK**. The value ranges from 1 to 300 (8 counts equal 1 second), with **8** as the default. The ACK packet check count of a client must be within the range. Otherwise, the client is deemed to have abnormal behaviors and will receive strict packet checks.
Max Check Count of ACK	This parameter is used with **Min Check Count of ACK**. The value ranges from 1 to 300 (8 counts equal 1 second), with **24** as the default. The ACK packet check count of a client must be within the range. Otherwise, the client is deemed to have abnormal behaviors and will receive strict packet checks.
RST TX Rate	Maximum TX rate of RST packets. The value ranges from 0 to 500000 for ADS NX3-2010/2020, NX3-4020/6025, and NX5-8000 and 0 to 250000 for other models, with **100000** as the default. The value **0** indicates that no

Parameter	Description
	RST packets are sent.

4.1.1.8 IP Behavior Control Policy

The system regards source IP addresses of packets that have been authenticated with the DDoS protection policy as trusted IP addresses. However, to protect against DDoS attacks from trusted IP addresses, the system needs to further process packets from trusted IP addresses. This process is called "IP behavior control". By limiting the TX rate of source IP addresses whose packet forwarding rate exceeds the threshold or adding such IP addresses to the blacklist, the system can effectively defend against botnet attacks. Figure 4-13 shows IP behavior control parameters.

Figure 4-13 IP Behavior Control Policy area

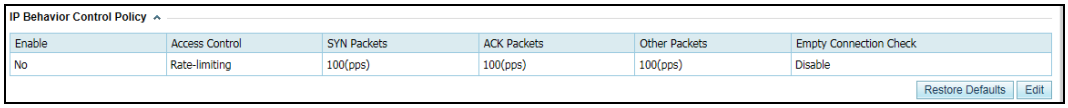


Table 4-7 describes IP behavior control parameters.

Table 4-7 IP behavior control parameters

Parameter	Description
Enable	Controls whether to enable IP behavior control.
Access Control	Action the system takes to exert access control for trusted IP addresses whose packet forwarding rate (pps) exceeds the threshold. It has the following values: • **Rate-limiting**: limits the traffic rate. • **Drop and add to blacklist**: adds an IP address to the blacklist and block packets from this IP address when its traffic exceeds the specified value. To select this value, you must enable the blacklist function first. For details, see section 4.2.8 Blacklist.
SYN Packets	Specifies the maximum rate (pps) at which a trusted IP address can send SYN packets. ADS drops excess SYN packets and generates attack logs.
ACK Packets	Specifies the maximum rate (pps) at which a trusted IP address can send ACK packets. When the actual rate of ACK packets exceeds the specified value, ADS drops excess ACK packets and generates attack logs.
Other Packets	Specifies the maximum rate (pps) at which a trusted IP address can send non-SYN packets, including UDP, ACK, and ICMP packets.
Empty Connection Check	Checks whether empty connections exist. It has the following values: • **Disable**: disables the empty connection check function. • **Drop and add to blacklist**: adds the IP address of the source host to the blacklist when the SYN or TCP packets are destined for an empty connection. • **Drop**: drops the current SYN or TCP packets that are destined for an

Parameter	Description
	empty connection. This function does not support IPv6. Therefore, you can use only IPv4 addresses when configuring this function.

4.1.1.9 SIP Protection Policy

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

With the SIP protection policy, the system provides protection against packets using the Session Initiation Protocol (SIP). Figure 4-14 shows parameters of the SIP protection policy.

Figure 4-14 SIP Protection Policy area

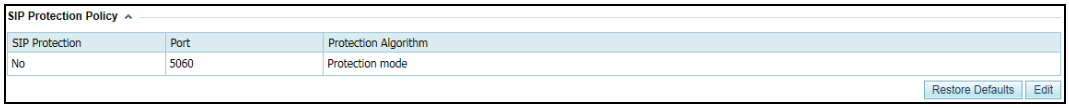


Table 4-8 describes parameters of the SIP protection policy.

Table 4-8 Parameters of the default SIP protection policy

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

4.1.1.10 UDP Payload Check Policy

With the UDP payload check policy, the system inspects the payload of UDP packets from clients and drops packets that do not meet specified conditions. Figure 4-15 shows UDP payload inspection parameters.

Figure 4-15 UDP Payload Check Policy area

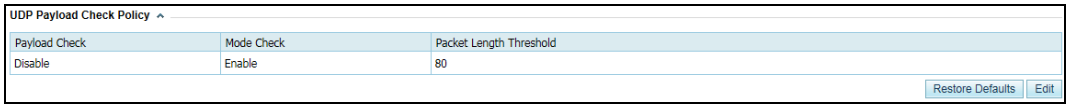


Table 4-9 describes UDP payload inspection parameters.

Table 4-9 UDP payload inspection parameters

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

4.1.1.11 UDP Protection Policy

With the UDP protection policy, the system checks UDP connection requests from clients, and drops requests that do not meet specified conditions. Figure 4-16 shows parameters of the default UDP protection policy.

Figure 4-16 UDP Protection Policy area

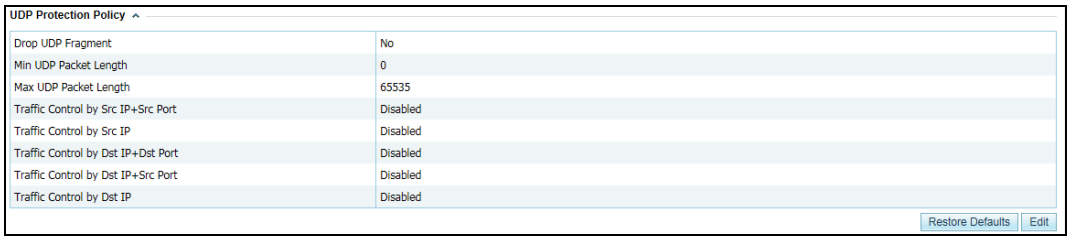


Table 4-10 describes parameters of the UDP protection policy.

Table 4-10 Parameters of the default UDP protection policy

Parameter	Description
Drop UDP Fragment	Controls whether to drop UDP fragments. The value **Yes** indicates that ADS discards detected UDP fragments of IPv4 addresses.

Parameter	Description
Min UDP Packet Length	Specifies the minimum packet length. The system discards 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. The system discards 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. Excessive UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–65535, 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. Excessive UDP fragments will be dropped. This parameter is enabled by default. The value range is 1–3000000, 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. Excessive UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–65535, 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. Excessive UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–65535, 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. Excessive UDP fragments will be dropped. This parameter is disabled by default. The value range is 1–3000000, with **3000000** as the default value.

4.1.1.12 ICMP Protection Policy

With the ICMP protection policy, the system checks ICMP connection requests from clients, and drops requests that do not meet specified conditions. Figure 4-17 shows parameters of the ICMP protection policy.

Figure 4-17 ICMP Protection Policy area

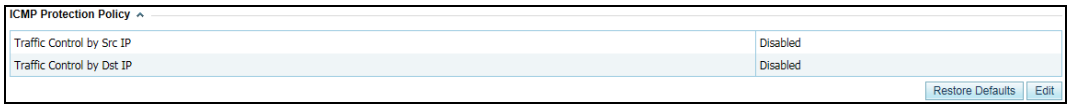


Table 4-11 describes parameters of the ICMP protection policy.

Table 4-11 Parameters of the ICMP protection policy

Parameter	Description
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 1–3000000, 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. Excessive ICMP fragments will be dropped. By default, it is disabled. The value range is 1–3000000, with **3000000** as the default value.

4.1.2 Protection Groups

As networks serve a large number of users who have various anti-DDoS requirements, 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 servers that are protected by ADS devices using the same policy. NSFOCUS ADS supports a maximum of 65535 IP addresses in total.

ADS can automatically generate protection groups based on policy auto-learning results. For details, see section 4.1.5 Policy Auto-Learning.

This section covers the following topics:

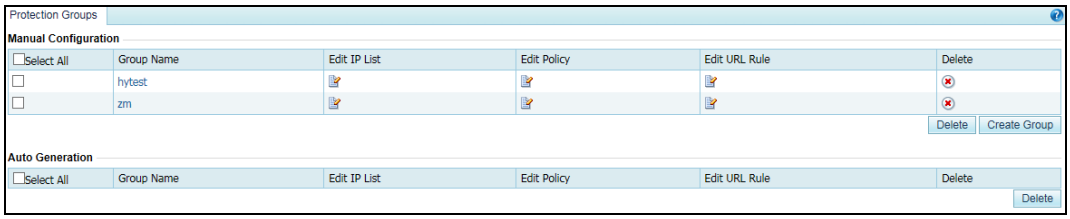
- Creating a Protection Group
- Viewing Protection Groups
- Editing a Protection Group (including IP address list, policies, and URL rules)
- Deleting a Protection Group

4.1.2.1 Creating a Protection Group

To create a protection group, perform the following steps:

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

Figure 4-18 Protection groups



Step 2 Configure basic information of the protection group.

To the lower right of the list, click **Create Group** to add a protection group. See Figure 4-19.

Figure 4-19 Basic information about a protection group

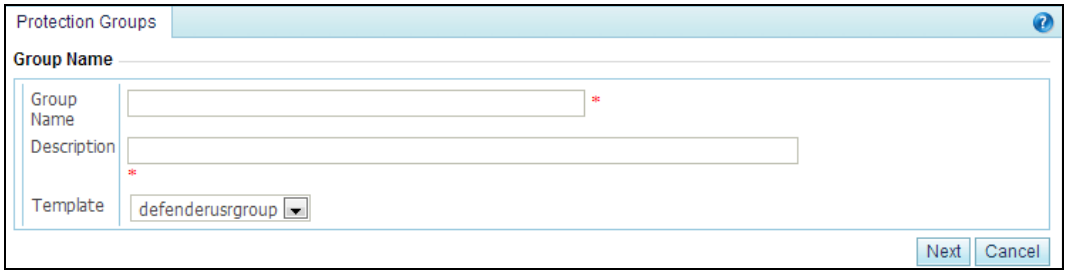


Table 4-12 describes parameters for creating a protection group.

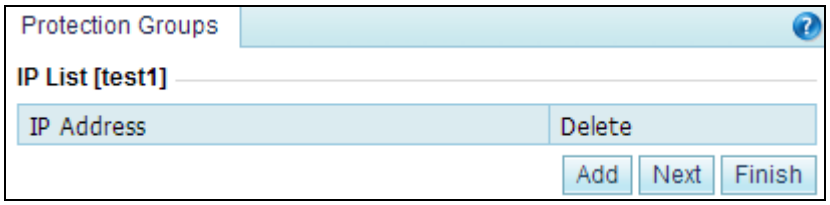
Table 4-12 Parameters for creating a protection group

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

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

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

Figure 4-20 IP List page



The administrator can add IP segments (one by one). If the administrator does not want to add IP segments at that time, click **Next** to skip this step or click **Finish** to end the creation of the protection group.

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

- Add an IP segment.

a. Click **Add** to the lower right of the IP address list to add an IP segment. See Figure 4-21.

Figure 4-21 Adding an IP segment

Table 4-13 describes parameters of an IP segment.

Table 4-13 Parameters of an IP segment

Parameter	Description
IP address format	You can type IPv4 or IPv6 addresses or segments, with one in each line, in the following formats: • Single IP address: If a single IP address such as 192.168.1.1 or 2::2 is typed, the page automatically displays it as 192.168.1.1-192.168.1.1 or 2::2-2::2. • IP address/netmask: IPv4 address with a netmask ranging from 16 to 32, such as 192.168.1.0/24; or IPv6 address with a netmask ranging from 112 to 128, such as fe80::250:56ff:fec0:0/114. • Start IP-End IP: an IPv4 address range within 256 addresses in a /24 segment, such as 192.168.1.1-10; or IPv6 address with a maximum of 16 bytes, such as 1::1-ffff. The IP addresses or IP segments cannot conflict with those in existing groups.

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

- Delete IP segments.

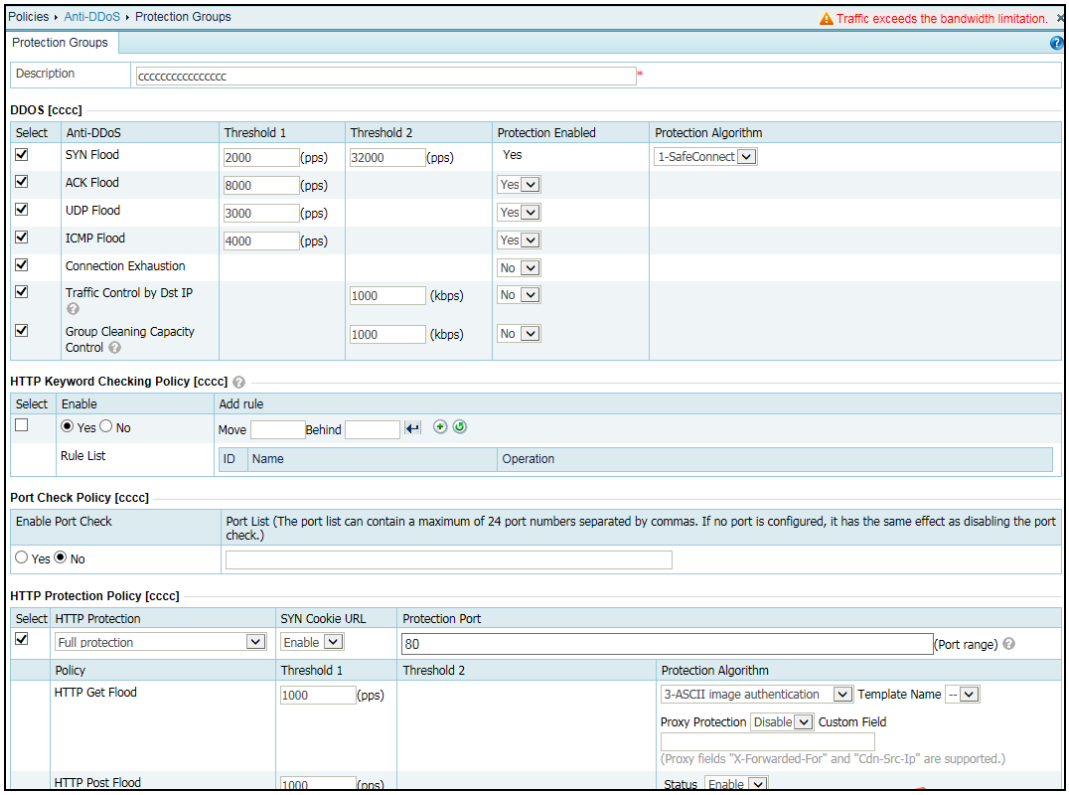
  Click ⊗ to the right of an IP segment, as shown in Figure 4-20, and then click **OK** in the confirmation dialog box to delete the IP segment.

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

Step 4 Configure policies for the protection group.

After configuring IP segments, click **Next** to configure policies.

Figure 4-22 Configuring policies



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

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

Group protection involves all policies on the **Anti-DDoS Policy** page. In addition, you can configure a TCP regular expression protection policy, port check policy, and watermark protection policy for a group. Note that the content of anti-DDoS policies and HTTP protection policies is different from that of the default anti-DDoS policies.

- DDoS

  The function of traffic control by destination IP address controls the number of packets to an IP address. When **Protection Enabled** of **Traffic Control by Dst IP** is set to **Yes**, excessive packets will be dropped.

  The group cleaning capacity control function controls the total number of packets to a group. When **Protection Enabled** of **Group Cleaning Capacity Control** is set to **Yes**, excessive packets will be dropped.

- HTTP Protection Policy

SYN Cookie URL can be enabled only after **HTTP Get Flood** and **HTTP Post Flood** are enabled.

Enabling **SYN Cookie URL** automatically disables **Proxy Protection**. To disable **SYN Cookie URL** for a group, you must disable **SYN Cookie URL** for all URL rules of the group in advance.

If **HTTP Protection** is set to **Only on the rules of URL protection**, protection is performed based on the rules of URL protection. **HTTP Post Flood** protection can be enabled only when **HTTP Protection** is set to **Protect** or **Only on the rules of URL protection**. If **HTTP Protection** is set to **Not protect**, **HTTP Post Flood** protection is disabled.

- TCP Regular Expression Protection Policy

  After configuring regular expression rules, you can enable TCP regular expression protection here and reference created regular expression rules. For details on regular expression rules, see section 4.2.3 Regular Expression Rules.

  Click to display the list of existing regular expression rules. Select one or more rules and click **OK**. Regular expression rules are thus added. The system automatically assigns numbers to added rules and displays them in the rule list. Regular expression rules are matched one by one in the ascending order of number. To change the matching sequence, enter rule numbers in Move To and then click . Then the rule sequence is changed as configured.

- Port Check Policy

  If the port check policy is enabled, the system checks the data arriving at the specified port but drops the data on other ports.

- Watermark Protection Policy

  You can add a watermark and configure watermark rules on ADS. After the watermark protection policy is enabled, 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 meet this rule to pass through and drop those which do not meet this rule. You can create a watermark protection rule by configuring **Protocol** (UDP or TCP), **Port range** (0–1480), **Offset** (must be a decimal integer), and **hashKey**. **Port range** can be a single port, port range, or multiple ports. Multiple ports must be separated by commas.

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

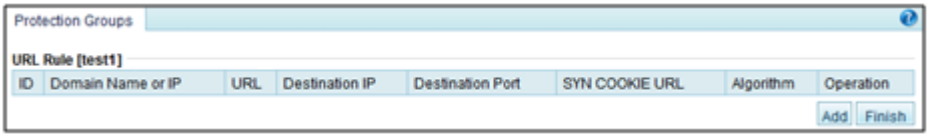
For how to configure other policies, see section 4.1.1 Default Anti-DDoS Parameters.

Note	The traffic control function of the anti-DDoS policy allows the system to control the number of packets transmitted to a destination IP address and drop excess packets if the maximum number is exceeded.

Step 5 Configure a URL rule for the protection group.

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

Figure 4-23 List of URL rules



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

Figure 4-24 Configuring a URL rule

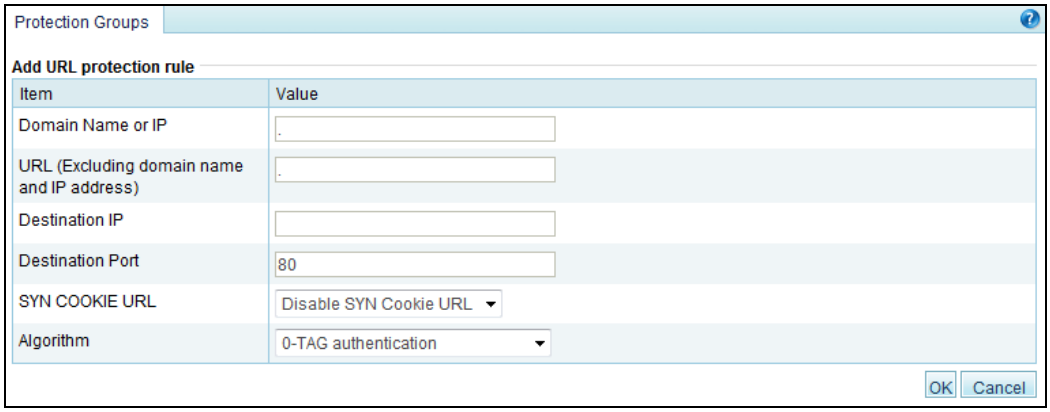


Table 4-14 describes parameters of a URL rule.

Table 4-14 Parameters of a URL rule

Parameter	Description
Domain Name or IP	Domain name or IP address of a URL protection object. The symbol "." indicates that this rule is valid for all domain names and IP addresses.
URL (Excluding domain name and IP address.)	Relative path of a URL protection object, that is, URL excluding the domain name or IP address. The symbol "." indicates that this rule is valid for all URLs.
Destination IP	IP address of the server. You can type IPv4 or IPv6 addresses according to the actual network deployment. **Note** The destination IP address must be included in the IP address range of the corresponding protection group.
Destination Port	TCP port of the server.
SYN COOKIE URL	Controls whether to enable **SYN COOKIE URL**. • If **SYN COOKIE URL** is enabled, a client attempting to access a server can access the server only after being authenticated by the ADS device, to protect the server from SYN cookie attacks. • Whether **SYN COOKIE URL** is enabled determines the number of

Parameter	Description
	available options for the **Algorithm** parameter. • Whether **SYN COOKIE URL** is enabled depends on whether **SYN COOKIE URL** is enabled for HTTP protection.
Algorithm	Protection algorithm for packets that match URL rules. This parameter is used in conjunction with **SYN COOKIE URL**. If **SYN COOKIE URL** is enabled, you can choose from algorithm 2 through 8; if **SYN COOKIE URL** is disabled, you can only choose from algorithm 0 through 5.

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

- Modify a URL rule.

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

- Delete a URL rule.

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

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

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

----End

4.1.2.2 Viewing Protection Groups

On the protection group list as shown in Figure 4-18, click the name of a protection group to view details. See Figure 4-25.

Figure 4-25 Viewing details of a protection group

Policies ▸ Anti-DDoS ▸ Protection Groups

Protection Groups

Group [hytest]

Item	Value
Group Name	hytest
Group Description	123

IP List [hytest]

86.43.21.2-86.43.21.2
86:86:86:10::2-86:86:86:10::2

DDoS -- [hytest]

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

HTTP Keyword Checking Policy [hytest]

Select	Enable	Rule	Description	Source IP	Action
Disable	Yes				

Port Check-- [hytest]

Port Check Protection	Port List
Disable	

HTTP Protection Policy--[hytest]

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

4.1.2.3 Editing a Protection Group

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

- Edit the IP address range of a protection group.

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

  After editing the IP address range, click **OK** to save the settings. Click **Next** to edit policies.

- Edit policies for a protection group.

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

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

- Edit URL rules for a protection group.

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

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

4.1.2.4 Deleting a Protection Group

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

- Method 1: On the protection group list shown in Figure 4-18, click to the right of a protection group and click **OK** in the confirmation dialog box to delete the protection group.
- Method 2: On the protection group list shown in Figure 4-18, select the protection groups (or select the **Select All** check box to select all protection groups) to be deleted, click **Delete** to the lower right of the protection group list, and then click **OK** in the confirmation dialog box to delete the selected protection groups.

Note	After a protection group is deleted, clients resort to default anti-DDoS policies, instead of using policies of the protection group.

4.1.3 Advanced Global Parameters

You can configure trust control parameters.

The procedure is as follows:

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

Step 2 Click **Edit** and configure the length of time an IP address is trusted based on the protection algorithm on the page shown in Figure 4-26.

Figure 4-26 Advanced Global Parameters page

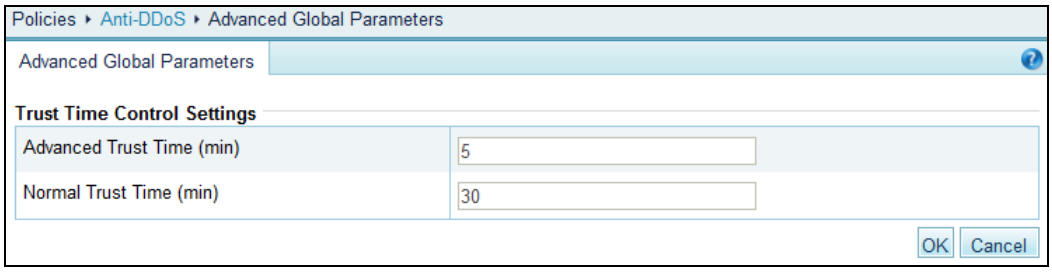


Table 4-15 describes advanced global parameters.

Table 4-15 Advanced global parameters

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

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

----End

4.1.4 Response Page Settings

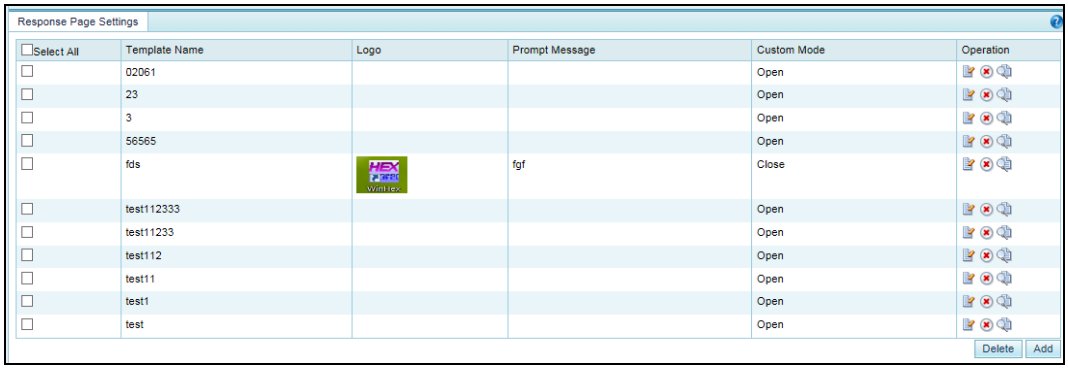
This section describes how to create, edit, delete, and preview response pages. If **4-BMP image authentication** is specified as the algorithm for the HTTP protection policy and a template is specified, a client attempting to access a server through ADS needs to input a code for authentication in the 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.

4.1.4.1 Creating a Response Page

To create a response page, perform the following steps:

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

Figure 4-27 Response Page Settings tab page



Step 2 Click **Add**.

The **Response Page Settings** page appears, as shown in Figure 4-28.

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 4-28 Response Page Settings page

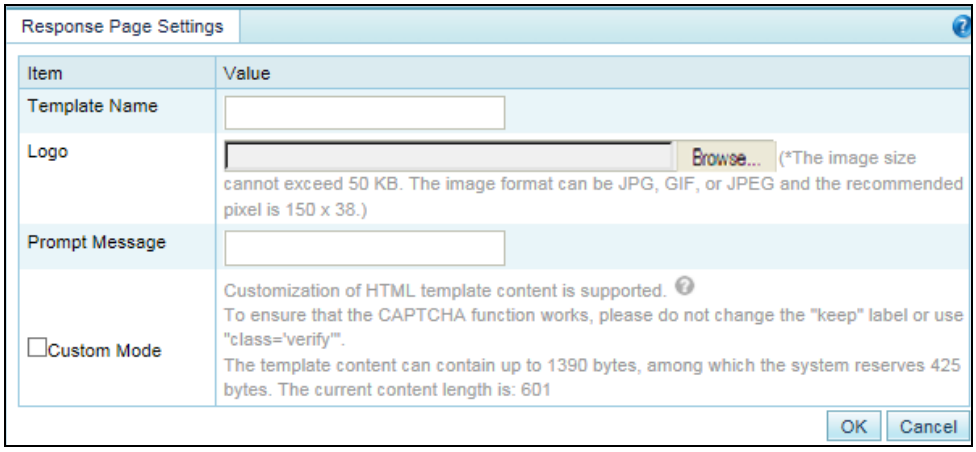


Table 4-16 describes parameters for creating a response page.

Table 4-16 Parameters for creating a response page

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

Step 3 Click **Browse** and select an image.

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

----End

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

4.1.4.2 Editing a Response Page

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

Step 1 On the page shown in Figure 4-27, click in the row of a response page.

Step 2 On the page for editing response page parameters, configure parameters of the response page, and then click **OK** to save settings and return to the response page list.

----End

4.1.4.3 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 4-27, click in the row 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 4-27, select one or more response pages (or select the **Select All** check box to select all response pages), click **Delete** in the lower-right corner of the tab page, and then click **OK** in the confirmation dialog box to delete selected response pages.

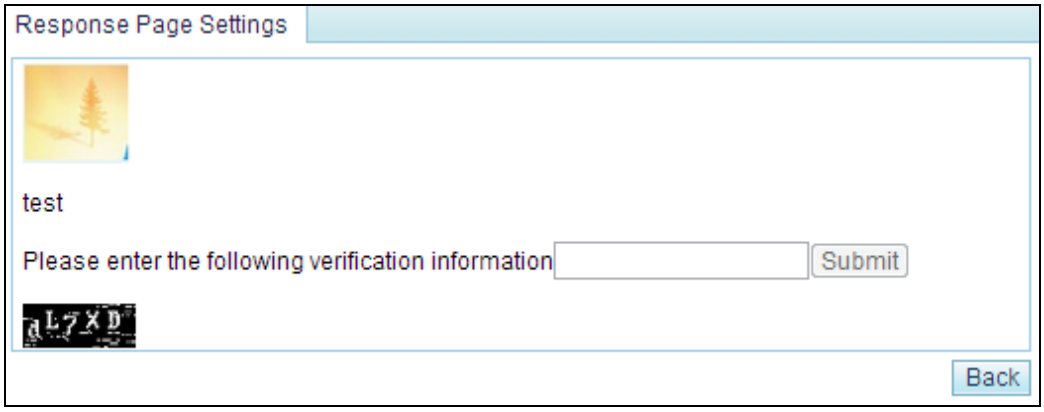
4.1.4.4 Previewing a Response Page

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

Step 1 On the tab page shown in Figure 4-27, click in the row of a response page.

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

Figure 4-29 Response page preview



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

----End

4.1.5 Policy Auto-Learning

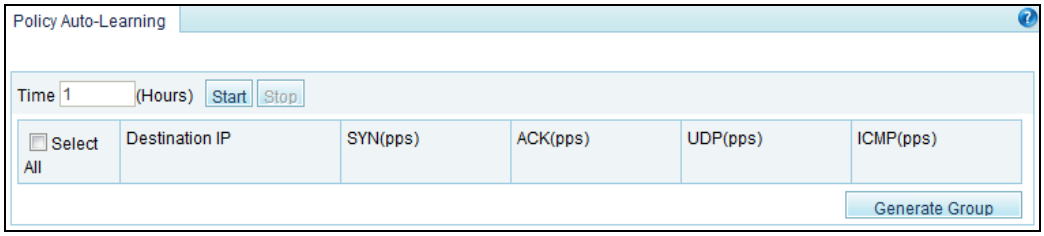
ADS supports policy auto-learning. This means ADS can collect and analyze statistics on normal SYN, ACK, UDP, and ICMP packets, generate protection policies based on built-in algorithms, and create protection group templates.

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

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

The **Policy Auto-Learning** page appears, as shown in Figure 4-30.

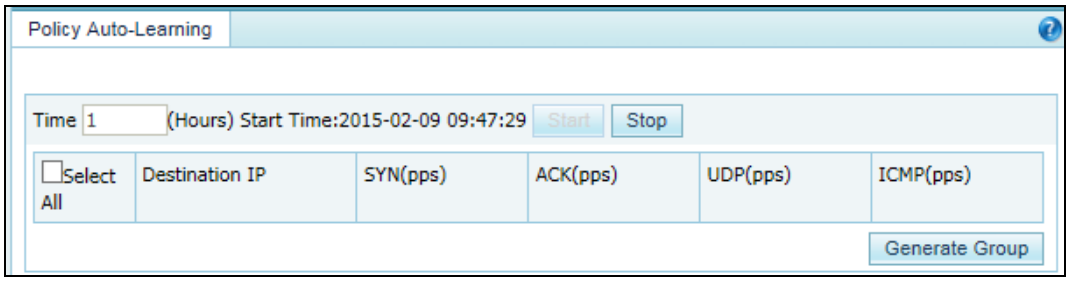
Figure 4-30 Policy Auto-Learning page



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

ADS starts to collect statistics, as shown in Figure 4-31.

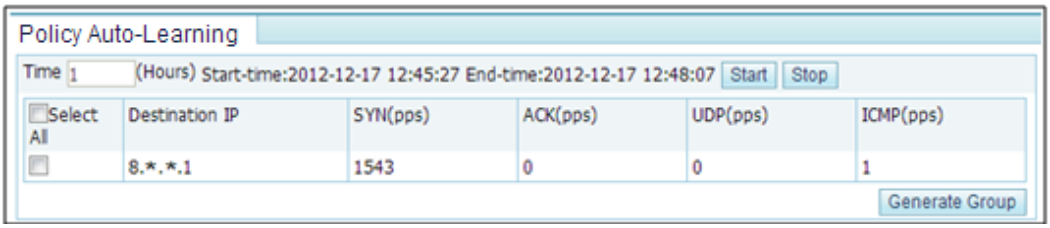
Figure 4-31 Starting learning



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

ADS automatically displays a learning record on the **Policy Auto-Learning** page, as shown in Figure 4-32. A learning record contains the destination IP address, SYN packet rate, ACK packet rate, UDP packet rate, and ICMP packet rate in pps.

Figure 4-32 Auto-learning record



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

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

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

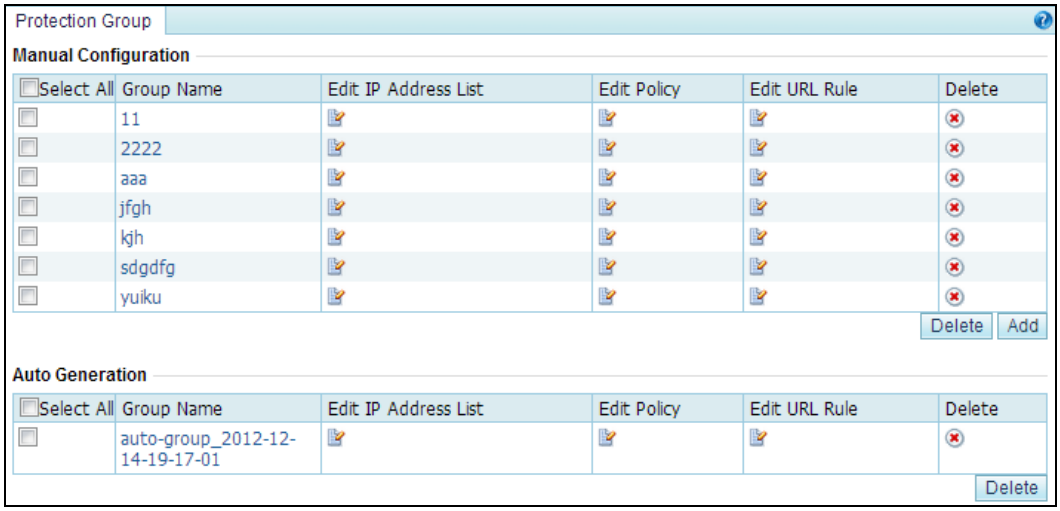
The **Protection Groups** page appears, as shown in Figure 4-33.

You can view, edit, and delete the automatically generated protection group in the **Auto Generation** list. By default, automatically generated protection groups are named in the **auto-group_***N* format. *N* indicates the generation time. For example, 2012-12-04-14-58-41

indicates that the generation time is 14: 58:41 on December 4, 2012. For how to configure protection groups, see section 4.1.2 Protection Groups.

Note	If a protection group cannot be generated based on the learning record due to a conflict with existing groups, the page shown in Figure 4-32 will display the conflicting protection groups.

Figure 4-33 Viewing automatically generated protection groups



----End

4.2 Access Control Policies

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

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

4.2.1 Access Control Rules

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

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

- Rules are divided into zero node rules and non-zero node rules.
- The destination IP address of 0.0.0.0 is taken as a zero node by default; others are non-zero nodes.
- Zero node rules have a higher priority than non-zero node rules.
- Nodes that have the same destination IP address are the same node. For the same node, rules that do not have ports are preferred over those that have ports.
- Non-zero node rules are automatically sorted according to the time they are added.

This section covers the following topics:

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

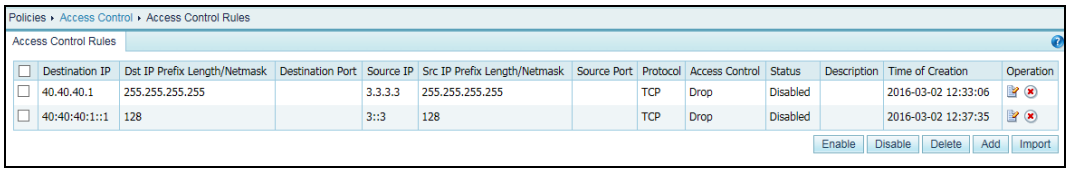
4.2.1.1 Creating an Access Control Rule

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

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

Initially, the rule list is empty.

Figure 4-34 List of access control rules



Step 2 Click **Add**.

Figure 4-35 Creating an access control rule

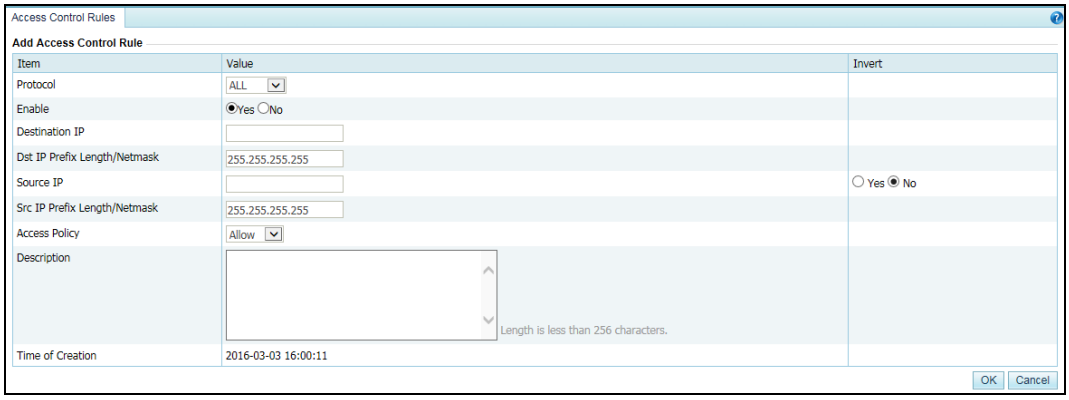


Table 4-17 describes parameters for creating an access control rule.

Table 4-17 Parameters for creating an access control rule

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

Parameter	Description
Time of Creation	Time automatically 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 can be used as the source IP address.

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

----End

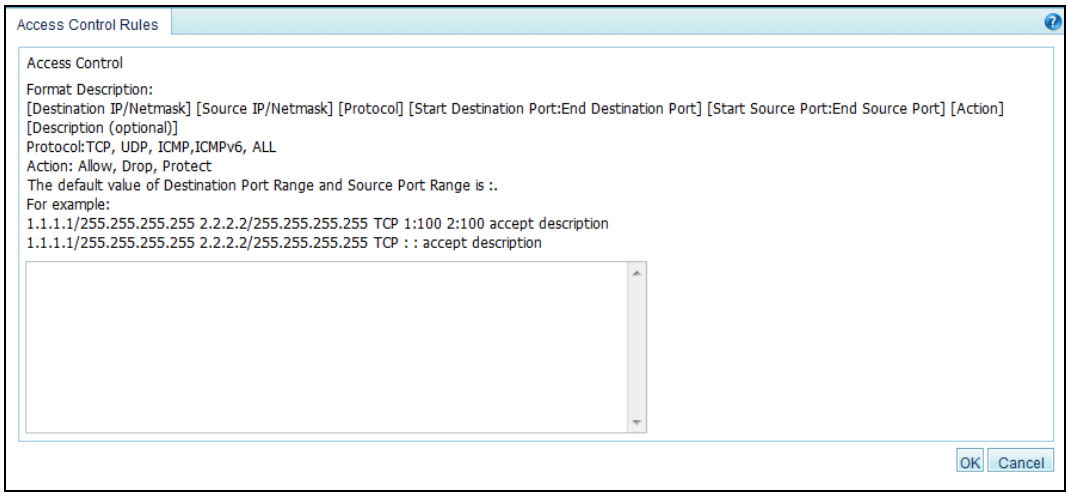
4.2.1.2 Creating Access Control Rules in Batches

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

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

Step 2 Click **Import**.

Figure 4-36 Creating access control rules in batches



Step 3 Type multiple access control rules as prompted.

Pay attention to the following format specifications:

- [Destination IP/Subnet Mask] [Source IP/Subnet Mask] [Protocol] [Start of Destination Port:End of Destination Port] [Start of Source Port:End of Source Port] [Action]
- Protocol: **TCP**, **UDP**, **ICMP**, **ICMPv6**, and **All**.
- Action: **Allow**, **Drop**, and **Protect**.
- If the value range of **Destination Port** and **Source Port** is not defined, the semicolon (:) is used to replace their values by default.

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

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

----End

4.2.1.3 Enabling/Disabling Access Control Rules

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

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

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

Enabling Access Control Rules

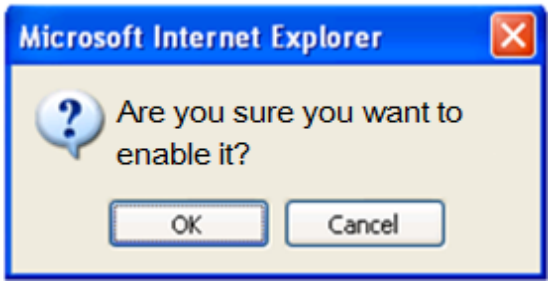
To enable access control rules, perform the following steps:

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

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

A dialog box appears, as shown in Figure 4-37.

Figure 4-37 Enabling access control rules



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

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

----End

Disabling Access Control Rules

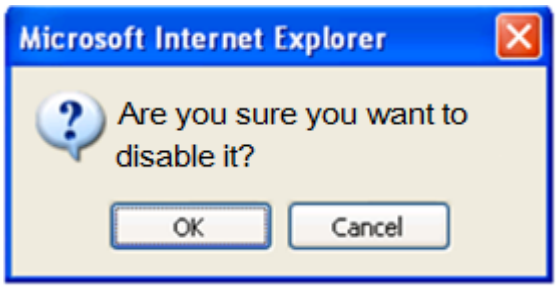
To disable access control rules, perform the following steps:

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

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

The following dialog box appears, as shown in Figure 4-38.

Figure 4-38 Disabling access control rules



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

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

----End

4.2.1.4 Editing an Access Control Rule

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

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

Step 2 Click to edit rule parameters.

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

----End

4.2.1.5 Deleting Access Control Rules

The administrator can delete one access control rule or multiple rules in batches on the ADS device by adopting either of the following methods:

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

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

4.2.2 GeoIP Rules

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

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

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

This section covers the following topics:

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

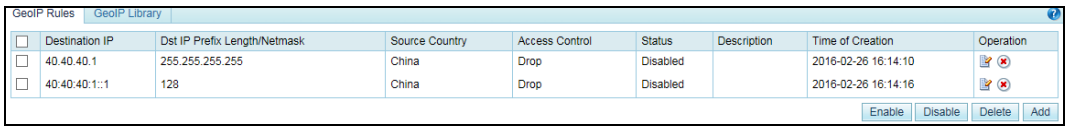
4.2.2.1 Creating a GeoIP Rule

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

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

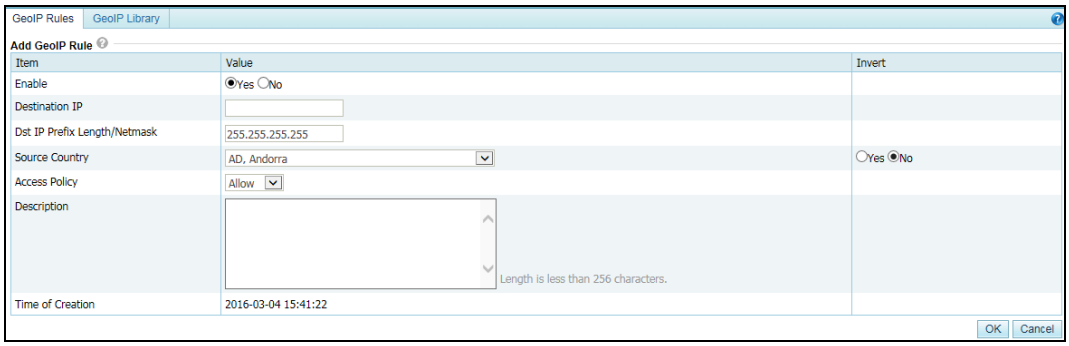
The **GeoIP Rules** page appears, as shown in Figure 4-39.

Figure 4-39 List of GeoIP rules



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

Figure 4-40 Creating a GeoIP rule



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

Table 4-18 Parameters for creating a GeoIP rule

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

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

----End

In addition to creating a GeoIP rule, you can enable, disable, edit, and delete such a rule. The procedures are the same as those for access control rules. For details, see related descriptions in section 4.2.1 Access Control Rules.

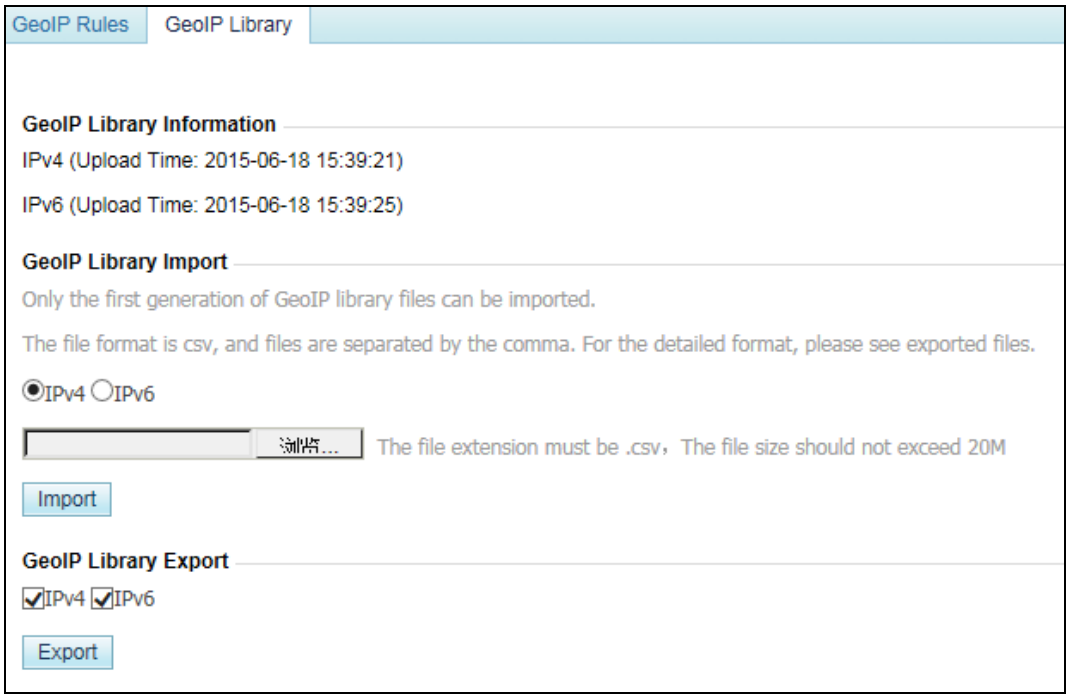
4.2.2.2 Importing and Exporting a GeoIP Library

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

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

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

Figure 4-41 Viewing the GeoIP library



Step 2 Import or export a GeoIP library.

- Importing a GeoIP library

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

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

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

- Exporting a GeoIP library

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

----End

4.2.3 Regular Expression Rules

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

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

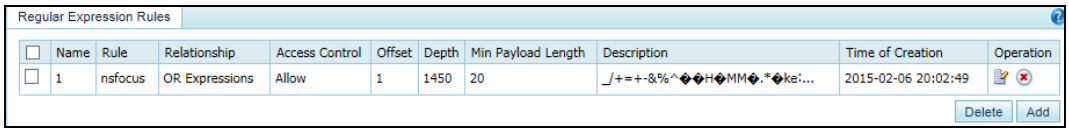
A regular expression rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting a regular expression rule are the same as those for access control rules.

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

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

Initially, the rule list is empty.

Figure 4-42 List of regular expression rules



Step 2 Click **Add**.

Figure 4-43 Creating a regular expression rule

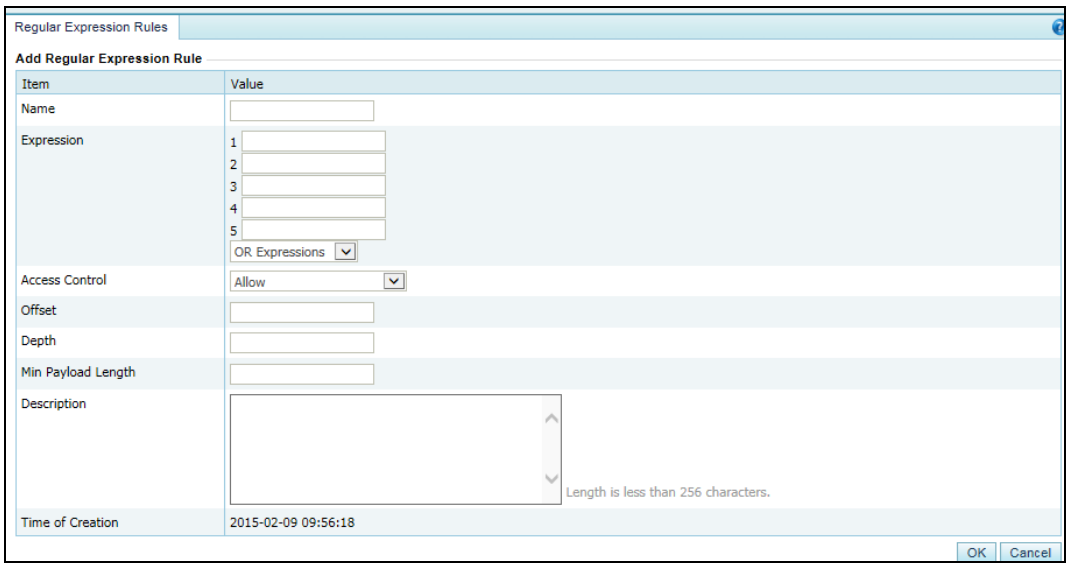


Table 4-19 describes parameters for creating a regular expression rule.

Table 4-19 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 5 expressions and then select **OR Expressions** or **AND Expressions**.
Access Control	Specifies the action the ADS device takes for packets with specified signatures. It has the following values: • **Allow**: allows such packets to pass through. • **Drop**: drops such packets once they are detected. • **Drop and add to blacklist**: drops such packets and adds their source IP addresses to the blacklist. Before selecting this option, you must enable the blacklist. For details on the blacklist, see section 4.2.8 Blacklist. • **Drop and disconnect**: drops such packets and disconnects the connection to

Parameter	Description
	their destination IP addresses.
Offset	Payload offset, counted from the first byte in the payload field of a TCP packet.
Depth	Specifies how deep the rule is matched. It is expressed in bytes.
Min Payload Length	Length of the payload below which the packet is not matched with regular expression rules. This does not affect subsequent protection actions.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

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

----End

4.2.4 DNS Keyword Checking

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

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

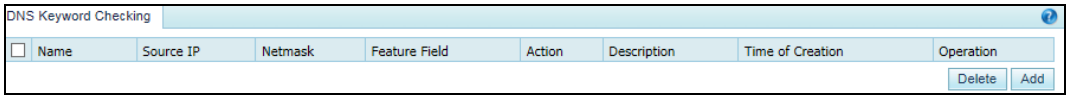
A DNS keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting DNS keyword checking rules are the same as those for access control rules.

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

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

Initially, the rule list is empty.

Figure 4-44 List of DNS keyword checking rules



Step 2 Click **Add**.

Figure 4-45 Creating a DNS keyword checking rule

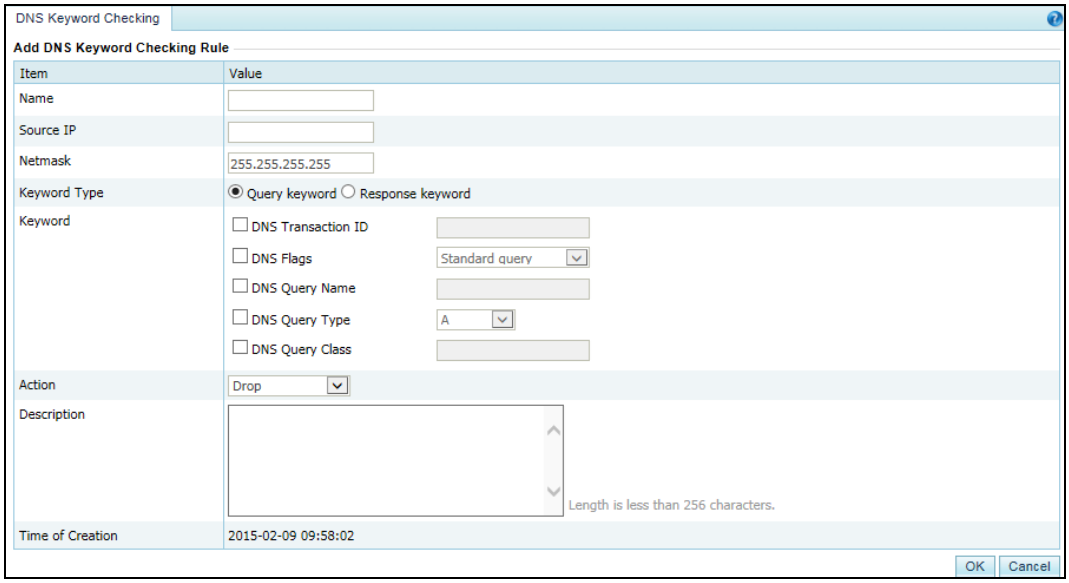


Table 4-20 describes parameters for creating a DNS keyword checking rule.

Table 4-20 Parameters for creating 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.
Description	Brief description of the rule.
Source IP	Specifies the source IP address. The value **0.0.0.0** indicates all source IP addresses.
Netmask	Specifies the netmask of the source IP address.
Keyword Type	Specifies what kind of packets will be checked. Options include **Query keyword** and **Response keyword**.
Keyword	Specifies the type of keywords to be checked. You can select one or more.
Action	Specifies the action to be taken against a packet that matches a DNS keyword checking rule. It can be any of the following: • **Allow**: indicates that a packet with the specified signature will be allowed through ADS and, after that, will not be checked against any pattern matching rules. • **Drop**: indicates that ADS drops a packet with the specified signature. • **Drop+Blacklist**: indicates that ADS drops a packet with the specified signature and adds its source IP address to the blacklist. To select this option, you must enable the blacklist function in advance. For details about this function, see section 4.2.8 Blacklist. • **Allow+Whitelist**: indicates that ADS allows a packet with the specified signature to pass through and adds its IP address to the whitelist. To select this option, you must enable the whitelist function in advance. For details about this function, see section 4.2.9 Whitelist.

Parameter	Description
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

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

----End

4.2.5 HTTP Keyword Checking

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

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

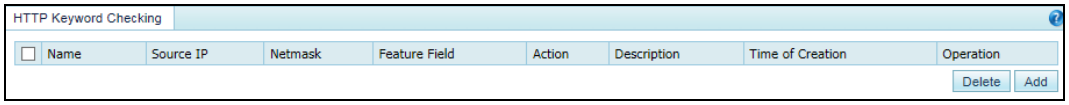
An HTTP keyword checking rule can be added, edited, and deleted. This document describes only how to add such a rule, as methods for editing and deleting HTTP keyword checking rules are the same as those for access control rules.

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

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

Initially, the rule list is empty.

Figure 4-46 List of HTTP keyword checking rules



Step 2 Click **Add**.

Figure 4-47 Creating an HTTP keyword checking rule

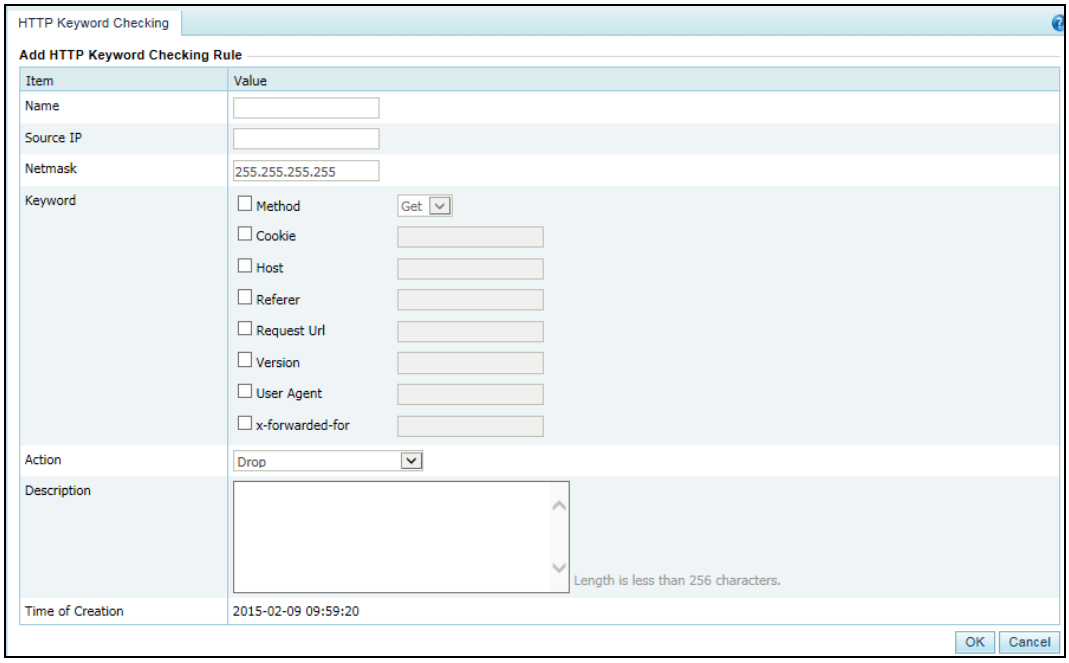


Table 4-21 describes parameters for creating an HTTP keyword checking rule.

Table 4-21 Parameters for creating 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.
Description	Brief description of the rule.
Source IP	Specifies the source IP address. The value **0.0.0.0** indicates all source IP addresses.
Netmask	Specifies the netmask of the source IP address.
Keyword	Specifies the type of keywords to be checked. You can select one or more.
Action	Specifies the action to be taken against a packet that matches an HTTP keyword checking rule. It can be any of the following: • **Allow**: indicates that a packet with the specified signature will be allowed through ADS. • **Drop**: indicates that ADS drops a packet with the specified signature. • **Drop+Blacklist**: indicates that ADS drops a packet with the specified signature and adds its source IP address to the blacklist. To select this option, you must enable the blacklist function in advance. For details about this function, see section 4.2.8 Blacklist. • **Drop+Disconnect**: indicates ADS drops a packet with the specified signature and disconnects the current connection. • **Drop+Blacklist+Disconnect**: indicates that ADS drops a packet with the specified signature, disconnects the current connection, and adds its source IP address to the blacklist. To select this option, you must enable the blacklist function in advance.

Parameter	Description
	• **Allow+Whitelist**: indicates that ADS allows a packet with the specified signature to pass through and adds its source IP address to the whitelist. To select this option, you must enable the whitelist function in advance. For details about this function, see section 4.2.9 Whitelist.
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

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

----End

4.2.6 Connection Exhaustion Rules

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

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

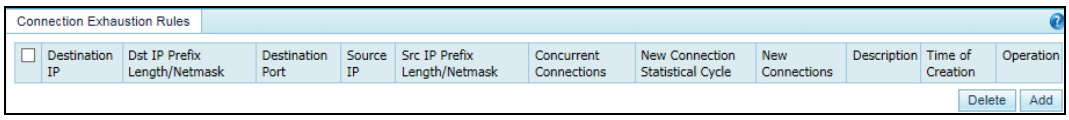
4.2.6.1 Creating a Connection Exhaustion Rule

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

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

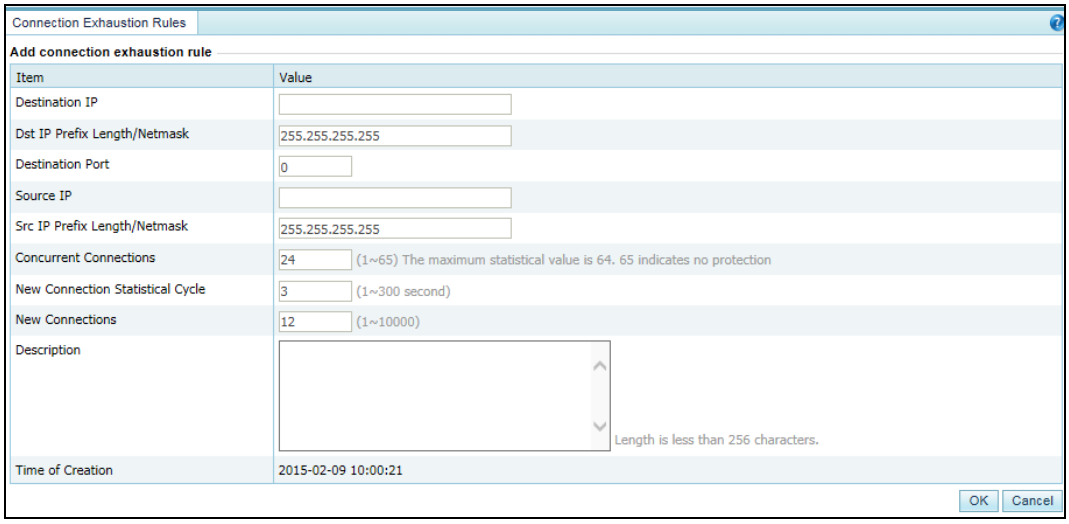
Initially, the rule list is empty.

Figure 4-48 List of connection exhaustion rules



Step 2 Click **Add**.

Figure 4-49 Creating a connection exhaustion rule



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

Table 4-22 describes parameters for creating a connection exhaustion rule.

Table 4-22 Parameters for creating a connection exhaustion rule

Parameter	Description
Destination IP	IP address of the server to be protected. You can type an IPv4 or IPv6 address according to the actual network deployment.
Dst IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address of the server to be protected.
Destination Port	Server ports to be protected. The port number ranges from 0 to 65535.
Source IP	Client IP address to be protected. You can type IPv4 or IPv6 addresses according to the actual network deployment.
Src IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the client IP address.
Connections	Maximum number of connections allowed for each source IP address. The maximum value is **2048** and the recommended value is **60**. The value **0** indicates that the source IP address is not allowed to connect to the specified IP address.
Lockout Period	A specified period (unit: second), in which the ADS device stops the source IP address from accessing the destination IP address because the number of connections from a source IP address exceeds the threshold.
New Connections per Second	Maximum number of new connections that can be established per second for the source IP address satisfying this rule. The value ranges from 1 to 10000. The default value is **1000**.
Description	Presents description of the rule, which cannot contain more than 256 characters.

Parameter	Description
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

4.2.6.2 Editing a Connection Exhaustion Rule

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

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

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

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

----End

4.2.6.3 Deleting Connection Exhaustion Rules

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

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

4.2.7 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

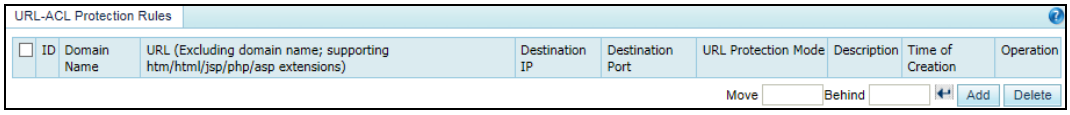
4.2.7.1 Creating a URL-ACL Protection Rule

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

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

Initially, the rule list is empty.

Figure 4-50 List of URL-ACL rules



Step 2 Click **Add**.

Figure 4-51 Adding a URL-ACL rule

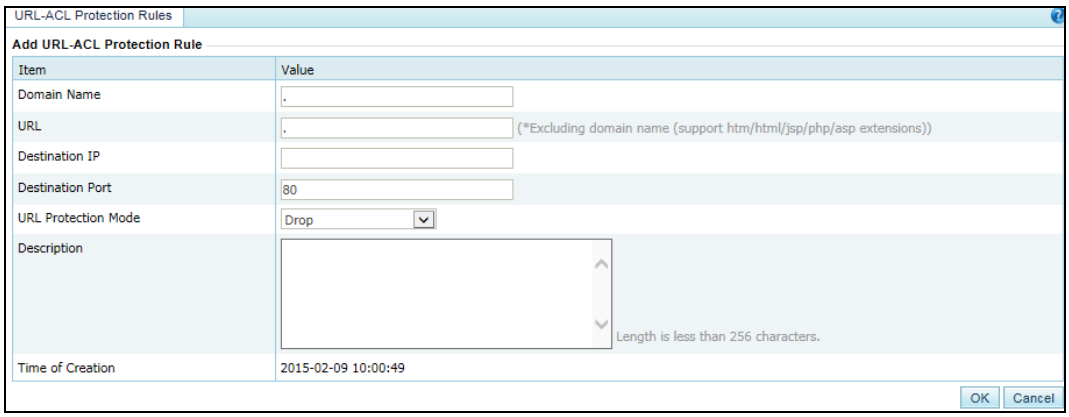


Table 4-23 describes parameters for creating a URL-ACL rule.

Table 4-23 Parameters for creating a URL-ACL rule

Parameter	Description
Domain Name	Domain name of a URL protection object. The symbol "." indicates that this rule is valid for all domain names.
URL	Relative path of a URL protection object, that is, URL excluding the domain name. The symbol "." indicates that this rule is valid for all URLs.
Destination IP	IP address of the server. You can type an IPv4 or IPv6 address according to the actual network deployment.
Destination Port	TCP port of the server.
URL Protection Mode	Action to be taken on packets that match this rule. The value can be one of the following: • **Drop**: drops packets. • **Trust**: allows packets to pass. • **Block proxy**: blocks the proxy if it is possible to use the proxy to transfer packets. • **Limit source IP speed**: limits the rate at which packets from the source IP address are forwarded.
Threshold	Maximum rate at which packets are forwarded. The value ranges from 1 to 10000, in pps. ADS drops packets failing to be sent in the case of the maximum rate. This parameter is available only when **URL Protection Mode** is set to **Limit source IP speed**.

Parameter	Description
Description	Presents description of the rule, which cannot contain more than 256 characters.
Time of Creation	Time automatically generated by the system on the creation of the rule. It cannot be edited.

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

----End

4.2.7.2 Editing a URL-ACL Protection Rule

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

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

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

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

----End

4.2.7.3 Deleting a URL-ACL Protection Rule

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

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

4.2.7.4 Changing the Priority of a URL-ACL Protection Rule

On the **URL-ACL Protection Rule** page, the administrator 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 .

4.2.8 Blacklist

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

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

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

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

- Once attack packets are filtered out through pattern matching, the source IP address of such packets is automatically added to the blacklist. For description of pattern matching, see section 8.2 Pattern Matching Rules.
- If **Add Abnormal IP to Blacklist** is set to **Yes**, you can also add source IP addresses that fail the HTTP keyword check to the blacklist.
- If **Add Abnormal IP to Blacklist** is set to **Yes**, you can also add source IP addresses that fail the DNS keyword check to the blacklist.
- If the number of new connections from a source IP address exceeds the threshold within the new connection statistical cycle of a connection exhaustion rule, ADS deems this IP address abnormal and automatically adds it to the blacklist.
- When **URL Protection Mode** is set to **Drop** for URL-ACL rules, the ADS device adds the source IP to the blacklist once detecting an HTTP request in IP packets and matching the source IP address with a URL-ACL rule.
- When **URL Protection Mode** is set to **Block proxy** for URL-ACL rules, the ADS device adds the IP address of the proxy server to the blacklist when detecting an HTTP request from the proxy server in packets and matching the source IP address with a URL-ACL rule.
- After **Slow attack protection** is triggered, if the blacklist function is enabled, the system automatically adds source IP addresses of matching packets to the blacklist.
- After a TCP control policy is triggered, if **Bandwidth Limit of SYN Source IP** is set to **Drop and add to blacklist**, the system adds the source IP address of corresponding packets to the blacklist.
- If **Access Control** or **Empty Connection Check** is set to **Drop and add to blacklist**, you can also add source IP addresses that fail the HTTP keyword check to the blacklist.
- If **Access Control** or **Empty Connection Check** is set to **Drop and add to blacklist**, you can also add source IP addresses that fail the DNS keyword check to the blacklist.
- After a TCP regular expression rule is triggered, the system adds the source IP address that matches the regular expression rule to the blacklist.

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

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

You can perform the following operations regarding the blacklist:

- Enabling and Disabling the Blacklist Function
- Adding a Blacklist Entry
- Viewing Blacklist Entries

- Deleting Blacklist
- Clearing Blacklist
- Searching the Blacklist
- Importing a Blacklist File
- Viewing the Import Result
- Exporting a Blacklist File

Enabling and Disabling the Blacklist Function

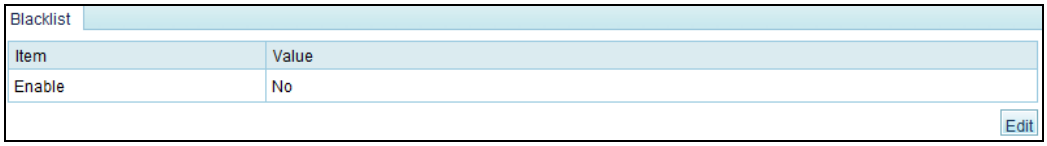
Enabling the Blacklist Function

To enable the blacklist function, perform the following steps:

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

Initially, the blacklist function is disabled.

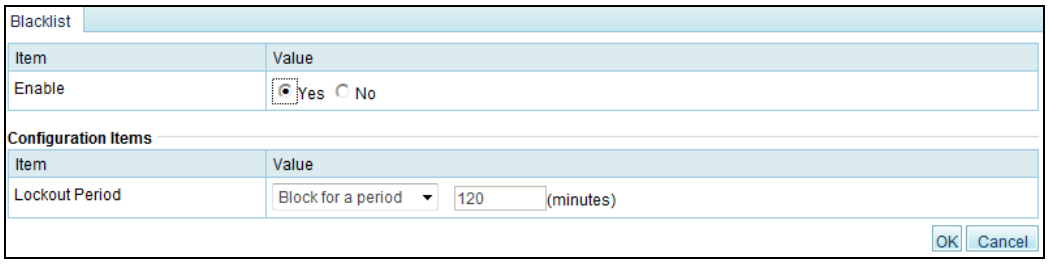
Figure 4-52 Blacklist status



Step 2 Click **Edit** and then select **Yes** to enable the blacklist function. See Figure 4-53.

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

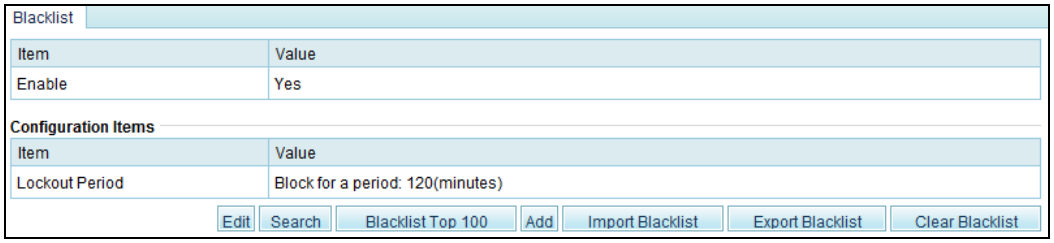
Figure 4-53 Enabling the blacklist policy



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

As shown in Figure 4-54, the blacklist function is enabled and blacklist configuration items are available.

Figure 4-54 Blacklist function enabled



----End

Disabling the Blacklist Function

To disable the blacklist function, perform the following steps:

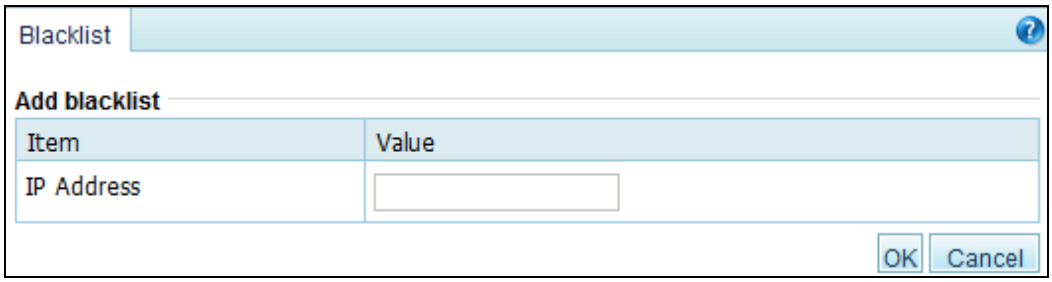
On the page shown in Figure 4-53, select **No**. Then the value of **Enable** turns to **No**, as shown in Figure 4-52.

Adding a Blacklist Entry

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

Step 1 On the page shown in Figure 4-54, click **Add** to add a blacklist entry.

Figure 4-55 Adding a blacklist entry



Step 2 On the page shown in Figure 4-55, type the source IP address (IPv4 address only) of packets to be blocked, and then click **OK** to save the settings.

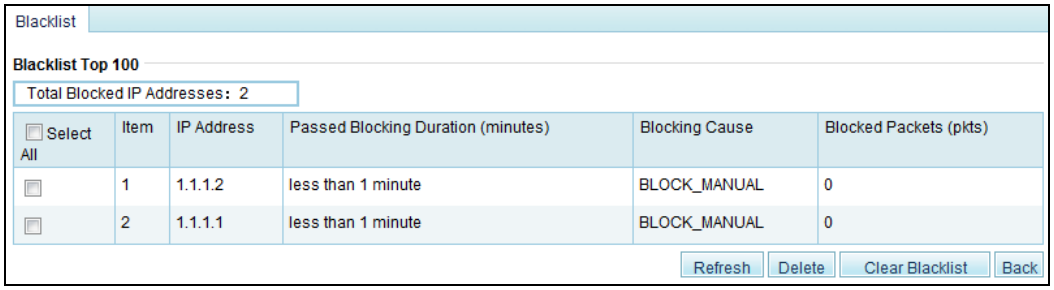
----End

Viewing Blacklist Entries

On the page shown in Figure 4-54, click **Blacklist Top 100**. The system displays a maximum of 100 IP addresses blocked recently, as shown in Figure 4-56.

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

Figure 4-56 Viewing blacklist entries



Deleting Blacklist Entries

To delete a blacklist entry, perform the following steps:

Step 1 On the page shown in Figure 4-56, select one or more blacklist entries and then click **Delete**.

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

----End

Clearing Blacklist Entries

To clear blacklist entries, perform the following steps:

Step 1 On the page shown in Figure 4-54 or Figure 4-56, click **Clear Blacklist**.

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

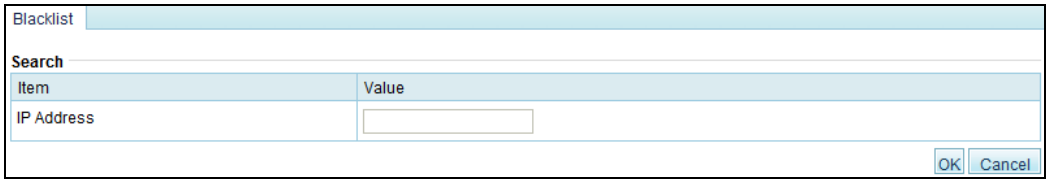
----End

Searching the Blacklist

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

Step 1 On the page shown in Figure 4-54, click **Search**.

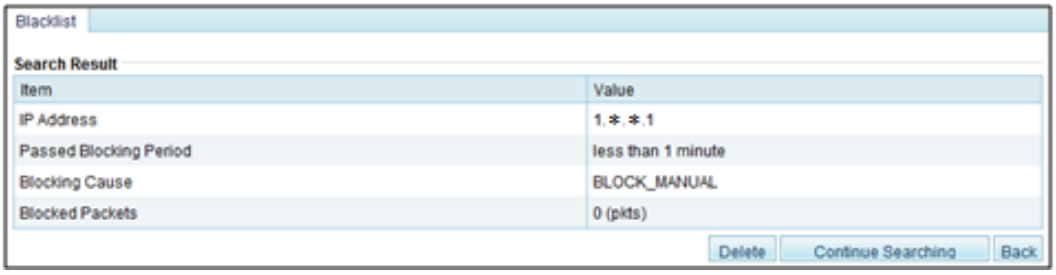
Figure 4-57 Searching for an IP address



Step 2 On the **Search** page shown in Figure 4-57, type an IP address, and click **OK**.

The blacklist search result is displayed, as shown in Figure 4-58.

Figure 4-58 Blacklist search result



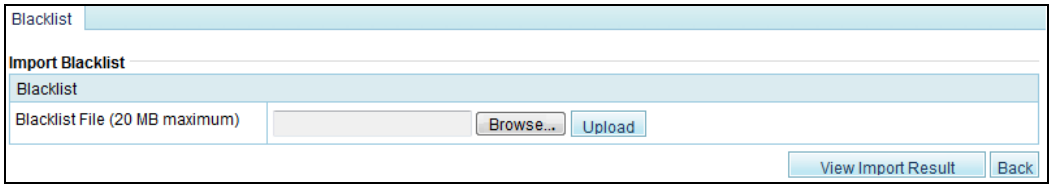
----End

Importing a Blacklist File

To import a blacklist file, perform the following steps:

Step 1 On the page shown in Figure 4-54, click **Import Blacklist**.

Figure 4-59 Importing a blacklist file



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

Step 2 On the page shown in Figure 4-59, click **Browse**.

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

Step 4 Click **Upload**.

After the upload is complete, the system prompts that the file is successfully imported, as shown in Figure 4-60.

Figure 4-60 Import success prompt

After the blacklist file is imported, the system automatically switches to the page shown in Figure 4-59.

----End

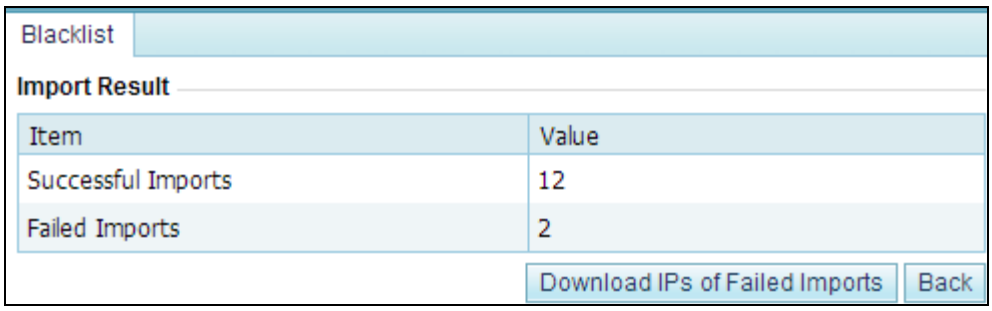
Viewing the Import Result

To view the import result, perform the following steps:

Step 1 On the page shown in Figure 4-59, 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 4-61.

Figure 4-61 Viewing import results



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

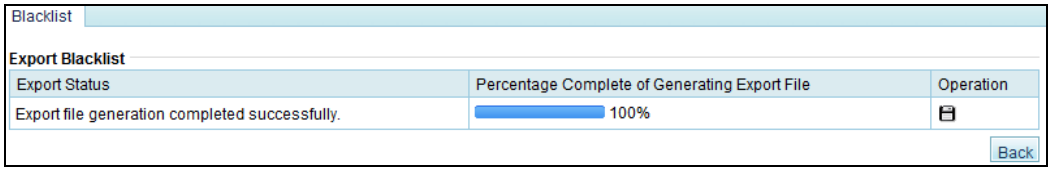
----End

Exporting a Blacklist File

To export a blacklist file, perform the following steps:

Step 1 On the page shown in Figure 4-54, click **Export Blacklist**.

Figure 4-62 Exporting a blacklist file



Step 2 On the Export Blacklist page shown in Figure 4-62, click .

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

The blacklist file is thus saved to the local disk.

----End

4.2.9 Whitelist

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

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

You can perform the following operations regarding the whitelist:

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

Enabling and Disabling the Whitelist Function

By default, the whitelist function is disabled on the ADS device. The administrator needs to enable this function before using it.

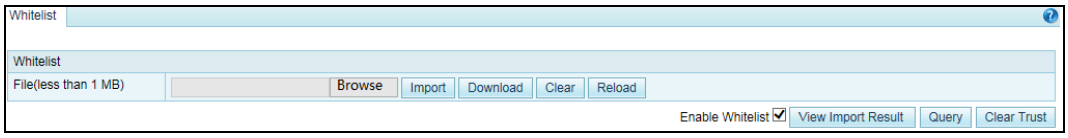
Enabling the Whitelist Function

To enable the whitelist function, perform the following steps:

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

By default, the whitelist function is disabled.

Figure 4-63 Whitelist configuration page



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

----End

Disabling the Whitelist Function

To disable the whitelist function, perform the following steps:

If the whitelist function is enabled, deselect **Enable Whitelist** to disable the whitelist, as shown in Figure 4-63.

Importing a Whitelist File

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

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

- 10.10.10.10
- 172.16.10.10
- 192.168.10.10

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

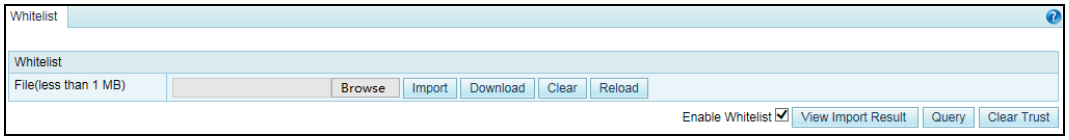
To import a whitelist file, perform the following steps:

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

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

Note that the file path in the red frame is used for illustration only.

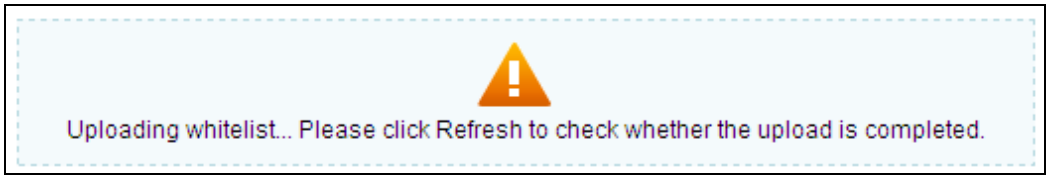
Figure 4-64 Importing the whitelist file



Step 3 Click **Import**.

A message is displayed, prompting that the import is in progress, as shown in Figure 4-65.

Figure 4-65 Import progress message



Step 4 After the whitelist file is imported, the system returns to the whitelist configuration page.

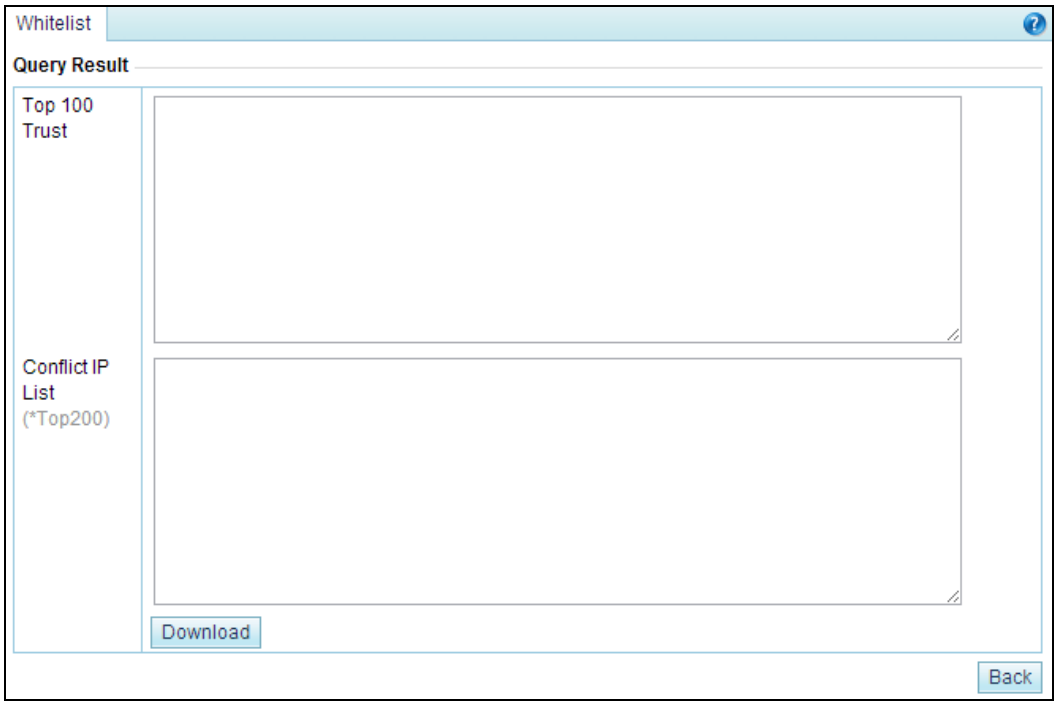
----End

Viewing the Import Result

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

Step 1 Click **View Import Result** on the whitelist configuration page in Figure 4-63 to view information that is successfully imported to the whitelist. See Figure 4-66.

Figure 4-66 Viewing the import result



TOP100 Trust shows top 100 IP addresses that are saved in the configuration file; **Conflict IP List** shows conflicting IP addresses that fail to be imported.

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

----End

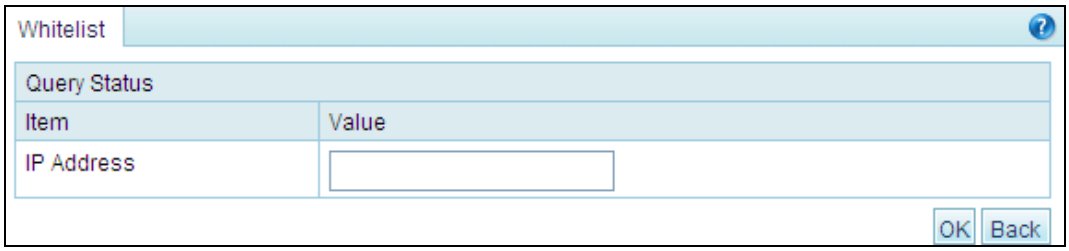
Querying the Trust Relationship

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

To query the trust relationship, perform the following steps:

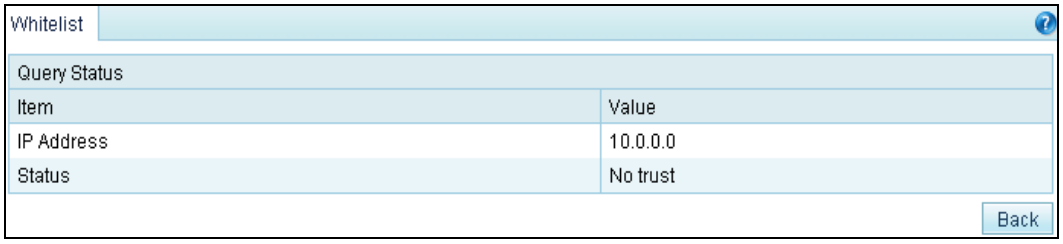
Step 1 On the whitelist configuration page in Figure 4-63, click **Query** to open the **Query Status** page.

Figure 4-67 Querying the trust relationship



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

Figure 4-68 Query result of the trust relationship



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

----End

Clearing the Trust Relationship

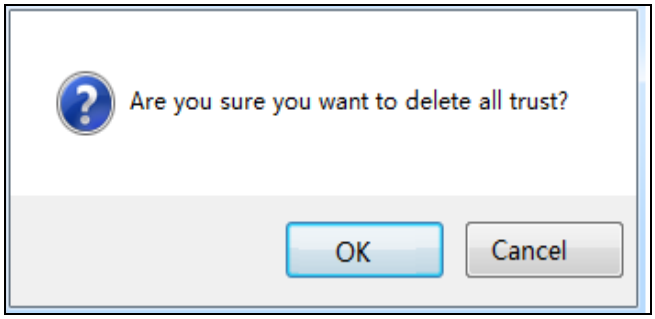
By clearing the trust relationship, you can only delete the trust status of all IP addresses listed in the whitelist on the engine, but cannot delete the whitelist file. If IP addresses in this whitelist need to be re-trusted after the trust relationship is cleared, the administrator needs to reload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

To clear the trust relationship, perform the following steps:

Step 1 Click **Clear Trust** on the whitelist configuration page in Figure 4-63.

Then, a dialog box appears, asking you whether to clear all trust relationships, as shown in Figure 4-69.

Figure 4-69 Clearing trust relationships



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

----End

Clearing the Configuration

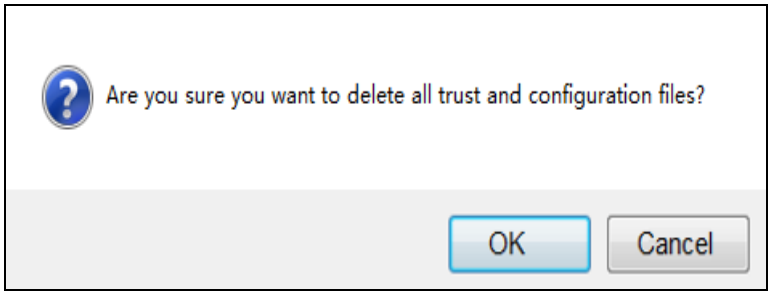
By clearing the configuration, the administrator can delete the whitelist file and trust relationships of IP addresses on the engine. You are advised to back up the whitelist file before clearing the configuration. For details, see Downloading the Configuration.

To clear the configuration, perform the following steps:

Step 1 Click **Clear** on the whitelist configuration page in Figure 4-63.

Then, a dialog box appears, asking you whether to delete the whitelist file and all trusted entries, as shown in Figure 4-70.

Figure 4-70 Clearing the configuration



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

----End

Downloading the Configuration

The administrator can download the whitelist file to the local device for backup.

To download the configuration, perform the following steps:

Step 1 Click **Download** on the whitelist configuration page in Figure 4-63.

Step 2 Click **Save** and select a file path to save the whitelist file in the path.

----End

Reloading the Whitelist File

During the reloading, the ADS device clears the list of trusted IP addresses and loads the list in the new whitelist configuration file to the engine.

Click **Reload** on the whitelist configuration page shown in Figure 4-63.

5 Diversion and Injection

This chapter provides detailed information about traffic diversion and injection.

Section	Description
General Settings	Describes how to configure the system running mode and interface IP addresses.
Diversion Route	Describes how to configure a diversion route.
Traffic Injection	Describes how to configure an injection rule.
Traffic Diversion	Describes how to configure traffic diversion information.
Advanced Route Setting	Describes how to configure an advanced route.
Syslog Diversion Configuration	Describes how to configure syslog-based traffic diversion.

Under **Diversion & Injection**, you can configure routes as well as diversion and injection rules for the ADS device in out-of-path mode. These rules can be configured only when the current running mode is **Diversion**.

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

5.1 General Settings

This section covers the following topics:

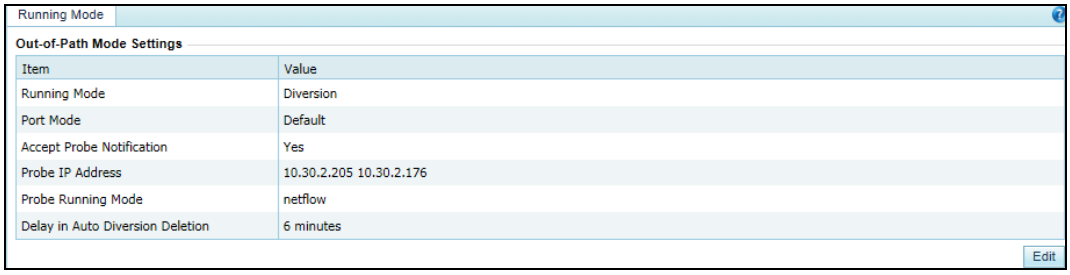
- Running Mode
- Port Channel Configuration
- GRE Tunnel Configuration
- IP Address Configuration

5.1.1 Running Mode

Under out-of-path deployment mode, you need to configure the running mode for the ADS device. The detailed procedure is as follows:

Step 1 Choose **Diversion & Injection** > **General Settings** > **Running Mode** to switch to the out-of-path deployment mode.

Figure 5-1 Running mode of the ADS device (diversion mode)



Step 2 Click **Edit** to edit parameters in out-of-path mode.

Figure 5-2 Editing the running mode of the ADS device (diversion mode)

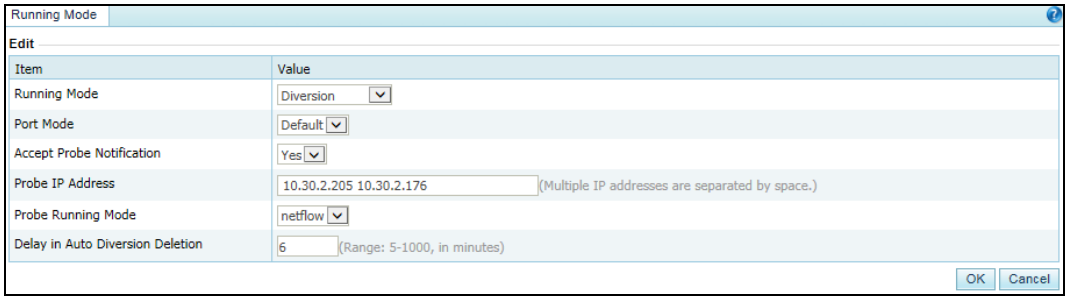


Table 5-1 describes parameters in out-of-path mode.

Table 5-1 Parameters in out-of-path mode

Parameter	Description
Running Mode	Current running mode of the ADS device. It has the following options: • **In-path**: indicates that a single ADS detection device is deployed in in-path mode. • **Diversion**: indicates that an NSFOCUS ADS detection device and multiple ADS devices are deployed in out-of-path mode. • **Cluster probe**: indicates that multiple NSFOCUS ADS detection devices are deployed in out-of-path mode. • **In-path cluster**: indicates that multiple ADS devices are deployed in in-path mode. Note

Parameter	Description
	• ADS NX5-8000 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 engineers for a new license.
Port Mode	Mode of the current port. Only **Default** is available for the ADS device.
Accept Probe Notification	Controls whether to receive notifications from the NSFOCUS ADS detection device when an attack event is detected. The value **Yes** indicates that an NSFOCUS ADS detection instructs the current ADS device to handle attacks that are detected. Note This parameter is required only when **Running Mode** is set to **Diversion**.
Probe IP Address	IP address of an NSFOCUS NTA or ADS M that coordinates with the ADS device. You can type one or more IP addresses separated by spaces. Note • This parameter is required only when Running Mode is set to Diversion. • Currently, NSFOCUS NTA is an IPv4-only device, while NSFOCUS ADS M supports both IPv4 and IPv6.
Probe Running Mode	Running mode of NSFOCUS ADS detection devices. It has the following values: • **netflow**: indicates that NSFOCUS ADS detection devices check the traffic output by the router in netflow format for abnormal traffic. • **span**: indicates that NSFOCUS ADS detection devices check mirrored traffic for abnormal traffic. Note This parameter is required only when **Running Mode** is set to **Diversion**.
Delay in Auto Diversion Deletion	After receiving a deletion diversion notification, ADS deletes the diversion after an automatic delay. The value ranges from 5 to 1000, in minutes. If ADS receives a diversion deletion notification, and then receives a diversion setup notification before **Delay in Auto Diversion Deletion** expires, ADS automatically ignores the diversion deletion notification and continues divert traffic.

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

----End

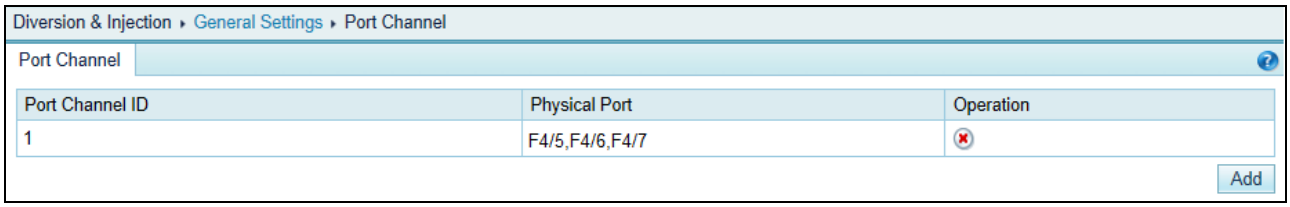
5.1.2 Port Channel Configuration

The Port channel allows a combination of arbitrary available interfaces on the device. The MAC address of the port channel is that of the interface with the smallest ID. For example, after G1/1 and G1/2 interfaces of ADS NX5-4020 are combined into a port channel, the MAC address of the port channel is that of the G1/1 interface.

Note	The number and names of ports are different for different ADS series, but have the same procedure for configuring the port channel. This section uses ADS NX5-4020 as an example to describe how to configure the port channel.

Choose **Diversion & Injection** > **General Settings** > **Port Channel** to open the port channel configuration page. See Figure 5-3.

Figure 5-3 Port channel configuration



Adding a Port Channel

Currently, only ports of the same type can be added to a port channel, for example, 1000M electrical ports and 1000M optical ports cannot be merged into one port channel. The same is true for 1000M and 10G optical ports. To the lower right of the port channel list shown in Figure 5-3, click **Add**. The **Add Port Channel Interface** page appears, as shown in Figure 5-4.

Figure 5-4 Adding a port channel for the ADS device

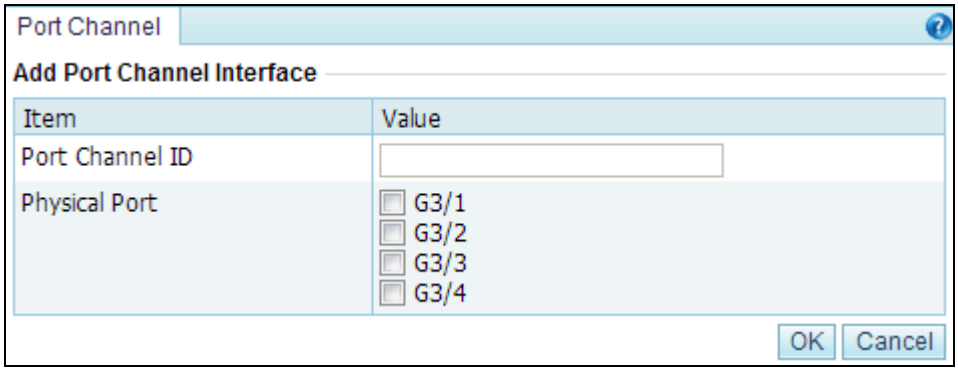


Table 5-2 describes parameters of a port channel.

Table 5-2 Parameters of a port channel

Parameter	Description
Port Channel ID	ID of the port channel. The value is an integer ranging from 0 to 31.
Physical Port	Available physical ports on the current ADS device. Note

Parameter	Description
	A port channel has one or several port IDs, but each port ID can be included in only one port channel.

Deleting a Port Channel

On the port channel list in Figure 5-3, click to delete a port channel.

Note	The port channel being used cannot be deleted.

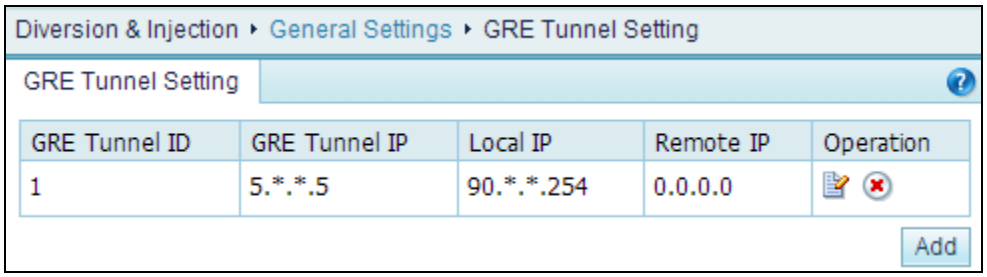
5.1.3 GRE Tunnel Configuration

GRE tunnel accomplishes data communication between two private networks. When one intranet is reachable for another via a route, the GRE tunnel encapsulates intranet packets (directed towards an intranet IP address in the other network) in IP packets on routes by default and sends them. On arriving at the peer IP address, the packets will be automatically decapsulated and then forwarded to the destination IP address in the intranet.

Note	Currently, the ADS device does not support GRE tunnel injection with encapsulated IPv6 headers. Therefore, in dual-stack mode, IPv6 packets re-injected through the GRE tunnel must be encapsulated with an IPv4 header.

Figure 5-5 shows the GRE tunnel configuration page.

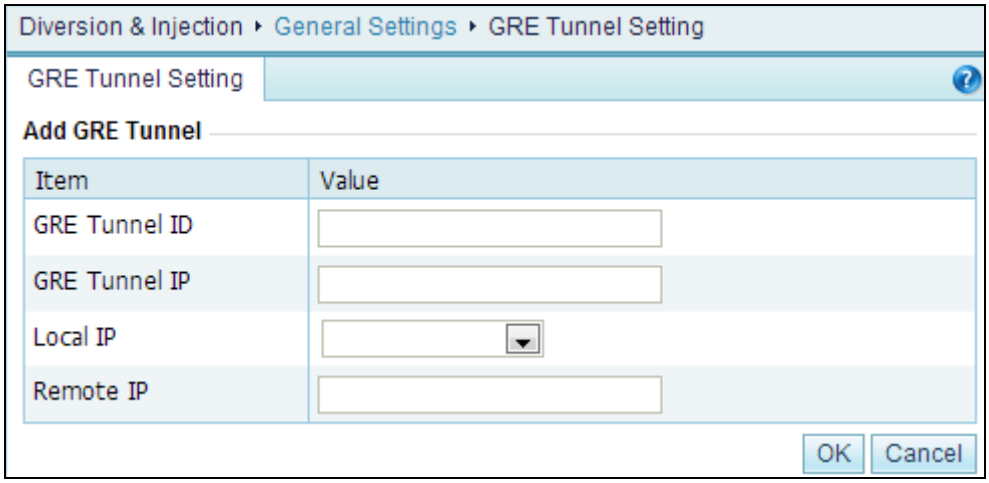
Figure 5-5 GRE tunnel configuration



Creating a GRE Tunnel

Step 1 To the lower right of the GRE tunnel list, click **Add**.

Figure 5-6 Creating a GRE tunnel



Step 2 On the **Add GRE Tunnel** page, configure parameters.

Table 5-3 describes parameters for creating a GRE tunnel.

Table 5-3 Parameters for creating a GRE tunnel

Parameter	Description
GRE Tunnel ID	GRE tunnel ID. The value is an integer ranging from 1 to 1023.
GRE Tunnel IP	IP address of a GRE tunnel. Generally, it is an internal IPv4 or IPv6 address.
Local IP	Source IP address of a GRE tunnel. This parameter can be set to an IPv4 address.
Remote IP	Destination IP address of a GRE tunnel. This parameter can be set to an IPv4 address.

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

Modifying a GRE Tunnel

Click to edit GRE tunnel configuration. The configuration of GRE tunnels being used cannot be edited.

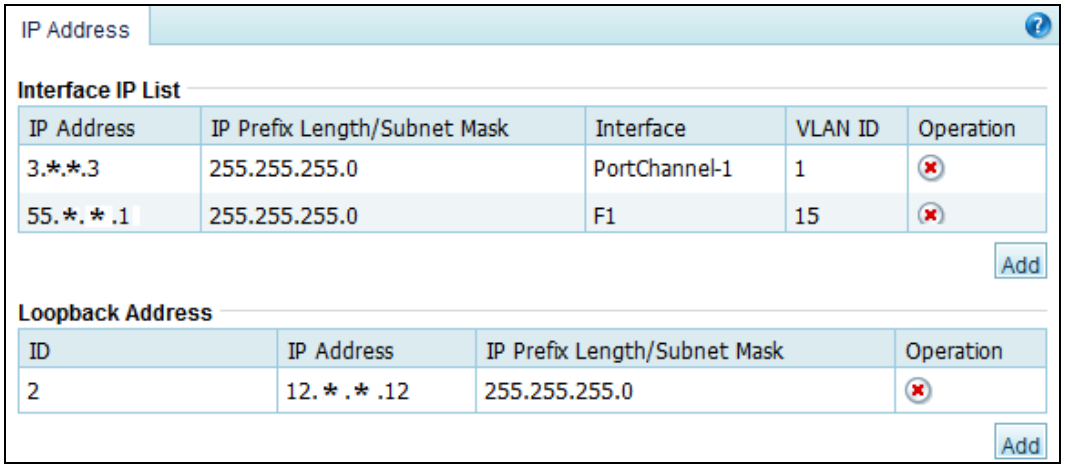
Deleting a GRE Tunnel

Click to delete a GRE tunnel. GRE tunnels being used cannot be deleted.

5.1.4 IP Address Configuration

As shown in Figure 5-7, in **Diversion** running mode, configure the IP addresses and loopback addresses for two interfaces that are used by the ADS device.

Figure 5-7 IP address list in diversion mode



Note	The number and names of ports are different for different ADS series, but have the same procedure for configuring port IP addresses. This section uses ADS NX5-4020 as an example to describe how to configure IP addresses.

Adding an IP Address

To the lower right of the interface IP list, click **Add** to add an IP address. The **Add interface IP** page appears, as shown in Figure 5-8.

Figure 5-8 Adding an IP address

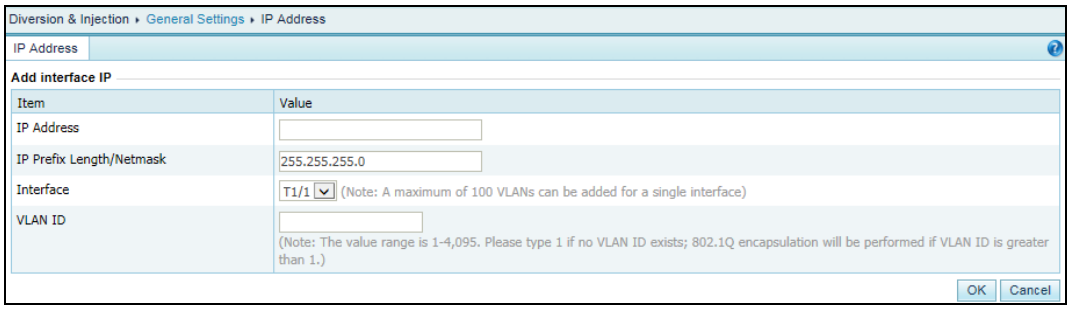


Table 5-4 describes parameters of an interface.

Table 5-4 Interface parameters

Parameter	Description
IP Address	IP address of a specified interface on the ADS device. You can type an IPv4 or IPv6 address according to the actual network deployment. The IPv4 address cannot be in the same /24 subnet as IP addresses of other interfaces. The IPv6 address embedded with an IPv4 address is not recommended.

Parameter	Description
	Note An interface can have multiple IP addresses.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the specified port.
Interface	Available ports on the current ADS device.
VLAN ID	ID of the VLAN that is connected to the port.

Deleting an IP Address

Click 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 5-9.

Figure 5-9 Adding a loopback address

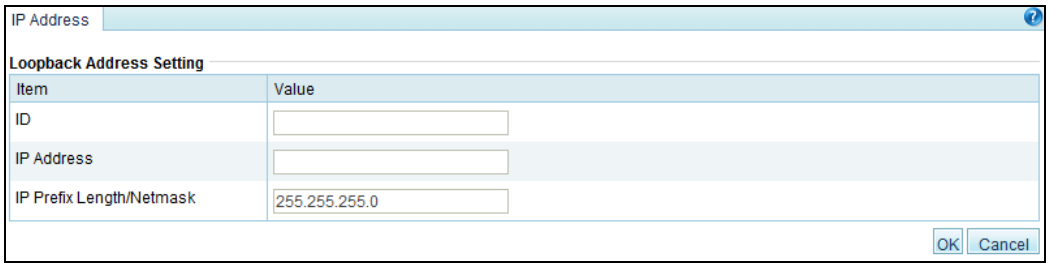


Table 5-5 describes parameters of a loopback address.

Table 5-5 Parameters of a loopback address

Parameter	Description
ID	Loopback address ID. The value is an integer ranging from 0 to 128.
IP Address	IP address of a loopback route to be added. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address.

Deleting a Loopback Address

Click to delete a loopback address. Loopback addresses that are being used cannot be deleted.

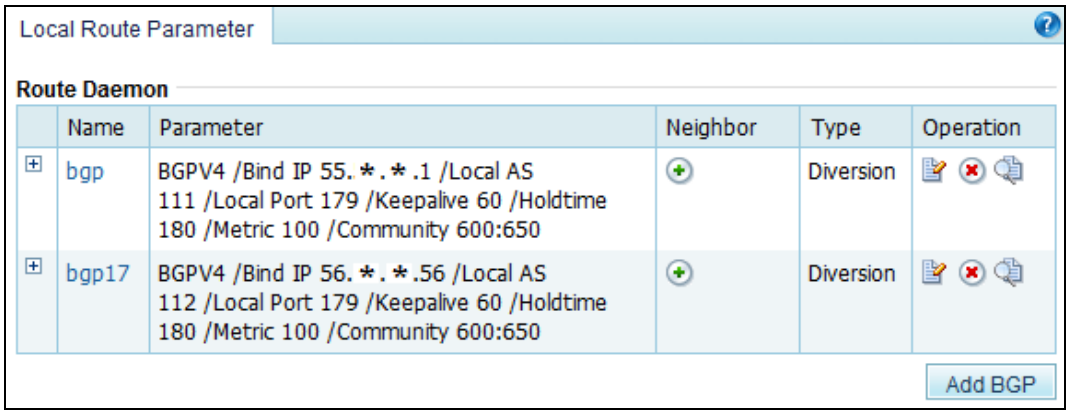
5.2 Diversion Route

The ADS device needs a dynamic routing protocol for diversion. To enable the dynamic routing protocol, you need to configure route parameters.

5.2.1 BGP Route

As shown in Figure 5-10, only BGP routes are displayed on the **Local Route Parameter** page.

Figure 5-10 Local route parameters



Creating a BGP Route

Click **Add BGP** to the lower right of the route daemon list to configure local BGP parameters. See Figure 5-11.

Figure 5-11 Creating a BGP route

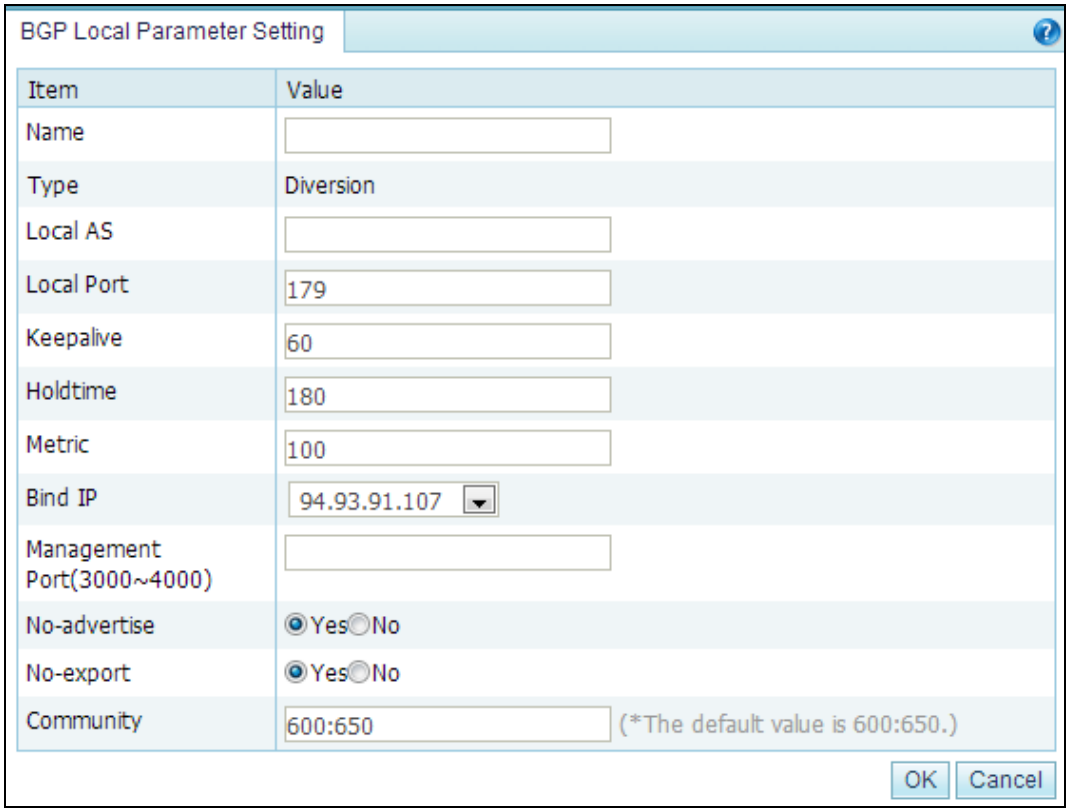


Table 5-6 describes parameters for creating a BGP route.

Table 5-6 Parameters for creating a BGP route

Parameter	Description
Name	Route daemon name.
Local AS	Autonomous system (AS) number of a BGP route daemon. **Note** You are advised to use the AS with number over 65000 and not use a private domain that is already used by other countries.
Local Port	BGP port of the route daemon. Generally, the default port **179** is used.
Bind IP	Local IP address of the route daemon. You can type an IPv4 or IPv6 address according to the actual network deployment.
Management Port(3000~4000)	Management port of the route daemon. The port ranges from 3000 to 4000.
Community	Community of the BGP route. The default value is **600:650**.

Other parameters including **Keepalive**, **Holdtime**, **Metric**, **No-advertise**, and **No-export** correspond to certain fields of the BGPv4 protocol.

Editing a BGP Route

On the route daemon list, click to edit a route.

Note	Modifying BGP settings during the running of the HA function may cause traffic switchover, and is not recommended.

Deleting a BGP Route

On the route daemon list, click to delete a route.

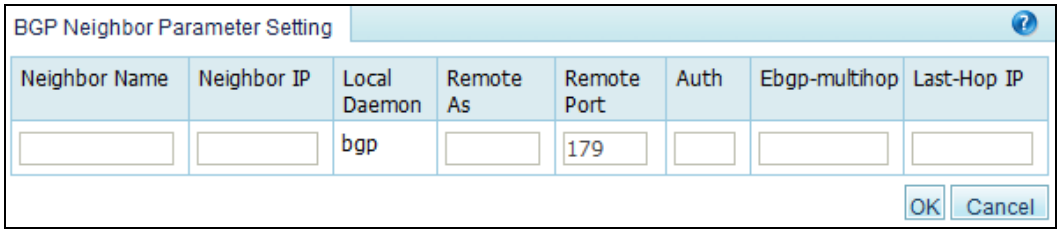
Viewing the Route Status

On the route daemon list, click to view status of the route.

Adding a BGP Neighbor

A BGP route is the only route that has neighbors. Click in the local route list to add a BGP neighbor. See Figure 5-12.

Figure 5-12 Adding a BGP neighbor



Note	After a neighbor is added, click to check whether it is connected.

Table 5-7 describes parameters of a BGP neighbor

Table 5-7 Parameters of a BGP neighbor

Parameter	Description
Neighbor Name	BGP neighbor name.

Parameter	Description
Neighbor IP	IP address of the BGP neighbor. Both IPv4 and IPv6 addresses are allowed.
Remote As	Autonomous system of the BGP neighbor.
Remote Port	Remote port of the BGP neighbor. The default port number is **179**.
Auth	Authentication password. This parameter is required only when you encrypt the BGP neighbor.
Ebgp-multihop	Maximum number of hops allowed by the External Border Gateway Protocol (EBGP).
Last-Hop IP	IP address of the router directly connecting to the ADS device. Both IPv4 and IPv6 addresses are allowed.

Hiding or Displaying a BGP Neighbor

All neighbors are displayed in the list by default. You can click ⊟ to hide neighbors of a route or click ⊞ to display all of them.

Other Operations on a BGP Neighbor

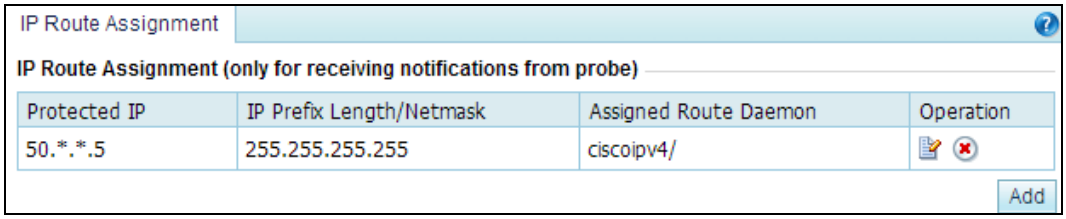
After all BGP neighbors are displayed, you can click to modify information of a neighbor, click to delete a neighbor, click to check whether a neighbor can be pinged, or click to view the connection status of a neighbor.

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

5.2.2 IP Route Assignment

IP routes enable the current ADS device to receive notifications (configured together with diversion filtering rules) from an NSFOCUS ADS detection device and to decide which route daemon sends notifications. See Figure 5-13.

Figure 5-13 IP route assignment



Creating an IP Route

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 5-14 Creating an IP route

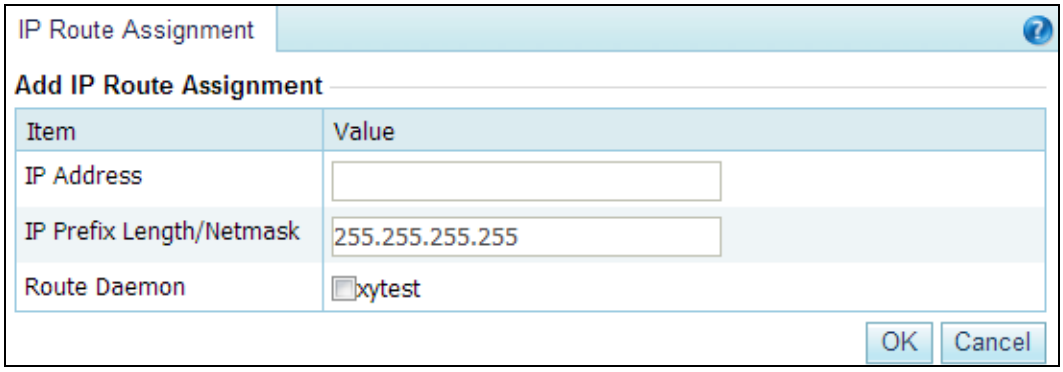


Table 5-8 describes parameters for creating an IP route.

Table 5-8 Parameters for creating an IP route

Parameter	Description
IP Address	IP address to which a route is assigned. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address.
Route Daemon	Route daemon that sends a routing notification.

Editing an IP Route

On the IP route assignment list, click to edit an IP route.

Deleting an IP Route

On the IP route assignment list, click to delete an IP route.

Note	For details on configuring diversion filtering rules, see section 5.4.1 Filtering Rules.

5.3 Traffic Injection

This section covers the following topics:

- Injection Interfaces
- Injection Routes
- MAC Address Table

5.3.1 Injection Interfaces

The number and names of ports are different for different ADS series, but the procedure for configuring injection interfaces is the same for them. This section uses ADS NX5-4020 as an example to describe how to configure injection interfaces.

To configure an injection interface, you need to configure parameters about the injection interface including interface IP address and netmask, VLAN ID and physical port of the interface. The injection interface determines the physical port and packet encapsulation format for traffic re-injection.

This section covers the following topics:

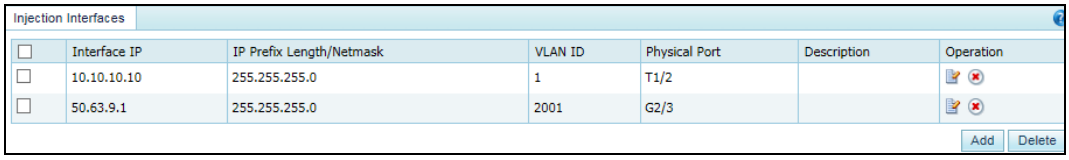
- Adding an Injection Interface
- Editing an Injection Interface
- Deleting Injection Interfaces

5.3.1.1 Adding an Injection Interface

To add an injection interface, perform the following steps:

Step 1 Choose **Diversion & Injection** > **Traffic Injection** > **Injection Interfaces**.

Figure 5-15 Injection interface list



Step 2 Click **Add** to open the page for adding an injection interface.

Figure 5-16 Adding an injection interface

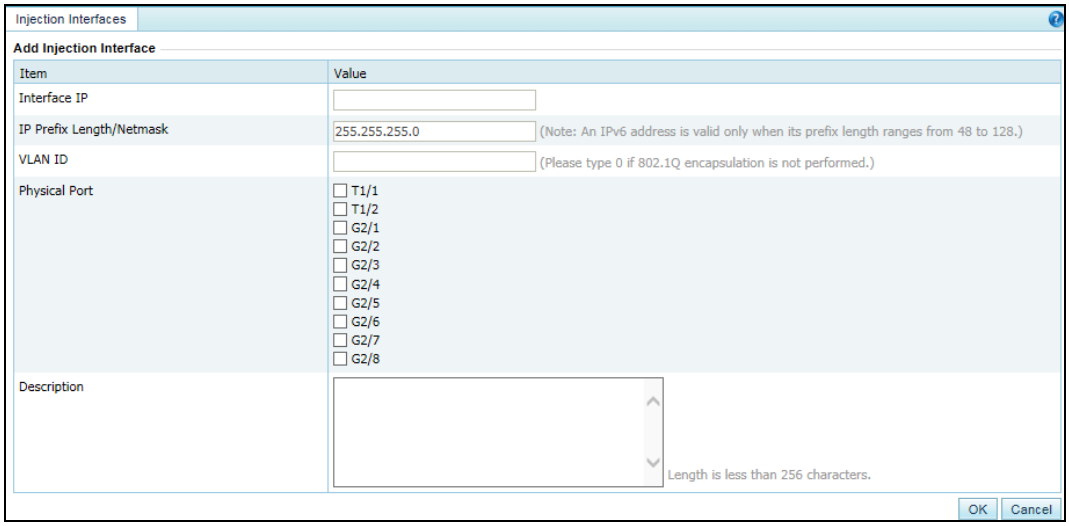


Table 5-9 describes parameters of an injection interface.

Table 5-9 Parameters of an injection interface

Parameter	Description
Interface IP	IP address of an injection interface. You can type an IPv4 or IPv6 address according to the actual network deployment. • If **Interface IP** is set to an IPv4 address, it can be either a network address in the format of *.*.*.0/24 or a broadcast address in the format of *.*.*.255/24. • If **Interface IP** is set to an IPv6 address, the value range of IPv6 prefix is 48–128 bits.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the interface IP address.
VLAN ID	VLAN ID of the injection interface. The value is an integer ranging from 0 to 4094.
Physical Port	Physical port of an injection interface. You can select multiple physical ports.

Note	IP address configured on the injection interface is a source IP address of the ARP query packets, which is mainly used by the ADS device to learn the next-hop MAC address. Other devices cannot communicate with this IP address. When VLAN ID is not 0, all packets will be encapsulated with the IEEE 802.1Q protocol and then be forwarded. When VLAN ID is 0, all packets will be encapsulated with a common Ethernet protocol. If the injection interface has several physical ports, traffic is forwarded in load balancing mode on these interfaces.

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

----End

5.3.1.2 Editing an Injection Interface

After configuring injection interfaces, the administrator can edit interface parameters by performing the following steps:

Step 1 On the injection interface list, click to the right of an interface to edit interface parameters.

Step 2 After editing interface parameters, click **OK** to save settings and return to the injection interface list.

----End

5.3.1.3 Deleting Injection Interfaces

You can delete one injection interface or multiple interfaces in batches on ADS devices.

- Method 1: On the injection interface list in Figure 5-15, click to the right of an interface and then click **OK** in the confirmation dialog box to delete an injection interface.
- Method 2: Select one or more injection interfaces (or select the **Select All** check box to select all injection interfaces) to be deleted, click **Delete** to the lower right of the interface list, and then click **OK** in the confirmation dialog box to delete selected interfaces.

5.3.2 Injection Routes

This section covers the following topics:

- Creating an Injection Route
- Creating Injection Routes in Batches
- Viewing Rule Status of Injection Routes
- Viewing Link Connectivity of Injection Routes
- Viewing Injection Routes
- Learning MAC Address
- Enabling and Disabling Injection Routes
- Resetting Link Switch Count
- Editing Injection Routes
- Deleting Injection Routes
- Editing Advanced Configurations

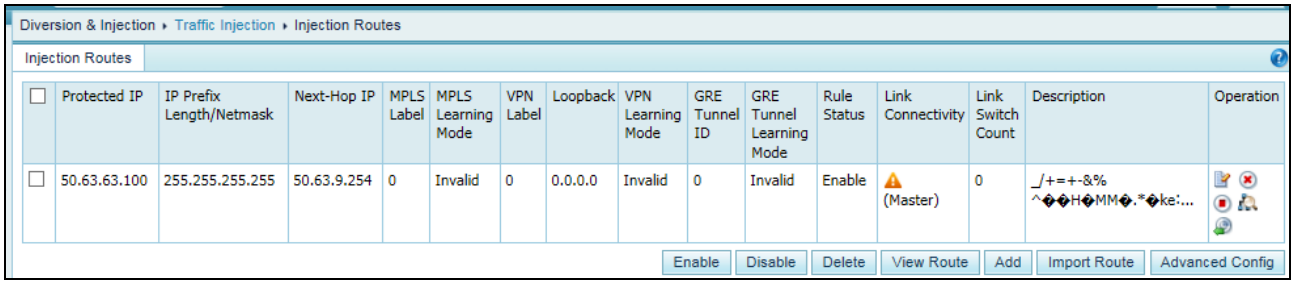
ADS supports multiple injection routes. If multiple routes have the same priority, ADS injects traffic along all the routes and checks the connectivity of all the routes. Once a route fails, ADS automatically invalidates the route and injects traffic along the other routes subsequently. If multiple injection routes have different priorities, ADS injects traffic along the route with the highest priority, and uses the other routes as standby routes. In this case, ADS checks the connectivity of all the routes. If the route with the highest priority fails, ADS considers it as an invalid one and injects traffic along the route with the highest priority among the standby routes. This master-slave mechanism among routes achieves high availability.

5.3.2.1 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 5-17.

Figure 5-17 Injection routes



Step 2 Click **Add**.

Figure 5-18 Creating an injection route

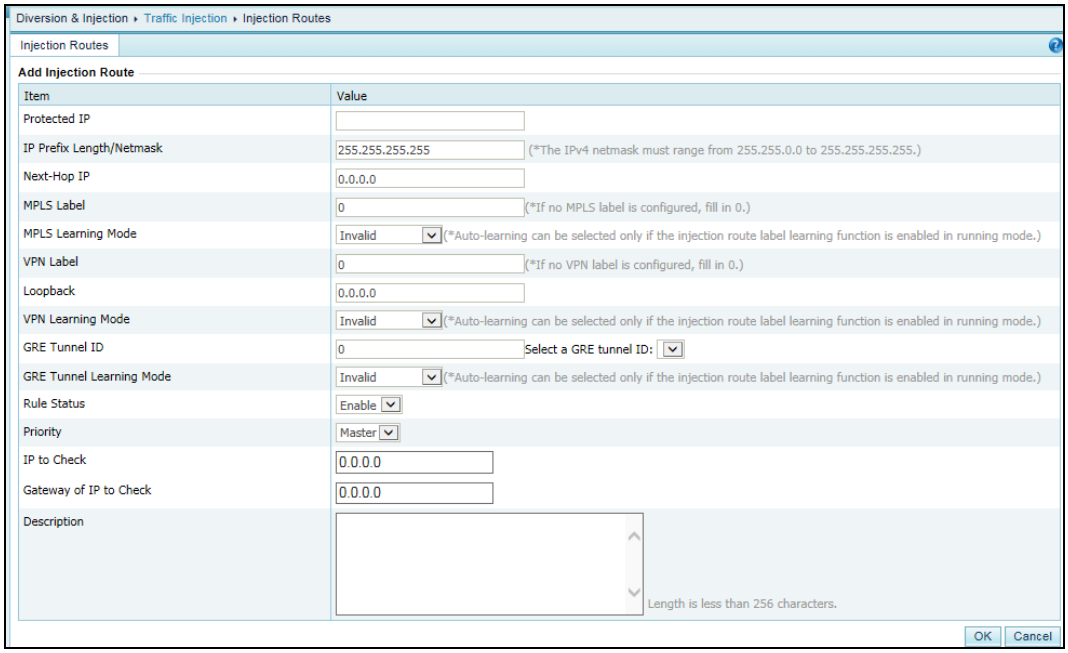


Table 5-10 describes parameters for creating an injection route.

Table 5-10 Parameters for creating an injection route

Parameter	Description
Protected IP	IP address or IPv4 segment of a protected host. You can type an IPv4 or IPv6 address according to the actual network deployment. **Note** Currently, you can add an injection route for IP addresses in the /16 or /24 subnet, but not for those in the /4 subnet.

Parameter	Description
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address. The netmask of an IPv4 address to be diverted must range from 255.255.255.0 to 255.255.255.255.
Next-Hop IP	Next-hop IP address of the traffic destined for the protected IP address (or IP segment). The next-hop IP address is often bundled with the injection interface of the ADS device. You can type an IPv4 or IPv6 address according to the actual network deployment.
MPLS Label	MPLS label of the packet forwarded by the injection route. Type **0** if the MPLS label is not configured.
MPLS Learning Mode	Specifies how to learn MPLS labels. It has the following values: • **Manual setting**: indicates that you need to specify the MPLS label manually. • **Auto-learning**: indicates that the ADS device automatically learns MPLS labels. • **Invalid**: indicates that no MPLS label is configured.
VPN Label	VPN label. Type **0** if no VPN label is configured.
VPN Learning Mode	Specifies how to learn the VNP label. It has the following values: • **Manual setting**: indicates that you need to specify the VPN label manually. • **Auto-learning**: indicates that the ADS device automatically learns VPN labels. • **Invalid**: indicates that no VPN label is configured.
Loopback	Loopback IP address set by the system.
GRE Tunnel ID	ID of a GRE tunnel. Leave it at the default value **0** if no GRE tunnel is configured.
GRE Tunnel Learning Mode	Specifies how to learn the GRE tunnel label. It has the following values: • **Auto-learning**: indicates that the ADS system automatically learns CRE tunnel labels. In this case, **Enable Injection MPLS Label Learning** must be set to **Yes** in **Running Mode**. • **Manual setting**: indicates that a GRE tunnel label needs to be configured manually. • **Invalid**: indicates that no GRE tunnel label is configured.
Rule Status	Controls whether to query the injection status. It has the following values: • **Enable**: indicates that the system queries the injection rule when forwarding packets. • **Disable**: indicates that the system does not query the injection rule when forwarding packets.
Priority	Route priority. The default value is **Master**. • **Master**: indicates a higher priority. • **Slave**: indicates a lower priority.
IP to Check	IP address to be pinged when the connectivity of the current route is checked.

Parameter	Description
	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. The default value is **0.0.0.0**, indicating that no corresponding static route is configured. If **IP to Check** and **Gateway of IP to Check** are set to other values than the default ones, the system automatically adds a static route to **IP to Check** and with the next hop as **Gateway of IP to Check**.

Note	When **Next-Hop IP Address** is set to **0.0.0.0**, the ADS device performs layer 2 forwarding. Assume that the protected IP address is 192.168.1.0, the netmask is 255.255.255.0, and the next-hop IP address is 0.0.0.0. Then the next-hop IP address of the traffic destined for 192.168.1.1 is 192.168.1.1, and that of 192.168.1.2 is 192.168.1.2. The rest may be deduced by analogy.

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

----End

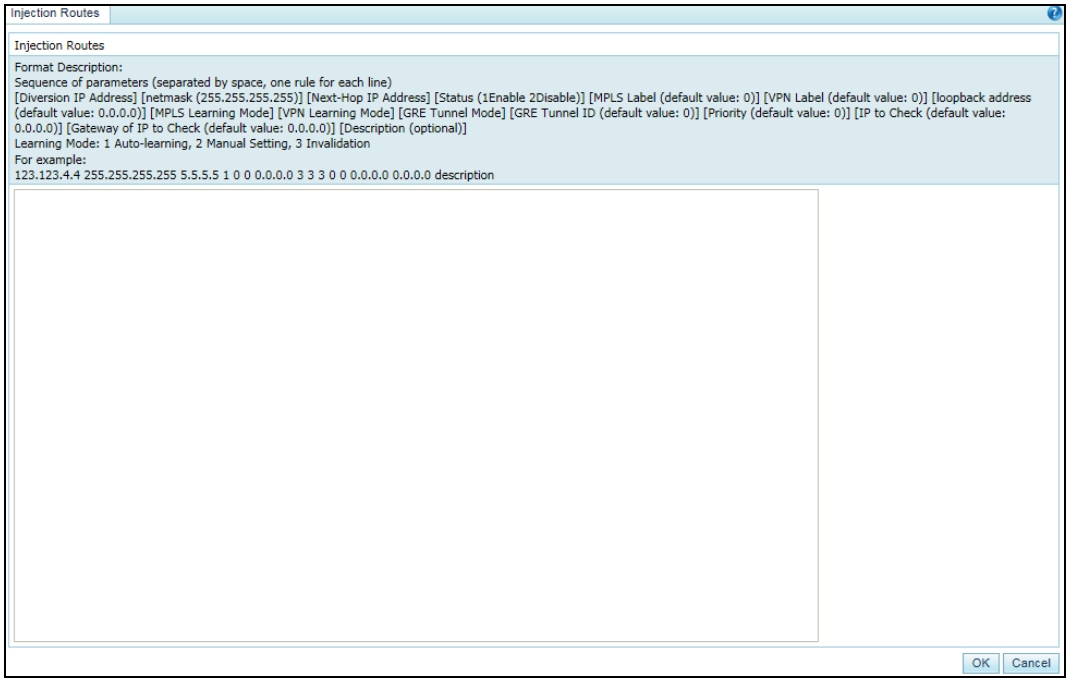
5.3.2.2 Creating Injection Routes in Batches

The administrator can create injection routes in batches on the NSFOCUS ADS system by performing the following steps:

Step 1 Click **Import Route** to the lower right of the injection route list.

A page appears, as shown in Figure 5-19.

Figure 5-19 Creating injection routes in batches



Step 2 Type multiple injection routes as prompted.

Pay attention to the following format specifications:

- An injection route is typed in the following format: [Diversion IP Address] [Subnet Mask (255.255.255.255)] [Next-Hop IP Address] [Status (1Enable 2Disable)] [MPLS Label (default value: 0)] [VPN Label (default value: 0)] [loopback address (default value: 0.0.0.0)] [MPLS Learning Mode] [VPN Learning Mode] [GRE Tunnel Mode] [GRE Tunnel ID (default value: 0)] [peer_lsr_id (default value: 0.0.0.0)]. For two learning modes, the value **1** indicates self-learning, the value **2** indicates manual setting, and the value **3** indicates invalid.
- An injection route example is as follows: 123.123.4.4 255.255.255.255 5.5.5.5 1 0 0 0.0.0.0 3 3 3 0 0.0.0.0
- Parameters of each injection route are separated by spaces.
- Each line can contain only one injection route.

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

----End

5.3.2.3 Viewing Rule Status of Injection Routes

After routes are configured and applied, the administrator can view rule status of the routes in the Rule Status column in Figure 5-17. The rule status could be one of the following:

- **Enable**: The rule is manually enabled, and the link is connected or not checked.
- **Enable (Block)**: The rule is enabled, but cannot be used because the link is disconnected for the injection route.
- **Disable (Block)**: The rule is disabled by the system because the injection link is disconnected and the number of link switches exceeds the specified number.

- **Disable**: The rule is manually disabled.

5.3.2.4 Viewing Link Connectivity of Injection Routes

After routes are configured and applied, the administrator can view link connectivity of the routes in the Link Connectivity column in Figure 5-17. The link connectivity could be one of the following:

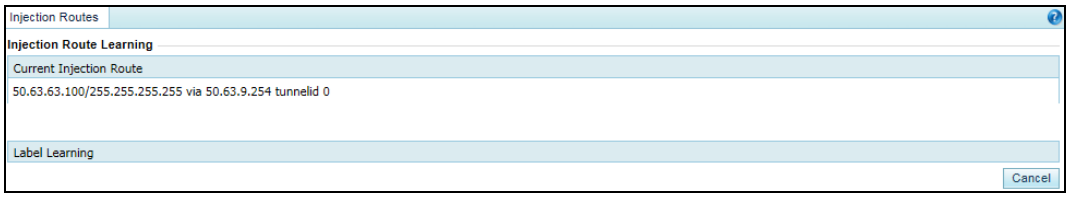
- : The link of this injection route functions properly. That is, ADS can successfully ping the IP to Check of the injection route.
- : The link of this injection route is faulty. That is, ADS fails to ping the IP to Check of the injection route. In this case, traffic cannot be injected along this route.
- : The link of this injection route is in unstable status. ADS does not check this injection route.
- : The link of this injection route is in unstable status. ADS is checking this injection route.

5.3.2.5 Viewing Injection Routes

After injection routes are configured and applied, the administrator can view information about such routes and MPLS labels learned by the device. The detailed procedure is as follows:

Step 1 Click **View Route** to the lower right of the injection route list to view current injection routes and learned labels.

Figure 5-20 Viewing injection routes and learned labels



- **Current Injection Route** lists current injection routes on the device.
- **Label Learning** lists MPLS labels learned by the device. An MPLS label is a local short identifier with a fixed length. It is used to identify the Forwarding Equivalence Class (FEC) to which a group belongs.

Note	MPLS labels are often classified into layer 1 labels and layer 2 labels. To enable MPLS label learning support on the device, you need to first start the Label Distribution Protocol (LDP) and then configure MPLS labels. To use layer 2 MPLS labels on the device, you also need to configure VPN labels.

Step 2 After viewing injection routes, click **Cancel** to return to the injection route list.

----End

5.3.2.6 Learning MAC Address

The MAC address self-learning function allows the ADS device to learn the MAC addresses of the protected IP addresses by sending ARP broadcast messages. The mapping between the protected IP addresses and the MAC addresses learned by the ADS device is displayed in the MAC address table. For the mapping details, see section 5.3.3 MAC Address Table.

To view MAC addresses learned by the ADS device, click to the right of an injection route, as shown in Figure 5-17.

Note	• If the ADS device takes a long time to learn the MAC address of a protected IPv6 address, you are advised to manually bind the protected IP address and the MAC address. • If the prefix length of the IPv6 address is not 128 bits and the next hop is not a specific IP address, MAC learning will be unavailable.

5.3.2.7 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 the administrator 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 5-17, click to the right 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 5-17, select one or more injection routes (or select the **Select All** check box to select all injection routes) to be deleted, click **Enable** to the lower right of the route list, and click **OK** in the confirmation dialog box to enable selected routes.

Disabling Injection Routes

- Method 1: On the injection route list shown in Figure 5-17, click to the right 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 5-17, select one or more injection routes (or select the **Select All** check box to select all injection routes) to be deleted, click **Disable** to the lower right of the route list, and then click **OK** in the confirmation dialog box to disable selected routes.

5.3.2.8 Resetting Link Switch Count

The administrator can view the number of link switches (from valid to invalid) of an injection route in the **Link Switch Count** column in Figure 5-17.

The administrator can click in the **Operation** column of an injection route to reset the number of link switches to **0**.

5.3.2.9 Editing Injection Routes

After configuring injection routes, the administrator can edit route parameters by performing the following steps:

Step 1 On the injection route list in Figure 5-17, click to the right of a route to edit route parameters.

Step 2 After editing parameters, click **OK** to save settings and return to the injection route list.

----End

5.3.2.10 Deleting Injection Routes

You can delete one injection route or more routes in batches on the ADS device.

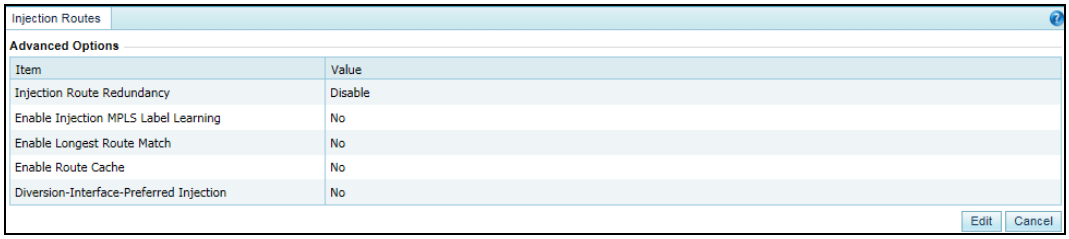
- Method 1: On the injection route list shown in Figure 5-17, click to the right of a route and click **OK** in the confirmation dialog box to delete an injection route.
- Method 2: Select one or more injection routes (or select the **Select All** check box to select all injection routes) to be deleted, click **Delete** to the lower right of the route list, and click **OK** in the confirmation dialog box to delete the selected routes.

5.3.2.11 Editing Advanced Configurations

The administrator can edit advanced configurations that apply to all injection routes.

Click **Advanced Config** in the lower-right corner of the injection route list shown in Figure 5-17. The page for editing advanced configurations appears, as shown in Figure 5-21.

Figure 5-21 Editing advanced configurations.



Then you can click **Edit** and start to edit advanced configurations.

Table 5-11 describes parameters for editing advanced configurations.

Table 5-11 Parameters for editing advanced configurations

Parameter		Description
Advanced Options	Injection Route Redundancy	Specifies whether to enable the injection route redundancy function. The **Injection Route Next-hop Health Check** area appears only when this function is enabled. **Note** The injection route redundancy function cannot be enabled simultaneously with either of injection

Parameter		Description
		MPLS label learning or diversion-interface-preferred injection.
	Enable Injection MPLS Label Learning	Controls whether to enable injection MPLS label learning. The default value is **No**. Injection MPLS label learning needs to be enabled only when MPLS injection is enabled. Note If injection MPLS label learning is enabled while MPLS injection is disabled, ordinary injection routes cannot be dispatched. Injection MPLS label learning cannot be enabled simultaneously with the injection route redundancy function.
	Enable Longest Route Match	Controls whether to enable longest route match. The default value is **No**. After longest route match is enabled, among routes destined for the same destination IP address, the system selects one based on their netmask lengths. The one with the longest netmask will be selected.
	Enable Route Cache	Controls whether to enable route cache. The default value is **No**. Route cache needs to be enabled only when longest route match is enabled. Enabling route cache is like having a fast forwarding table. The system does not need to check the entire injection route table every time.
	Diversion-Interface-Preferred Injection	Controls whether to enable diversion-interface-preferred injection. The default value is **No**. After it is enabled, traffic will be preferentially injected over the diversion interface, ensuring that traffic is diverted and injected over the same interface. Note To enable diversion-interface-preferred injection, you need to enable longest route match in advance. Diversion-interface-preferred injection and injection redundancy cannot be enabled simultaneously. To enable diversion-interface-preferred injection, you need to ensure that the injection route over the diversion interface has the highest priority or all injection routes have the same priority.
Injection Route Next-hop Health Check	Detection Period	Controls the interval between two link availability checks. The value ranges from 10 to 600, in seconds. The default value is **60**.
	Attempts	Controls the allowed number of attempts to check injection link availability. The value ranges from 1 to 10, and the default value is **3**. If a link remains unavailable after the specified number of check attempts, the link is considered invalid.
	Link Switch Limit	Controls the maximum number of link status switches before the priority of a link is degraded. The value ranges

Parameter		Description
		from 0 to 10, and the default value is **5**. The value **0** indicates no limit on the number of link status switches. Note The link status changing from Up to Down is counted as one time of switching, but changing from Down to Up is not. After the number of link status switches exceeds the specified maximum number, the link will be disabled and can be enabled manually only.

5.3.3 MAC Address Table

The MAC address table specifies the mapping between IP addresses and MAC addresses on the ADS device for fast data forwarding. The MAC address table can be added manually or learned by the ADS device dynamically. For details on dynamic learning of MAC addresses, see section 5.3.2.6 Learning MAC Address. This section covers the following topics:

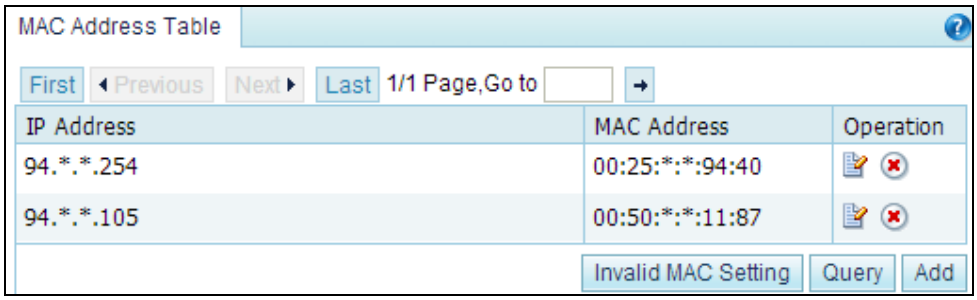
- Adding an MAC Address Entry
- Editing a MAC Address Entry
- Deleting a MAC Address Entry
- Querying MAC Addresses
- Configuring Invalid MAC Addresses

5.3.3.1 Adding an MAC Address Entry

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

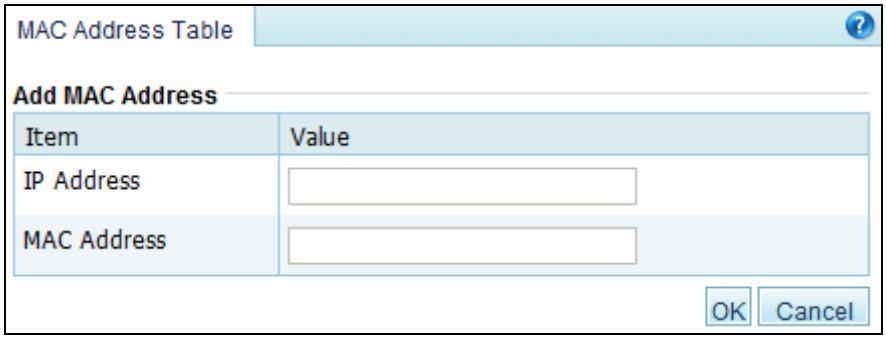
Step 1 Choose **Diversion & Injection** > **Traffic Injection** > **MAC Address Table** to open the configuration page for the MAC address table.

Figure 5-22 MAC address table



Step 2 Click **Add** to the lower right of the MAC address table to open the page for adding the mapping between an IP address and an MAC address.

Figure 5-23 Adding the mapping between an IP address and an MAC address



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

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

----End

5.3.3.2 Editing a MAC Address Entry

After configuring MAC address entries, the administrator can edit parameters of this entry by performing the following steps:

Step 1 On the page shown in Figure 5-22, click to the right of an MAC address to edit its parameters.

Step 2 After editing parameters, click **OK** to save settings and return to the MAC address table.

----End

5.3.3.3 Deleting a MAC Address Entry

The administrator can delete MAC address entries one by one on the ADS device.

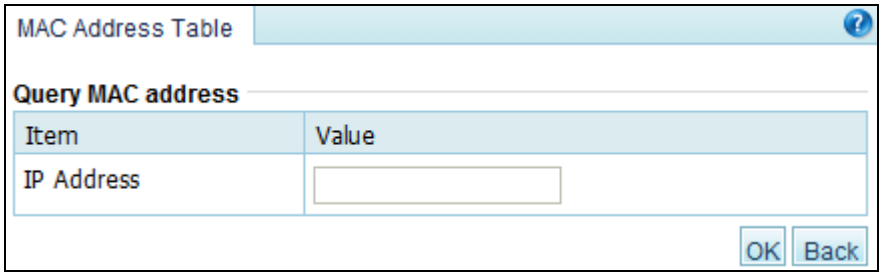
In the MAC address table shown in Figure 5-22, click to the right of an MAC address entry and then click **OK** to delete an entry.

5.3.3.4 Querying MAC Addresses

To query the MAC address mapping an IPv4 or IPv6 address, perform the following steps:

Step 1 Click **Query** to the lower right of the MAC address table to open the MAC address query page.

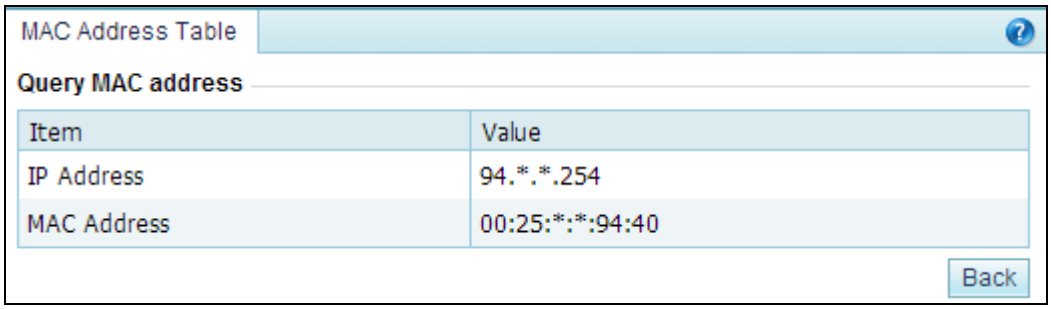
Figure 5-24 Querying the MAC address mapping an IP address



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

Then, the MAC address mapping this IP address is displayed, as shown in Figure 5-25.

Figure 5-25 Query result



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

----End

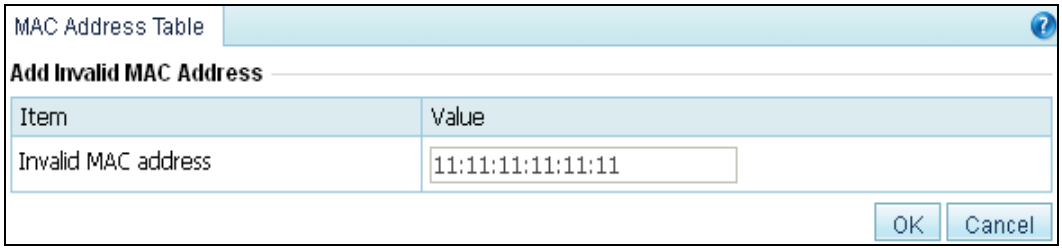
5.3.3.5 Configuring Invalid MAC Addresses

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

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

Step 1 Click **Invalid MAC Setting** to the lower right of the MAC address table in Figure 5-22 to open the page of configuring invalid MAC addresses. See Figure 5-26.

Figure 5-26 Configuring invalid MAC addresses



Step 2 Configure invalid addresses. The default invalid MAC address is **11:11:11:11:11:11**. You can configure other invalid addresses as required.

Note	MAC addresses typed on the web page must be separated by colons.

----End

5.4 Traffic Diversion

This section covers the following topics:

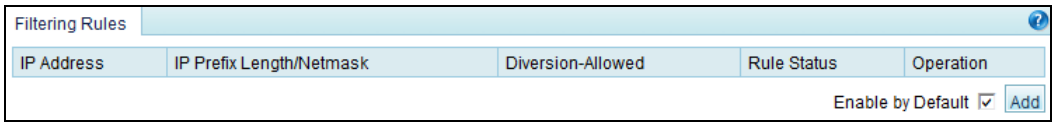
- Filtering Rules
- Manual Diversion
- Group Diversion
- Diversion Routing Table

5.4.1 Filtering Rules

A diversion filtering rule enables the ADS device to filter attack traffic transmitted from NSFOCUS ADS detection devices, to determine whether to send routing notifications, and to activate diversion automatically.

As shown in Figure 5-27, diversion filtering rules are listed by time of addition. The device matches rules (of **Enable** status) from top to bottom and uses the default rule if no rule is matched.

Figure 5-27 Filtering rules



Creating a Diversion Filtering Rule

Click **Add** to the lower right of the list. On the **Add Diversion Filtering Rule** page, configure parameters and click **OK**.

Figure 5-28 Creating a diversion filtering rule

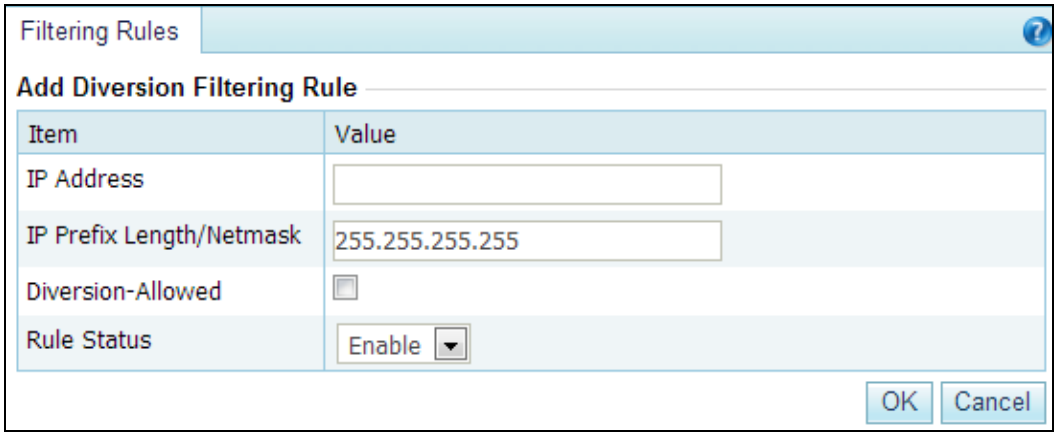


Table 5-12 describes parameters for creating a diversion filtering rule.

Table 5-12 Parameters for creating a diversion filtering rule

Parameter	Description
IP Address	IP address or segment to be protected. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be protected. This parameter allows you to configure a network segment.
Diversion-Allowed	Controls whether to enable diversion. A check in the checkbox indicates that the ADS device allows diversion. This check box is deselected by default, indicating that the ADS device does not allow diversion.
Rule Status	Controls whether to enable the rule immediately after the rule is added. It has the following values: • **Enable**: enables a diversion filter rule immediately after it is added. • **Disable**: disables the diversion filter rule that can be enabled later manually.

Editing a Diversion Filtering Rule

On the diversion filtering rule list, click to edit a rule.

Deleting a Diversion Filtering Rule

On the diversion filtering rule list, click to delete a rule.

Changing the Status of a Diversion Filtering Rule

On the diversion filtering rule list, click 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, click and to change the priority of the rules in the list.

5.4.2 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 the list, without requiring a click on the **Save** button.

Note	In manual diversion mode, each time ADS diverts traffic to only one /24 subnet address to the ADS device. If you want the ADS device to divert traffic to multiple /24 subnet addresses, please configure multiple manual traffic diversion rules.

This section covers the following topics:

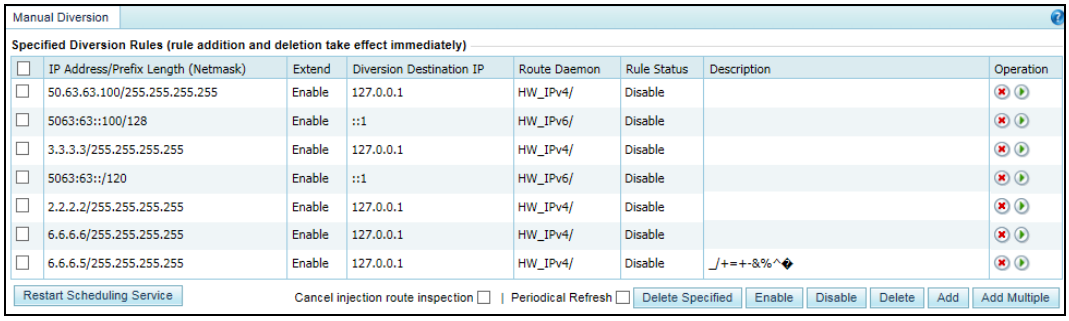
- Creating a Manual Traffic Diversion Rule
- Creating Manual Diversion Rules in Batches
- Enabling and Disabling Manual Diversion Rules
- Deleting Manual Diversion Rules
- Deleting a Specified Route
- Refreshing Routes Periodically
- Canceling Injection Route Inspection
- Restarting the Scheduling Service

5.4.2.1 Creating a Manual Traffic Diversion Rule

To create a traffic diversion rule, perform the following steps:

Step 1 Choose **Diversion & Injection** > **Traffic Diversion** > **Manual Diversion** to open the diversion rule configuration page.

Figure 5-29 Traffic diversion rules



IP Address/Prefix Length (Netmask)	Extend	Diversion Destination IP	Route Daemon	Rule Status	Description	Operation
50.63.63.100/255.255.255.255	Enable	127.0.0.1	HW_IPv4/	Disable		
5063:63::100/128	Enable	::1	HW_IPv6/	Disable		
3.3.3.3/255.255.255.255	Enable	127.0.0.1	HW_IPv4/	Disable		
5063:63::/120	Enable	::1	HW_IPv6/	Disable		
2.2.2.2/255.255.255.255	Enable	127.0.0.1	HW_IPv4/	Disable		
6.6.6.6/255.255.255.255	Enable	127.0.0.1	HW_IPv4/	Disable		
6.6.6.5/255.255.255.255	Enable	127.0.0.1	HW_IPv4/	Disable	_/+=+-&%^@	

Step 2 Click **Add**.

Figure 5-30 Creating a traffic diversion rule

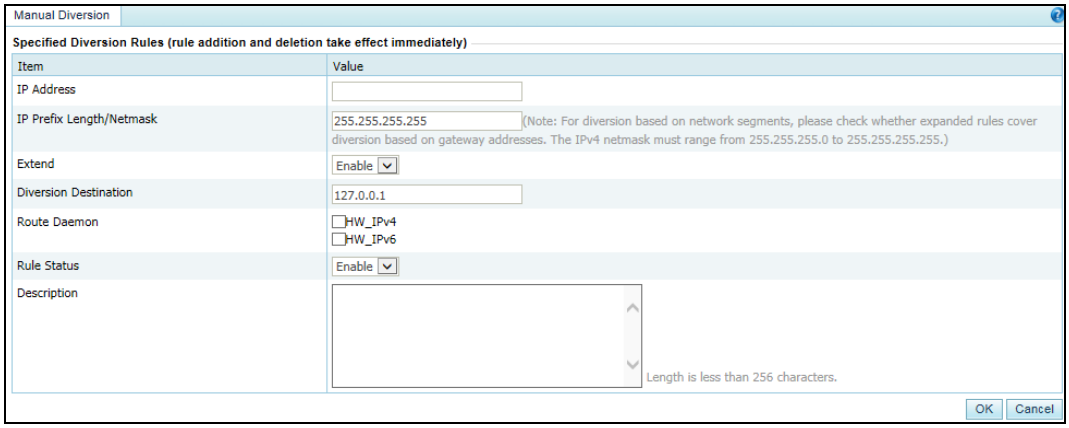


Table 5-13 describes parameters for creating a diversion rule.

Table 5-13 Parameters for creating a diversion rule

Parameter	Description
IP Address	IP address or IP segment to be protected, usually the IP address of the protected server. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be diverted. **Note** The netmask of an IPv4 address to be protected can range from 255.255.255.0 to 255.255.255.255.
Extend	Controls whether to extend the netmask. It has the following values: • **Enable**: indicates that the netmask is extended. • **Disable**: indicates that the netmask is not extended.
Diversion Destination	Next-hop IP address of the route notification sent from the route daemon. It is usually the IP address of the diversion interface of the ADS device or ::1. The default value is 127.0.0.1.
Route Daemon	Route daemon that sends a routing notification.
Rule Status	Controls whether to enable the rule immediately after the rule is added. It has the following values: • **Enable**: enables a diversion filter rule immediately after it is added. • **Disable**: disables the diversion filter rule that can be enabled later manually.

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

Note	To ensure the injection of the diverted traffic, you must configure the injection route and injection MAC address correctly before manual diversion.

Step 4 Click **Apply** in the upper-right corner of the web page to make the settings take effect.

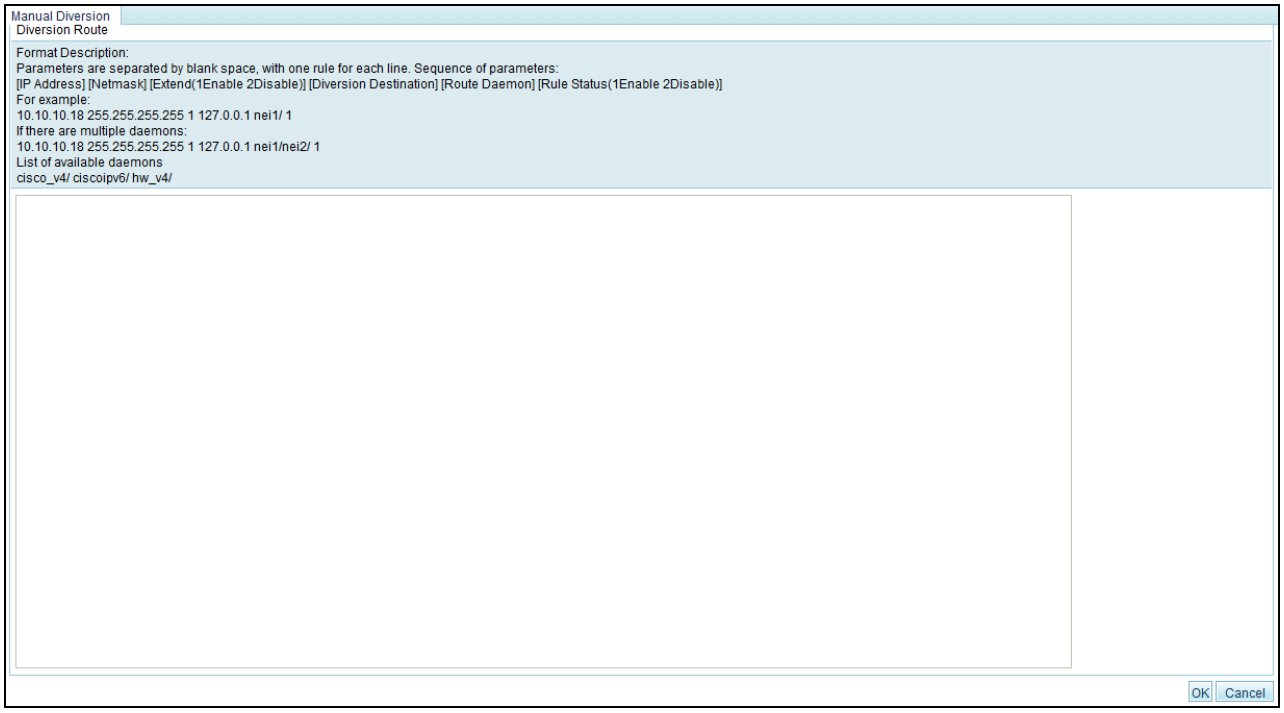
----End

5.4.2.2 Creating Manual Diversion Rules in Batches

To simplify operations, the administrator 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.

Figure 5-31 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] [Subnet mask] [Route daemon], for example, 10.10.10.18 255.255.255.255 nei1. For multiple daemons, a manual diversion rule is added as follows: 10.10.10.18 255.255.255.255 nei1/nei2/.
- Three types of daemons are available: bgp, ospf, and rip.
- Parameters of a manual diversion rule are separated by spaces.
- Each line can contain only one manual diversion rule.

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

----End

5.4.2.3 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 the administrator 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 5-29, click to the right 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 5-29, select one or more rules (or select the **Select All** check box to select all manual diversion rules) to be deleted, click **Enable** to the lower right of the rule list, and click **OK** in the confirmation dialog box to enable selected rules.

Disabling Manual Diversion Rules

- Method 1: On the manual diversion rule list shown in Figure 5-29, click to the right 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 5-29, select one or more rules (or select the **Select All** check box to select all manual diversion rules) to be deleted, click **Disable** to the lower right of the rule list, and click **OK** in the confirmation dialog box to disable selected rules.

5.4.2.4 Deleting Manual Diversion Rules

You can delete a single manual diversion rule or more rules in batches on the ADS device. This section describes how to delete unused diversion rules. For details on deleting diversion rules that are being used, see section 5.4.2.5 Deleting a Specified Route.

- Method 1: On the manual diversion rule list shown in Figure 5-29, click in the **Operation** column and click **OK** in the confirmation dialog box to delete a rule.
- Method 2: On the manual diversion rule list shown in Figure 5-29, select one or more rules (or select the **Select All** check box to select all manual diversion rules) to be deleted, click **Delete** to the lower right of the rule list, and then click **OK** in the confirmation dialog box to delete selected rules.

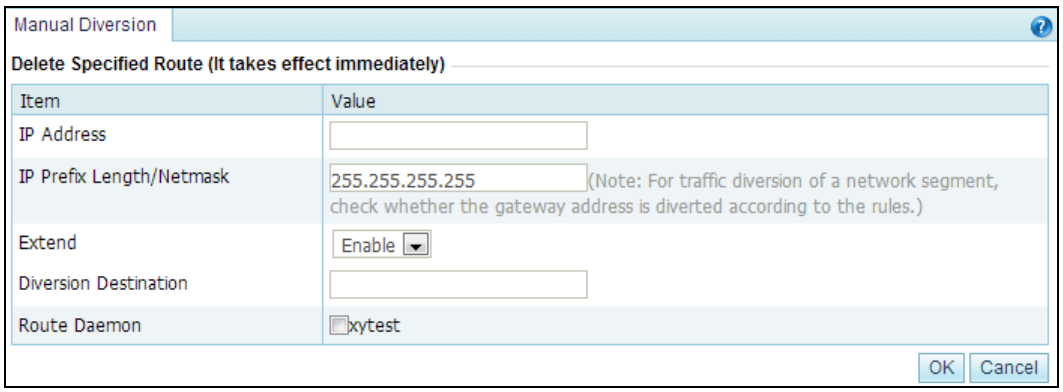
Note	For details on deleting diversion rules that are being used, see section 5.4.2.5 Deleting a Specified Route.

5.4.2.5 Deleting a Specified Route

Delete Specified is used to delete diversion rules that are being used. The detailed procedure is described as follows:

Step 1 On the manual diversion rule list in Figure 5-29, click **Delete Specified** to open the diversion rule deletion page.

Figure 5-32 Deleting a specified diversion rule



Step 2 Type the information about a diversion rule to be deleted and click **OK** to make the settings take effect.

----End

5.4.2.6 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 5-29, you can select **Periodical Refresh** to enable the periodical route refresh function or deselect it to disable the periodical route refresh function.

5.4.2.7 Canceling Injection Route Inspection

If **Cancel injection route inspection** is selected, manually configured diversion rules can be used without injection route inspection. If **Cancel injection route inspection** 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 tab page shown in Figure 5-29, you can select **Cancel injection route inspection** to disable injection route inspection, or deselect it to enable injection route inspection.

5.4.2.8 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 5-29, you can click **Restart Scheduling Service** and then click **OK** in the displayed dialog box, to restart the scheduling service.

5.4.3 Group Diversion

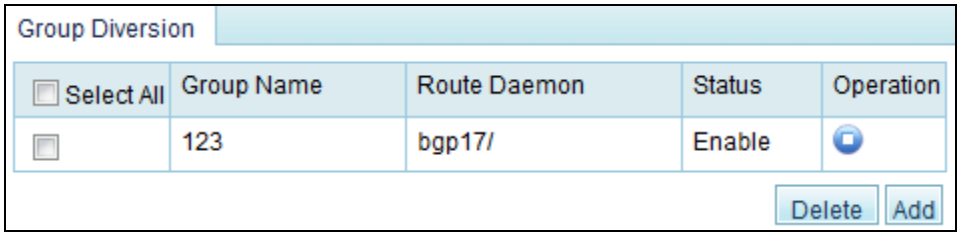
Group diversion rules are used to divert the traffic destined for a protection group to the diversion interface on the ADS device. This section describes how to add, delete, enable, and disable group diversion rules.

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 5-33 Group diversion rules



Step 2 Click **Add**.

Figure 5-34 Creating a group diversion rule

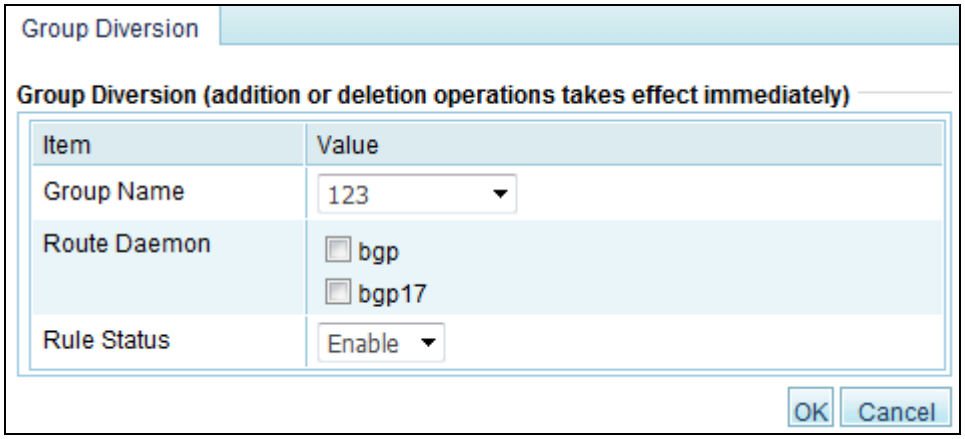


Table 5-14 describes parameters for creating a group diversion rule.

Table 5-14 Parameters for creating a group diversion rule

Parameter	Description
Group Name	Protection group whose traffic is to be diverted. For details on configuring a protection group, see section 4.1.2 Protection Groups.
Route Daemon	Route daemon
Rule Status	Controls whether to enable the group diversion rule.

Parameter	Description
	• **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 5-33, select one or more group diversion rules (or select the **Select All** check box to select all rules) to be deleted, click **Delete** to the lower right of the group diversion rule list, and click **OK** in the confirmation dialog box to delete 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 **Enable** for enabled rules and **Disable** for disabled rules.

- To delete group diversion rules, perform the following steps:

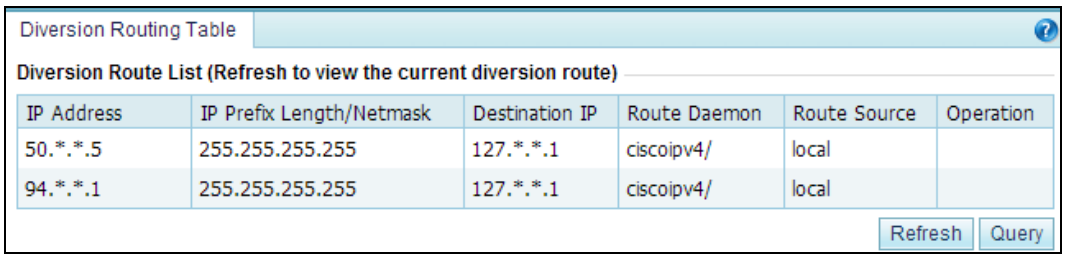
  On the group diversion rule list shown in Figure 5-33, click in the **Operation** column of a group diversion rule to enable it.
- To disable a group diversion rule, perform the following steps:

  On the group diversion rule list shown in Figure 5-33, click in the **Operation** column of a group diversion rule to disable it.

5.4.4 Diversion Routing Table

As shown in Figure 5-35, a diversion routing table stores diversion routes that are being used by the ADS device. It is automatically generated based on traffic diversion policies and diversion notifications from NSFOCUS ADS detection devices. Click **Refresh** to view the latest diversion routes of the system.

Figure 5-35 Diversion routing table



Searching for a Diversion Route

Step 1 Click **Query** to the lower right of the diversion routing table to open the diversion route search page.

The **Query Diversion Route** page appears, as shown in Figure 5-36.

Figure 5-36 Search for diversion routes

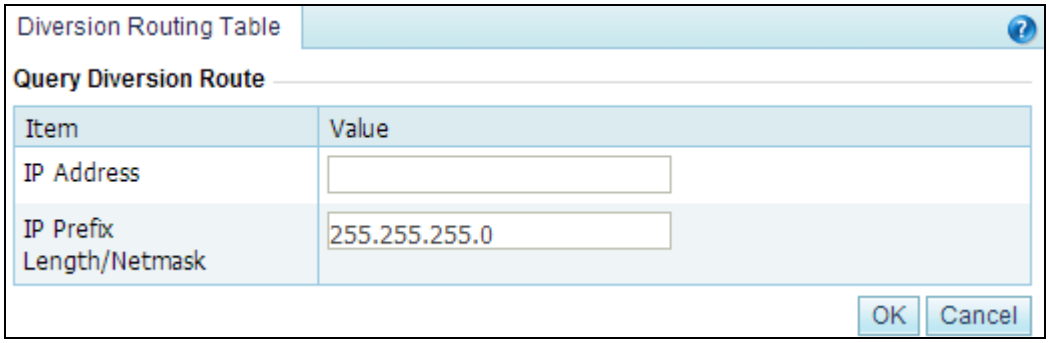


Table 5-15 describes parameters of a diversion route.

Table 5-15 Parameters of a diversion route

Parameter	Description
IP Address	IP address or IP segment specified by **IP Address** in the diversion routing table. You can type an IPv4 or IPv6 address according to the actual network deployment.
IP Prefix Length/Netmask	Prefix length (for the IPv6 protocol) or netmask (for the IPv4 protocol) of the IP address to be searched. **Note** The netmask of an IPv4 address to be searched must be 255.255.255.255.

Step 2 After parameters are configured, click **OK** to query the results.

Step 3 After querying the results, click **Back** to return to the diversion route list.

----End

5.5 Advanced Route Setting

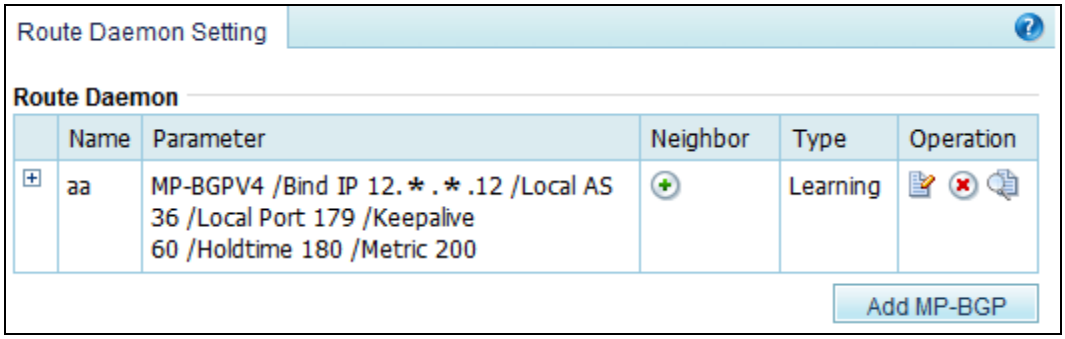
This section covers the following topics:

- MPLS Route
- Other Routes

5.5.1 MPLS Route

As shown in Figure 5-37, you can configure MPLS routes to accomplish layer 2 label learning between VPNs.

Figure 5-37 List of MPLS routes



Creating an MPLS Route

To the lower right of the route daemon list, click **Add MP-BGP**. On the **MP-BGP Local Parameter Setting** page, configure parameters and then click **OK**.

Figure 5-38 Creating an MPLS route

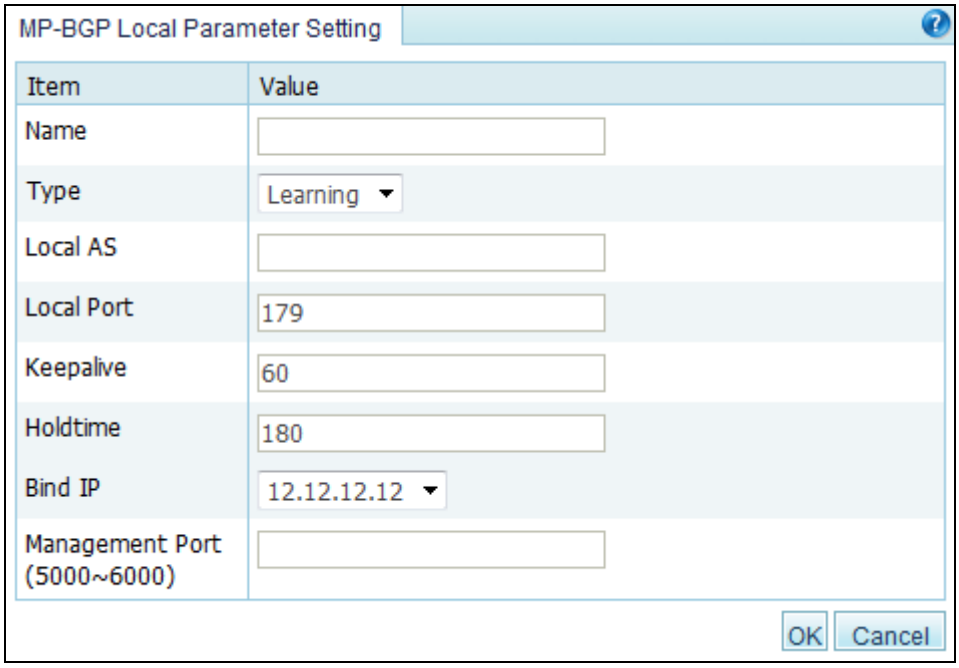


Table 5-16 describes parameters for creating an MPLS route.

Table 5-16 Parameters for creating an MPLS route

Parameter	Description
Name	Route daemon name.
Type	Type of the route. Currently, only **Learning** is available for selection.
Local AS	AS number of a BGP route daemon.
Local Port	BGP port of the route daemon. Generally, the default port **179** is used.
Bind IP	Local IPv4 address of a route daemon.
Management Port(5000~6000)	Management port of the route daemon. The port ranges from 5000 to 6000.

Other parameters such as **Keepalive** and **Holdtime** correspond to certain fields within the BGPv4 protocol.

Editing a Route

In the list of MPLS routes, click to edit the corresponding route.

Deleting a Route

In the list of MPLS routes, click to delete the corresponding route.

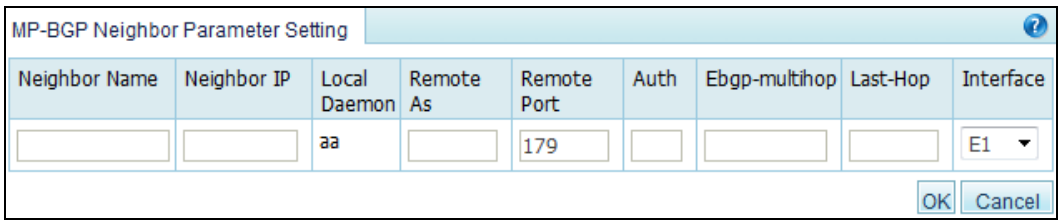
Viewing Route Status

In the list of MPLS routes, click to view status of the corresponding route.

Adding a Neighbor

In the list of local routes, click to add a neighbor for the MPLS route. See Figure 5-39.

Figure 5-39 Adding a neighbor for MPLS route



Note	After adding a neighbor, click to check whether the neighbor is connected.

Viewing Neighbor Status

In the list of local routes, click to view connection status of the MPLS neighbor.

Hiding a Neighbor

Neighbors of each route are displayed in the MPLS route list initially. Click ⊟ of a route to hide its neighbors and click ⊞ to display them.

5.5.2 Other Routes

In addition to routing protocols described above, the ADS device supports such advanced routing protocols as OSPF, ISIS, RIP, OSPF6, and LDP.

Currently, the administrator, **admin**, can configure LDP routes or view, enable, or disable OSPF, ISIS, RIP, OSPF6, and LDP routes on the web-based manager, while the CLI administrator, **routerman**, can configure OSPF, ISIS, RIP, and OSPF6 routes on the CLI.

Configuring an LDP Route

Step 1 After logging in to the web-based manager, choose **Diversion & Injection** > **Advanced Route Setting** > **Others** to open the list of other routes.

Figure 5-40 List of other routes

Step 2 Click in the **Operation** column to edit LDP route parameters.

Figure 5-41 Editing LDP route parameters

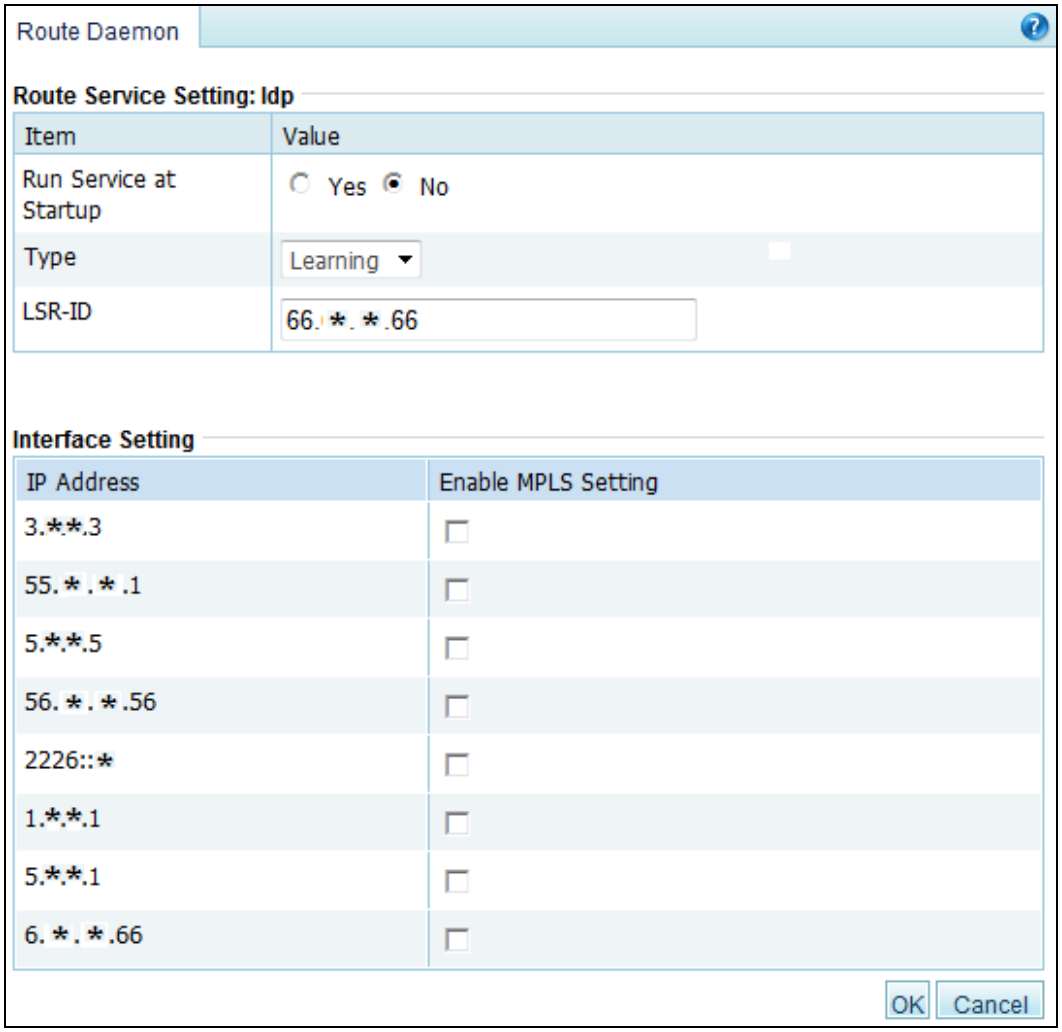


Table 5-17 describes LDP route parameters.

Table 5-17 LDP route parameters

Parameter	Description
Run Service at Startup	Controls whether to run LDP upon system startup. • **Yes**: indicates that the system runs LDP upon system startup. • **No**: indicates that the system does not run LDP upon system startup.
Type	Route type. The default route type is **Learning**.
LSR-ID	Label switching router ID.
Interface Setting	Interfaces on which MPLS and LDP are enabled.

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

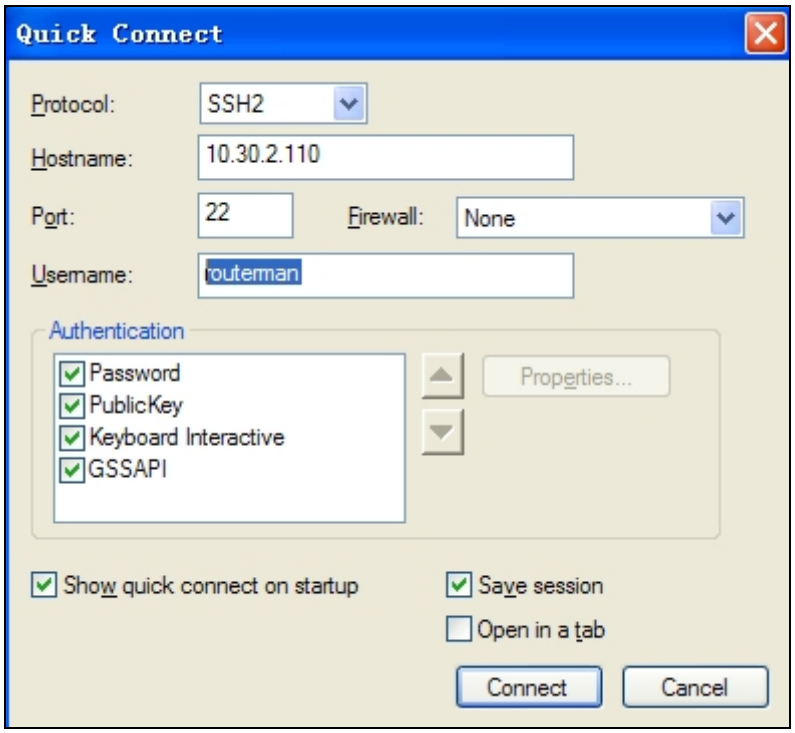
----End

Configuring OSPF, ISIS, RIP, and OSPF6 Routes

Here, the OSPF route is used as an example to describe the route configuration procedure.

Step 1 As the CLI administrator, **routerman**, log in to the ADS device in SSH mode.

Figure 5-42 ADS login in SSH mode



Step 2 Enable OSPF on the interface via the CLI.

Figure 5-43 Editing OSPF route parameters

```
COLLAPSAR-4000#router ospf session
Trying 127.*.*.1...
                    Connected to 127.*.*.1.
                                            Escape character is '^]'.

Hello, this is Quagga (version 0.99.5).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password:
```

Step 3 After the parameter configuration is complete, save the settings and exit.

----End

Viewing Route Status

After logging in to the web-based manager, the administrator, **admin**, can click to view the status of a route of a specific protocol in the route protocol list shown in Figure 5-40.

Enabling/Disabling the Route Protocol

After logging in to the web-based manager, the administrator, **admin**, can click to enable a route of a specific protocol or click to disable a route in the route protocol list as shown in Figure 5-40.

Note	Routes under **Others** cannot be deleted.

5.6 Syslog Diversion Configuration

NSFOCUS ADS can collaborate with abnormal traffic detection devices from other vendors, such as Genie, Arbor, Samurai, and Kuanguang, to jointly protect customers' networks against DDoS attacks.

Third-party devices provide effective abnormal traffic detection. After accurately locating the potential attack source and attack target, such a device handles the event according to the syslog-based diversion settings configured on ADS. If the diversion type is set to **Auto**, it notifies ADS, which then automatically diverts the abnormal traffic for cleaning. After filtering the traffic, ADS injects the normal traffic back into the network. If the diversion type is set to **Manual**, it notifies ADS, which, in turn, notifies the O&M personnel, who will then decide whether to divert the traffic.

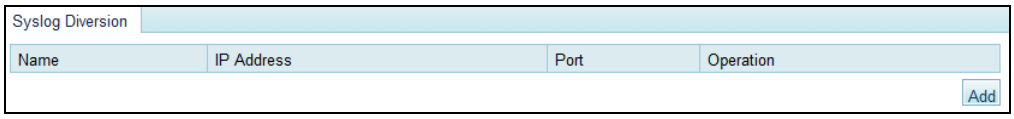
Note	For Genie and Arbor devices, the diversion type can be either **Auto** or **Manual**. For Samurai and Kuanguang devices, the diversion type can only be **Auto**.

5.6.1 Diversion Configuration

To configure syslog-based traffic diversion, follow the following steps:

Step 1 Choose **Diversion & Injection** > **Syslog Diversion Config** > **Diversion Config**.

Figure 5-44 Syslog-based diversion rule list



Step 2 Click **Add**.

Figure 5-45 Creating a diversion rule

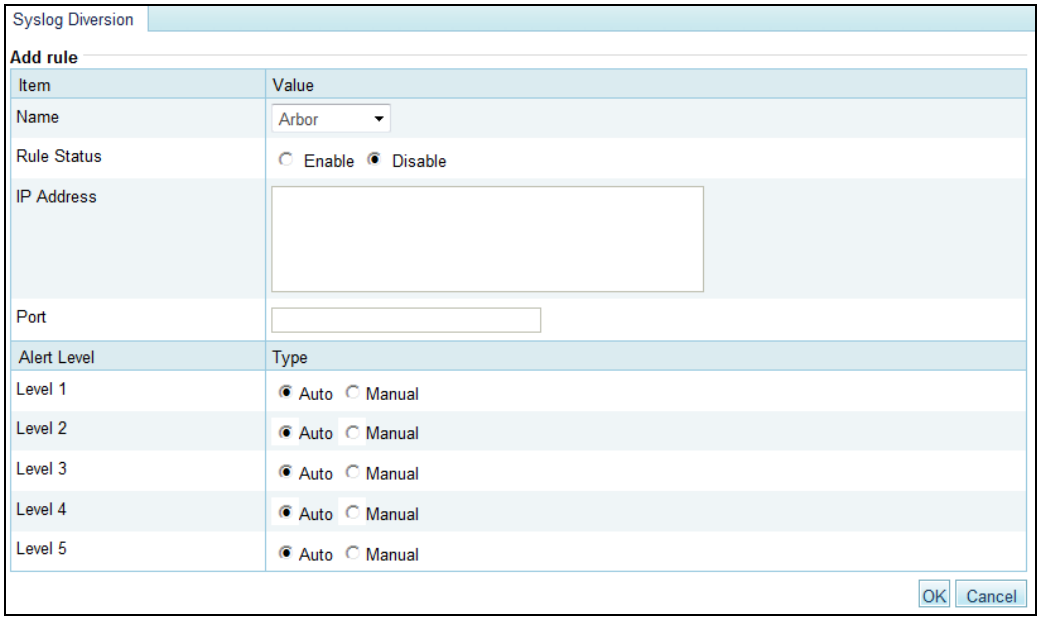


Table 5-18 describes parameters on the page.

Table 5-18 Parameters for creating a syslog-based diversion rule

Parameter	Description
Name	Specifies the type of the device to collaborate with ADS for syslog-based traffic diversion. It can be **Genie**, **Arbor**, **Samurai**, or **Kuanguang**.
Rule Status	Status of the rule. The rule takes effect only after it is enabled.
IP Address	IP address of the third-party device.
Port	Port for communicating with the third-party device.
Alert Level	Specifies the alert level that will trigger traffic diversion. This parameter is available only for Genie and Arbor devices. • On a Genie ATM device, alert levels for abnormal traffic are classified into critical and warning. **Auto** indicates that the Genie ATM device, after detecting abnormal traffic of the corresponding alert level, notifies ADS, which then automatically diverts such traffic for cleaning. **Manual** indicates that the Genie ATM device, after detecting abnormal traffic, notifies ADS, which, in turn, notifies the O&M personnel, who will then determine whether to divert the traffic. • On an Arbor device, alert levels for abnormal traffic are classified into five levels (level 1 to level 5). **Auto** indicates that the Arbor device, after detecting abnormal traffic of the corresponding alert level, notifies ADS, which then automatically diverts such traffic for cleaning. **Manual** indicates that the Arbor device, after detecting abnormal traffic, notifies ADS, which, in turn, notifies the O&M personnel, who will then determine whether to divert the traffic.

Step 3 After configuring parameters, click **OK** to save the settings.

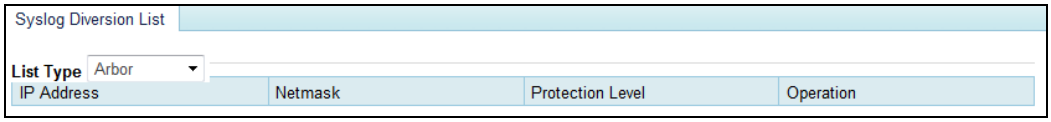
----End

5.6.2 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 5-46 Syslog Diversion list



6 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.

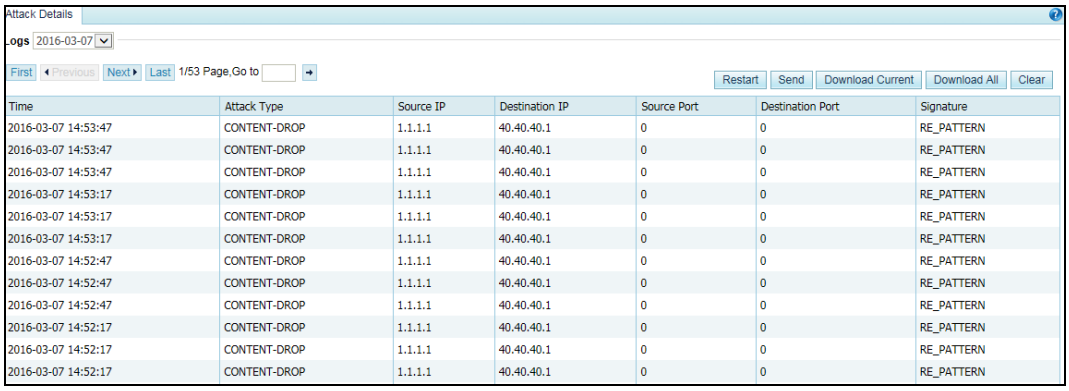
6.1 Attack Logs

All attack logs are displayed in two ways for easier viewing: statistical graph and data table.

6.1.1 Attack Details

You can view attack logs of the last 15 days, as shown in Figure 6-1. By default, attack logs of the current day are listed.

Figure 6-1 Attack logs



Time	Attack Type	Source IP	Destination IP	Source Port	Destination Port	Signature
2016-03-07 14:53:47	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:53:47	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:53:47	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:53:17	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:53:17	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:53:17	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:52:47	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:52:47	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:52:47	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:52:17	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:52:17	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN
2016-03-07 14:52:17	CONTENT-DROP	1.1.1.1	40.40.40.1	0	0	RE_PATTERN

Table 6-1 describes attack log parameters.

Table 6-1 Attack log parameters

Parameter	Description
Time	Time when the attack occurs.
Attack Type	Type of the attack.
Source IP/Port	Source IP address and port of the attack.
Destination IP/Port	Destination IP address and port of the attack.
Signature	Signature defined by the system for various types of attacks. For example, the signature of SYN flood attacks is **SYN-CHECK**.

To the upper right of the log table, you can operate on attack logs as follows:

- Restart the log service.

  Click **Restart** to restart the log service program.
- Send logs.

  Click **Send** to send current attack logs to a specific email address.
- Download logs.

  Click **Download Current** to download logs of the specified date or click **Download All** to download all logs. This makes it easier for administrator to search and handle logs.
- Clear logs.

  Click **Clear** to clear all the attack information of the current day.

6.1.2 Statistical Graph

At the bottom of the **Statistical Graph** page, you can click **Pie Chart** to view the proportion of each type of attacks or click **Bar Chart** to view the number of attacks of each type on the current day. See Figure 6-2 and Figure 6-3.

Figure 6-2 Attack proportion

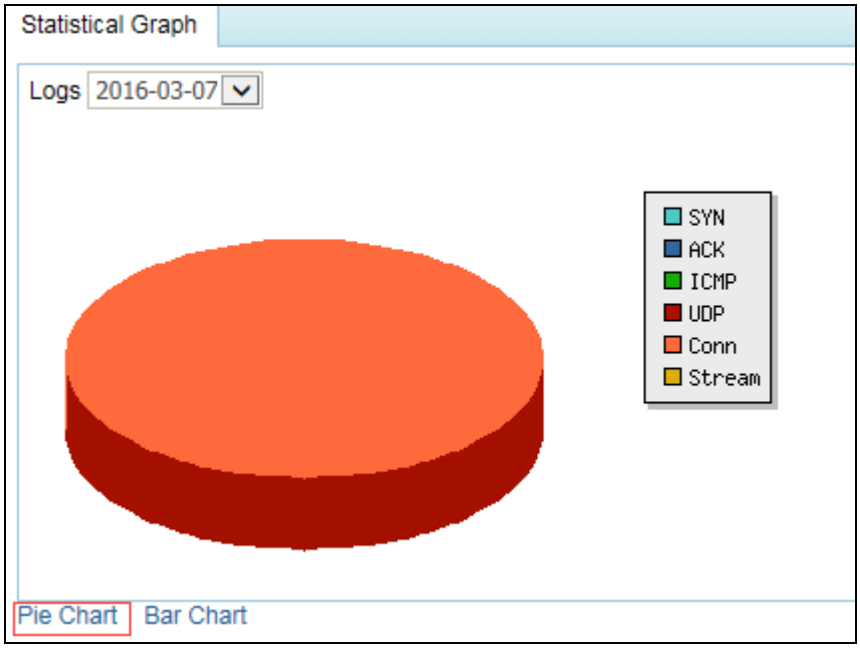
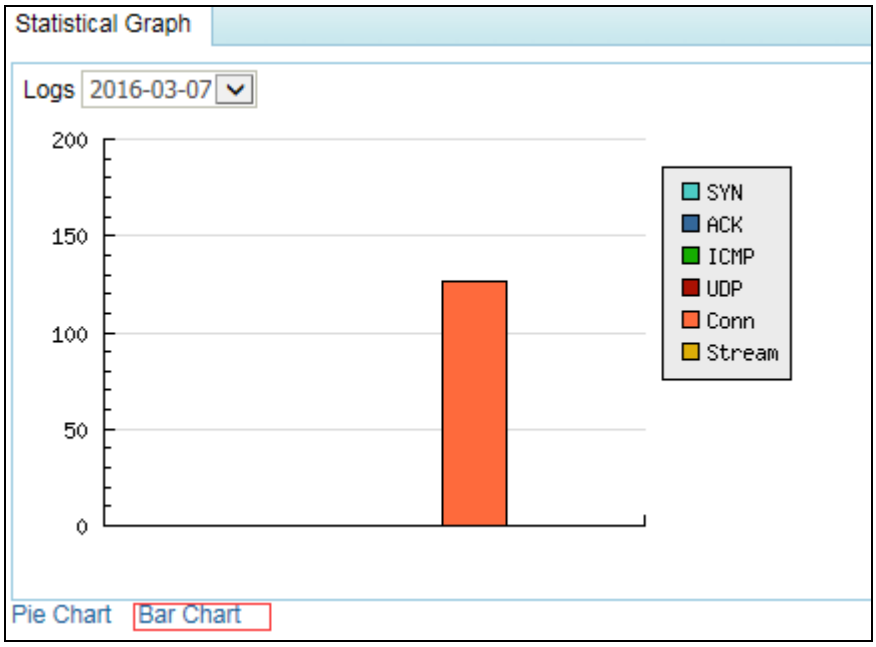


Figure 6-3 Number of attacks of each type



6.2 System Logs

System logs include the following:

- System Operation Logs
- System Login Logs

- Link Status Logs
- Traffic Diversion Logs
- HA Synchronization Logs
- Syslog Diversion Logs

6.2.1 System Operation Logs

As shown in Figure 6-4, the system operation log table displays main operations of users in the system.

Figure 6-4 System operation logs

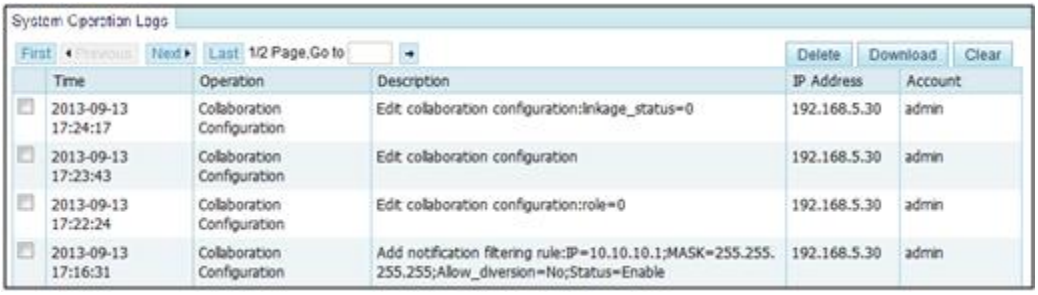


Table 6-2 describes parameters of system operation logs.

Table 6-2 Parameters of system operation logs

Parameter	Description
Time	Time when a user performs an operation.
Operation	Operation performed by a user.
Description	Details about an operation.
IP Address	IP address of the host on which the operation is performed.
Account	Account of the user that performs the operation.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download operation logs to the local host in text format.
- Clear logs.

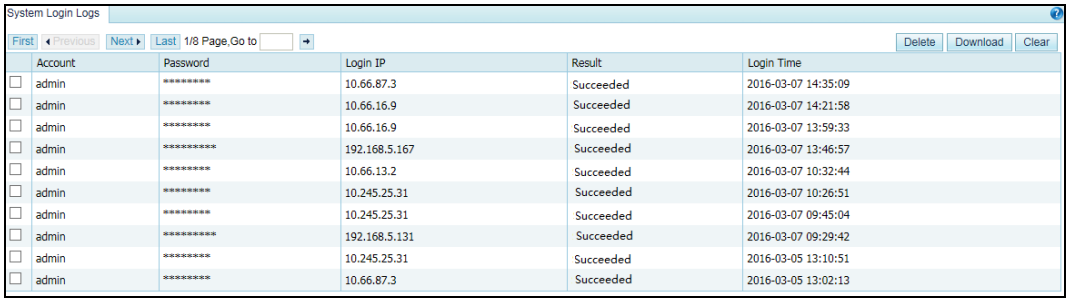
  Click **Clear** to clear all the current operation logs after confirmation.
- Delete logs.

  Select one or more checkboxes preceding logs and click **Delete** to delete logs.

6.2.2 System Login Logs

As shown in Figure 6-5, the system login log table displays system login details.

Figure 6-5 System login logs



Account	Password	Login IP	Result	Login Time
admin	********	10.66.87.3	Succeeded	2016-03-07 14:35:09
admin	********	10.66.16.9	Succeeded	2016-03-07 14:21:58
admin	********	10.66.16.9	Succeeded	2016-03-07 13:59:33
admin	*********	192.168.5.167	Succeeded	2016-03-07 13:46:57
admin	********	10.66.13.2	Succeeded	2016-03-07 10:32:44
admin	********	10.245.25.31	Succeeded	2016-03-07 10:26:51
admin	********	10.245.25.31	Succeeded	2016-03-07 09:45:04
admin	*********	192.168.5.131	Succeeded	2016-03-07 09:29:42
admin	********	10.245.25.31	Succeeded	2016-03-05 13:10:51
admin	********	10.66.87.3	Succeeded	2016-03-05 13:02:13

Table 6-3 describes parameters of system login logs.

Table 6-3 Parameters of system login logs

Parameter	Description
Account	User name used by a user for login
Password	Password used by a user for login
Local IP	IP address of a login user
Result	Whether the login succeeded or failed
Login Time	Time when an account logs in

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download login logs to the local host in text format.
- Clearing logs.

  Click **Clear** to clear all current login logs after confirmation.
- Delete logs.

  Select one or more checkboxes preceding logs and click **Delete** to delete logs.

6.2.3 Link Status Logs

As shown in Figure 6-6, the link status log table displays the interface connection status (UP to DOWN or DOWN to UP) of ADS.

Figure 6-6 Link status logs

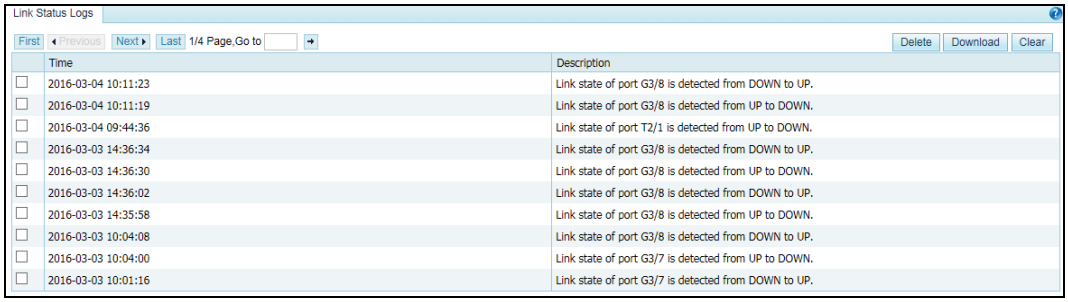


Table 6-4 describes parameters of link status logs.

Table 6-4 Parameters of link status logs

Parameter	Description
Time	Time when the status of an interface changes.
Description	Status change details of an interface.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download link status logs to the local host in text format.
- Clear logs.

  Click **Clear** to clear all current link status logs after confirmation.
- Delete logs.

  Select one or more checkboxes preceding logs and click **Delete** to delete logs.

6.2.4 Traffic Diversion Logs

As shown in Figure 6-7, the traffic diversion log table displays the route operations performed by ADS upon receiving alerts from NSFOCUS ADS detection devices, as well as manual diversion routing operations performed on the web-based manager. Logs remain available for 10 days at most.

Note	Traffic diversion logs can be viewed only in cluster running modes.

Figure 6-7 Traffic diversion logs

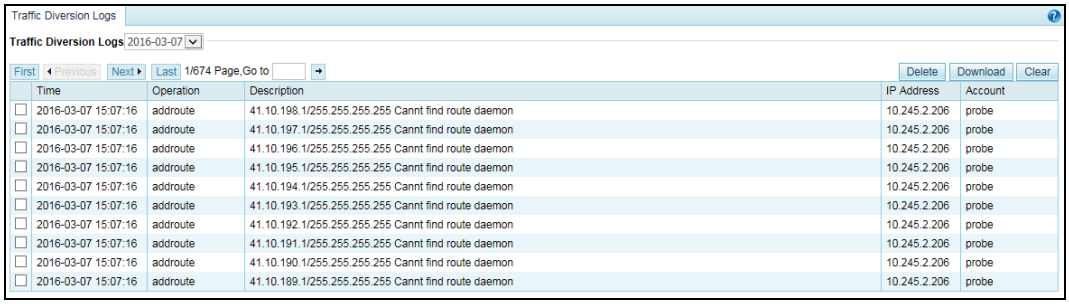


Table 6-5 describes parameters of traffic diversion logs.

Table 6-5 Parameters of traffic diversion logs

Parameter	Description
Time	Time when traffic diversion happens.
Operation	Type of traffic diversion operations.
Description	Destination IP address and of the traffic to be diverted, netmask of the destination IP address, and the diversion destination IP address. If the operation is **Change Status**, changes of the status will also be displayed.
IP Address	IP address of ADS that divert the traffic or NSFOCUS NTA that detects attack traffic. Either an IPv4 or IPv6 address is allowed.
Account	User name (for example, **admin**) that performs traffic diversion or device name (for example, **probe**) of NSFOCUS NTA.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download traffic diversion logs to the local host in text format.
- Clear logs.

  Click **Clear** to clear all current traffic diversion logs after confirmation.
- Delete logs.

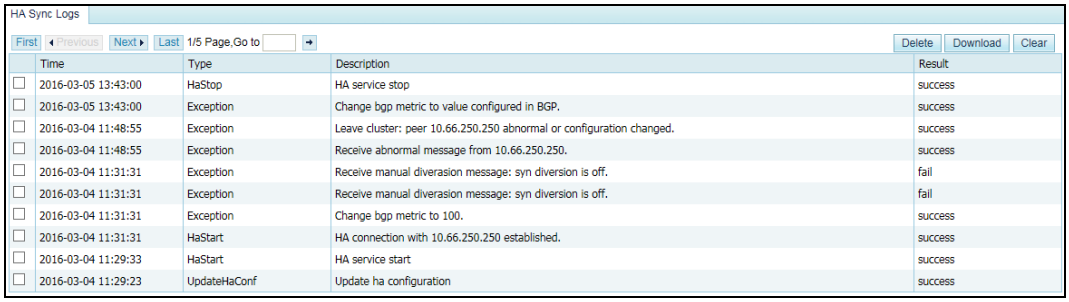
  Select one or more checkboxes preceding logs and click **Delete** to delete logs.

6.2.5 HA Synchronization Logs

When the keepalive information, synchronization information (MAC address, diversion information, and protection group information), and engine failure information is synchronized between active and standby ADS devices, the two devices record such operations as HA synchronization logs for statistics and analysis.

Choose **Logs** > **System Logs** > **HA Sync Logs**. The **HA Sync Logs** page appears, as shown in Figure 6-8.

Figure 6-8 HA synchronization logs



Time	Type	Description	Result
2016-03-05 13:43:00	HaStop	HA service stop	success
2016-03-05 13:43:00	Exception	Change bgp metric to value configured in BGP.	success
2016-03-04 11:48:55	Exception	Leave cluster: peer 10.66.250.250 abnormal or configuration changed.	success
2016-03-04 11:48:55	Exception	Receive abnormal message from 10.66.250.250.	success
2016-03-04 11:31:31	Exception	Receive manual diverasion message: syn diversion is off.	fail
2016-03-04 11:31:31	Exception	Receive manual diverasion message: syn diversion is off.	fail
2016-03-04 11:31:31	Exception	Change bgp metric to 100.	success
2016-03-04 11:31:31	HaStart	HA connection with 10.66.250.250 established.	success
2016-03-04 11:29:33	HaStart	HA service start	success
2016-03-04 11:29:23	UpdateHaConf	Update ha configuration	success

Table 6-6 describes parameters of HA synchronization logs.

Table 6-6 Parameters of HA synchronization logs

Parameter	Description
Time	Time when a log is recorded.
Type	What type of information a log records. • **HaStart**: indicates that the log records HA connection establishment. • **Exception**: indicate that the log records exceptions. • **SyncConf**: indicates that the log records file and heartbeat synchronization.
Description	Log details.
Result	Operation result, which could be **success** or **fail**.

To the upper right of the log table, you can operate on logs as follows:

- Download logs.

  Click **Download** to download HA synchronization logs to the local host in text format.
- Clear logs.

  Click **Clear** to clear all current HA synchronization logs after confirmation.
- Delete logs.

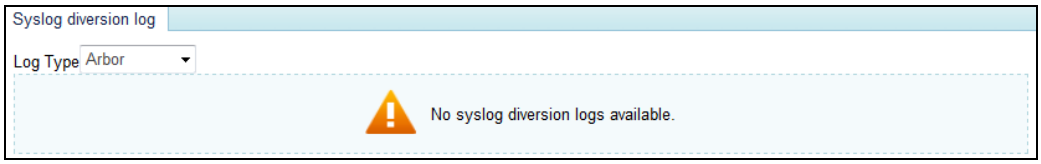
  Select one or more checkboxes preceding logs and click **Delete** to delete logs.

6.2.6 Syslog Diversion Logs

As shown in Figure 6-9, the syslog diversion log list displays logs generated during collaboration between NSFOCUS ADS and a third-party device from Genie, Arbor, Samurai, or Kuanguang. Logs can be retained for 10 days at most.

Note	• Syslog diversion logs can be viewed only in cluster running mode. • Currently, ADS uses only IPv4 addresses to collaborate with third-party devices in either IPv4 or dual-stack mode.

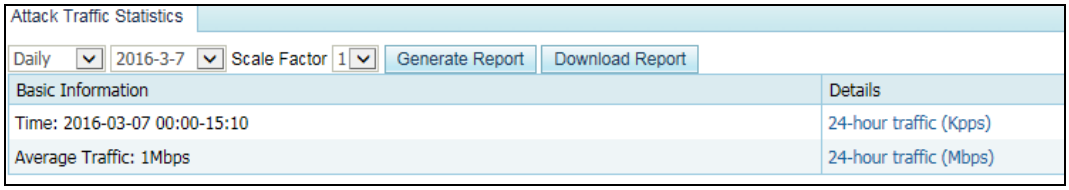
Figure 6-9 Syslog diversion logs



6.3 Log Analysis

As shown in Figure 6-10, you can set query conditions and click **Generate Report** to generate reports in chronological order. ADS supports three types of reports: daily report, weekly report, and monthly report. Note that the scale factor cannot be changed for a daily report. In addition, you can click **Download Report** to download the generated report to the local host.

Figure 6-10 Attack traffic statistics



Daily Attack Traffic Report

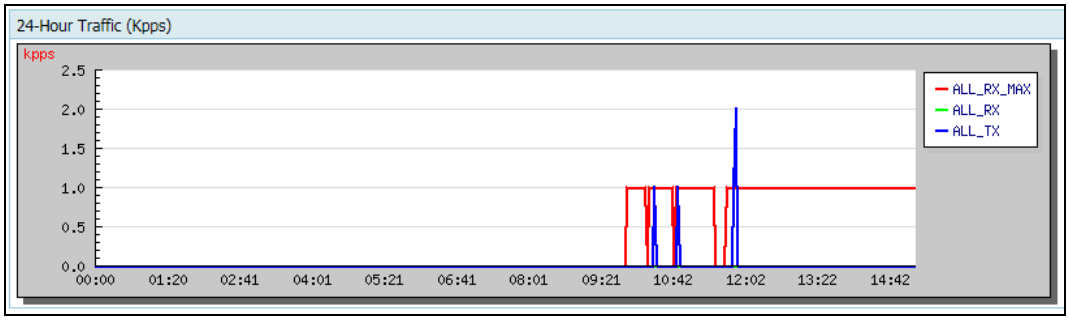
The **Basic Information** column includes statistical time, average incoming traffic, average normal incoming traffic, and average outgoing traffic (unit: Mbps) about attacks on a specific day.

The Details column contains the following information:

- 24-hour traffic (kpps)

  As shown in Figure 6-11, incoming/outgoing traffic (unit: kpps) of a specific day is displayed.

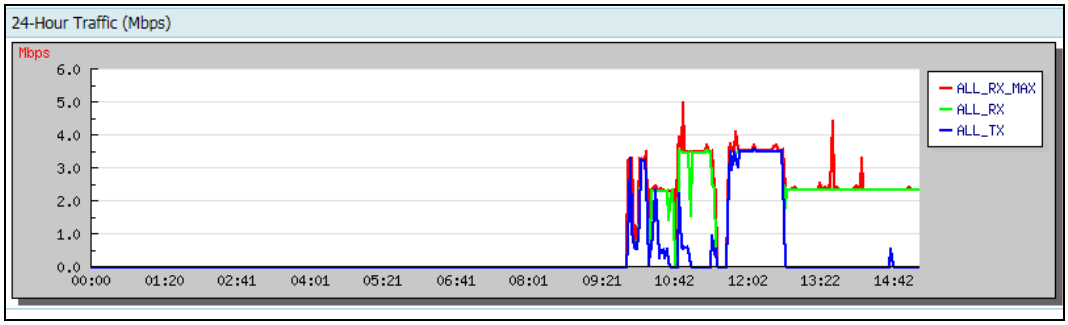
Figure 6-11 24-hour traffic (kpps)



- 24-hour traffic (Mbps)

  As shown in Figure 6-12, incoming/outgoing traffic (unit: Mbps) of a specific day is displayed.

Figure 6-12 24-hour traffic (Mbps)



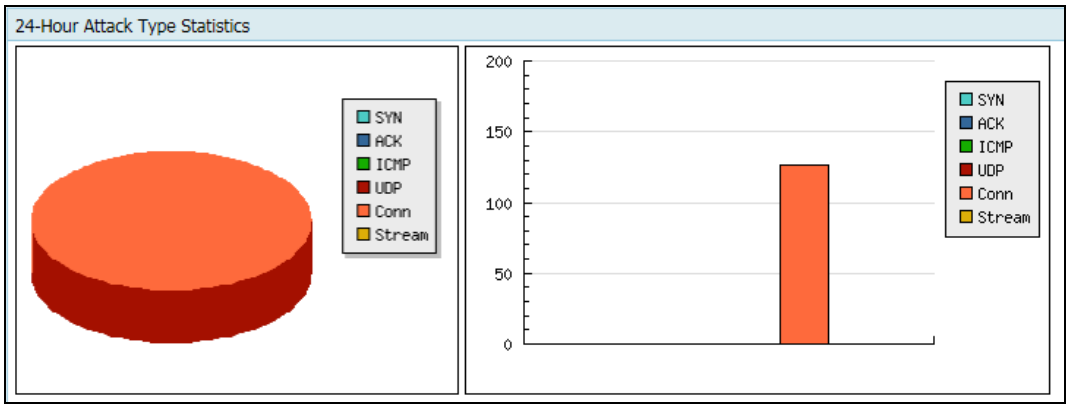
- 24-hour attack type statistics

  As shown in Figure 6-13, types of attacks on a specific day are displayed in a pie chart and a bar chart.

  – Pie chart: Proportion of each type of attacks on the current day.

  – Bar chart: Number of each type of attack logs on the current day.

Figure 6-13 24-hour attack type statistics



- 24-hour attacked IP statistics

  As shown in Figure 6-14, attacked IP addresses and attack traffic on a specific day are displayed in the list.

Figure 6-14 24-hour attacked IP statistics

24-Hour Attacked IP Statistics(Top5)

Attacked IP	SYN Flood	ACK Flood	ICMP Flood	UDP Flood	Connection Flood	Stream Flood
40.40.40.1	0	0	0	0	8	0
0040:0040:0040:0001:0000:0000:0000:0001	0	0	0	0	16	0

Weekly Attack Traffic Report

A weekly report is similar to a daily report, except that the statistical period is one week.

Monthly Attack Traffic Report

A monthly report is similar to a daily report, except that the statistical period is one month.

Note	The system can generate data only when it is running.

7 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 Service	Describes how to configure system log services and export SFTP/SSH logs.
Others	Describes how to upgrade the system, manage the license, enable remote assistance, and view version information.

7.1 Local Settings

This section covers the following topics:

- Basic Information
- Interface Configuration
- User Management
- Management Mode Configuration
- Configuration File Import and Export
- HA Configuration
- (Optional) Bypass Configuration
- Collaboration Configuration
- Bandwidth Overrun Limit Configuration

7.1.1 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 the communication with IPv4 nodes and IPv6 nodes.

Note	The dual-stack technology is an IPv4-to-IPv6 transition technology. If a source node supports both IPv4 and IPv6 protocol stacks, it transmits packets based on the protocol stack that adopted by the destination node.

The administrator 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 7-1.

Figure 7-1 Basic Settings page

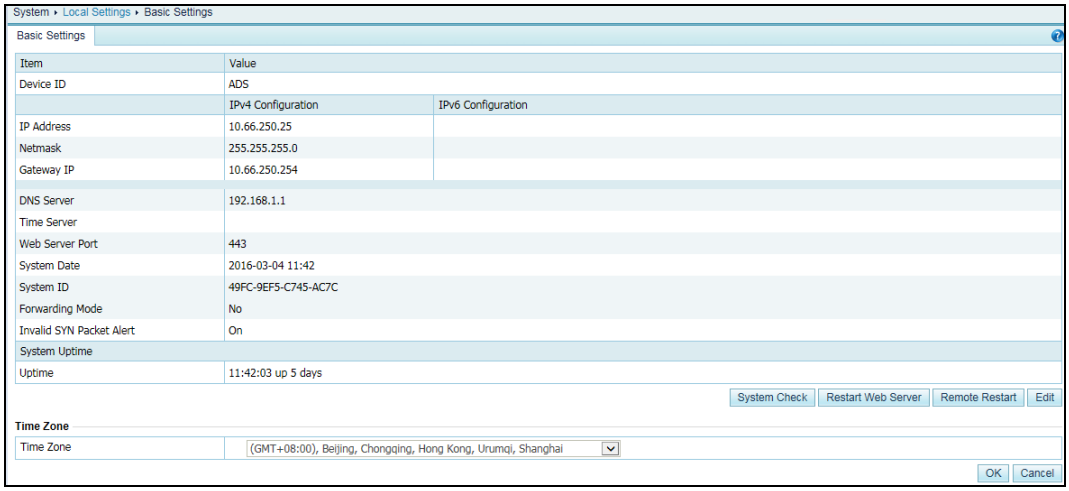


Table 7-1 Basic system settings

Parameter	Description
Device ID	Device model. It cannot exceed 26 characters.
IP Address/Netmask	IPv4 address/netmask or IPv6 address/prefix length of the management interface of ADS. Note • ADS supports the IPv4/IPv6 dual-stack. Therefore, you can configure the IPv4 or IPv6 address for the management interface according to the actual network deployment. • The device administrator can use this IP address to exercise remote vulnerability management via HTTPS, perform log-related operations, and send emails.
Gateway IP	IP address of the gateway for the IPv4 or IPv6 address of the management interface.
DNS Server	IP address of the DNS server used by the management interface of the current ADS device.
Time Server	IP address or domain name of a server that synchronizes time on the current ADS and other NSFOCUS devices. All connected NSFOCUS

Parameter	Description
	devices will synchronize the time with the time server automatically. Note: When you type a domain name here, you must configure the DNS server. If you do not want to specify the DNS server, you must type an IP address for the time server.
Web Server Port	The 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	A unique ID of ADS. It is the credential for applying for the device license.
Forwarding Mode	It is used for network troubleshooting. The value **Yes** indicates that the current ADS directly forwards the packets without any check.
Invalid SYN Packet Alert	• After **Invalid SYN Packet Alert** is set to **On**, when detecting a SYN packet smaller than 64 bytes, ADS logs a SYN_INVALID event, generates a sound alert, and drops the illegitimate packet. • After **Invalid SYN Packet Alert** is set to **Off**, when detecting a SYN packet smaller than 64 bytes, ADS does not log SYN_INVALID attacks or generate a sound alert, but drops illegitimate packets.
Uptime	Length of time during which the current ADS operates properly.

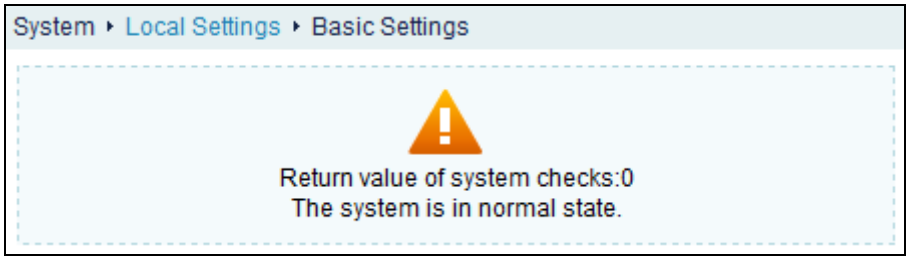
On the **Basic Settings** page shown in Figure 7-1, you can perform the following operations:

- Edit basic system information.

  Click **Edit** to open the **Modify basic settings** page. Modify parameter settings and click **OK** to commit 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 7-2.

Figure 7-2 System check results



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

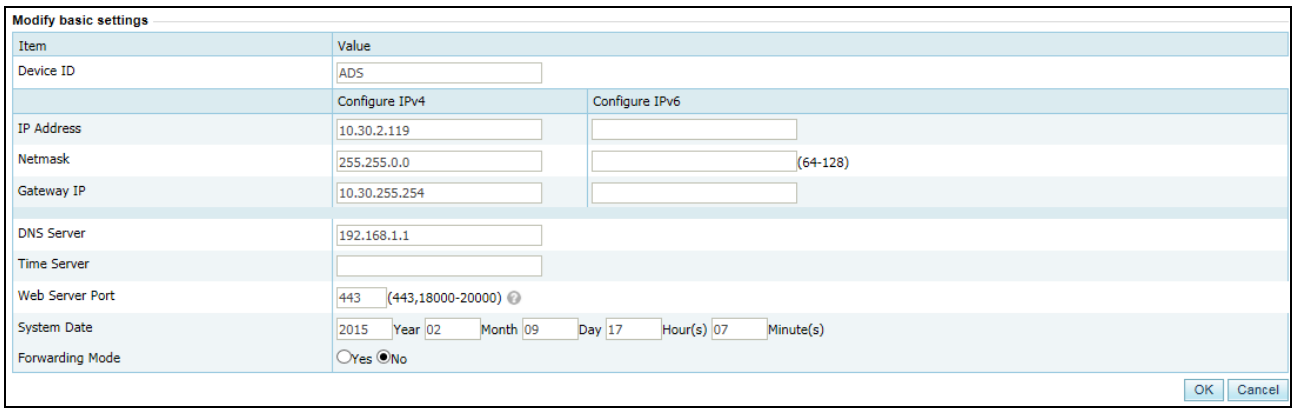
- Change the web server port.

b. Click **Edit** to open the **Modify basic settings** page and modify the web server port, as shown in page Figure 7-3.

It can be 443 or an integer ranging from 18000 to 20000.A conflicting port may make the web service inaccessible. If **Web Server Port** is not set to 443, the third-party device

and ADS M management function may be affected. For example, if **Web Server Port** is not set to 441, the accessible address of ADS is changed to https://*.*.*.*:441.

Figure 7-3 Modify basic settings page



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

d. Click **Restart Web Server** on the page shown in Figure 7-1.

----End

- Restart the system remotely.

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

- Configure the time zone.

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

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

7.1.2 Interface Configuration

The number and type of interfaces vary with ADS models.

ADS NX3-2010, NX3-2020, NX3-4020, and NX5-6025 provide the following numbers of working interfaces at most:

- Eight 1000M electrical ports
- Eight 1000M optical ports
- Four 1000M electrical ports
- Four 1000M optical ports
- Two 10G optical ports

ADS NX5-8000 provides the following working interfaces:

- Eight 1000M electrical ports
- Eight 1000M optical ports
- Four 10G optical ports

ADS NX3-200E and NX3-600E provide six 1000M electrical ports.

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

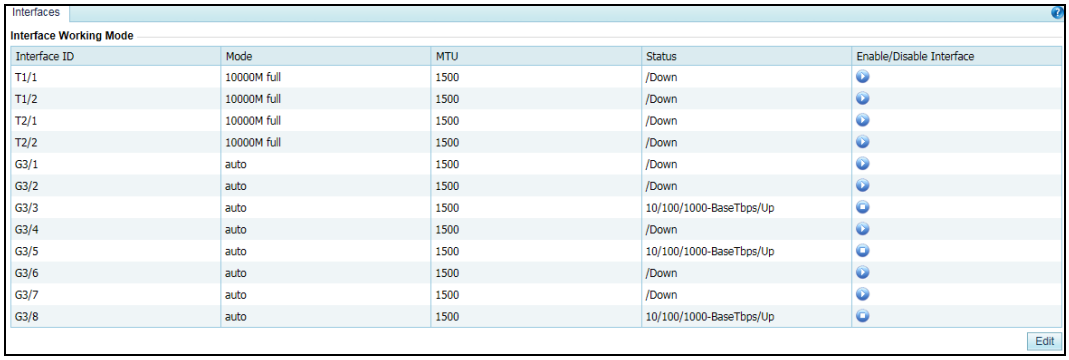
This section describes those operations in detail.

Enabling or Disabling Working Interfaces

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

Figure 7-4 shows the interface working mode of ADS NX5-4020.

Figure 7-4 Interface working mode of ADS NX5-4020



Interfaces

Interface Working Mode

Interface ID	Mode	MTU	Status	Enable/Disable Interface
T1/1	10000M full	1500	/Down	
T1/2	10000M full	1500	/Down	
T2/1	10000M full	1500	/Down	
T2/2	10000M full	1500	/Down	
G3/1	auto	1500	/Down	
G3/2	auto	1500	/Down	
G3/3	auto	1500	10/100/1000-BaseTbps/Up	
G3/4	auto	1500	/Down	
G3/5	auto	1500	10/100/1000-BaseTbps/Up	
G3/6	auto	1500	/Down	
G3/7	auto	1500	/Down	
G3/8	auto	1500	10/100/1000-BaseTbps/Up	

Edit

Table 7-2 describes interface working mode parameters.

Table 7-2 Interface working mode parameters

Parameter	Description
Interface ID	ADS NX3-2010, NX3-2020, NX3-200E, NX3-600E, NX5-4020, and NX5-6025: • T1/1 and T1/2: 10G optical ports. • G2/1 through G2/8:1000M electrical ports. • F3/1 through F3/8: 1000M optical ports. ADS NX5-8000: • T1/1 and T1/2: 10G optical ports. • G2/1 through G2/8:1000M electrical ports. • F3/1 through F3/8: 1000M optical ports. **Note** Interface numbers here are provided for illustration only. They may differ from the actual numbers as boards may be inserted into different slots.
Mode	The default value is **auto**, indicating that the interface is working in auto negotiation mode. • **10M full**: indicates that the interface is currently operating at 10 Mbps and in full duplex mode. • **10M half**: indicates that the interface is currently operating at 10 Mbps and in half duplex mode. • **100M full**: indicates the interface is currently operating at 100 Mbps and in full duplex mode.

Parameter	Description
	• **100M half**: indicates the interface is currently operating at 100 Mbps and in half duplex mode. • **1000M full**: indicates the interface is currently operating at 1000 Mbps and in full duplex mode. • **1000M half**: indicates the interface is currently operating at 1000 Mbps and in half duplex mode. • **10000M full**: indicates the interface is currently operating at 10000 Mbps and in full duplex mode.
MTU	By default, the MTU is **1500** for all working interfaces. It cannot be edited.
Status	• **Up**: indicates that the current interface is enabled. • **Down**: indicates the current interface is disabled. • **Unknown**: indicates that the status of the current interface is unknown because the network cable is disconnected or the current interface cannot work with the peer interface. **10/100/1000-Base Tbps** and **10 Gbps** are Tx rates of interfaces.

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

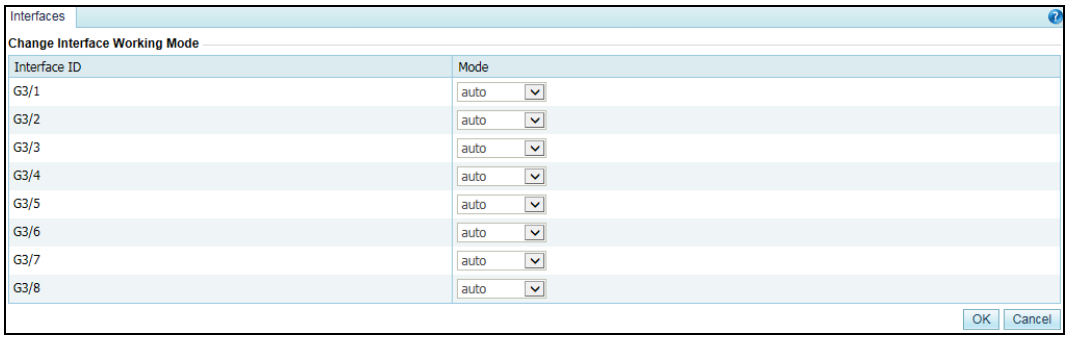
----End

Changing the Working Mode of 1000M Electrical Ports

ADS NX5-4020 is used as an example here.

On the **Interface** page in Figure 7-4, click **Edit** to change the working mode of 1000M electrical ports (G3/1 through G3/4).

Figure 7-5 Changing the working mode of 1000M electrical ports

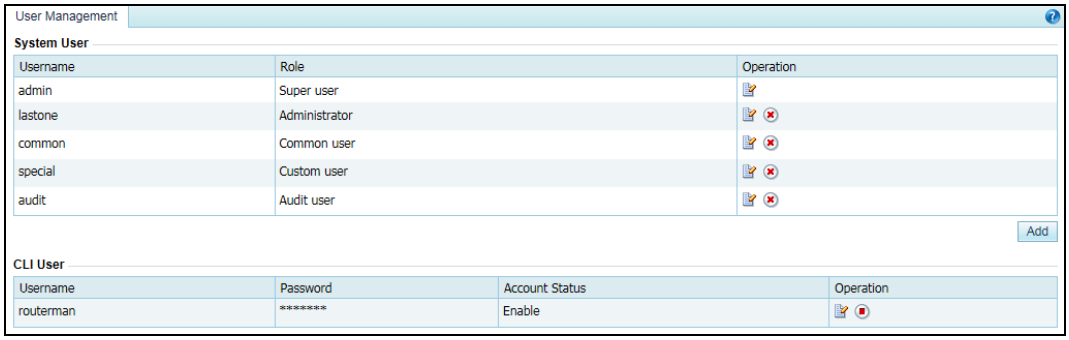


After changing the working mode, click **OK** to save the settings.

7.1.3 User Management

As shown in Figure 7-6, the **User Management** page displays all system users. Initially, only the default web user **admin** and the CLI user **routerman** are available.

Figure 7-6 System users

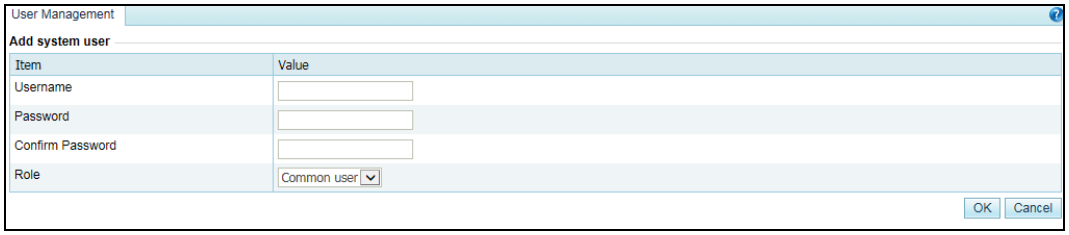


User roles include super user (**admin** by default), CLI user (**routerman** by default), custom user, common user, administrator, and audit user. For privileges of these user roles, see Table 2-1.

Adding a User

Click **Add** in the **System User** area to add a system user. On the page shown in Figure 7-7, configure the user name and login password, and select a role that defines its operation privilege.

Figure 7-7 Adding a system user



Note	• The user name can only consist of digits or letters and should be 5 to 14 characters long. The password can contain 6 to 20 characters. • Type the same password for **Password** and **Confirm Password**.

Editing a User

Click in the system user table to edit the information about a system user.

Note	You cannot delete the super user or edit its privileges.

Deleting a User

Click in the system user table to delete a system user.

Enabling a CLI User

CLI users can be enabled or disabled only by the administrator.

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 to the password page, as shown in Figure 7-7.

The password must be 6 to 20 characters long. The CLI user name is defined by the system and cannot be edited. After the password is configured, you do not need to change it during next enabling.

Figure 7-8 Configuring the password of a CLI user

Item	Value
Username	routerman
New Password	
Confirm Password	

Editing a CLI User

Click in the CLI user table to change the password of a CLI user.

Figure 7-9 Editing CLI user

User Management

Modify CLI User

Item	Value
Username	routerman
New Password	
Confirm Password	

OK Cancel

Note

- The CLI user name is defined by the system and cannot be edited.
- The password of a CLI user is 6 to 20 characters long.

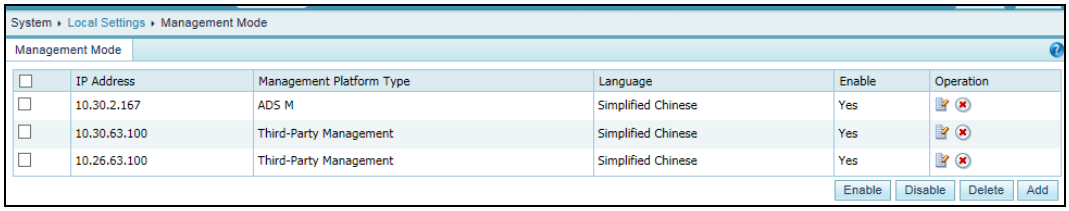
7.1.4 Management Mode Configuration

Currently, the administrator can exercise centralized management and monitoring over ADS in two ways: third-party interface management and ADS M management. ADS M management and third-party management cannot be used concurrently.

- Third-party interface management: The administrator employs third-party programs to manage ADS devices.
- Cloud platform management: The ADS daemon uploads files to ESPC or ESPP.
- ADS M management: The ADS daemon uploads files to ADS M, and ADS M dispatches configuration to ADS devices. ADS M conducts centralized management and maintenance for ADS devices.

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

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



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

Figure 7-10 Add Mgmt Mode Config page

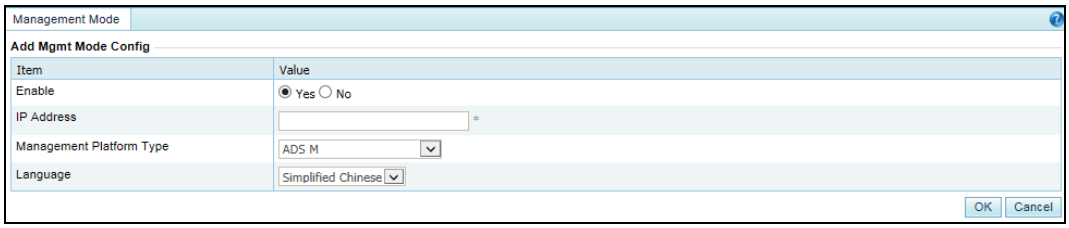


Table 7-3 describes management mode parameters.

Table 7-3 Management mode parameters

Parameter	Description
Accept Management	Controls whether ADS accepts centralized management. • **Yes**: indicates that ADS is subject to centralized management. • **No**: indicates that ADS is not subject to centralized management.
IP Address	IP address of ESPC, ESPP, ADS M, or the third-party device to which ADS submits data. You can type either an IPv4 or IPv6 address. **Note** Currently, ADS can submit data to five servers simultaneously.

Parameter	Description
Management Platform Type	Type of the device to which ADS submits data. The value can be one of the following: • **ADS M**: ADS M. • **ESPC/ESPP**: ESPC or ESPP. • **Third-Party Management**: third-party device.
Key	Specifies the key used for configuring the web API. This parameter is available only when **Management Platform Type** is set to **Third-Party Management**. The key must be a combination of 6 to 15 upper-case letters, lower-case letters, and digits.
Language	Specifies the language of messages sent by ADS to ADS M. Generally, after you configure protection policies on ADS M for ADS, ADS returns related messages.

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

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

----End

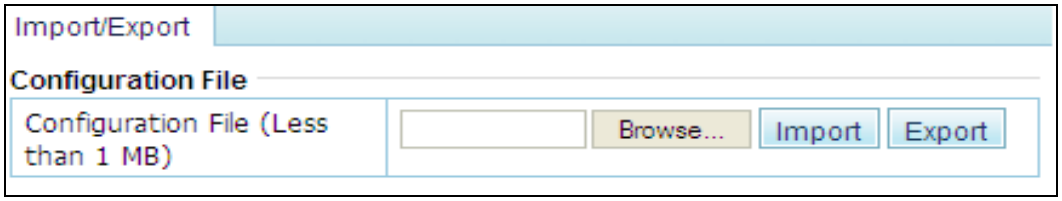
7.1.5 Configuration File Import and Export

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

Exporting a Configuration File

On the **Import/Export** page shown in Figure 7-11, click **Export** to export a configuration file with the default filename **collapsar.conf**.

Figure 7-11 Import/Export page



Note	• You are advised not to change the name of the imported configuration file, **collapsar.conf**. • Configuration files of one ADS model are specific to ADS devices of this model, for example, configuration files of ADS NX5-4020&2020&2010 devices are inconsistent with ADS NX5-4000 or ADS M.

Importing a Configuration File

On the page shown in Figure 7-11, click **Brow** and select a configuration file from the local host. Then click **Import** to import the configuration information and restore the system back to the state right before the configuration file was exported.

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

- The size of the configuration file should be no greater than 1 MB; otherwise, the import fails.
- Configuration files cannot be imported across different product models.
- Configuration files cannot be imported across the same product models running in different modes.

7.1.6 HA Configuration

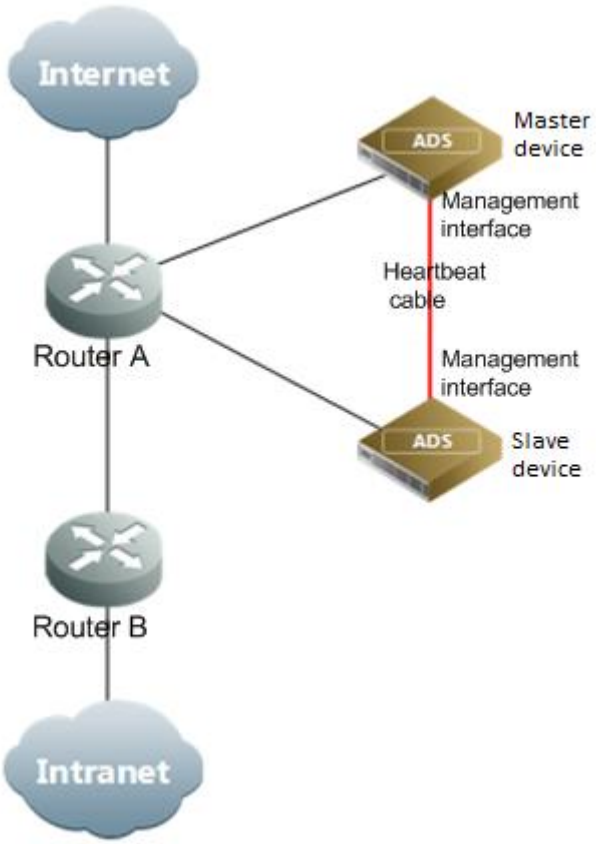
Currently, ADS supports two dual-system hot standby modes: Active-Active and Active-Standby.

In Active-Active mode, an ADS device functions as the master device, and another ADS device functions as the slave device. Both the master and slave devices handle services and achieve load balancing. If the master device fails, the slave takes over all services and traffic, ensuring that services are provided properly.

In Active-Standby mode, an ADS device functions as the master device, and another ADS device functions as the slave device. By default, the master device handles all traffic and synchronizes heartbeat information and real-time status to the slave device that is only a backup device and does not handle services. If the master device fails, the slave device will take over all the services and traffic handled by the master device, ensuring that services are provided properly.

Currently, ADS supports the dual-system hot standby function only in out-of-path mode. As shown in Figure 7-12, the master and slave devices are connected by heartbeat interfaces (management interfaces on devices) to synchronize heartbeat information and real-time status and establish the BGP neighbor relationship with the peer router.

Figure 7-12 HA topology



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

Before dual-server hot standby deployment, the administrator needs to perform the following interface configuration on active and standby devices (see section 9.2.1 Configuring IPv4 Network Settings for details):

- Configure the heartbeat interface (management interface).

  The heartbeat interface is used by the master device to synchronize specified configuration files to the slave device. For details, see section 7.1.6.2 HA File Synchronization Configuration. The heartbeat interfaces on the master and slave devices must be reachable for each other.
- Configure other communication interfaces.

After the interface configuration, enable the dual-server hot standby function and configure HA parameters, including:

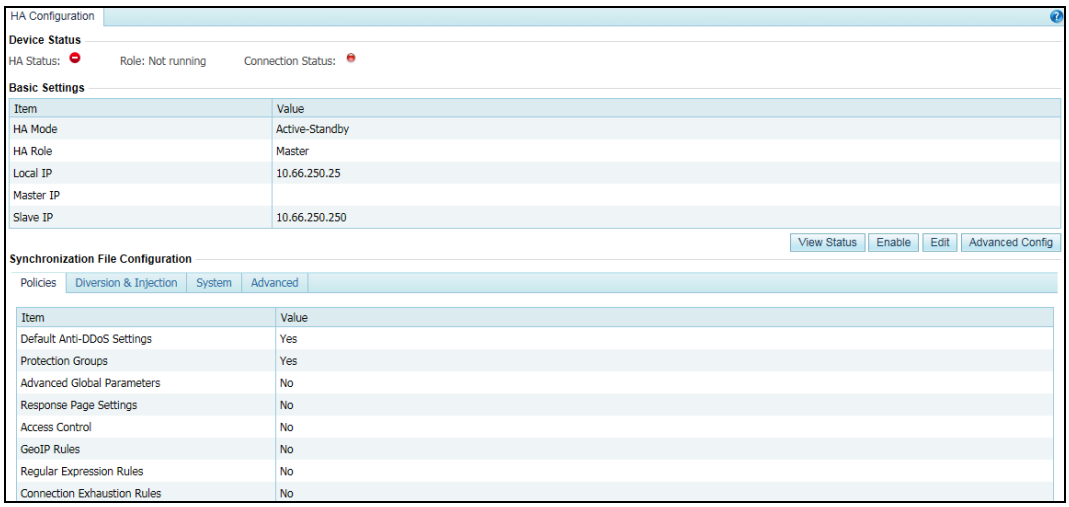
- Basic settings
- Synchronization file configuration

7.1.6.1 Basic HA Settings

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

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

Figure 7-13 HA Configuration page



Step 5 Click **Edit** in the lower-right corner of the **Basic Settings** area to open the editing page.

Figure 7-14 Edit Basic Settings area

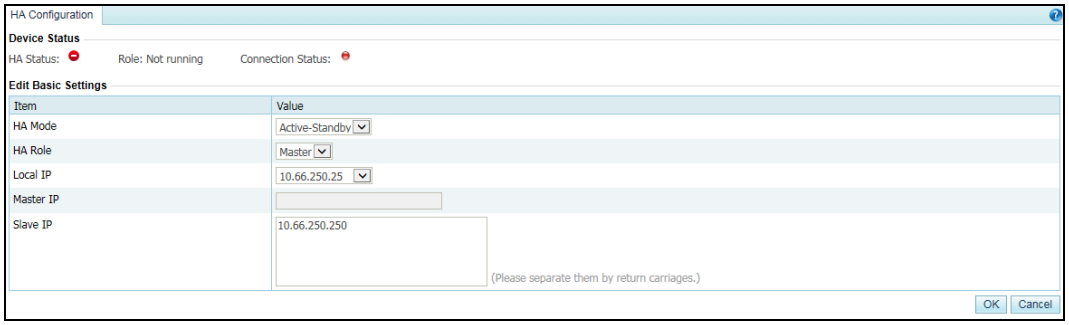


Table 7-4 describes parameters of basic HA settings.

Table 7-4 Parameters of basic HA settings

Parameter	Description
HA Mode	HA mode, which can be **Active-Active** or **Active-Standby**.
HA Role	Role played by the current device in dual-server hot standby mode. In Active-Standby mode:

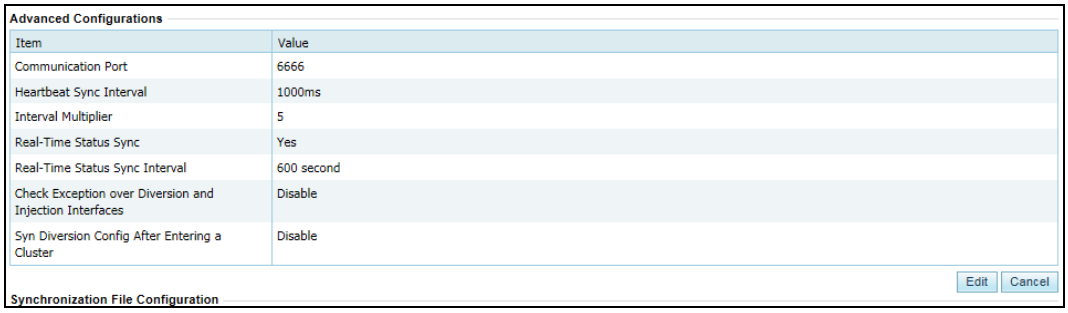
Parameter	Description
	• **Master**: indicates that this device works as a master device. After HA is enabled, it starts handling user services until a failure occurs. • **Slave**: indicates that this device acts as a slave device. After HA is enabled, this device is in backup state and starts handling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

Step 6 Set parameters and click **OK** to save the setting.

Step 7 (Optional) Set advanced HA configurations.

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

Figure 7-15 Advanced Configurations area



b. Click **Edit**.

Figure 7-16 Edit Advanced Configurations area

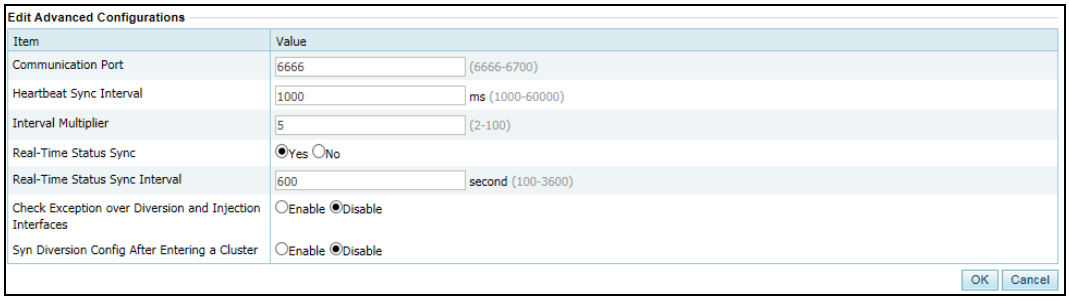


Table 7-5 describes the parameters of advanced HA configurations.

Table 7-5 Parameters of advanced HA configurations

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

Step 8 Click **OK** to save the settings.

----End

7.1.6.2 HA File Synchronization Configuration

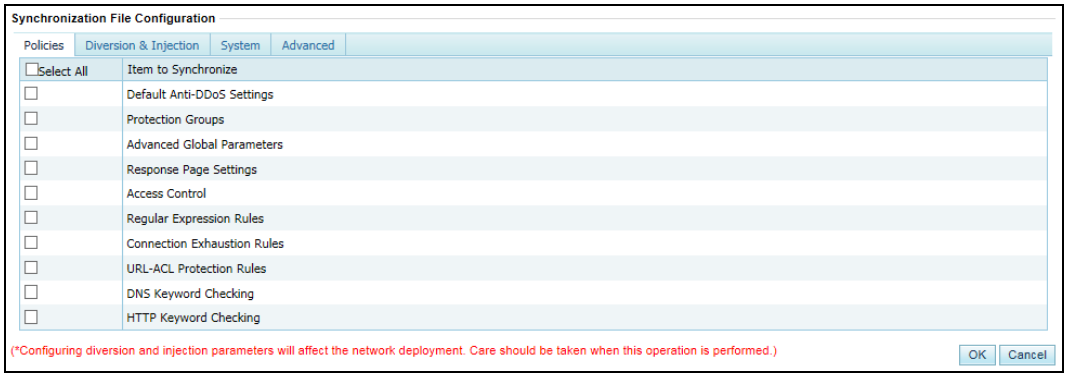
After configure basic HA settings, on both the master and slave devices, you need to specify configuration files to be synchronized, including configurations about policies, diversion and injection, system, and advanced applications.

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

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

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

Figure 7-17 Policy configurations to be synchronized



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

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

The area for selecting diversion and injection configurations to be synchronized appears, as shown in Figure 7-18.

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

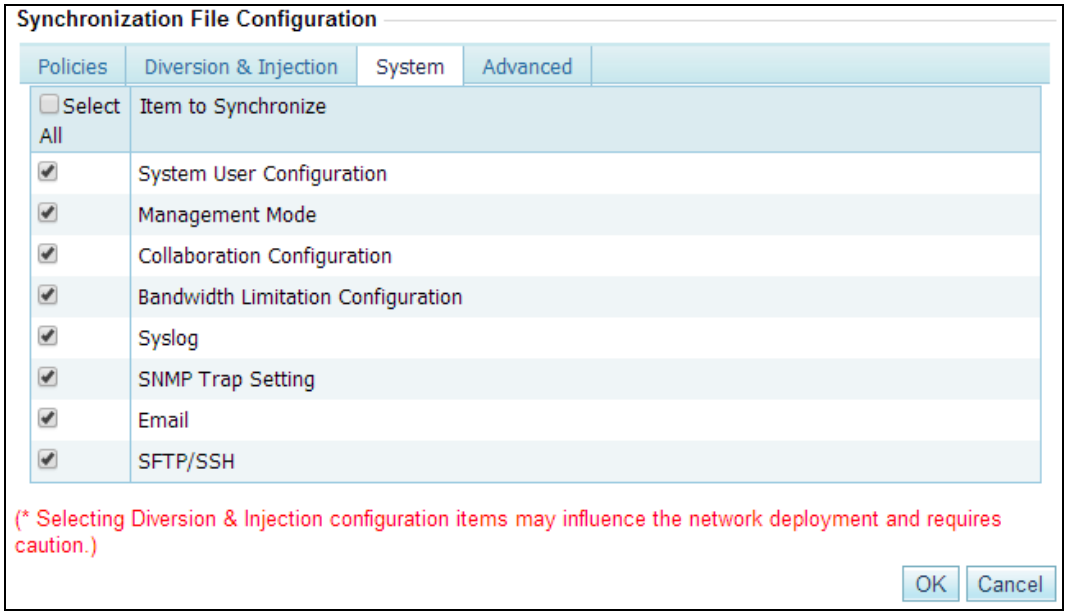
Figure 7-18 Diversion and injection configurations to be synchronized

Step 5 Select desired configurations and click **OK**.

Step 6 Click the **System** tab.

The area for selecting system configurations to be synchronized appears, as shown in Figure 7-19.

Figure 7-19 System configurations to be synchronized

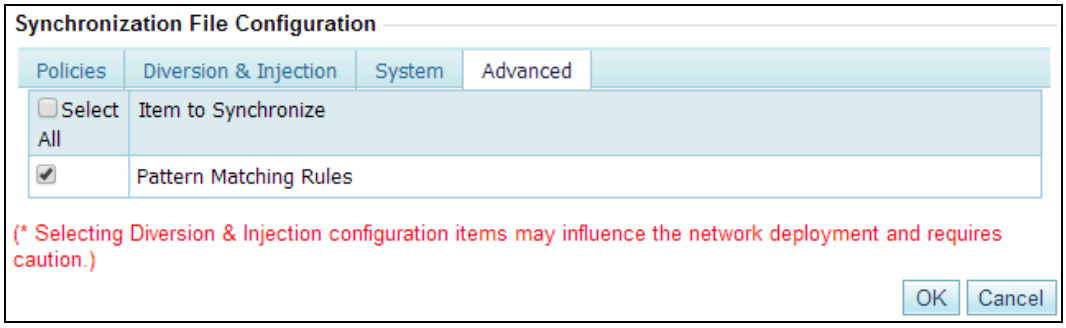


Step 7 Select desired configurations and click **OK**.

Step 8 Click the **Advanced** tab.

The area for selecting advanced configurations to be synchronized appears, as shown in Figure 7-20.

Figure 7-20 Advanced configurations to be synchronized



Step 9 Select the configuration and click **OK**.

----End

7.1.6.3 Enabling HA

After finishing basic HA settings and file synchronization configuration on both the master and slave devices, you can enable HA on them, separately, by clicking **Enable** in the lower right corner of the **Basic Settings** area in the **HA Configuration** tab page shown in Figure 7-13.

After HA is enabled, the **HA Configuration** tab page on a master device is as shown in Figure 7-21, and that on a slave device is as shown in Figure 7-22.

Figure 7-21 HA Configuration tab page on a master device

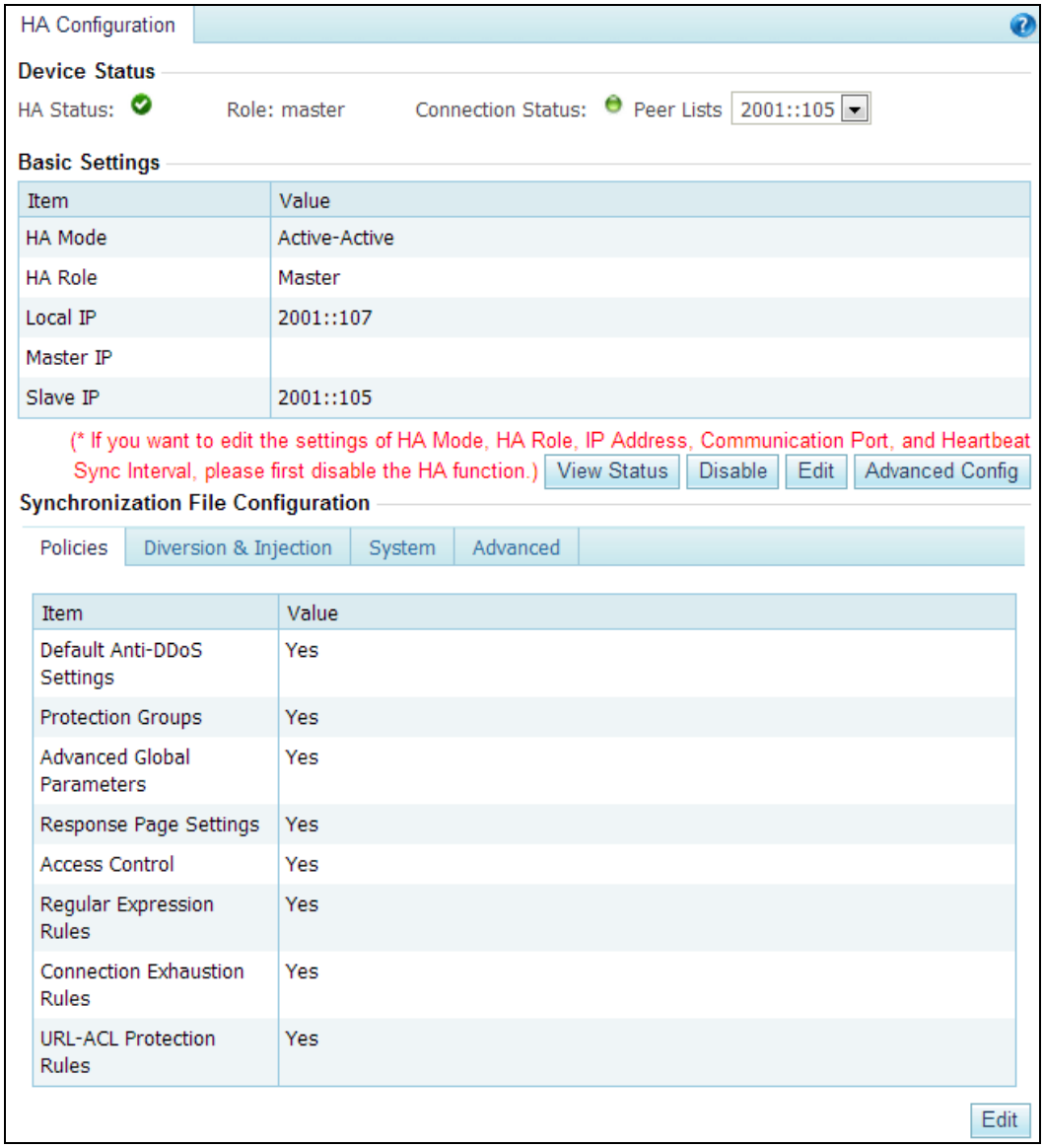
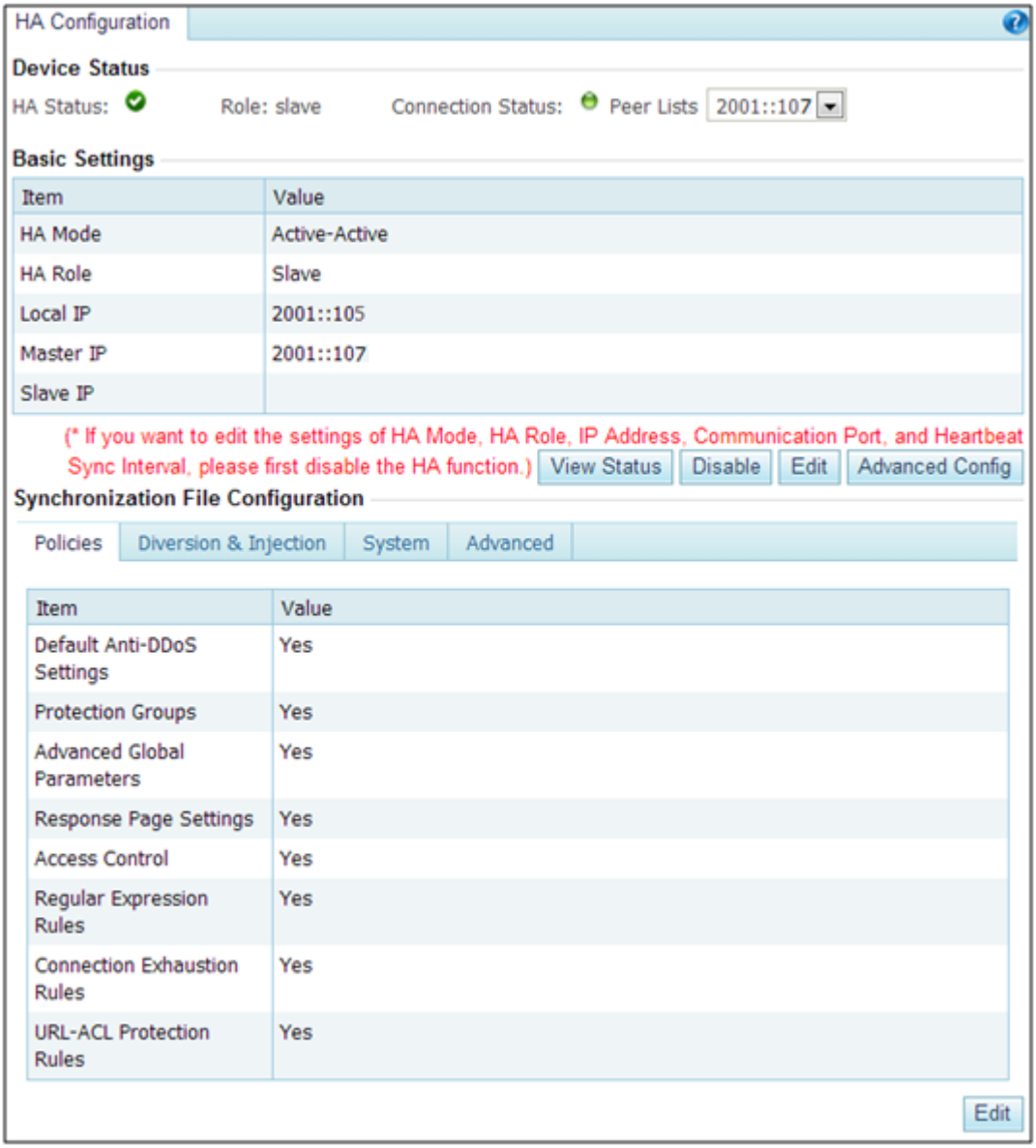


Figure 7-22 HA Configuration tab page on a slave device



7.1.6.4 Disabling HA

After HA is enabled, in the lower-right corner of the **Basic Settings** area in the **HA Configuration** tab page shown in Figure 7-13, the **Enable** button changes to a **Disable** button. You can click **Disable** to disable HA.

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

7.1.6.5 Viewing HA Status

After HA is enabled, the work status, role, connection status, and peer list of HA are displayed in the **Device Status** area shown in Figure 7-13.

To view detailed status of the HA configurations, you can click the **View Status** in the lower right corner of the **Basic Settings** area shown in Figure 7-13.

Figure 7-23 shows the status viewing result on a master device in Active-Active mode, and Figure 7-24 shows that on a slave device in Active-Active mode.

Figure 7-23 Status viewing result on a master device

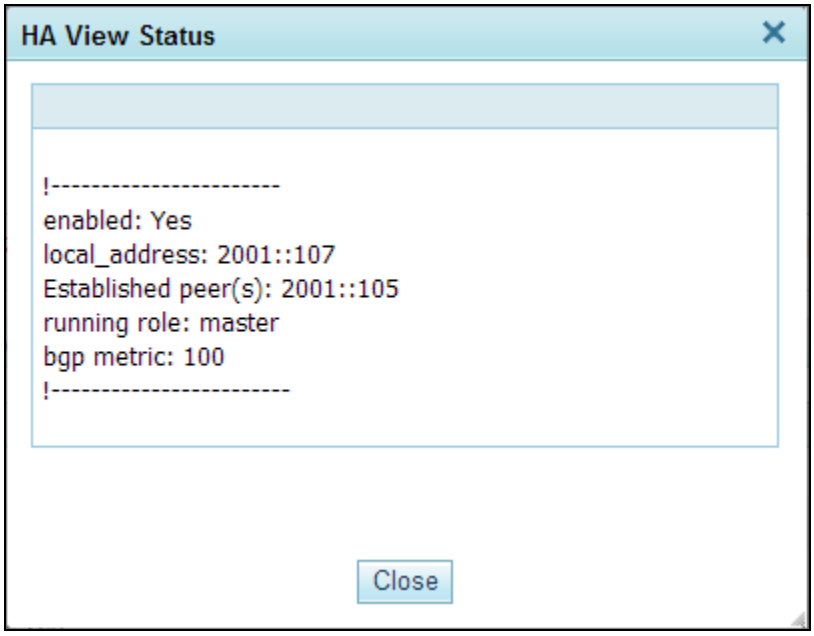
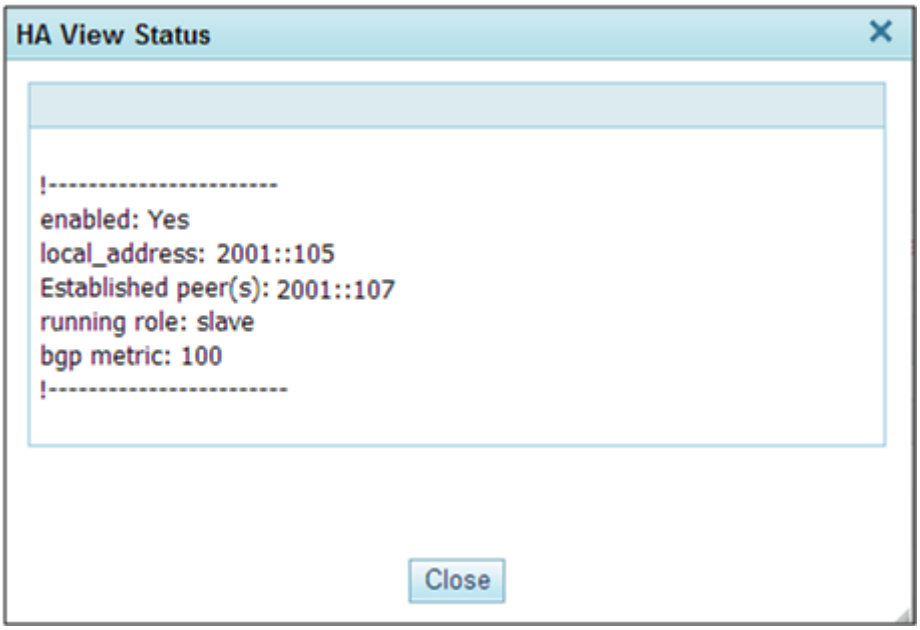


Figure 7-24 Status viewing result on a slave device

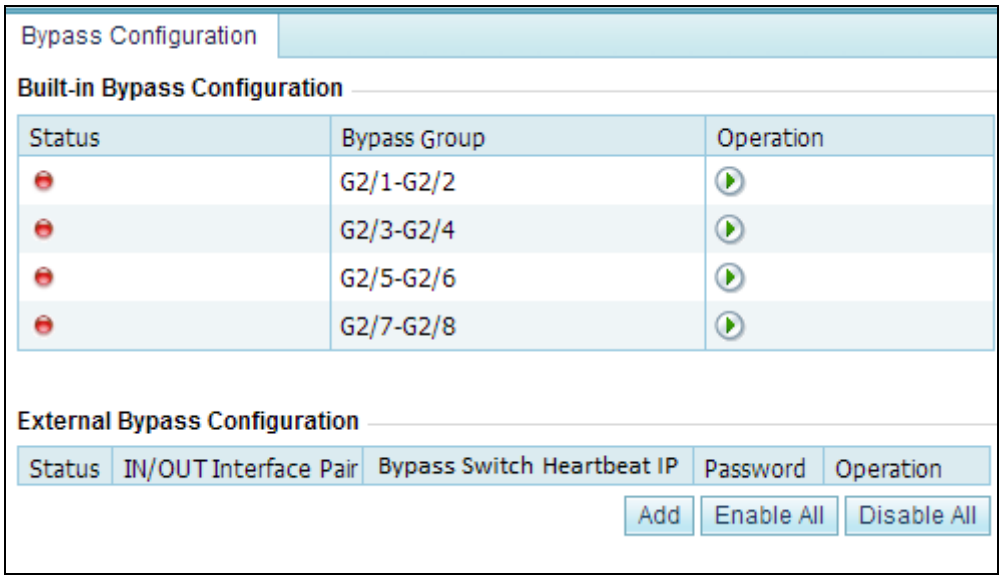


7.1.7 (Optional) Bypass Configuration

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

This function ensures smooth network communications when ADS fails. ADS devices provide the built-in bypass function. To configure this function, choose **System** > **Local Settings** > **Bypass Configuration**.

Figure 7-25 Bypass Configuration page



7.1.7.1 Built-in Bypass

The built-in bypass function is disabled by default, as shown in Figure 7-25.

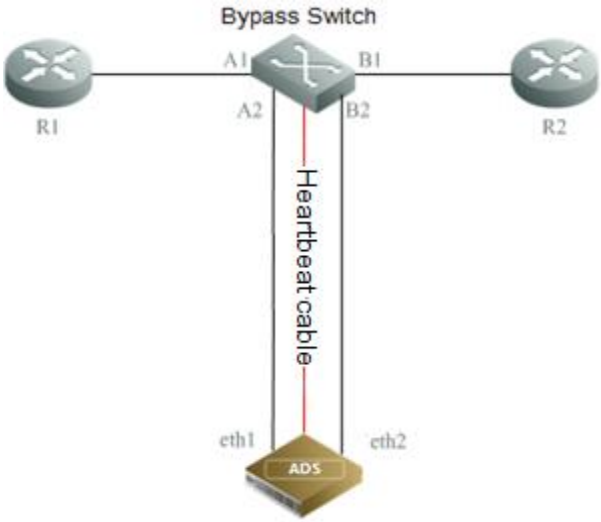
- To enable this function, click in the **Operation** column. Then the indicator in the **Status** column turns to , indicating the built-in bypass function is enabled. At the same time, the button in the **Operation** column turns to .
- To disable this function, click in the **Operation** column. Then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

7.1.7.2 External Bypass

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

Figure 7-26 shows the topology for the interaction between ADS and the bypass switch.

Figure 7-26 Topology for the interaction between ADS and the bypass switch



When any of the following occurs:

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

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

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

	the management interface on ADS and the heartbeat interface on the NSF-BS.

On the **External Bypass** area shown in Figure 7-25, 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 7-27.

Figure 7-27 Adding an external bypass group

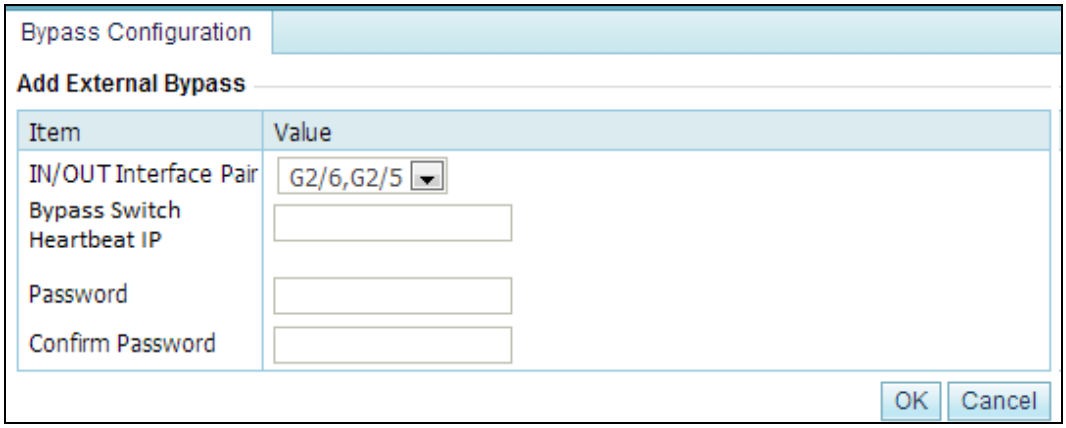


Table 7-6 describes parameters of the external bypass group.

Table 7-6 Parameters of the external bypass group

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

Editing an External Bypass Group

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

Deleting an External Bypass Group

Click in the **Operation** column of the external bypass table and then click **OK** to delete an external bypass 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 the bypass group is enabled.
- To enable all external groups, click **Enable All** 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 the bypass group is disabled.
- To disable all bypass groups, click **Disable All** and click **OK** in the displayed dialog box.

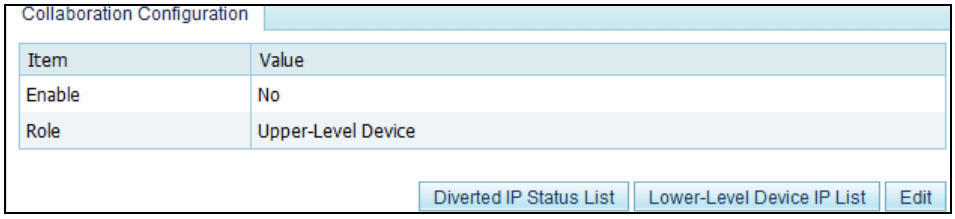
7.1.8 Collaboration Configuration

Note	This collaboration module supports only IPv4 addresses.

ADS devices can work in hierarchical mode to provide complete security protection: Once detecting that the 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 to the lower-level ADS.

Choose **System** > **Local Settings** > **Collaboration Configuration**. The **Collaboration Configuration** page appears, as shown in Figure 7-28.

Figure 7-28 Collaboration Configuration page



7.1.8.1 Managing Upper-Level ADS Devices

Configuring an Upper-Level ADS

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

Step 1 On the **Collaboration Configuration** page shown in Figure 7-28, click **Edit** and set **Enable** to **Yes** and **Role** to **Upper-Level Device**, as shown in Figure 7-29.

Note	For an upper-level device, **Accept Management** must be set to **Yes** in **Management Mode** under **System > Local Settings**.

Figure 7-29 Configuring an upper-level ADS

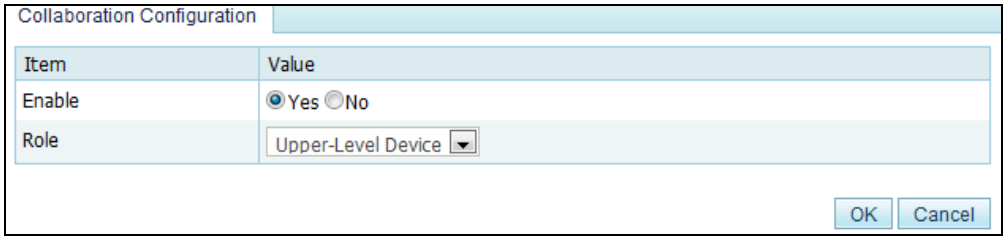


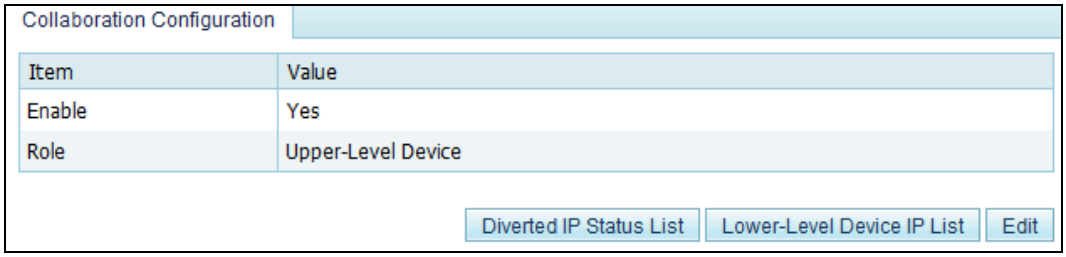
Table 7-7 describes parameters for configuring an upper-level ADS.

Table 7-7 Parameters for configuring an upper-level ADS

Parameter	Description
Enable	Controls whether to enable the collaboration between lower-level and upper-level ADS devices. • **Yes**: indicates that the collaboration function is enabled. • **No**: indicates that the collaboration function is disabled. If **Yes** is selected, you need to set **Accept Management** to **Yes** on the **Management Mode** page (**System** > **Local Settings**). For details, see section 7.1.4 Management Mode Configuration.
Role	Role played by the device. **Upper-Level Device** indicates that the device is an upper-level one. **Lower-Level Device** indicates that the device is a lower-level one.

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

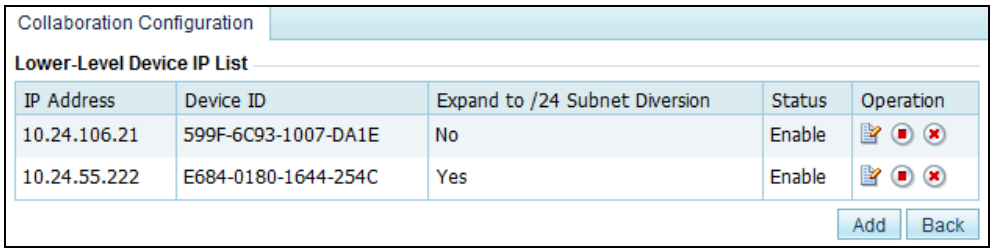
Figure 1-1 Collaboration Configuration page



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

IP addresses of lower-level ADS devices are displayed. See Figure 7-30.

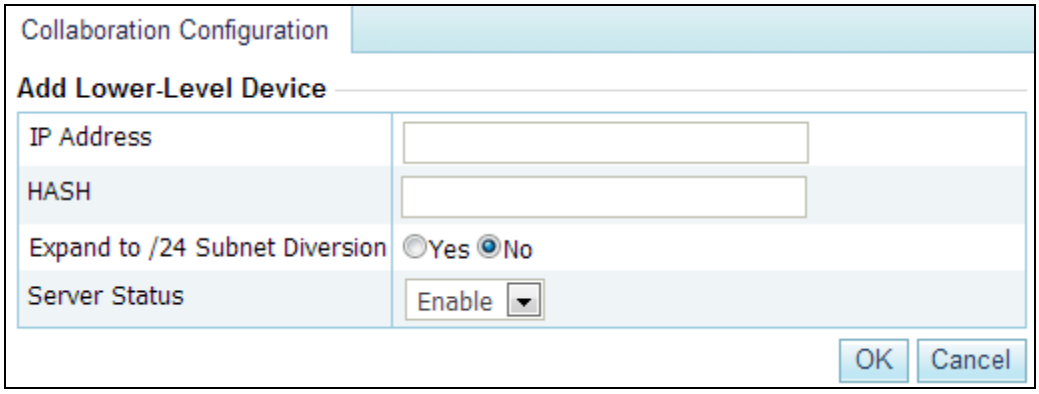
Figure 7-30 List of IP addresses of lower-level devices



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

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

Figure 7-31 Adding a lower-level ADS



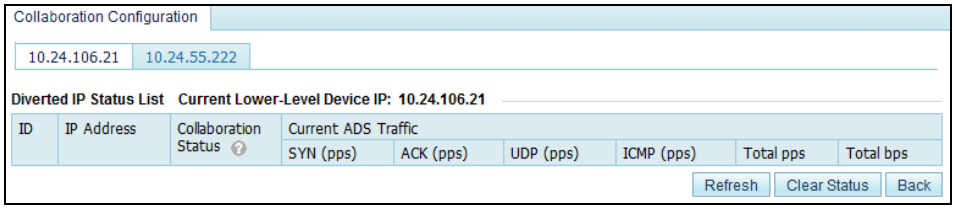
Step 5 Click **OK** to complete the configuration.

----End

Viewing Diverted IP Status List

On the **Collaboration Configuration** page shown in Figure 7-28, click **Diverted IP Status List** to view the IP addresses for which the diverted traffic is destined as well as the traffic information of the current ADS.

Figure 7-32 Viewing diverted traffic



7.1.8.2 Managing Lower-Level ADS Devices

Configuring a Lower-Level ADS

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

Step 1 On the **Collaboration Configuration** page shown in Figure 7-28, click **Edit** and set **Enable** to **Yes** and **Role** to **Lower-Level Device**, as shown in Figure 7-33.

Figure 7-33 Configuring a lower-level ADS

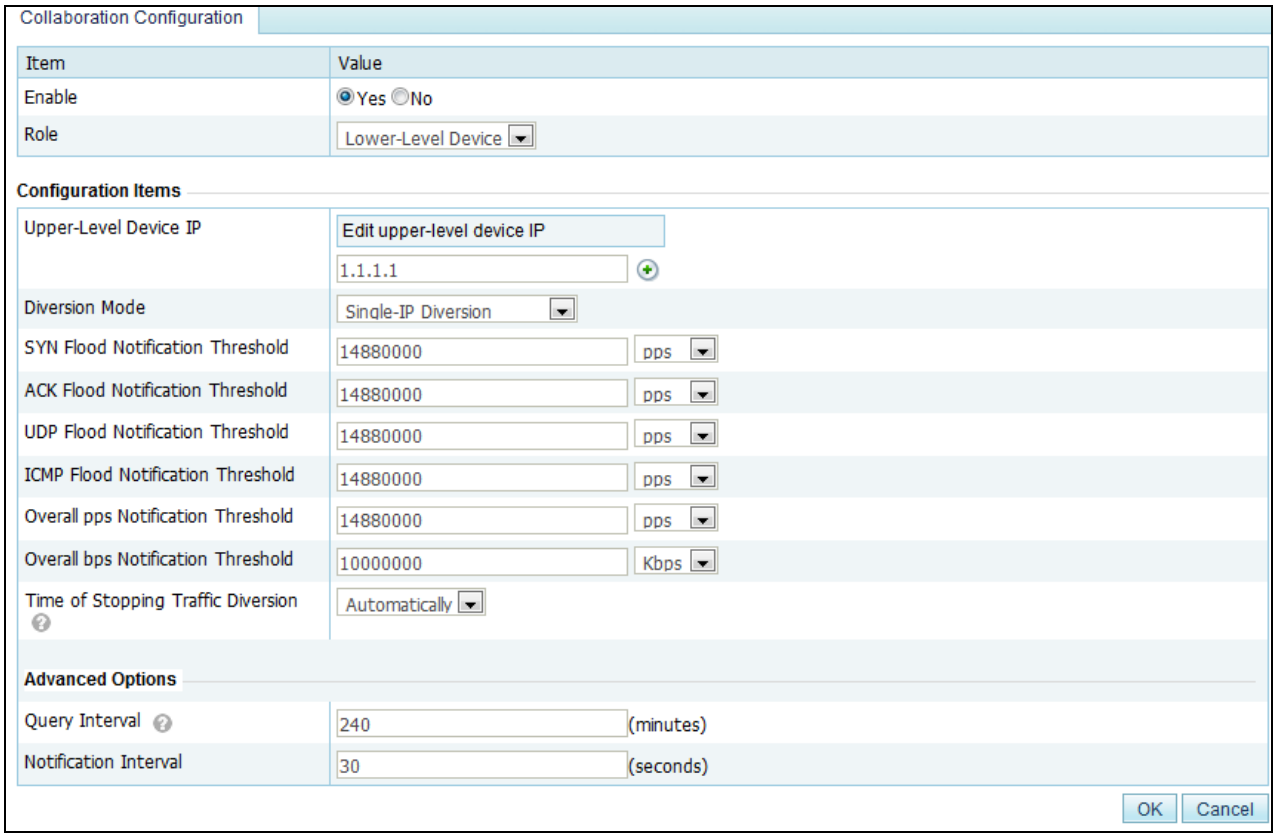


Table 7-8 describes parameters for configuring a lower-level ADS.

Table 7-8 Parameters for configuring a lower-level ADS

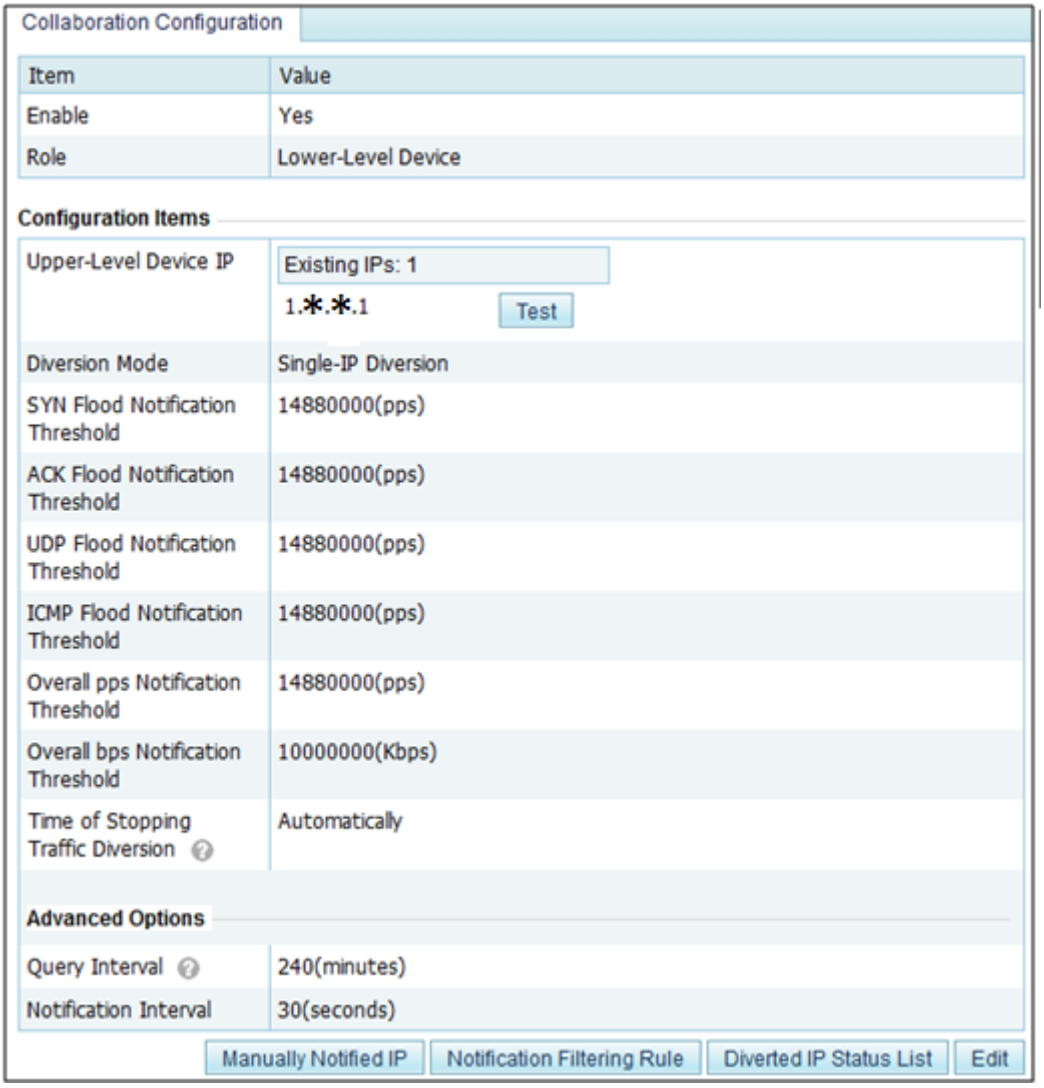
Parameter	Description
Enable	Controls whether to enable the collaboration between lower-level and upper-level ADS devices. • **Yes**: indicates that the collaboration is enabled. • **No**: indicates that the collaboration is disabled. Note The lower-level device notifies the upper-level ADS of traffic diversion if the traffic exceeds a notification threshold.
Role	Role played by the device. • **Superior Server**: indicates that the device is an upper-level one. • **Subordinate**: indicates that the device is a lower-level one.
Upper-Level Device IP	IP address of the management interface of the upper-level ADS.
Diversion Mode	Mode of traffic diversion between upper-level and lower-level devices. • **Single-IP Diversion**: indicates that traffic diversion is triggered when traffic destined for a single IP address exceeds a threshold. • **Device Overall Threshold**: indicates that traffic diversion is triggered if the overall traffic of the lower-level device exceeds a threshold.
SYN Flood Notification Threshold	Threshold for SYN flood traffic. When the traffic rate of SYN packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic. Note When flood protection is enabled on the lower-level ADS, this threshold must be greater than that specified in the SYN flood protection policy.
ACK Flood Notification Threshold	Threshold for ACK flood traffic. When the traffic rate of ACK packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic. Note When flood protection is enabled on the lower-level ADS, this threshold must be greater than that specified in the ACK flood protection policy.
UDP Flood Notification Threshold	Threshold for UDP flood traffic. When the traffic rate of UDP packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic. Note When flood protection is enabled on the lower-level ADS, this threshold must be greater than that specified in the UDP flood protection policy.
ICMP Flood Notification Threshold	Threshold for ICMP flood traffic. When the traffic rate of ICMP packets reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.

Parameter	Description
	Note When flood protection is enabled on the lower-level ADS, this threshold must be greater than that specified in the ICMP flood protection policy.
Traffic Rate (pps) Notification Threshold	Threshold for traffic in pps. When the traffic rate reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
Traffic Rate (bps) Notification Threshold	Threshold for traffic in bps. When the traffic rate reaches the threshold, the lower-level ADS instructs the upper-level ADS to divert the traffic.
Time of Stopping Traffic Diversion	• **Automatically decided**: The lower-level ADS automatically determines whether to send notifications to the upper-level ADS on stopping traffic diversion. • **Manually configured**: The lower-level ADS sends notifications to the upper-level ADS on stopping traffic diversion on manually configured time. You also need to specify how many minutes later traffic diversion will be stopped. When the scheduled time arrives, the lower-level ADS sends notifications to the upper-level ADS on stopping traffic diversion. After that, if the traffic reaching the lower-level ADS reaches one of the preceding threshold, the lower-level ADS sends notification to the upper-level ADS on starting traffic diversion. Note When ADS diverts traffic, the lower-level ADS suspends flood protection for the diverted IP address. After the upper-level ADS's traffic diversion stops, the lower-level ADS resumes flood protection for this IP address.
Query Interval	Interval between which the lower-level device queries the upper-level device about the current traffic destined for an IP address, after the traffic destined for the IP address is diverted. The interval should be larger than 5 minutes; otherwise, route flapping may occur.
Notification Interval	Interval that 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 7-34.

Figure 7-34 Lower-level ADS configuration



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

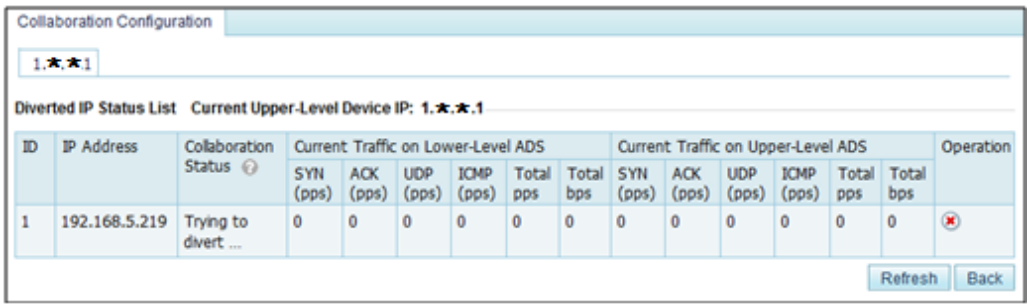
If the icon appears to the left of the **Test** button, the connection succeeds.

----End

Viewing Diverted IP Status List

On the **Collaboration Configuration** page shown in Figure 7-34, click **Diverted IP Status List** to view the current traffic on the upper-level and lower-level ADS devices. See Figure 7-35.

Figure 7-35 Status of diverted traffic



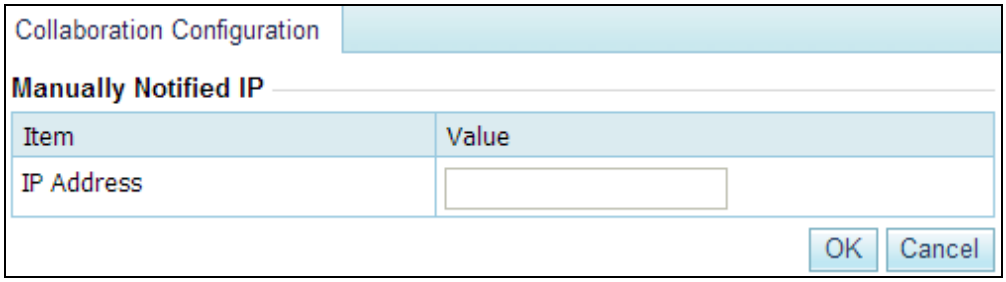
Configuring Manually Notified IPs

If you need to divert traffic from specified IP addresses to an upper-level ADS, you can specify manually notified IP addresses. All traffic destined for manually notified IP addresses will be diverted to the upper-level ADS.

To specify manually notified IP addresses, perform the following steps:

Step 1 On the **Collaboration Configuration** page shown in Figure 7-34, click **Manually Notified IP**.

Figure 7-36 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 one by one.

----End

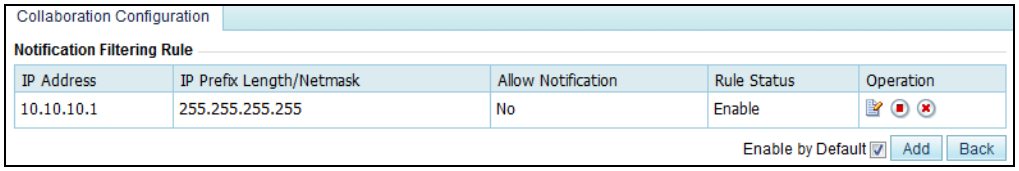
Configuring Notification Filtering Rules

The upper-level ADS can successfully divert traffic destined for manually and automatically notified IP addresses only when notification filtering rules are configured.

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

Step 1 On the **Collaboration Configuration** page shown in Figure 7-34, click **Notification Filtering Rule**.

Figure 7-37 Notification filtering rule page



Step 2 Click **Add**.

Figure 7-38 Adding a notification filtering rule

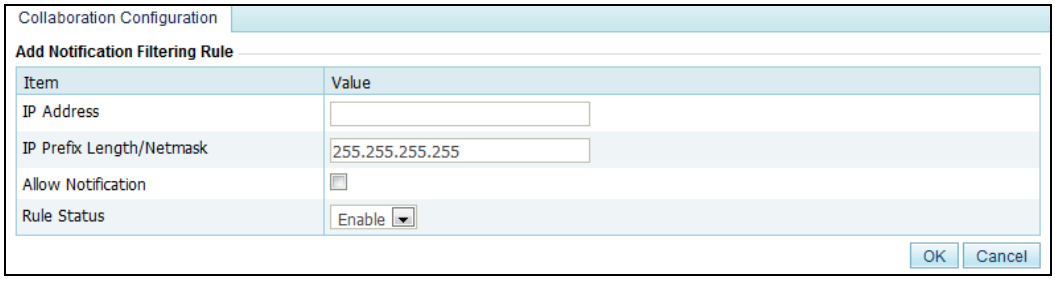


Table 7-9 describes parameters for creating a notification filtering rule.

Table 7-9 Parameters for creating a notification filtering rule

Parameter	Description
IP Address	IP addresses for which you need to manually decide whether their diversion notification can be sent to the upper-level device.
IP Prefix Length/Netmask	Prefix length or netmask of an 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 for the IP address only after **Allow Notification** is checked."
Rule Status	Controls whether to enable this rule. • **Yes**: indicates that this rule is enabled. This rule takes effect only when it is enabled. • **No**: indicates that this rule is disabled.

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

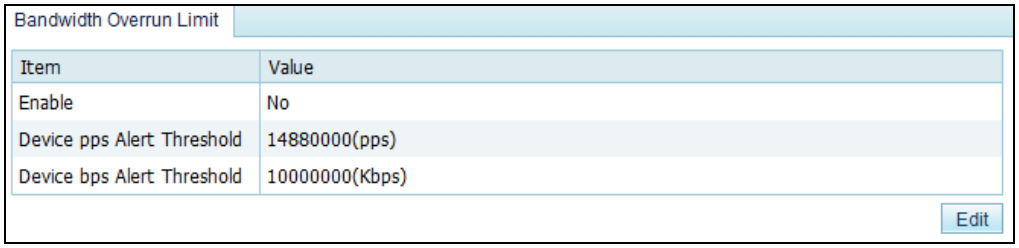
----End

7.1.9 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 in red, prompting bandwidth overrun. Also, the system generates system operation logs to record when the alert is reported and fixed.

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

Figure 7-39 Bandwidth Overrun Limit page



Step 2 Click **Edit**.

Figure 7-40 Editing bandwidth overrun thresholds

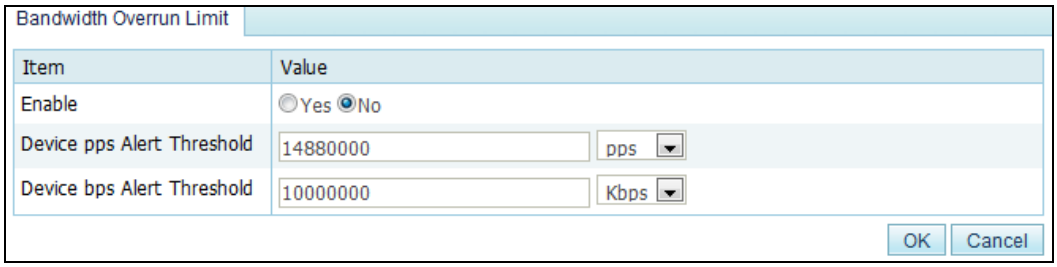


Table 7-10 describes bandwidth overrun threshold parameters.

Table 7-10 Bandwidth overflow threshold parameters

Parameter	Description
Enable	Controls whether to enable the bandwidth overrun alerting. • **Yes**: indicates that an alert is reported. • **No**: indicates that no alert is reported.
Device pps Alert Threshold	Alert triggering threshold for device overall traffic in pps. A bandwidth overrun alert is generated if this threshold is exceeded.
Device bps Alert Threshold	Alert triggering threshold for device overall traffic in bps. A bandwidth overrun alert is generated if this threshold is exceeded.

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

----End

7.2 Security Configuration

This section covers the following topics:

- Login Security Settings
- Locked User Management

- Authentication Configuration

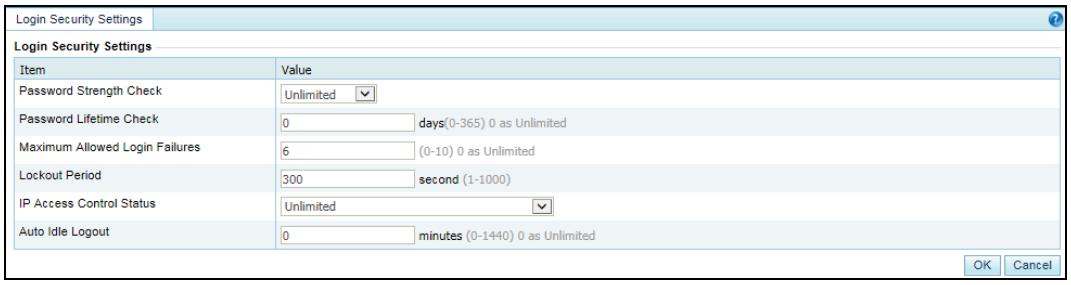
7.2.1 Login Security Settings

This section describes how to configure login security parameters.

The procedure is as follows:

Step 4 Choose **System** > **Security Configuration** > **Login Security Settings**, and then click **Modify**.

Figure 7-41 Configuring login security parameters



Step 5 On the page that appears, configure login security parameters.

Table 7-11 describes parameters on this page.

Table 7-11 Login security parameters

Parameter	Description
Password Strength Check	Specifies the type of characters to be automatically checked for password strength when you configure or change the password. Only a password conforming to the requirement can be successfully specified. • **Unlimited**: indicates no password strength check will be performed. • **Must include**: indicates the type of characters (digits, special characters, uppercase letters, and lowercase letters) to be checked. You can select one or more types.
Password Lifetime Check	Specifies the lifetime of the password that is successfully configured. A password whose lifetime has expired cannot be used. The value ranges from 0 to 365 days. The value **0** indicates that this function is disabled.
Maximum Allowed Login Failures	Specifies the maximum number of consecutive failed login attempts in the allowed login interval. The value ranges from 0 to 10. The value **0** indicates that this function is disabled, that is, the number of failed login attempts is not limited.
Lockout Period	Specifies how long a user will be locked after **Maximum Allowed Login Failures** is exceeded. During the lockout period, the user is prevented from logging in to the system. The value ranges from 1 to 1000 seconds. You are advised to set it to a value no smaller than 180 seconds.
IP Access Control Status	Controls whether to control access from certain IP addresses.

Parameter	Description
	• **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.
Auto Idle Logout	Specifies the time, in minutes, that a user is allowed to remain idle. When this period expires, a user is logged out and has to log in again before continuing using this system. The value ranges from 0 to 1440. You are advised to set it to a value no greater than 10. The value **0** indicates that this function is disabled.

Step 6 Click **OK** to save the settings.

----End

7.2.2 Locked User Management

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

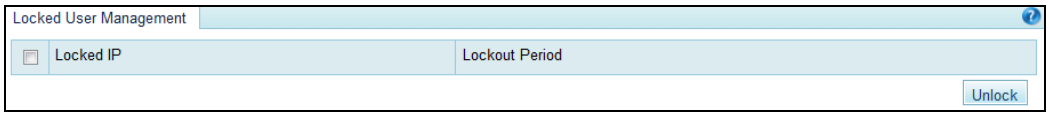
Note	Only the user **admin** can unlock user accounts.

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

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

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

Figure 7-42 Locked User Management page



----End

7.2.3 Authentication Configuration

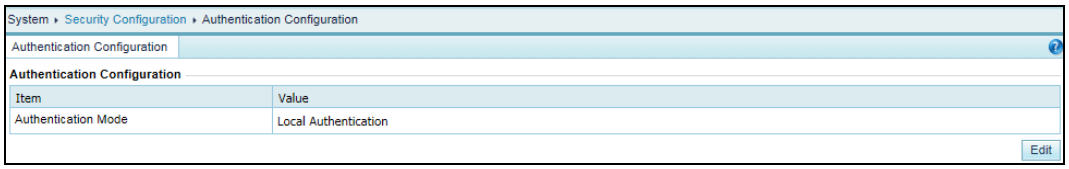
When a user logs in to the web-based manager of ADS, the following two authentication modes are supported:

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

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

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

Figure 7-43 Authentication Configuration page



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

Figure 7-44 Configuring the authentication configuration.

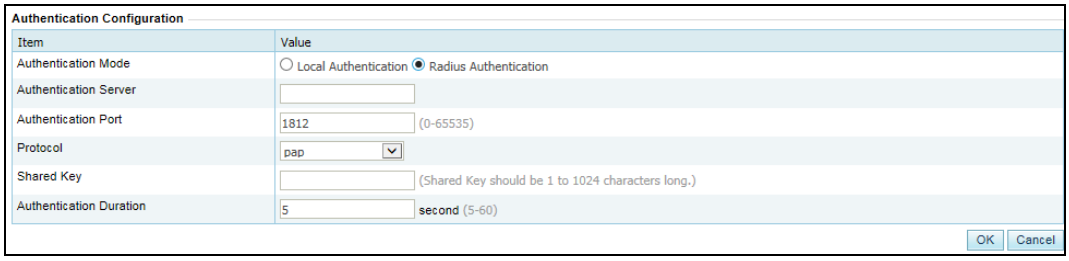


Table 7-12 Parameters for configuring the authentication mode

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

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

----End

7.3 Log Services

This section covers the following topics:

- Syslog Settings
- SNMP Settings
- Email Settings
- SFTP/SSH Settings

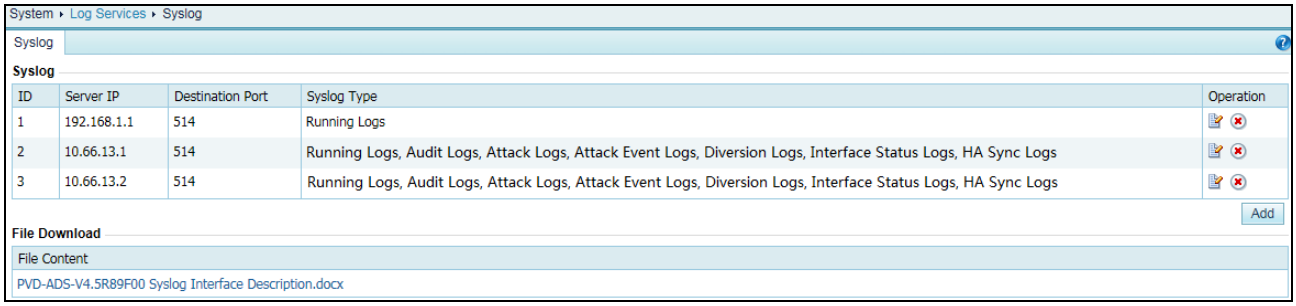
7.3.1 Syslog Settings

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 7-45, you can click the file name in the **File Download** area to download the syslog file to a local disk drive.

Figure 7-45 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, without mutual influence. Syslog servers can share a device ID and port number.

Figure 7-46 Configuring a syslog server

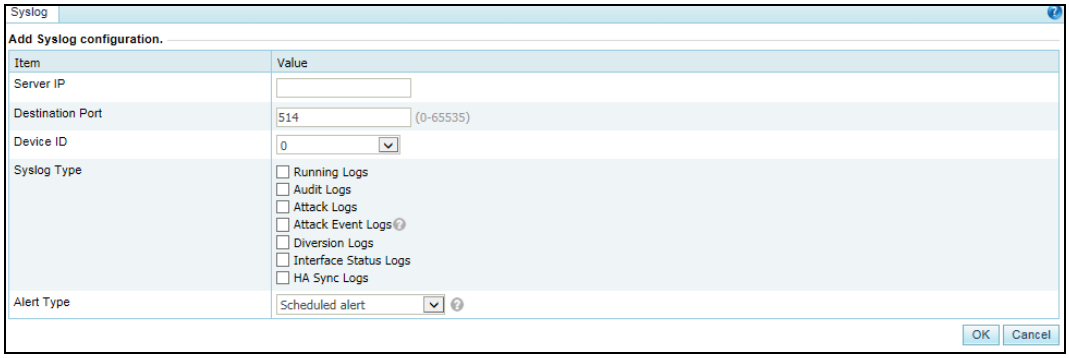


Table 7-13 Parameters for configuring a Syslog server

Parameter	Description
Server IP	Specifies the IPv4 or IPv6 address of the Syslog server.
Destination Port	Specifies the port of the Syslog server.
Device ID	Specifies the device ID that identifies the device that receives logs from the Syslog server. It is an important parameter, ranging from 0 to 7.
Syslog Type	Specifies the type of logs that are sent to the Syslog server, which can be: • **Running Logs** • **Audit Logs** • **Attack Logs** • **Attack Event Logs** • **Diversion Logs** • **Interface Status Logs** • **HA Sync Logs** By default, the system sends logs every 30 seconds.
Alert Type	Specifies the type of alerts, which can be either of the following: • **Scheduled alert**: indicates common alerts. • **Threshold exceeding alert**: indicates the alerts for exceeding the threshold. This parameter is valid only for running logs.
CPU Threshold	Specifies the threshold of the ADS's CPU usage. This parameter is required only when **Alert Type** is set to **Threshold exceeding alert.**
Memory Threshold	Specifies the threshold of the ADS's memory usage. This parameter is required only when **Alert Type** is set to **Threshold exceeding alert.**

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

----End

7.3.2 SNMP Settings

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 arbitrary network node.

SNMP adopts the polling mechanism with basic functions, which is applicable for small, rapid, and low-price environment. The SNMP implementation is based on the UDP protocol, which facilitates it to smoothly connect to many products.

SNMP configuration on ADS includes:

- SNMP agent: collects information that can be reported to NMS on ADS. SNMP V2C and SNMP V3 are supported.
- SNMP trap: collects trap messages on ADS, namely SNMP server-related information.

After SNMP is configured, ADS will send SNMP trap messages to SNMP NMS.

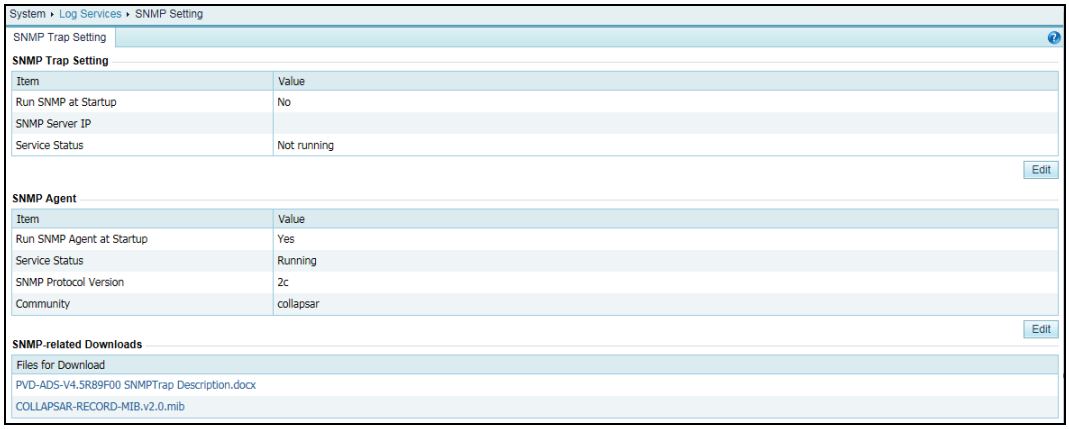
To configure SNMP, perform the following steps:

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

The **SNMP Trap Setting** page appears, as shown in Figure 7-47.

Before configuration, you can download the related SNMP description and MIB files. In Figure 7-47, you can click a file name in the **SNMP-related Downloads** area to download the file to a local disk drive.

Figure 7-47 SNMP Trap Setting page



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

Table 7-14 describes SNMP Trap parameters.

Table 7-14 SNMP Trap parameters

Parameter	Description
Run SNMP at Startup	Controls whether the SNMP Trap service runs when ADS is started. • **Yes**: indicates that the SNMP Trap service runs when ADS is started.

Parameter	Description
	• **No**: indicates that the SNMP Trap service does not run when ADS is started.
SNMP Server IP	IPv4 or IPv6 address of the SNMP server.
Service Status	Running status of the SNMP server
Run SNMP at Startup	Controls whether the SNMP agent runs when ADS is started. • **Yes**: indicates that the SNMP agent runs when ADS is started. • **No**: indicates that the SNMP agent does not run when ADS is started.
Service Status	Running status of the SNMP agent server
SNMP Protocol Version	SNMP protocol supported by the SNMP agent, such as SNMPv2c or SNMPv3
Community	Community supported by the SNMP agent. When the SNMP agent function is disabled, this parameter is unavailable.

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

----End

7.3.3 Email Settings

Email settings are required when ADS is configured to send one or multiple types of logs to a specified email address.

To configure email parameters, follow the following steps:

Step 1 Choose **System** > **Log Services** > **Email** and click **Edit** to open the email configuration page. See Figure 7-48.

Figure 7-48 Log sending by email

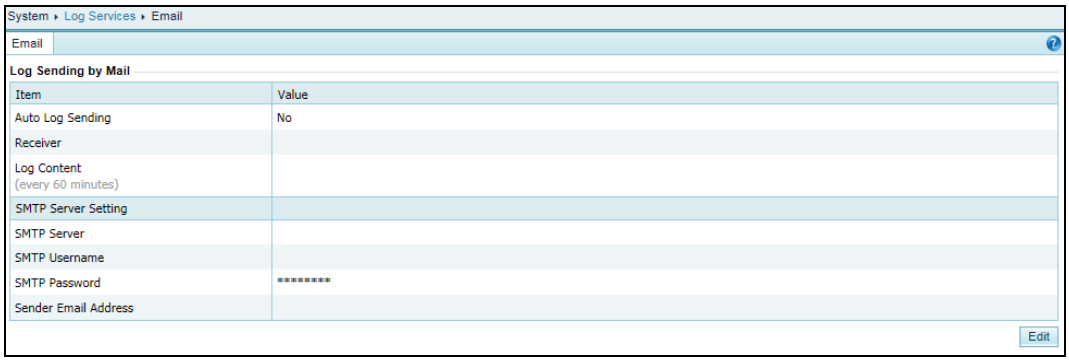


Table 7-15 describes parameters of sending logs by email.

Table 7-15 Parameters of sending logs by email

Parameter	Description
Auto Log Sending	Controls whether the system sends the selected logs to a specific email

Parameter	Description
	address. The value **Yes** indicates that the system sends the selected logs to a specific email address. If this function is enabled, you need to configure **Receiver** and **Log Content**.
Receiver	Email address that receives logs.
Log Content	Logs to be sent. The values can be **Attack Logs**, **System Logs**, **Traffic Diversion Logs**, **Link Status Logs**, and **HA log**. By default, the system sends logs every 60 minutes.
SMTP Server	IP address or domain name of the SMTP server that sends emails. You can type either an IPv4 or IPv6 address.
SMTP Username/SMTP Password	User name and password for sending emails.
Sender Email Address	Email address that sends logs.

Step 2 Set parameters and click **OK** to save the settings.

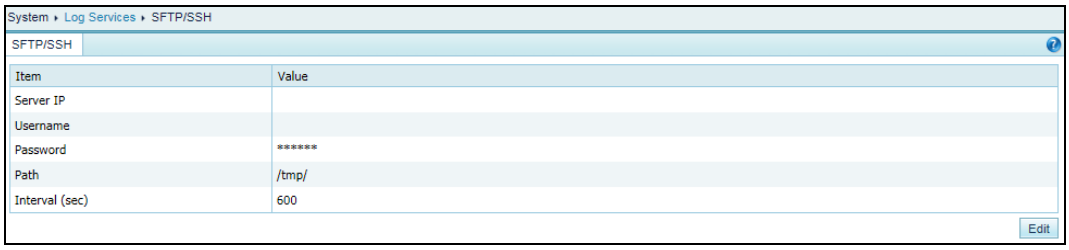
Note	After email parameters are configured, when the engine fails for three times, the system will automatically send engine fault logs to the specified email address.

----End

7.3.4 SFTP/SSH Settings

As shown in Figure 7-49, ADS can be configured to export logs of the protected server to a specified directory via SFTP or SSH.

Figure 7-49 Exporting logs via SFTP or SSH



Step 1 Click **Edit** in the lower-right corner of the page and configure the information for exporting logs via SFTP or SSH. See Figure 7-50.

Figure 7-50 Modifying the SFTP SSH service settings

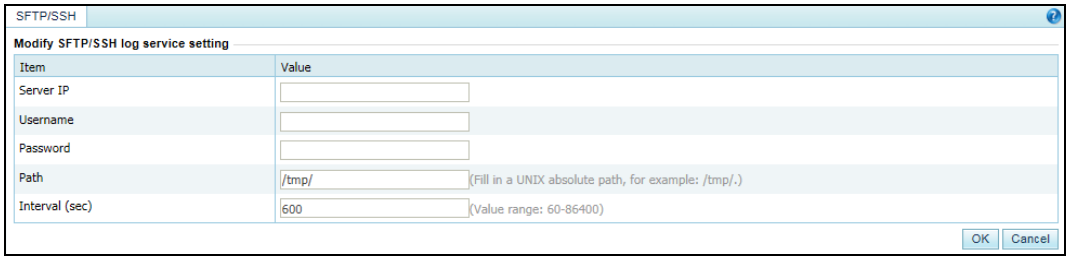


Table 7-16 describes parameters for exporting logs via SFTP or SSH.

Table 7-16 Parameters for exporting logs via SFTP or SSH

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

Step 2 After the parameter configuration is complete, click **OK** to save the settings.

----End

7.4 Others

This section covers the following topics:

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

7.4.1 License

ADS licenses fall into the following types:

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

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

Choose **System** > **Others** > **License Info**. The **License Info** page appears, as shown in Figure 7-51.

Figure 7-51 License information of ADS

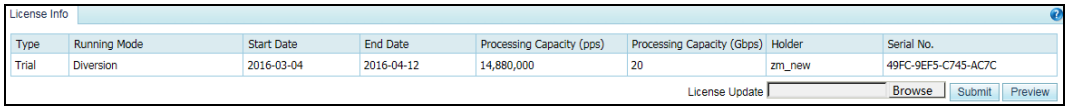


Table 7-17 describes ADS device license parameters.

Table 7-17 ADS device license parameters

Parameter	Description
Type	Two values are available: **Trial** and **Paid**.
Running Mode	Four values are available: **In-path**, **Cluster probe**, **Diversion**, and **In-path cluster**.
Start Date	Date when the license is produced. Note The current service indicates the authorized ADS upgrade service.
End Date	Date when the license is terminated. If a trial license expires, you cannot upgrade ADS that later works in packet forwarding mode and loses the protection function. If a paid license expires, you cannot upgrade ADS that still maintains the protection function. Note The current service indicates the authorized ADS upgrade service.
Processing Capacity (pps)	Maximum number of packets that ADS can process per second.
Processing Capacity (Gbps)	Maximum bandwidth for traffic cleansing. Note If the traffic exceeds the specified maximum bandwidth, ADS generate a system operation log to report an alert.
Holder	Customer who owns the current ADS device.
Serial No.	Serial number of the current ADS device.

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

- Preview a License

In the lower-right corner of the license information table, click **Browse t**o select a license file from the local host and then click **Preview** to preview details about the file.

- Import a License

In the lower-right corner of the license information table, click Browse to select a license file from the local host and then click **Submit** to import it. After the license is imported, it takes effect immediately. You can fresh the page to update the license information.

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

7.4.2 System Upgrade

You can manually import the upgrade file to upgrade ADS.

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

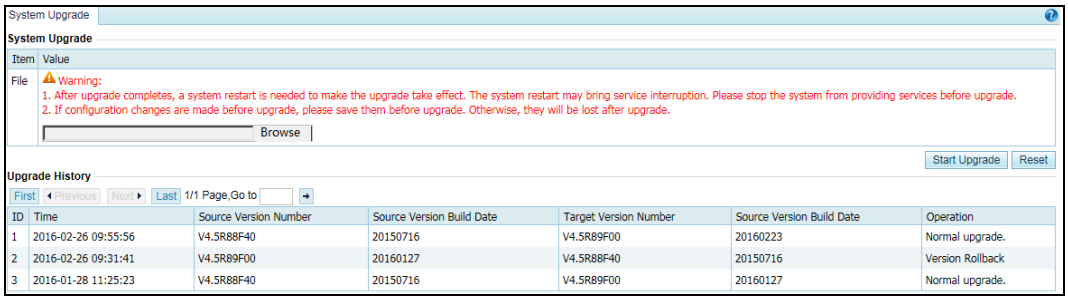
To upgrade ADS, perform the following steps:

Step 1 Contact technical support personnel of NSFOCUS for ADS upgrade packages.

Make sure that the package matches your product.

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

Figure 7-52 System Upgrade page



Step 3 Click **Browse** and select the **update.b64** file. Then click **Submit**.

Note	The upgrade process may take a long time. Wait until an upgrade success message appears. If problems emerge after upgrade and version rollback is needed, the system can only rolled back to the source version. For details, see section 9.2.9 Rolling Back the Version.

Step 4 After an upgrade success message appears, restart the system without clicking **Save**.

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

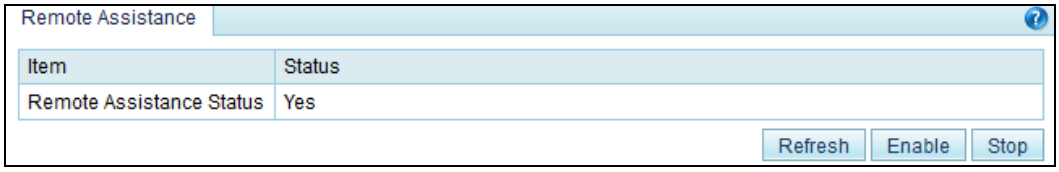
Alternatively, you can view the current version information in the **Upgrade History** table in the **System Upgrade** page shown in Figure 7-52.

----End

7.4.3 Remote Assistance

When a failure occurs in the system, contact technical support personnel of NSFOCUS for remote assistance. Enable remote assistance on the **Remote Assistance** page as shown in Figure 7-53. This function is disabled by default.

Figure 7-53 Remote assistance



Meanings of the buttons are as follows:

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

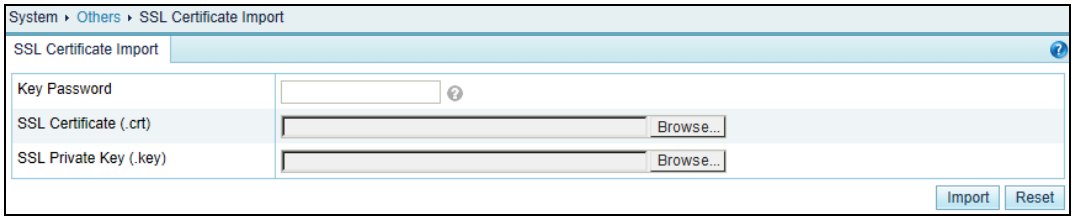
7.4.4 SSL Certificate Import

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 7-54 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

7.4.5 One-Click Info Collection

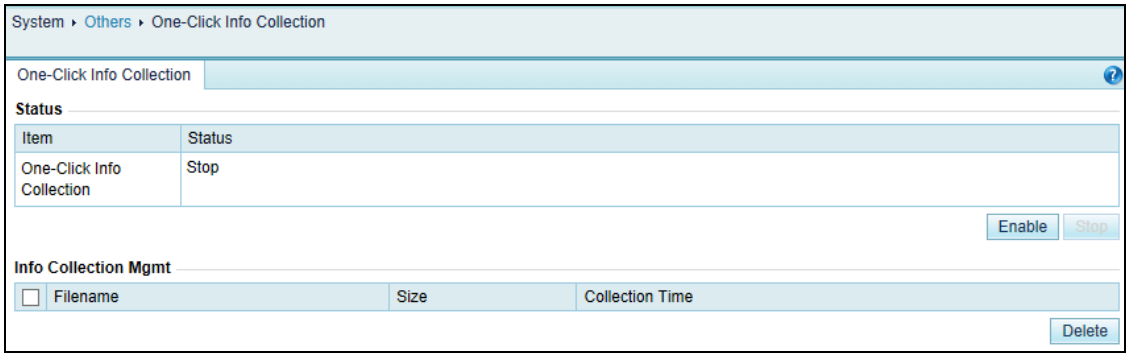
When ADS fails, users can collect device information by using the one-click information collection function, and deliver such information to technical support personnel of NSFOCUS, who therefore do not need to log in to ADS for collection of such information.

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

To collect the preceding information, perform the following steps:

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

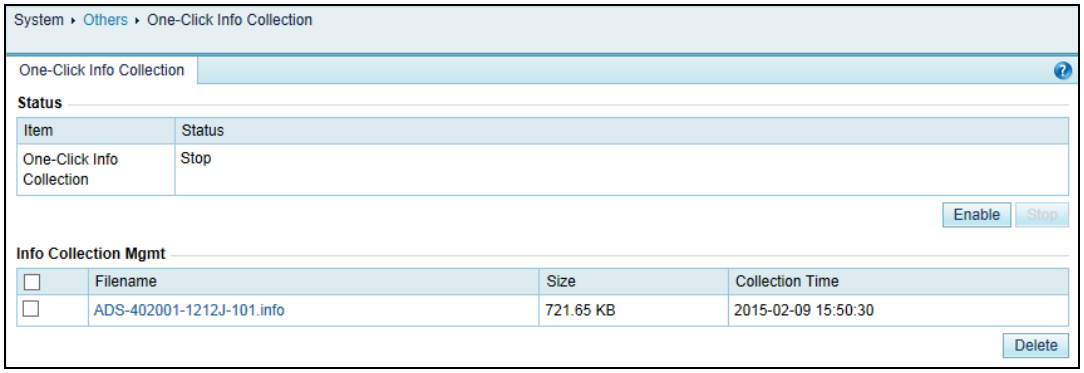
Figure 7-55 One-Click Info Collection page



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

After fault information is successfully collected, an information file is displayed in the **Info Collection Mgmt** table, as shown in Figure 7-56.

Figure 7-56 One-click information collection result



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

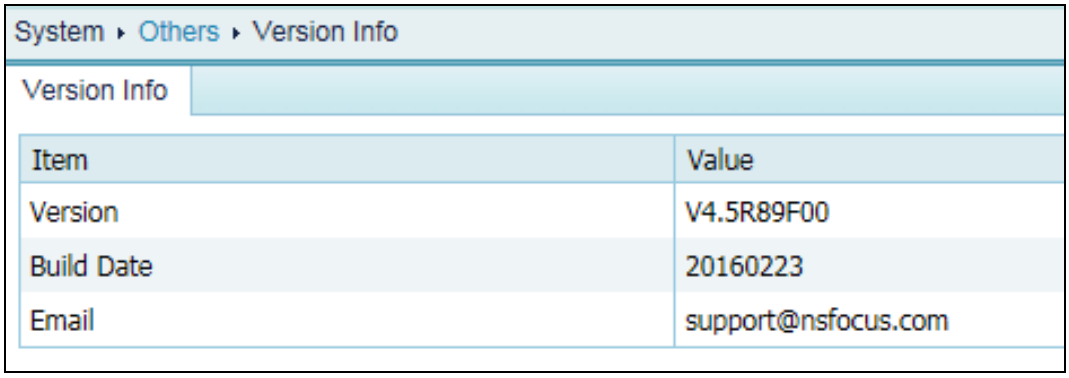
Users can send this file to technical support personnel of NSFOCUS for troubleshooting.

----End

7.4.6 Version Information

Choose **System** > **Others** > **Version Info**. The **Version Info** page displays the version number and the email address of NSFOCUS for technical support, as shown in Figure 7-57.

Figure 7-57 Version information



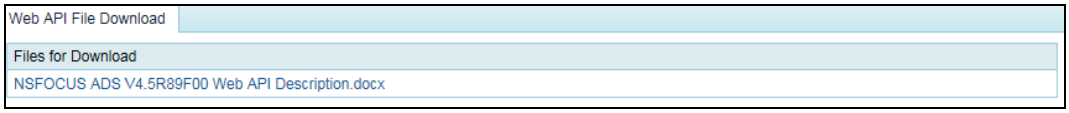
7.4.7 Web API File Download

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

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

In Figure 7-58, you can click a file name in the **Files for Download** area to download the file to a local disk drive.

Figure 7-58 Web API File Download page



8 Advanced Applications

This chapter dwells upon two advanced functions of the system, containing the following sections:

Section	Description
Packet Capture Management	Describes a tool usually used to analyze transmitted packets in the network.
Pattern Matching Rules	Describes a protection rule used to filter packets based on signature patterns.
IP Reputation	Describes how to configure collaboration between ADS and the cloud-side reputation database.

8.1 Packet Capture Management

Packet capture is the act of capturing network packets that comply with the conditions specified by users, so as to provide evidence for electronic forensics. ADS supports manual packet capture and automatic packet capture.

This section consists of the following:

- Configuring a manual packet capture task, including configuring task parameters and starting the task
- Configuring an automatic packet capture task, including configuring and viewing task parameters
- Managing the status of packet capture tasks, including viewing and refreshing the task status and stopping the ongoing task
- Managing the packet capture file, including viewing, downloading, and deleting the packet capture file
- Managing the auto packet capture file, including viewing, downloading, and deleting the packet capture file

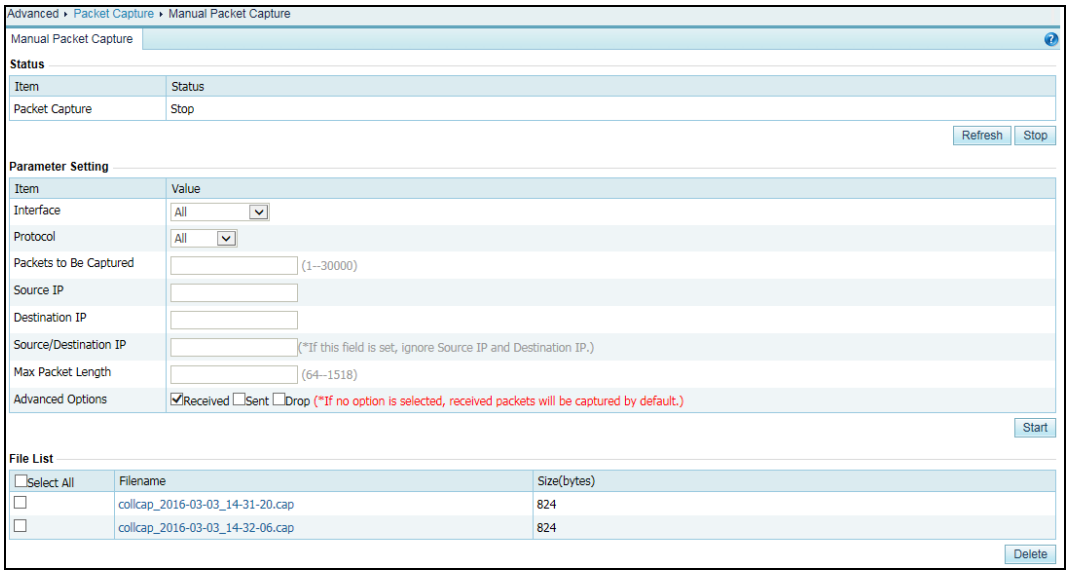
8.1.1 Configuring a Maunal Packet Capture Task

To configure and start the packet capture service, perform the following steps:

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

At the top of the **Manual Packet Capture** page, the status of packet capture tasks is displayed. For an ongoing packet capture task, **Status** is displayed as **Running**. Otherwise, **Status** is displayed as **Stop**. In the middle of the page, you can configure and start the packet capture task. At the bottom of the page, packet capture files are listed for ongoing and completed packet capture tasks.

Figure 8-1 Manual packet capture



Step 2 Configure parameters for manual packet capture.

Table 8-1 describes parameters for manual packet capture.

Table 8-1 Parameters for manual packet capture

Parameter	Description
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 are **All**, **TCP**, **UDP**, and **ICMP**, and **ICMPV6**. **All** is the default value.
Packets to Be Captured	Number of packets to be captured. The value ranges from 1 to 30,000.
Source IP	Source IP address of this task. This parameter is optional. If the source IP address is empty, it indicates that packets from any IP address can be captured. **Note** The source IP address can be an IPv4 or IPv6 address.
Destination IP	Destination IP address of this task. This parameter is optional. If the destination IP address is empty, it indicates that packets destined to any IP address can be captured. **Note**

Parameter	Description
	The destination IP address can be an IPv4 or IPv6 address.
Source/Destination IP	Source or destination IP address of the task. This parameter is optional. If you set this parameter, ignore **Source IP** and **Destination IP**. Note An IPv4 or IPv6 address is allowed.
Max Packet Length	Maximum length of the packet to be captured. The value ranges from 64 to 1518.
Advanced Options	This parameter is optional. Three options are available: **Received**, **Sent**, and **Drop**. **Received** indicates that ADS captures received packets. **Sent** indicates that ADS captures packets that are sent. **Drop** indicates that ADS captures dropped packets. If none is selected, received packets will be captured by default.

Step 3 Start the manual packet capture task.

After manual packet capture parameters are configured, click **Start** to start a new packet capture task.

When the packet capture task is in progress, **Status** is displayed as **Running and** the related packet capture file is displayed in the File List. When the packet capture task is complete, **Status** is displayed as **Stop**.

----End

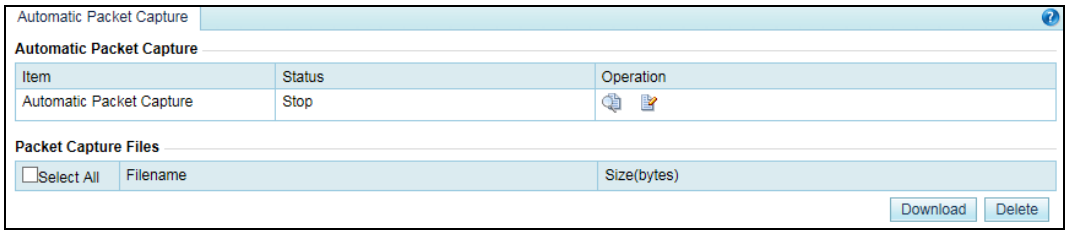
8.1.2 Configuring an Automatic Packet Capture Task

To configure and start an automatic packet capture service, perform the following steps:

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

At the top of the page, the status of the automatic packet capture task is displayed. If a packet capture task is operating, **Status** is displayed as **Running**. Otherwise, **Status** is displayed as **Stop**. In the middle of the page, you can configure and start the packet capture task. In the lower part of the page, the forensics file is listed for the completed packet capture task.

Figure 8-2 Automatic packet capture



Step 2 Configure parameters for automatic packet capture.

In the **Automatic Packet Capture** area, you can click in the **Operation** column to configure parameters for automatic packet capture.

In the **Automatic Packet Capture** area, you can click in the **Operation** column to view parameters for automatic packet capture.

Note	The number of automatic packet capture files should not exceed 20 and the total file size should be no greater than 500 MB. Otherwise, the system will automatically delete existing packet capture files.

Figure 8-3 Automatic Packet Capture page

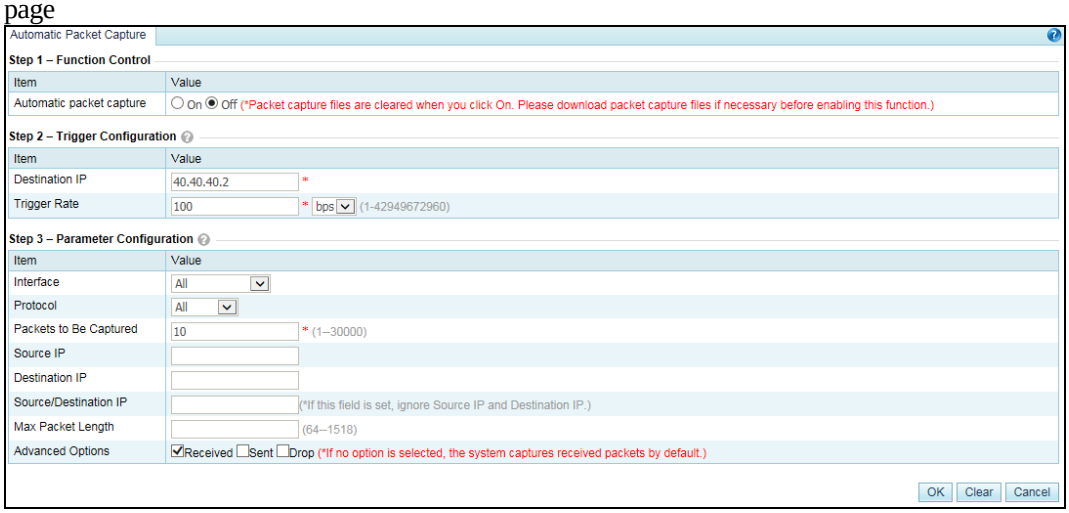


Table 8-2 describes parameters for automatic packet capture. For details, see Table 8-1

Table 8-2 Automatic packet capture parameters

Parameter	Description
Automatic Packet Capture	Controls whether to enable automatic packet capture. By default, it is disabled. When automatic packet capture is enabled, if the device storage is insufficient, the system will automatically clear existing automatic packet capture files.
Destination IP	Specifies the destination IP address for this packet capture task.
Trigger Rate	Specifies the number of packets received by the destination IP address per second that will trigger automatic packet capture. The value range is 1–4294967295 pps or 1–42949672960 bps.

Step 3 Start the automatic packet capture task.

After automatic packet capture parameters are configured, click **Start**. The automatic packet capture task starts only when specified conditions are triggered.

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 finished, **Status** is displayed as **Stop**.

----End

8.1.3 Managing the Status of Packet Capture Tasks

You can view the status of packet capture tasks in real time. When the packet capture task is in progress, the task status is **Running**. When the packet capture task is finished, the task status is **Stop**.

Note	Only one packet capture task runs at a time. Therefore, you can start a new task only after the previous task is finished or stopped.

On the page shown in Figure 8-1, click **Refresh** to refresh the status of the packet capture task on the **Packet Capture Management** page; click **Stop** to stop the ongoing packet capture task.

8.1.4 Managing Manual Packet Capture Files

After a manual packet capture task is ended, the manual packet capture file is displayed on the file list. You can view, download, or delete the packet capture file.

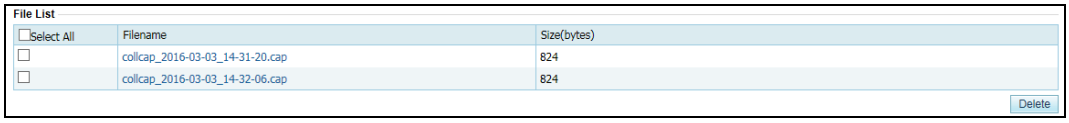
Note	ADS can manage a maximum of five latest packet capture files, each of which cannot exceed 16 MB.

Viewing a Manual Packet Capture File

Viewing Summary

Choose **Advanced** > **Packet Capture** > **Manual Packet Capture** to view the summary of a packet capture file, including the file name and size, as shown in Figure 8-4.

Figure 8-4 List of packet capture files

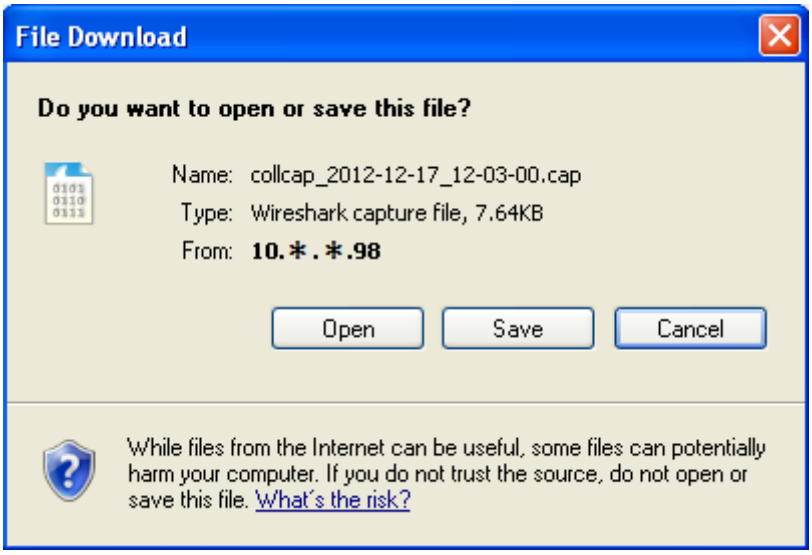


Viewing Details

Step 1 In the **File List** area shown in Figure 8-4, click a packet capture file name.

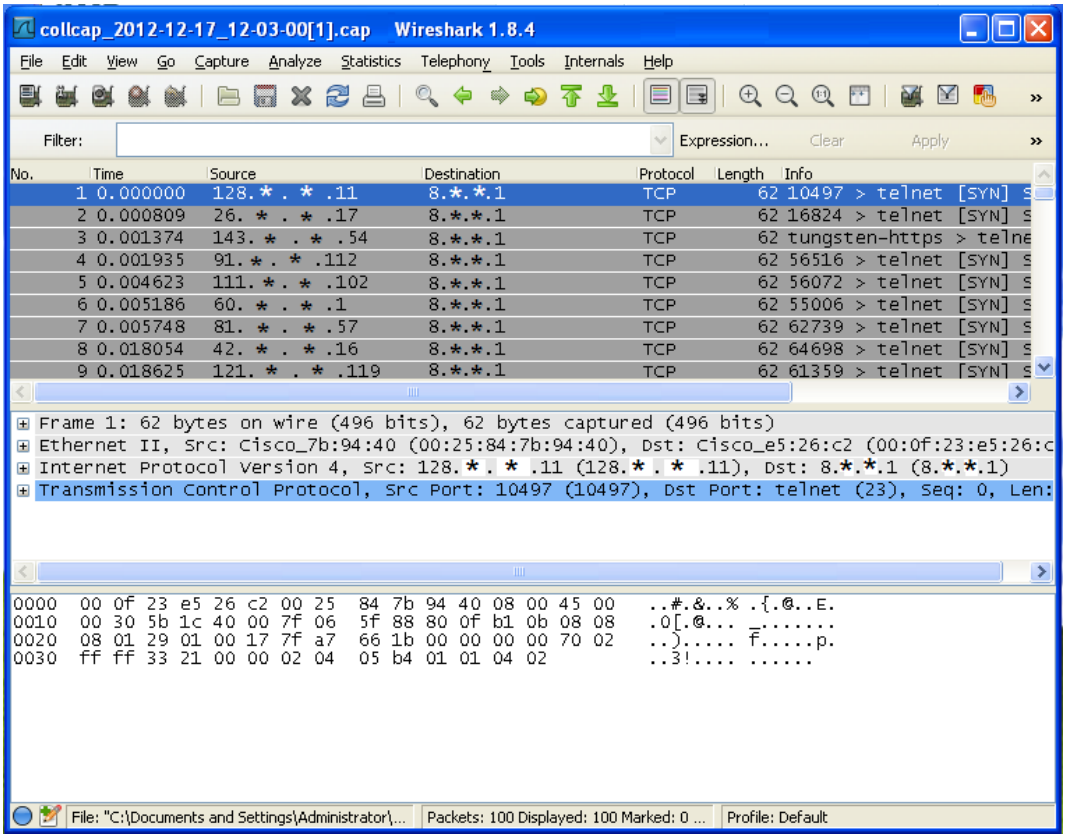
The following dialog box appears, as shown in Figure 8-5.

Figure 8-5 Viewing a packet capture file



Step 2 Click **Open** to view details of the packet capture file.

Figure 8-6 Details of a packet capture file



Step 3 After viewing details, click ✕ in the upper-right corner of the window to close the window.

----End

Downloading a Packet Capture File

Step 1 In the **File List** area shown in Figure 8-4, click the packet capture file name.

Step 2 Click **Save** in the dialog box.

Step 3 Select a file path and rename the file (or use the default file name and file path) and click **Save**.

----End

Deleting a Packet Capture File

Step 1 In the **File List** area shown in Figure 8-4, select one or more packet capture files (or select the **Select All** check box to select all files) of complete tasks and click **Delete** below the file list.

Step 2 Click **OK** in the deletion confirmation dialog box to delete selected packet capture files.

Note	The packet capture file of an ongoing task cannot be deleted.

----End

8.1.5 Managing Automatic Packet Capture Files

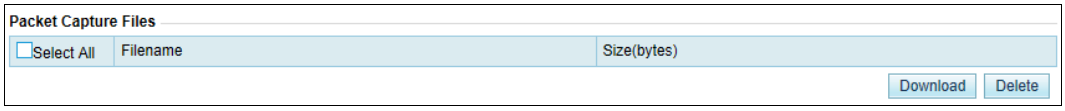
After an automatic packet capture task is over, the related packet capture file is displayed on the file list. You can view, download, and delete packet capture files.

Viewing an Automatic Packet Capture File

Viewing Summary

Choose **Advanced** > **Packet Capture** > **Automatic Packet Capture**. In the **Packet Capture Files** area, you can view the summary of packet capture files, including the file name and size, as shown in Figure 8-7.

Figure 8-7 List of packet capture files



Viewing Details

Step 2 On the file list shown in Figure 8-7, click the file name of a packet capture file.

Step 3 In the dialog box shown in Figure 8-5, click **Open**.

Then you can view details of this packet capture file.

----End

Downloading an Automatic Packet Capture File

Step 1 On the page shown in Figure 8-7, select one or more packet capture files (or select the **Select All** check box to select all files) and click **Download** below the file list.

Step 2 In the dialog box shown in Figure 8-5, click **Save**.

Step 3 In the dialog box that appears, select a file path, rename the file (you can also use the default file name and file path), and click **Save**.

----End

Deleting Packet Capture Files

Step 1 On the page shown in Figure 8-7, select one or more packet capture files (or select the **Select All** check box to select all files) and click **Delete** below the file list.

Step 2 In the deletion confirmation dialog box, click **OK** to delete the selected files.

Note	The packet capture file of an ongoing task cannot be deleted.

----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:

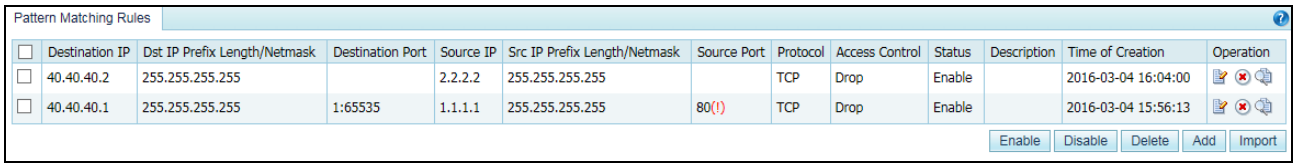
- Adding a Pattern Matching Rule
- Adding Pattern Matching Rules in Batches
- Enabling and Disabling Pattern Matching Rules
- Modifying Pattern Matching Rules
- Deleting Pattern Matching Rules
- Viewing Pattern Matching Rules

8.2.1 Adding a Pattern Matching Rule

To add a pattern matching rule, perform the following steps:

Step 1 Choose **Advanced** > **Pattern Matching** > **Pattern Matching Rules**.

Figure 8-8 Pattern Matching Rules page



Pattern Matching Rules

	Destination IP	Dst IP Prefix Length/Netmask	Destination Port	Source IP	Src IP Prefix Length/Netmask	Source Port	Protocol	Access Control	Status	Description	Time of Creation	Operation
	40.40.40.2	255.255.255.255		2.2.2.2	255.255.255.255		TCP	Drop	Enable		2016-03-04 16:04:00	
	40.40.40.1	255.255.255.255	1:65535	1.1.1.1	255.255.255.255	80(!)	TCP	Drop	Enable		2016-03-04 15:56:13	

Enable Disable Delete Add Import

Step 2 Click **Add**.

Figure 8-9 Adding a pattern matching rule (TCP)

Pattern Matching Rules

Add Pattern Matching Rule

Item	Value	Invert
Destination IP	*	
Dst IP Prefix Length/Netmask	255.255.255.0 *	
Destination Port	From To	Yes No
Source IP	*	Yes No
Src IP Prefix Length/Netmask	255.255.255.0 *	
Source Port	From To	Yes No
Protocol	TCP	
Access Control	Drop	
Enable	Yes No	
Interface	From To	Yes No
Packet Length	From To	
TOS	--	
TTL/HopLimit	--	
UDP Validation	(0 indicates that packets whose checksum is 0 are matched; 1 indicates that packets whose checksum is not 0 are matched; an empty value indicates that all packets are matched.)	
ICMP Header Type	--	
ICMPv6 Header Type	--	
TCP Option	--	
TCP Flag	SYN ACK FIN RST URG PSH No flag checking	
Offset	0 (Bytes)(0--1480)	
Depth	0 (Bytes)(0--1480)	
Match Case	Yes No	
Signature	Ordinary characters (When entering the signature, hexadecimal characters cannot contain \x, such as ababab or \xab\xab, and ordinary characters cannot contain !, $, ", or \x.)	Yes No
Description	Length is less than 256 characters.	
Time of Creation	2015-02-06 17:01:32	

OK Cancel

Table 8-3 describes parameters of a pattern matching rule

Table 8-3 Parameters of a pattern matching rule

Parameter	Description
Destination IP	Destination IP address of packets matching this rule. You can type an IPv4 or IPv6 address according to the actual network deployment.
Dst IP Prefix Length/Netmask	Prefix length (for IPv6 protocol) or netmask (for IPv4 protocol) of the destination IP address.
Destination Port	Destination port range. This is required only when **Protocol** is set to **TCP** or **UDP**. For example, 1049-5094 indicates packets with the destination port in the range from 1049 to 5094. If only 1049 is filled, it indicates that only packets with the destination port 1049 will be deemed to match this rule.
Source IP	Source IP address of packets to be matched with this rule. You can type an IPv4 or IPv6 address according to the actual network deployment.
Src IP Prefix Length/Netmask	Prefix length (for IPv6 protocol) or netmask (for IPv4 protocol) of the source IP address.
Source Port	Source port range. This is required only when **Protocol** is set to **TCP** or **UDP**. For example, 1049-5094 indicates packets with the source port in the range from 1049 to 5094. If only 1049 is filled, it indicates that only packets with the source port 1049 will be deemed to match this rule.
Protocol	Values are **TCP**, **UDP**, **ICMP**, and **ICMPv6**.
Access Control	Action performed by ADS on packets matching this rule. • **Protect** indicates that ADS allows packets matching this rule to pass through. • **Drop** indicates that ADS drops packets matching this rule. • **Drop and add to blacklist** indicates that ADS drops packets matching this rule and adds their source IP addresses to the blacklist. • **Drop and disconnect** indicates that ADS drops packets matching this rule and sends an RST packet to the server to interrupt the connections. • **Drop,add to blacklist,and disconnect** indicates that ADS drops packets matching this rule, adds their source IP addresses to the blacklist, and sends an RST packets to the server to interrupt connections. Note If **Access Control** is set to **Drop and add to blacklist** or **Drop,add to blacklist,and disconnect**, you also need to enable the blacklist function. Otherwise, the blacklist is invalid. For details, see section 4.2.8 Blacklist.
Enable	Controls whether to enable this rule. The value **Yes** indicates this rule is enabled.
Interface	Range of the interfaces (working interfaces on the front panel of ADS) through which packets are transmitted.
Packet Length	Length range of packets to be matched with this rule.
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**.

Parameter	Description
UDP Validation	Checksum of UDP packets. This is available only when **Protocol** is set to **UDP**.
ICMP Header Type	Type of the ICMP packet header. This is available only when **Protocol** is set to **ICMP**.
ICMPv6 Header Type	Type of the ICMPv6 packet header. This is available only when **Protocol** is set to **ICMPv6**.
TCP Option	Three options are available: **Max Packet Length**, **Window Scale**, and **Timestamp**. This is available only when **Protocol** is set to **TCP**.
TCP Flag	Flag bit of the TCP packet header. This is available only when **Protocol** is set to **TCP**.
Offset	Number of bytes from the start of the packet body to a given position where the search starts. Its value should be smaller than the total length of the packet body. For TCP packets, the packet body includes the TCP header. For UDP packets, the packet body refers to the payload.
Depth	Maximum number of bytes allowed for searching. The depth is equal to the total length of packet body minus the offset.
Match Case	Controls whether signature characters are case sensitive. Only English letters are under this restriction.
Signature	Signature characters to be searched. Special and unprintable characters need to be translated into hex format (for example, translate carriage return and line feed into \x0d\x0a). You can also leave this field empty. In this case, **Offset** and **Depth** are both **0**, which cannot be changed. Requirements for typing ordinary characters are as follows: • Special characters (! $ ") and spaces, and GBK encoded characters (Chinese) are not supported. • Characters preceded with \\x will be interpreted as hexadecimal characters. As \x is used to differentiate hexadecimal characters from ordinary characters, characters preceded with \x are not allowed if **Ordinary characters** is selected. Requirements for typing hexadecimal characters are as follows: • Hexadecimal characters with or without \x, such as \x67\x1f and 671f, are supported. • Only single-byte characters, like \x67\x1f, are allowed. • Double-byte characters, like \x671f\x1a, are not allowed. • Characters like \x6\x1a are not allowed. • Spaces are not allowed. You can select **Ordinary characters** or **Hexadecimal characters** for **Signature**. You are advised to copy the signature characters from the packet capture file and paste them to the **Signature** text box. If certain characters are not required, delete them. The following shows how to copy signature characters from Wireshark: Use Wireshark to open a captured packet, right-click the target signature character line, and choose **Copy** > **Bytes** > **Hex Stream** to copy the selected hexadecimal character line.

Parameter	Description
Description	Brief description of this rule.
Time of Creation	Time when the rule is created, which is automatically generated by the system.

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

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

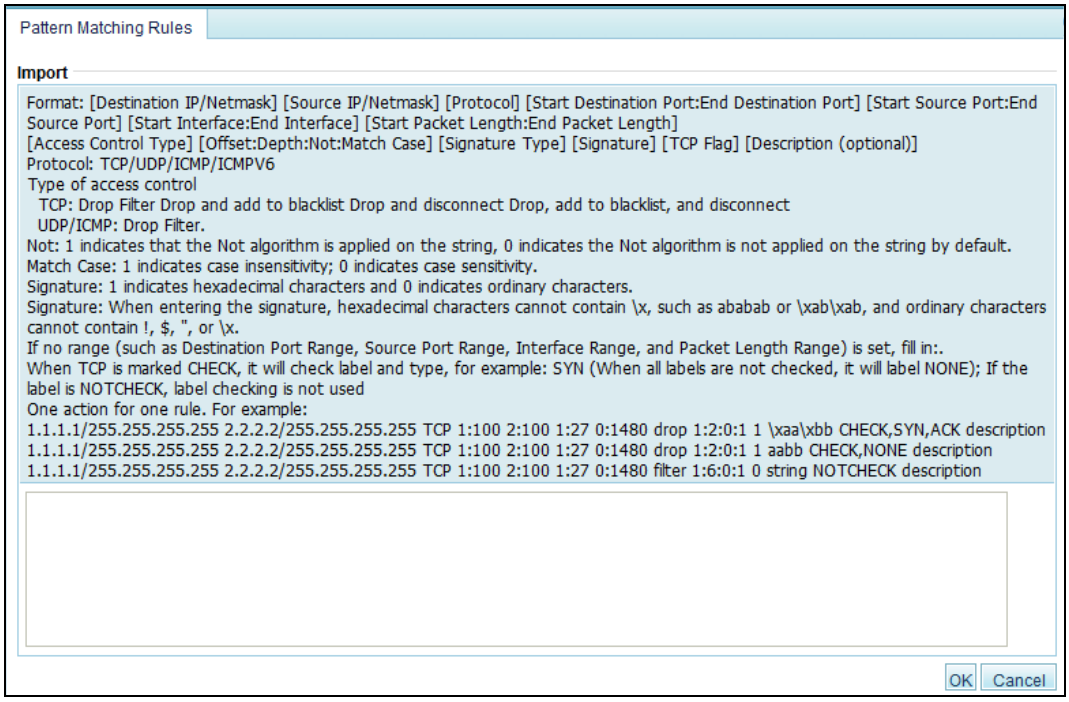
----End

8.2.2 Adding Pattern Matching Rules in Batches

You can add pattern matching rules in batches on ADS by performing the following steps:

Step 1 On the **Pattern Matching Rules** page shown in Figure 8-8, click **Import** below the table to add pattern matching rules in batches.

Figure 8-10 Adding pattern matching rules in batches



Step 2 Type pattern matching rules as prompted.

Pay attention to the following format specifications:

- Parameters of each pattern matching rule are separated by spaces.

- Each line contains only one rule.

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

----End

8.2.3 Enabling and Disabling Pattern Matching Rules

On ADS, only enabled pattern matching rules are valid, while disabled ones are invalid. Enabling and disabling pattern matching rules can free the administrator 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 8-8, select one or more pattern matching rules (or select the **Select All** check box to select all rules), click **Enable** below the table, and then click **OK** in the confirmation dialog box to enable selected rules.

Disabling Pattern Matching Rules

Disable pattern matching rules that are enabled.

On the **Pattern Matching Rules** page shown in Figure 8-8, select one or more pattern matching rules (or select the **Select All** check box to select all rules), click **Disable** below the table, and then click **OK** in the confirmation dialog box to disable selected rules.

8.2.4 Modifying Pattern Matching Rules

After configuring pattern matching rules, the administrator can edit rule parameters by performing the following steps:

Step 1 On the **Pattern Matching Rules** page shown in Figure 8-8, click to edit parameters of a rule, as shown in Figure 8-9.

Step 2 Click **OK** to save settings and return to the **Pattern Matching Rules** page.

----End

8.2.5 Deleting Pattern Matching Rules

You can delete one pattern matching rule or multiple rules in batches on ADS in one of the following way:

- On the **Pattern Matching Rules** page shown in Figure 8-8, click on the right of a rule and then click **OK** in the confirmation dialog box to delete a rule.
- On the **Pattern Matching Rules** page shown in Figure 8-8, select one or more pattern matching rules (or select the **Select All** check box to select all rules on the list) to be deleted, click **Delete** below the table, and then click **OK** in the confirmation dialog box to delete selected rules.

8.2.6 Viewing Pattern Matching Rules

On the **Pattern Matching Rules** page shown in Figure 8-8, click to open the dialog box for viewing pattern matching rules.

After viewing rules, click **Back** to return to the **Pattern Matching Rules** page.

8.3 IP Reputation

ADS can collaborate with NSFOCUS's IP reputation library in the cloud. Specifically, ADS uploads blacklists of source IP addresses to the IP reputation library in the cloud, which sends the latest reputation data to ADS. For high-risk IP addresses, ADS automatically lists them on blacklists and blocks packets from these addresses.

To use this function, you need to buy an additional license. For details, contact technical support personnel of NSFOCUS.

Choose **Advanced** > **IP Reputation**. The **Cloud IP Reputation** page appears, as shown in Figure 8-11.

Figure 8-11 Cloud IP Reputation page

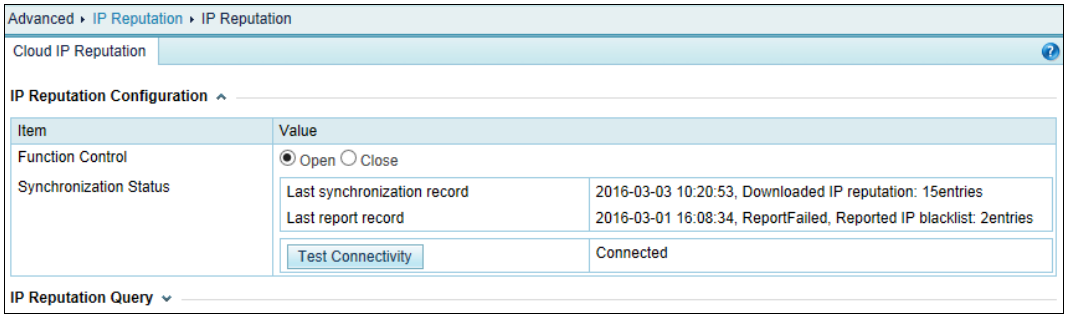


Table 8-4 describes IP reputation configuration parameters.

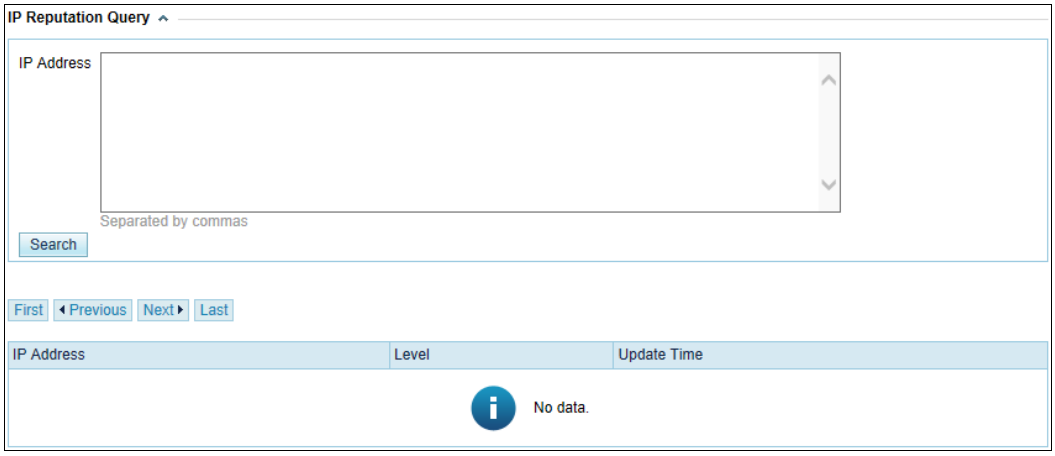
Table 8-4 IP reputation configuration parameters

Parameter	Description
Function Control	Controls whether to enable synchronization with the IP reputation library in the cloud. After this function is enabled, ADS immediately downloads data from the IP reputation library in the cloud and refreshes the current blacklist. For high-risk IP addresses, ADS will block packets from them. If you need to enable this function, you are advised to enable the blacklist function at the same time. Only in this way, can ADS automatically upload local blacklists of source IP addresses to the cloud. For details about the blacklist function, see section 4.2.8 Blacklist.
Synchronization Status	• **Last synchronization record**: provides information about the last synchronization from the IP reputation library in the cloud. This information is automatically updated on a daily basis. • **Last record report**: provides information about the last upload of data to the

Parameter	Description
	IP reputation library in the cloud. This information is automatically updated on an hourly basis.
Test Connectivity	A button for you to test whether ADS is properly connected to the IP reputation library in the cloud. After you click this button, if **Connected** is displayed, ADS can properly communicate with the IP reputation library; if another word is displayed, you must check the network status to ensure the proper communication between ADS and the IP reputation library.

You can also query the IP reputation library in the cloud from ADS. In the area shown in Figure 8-12, type one or more IP addresses separated by commas, and then click **Search** to check whether specific IP addresses exist in the library. The matched IP addresses are displayed in the lower part of the page together with the credit level and update time.

Figure 8-12 IP Reputation Query area



9 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.

9.1 Login to the Console

Before logging in to the console, you need to prepare the following:

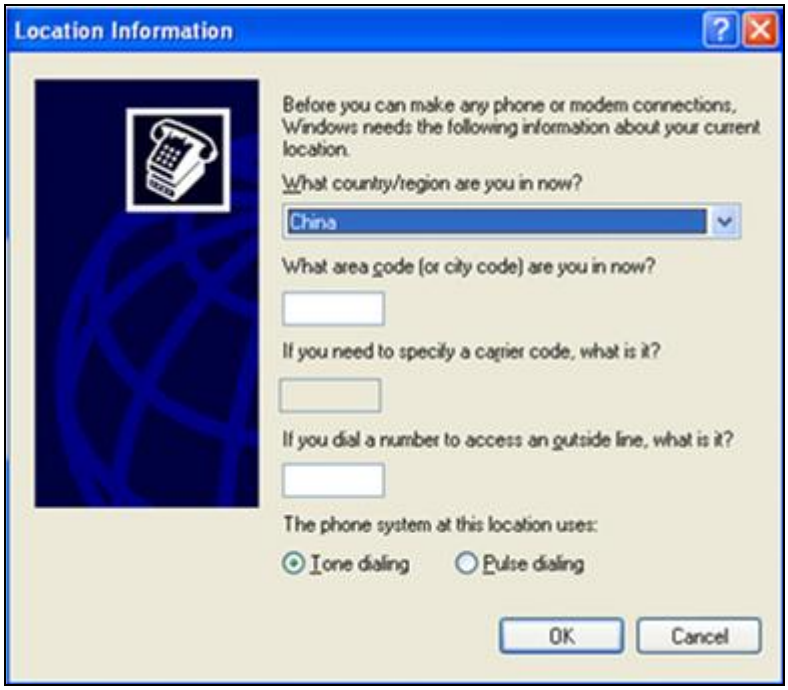
- One computer
- One serial cable included in the accessory box
- Terminal software (such as the HyperTerminal software included in Microsoft Windows) that can establish communication to the ADS device via the console
- Connection of ADS to the computer with a console cable

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:

Step 1 Choose **Start** > **All Programs** > **Accessories** > **Communications** > **HyperTerminal** to launch the HyperTerminal.

- If the **Location Information** dialog box shown in Figure 9-1 appears, go to Step 2.
- If the **Connection Description** dialog box shown in Figure 9-2 appears, go to Step 3.

Figure 9-1 Location Information dialog box



Step 2 Click **Cancel**, **Yes,** and then **OK**.

Figure 9-2 Connection Description dialog box

Step 3 In the **Connection Description** dialog box, type the connection name (ADS in this case) and click **OK**.

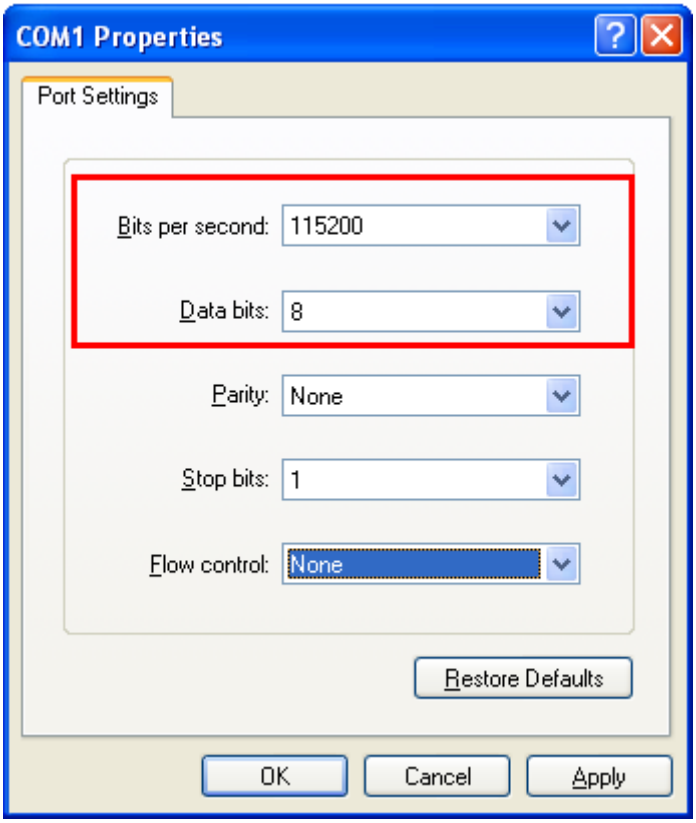
Step 4 Select a port (COM1 in this example) that is connected to the computer through a serial cable. Then click **OK**.

Figure 9-3 Port connected to HyperTerminal

Step 5 Configure port attributes, for example, setting **Bits per second** to **115200** and **Data bits** to **8**, as shown in Figure 9-4.

For ADS NX5-8000, **Flow control** can be set to any value.

Figure 9-4 Configuring port attributes



Step 6 Click **OK** and then press **Enter**.

Step 7 After the **login:** prompt appears, type the user name and password (**admin** and **nsfocus** respectively by default) of the console administrator.

Figure 9-5 Login to the console

```
nsfocus-ads login: admin
Password:
```

If the user name and password are correct, the administrator will successfully log in to the console. Optimal display effect will be achieved for terminal ID VT100.

----End

9.2 Details

After you successfully log in to the console of the ADS device, the main menu is displayed, as shown in Figure 9-6. Type a sequence number as prompted and press **Enter** to open a menu.

Figure 9-6 Main menu of the console

```
Welcome to Nsfocus ADS
========================================
      1.  IPv4 Network setting
      2.  IPv6 Network setting
      3.  DNS setting
      4.  Console Password change
      5.  Datetime setting
      6.  All Default setting
      7.  Web Password Default setting
      8.  Console time out setting
      9.  Rollback system
      10. Logout
========================================
Your password is the initial password.
Please choose "Console Password Change" to customize a new one.
Input your selection:

ADS login:
```

9.2.1 Configuring IPv4 Network Settings

On the main menu, type **1** and press **Enter** to open the IPv4 address configuration screen. Type the IPv4 address, netmask, and gateway address, with each followed by a carriage return. The system displays the settings, as shown in Figure 9-7.

After confirming the settings, type **y** and press **Enter** to save the settings and return to the main menu.

Figure 9-7 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):
```

9.2.2 Configuring IPv6 Network Settings

On the main menu, type **2** and press **Enter** to open the IPv6 address configuration screen. Type the IPv6 address, prefix length, and gateway address, with each followed by a carriage return. The system displays the settings, as shown in Figure 9-8.

After confirming the settings, type **y** and press **Enter** to save the settings and return to the main menu.

Figure 9-8 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):
```

9.2.3 Configuring DNS Settings

On the main menu, type **3** and press **Enter** to open the DNS configuration screen.

As shown in Figure 9-9, type the IP address of the DNS server as prompted, and press **Enter** to save the settings and return to the main menu.

Figure 9-9 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!
```

9.2.4 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 9-10.

Type the current password and new password, and press **Enter**. Then the system displays a message notifying you whether the password is successfully changed.

Figure 9-10 Changing the console password

```
Note: a good password should have different characters such as [A-Z][a-z][0-9][!@#$%
],and no less than 8 characters

Thu Mar 28 09:11:17 CST 2013
Changing password for admin
Old password:
```

Note	Please set the login password of the console as prompted. See appendix B Default Parameters for the initial account of the console.

9.2.5 Setting System Time

On the main menu, type **5** and press **Enter** to set system time, as shown in Figure 9-11.

Type the new system date and time (format: 2013-03-26 14:52:12), and then press **Enter** to save the settings and return to the main menu.

Figure 9-11 Setting system time

```
Datetime set:
Current date is 2012-03-26 14:52:12
Input the new date:
```

Caution	Changing system time may interrupt BGP routes and suspend traffic diversion. Please handle with caution.

9.2.6 Restoring Default Settings

On the main menu, type **6** and press **Enter** to restore default settings, including network settings and password of the web administrator. This operation takes effect immediately.

Note that the IP address of the management interface is restored as follows:

- If the management interface is configured with an IPv6 address, the IPv6 address is cleared.
- If the management interface is configured with an IPv4 address, the default IPv4 address is restored.

9.2.7 Restoring Initial Password of Web Administrator

On the main menu, type **7** and press **Enter** to restore the initial password of the web administrator, as shown in Figure 9-12.

Type **y** as prompted and press **Enter** to restore the initial password, **nsfocus**.

Figure 9-12 Restoring the initial password of the web administrator

```
Input your selection:7
Warning: it will reset web password as default
Are you sure to continue(y/n)?:
```

9.2.8 Setting the Console Timeout Value

On the main menu, type **8** and press **Enter** to open the console timeout setting window.

Figure 9-13 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 9-14, 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 is an integer in the range of 1 to 60.

Figure 9-14 Setting the timeout value

```
Console time out is close.
=================================
      1. Enable console time out
      2. Disable console time out
      3. Set console time out value
      4. return
=================================
Input your selection:3
Time value in minute[1~60]:
```

- Type **4** and press **Enter** to return to the main menu.

9.2.9 Rolling Back the Version

Note	This function works only for ADS V4.5R88F30 and later.

On the main menu, type **9** and press **Enter** to open the version rollback window.

Figure 9-15 Rolling back the version

```
Welcome to Nsfocus ADS
========================================
      1.  IPv4 Network setting
      2.  IPv6 Network setting
      3.  DNS setting
      4.  Console Password change
      5.  Datetime setting
      6.  All Default setting
      7.  Web Password Default setting
      8.  Console time out setting
      9.  Rollback system
      10. Logout
========================================
Your password is the initial password.
Please choose "Console Password Change" to customize a new one.
Input your selection:9
This operation will rollback system to last avaliable version.
And it will reboot system automatically if rollback succeed. Are you sure want to rollback system[y|n]?y
It will rollback to version V4.5R88F30 (build date: 20150127). Are you sure to continue?[y|n]
y
Start to rollback system and it will take a few minutes. Please wait.......
[  371.646461] EXT2-fs (sda1): warning: mounting unchecked fs, running e2fsck is recommended
Rollback succeed and it will reboot system after a few seconds.
```

In the window shown in Figure 9-15, 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.

9.2.10 Exiting the Console

On the main menu, type **10** and press **Enter** to log out of the console management interface.

A Abbreviations

ACL	access control list
ARP	Address Resolution Protocol
CGI	Common Gateway Interface
CSRF	cross-site request forgery
CSS/XSS	cross-site scripting
DDoS	distributed denial-of-service
HTTP	Hypertext Transfer Protocol
IDC	Internet Data Center
IP	Internet Protocol
LAN	local area network
MAC	Media Access Control
MIME	MultIPurpose Internet Mail Extensions
NSFOCUS WAF	NSFOCUS Web Application Firewall
SQL	Structured Query Language
URL	Uniform Resource Locator
WAN	wide area network

B Default Parameters

B.1 Default Console Parameters

IP Address	192.168.1.100
Netmask	255.255.255.0
Gateway	192.168.1.1

B.2 Default Web Administrator Account

User Name	admin
Password	nsfocus

B.3 Default Console Administrator Account

User Name	admin
Password	nsfocus

B.4 Default CLI Administrator Account

User Name	routerman

B.5 Console Specification

Serial Port	RJ-45
Baud Rate	115200 bps

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	√	×
	TCP control parameters	√	√
	IP behavior control	√	×
	SIP protection – default DDoS	√	×
	SIP protection – groups	√	√
	UDP payload check	√	×
	UDP protection – drop UDP fragments – default DDoS	√	×
	UDP protection – drop UDP fragments – groups	√	×
	UDP protection – maximum packet length	√	√
	UDP protection – traffic control by Src IP + Src port	√	√
	UDP protection – traffic control by Dst IP + Dst port	√	√
	UDP protection – traffic control by Src IP	√	√
	UDP protection – traffic control by Dst IP	√	√
	UDP protection – minimum packet length	√	√

Module	Function	IPv4	IPv6
	UDP protection – traffic control by Dst IP + Src port	√	√
	ICMP traffic rate limiting	√	√
	Watermark protection	√	×
	Group traffic control	√	√
	Port check	√	√
	URL rules	√	√
	Advanced global parameters	√	√
	Policy auto-learning	√	√
	Access control rules	√	√
	GeoIP rules	√	√
	Regular expression rules	√	×
	Hardware access control rules	√	√
	Connection exhaustion rules	√	×
	URL-ACL protection rules	√	√
	Blacklist	√	×
	Whitelist	√	√
	HTTP keyword checking	√	×
	DNS keyword checking	√	×
Diversion & Injection	Running mode	√	√
	Port channel configuration	√	√
	IP address configuration	√	√
	BGP diversion	√	√
	OSPF diversion	√	√
	ISIS diversion	√	×
	RIP diversion	√	×
	LDP diversion	√	×
	IP route assignment	√	√
	Injection interface	√	√
	Layer 2 injection	√	√
	Layer 3 injection	√	√
	MPLS injection	√	×
	MPLS VPN injection	√	×
	GRE tunnel injection	√	×

Module	Function	IPv4	IPv6
	MAC address table	√	√
	Filtering rules	√	√
	Manual diversion	√	√
	Group diversion	√	√
	Diversion routing table	√	√
	MPLS route	√	×
	Syslog diversion configuration – collaboration with Genie devices	√	×
	Syslog diversion configuration – collaboration with Arbor devices	√	×
	Syslog diversion configuration – collaboration with Samurai devices	√	×
	Syslog diversion configuration – collaboration with Kuanguang devices	√	×
Collaboration	Collaboration with ADS M	√	√
	Collaboration with ESPP	√	×
	Collaboration with NTA V4.5.61	√	×
	Collaboration with NTA V4.5.88	√	√
Logs	Attack logs	√	√
	System operation logs	√	√
	System login logs	√	√
	Link status logs	—	—
	Traffic diversion logs	√	√
	HA synchronization logs	√	√
	Syslog diversion logs	√	×
System	Basic settings	√	√
	Interface link configuration	—	—
	System user management	√	√
	Management mode configuration	√	√
	Configuration file import and export	√	√
	HA configuration	√	√
	Collaboration configuration	√	×
	Bandwidth overrun limit	√	×
	Login security settings	√	×
	Locked user management	√	×

Module	Function	IPv4	IPv6
	Authentication configuration	√	√
	Syslog configuration	√	√
	SNMP trap configuration	√	√
	SNMP agent setting	√	×
	Email configuration	√	√
	SFTP/SSH log export	√	×
	License interface	—	—
	License speed limit	—	—
	System upgrade	—	—
	Remote assistance	—	—
	SSL certificate import	—	—
	One-click information collection	—	—
	Version information	—	—
Advanced	Packet capture management	√	√
	Pattern matching rules	√	√
IP Reputation	Upload	√	√
	Synchronization	√	×
	Query	√	×