NSFOCUS ADS M

User Guide

Version: V4.5R90F00 (2017-12-01)

© 2018 NSFOCUS

■ Copyright © 2017 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 1
Conventions 2
Customer Support 2
1 Overview 3
2 Web-based Manager 4
2.1 Login 4
2.2 Layout 6
2.3 Other Operations 7
3 Web-based System Management 9
3.1 Local Settings 9
3.1.1 Basic Settings 9
3.1.2 License Management 12
3.1.3 System Upgrade 14
3.1.4 Data Storage 15
3.1.5 Network Configuration 17
3.1.6 DNS Server 24
3.1.7 HA Configuration 24
3.1.8 Performance Alert Configuration 28
3.2 User and Audit 28
3.2.1 User Management 29
3.2.2 Security Settings 31
3.2.3 Authentication Configuration 34
3.2.4 Audit Logs 35
3.3 Third-Party Interface 36
3.3.1 SNMP Configuration 36
3.3.2 Syslog Configuration 39
3.3.3 Data Export 40
3.3.4 Mail Alert Settings 42
3.3.5 SMTP Server Configuration 43
3.4 Debug Information Collection 44

4 Traffic Monitoring 45
4.1 Overview 45
4.1.1 Adding a Panel 46
4.1.2 Changing a Panel 49
4.1.3 Deleting a Panel 51
4.1.4 Downloading a Report 52
4.1.5 Viewing the System Status Bar 52
4.1.6 Generating Sound Alerts 53
4.1.7 Viewing Attack Traffic Trends 54
4.1.8 Viewing Protocol-Specific Traffic 57
4.1.9 Viewing Traffic of Top Destination IP Addresses 64
4.1.10 Viewing Attack Traffic of Top Regions 70
4.1.11 Viewing Traffic of Top Source Countries 72
4.1.12 Viewing Attack Traffic 77
4.1.13 Viewing Top Alerts Reported by NTA 80
4.1.14 Viewing Top Ongoing Attack Events 83
4.1.15 Viewing Top 10 Source IP Addresses 89
4.1.16 Viewing Attack Type Distribution 94
4.1.17 Viewing Device Monitoring Information 98
4.1.18 Viewing Traffic of Top NTA's Regions 100
4.1.19 Viewing Trends of Traffic on NTA 102
4.2 DDoS Attack Traffic Monitoring 105
4.2.1 Viewing Real-Time Attack Traffic Information 105
4.2.2 Viewing Region-Specific Traffic Information 112
4.2.3 Viewing Device-Specific Traffic Information 113
4.2.4 Viewing Object-Specific Traffic Information 114
4.2.5 Viewing Traffic Information of an IP Address in the Default Protection Group 116
4.2.6 Viewing Historical Attack Traffic Trends 118
4.2.7 Switching the Traffic Unit 120
4.2.8 Refreshing the Attack Traffic Trend Graph 120
4.2.9 Downloading a Traffic Trend Report 121
4.2.10 Managing Filters 121
4.2.11 Managing Panels 123
4.3 Network Traffic Monitoring 124
4.3.1 Viewing Real-Time Network Traffic Information 125
4.3.2 Viewing Device-Specific Network Traffic Information 130
4.3.3 Viewing Region-Specific Network Traffic Information 131
4.3.4 Viewing IP Group-Specific Network Traffic Information 132
4.3.5 Viewing Object-Specific Network Traffic Information 133
4.3.6 Viewing Historical Network Traffic Trends 134
4.3.7 Switching the Traffic Unit 136
4.3.8 Refreshing the Traffic Trend Graph 136

4.3.9 Downloading a Traffic Trend Report 136
4.3.10 Managing Filters 136
4.3.11 Managing Panels 138
4.4 Attack Events 139
4.4.1 Viewing Attack Events in Real Time Mode 140
4.4.2 Viewing Region-Specific Attack Events 142
4.4.3 Viewing Device-Specific Attack Events 143
4.4.4 Viewing Object-Specific Attack Events 144
4.4.5 Viewing Attack Event Information of an IP Address in the Default Protection Group 146
4.4.6 Viewing Attack Events in Historical Mode 148
4.4.7 Switching the Traffic Unit 150
4.4.8 Refreshing the Attack Traffic Trend Graph 150
4.4.9 Downloading an Attack Traffic Trend Report 150
4.4.10 Managing Filters 150
4.4.11 Managing Panels 153
5 Reports 155
5.1 Built-in Reports 155
5.2 Custom Reports 156
5.3 Email Report 160
5.4 Custom Logo 162
6 Logs 164
6.1 Attack Summary Log 164
6.2 Login Log 165
6.3 Operation Log 166
6.4 Link Status Log 167
6.5 Diversion Log 167
6.6 Performance Log 168
6.7 Performance Alert Log 169
6.8 HA Log 170
6.9 Traffic Alert Log 171
6.10 Cloud Authentication Logs 174
7 Region Management 175
7.1 Managing Group Labels 175
7.1.1 Creating a Group Label 176
7.1.2 Editing a Group Label 176
7.1.3 Deleting a Group Label 177
7.2 Managing Region Managers 177
7.2.1 Creating a Region Manager 177
7.2.2 Configuring Permissions of a Region Manager 178
7.2.3 Editing a Region Manager 179
7.2.4 Deleting a Region Manager 179

7.3 Configuring a Region 179
7.3.1 Creating a Region 180
7.3.2 Viewing Details of a Region 186
7.3.3 Editing a Region 187
7.3.4 Deleting a Region 187
7.4 Configuring a Regional IP Group 187
7.4.1 Adding a Regional IP Group 187
7.4.2 Modifying a Regional IP Group 195
7.4.3 Deleting a Regional IP Group 195
7.4.4 Viewing Configuration Information of a Regional IP Group 196
7.5 Configuring Traffic Diversion for a Region 196
7.5.1 Viewing the Region Under Traffic Diversion 197
7.5.2 Configuring IP Addresses for Diversion 197
7.6 Configuring an ADS Protection Policy Template 198
8 Device Management 200
8.1 Managing ADS Devices 200
8.1.1 Adding an ADS Device 201
8.1.2 Editing ADS Device Settings 202
8.1.3 Deleting an ADS Device 203
8.1.4 Modifying Access Accounts in Batches 203
8.1.5 Synchronizing Time 204
8.1.6 Manually Synchronizing Configurations 204
8.1.7 Saving the Configuration 204
8.1.8 Configuring an ADS Device 205
8.2 Managing ADS Clusters 205
8.2.1 Adding an ADS Cluster 205
8.2.2 Configuring a Cluster Blacklist 207
8.2.3 Cluster Packet Capture 212
8.2.4 Adding an ADS Device to the Cluster 218
8.2.5 Modifying a Cluster 219
8.2.6 Deleting a Cluster 220
8.2.7 Saving the Configuration 221
8.3 Managing NTA Devices 221
8.3.1 Adding an NTA Device 222
8.3.2 Modifying NTA Device Settings 223
8.3.3 Deleting an NTA Device 223
8.3.4 Modifying Access Accounts in Batches 223
8.3.5 Configuring an NTA Device 223
9 Console-based System Management 224
9.1 Overview 224
9.2 Login to the Console 224

9.3 Console Configuration 224
9.3.1 Checking System Status 225
9.3.2 Configuring Network Settings 225
9.3.3 Setting System Time 230
9.3.4 Setting the System Time Zone 231
9.3.5 Setting the System Language 231
9.3.6 Changing the Console Password 231
9.3.7 Resetting the Web Administrator's Password 232
9.3.8 Restoring Factory Settings 232
9.3.9 Restoring the Database 233
9.3.10 Setting the Web Service Port 233
9.3.11 Restarting System Services 233
9.3.12 Rebooting the System 233
9.3.13 Shutting Down the System 233
9.3.14 Exiting the System 234
A Parameters 235
A.1 Anti-DDoS Policy 235
A.2 UDP Policy Parameters 235
A.3 Diversion Filtering Rules 236
B Default Parameters 237
B.1 Default Parameters of the Communication Interface 237
B.2 Default Account of the Web Administrator 237
B.3 Default Account of the Console Administrator 237
B.4 Communication Parameters of the Console Port 237
B.5 Default Account of the Web Administrator 238

Figures

Figure 2-1 Security alert page 4
Figure 2-2 Login page of the web-based manager 5
Figure 2-3 Homepage 6
Figure 2-4 Layout of the web-based manager 7
Figure 2-5 Language options 8
Figure 2-6 Password resetting page 8
Figure 3-1 Basic system information 9
Figure 3-2 Exporting configurations 11
Figure 3-3 Upload Configuration File dialog box 11
Figure 3-4 License page 12
Figure 3-5 System Upgrade page 14
Figure 3-6 Selecting an upgrade file 14
Figure 3-7 Upgrade confirmation 15
Figure 3-8 Data Storage page 16
Figure 3-9 Modifying the backup configuration 17
Figure 3-10 IPv4 network configuration page 18
Figure 3-11 Configuring an interface in IPv4 mode 19
Figure 3-12 Front panel of ADS NX3-M1600E 19
Figure 3-13 ADS NX3-M1600E – IPv4 address configuration 20
Figure 3-14 ADS NX3-M1600E – Configuring an interface in IPv4 mode 21
Figure 3-15 IPv6 network configuration page 22
Figure 3-16 Configuring an interface in IPv6 mode 22
Figure 3-17 IPv6 address configuration 23
Figure 3-18 Configuring an interface in IPv6 mode 23
Figure 3-19 DNS Server page 24
Figure 3-20 Topology for HA 25
Figure 3-21 HA Configuration page 26

Figure 3-22 Performance Alert Configuration page 28
Figure 3-23 User Management page 29
Figure 3-24 Creating a user 30
Figure 3-25 Security settings 32
Figure 3-26 Authentication Configuration page 34
Figure 3-27 Configuring the Radius server 35
Figure 3-28 Audit logs 36
Figure 3-29 SNMP configuration 37
Figure 3-30 Adding an SNMP client 38
Figure 3-31 Syslog configuration 39
Figure 3-32 Adding a syslog server 39
Figure 3-33 Data export 40
Figure 3-34 Adding a data server 41
Figure 3-35 Mail alert settings 42
Figure 3-36 SMTP server configuration 43
Figure 3-37 Debug information collection 44
Figure 4-1 Overview page 47
Figure 4-2 Adding a panel 48
Figure 4-3 New panel displayed 49
Figure 4-4 Reversed panel 50
Figure 4-5 Specifying another panel to display 50
Figure 4-6 New panel displayed 51
Figure 4-7 Reversed panel 52
Figure 4-8 System status bar 53
Figure 4-9 Detailed system status information 53
Figure 4-10 Sound alert 54
Figure 4-11 Attack Traffic Trend panel 54
Figure 4-12 Detailed traffic information at a specific point of time 55
Figure 4-13 Searching for an object 56
Figure 4-14 Real-time traffic trends of a specified object 56
Figure 4-15 Switching the traffic unit 57
Figure 4-16 Protocols Analysis panel 58
Figure 4-17 Traffic of different protocols at a specific point of time 58

Figure 4-18 Searching for an object 59
Figure 4-19 Real-time traffic trends of a specified object 60
Figure 4-20 Switching the display mode 60
Figure 4-21 Display of traffic data in an area graph and pie chart 61
Figure 4-22 Display of traffic data in a pie chart 62
Figure 4-23 Percentage of protocol-specific traffic 62
Figure 4-24 Area representing traffic of a protocol separated from other areas 63
Figure 4-25 Switching the traffic unit 63
Figure 4-26 Top Destination IP panel 64
Figure 4-27 Display of the country name 65
Figure 4-28 Percentage of dropped traffic to incoming traffic 66
Figure 4-29 Traffic of a specific IP address 67
Figure 4-30 Searching for objects containing the current IP address 67
Figure 4-31 Viewing traffic information of a specified object 68
Figure 4-32 Searching for an object 69
Figure 4-33 Top destination IP addresses associated with a specified object 69
Figure 4-34 Top Region Attack Traffic panel 70
Figure 4-35 Traffic of a specific region 71
Figure 4-36 Percentage of dropped traffic for a specific region 71
Figure 4-37 Top Source Countries panel 72
Figure 4-38 Display of the value of attack traffic from a country 73
Figure 4-39 Switching the display mode 73
Figure 4-40 Display of traffic data in both a map and a list 74
Figure 4-41 Display of traffic data only in a list 74
Figure 4-42 Percentage of dropped traffic of a source country 75
Figure 4-43 Searching for a specific object 76
Figure 4-44 Traffic of top source countries associated with a specific object 76
Figure 4-45 Attack traffic 77
Figure 4-46 Traffic at a specific point of time 78
Figure 4-47 Searching for an object 79
Figure 4-48 Attack traffic trend of a specified object 80
Figure 4-49 Top alerts reported by NTA 81
Figure 4-50 More details about alerts generated by NTA 81

Figure 4-51 Start time of an alert reported by NTA 82
Figure 4-52 Top alerts reported by NTA in terms of smallest traffic 83
Figure 4-53 Top ongoing attack events 84
Figure 4-54 Start time of an ongoing attack event 85
Figure 4-55 Top ongoing attack events by total minimum dropped traffic 85
Figure 4-56 Percentage of forwarded traffic in an ongoing attack event 86
Figure 4-57 Attack traffic targeting an IP address 87
Figure 4-58 Searching for an IP address object 88
Figure 4-59 Attack event information of an IP address 89
Figure 4-60 Top 10 source IP addresses 90
Figure 4-61 Display of the country name 91
Figure 4-62 Percentage of dropped traffic of a source IP address 92
Figure 4-63 Searching for an object 93
Figure 4-64 Traffic of top 10 source IP addresses associated with a specific object 93
Figure 4-65 Area representing traffic of an attack type separated from other areas 94
Figure 4-66 Percentage of traffic of an attack type 95
Figure 4-67 Separating the area of an attack type from other areas 96
Figure 4-68 Searching for an object 97
Figure 4-69 Attack type distribution of a specified object 97
Figure 4-70 Device monitoring information 98
Figure 4-71 More details about the monitored devices 98
Figure 4-72 License expiration reminder 99
Figure 4-73 Device monitoring information in full screen mode 100
Figure 4-74 Top NTA Region Traffic panel 101
Figure 4-75 Traffic of a specific region 101
Figure 4-76 NTA Traffic Trend panel 102
Figure 4-77 Detailed traffic information at a specific point of time 103
Figure 4-78 Searching for an object 103
Figure 4-79 Real-time traffic trends of a specified object 104
Figure 4-80 Switching the traffic unit 104
Figure 4-81 Attack traffic information of all objects 106
Figure 4-82 Real-time traffic trend graph of a specified object 107
Figure 4-83 Real-time attack traffic trend graph of all objects 108

Figure 4-84 DDoS attack traffic information at a specific time 109
Figure 4-85 Finer-granularity traffic information 109
Figure 4-86 Traffic information of a specific region 110
Figure 4-87 Summary of real-time attack traffic monitoring 111
Figure 4-88 Searching for information associated with an IP address 111
Figure 4-89 Real-time traffic monitoring of an IP address 112
Figure 4-90 Traffic Monitoring page 113
Figure 4-91 Device-specific traffic information 114
Figure 4-92 Searching for a traffic monitoring object 115
Figure 4-93 Traffic information of a specified object 116
Figure 4-94 Searching for a traffic monitoring object 117
Figure 4-95 Attack traffic information of an IP address in the default protection group 118
Figure 4-96 Historical attack traffic – objects 119
Figure 4-97 Historical attack traffic – summary 120
Figure 4-98 Adding a filter 121
Figure 4-99 Viewing a filter 122
Figure 4-100 Deleting a filter 123
Figure 4-101 Default panels on the DDOS Attack Traffic Monitoring page 124
Figure 4-102 Network traffic information of all objects 125
Figure 4-103 Real-time network traffic trend graph of a specified object 126
Figure 4-104 Real-time network traffic trend graph of all objects 127
Figure 4-105 Network traffic information at a specific time 128
Figure 4-106 Finer-granularity network traffic information 128
Figure 4-107 Network traffic of a specific region 129
Figure 4-108 Associated region information displayed 129
Figure 4-109 Summary of network traffic monitoring information 130
Figure 4-110 Device-specific network traffic information 131
Figure 4-111 Region-specific network traffic information 132
Figure 4-112 IP group-specific network traffic information 132
Figure 4-113 Searching for a network traffic monitoring object 133
Figure 4-114 Object-specific network traffic information 134
Figure 4-115 Historical network traffic – objects 135
Figure 4-116 Historical network traffic – summary 136

Figure 4-117 Creating a filter 137
Figure 4-118 Filtered network traffic information 138
Figure 4-119 Deleting a filter 138
Figure 4-120 Default panels displayed on the NET Traffic Monitoring page 139
Figure 4-121 Attack Events page – Attack Types panel 140
Figure 4-122 Attack traffic information of a specific time 141
Figure 4-123 Finer-granularity traffic monitoring information 141
Figure 4-124 Attack traffic – attack events 142
Figure 4-125 Region-specific attack events 143
Figure 4-126 Device-specific attack events 144
Figure 4-127 Searching for attack event objects 145
Figure 4-128 Object-specific attack event information 146
Figure 4-129 Searching for attack event objects 147
Figure 4-130 Attack event information of an IP address in the default protection group 148
Figure 4-131 Historical attack traffic trend 149
Figure 4-132 Customization of the attack traffic trend graph 149
Figure 4-133 Creating a filter 151
Figure 4-134 Viewing a filter 152
Figure 4-135 Deleting a filter 153
Figure 4-136 Default panels on the Attack Events page 154
Figure 5-1 Network Traffic Report page 155
Figure 5-2 Editing a report 156
Figure 5-3 Custom Report page 157
Figure 5-4 Creating a custom report 158
Figure 5-5 Editing a custom report 159
Figure 5-6 Email Report Sending Schedule page 160
Figure 5-7 Creating an email report sending schedule 161
Figure 5-8 Custom Logo page 162
Figure 6-1 Attack summary logs 165
Figure 6-2 Login logs 166
Figure 6-3 Operation logs 167
Figure 6-4 Link status logs 167
Figure 6-5 Diversion logs 168

Figure 6-6 Performance logs 169
Figure 6-7 Performance alert logs 170
Figure 6-8 HA logs 171
Figure 6-9 Traffic alert logs 172
Figure 6-10 Alert summary 173
Figure 6-11 Cloud Authentication Logs page 174
Figure 7-1 Region list 175
Figure 7-2 Group label management page 175
Figure 7-3 Creating a group label 176
Figure 7-4 List of region managers 177
Figure 7-5 Creating a region manager 178
Figure 7-6 Configuring permissions of a region manager 179
Figure 7-7 Configuring basic information of a region 180
Figure 7-8 Configuring region traffic alert parameters 182
Figure 7-9 Configuring region DDoS alert parameters 183
Figure 7-10 Configuring traffic diversion rules 184
Figure 7-11 Configuring the Portal 185
Figure 7-12 Details of a region 186
Figure 7-13 Adding an IP group in NTA detection mode 188
Figure 7-14 Configuring IP group traffic alert parameters 189
Figure 7-15 Configuring IP group DDoS alert parameters 189
Figure 7-16 Configuring IP group traffic diversion rules 190
Figure 7-17 Configuring IP group protection policies 192
Figure 7-18 Configuring a URL rule 192
Figure 7-19 Adding a URL rule 193
Figure 7-20 Adding an IP group in "None" detection mode 194
Figure 7-21 Configuring IP group protection policies in "None" detection mode 194
Figure 7-22 Configuring URL rules in "None" detection mode 195
Figure 7-23 Region traffic diversion 196
Figure 7-24 Viewing the region under traffic diversion 197
Figure 7-25 Searching for IP addresses whose traffic can be diverted 197
Figure 7-26 Anti-DDoS policy template 198
Figure 8-1 ADS Device page 200

Figure 8-2 ADS devices 201
Figure 8-3 Adding an ADS device 201
Figure 8-4 Modifying access accounts in batches 203
Figure 8-5 Modifying access accounts 204
Figure 8-6 Adding an ADS cluster 206
Figure 8-7 Configuring an ADS cluster 208
Figure 8-8 Blacklist Configuration page 208
Figure 8-9 Blacklist configuration 209
Figure 8-10 Adding a blacklist 209
Figure 8-11 Viewing blacklist entries 210
Figure 8-12 Blacklist import result 211
Figure 8-13 Querying a blacklist entry 211
Figure 8-14 Query result 212
Figure 8-15 Manual Packet Capture area 213
Figure 8-16 Creating a manual packet capture task 213
Figure 8-17 Automatic Packet Capture area 216
Figure 8-18 Creating an automatic packet capture task 216
Figure 8-19 Packet capture files 218
Figure 8-20 Adding an device to the cluster 219
Figure 8-21 Modifying an ADS cluster 220
Figure 8-22 NTA Device page 221
Figure 8-23 Adding an NTA device 222
Figure 9-1 Main menu of the console 224
Figure 9-2 Checking system status 225
Figure 9-3 Network setting menu 225
Figure 9-4 Viewing network settings 226
Figure 9-5 Adding an IP address 227
Figure 9-6 Deleting an IP address 227
Figure 9-7 Adding a default gateway 228
Figure 9-8 Adding a route 229
Figure 9-9 Deleting a route 229
Figure 9-10 Configuring the DNS server 230
Figure 9-11 Restoring default network settings 230

Figure 9-12 Console management – Setting system time 230
Figure 9-13 Console management – setting system time zone..... 231
Figure 9-14 Console management – Setting system language 231
Figure 9-15 Console management – changing console password 231
Figure 9-16 Console management – resetting the administrator's password..... 232
Figure 9-17 Restoring factory settings 232

Tables

Table 2-1 Webpage layout 7
Table 3-1 Basic system information 9
Table 3-2 License parameters 12
Table 3-3 Parameters for configuring an interface in IPv4 mode 19
Table 3-4 Front panel of ADS NX3-M1600E 20
Table 3-5 Parameters for configuring an interface in IPv4 mode 21
Table 3-6 Parameters for configuring an interface in IPv6 mode 22
Table 3-7 Parameters for configuring an interface in IPv6 mode 23
Table 3-8 HA parameters 26
Table 3-9 ADS M user groups and their respective privileges 29
Table 3-10 Parameters for creating a user 30
Table 3-11 Parameters of security settings 33
Table 3-12 Parameters for configuring the Radius server 35
Table 3-13 Audit log parameters 36
Table 3-14 Parameters for configuring an SNMP server 37
Table 3-15 Parameters for configuring an SNMP client 38
Table 3-16 Syslog server parameters 40
Table 3-17 Parameters for adding a data server 41
Table 3-18 Parameters for configuring an SMTP server 43
Table 4-1 Monitoring information displayed on the Overview page 45
Table 4-2 Mappings between attack types and curve colors 78
Table 4-3 Mappings between attack types and colors 94
Table 4-4 Real-time attack traffic trend – parameters on the Objects tab page 106
Table 4-5 Real-time traffic trend – parameters on the Summary tab page 110
Table 4-6 Historical attack traffic trend – parameters on the Objects tab page 119
Table 4-7 Real-time network traffic trend – parameters on the Objects tab page 125
Table 4-8 Real-time network traffic trend – parameters on the Summary tab page 130

Table 4-9 Historical network traffic trend – parameters on the Objects tab page 135
Table 4-10 Attack type parameters 140
Table 4-11 Attack event parameters 142
Table 5-1 Parameters for configuring an email report sending schedule 161
Table 6-1 Parameters of attack summary logs 165
Table 6-2 Parameters of login logs 166
Table 6-3 Parameters of performance alert logs 170
Table 6-4 Parameters of HA logs 171
Table 6-5 Parameters of traffic alert logs 172
Table 6-6 Parameters for querying cloud authentication logs 174
Table 7-1 Parameters for creating a group label 176
Table 7-2 Parameters for creating a region manager 178
Table 7-3 Parameters for configuring permissions of a region manager 179
Table 7-4 Parameters for configuring basic information 180
Table 7-5 Region traffic alert parameters 182
Table 7-6 Parameters for configuring traffic diversion rules 184
Table 7-7 Parameters for configuring the Portal 185
Table 7-8 Parameters for configuring basic information of an IP group 188
Table 7-9 Parameters for configuring diversion rules for an IP group 190
Table 7-10 URL rule parameters 193
Table 8-1 Parameters of an ADS device 202
Table 8-2 ADS cluster parameters 206
Table 8-3 Parameters for creating a manual packet capture task 214
Table 8-4 Parameters for creating an automatic packet capture task 217
Table 8-5 NTA device parameters 222

Preface

Scope

This document describes all functions and usage of ADS NX3-M 600A/1600A/1600E (ADS M) in detail. It provides guidance in use of ADS M products. Descriptions here may slightly differ from actual products due to version upgrade or other reasons.

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 protocols
- Network security

Organization

Chapter	Overview
1 Overview	Describes ADS M briefly.
2 Web-based Manager	Describes the login method and layout of the web-based manager.
3 Web-based System Management	Describes how to perform system management and maintenance.
4 Traffic Monitoring	Describes in detail the traffic and attacks monitored by the managed devices.
5 Reports	Describes various types of reports and how to query these reports.
6 Logs	Describes how to view device logs.
7 Region Management	Describes how to configure device regions and region IP groups.
8 Device Management	Describes device management, policy configuration, and abnormal traffic detection.
9 Console-based System Management	Describes menus of the console management interface.

Chapter	Overview
A Parameters	Describes parameters of policy templates.
B Default Parameters	Introduces default settings of ADS M.

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.
	Reminds users to take note.
	Indicates a tip to make your operations easier.
	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Customer Support

Email: support@nsfocusglobal.com

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

Contacts:

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

1 Overview

ADS M is used to perform centralized management over ADS devices deployed in cluster mode and to generate reports. ADS M monitors traffic and operating status of multiple ADS devices, collects traffic information and attack alerts from these devices, and displays the collected information on the web-based manager. On the web-based manager, the administrator, in a unified way, can modify configuration files of ADS devices on ADS M and then dispatch these files to ADS devices.

2 Web-based Manager

2.1 Login

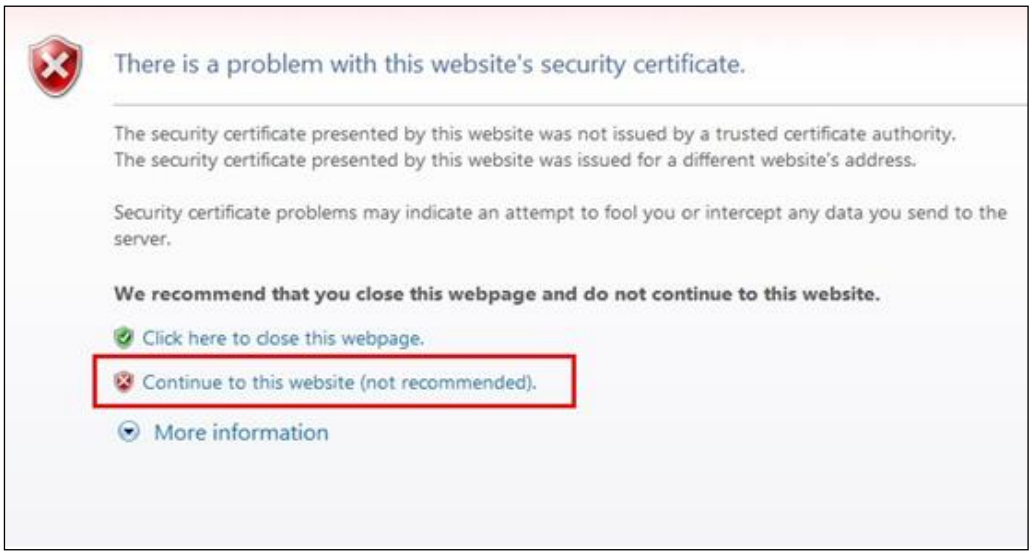
To log in to the web-based manager of ADS M, follow these steps:

Step 1 Make sure that your PC properly communicates with ADS M.

Step 2 Open a browser (for example, Microsoft Internet Explorer) and connect to the IP address of the management interface of ADS M over HTTPS, for example, type **https://192.168.1.100** in the address bar.

A security alert page appears, as shown in Figure 2-1.

Figure 2-1 Security alert page



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

The login page of the web-based manager appears, as shown in Figure 2-2.

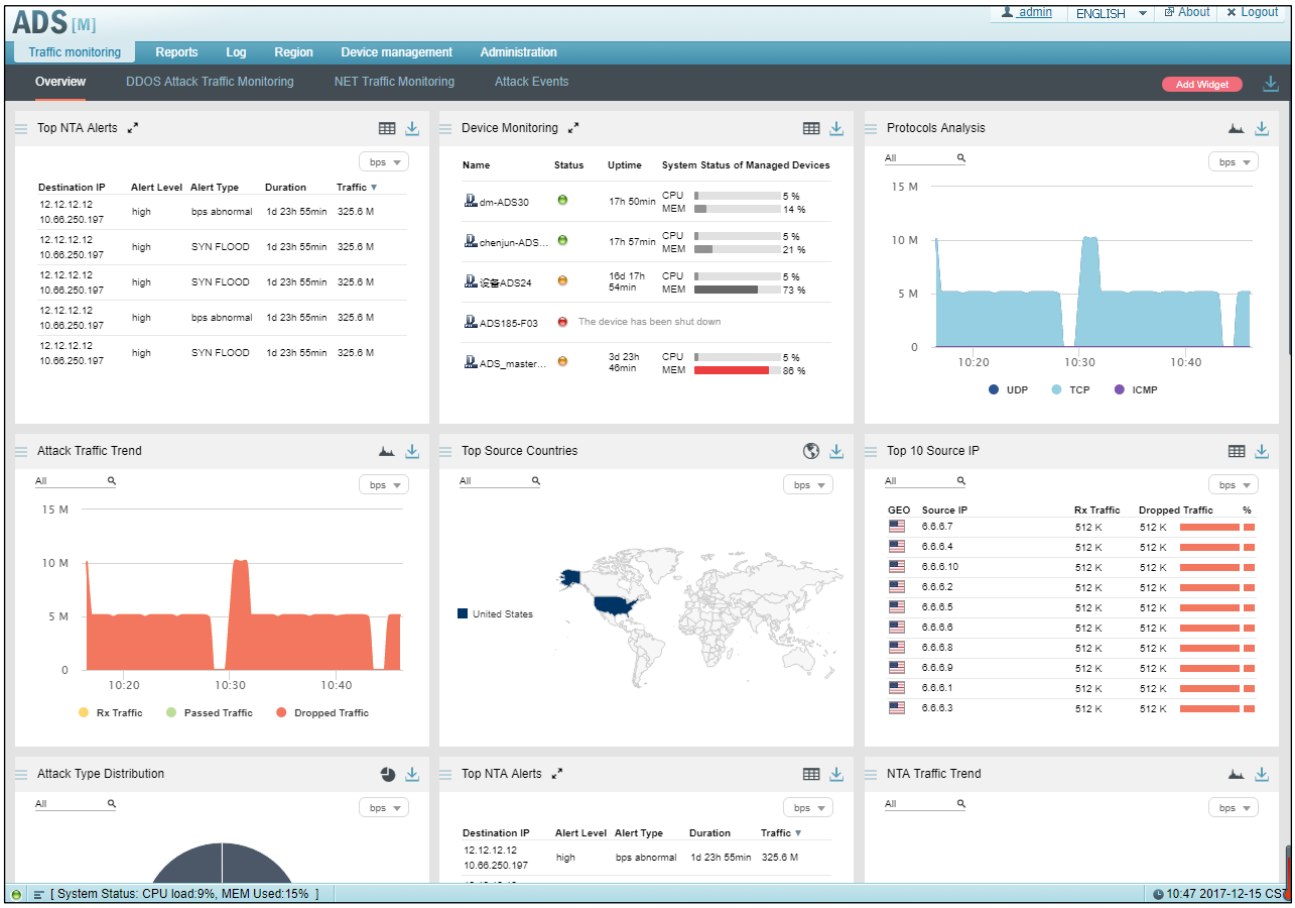
Figure 2-2 Login page of the web-based manager

Step 4 Type the correct user name and password and then click **Login** or press **Enter** to log in to the web-based manager.

Note	During the first login to ADS M that has just been upgraded to V4.5R90F00, the configuration wizard appears. You can log in to the system only after you set the locality, system time zone, and system time, but do not need to change the initial password. For details, see *NSFOCUS ADS M Installation Guide*. During the first login to the web-based manager with the initial user name and password, the configuration wizard appears only after you change the initial password.

For the first login, you must import a valid license before using the system. After a successful login, the web-based manager appears, as shown in Figure 2-3.

Figure 2-3 Homepage



----End

Caution	• The browser you use must support JavaScript, cookies, and frames. • You are advised to use Internet Explorer 11 or later, Chrome, or Firefox and set the display resolution to 1280 x 700 or higher. If you use the IE-based tabbed browsers (such as MyIE and Maxthon), pages may be displayed improperly. • You must change the password immediately after the first login. • The system will return to the login page if you remain inactive on a page other than the three tab pages of the **Traffic monitoring** module for over 10 minutes after successful login. The system does not automatically log you out of a tab page under **Traffic module** no matter how long you stay inactive on this page. • For the first login, you must import a valid license before using the system. For details, see section 3.1.2 License Management.

2.2 Layout

Figure 2-4 shows the layout of the web-based manager.

Figure 2-4 Layout of the web-based manager

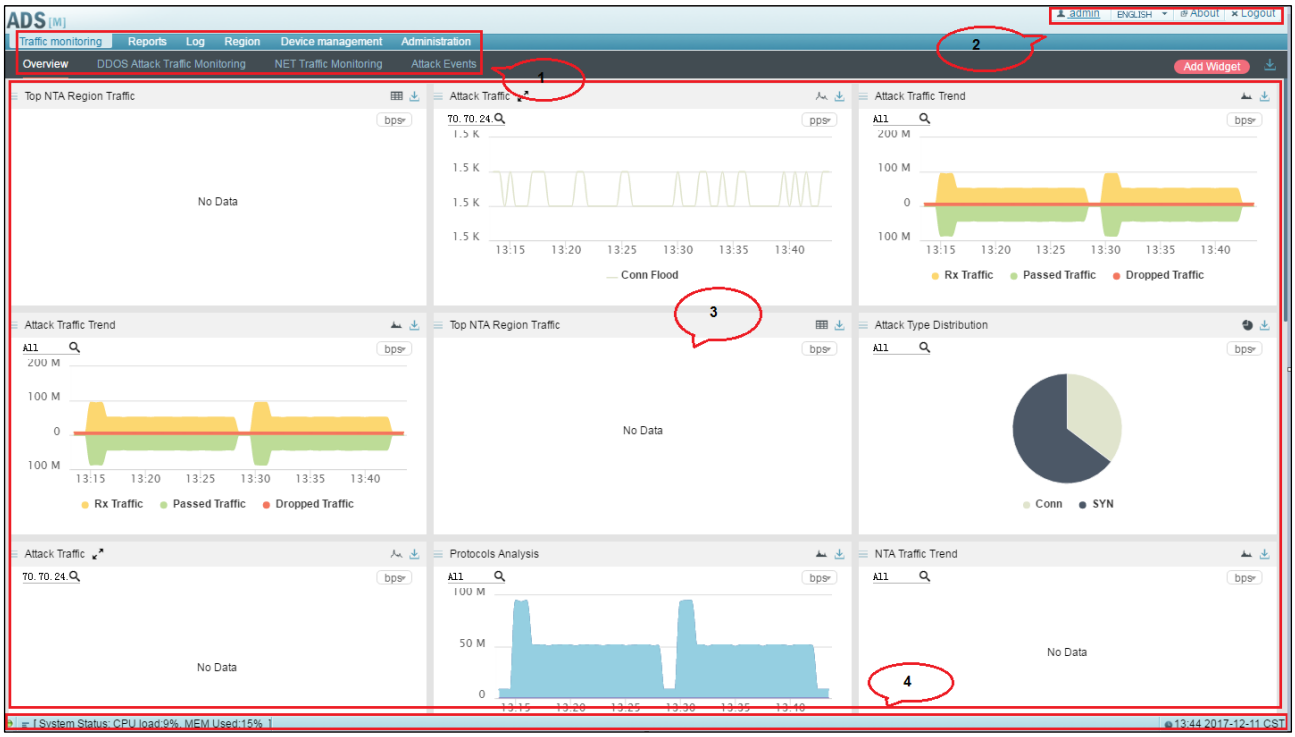


Table 2-1 describes areas of the web-based manager.

Table 2-1 Webpage layout

No.	Area	Description
1	Menu bar	Main menus of the system.
2	Quick access bar	Provides buttons for common operations on the web-based manager. • admin : enables you to modify your information. See section 3.2.1 User Management for details. • ENGLISH : switches between languages. See section 3.1.1 Basic Settings for details. • About : displays product information of ADS M devices. • Logout : logs you out of the system.
3	Work area	Area where you can perform configurations and operations and view data.
4	Status bar	Displays current system time, CPU usage, memory usage, and data partition usage.

2.3 Other Operations

On the web-based manager, you can also switch the language and reset the password.

Switching the Language

On the login page shown in Figure 2-2, move the cursor to the **Language** button in the lower-right corner. Then all languages available are automatically displayed, as shown in Figure 2-5. Click the desired language. The interface language is now changed to the one that you selected.

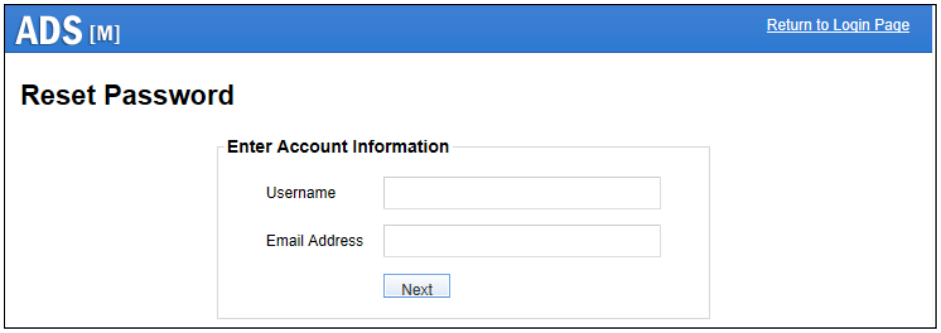
Figure 2-5 Language options

Resetting the Password

On the login page shown in Figure 2-2, click **Forgot Password** in the lower-right corner. On the **Reset Password** page shown in Figure 2-6, type the correct user name and email address, and then click **Next**. After that, the system automatically sends a link for resetting the password to your registered email address.

Note	• Only the user **admin** can enable the password resetting function. In addition, the login page displays **Forgot Password** only after you enable **Reset Password** on the **Security Settings** page. For how to enable password resetting, see section 3.2.2 Security Settings. • When you reset the password, you must type the same email address as the one that you used to register. This email address must be a valid one; otherwise, you would not receive the password resetting email. • The password resetting function also requires a Simple Mail Transfer Protocol (SMTP) server. For details, see section 3.3.5 SMTP Server Configuration.

Figure 2-6 Password resetting page



3 Web-based System Management

This chapter describes routine management and maintenance of ADS M via the web-based manager.

3.1 Local Settings

This section describes basic configuration of ADS M, including basic system parameters, license management, system upgrade, data storage, network configuration, DNS server configuration, HA configuration, and running alert configuration.

3.1.1 Basic Settings

As shown in Figure 3-1, the **Basic Settings** page displays basic system information. You can click to edit the device ID, system time, NTP server, and default system language, except system ID that identifies the system uniquely.

Figure 3-1 Basic system information

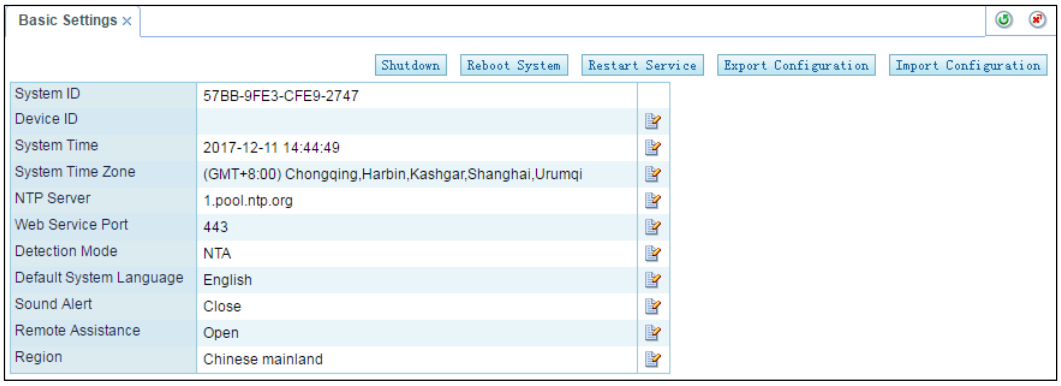


Table 3-1 describes detailed system information.

Table 3-1 Basic system information

Parameter	Description
System ID	Hardware ID of ADS M.

Parameter	Description
Device ID	Name of ADS M.
System Time	Current system time, in the format of 2012-09-27 17:07:07. Changing the system time may cause a loss of certain data. Therefore, you must perform this operation with caution.
System Time Zone	Time zone of the system time. When daylight saving time (DST) is used, the page will prompts a message, indicating that the clock is automatically adjusted based on the DST.
NTP Server	IP address of the server with which ADS M synchronizes time.
Web Service Port	Port via which you log in to the web-based manager of ADS M. The port number can be **80**, **443**, or any integer from 10000 to 65534. Assume that the IP address of ADS M is https://192.168.1.100. If the port number is changed to **80**, you need to type **https://192.168.1.100:80** in the address bar of the browser. Note Changing the web service port will cause the web-based manager of ADS M to restart. If the Portal is enabled, you also need to re-deploy the Portal.
Detection Mode	Detection mode adopted by the system. The default value is **NTA**, indicating that ADS M coordinates with NTA for traffic analysis. If there is no NTA, the default value is **None**, indicating that NTA coordination is unavailable.
Default System Language	Default language used by the system to save audit logs. The web-based manager supports both **Chinese** and **English**. The default language is **English**. The new default language takes effect only after the system is restarted.
Sound Alert	Controls whether to enable sound alerting. After sound alerting is enabled, the system makes a sound and displays an alert reminder box when either of the following conditions is met: • An attack alert or link status alert is generated by ADS. • A traffic alert is generated by NTA. For details about the sound alerting function, see section 4.1.6 Generating Sound Alerts.
Remote Assistance	By default, remote assistance is disabled. Selecting **Open** allows NSFOCUS technical personnel to log in to the system in the background for remote assistance. Selecting **Close** disables this function. SSH is used for remote login, running on port 50022.

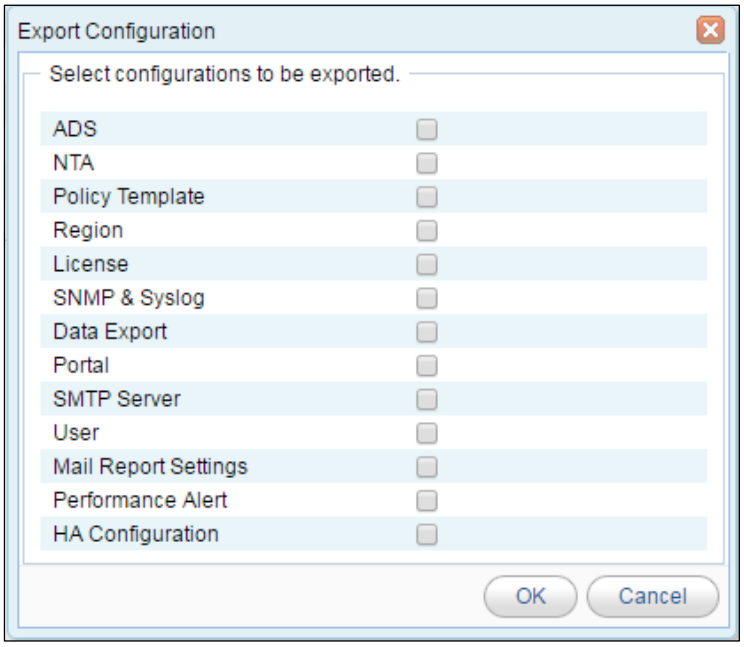
In addition to adjusting basic system parameters, you can also perform the following operations:

- Shut down the system: Click **Shutdown** to shut down ADS M.
- Reboot the system: Click **Reboot System** to reboot ADS M.

- Restart system services: Click **Restart Services** to restart system service programs (including the web-based manager and engine) of ADS M. For example, after you change the default language, the system asks you to restart system services.
- Export configuration files

  Click **Export Configuration** and select configuration items to be exported in the **Export Configuration** dialog box shown in Figure 3-2. Click **OK** to save the configuration file to the target path.

Figure 3-2 Exporting configurations

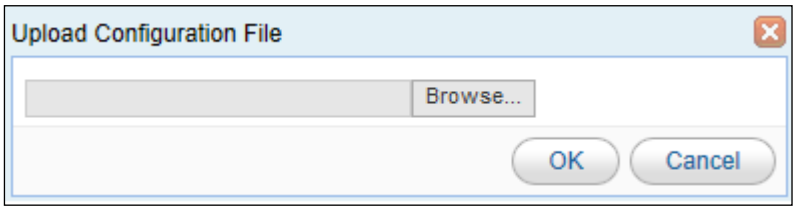


Note	The configuration files will be exported as an encrypted package which is not editable and can be used for backup or imported to the device.

- Import a configuration file

  Click **Import Configuration** and upload a file in the **Upload Configuration File** dialog box shown in Figure 3-3 to overwrite the original configuration file. This operation reconfigures ADS devices, NTA devices, and policy templates.

Figure 3-3 Upload Configuration File dialog box



Note	• The imported configuration file takes effect only after the system restarts. • Certificates may be necessary to perform certain configurations. As different devices have different certificates, ensure that proper certificates are used. • The imported configuration file will overwrite the original one. Please perform this operation with caution.

3.1.2 License Management

After an ADS M device is installed, you need to import a license before using it. On the **License** page, click **Browse** to select a license file and then click **Update** to import a license. After it is imported, the **License** page displays the license information, as shown in Figure 3-4.

Figure 3-4 License page

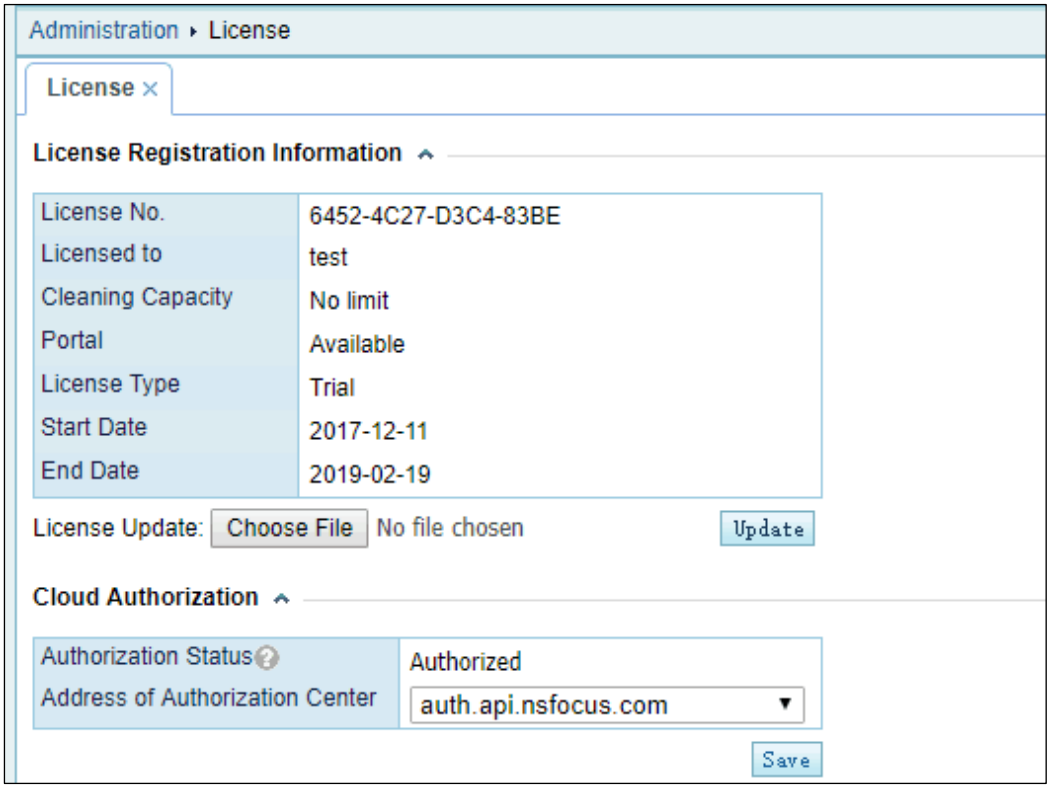


Table 3-2 describes license parameters.

Table 3-2 License parameters

Parameter	Description
License No.	License number of the current ADS M.
Licensed to	Customer that is authorized to use this system.
Cleaning Capacity	Maximum bandwidth allowed for traffic cleaning. **No limit** indicates no limit to the maximum bandwidth.

Parameter	Description
	Note This parameter is available only for an ADS M virtual machine.
Number of Monitored Devices	Maximum number of ADS devices that can be monitored by the current ADS M.
Portal	Whether ADS Portal is available.
License Type	License type, which may be **Trial** or **Paid**.
Start Date	Sart date of the license validity, which is usually the production date of the current license.
End Date	End date of the license validity. If a trial license expires, ADS M can be upgraded but no longer collects data of ADS devices under it. That is, ADS M loses the protection function. If a paid license expires, ADS M still works but cannot be upgraded.
Authorization Status	Note The cloud authentication function is available only for an ADS M virtual machine. Meanwhile, an ADS M virtual machine can be used only after it is connected to the cloud authentication center. After you configure the address of the cloud authorization center, the virtual machine automatically sends authentication requests to the cloud once started. • If the address is correct and connection is established, the status is **Authorized**. • If you enter a wrong authorization center address when the authorization status is **Authorized**, the authorization status changes to **Offline**, and you can still use the web-based manager for the time being. • If the cloud authorization center remains **Offline** for more than 7 days, the status changes to **Unauthorized**, and you cannot use the web-based manager. During its operation, the virtual machine periodically sends authentication requests to the cloud. Therefore, the virtual machine must remain connected to the cloud.
Address of Authorization Center	URL of the cloud authorization server. • For use on the Chinese mainland, choose **auth.api.nsfocus.com**. • For use in other countries and regions, choose **auth.nsfocusglobal.com**.

Note	Once the license expires, please update it or contact NSFOCUS technical support for a new license.

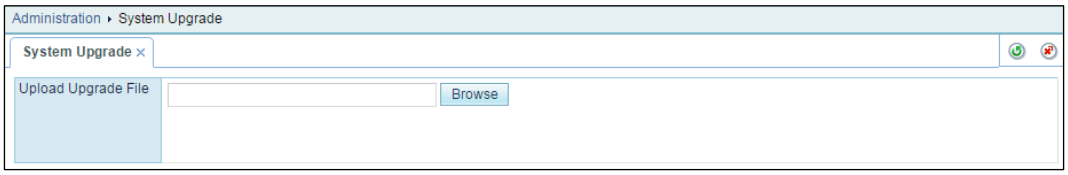
3.1.3 System Upgrade

To upgrade ADS M, follow these steps:

Step 1 Contact NSFOCUS technical support for an applicable upgrade packages of ADS M.

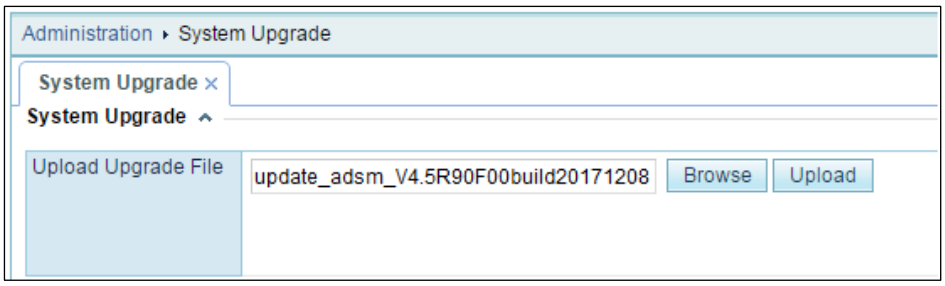
Step 2 Choose **Administration > System Upgrade**.

Figure 3-5 System Upgrade page



Step 3 Click **Browse** to select an upgrade package file.

Figure 3-6 Selecting an upgrade file



Step 4 Click **Upload**.

After the upgrade package is uploaded, the system displays update-related information for you to confirm.

Figure 3-7 Upgrade confirmation

Step 5 Click **Confirm Upgrade**.

Then the upgrade proceeds. During the upgrade, the system displays a progress bar, indicating how much of the task has been completed.

Step 6 After the upgrade is complete, click **OK** in the dialog box, which prompts that the system service will be rebooted.

If the system does not prompt the upgrade success, wait about 3 minutes and then the system will automatically restart.

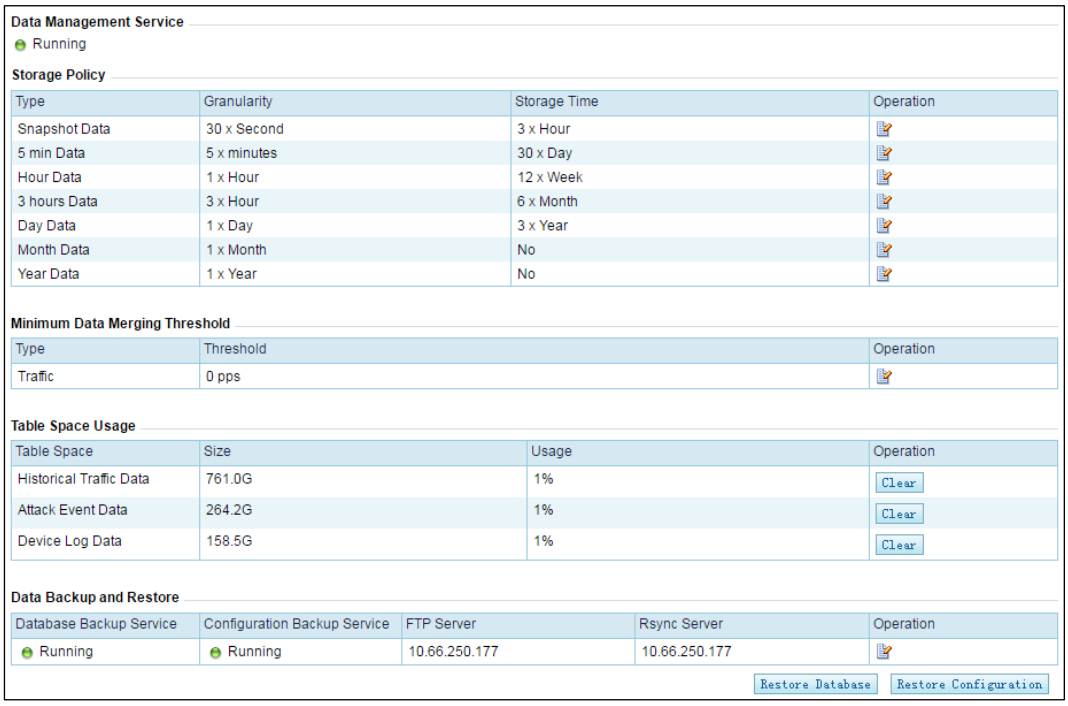
Step 7 Click in the **Operation** column of the upgrade package in the **Upgrade History** list to view information about the new version.

----End

3.1.4 Data Storage

Choose **Administration** > **Local Settings** > **Data Storage** to open the **Data Storage** page.

Figure 3-8 Data Storage page



You can perform the following operations on the **Data Storage** page:

- View the data management service status.

  In the **Data Management Service** area, you can check whether the data management service is running or has stopped running.

- Edit data storage policies.

  In the **Storage Policy** area, click in the **Operation** column to edit the storage period of the corresponding data type.

Caution	If the storage time is 0, it indicates that there is no limit to the data storage time. In addition, the system automatically clears out-of-date data.

- Edit the minimum data merging threshold.

  In the **Minimum Data Merging Threshold** area, click in the **Operation** column to edit the minimum data merging threshold.

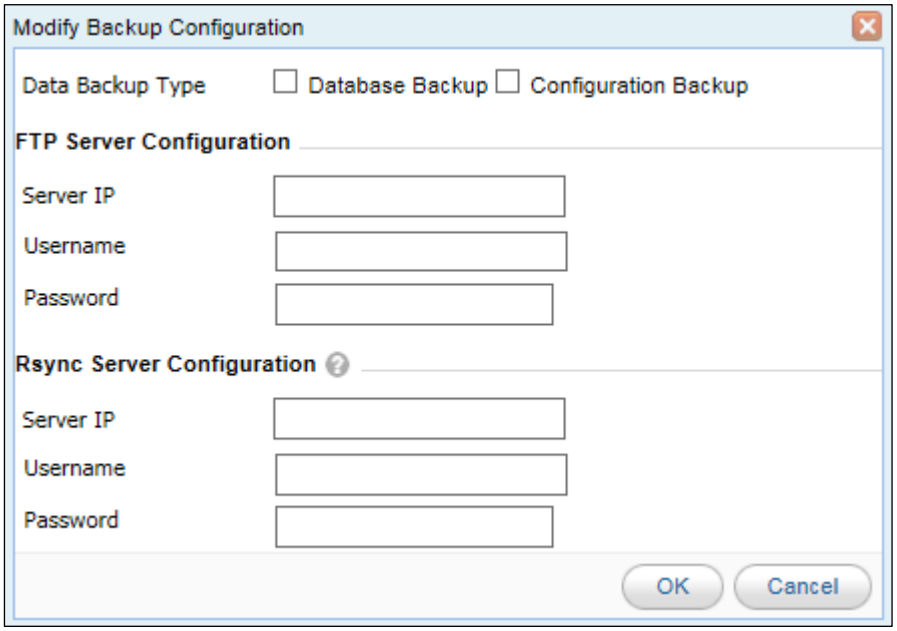
- View the table space usage.

  In the **Table Space Usage** area, you can view the space used by historical traffic data, attack event data, and device log data as well as the related percentage of usage.

- Manage data backup and restoration.
  - Modify the backup configuration.

In the **Data Backup and Restore** area, click in the **Operation** column to edit the backup configuration in the dialog box shown in Figure 3-9.

Figure 3-9 Modifying the backup configuration



Select the data backup type and configure parameters of the FTP server and Rsync server.

Note	For **Data Backup Type**, if only **Configuration Backup** is selected, you need to configure the Rsync server; if only **Database Backup** is selected, you need to configure both the FTP server and the Rsync server.

- Restore the database.

  In the **Data Backup and Restore** area, click **Restore Database** below the table to restore the database information backed up on the server to the ADS M device.
- Apply the backup file for restoration.

  In the **Data Backup and Restore** area, click **Restore Configuration** below the table to restore the configuration files backed up on the server to the ADS M device. The ADS M configuration is backed up to the server at 23:50 each day.

3.1.5 Network Configuration

ADS M supports both IPv4 and IPv6 protocols. The following sections describe how to configure IPv4 and IPv6 network settings respectively.

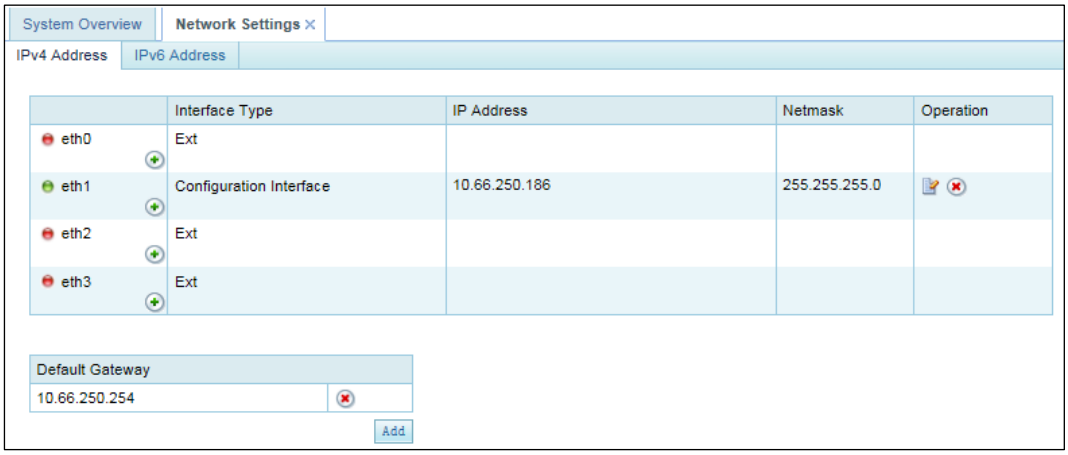
3.1.5.1 Configuring IPv4 Network Settings

ADS NX3-M600A/M1600A

ADS M provides multiple interfaces, as shown in Figure 3-10. eth1 acts as a management interface of ADS M. It is used to configure the IP address, subnet mask, and default network gateway of ADS M. Other interfaces are expansion interfaces. indicates that interfaces are connected to the network. indicates that interfaces are disconnected from the network. Each interface can be configured with two IP addresses. Initially, default parameters are displayed. You need to configure the IP address and subnet mask for the network adapter. To unbind the IP address from an interface, click in the **Operation** column.

Caution	If the IP address of a management interface is deleted, you may be denied access to the web-based manager of ADS M.

Figure 3-10 IPv4 network configuration page



On the interface list shown in Figure 3-10, click next to an interface to configure the IP address and other parameters for this interface, as shown in Figure 3-11.

Figure 3-11 Configuring an interface in IPv4 mode

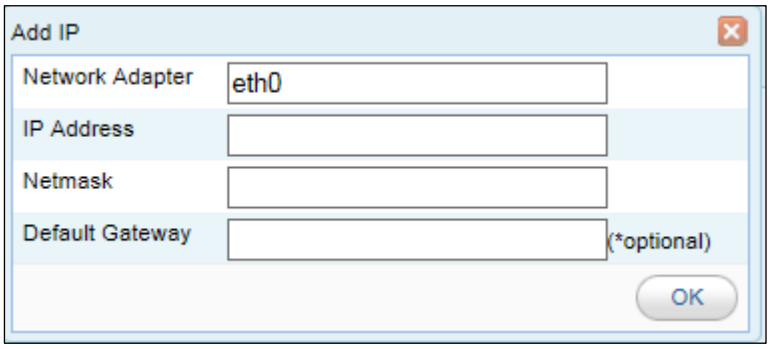


Table 3-3 describes parameters for configuring an interface in IPv4 mode.

Table 3-3 Parameters for configuring an interface in IPv4 mode

Parameter	Description
Network Adapter	Management interface or expansion interface of ADS M
IP Address	IP address of ADS M, which should be an IPv4 address here
Netmask	Netmask of the IPv4 address of ADS M
Default Gateway	IP address of the network gateway of the subnet where ADS M is on

ADS NX3-M1600E

ADS NX3-M1600E differs greatly from ADS NX3-M600A/M1600A in the front panel.

Figure 3-12 Front panel of ADS NX3-M1600E

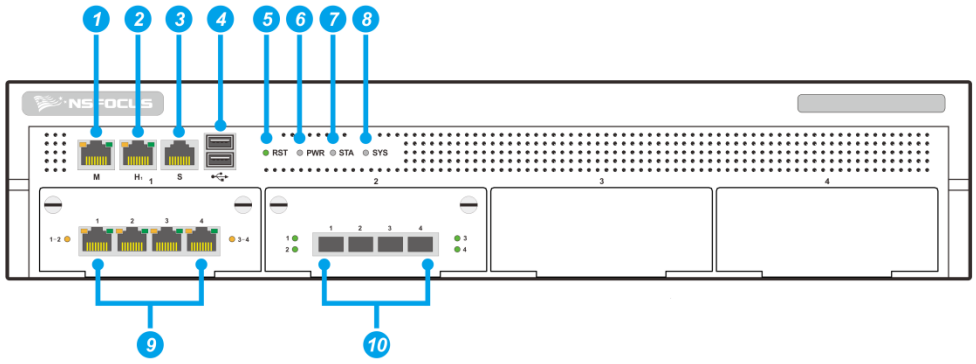


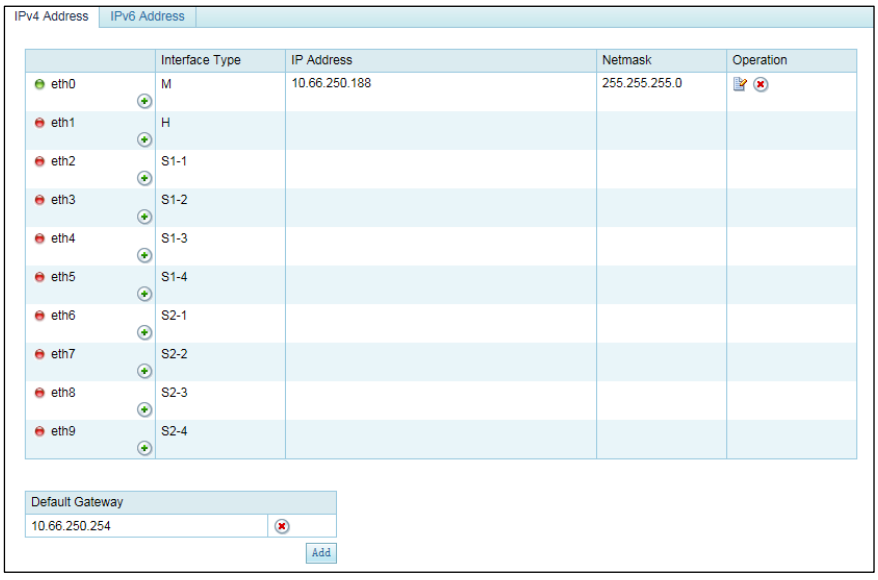
Table 3-4 describes the interfaces on the front panel of ADS NX3-M1600E.

Table 3-4 Front panel of ADS NX3-M1600E

① Management interface: M	② Management interface: H	③ –	④ –
⑤ –	⑥ –	⑦ –	⑧ –
⑨ Working interface: GE electrical (RJ-45) Electrical interfaces are, from left to right, indicated by S1-1, S1-2, S1-3, and S1-4.	⑩ Working interface: GE optical (SFP) Optical interfaces are, from left to right, indicated by S2-1, S2-2, S2-3, and S2-4.	–	–

ADS NX3-M1600E's network interfaces include interface M (1000M), interface H (1000M), four 1000M electrical interfaces, and four 1000M optical interfaces, whose indications on the front panel are listed in the **Interface Type** column on the IPv4 Address page under **Administration > Local Settings > Network Settings**. These 1000M electrical interfaces and optical interfaces are, from left to right, respectively indicated by S1-1, S1-2, S1-3, S1-4, S2-1, S2-2, S2-3, and S2-4 on the front panel of the device.

Figure 3-13 ADS NX3-M1600E – IPv4 address configuration



The interface LED on the left of the interface name indicates the network connection status of this interface.

- : indicates that the network connection of the interface is up.
- : indicates that the network connection of the interface is down.

Though the device does not clearly specify roles of interfaces, interfaces M and H are recommended for configuration and management purposes and other interfaces are used as working interfaces.

Each interface can have two IP addresses. Initially, default parameters are displayed. You need to configure the IPv4 address and subnet mask for the network adapter.
To unbind the IP address from an interface, click in the **Operation** column.

Caution	If the IP address of a management interface is deleted, you may be unable to access the web-based manager of ADS-M.

On the interface list in Figure 3-13, click next to an interface to configure the IPv4 address and other parameters for this interface, as shown in Figure 3-14.

Figure 3-14 ADS NX3-M1600E – Configuring an interface in IPv4 mode

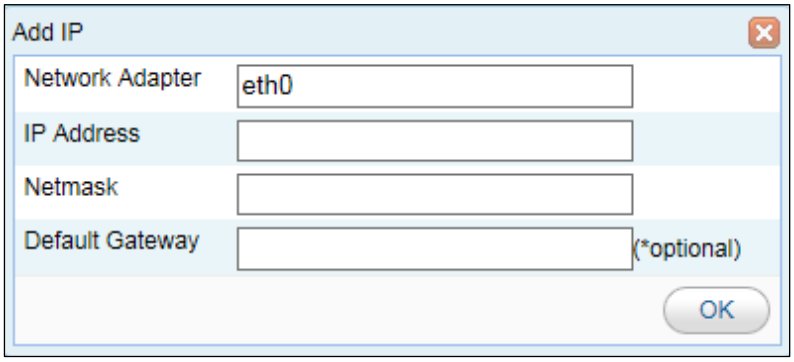


Table 3-5 describes IPv4 network parameters.

Table 3-5 Parameters for configuring an interface in IPv4 mode

Parameter	Description
Network Adapter	Management interface or expansion interface of ADS M
IP Address	IP address of ADS M, which should be an IPv4 address here
Netmask	Subnet mask of the IPv4 address of ADS-M
Default Gateway	IP address of the network gateway of the subnet where ADS M is on

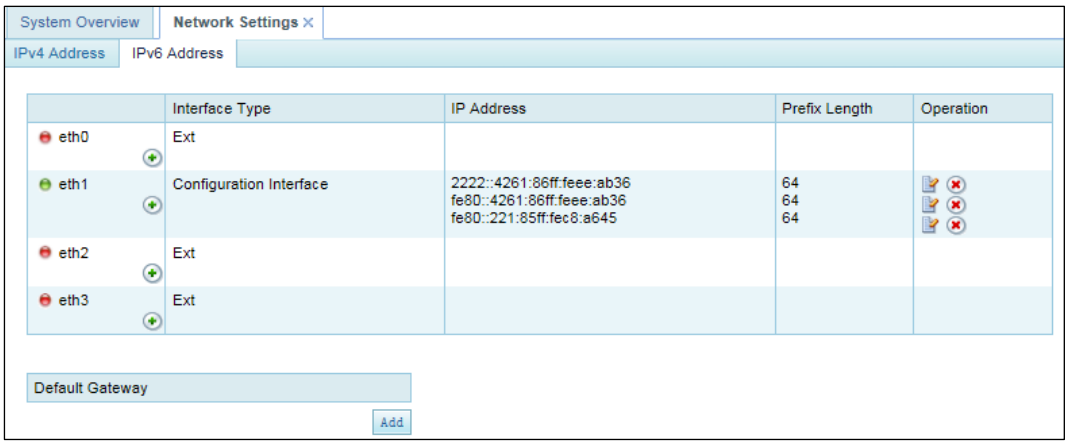
Tip	After you change the IP address of the management interface, the current window may be unavailable. In this case, re-log in to the system from a new browser window.

3.1.5.2 Configuring IPv6 Network Settings

ADS NX3-M600A/M1600A

On the **Network Settings** page shown in Figure 3-10, click **IPv6 Address** to open the IPv6 address configuration page. See Figure 3-15.

Figure 3-15 IPv6 network configuration page



On the interface list shown in Figure 3-15, click next to an interface to configure the IPv6 address and other parameters for this interface in the dialog box, as shown in Figure 3-16.

Figure 3-16 Configuring an interface in IPv6 mode

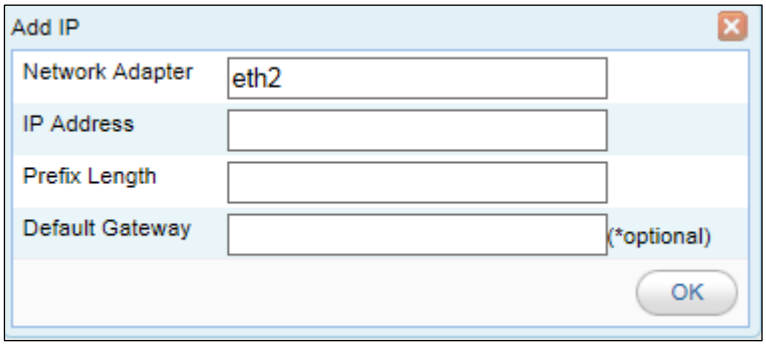


Table 3-6 describes parameters for configuring an interface in IPv6 mode.

Table 3-6 Parameters for configuring an interface in IPv6 mode

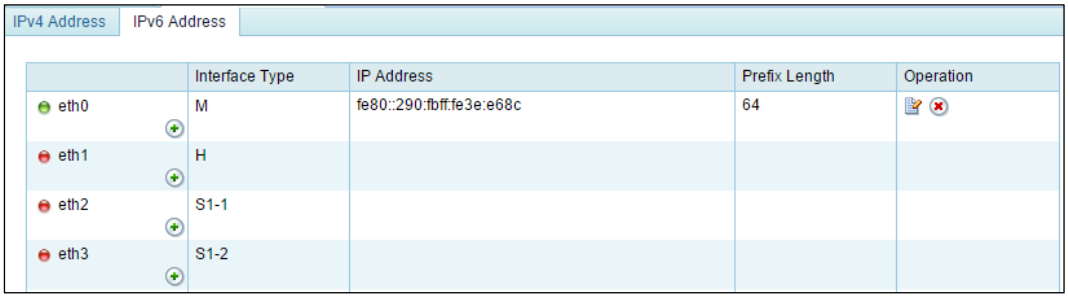
Parameter	Description
Network Adapter	Management interface or expansion interface of ADS M
IP Address	IP address of ADS M, which should be an IPv6 address here
Prefix Length	Prefix length of the configured IPv6 address

Parameter	Description
Default Gateway	IP address of the network gateway of the subnet where ADS M is on

ADS NX3-M1600E

On the **Network Settings** page in Figure 3-10, click **IPv6 Address** to open the IPv6 address configuration page, as shown in Figure 3-17.

Figure 3-17 IPv6 address configuration



On the interface list in Figure 3-17, click next to an interface to configure the IPv6 address and other parameters for this interface, as shown in Figure 3-18.

Figure 3-18 Configuring an interface in IPv6 mode

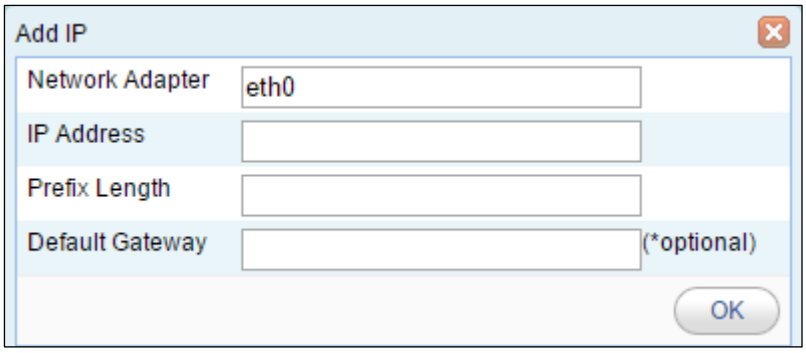


Table 3-7 describes IPv6 network parameters.

Table 3-7 Parameters for configuring an interface in IPv6 mode

Parameter	Description
Network Adapter	Management interface or expansion interface of ADS M
IP Address	Specifies the IP address of ADS M, which should be an IPv6 address here
Prefix Length	Prefix length of the IPv6 address
Default Gateway	IP address of the network gateway of the subnet where ADS M is on

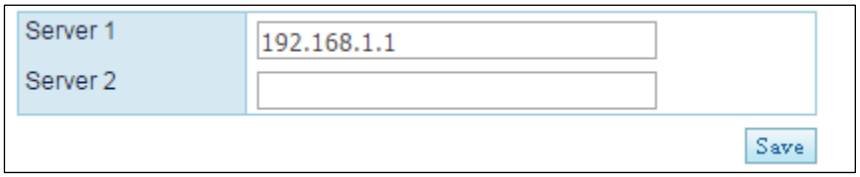
Tip	After you change the IP address of the management interface, the current window may be unavailable. In this case, re-log in to the system from a new browser window.

3.1.6 DNS Server

As an essential and fundamental service, the DNS service is used to determine the mapping between host domain names and IP addresses. You are allowed to configure DNS servers for ADS M.

Choose **Administration** > **Local Settings** > **DNS Server** to open the **DNS Server** page. On this page, type the IP address (two IP addresses at most) of the DNS server of ADS M, as shown in Figure 3-19.

Figure 3-19 DNS Server page

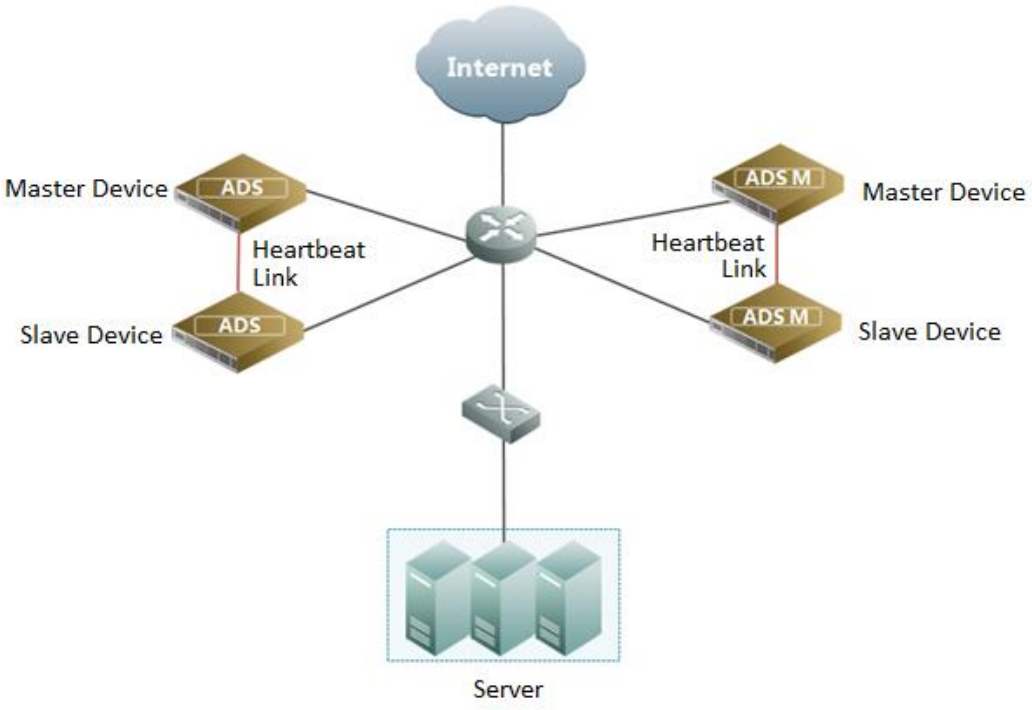


3.1.7 HA Configuration

Currently, ADS M supports the dual-system hot backup function, with one ADS M as the master device and the other as the slave device. By default, the master device handles all traffic and synchronizes heartbeat information and real-time status to the slave device that is only a backup device and does not handle services. If the master device fails, the slave device will take over all the services and traffic handled by the master device, ensuring business continuity to the maximum extent possible.

Routes must be reachable between the master and slave ADS M devices, and the two devices are connected via their heartbeat interfaces (management or work interface) to synchronize heartbeat information and configuration files. Figure 3-20 shows a simple topology for HA.

Figure 3-20 Topology for HA



Configuring HA

During the dual-system hot backup deployment, you must first configure interfaces on the master and slave devices (for details, see section 9.3.2 Configuring Network Settings):

- Configure the heartbeat interfaces (management interface or working interface).

  The heartbeat interfaces are used for the master device to synchronize configuration files to the slave device.

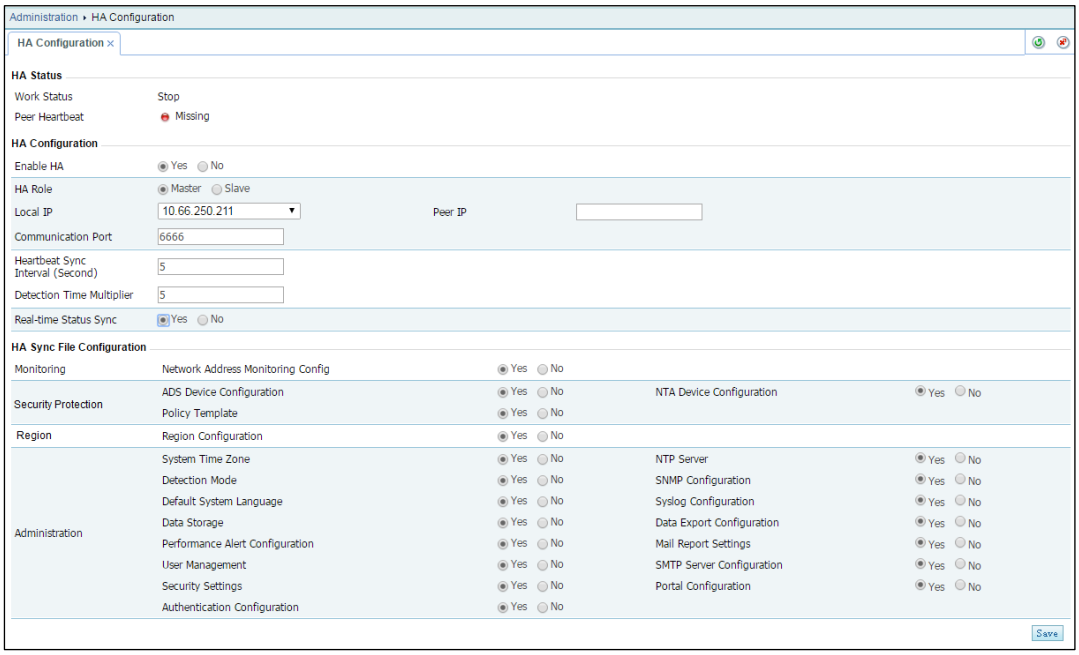
  Routes must be reachable between heartbeat interfaces of master and slave devices.
- Configure other communication interfaces.

After the interface configuration, enable the dual-system hot backup function and configure HA parameters by performing the following steps:

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

The **HA Configuration** page appears, as shown in Figure 3-21.

Figure 3-21 HA Configuration page



Step 2 Set HA parameters under **HA Configuration**.

Table 3-8 describes HA parameters.

Table 3-8 HA parameters

Parameter	Description
Enable HA	Controls whether to enable the HA function. • **Yes** indicates that the HA function is enabled. • **No** indicates that the HA function is disabled.
HA Role	Role played by this device in dual-system hot backup mode. • **master**: indicates that this device functions as the master device and starts to handle services immediately after HA is enabled and will not stop until a failover. • **slave**: indicates that this device functions as the slave device. After HA is enabled, the slave device stays in the backup state without handling services, until a failover.
Local IP	IP address of the heartbeat interface of the current device. It can be an IPv4 or IPv6 address. This IP address can be the IP address of a management interface.
Peer IP	IP address of the heartbeat interface of the peer device. It can be an IPv4 or IPv6 address. This IP address can be the IP address of a management interface. Note Routes must be reachable between heartbeat interfaces of master and slave devices.

Parameter	Description
Communication Port	Port used by the device for communication with the peer. Note The master and slave devices must be configured with the same monitoring port.
Heartbeat Sync Interval (Second)	Interval for the device to synchronize keepalive messages to the peer device. Note The heartbeat synchronization intervals on the master and slave devices should be as close as possible. After an HA connection is established between the master and slave devices, the heartbeat synchronization interval on the slave device will automatically synchronized to that on the master device.
Detection Time Multiplier	Multiple of the heartbeat synchronization interval. This parameter, together with **Heartbeat Sync Interval (Second)**, determines whether the keepalive message times out. If the keepalive message from the peer is not detected within the specified period, this message is considered expired. After an HA connection is established between the master and slave devices, the detection time multiple on the slave device will be automatically synchronized with that on the master device.
Real-Time Status Sync	Whether to enable real-time status synchronization. **Real-Time Status Sync** should be enabled on both the master and slave devices so that files can be synchronized between the two devices. After an HA connection is established between the master and slave devices, the real-time status synchronization setting on the slave device will be automatically synchronized to that on the master device.

Step 3 In the **HA Sync File Configuration** area, select configuration files that need to be synchronized between the master and slave devices.

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

----End

Viewing HA Status

After HA is enabled, the HA working status and peer heartbeat status are displayed under **HA Status** shown in Figure 3-21. The working status can be one of the following:

- **Active**: indicates that the current device works as the master device.
- **Standby**: indicates that the current device works as the slave device.
- **Error**: indicates that the HA function is abnormal on the current device.
- **Stop**: indicates that the HA function is disabled or stopped on the current device.

The peer heartbeat status can be either of the following:

- **Normal**: indicates that the current device can receive heartbeat messages from the peer. The communication is normal.

- **Missing**: indicates that the current device cannot receive heartbeat messages from the peer. The communication is abnormal.

3.1.8 Performance Alert Configuration

On the **Performance Alert Configuration** page, you can set the CPU and memory usage thresholds corresponding to alert levels under **CPU/Memory Alert Config**.

- **Global Configuration** allows you to set alert thresholds for the CPU and memory usage of ADS M itself and all devices under ADS M.
- **ADS Alert Configuration** allows you to set alert thresholds for the CPU and memory usage of all ADS devices under ADS M.
- **NTA Alert Configuration** allows you to set alert thresholds for the CPU and memory usage of all NTA devices under ADS M.

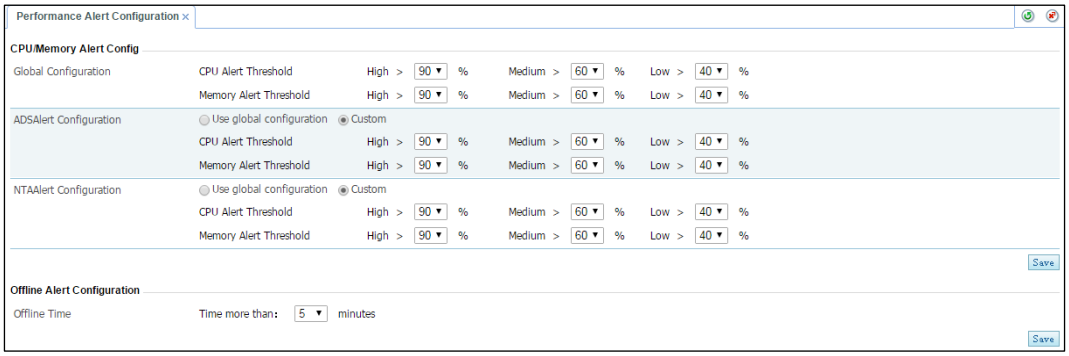
After setting alert thresholds, you can view the status of CPU and memory usage alerts under **Traffic Monitoring > Overview > Device Monitoring**. For details, see section 4.1.5 Viewing the System Status Bar.

Under **Offline Alert Configuration**, you can set the time threshold for triggering device offline alerts. When a device under ADS M remains offline for a period longer than specified, a device offline alert is generated and sent via syslog or email (syslog server and email settings should be completed in advance). For related configuration, see sections 3.3.2 Syslog and 3.3.4 Mail Alert Settings.

To configure performance alerts, follow these steps:

Step 1 Choose **Administration > Local Settings > Performance Alert Configuration**.

Figure 3-22 Performance Alert Configuration page



Step 2 Set CPU and memory alert thresholds and the offline alert parameter.

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

----End

3.2 User and Audit

This section describes how to perform ADS M user management, security settings, authentication configuration as well as how to view audit logs.

3.2.1 User Management

As shown in Figure 3-23, the **User Management** page displays all current users. Initially, only the default user **admin** is displayed.

Figure 3-23 User Management page

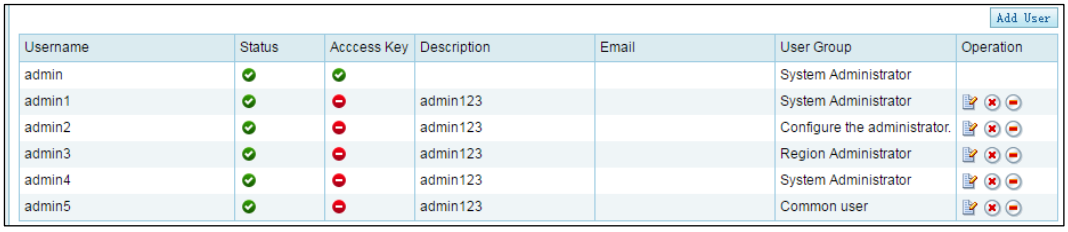


Table 3-9 describes ADS M user groups and their respective privileges.

Table 3-9 ADS M user groups and their respective privileges

User Group	Privileges
System administrator	Has all system management privileges.
Configuration administrator	Has privileges of managing device configurations and viewing system monitoring information, reports, logs, and region information, without system management privileges.
Region administrator	Has privileges of configuring regions, viewing system monitoring information, reports, and logs, and viewing device configurations, without system management privileges.
Common user	Has privileges of viewing information of all modules, except the system management module.

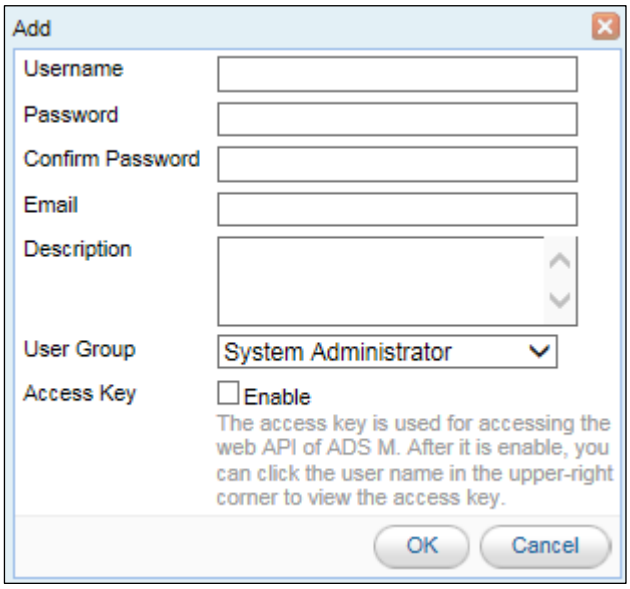
Creating a User

Only the user **admin** can create system administrators. Only system administrators can create configuration administrators, region administrators, and common users.

To create a user, follow these steps:

Step 1 Click **Add User** in the upper-right corner of the **User Management** page.

Figure 3-24 Creating a user



Step 2 Set parameters in the dialog box and click **OK**.

Table 3-10 Parameters for creating a user

Parameter	Description
Username	Specifies the user name. The user name must be 4 to 20 characters and cannot contain invalid characters such as the tab character, carriage return, \0, space, vertical bar (|), slash (/), angle bracket (<, or >), quotation mark (" or '), and semicolon (;).
Password	Specifies the password. The minimum length and strength of the password can be configured under **Administration** > **User and Audit** > **Security Settings**.
Confirm Password	Password confirmation. The password you type here must be the same as the one you typed for **Password**.
Email	A valid email address of the user. This parameter is optional.
Description	Brief description of this user. This parameter is optional.
User Group	User role. Different roles have different operation privileges.
Access Key	Used for accessing the web API of ADS M. For details about configuration of the web API, please contact NSFOCUS technical support.

----End

Modifying User Information

Only user **admin** and other system administrators can modify information of all users. Other users can only modify their own information.

On the **User Management** page, click in the **Operation** column of a user to edit information of this user. Note that the user name cannot be changed. To edit the default system administrator **admin**, you need to log in to the system as **admin** and click admin in the quick access bar in the upper-right corner of the page.

Deleting a User

Only the user **admin** and other system administrators can delete users.

On the user list, click in the **Operation** column to delete a user. The default system administrator **admin** cannot be deleted.

Disabling a User

Only the user **admin** and other system administrators can disable users.

By default, new users are enabled, that is, the **Status** column is displayed as . On the user list, click in the **Operation** column to disable a user. Then the icon is displayed as in the **Status** column. Disabled users cannot log in to the web-based manager of ADS M. The default system administrator **admin** cannot be disabled.

Enabling a User

To enable a user that is disabled, click in the **Operation** column on the user list.

Note	Only the user **admin** and other system administrators can enable users.

3.2.2 Security Settings

Only the system user **admin** can view and manage security settings. Therefore, this module is unavailable for other users.

Note	All users, including region users, can set **Password Strength** and **Weak Password Dictionary**, but **Login Security Settings** is configurable only for ADS M users.

Choose **Administration** > **User and Audit** > **Security Settings**. The **Security Settings** page appears, as shown in Figure 3-25.

Figure 3-25 Security settings

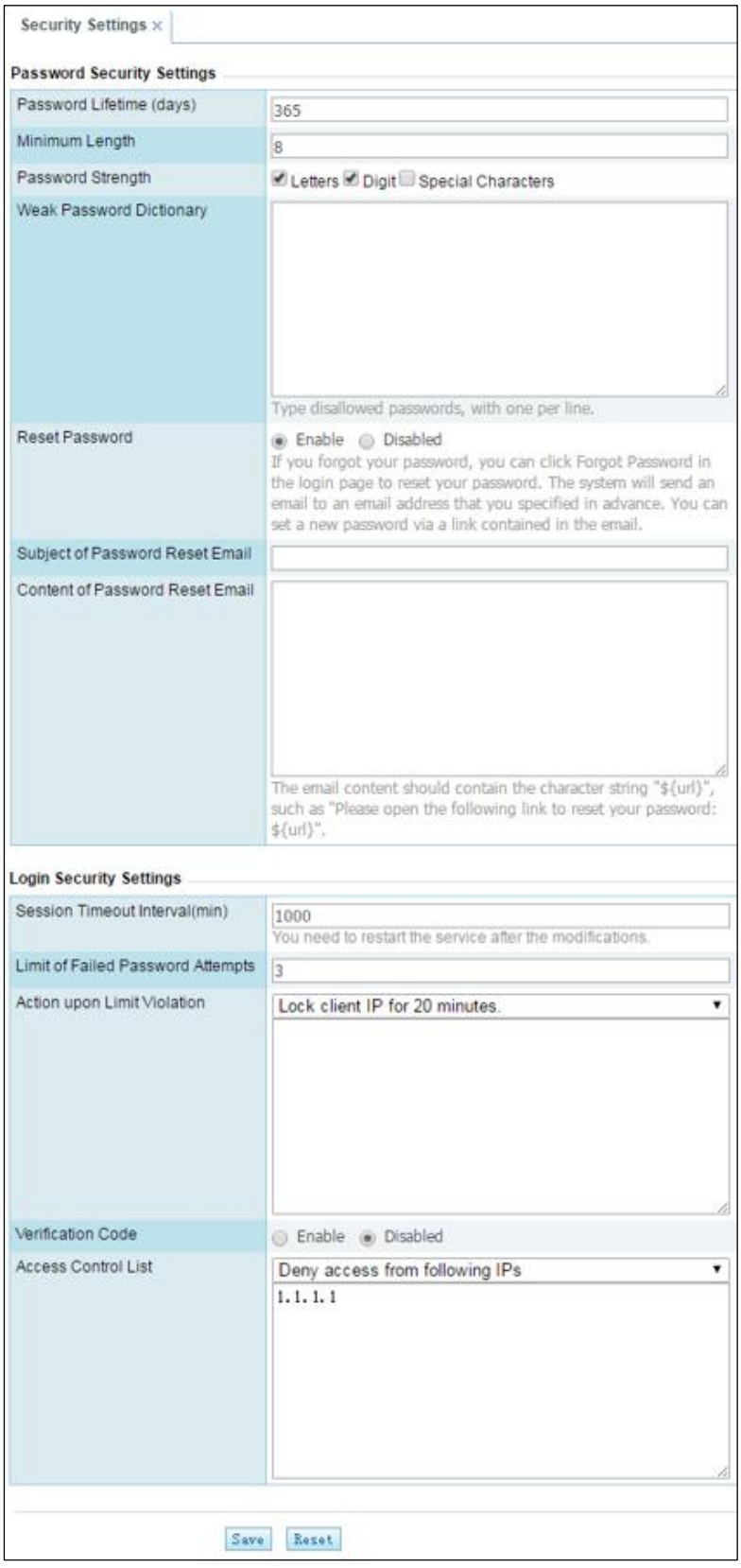


Table 3-11 describes parameters of security settings.

Table 3-11 Parameters of security settings

Parameter	Description
Password Lifetime (days)	Specifies the password validity. The value range is 0–65535. **0** indicates that there is no limit on the validity. The default value is **365** days.
Minimum Length	Specifies the minimum password length. The value is an integer ranging from 8 to 99, with **8** as the default.
Password Strength	Specifies the complexity of a password. By default, the password must contain letters and digits. Also, you can define that the password must contain at least two types of the following: letters, digits, and special characters.
Weak Password Dictionary	Specifies the passwords that are prohibited for use due to weak security. Each weak password should be in a separate line.
Reset Password	Controls whether the password resetting function is enabled. After this function is enabled, you can reset the password by email. For details about how to reset the password, see Resetting the Password in section 2.3 Other Operations.
Subject of Password Reset Email	Specifies the subject of the email message notifying password resetting. This can be defined by users.
Content of Password Reset Email	Specifies the content of the email message notifying password resetting. This can be defined by users, but the content must contain the string, ${url}; otherwise, password resetting would fail.
Session Timeout Interval(min)	Specifies how long a user can stay inactive before being automatically logged out of the system.
Limit of Failed Password Attempts	Specifies the maximum number of consecutive failed password attempts.
Action upon Limit Violation	Specifies the action that the system will take after the number of consecutive failed password attempts reaches the specified value. Values include the following: • **Return result after 3-second pause** • **Lock client IP for 20 minutes**: The currently locked IP addresses are listed in the text box below. By default, a locked IP address will be automatically unlocked in 20 minutes. Alternatively, the administrator can delete a locked IP address from the list and then click **Save** to manually unlock this IP address.
Verification Code	Controls whether to enable the use of verification codes for login authentication. By default, it is disabled. • **Enable**: allows use of login verification codes, indicating that a user can successfully log in to ADS M only after typing a correct verification code. • **Disable**: disables use of verification codes for login authentication.
Access Control List	Specifies whether to allow a client to access the system. It has the following values:

Parameter	Description
	• **No**: indicates any clients can access to the system. • **Permit access from the following IP addresses**: indicates that only clients with IP addresses included in the text box below can access the system. • **Deny access from the following IPs**: indicates that clients with IP addresses included in the text box below cannot access the system. When you access ADS from a blocked IP address, the system displays "You cannot log in from the current IP address. Please contact the administrator to check access control settings." on the login page. Note After the access control list is successfully modified, you are advised to wait at least 3 minutes for the settings to take effect.

3.2.3 Authentication Configuration

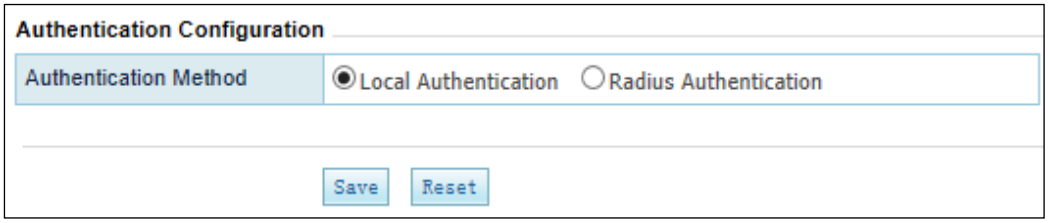
ADS M supports local authentication and third-party Radius server authentication for user authentication.

Note	• When local authentication is used, users can access ADS M using the user name and password configured under **Administration > User and Audit > User Management**. • When third-party Radius server authentication is used, users must add the user name and password configured on the third-party Radius server to ADS M and use such user name and password to access ADS M.

To configure an authentication method, follow these steps:

Step 1 Choose **Administration** > **User and Audit** > **Authentication Configuration**.

Figure 3-26 Authentication Configuration page



Step 2 Select an authentication method, which can be **Local Authentication** or **Radius Authentication**.

Step 3 (Optional) When **Authentication Method** is set to **Radius Authentication**, set Radius server parameters in the dialog box shown in Figure 3-27.

Figure 3-27 Configuring the Radius server

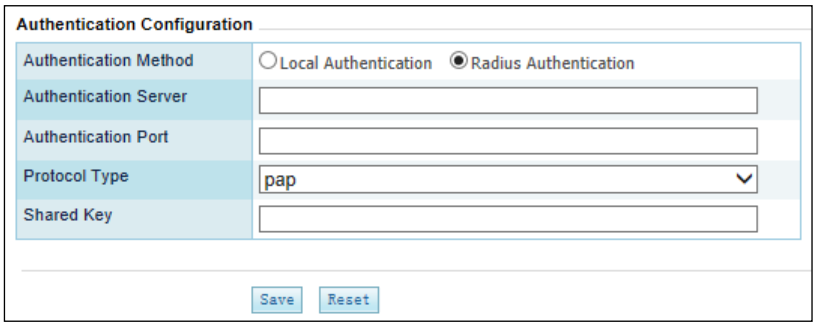


Table 3-12 describes parameters for configuring the Radius server.

Table 3-12 Parameters for configuring the Radius server

Parameter	Description
Authentication Server	Specifies the IP address of the third-party Radius server.
Authentication Port	Specifies the port of the third-party Radius server that is used for data communication.
Protocol Type	Specifies the protocol used for authenticating the third-party Radius server, which can be **pap**, **chap**, **spap**, **mschapv1**, or **mschapv2**.
Shared Key	Specifies the key shared between ADS M and the third-party Radius server.

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

----End

3.2.4 Audit Logs

Audit logs refer to all audit logs generated during ADS M operation and user operations. Only the system administrator can view audit logs.

Choose **Administration** > **User and Audit** > **Audit Logs** to open the **Audit Logs** page, as shown in Figure 3-28. By default, no audit log is available. After you click **Search**, all audit logs of ADS M are displayed, including generation time, user name, client IP address, functional module, operation result, and log description.

Figure 3-28 Audit logs

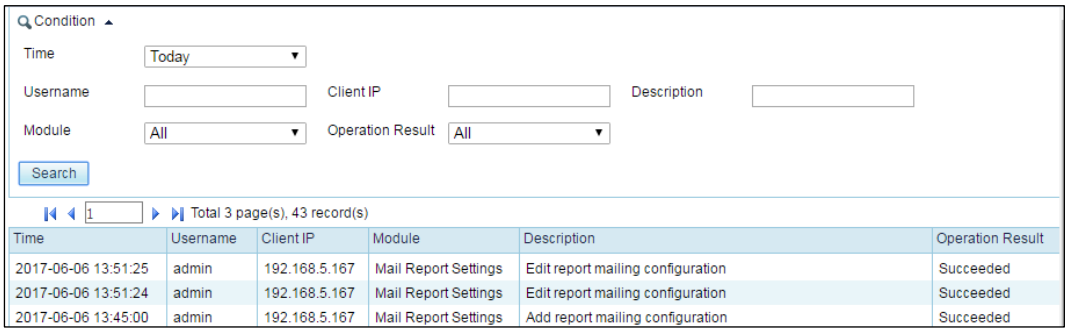


Table 3-13 describes audit log parameters.

Table 3-13 Audit log parameters

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Username	Specifies the login user name. The full user name is required because fuzzy query is not allowed here.
Client IP	Specifies the IP address of the user device. The full IP address is required because fuzzy query is not allowed here.
Module	Specifies the functional module whose logs are queried.
Description	Specifies the keyword of logs to be queried.
Operation Result	Specifies the result of the operations performed on the client. **All** indicates that all operation result logs are displayed.

3.3 Third-Party Interface

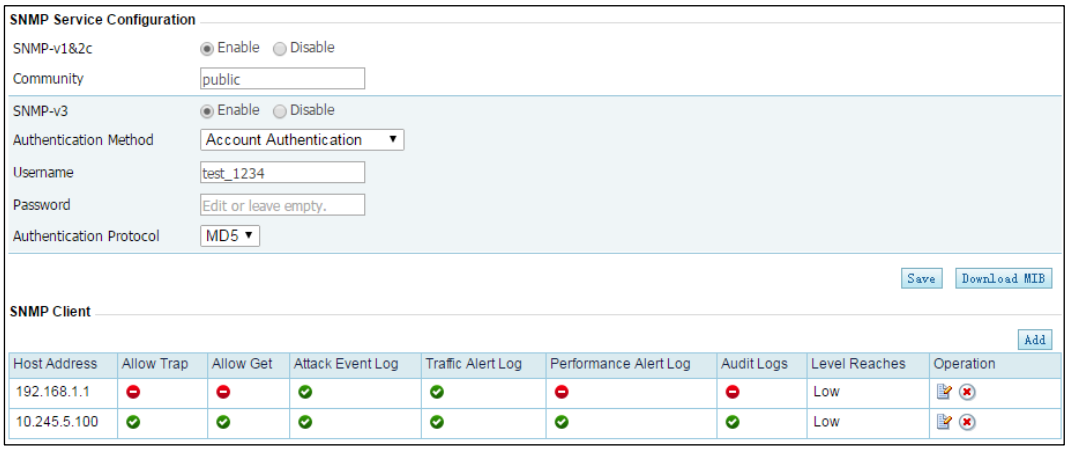
ADS M exchanges data with external systems via SNMP and syslog interfaces. The third-party interface configuration includes configuration of an SNMP server, syslog server, SMTP server, and other servers.

3.3.1 SNMP Configuration

ADS M supports management via the Simple Network Management Protocol (SNMP). ADS M can not only respond to queries from the SNMP manager as an agent by returning information about its running status, but also send trap messages to the SNMP manager.

Choose **Administration** > **Third-Party Interface** > **SNMP Configuration** to open the **SNMP Configuration** page. If an SNMP server is configured, the system automatically displays the client IP addresses that access ADS M through SNMP, as shown in Figure 3-29.

Figure 3-29 SNMP configuration



Downloading a MIB File

Click **Download MIB** in the upper-right corner of the page shown in Figure 3-29. In the dialog box that appears, click **Save**. Then the MIB file is downloaded to the local disk drive.

Configuring an SNMP Server

On the **SNMP Configuration** page, set SNMP client IP addresses and related parameters, and click **Save** to save the settings.

Table 3-14 describes parameters for configuring an SNMP server.

Table 3-14 Parameters for configuring an SNMP server

Parameter	Description
SNMP-v1&2c	Controls whether SNMPv1 and SNMPv2c are enabled for management.
Community	Specifies the community supported by the SNMP agent. This parameter is required when **SNMP-v1&2c** is set to **Enable**.
SNMP-v3	Controls whether SNMPv3 is enabled for management. Note When both **SNMP-v1&2c** and **SNMP-v3** are set to **Enable**, ADS M uses SNMP-v3 for authentication.
Authentication Method	Specifies the authentication method when **SNMP-v3** is set to **Enable**, which can be **No authentication**, **Account Authentication**, or **Private key Authentication**.
Username	Specifies the SNMP V3 user name.
Password	Specifies the password for user authentication via SNMPv3. This parameter is required when **Authentication Method** is set to **Account Authentication** or **Private key Authentication**.
Authentication Protocol	Specifies the protocol used for user authentication via SNMPv3, which can be **MD5** or **SHA**.

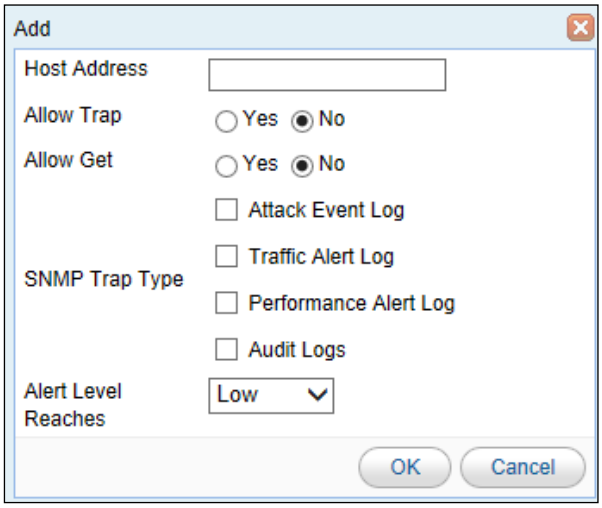
Parameter	Description
	This parameter is required when **Authentication Method** is set to **Account Authentication** or **Private key Authentication**.
Private Key Protocol	The DES protocol is used by default and cannot be changed. This parameter is required only when **Authentication Method** is set to **Private key Authentication**.
Private Key Password	Specifies the encrypted key password used during data transmission. This parameter is required only when **Authentication Method** is set to **Private key Authentication**.

Configuring an SNMP Client

Step 1 Click **Add** in the **SNMP Client** area shown in Figure 3-29.

A dialog box appears, as shown in Figure 3-30.

Figure 3-30 Adding an SNMP client



Step 2 Configure parameters in the dialog box.

Table 3-15 Parameters for configuring an SNMP client

Parameter	Description
Host Address	Specifies the IP address of the client that accesses ADS M through SNMP. Both the IPv4 and IPv6 addresses are allowed.
Allow Trap	Controls whether to allow the client to send trap messages to ADS M.
Allow Get	Controls whether to allow ADS M to acquire information about the client through SNMP GET messages.
SNMP Trap Type	Specifies the type of SNMP trap messages, which can be **Attack Event Log**, **Traffic Alert Log**, **Performance Alert Log**, or **Audit Logs**.

Parameter	Description
Alert Level Reaches	Specifies which level of alert messages will be filtered, which can be **Low**, **Medium**, or **High**.

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

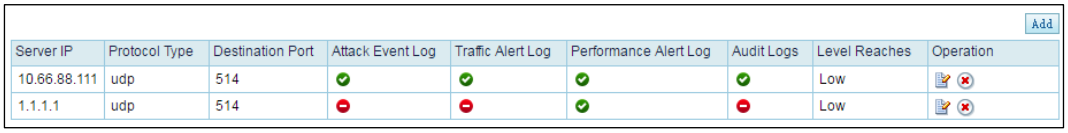
----End

3.3.2 Syslog Configuration

If the syslog server is used to transmit data between ADS M and devices under it, you need to configure syslog settings.

Choose **Administration** > **Third-Party Interface** > **Syslog Configuration** to open the **Syslog Configuration** page, as shown in Figure 3-31.

Figure 3-31 Syslog configuration



Adding a Syslog Server

On the **Syslog Configuration** page shown in Figure 3-31, click **Add** to add a syslog server, as shown in Figure 3-32.

Figure 3-32 Adding a syslog server

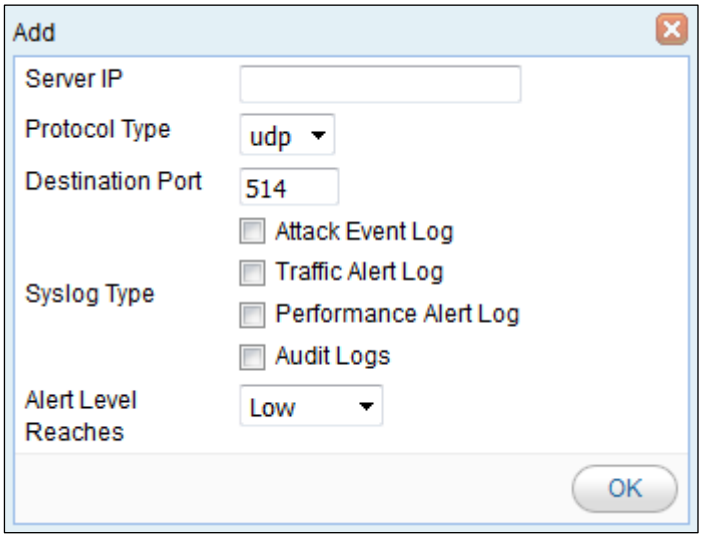


Table 3-16 describes syslog server parameters.

Table 3-16 Syslog server parameters

Parameter	Description
Server IP	Specifies the IP address of the syslog server.
Protocol Type	Specifies the protocol used for data transmission. By default, the UDP protocol is used.
Destination Port	Specifies the port of the syslog server.
Syslog Type	Specifies the type of data transmitted by the syslog server. Values are **Attack Event Log**, **Traffic Alert Log**, **Performance Alert Log**, and **Audit Logs**. **Traffic Alert Log** is available only when ADS M works in NTA detection mode.

Editing a Syslog Server

On the **Syslog Configuration** page shown in Figure 3-31, click in the **Operation** column of a syslog server to edit all its parameters, except **Server IP**.

Deleting a Syslog Server

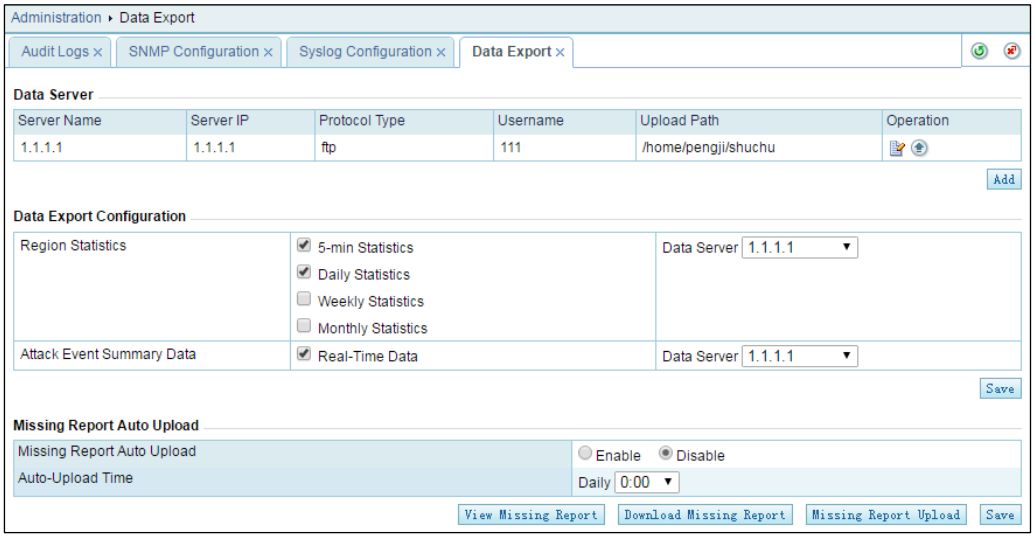
On the **Syslog Configuration** page shown in Figure 3-31, click in the **Operation** column of a syslog server to delete it.

3.3.3 Data Export

Under **Administration** > **Third-Party Interface** > **Data Export**, you can export the data and upload it to a remote server for access by other users. You can add a data server and upload the reports generated by ADS M to it, as shown in Figure 3-33.

For missing reports that failed to be uploaded to the specified data server, you can configure automatic or manual upload for them.

Figure 3-33 Data export



Adding a Data Server

You can export data only after a data server is configured.

Step 1 On the **Data Export** page shown in Figure 3-33, click **Add** to the lower right of the data server list.

Step 2 In the **Add** dialog box, configure parameters.

Figure 3-34 Adding a data server

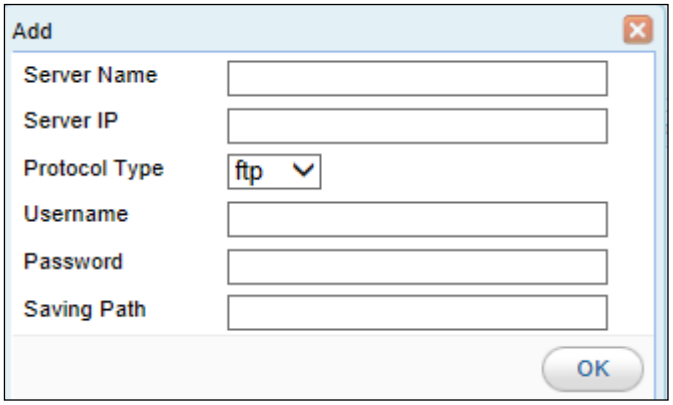


Table 3-17 describes parameters for adding a data server.

Table 3-17 Parameters for adding a data server

Parameter	Description
Server Name	Specifies the data server name.
Server IP	Specifies the IP address of the data server.
Protocol Type	Specifies the protocol used for data transmission, which can be **ftp**, **sftp**, or **scp**. By default, the FTP protocol is used.
Username	Specifies the user name for logging in to the remote data server.
Password	Specifies the password for logging in to the remote data server.
Saving Path	Specifies the path for saving the data uploaded to the remote data server.

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

----End

Editing a Remote Data Server

On the data server list, click in the **Operation** column to edit settings of a remote data server.

Deleting a Remote Data Server

On the data server list, click in the **Operation** column to delete a remote data server.

Uploading Data to a Remote Data Server

On the data server list, click in the **Operation** column to test whether files can be uploaded to a remote data server.

Configuring Data Export

Step 1 In the **Data Export Configuration** area, select the type of data to be exported and the server to which the data is uploaded.

Step 2 Click **Save** to complete the configuration.

----End

Configuring Missing Report Upload

Step 1 In the **Missing Report Auto Upload** area, set **Missing Report Auto Upload** to **Enable**.

Step 2 Specify the upload time and then click **Save** to save the settings.

----End

For missing reports that failed to be uploaded automatically, click **Missing Report Upload** to manually upload them to the data server. You can also click **View Missing Report** and **Download Missing Report** to view and download missing reports respectively.

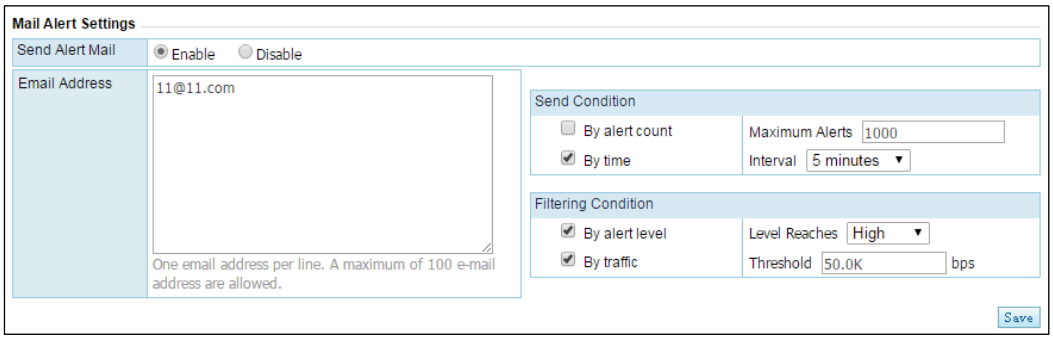
3.3.4 Mail Alert Settings

You can configure mail settings on the **Mail Alert Settings** page.

To configure alert mail settings, perform these steps:

Step 1 Choose **Administration > Third-Party Interface > Mail Alert Settings**.

Figure 3-35 Mail alert settings



Step 2 Set **Send Alert Mail** to **Enable**.

Step 3 Specify email addresses that receive alert mails, and set mail sending and filtering conditions for alert mails.

Note	Alerts of ADS devices and alerts related to HA are all high-level alerts. Alerts from NTA devices can be classified into low-level, medium-level, and high-level.

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

----End

3.3.5 SMTP Server Configuration

After enabling **Reset Password** (**Administration > User and Audit > Security Settings**), you must configure an SMTP server for sending the password resetting link to the user's email address. Figure 3-36 is the page for configuring an SMTP server for sending mails. You can modify related values in text boxes as required and then click **Save** in the upper-right corner.

Figure 3-36 SMTP server configuration

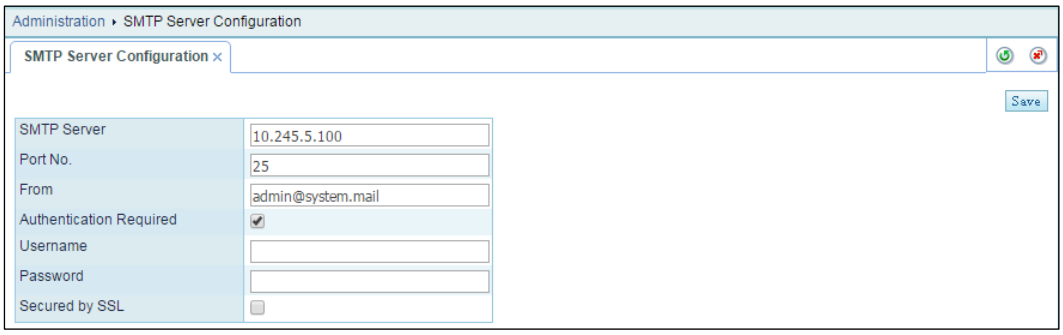


Table 3-18 lists parameters for configuring an SMTP server.

Table 3-18 Parameters for configuring an SMTP server

Parameter	Description
SMTP Server	Specifies the IP address or domain name of the SMTP server that sends emails.
Port No.	Specifies the port of the SMTP server.
From	Specifies the email address from which emails are sent.
Username	Specifies the user name of the account from which emails are sent. This parameter is required only when **Authentication Required** is selected.
Password	Specifies the password of the account from which emails are sent. This parameter requires a value only when **Authentication Required** is selected.
Secured by SSL	Controls whether a security password is required for the email sender for identity authentication.

3.4 Debug Information Collection

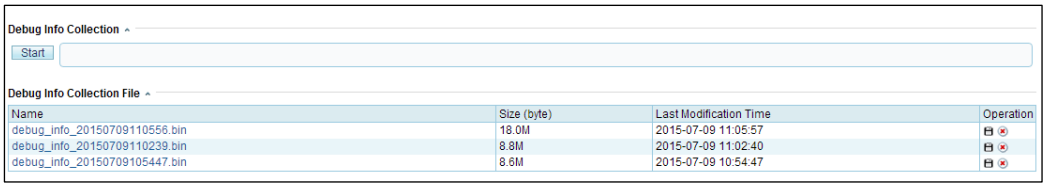
When ADS M fails, you can collect debug information, including the device's basic information and configuration information, for which a compressed file is generated. You can download this file and send it to NSFOCUS technical support for fault diagnosis.

Choose **Administration > Diagnosis > Debug Info Collection**. Then click **Start** on the **Debug Info Collection** page to collect information about the current device. The generated information file will be saved in the debug information file list. See Figure 3-37.

You can click in the **Operation** column to download the file to a local disk drive.

A maximum of five debug information files are listed on the **Debug Info Collection** page. If more files are generated, the file with the earliest **Last Modification Time** will be deleted automatically.

Figure 3-37 Debug information collection



4 Traffic Monitoring

Traffic monitoring provides the following information:

Section	Description
Overview	Displays monitoring information regarding four types of traffic, six types of attack events, and status information of the managed devices (NTA and ADS).
DDoS Attack Traffic Monitoring	Displays traffic information of specified IP addresses, protection groups, regions, region IP groups, and ADS.
Network Traffic Monitoring	Displays traffic information of a specified IP group, region, regional IP group, and NTA device.
Attack Events	Displays attack information of specified IP addresses, protection groups, regions, region IP groups, and ADS.

4.1 Overview

After you log in to the web-based manager, the **Overview** page appears, displaying the following monitoring information:

- Four types of traffic and five types of attack events detected by ADS
- Top NTA alerts
- System status of NTA and ADS

Table 4-1 describes in detail the monitoring information on the **Overview** page.

Table 4-1 Monitoring information displayed on the Overview page

Category	Monitoring Information	Description
DDoS traffic	Top destination IP addresses	Displays in real time top 10 protected IP addresses ranked according to traffic dropped by ADS in the last 30 seconds, letting users know which IP addresses see the largest traffic or are most severely attacked.
	Top regions by attack traffic	Displays in real time top 10 protected regions ranked according to traffic dropped by ADS in the last 30 seconds, letting users know which regions see the largest traffic or are most severely attacked.
	Protocol analysis	Provides an overview of TCP, UDP, and ICMP traffic handled by ADS in the last 30 minutes as well as details about each type of traffic.

Category	Monitoring Information	Description
	Attack traffic trend	Displays the trends of traffic received, dropped, and forwarded by ADS in the last 30 minutes.
Attack events	Top source countries	Displays in real time top 10 attack source countries/regions ranked according to attack traffic dropped by ADS in the last 30 seconds.
	Attack traffic	Displays the trend of attack traffic handled by ADS in the last 30 minutes and traffic statistics of various attack types at each point of time.
	Top NTA alerts	Displays in real time top 5 traffic alerts generated by NTA in the last 30 seconds.
	Top ongoing attack events	Displays in real time top 10 ongoing attack events handled by ADS in the last 30 seconds.
	Top 10 source IP addresses	Displays in real time top 10 source IP addresses ranked according to traffic dropped by ADS in the last 30 seconds.
	Attack type distribution	Displays in real time all attack types handled by ADS in the last 30 seconds and the percentage of each type of attack traffic to the total attack traffic.
Devices	Device monitoring	Displays in real time the status, CPU usage, and memory usage of NTA and ADS in the last 30 seconds.
Network traffic	Top NTA regions by traffic	Displays traffic in the last 30 minutes received and transmitted by regions configured on NTA under monitoring of ADS M.
	Trend of traffic on NTA	Displays trends of traffic in the last 30 minutes received and transmitted by NTA under monitoring of ADS M.

4.1.1 Adding a Panel

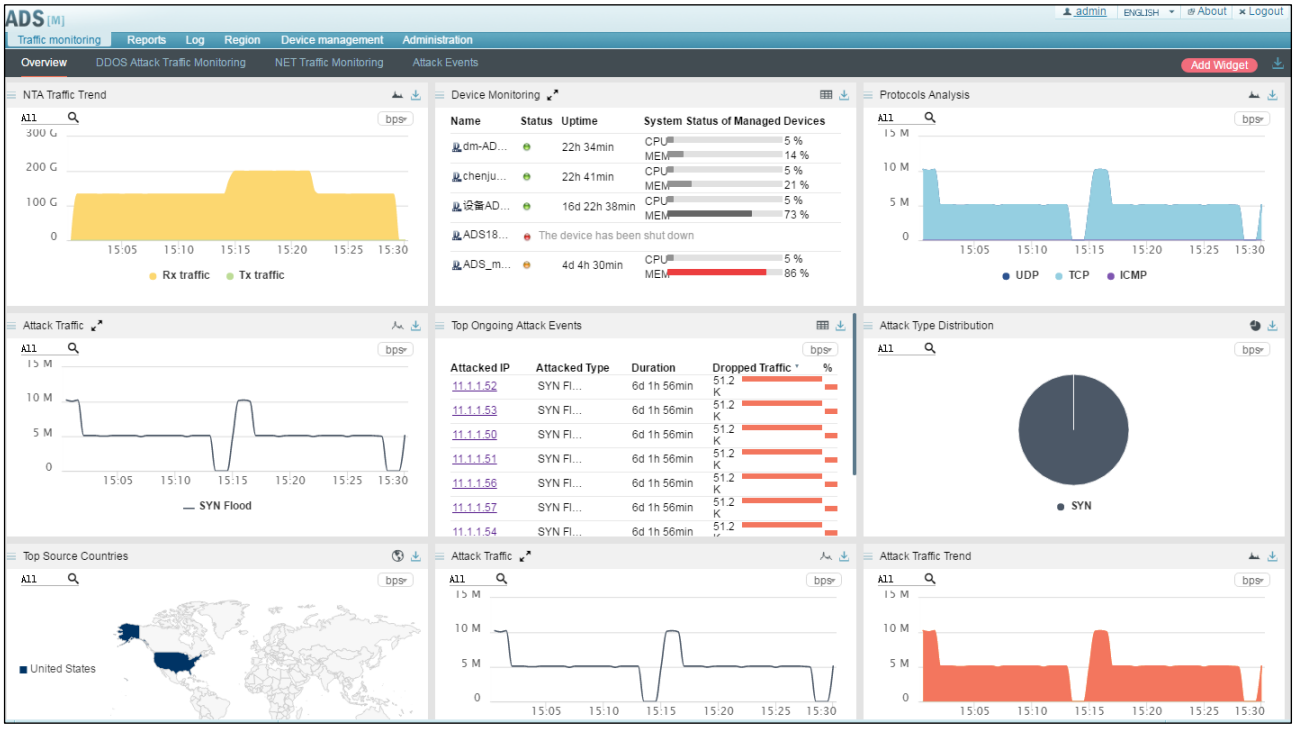
The **Overview** page can present the following panels:

- Attack Traffic Trend
- Protocol Analysis
- Top Destination IP
- Top Region Attack Traffic
- Top Source Countries
- Attack Traffic
- Top NTA Alerts
- Top Ongoing Attack Events
- Top 10 Source IP
- Attack Type Distribution
- Device Monitoring
- Top NTA Region Traffic
- NTA Traffic Trend

You can add panels as required by performing the following steps:

Step 1 Choose **Traffic monitoring > Overview**.

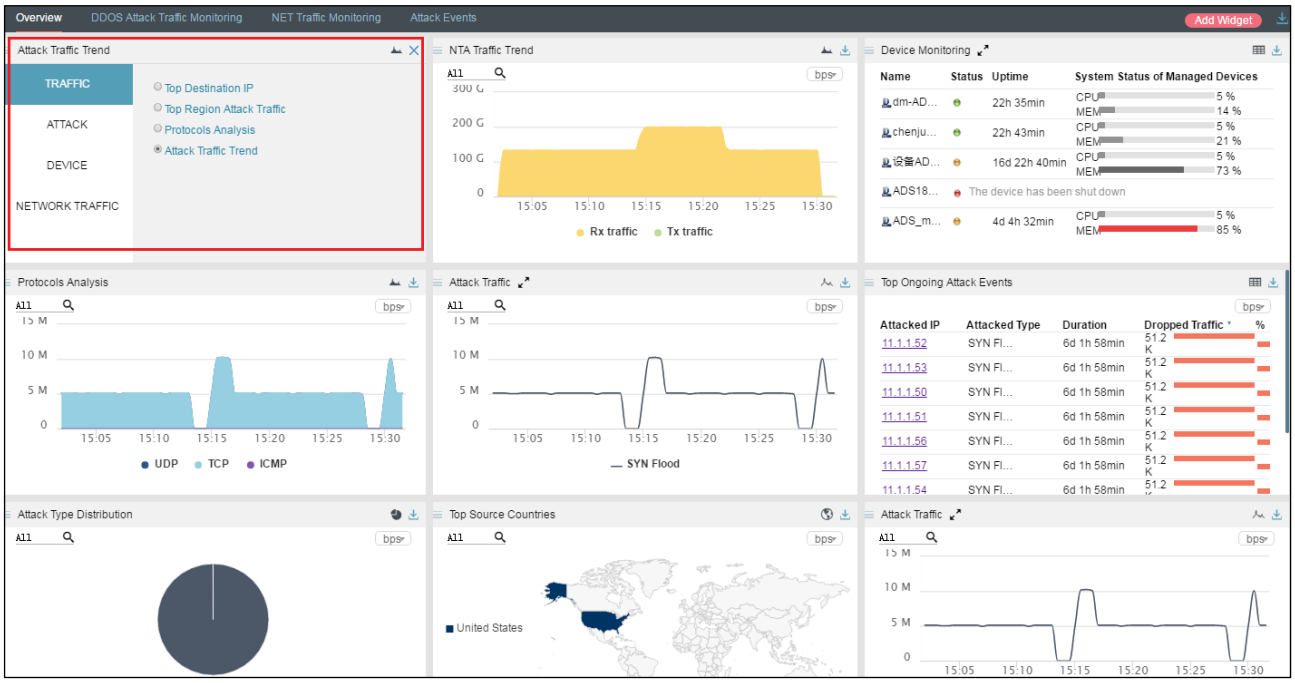
Figure 4-1 Overview page



Step 2 Click **Add Widget** in the upper-right corner of the page.

Then a box appears in the upper-left corner, as shown in Figure 4-2, for you to choose a panel to display on the **Overview** page.

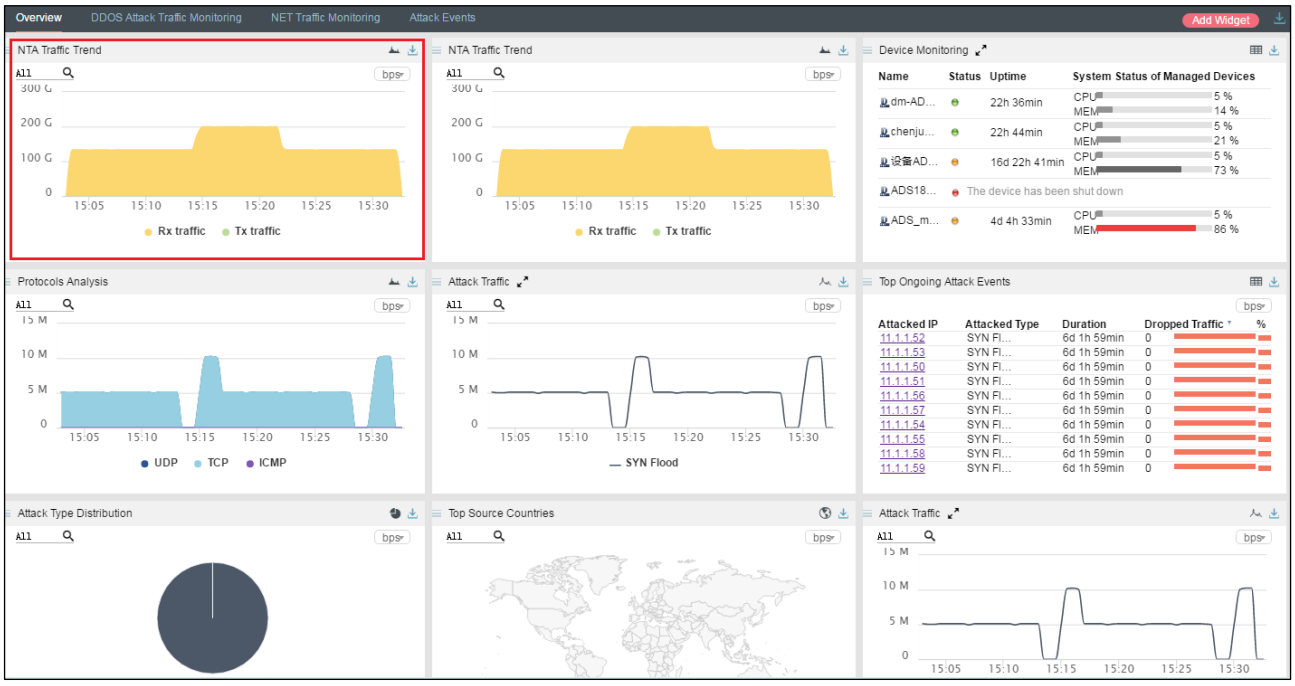
Figure 4-2 Adding a panel



Step 3 Select a category (TRAFFIC, ATTACK, DEVICE, or NETWROK TRAFFIC) from the left pane and then click a panel in the right pane.

Then the new panel appears on the **Overview** page. For example, if you select **NETWORK TRAFFIC** and **NTA Traffic Trend** respectively, the new panel appears in the upper-left corner, as shown in Figure 4-3.

Figure 4-3 New panel displayed



----End

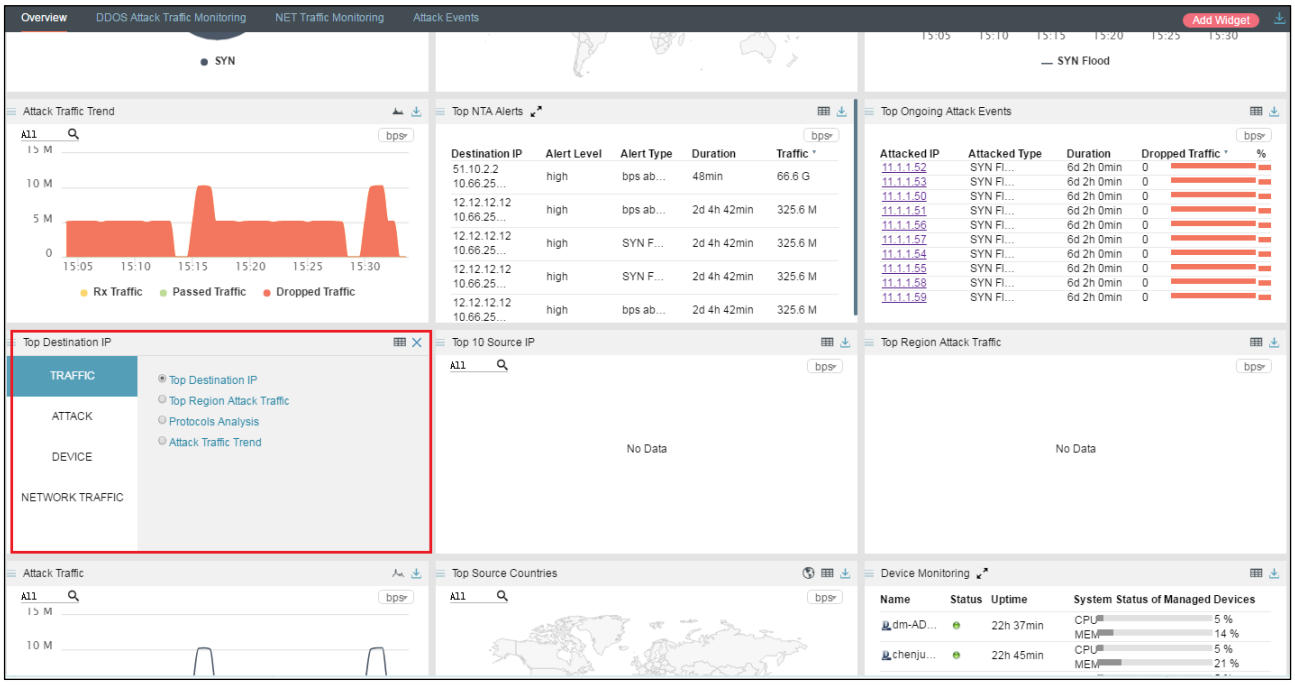
4.1.2 Changing a Panel

You can change a panel by performing the following steps:

Step 1 On the page shown in Figure 4-1, click in the upper-left corner of a panel, for example, **Top Destination IP**.

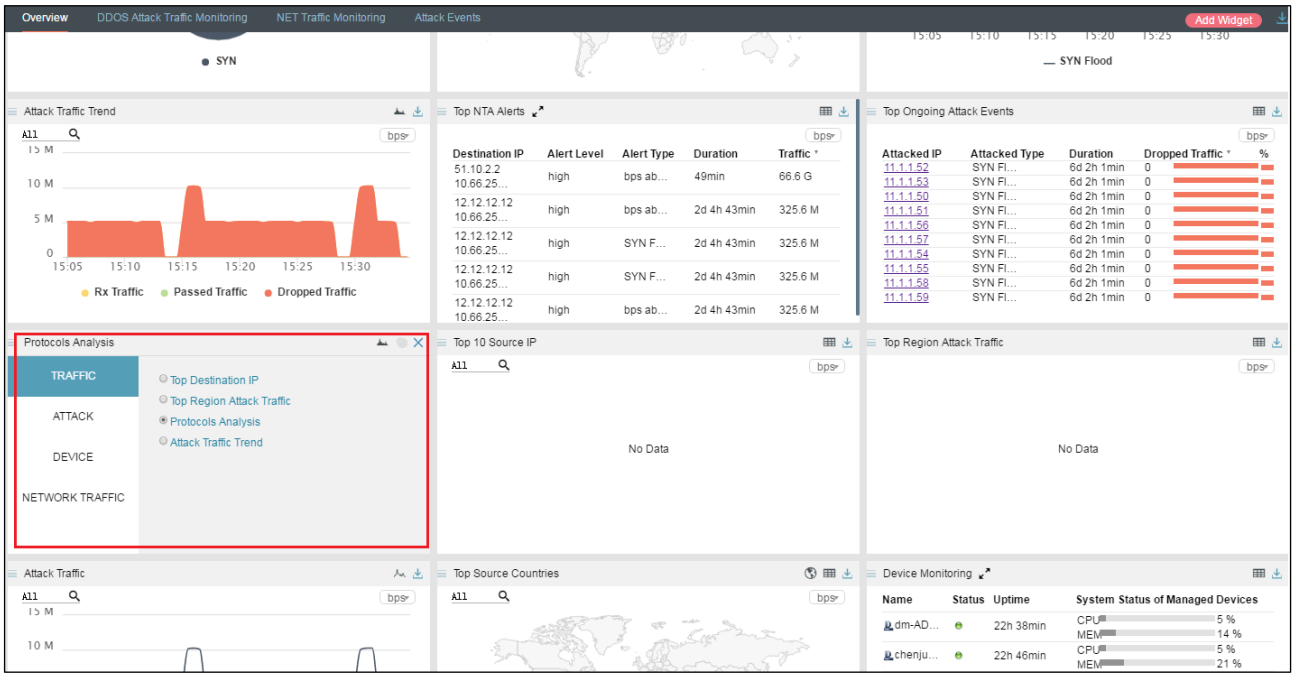
Then the panel reverses, as shown in Figure 4-4.

Figure 4-4 Reversed panel



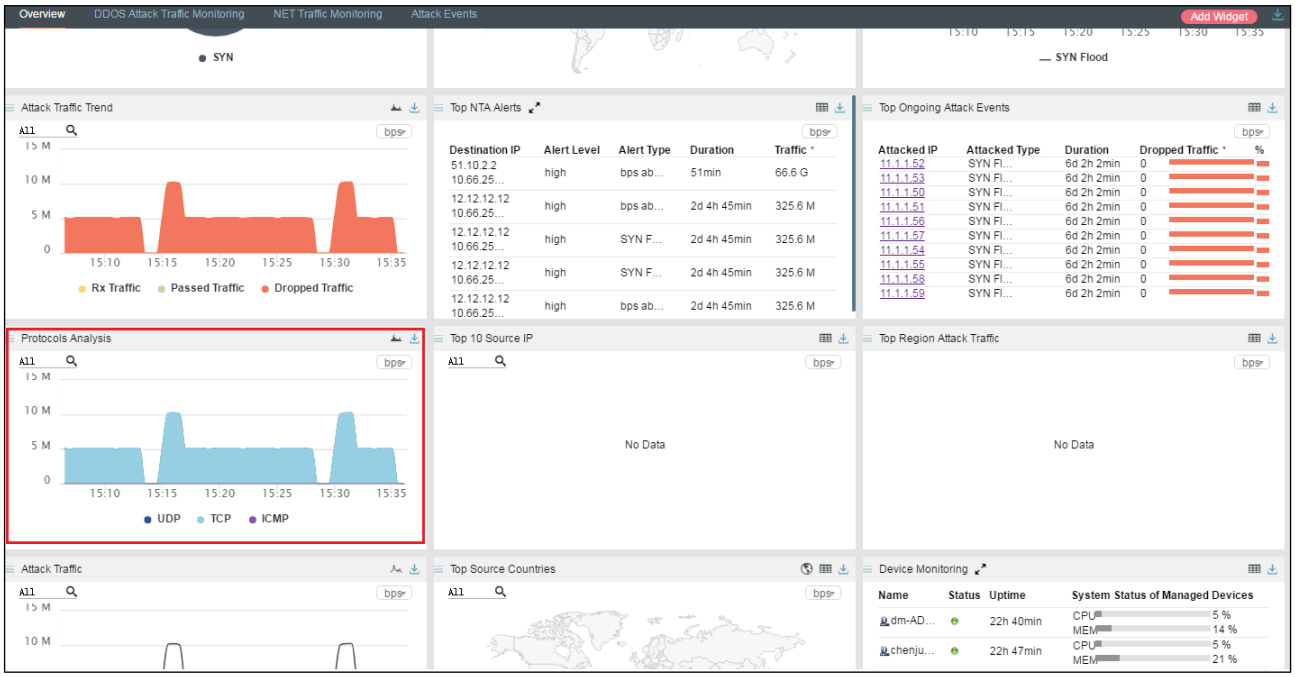
Step 2 Specify another panel to display, for example, **Protocols Analysis** under **Traffic**, as shown in Figure 4-5.

Figure 4-5 Specifying another panel to display



After you click the panel name, the box reverses to display the selected panel, as shown in Figure 4-6.

Figure 4-6 New panel displayed



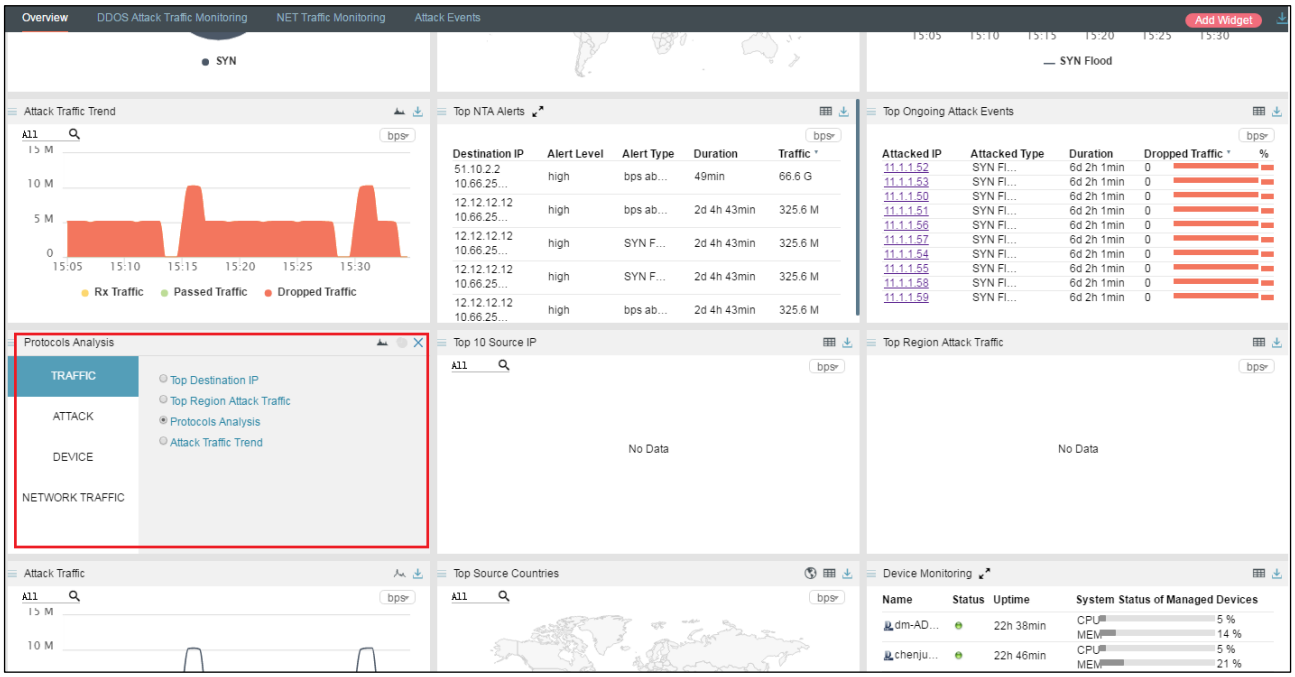
----End

4.1.3 Deleting a Panel

You can delete an unnecessary panel by performing the following steps:

Step 1 On the page shown in Figure 4-1, click in the upper-left corner of the unnecessary panel. Then the panel reverses, as shown in Figure 4-7.

Figure 4-7 Reversed panel



Step 2 Click in the upper-right corner of the panel.

Then the panel is deleted.

----End

4.1.4 Downloading a Report

You can export panel-specific reports and then download them in PDF format to a local disk drive. In addition, you can export an integrated report that provides data of all panels.

The procedure is as follows:

On the page shown in Figure 4-1, export a report of data displayed on a single panel or an integrated report of data displayed on all panels.

- Click in the upper-right corner of a panel and then data of this panel is exported as a report.
- Click in the upper-right corner of the page and then all data displayed on this page is exported as an integrated report.

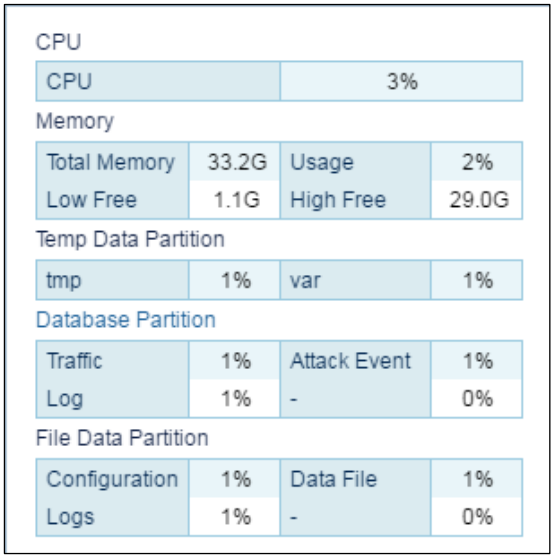
4.1.5 Viewing the System Status Bar

The system status bar at the bottom of the web-based manager displays the system service status (indicates that the device operates properly), system status (CPU usage and memory usage), and system time, as shown in Figure 4-8.

Figure 4-8 System status bar

Clicking system status information in the status bar shows details such as CPU usage, memory usage, temporary data partition, database partition, and file data partition, as shown in Figure 4-9. Clicking system status information in the status bar again will hide it.

Figure 4-9 Detailed system status information



4.1.6 Generating Sound Alerts

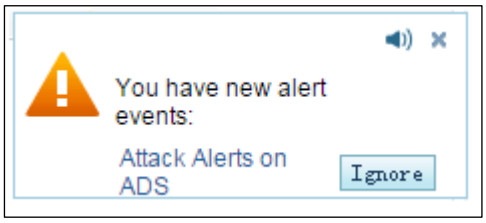
After sound alerting is enabled, the system makes a sound and displays an alert reminder box, as shown in Figure 4-10, when either of the following conditions is met:

- An attack alert or link status alert is generated by ADS.
- A traffic alert is generated by NTA.

In the box shown in this figure, you can perform the following operations:

- Click to disable sound alerting.
- Click to close this box.
- Click **Ignore** to ignore this new alert.

Figure 4-10 Sound alert



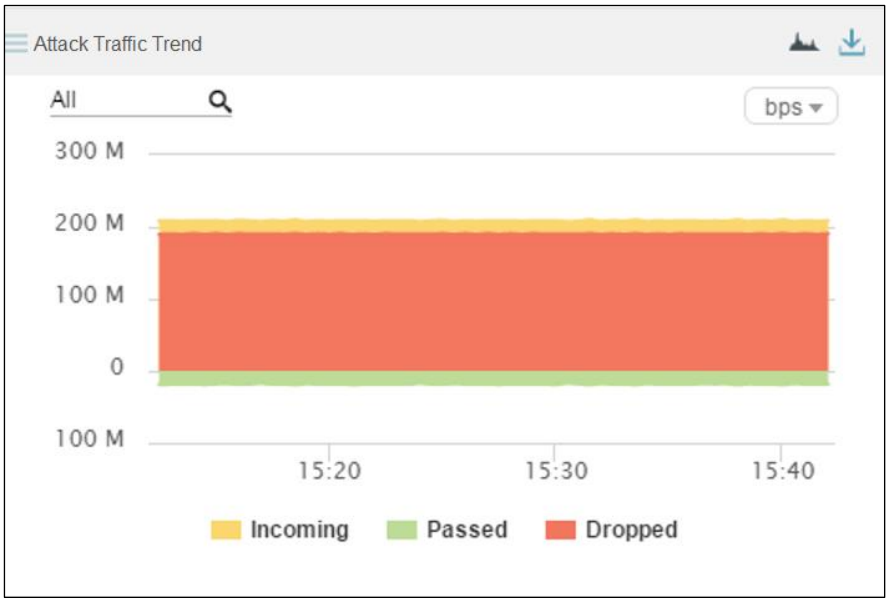
For how to disable sound alerting, see section 3.1.1 Basic Settings.

4.1.7 Viewing Attack Traffic Trends

The **Attack Traffic Trend** panel shows trends of traffic received, forwarded, and dropped by ADS in the last 30 minutes, as shown in Figure 4-11.

Data on this panel refreshes every 30 seconds.

Figure 4-11 Attack Traffic Trend panel



4.1.7.1 Understanding Data on the Panel

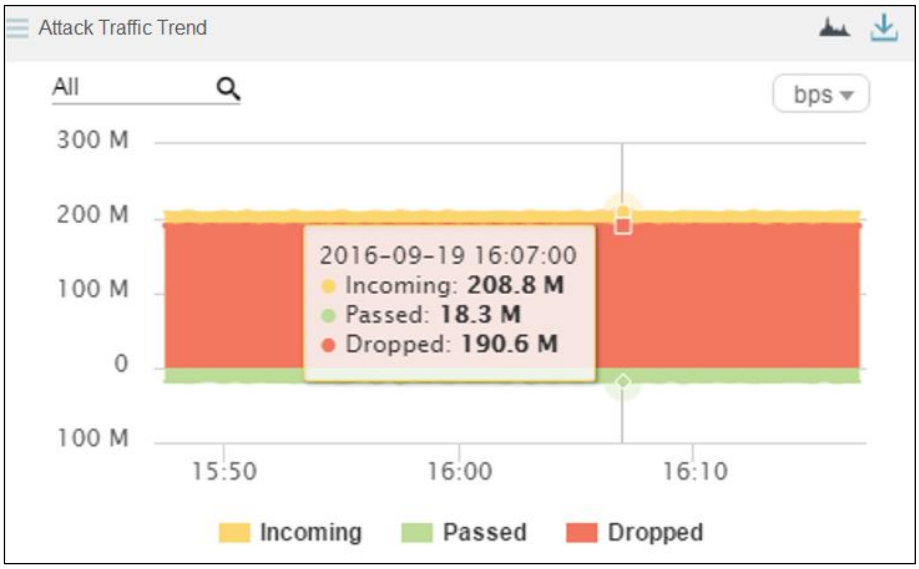
In the **Attack Traffic Trend** graph,

- The x-axis indicates time, spanning the last 30 minutes.
- The y-axis indicates traffic:
  - Traffic above 0: The yellow color indicates the total traffic received by ADS and the red color indicates dropped traffic.
  - Traffic below 0: The green color indicates legitimate traffic allowed by ADS to pass through.

4.1.7.2 Viewing Traffic at a Random Point of Time

Pointing to a random point in the **Attack Traffic Trend** graph displays the specific time and values of incoming traffic, forwarded traffic, and dropped traffic, as shown in Figure 4-12.

Figure 4-12 Detailed traffic information at a specific point of time



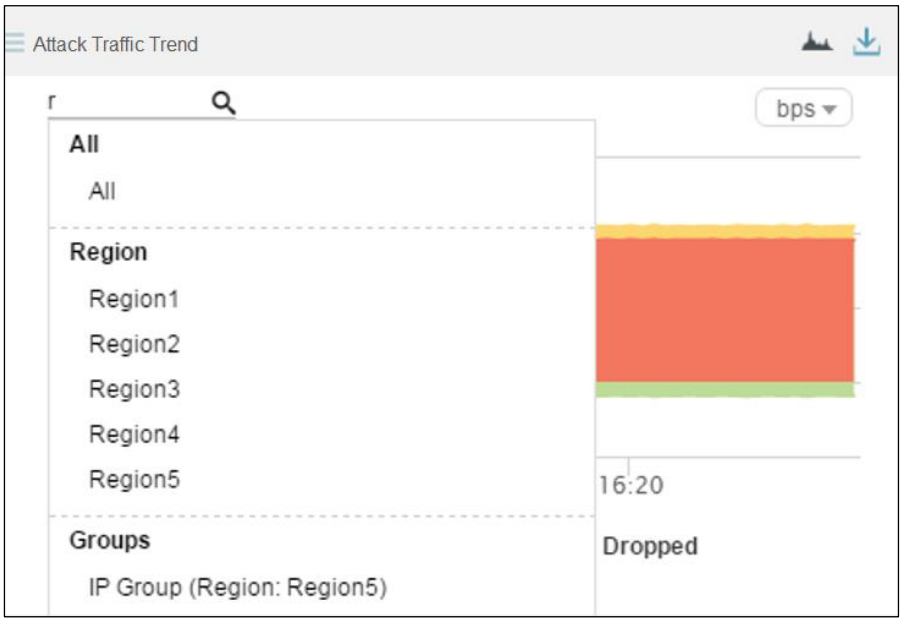
4.1.7.3 Viewing Traffic of a Specified Object

By default, the **Attack Traffic Trend** graph presents trends of traffic handled by all ADS devices. You can view real-time traffic trends of a specified region, regional IP group, ADS device, ADS-protected group, or IPv4/IPv6 address.

Step 1 On the page shown in Figure 4-12, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-13.

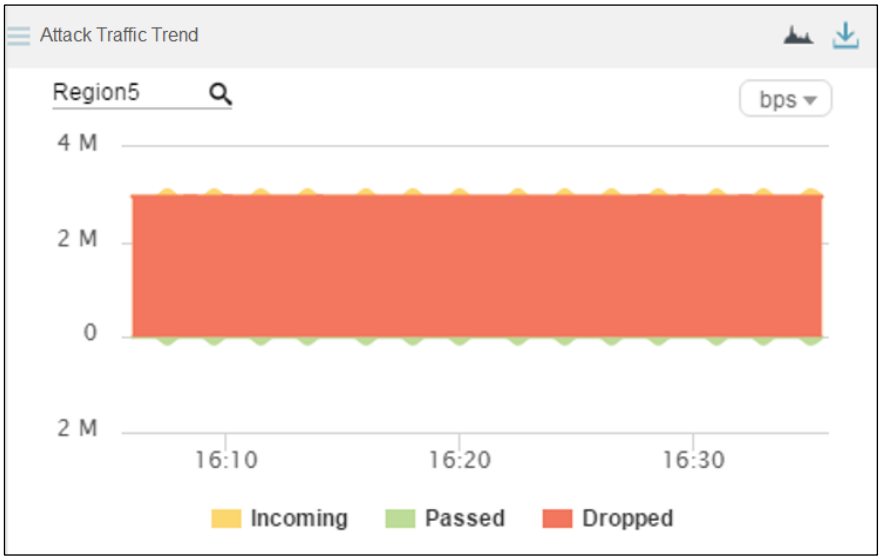
Figure 4-13 Searching for an object



Step 2 Select an object and press **Enter**.

Traffic trends of the specified object are displayed, as shown in Figure 4-14.

Figure 4-14 Real-time traffic trends of a specified object

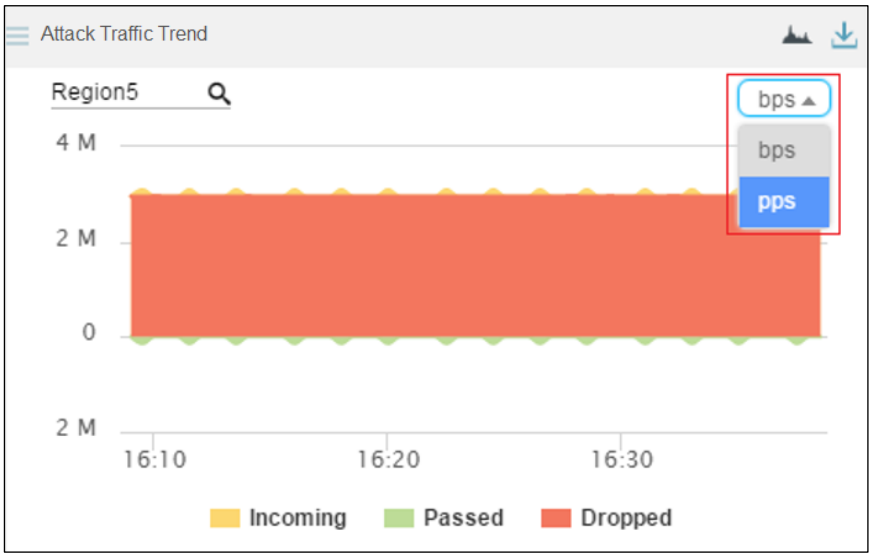


----End

4.1.7.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic Trend** panel to display traffic data in pps, as shown in Figure 4-15.

Figure 4-15 Switching the traffic unit



4.1.7.5 Downloading a Report

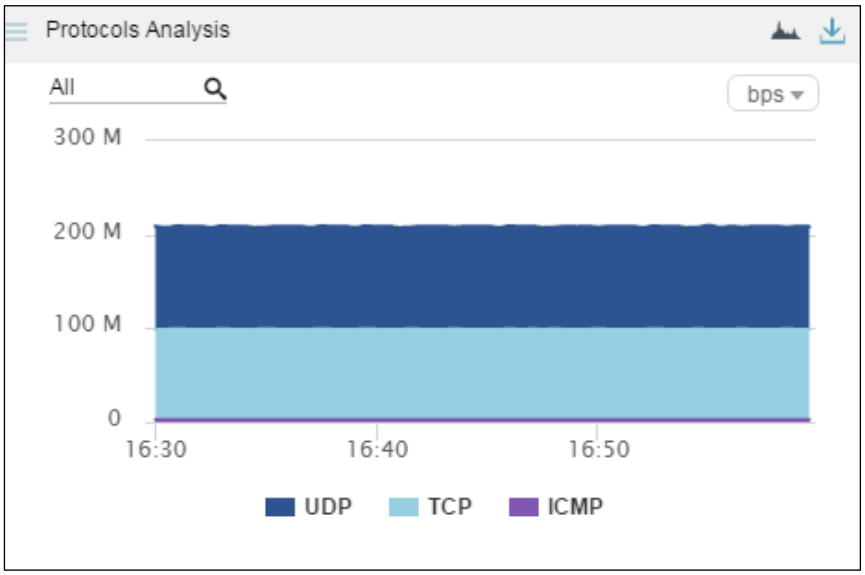
Click in the upper-right corner of the **Attack Traffic Trend** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.8 Viewing Protocol-Specific Traffic

The **Protocols Analysis** panel provides an overview of TCP, UDP, and ICMP traffic handled by ADS in the last 30 minutes as well as details about each type of traffic, as shown in Figure 4-16.

Data on this panel refreshes every 30 seconds.

Figure 4-16 Protocols Analysis panel



4.1.8.1 Understanding Data on the Panel

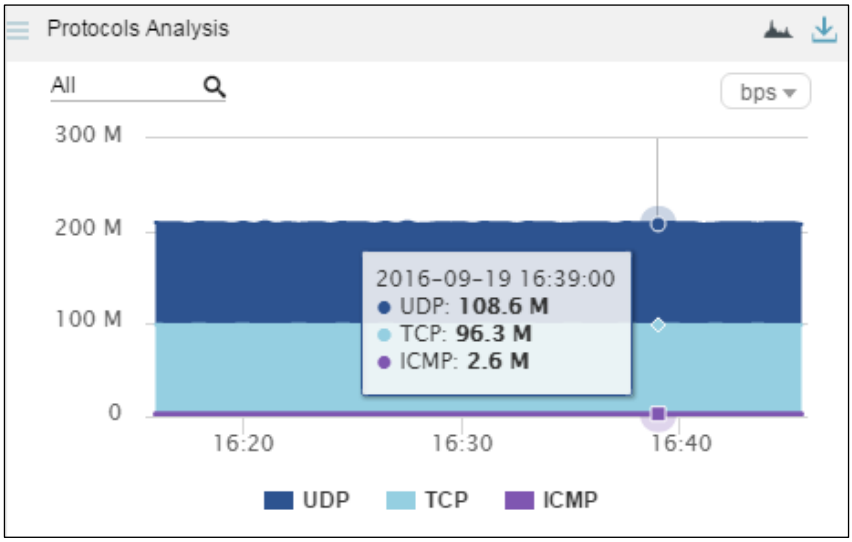
In the **Protocols Analysis** graph,

- The x-axis indicates time, spanning the last 30 minutes.
- The y-axis indicates traffic. UDP, TCP, and ICMP traffic is presented in dark blue, light blue, and purple respectively.

4.1.8.2 Viewing Traffic of Different Protocols at a Random Point of Time

Pointing to a random point in the **Protocols Analysis** graph displays the time and values of UDP traffic, TCP traffic, and ICMP traffic, as shown in Figure 4-17.

Figure 4-17 Traffic of different protocols at a specific point of time



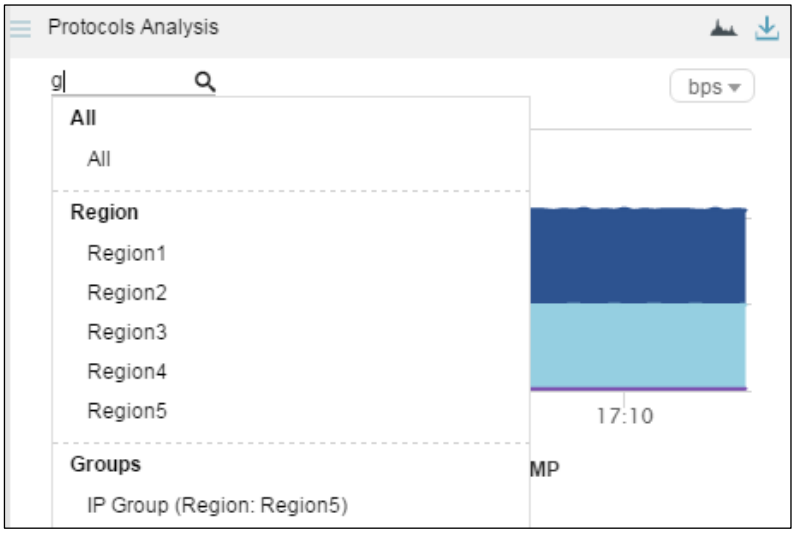
4.1.8.3 Viewing Traffic of a Specified Object

By default, the **Protocols Analysis** graph presents traffic of various protocols based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, ADS-protected group, or IPv4 or IPv6 address to view its real-time, protocol-specific traffic.

Step 1 On the page shown in Figure 4-17, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-18.

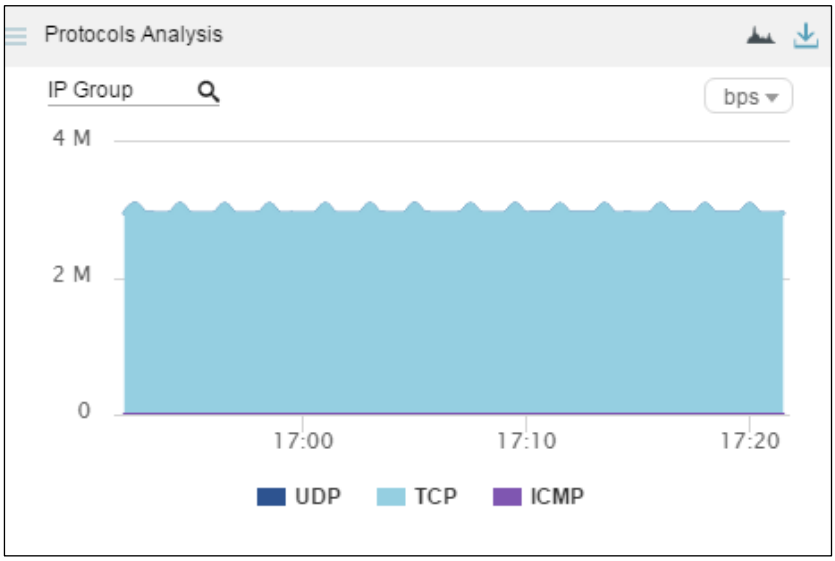
Figure 4-18 Searching for an object



Step 2 Select an object and press **Enter**.

Traffic trends of the specified object in the last 30 minutes are displayed, as shown in Figure 4-19.

Figure 4-19 Real-time traffic trends of a specified object

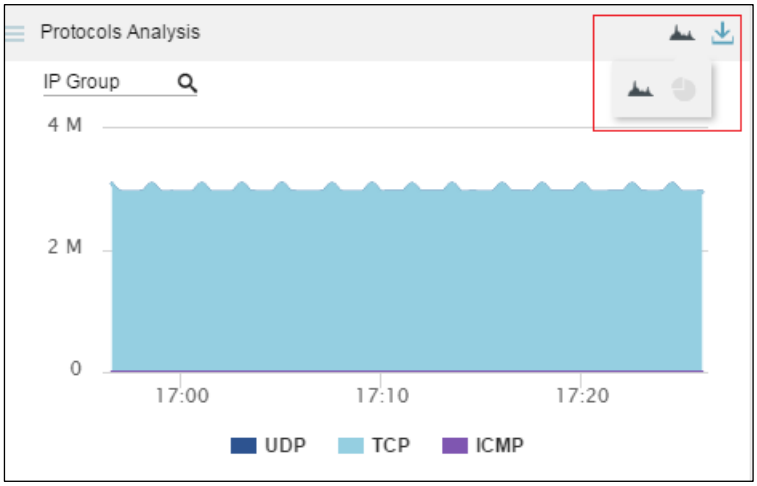


----End

4.1.8.4 Switching the Display Mode

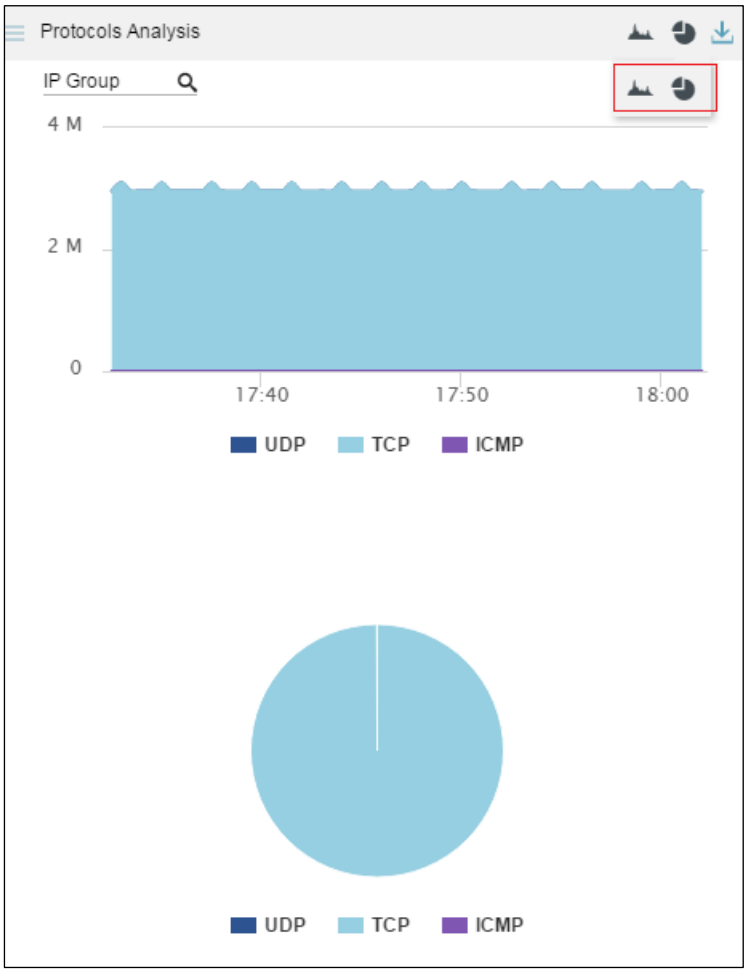
By default, protocol-specific traffic data is presented in an area graph. You can click and/or to display real-time traffic data in an area graph and/or pie chart, as shown in Figure 4-20.

Figure 4-20 Switching the display mode



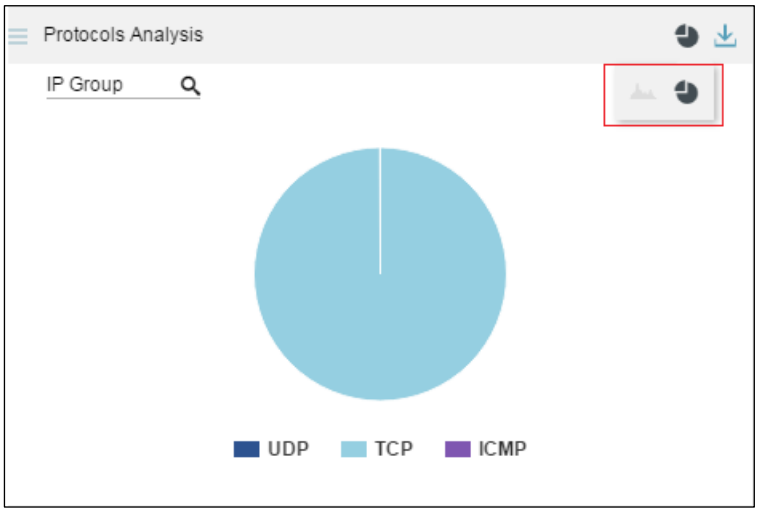
In Figure 4-20, appears normal, while appears dimmed. Therefore, data is presented only in an area graph. After you click , this icon turns . In this case, traffic data is presented in both an area graph and pie chart, as shown in Figure 4-21.

Figure 4-21 Display of traffic data in an area graph and pie chart



Clicking makes this icon dimmed and hides the area graph, as shown in Figure 4-22.

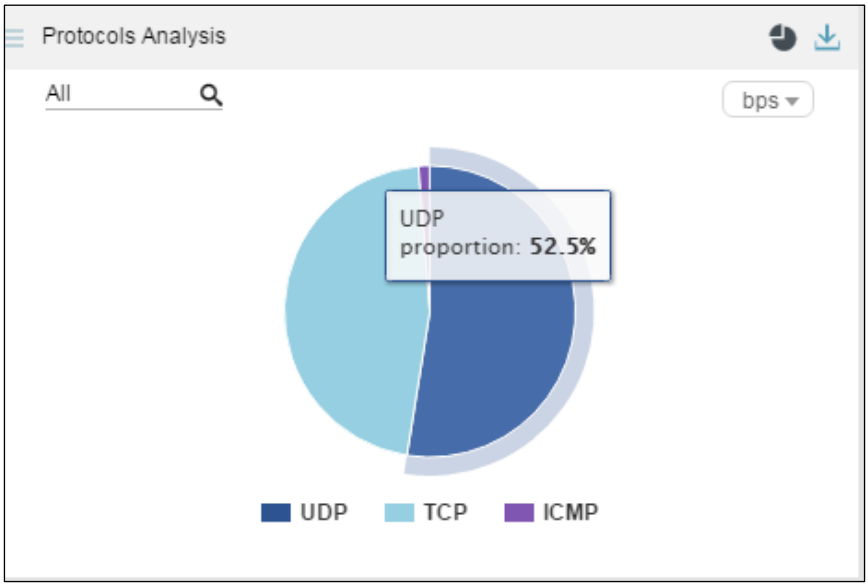
Figure 4-22 Display of traffic data in a pie chart



4.1.8.5 Viewing the Percentage of Protocol-Specific Traffic

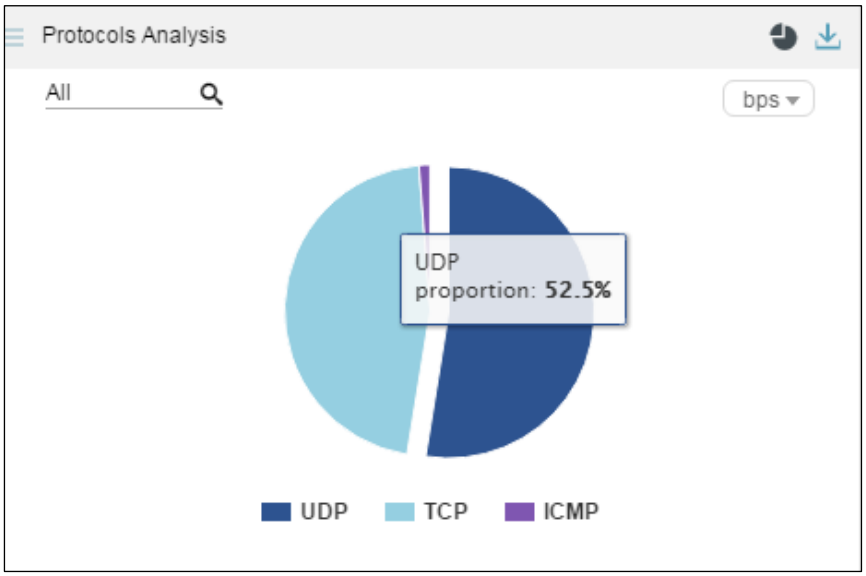
Pointing to a random point in the pie chart displays the protocol name and the percentage of protocol-specific traffic to the total traffic, as shown in Figure 4-23.

Figure 4-23 Percentage of protocol-specific traffic



Clicking in this area separates this area from other areas, as shown in Figure 4-24.

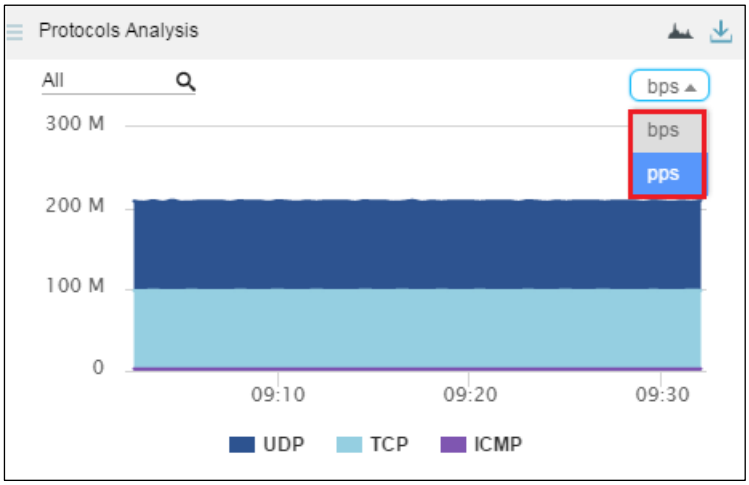
Figure 4-24 Area representing traffic of a protocol separated from other areas



4.1.8.6 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Protocols Analysis** panel to display traffic data in pps, as shown in Figure 4-25.

Figure 4-25 Switching the traffic unit



4.1.8.7 Downloading a Report

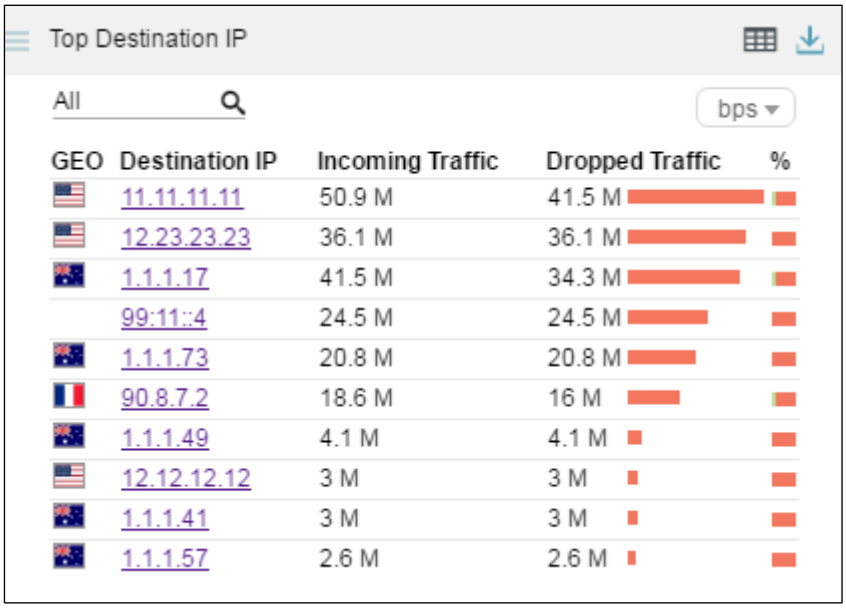
Click in the upper-right corner of the **Protocols Analysis** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.9 Viewing Traffic of Top Destination IP Addresses

The **Top Destination IP** panel displays in real time top 10 destination IP addresses with the largest traffic dropped by ADS in the last 30 seconds, letting users know which IP addresses see the largest traffic or are most severely attacked, as shown in Figure 4-26.

Data on this panel refreshes every 30 seconds.

Figure 4-26 Top Destination IP panel

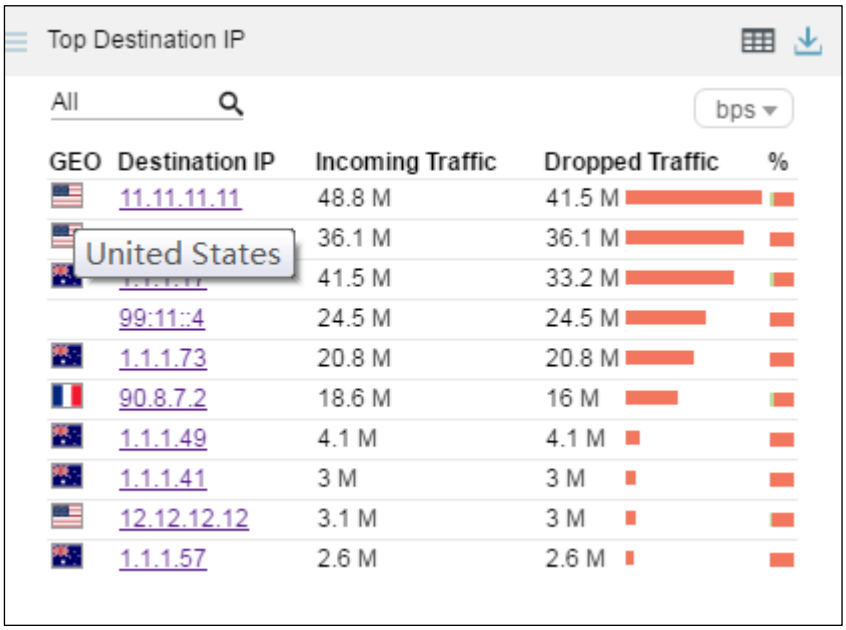


4.1.9.1 Understanding Data on the Panel

The list ranks top 10 destination IP addresses according to traffic dropped by ADS in the last 30 seconds.

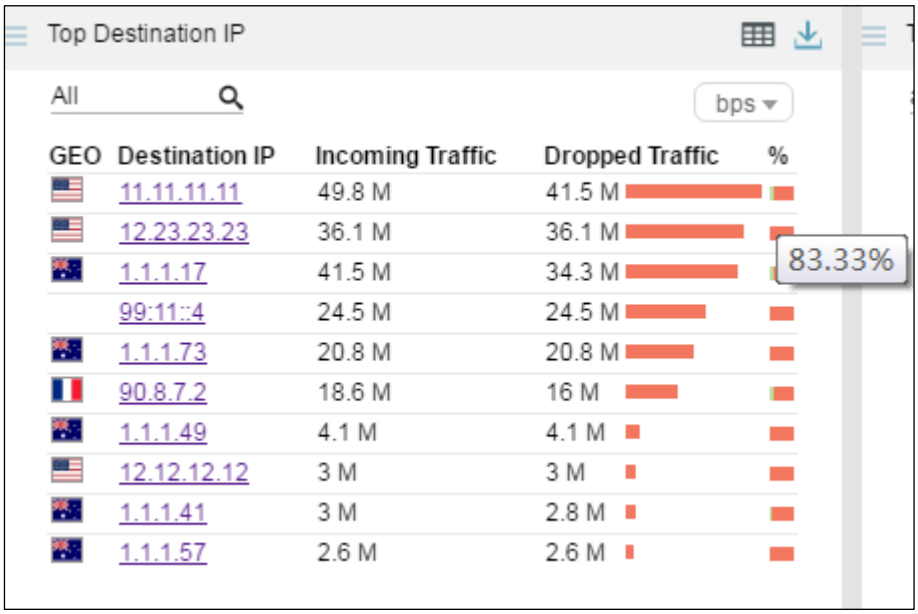
- **GEO**: shows the national flag icons. Pointing to a national flag displays the corresponding country name, as shown in Figure 4-27.

Figure 4-27 Display of the country name



- **Destination IP**: shows destination IP addresses. Clicking an IP address opens the **Traffic Monitoring** tab page, where you can view more details about traffic destined for this IP address. For details, see section 4.1.9.2 Viewing Comprehensive Traffic Information of a Specified Object.
- **Incoming Traffic**: shows the value of traffic received by ADS in the last 30 seconds.
- **Dropped Traffic**: shows the value of traffic dropped by ADS in the last 30 seconds. The red bar to the right of the traffic value indicates the volume of dropped traffic. A longer bar indicates more traffic dropped.
- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. When you point to a bar in this column, the specific percentage is displayed. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-28, the percentage of dropped traffic for 11.11.11.11 is 83.33%.

Figure 4-28 Percentage of dropped traffic to incoming traffic



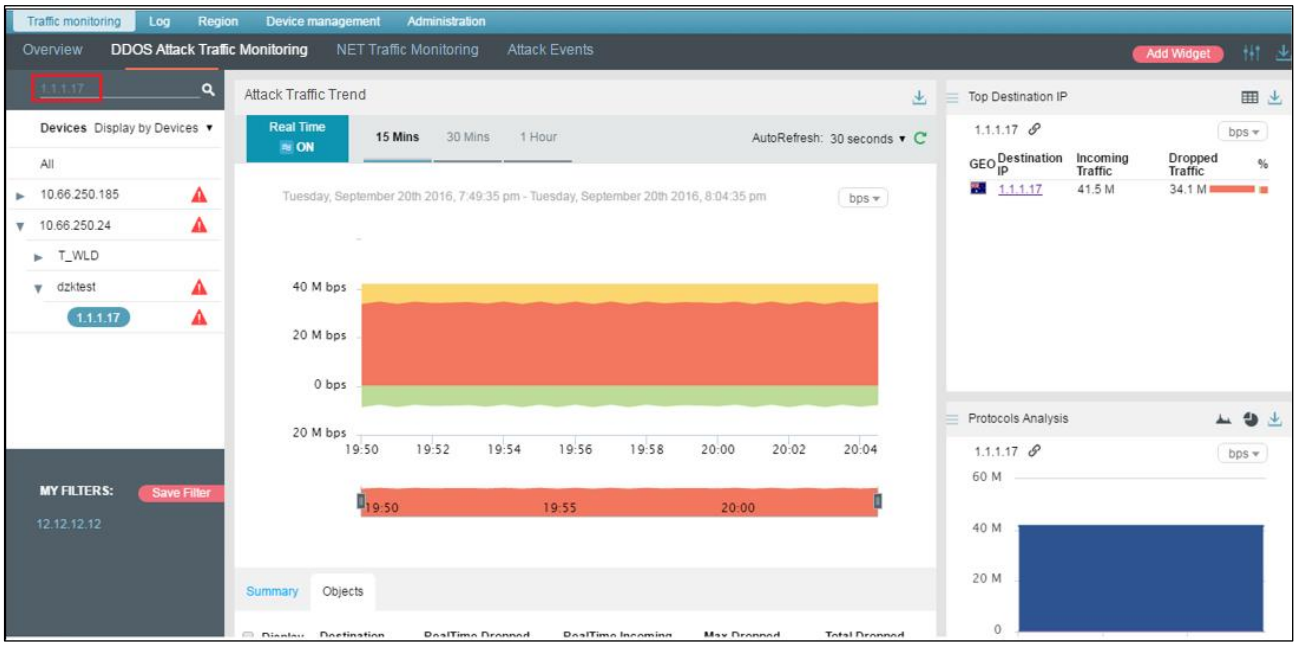
4.1.9.2 Viewing Comprehensive Traffic Information of a Specified Object

You can conveniently view comprehensive traffic information of a top 10 destination IP address and that of a specified object by performing the following steps:

Step 1 On the page shown in Figure 4-28, click an IP address, for example, 1.1.1.17.

The **DDOS Attack Traffic Monitoring** page is displayed, with the IP address in question already in the search box, as shown in Figure 4-29.

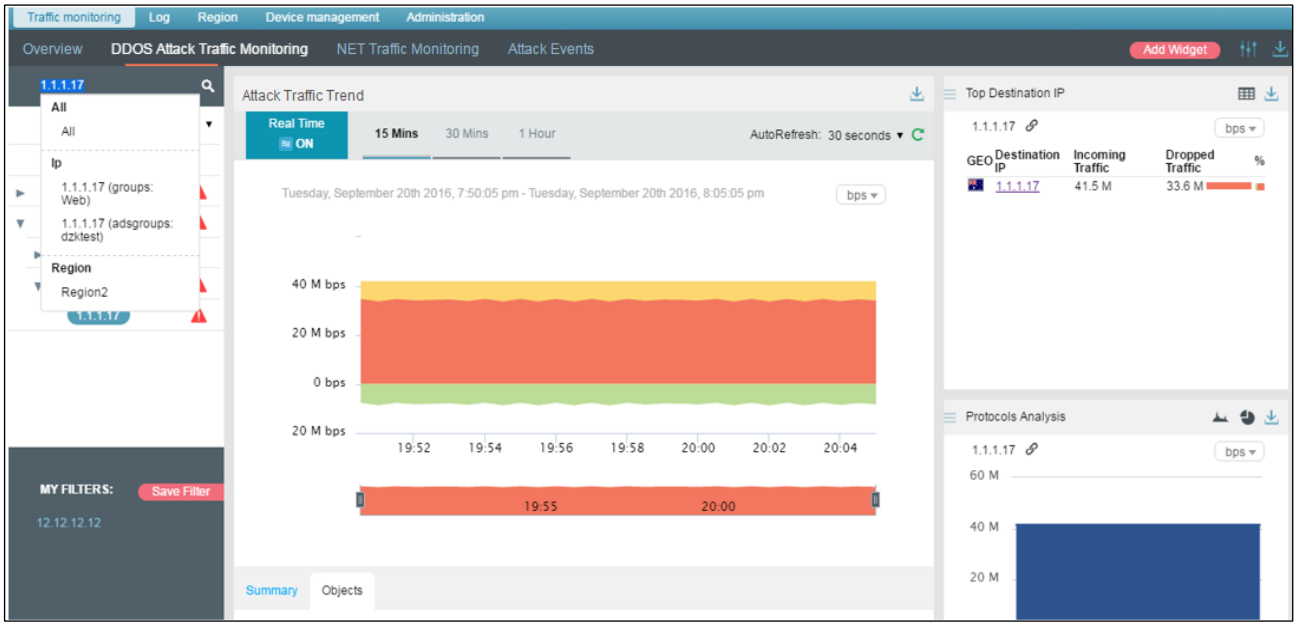
Figure 4-29 Traffic of a specific IP address



Step 2 Click in the search box.

The system displays all objects containing the current IP address, as shown in Figure 4-30.

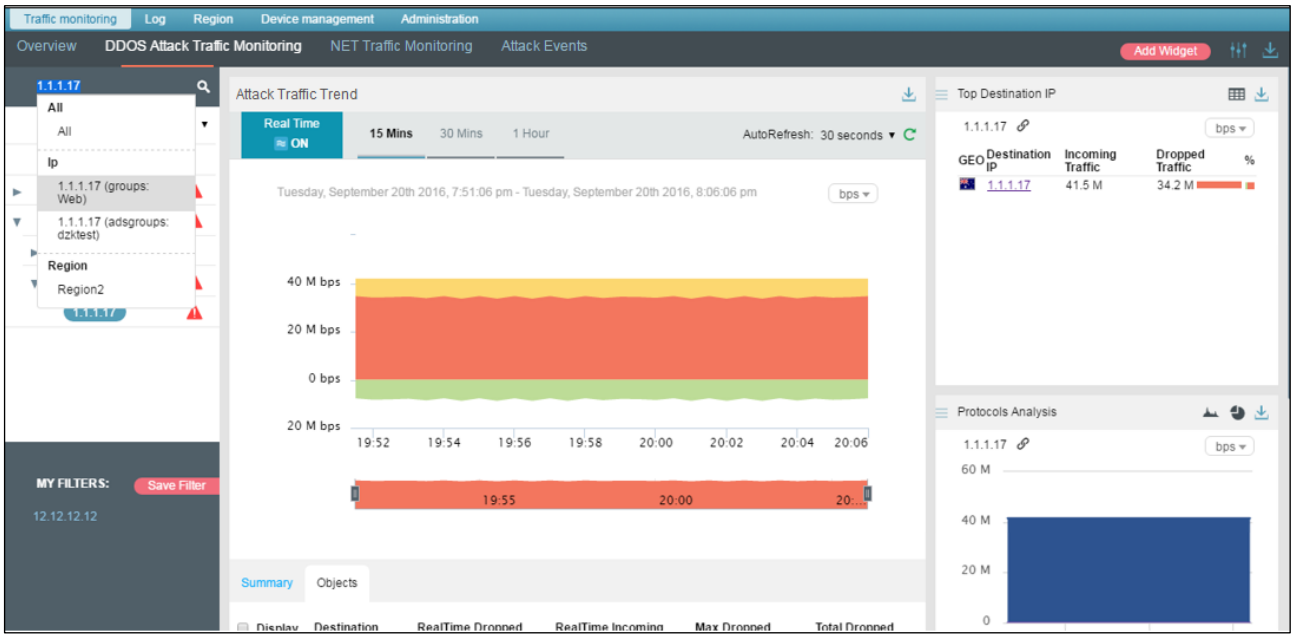
Figure 4-30 Searching for objects containing the current IP address



Step 3 Select an object and press **Enter**.

Comprehensive traffic information of the specified object is displayed, as shown in Figure 4-31.

Figure 4-31 Viewing traffic information of a specified object



----End

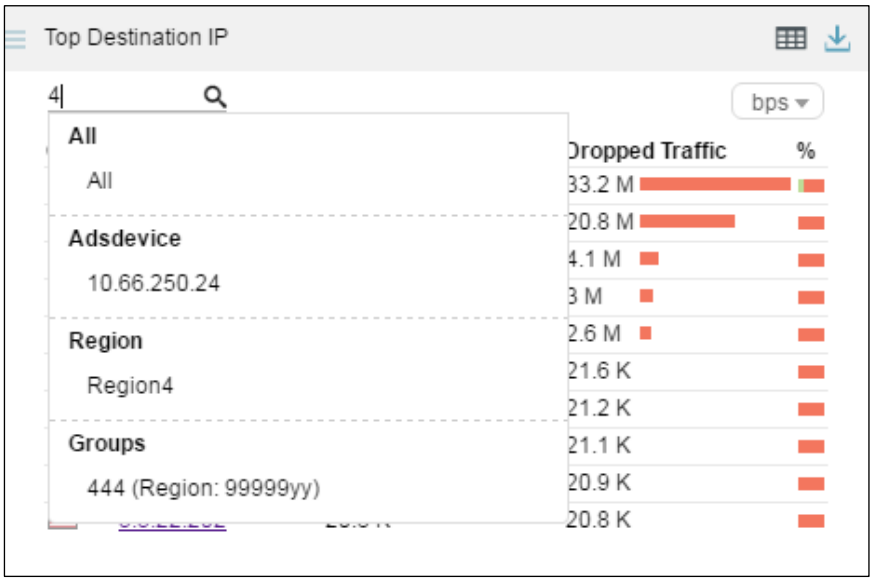
4.1.9.3 Viewing Top Destination IP Addresses of a Specified Object

By default, the **Top 10 Destination IP** panel presents top 10 destination IP addresses based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, or ADS-protected group to view its top destination IP addresses ranked according to traffic dropped in the last 30 minutes. You can also specify a destination IPv4 or IPv6 address to view its traffic information in the last 30 minutes.

Step 1 On the page shown in Figure 4-26, type a character string and then press **Enter**.

The system automatically displays all objects containing the typed character string, as shown in Figure 4-32.

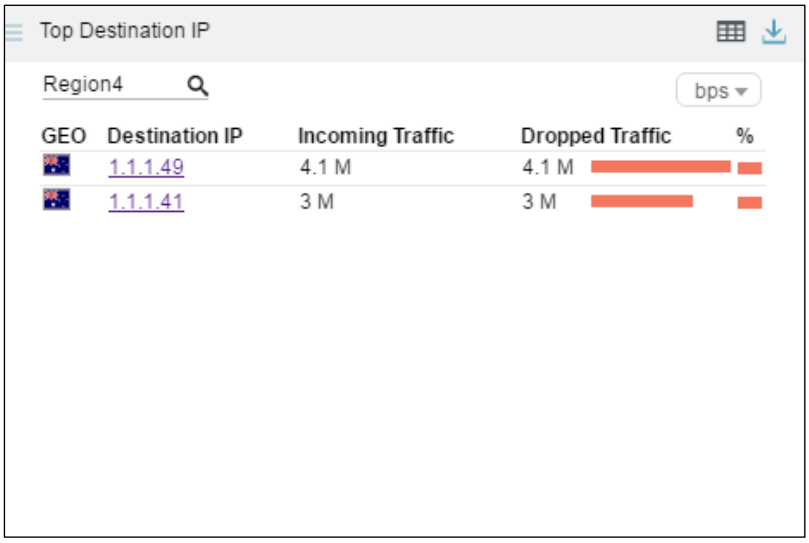
Figure 4-32 Searching for an object



Step 2 Select an object and press **Enter**.

Then destination IP addresses associated with the specified object are displayed, ranked in descending order of traffic dropped by ADS in the last 30 minutes.

Figure 4-33 Top destination IP addresses associated with a specified object



----End

4.1.9.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Destination IP** panel to display traffic data in pps.

4.1.9.5 Downloading a Report

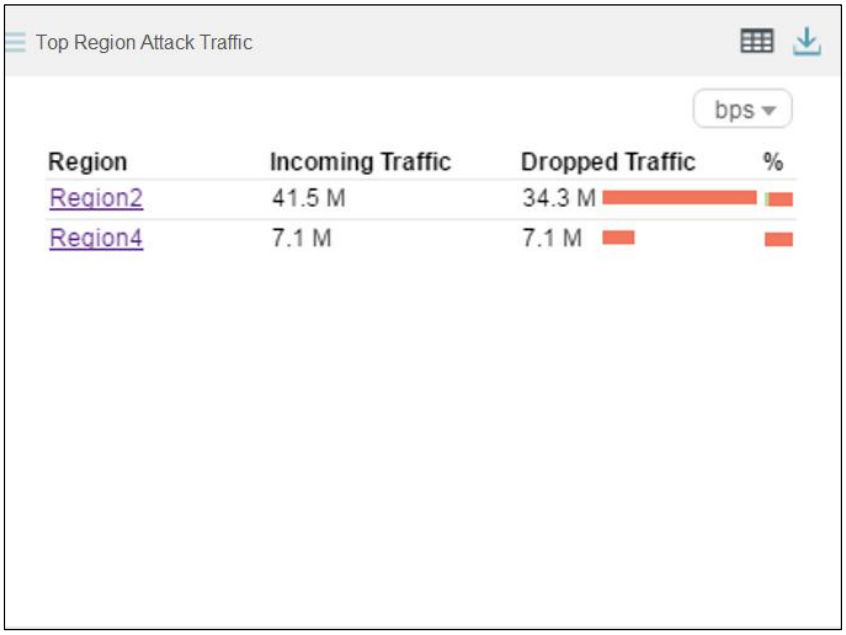
Click in the upper-right corner of the **Top Destination IP** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.10 Viewing Attack Traffic of Top Regions

The **Top Region Attack Traffic** panel presents in real time top 10 regions with the largest traffic dropped by ADS in the last 30 seconds, as shown in Figure 4-34, letting users know which regions see the largest traffic or are most severely attacked.

Data on this panel refreshes every 30 seconds.

Figure 4-34 Top Region Attack Traffic panel

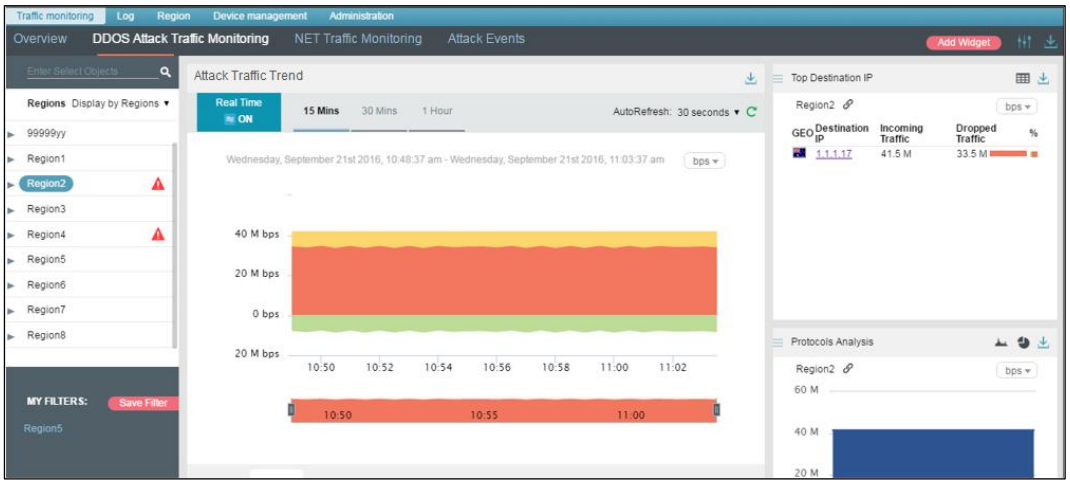


4.1.10.1 Understanding Data on the Panel

The list ranks top 10 regions according to traffic dropped by ADS in the last 30 seconds.

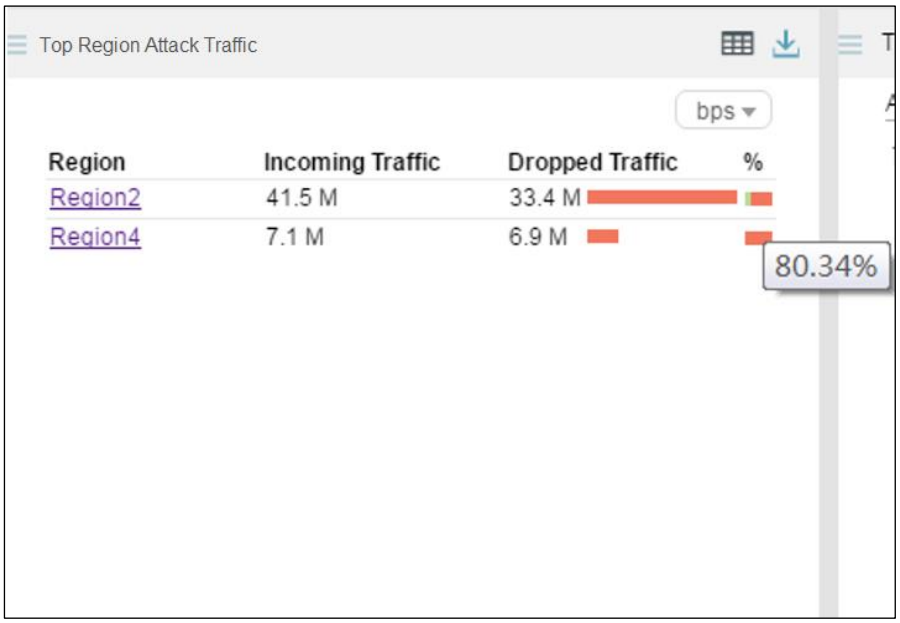
- **Region**: region for which traffic is dropped by ADS. Clicking a region name, for example, **Region2**, opens the **Traffic Monitoring** tab page, where you can view more details about traffic destined for this region, as shown in Figure 4-35.

Figure 4-35 Traffic of a specific region



- **Incoming Traffic**: shows the value of traffic received by ADS in the last 30 seconds.
- **Dropped Traffic**: shows the value of traffic dropped by ADS in the last 30 seconds. The red bar to the right of the traffic value indicates the volume of dropped traffic. A longer bar indicates more traffic dropped.
- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. When you point to a bar in this column, the specific percentage is displayed. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-36, the percentage of dropped traffic for Region2 is 80.34%.

Figure 4-36 Percentage of dropped traffic for a specific region



4.1.10.2 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Region Traffic** panel to display traffic data in pps.

4.1.10.3 Downloading a Report

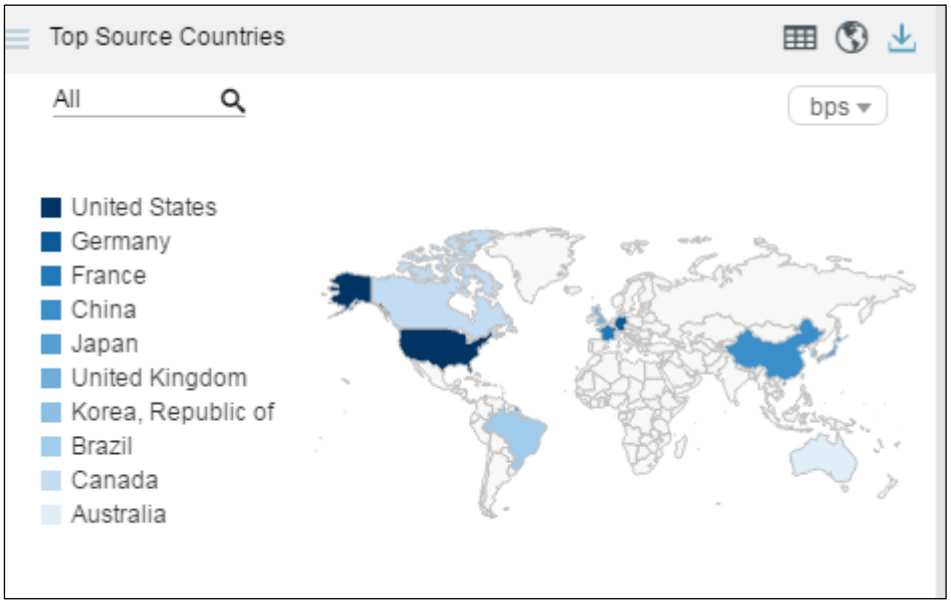
Click in the upper-right corner of the **Top Region Traffic** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.11 Viewing Traffic of Top Source Countries

The **Top Source Countries** panel presents in real time top 10 source countries/regions with the largest attack traffic dropped by ADS in the last 30 seconds, as shown in Figure 4-37.

Data on this panel refreshes every 30 seconds.

Figure 4-37 Top Source Countries panel

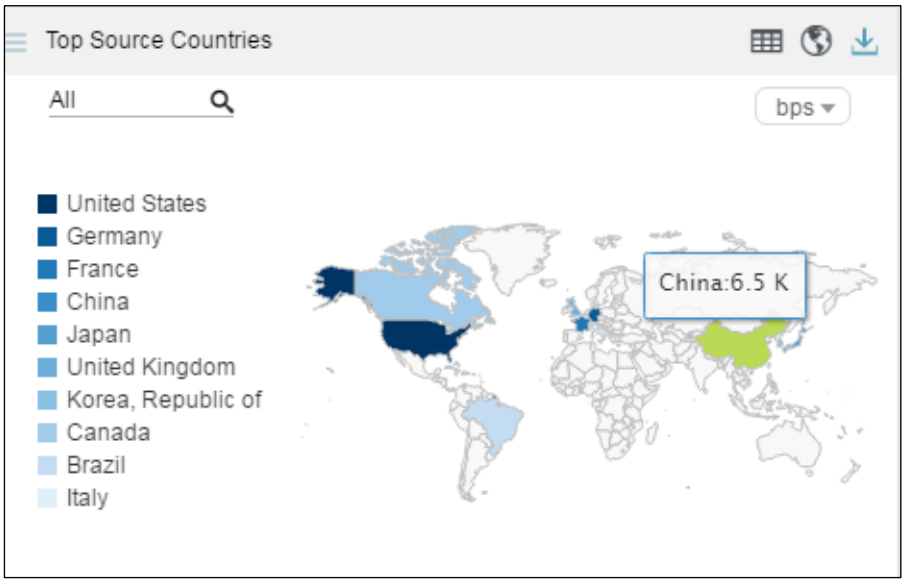


4.1.11.1 Understanding Data Displayed in a Map

Top 10 source countries are ranked on the left according to attack traffic handled by ADS, indicated with a color that shades from dark blue to very light blue. On the right, areas of these countries are indicated in a map with the same colors.

Pointing to the area of a top 10 country changes its color to green and displays the country name and the value of traffic dropped by ADS, as shown in Figure 4-38.

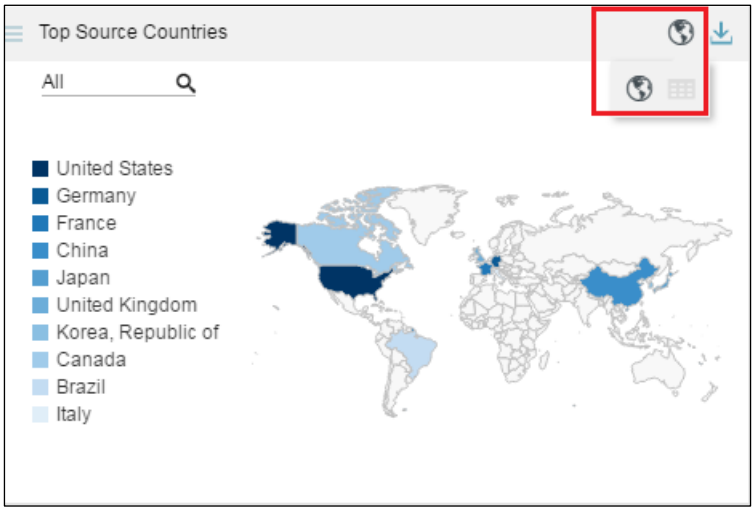
Figure 4-38 Display of the value of attack traffic from a country



4.1.11.2 Switching the Display Mode

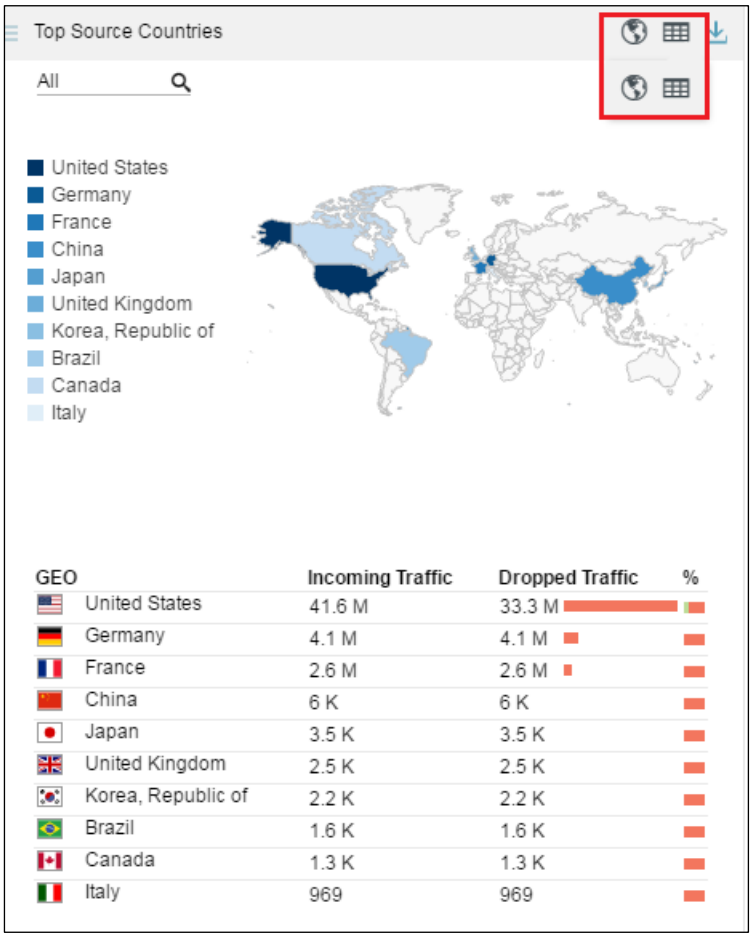
By default, traffic of top 10 source countries is presented in a map of the world. You can click in the upper-right corner of the **Top Source Countries** panel to choose a display mode (list or map) or both modes, as shown in Figure 4-39.

Figure 4-39 Switching the display mode



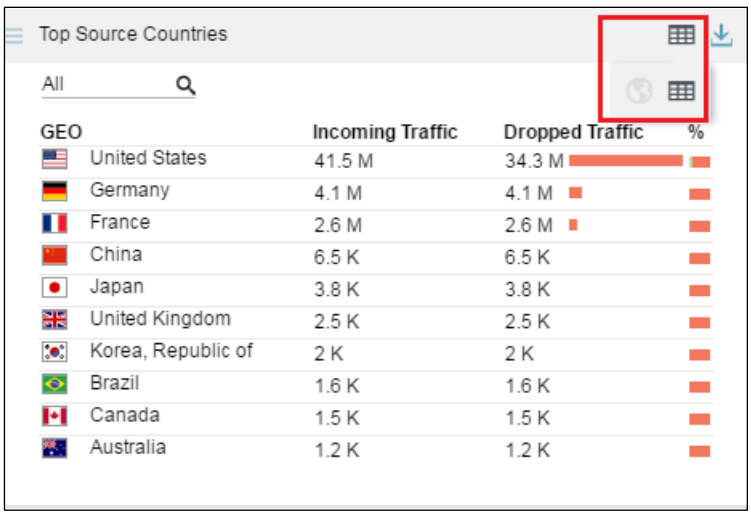
In Figure 4-39, appears normal, while appears dimmed. Therefore, data is presented only in a map. After you click , this icon turns . In this case, traffic data is presented in both a map and a list, as shown in Figure 4-40.

Figure 4-40 Display of traffic data in both a map and a list



Clicking makes this icon dimmed and hides the map, as shown in Figure 4-41.

Figure 4-41 Display of traffic data only in a list

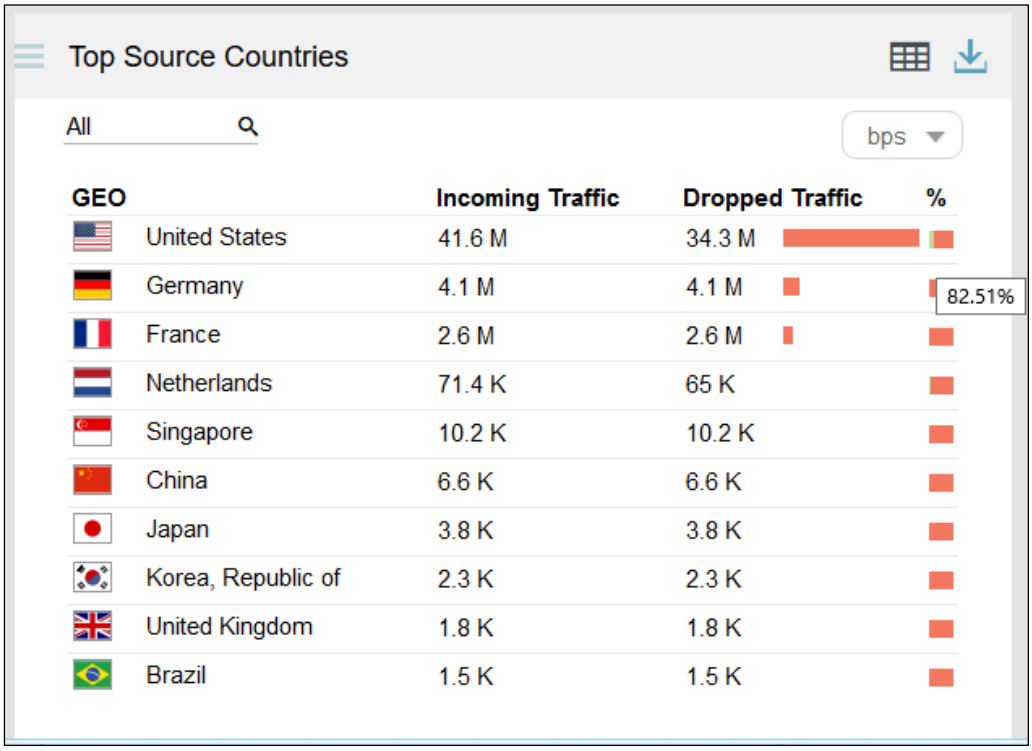


4.1.11.3 Viewing the List of Top Source Countries

The list ranks top 10 countries according to traffic dropped by ADS in the last 30 seconds.

- **GEO**: shows national flag icons. Pointing to an icon displays the country name, as shown in Figure 4-27.
- **Incoming Traffic**: shows the traffic received by ADS from a country in the last 30 seconds.
- **Dropped Traffic**: shows the traffic dropped by ADS for the country in the last 30 seconds. The red bar to the right of the traffic value also indicates the dropped traffic. A longer bar indicates more traffic dropped.
- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. Pointing to a bar in this column displays a specific percentage. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-42, the percentage of dropped traffic for United States is 82.51%.

Figure 4-42 Percentage of dropped traffic of a source country

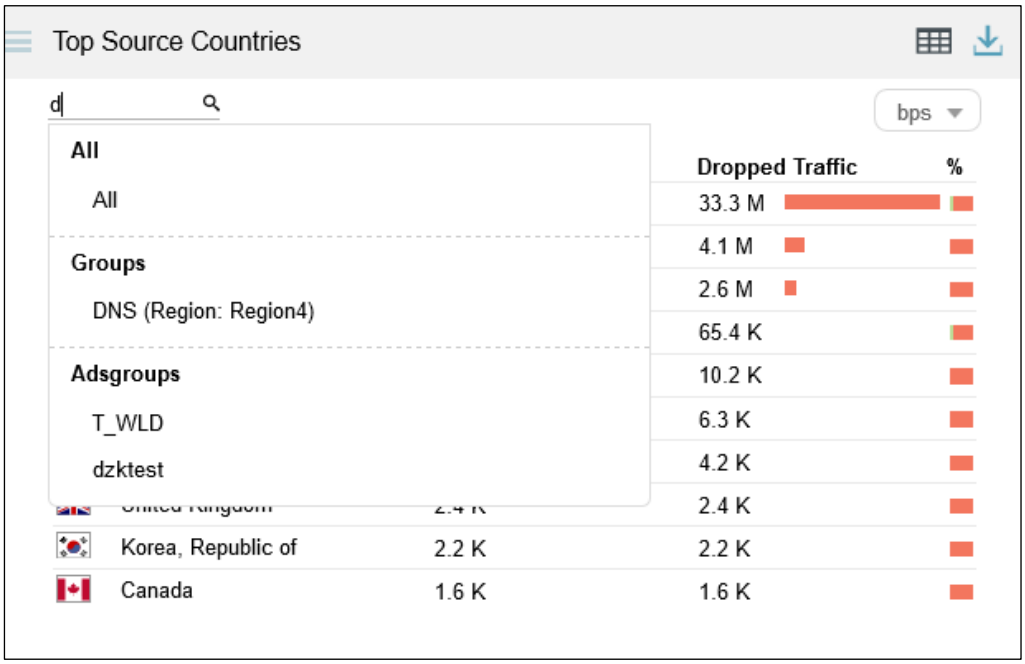


4.1.11.4 Viewing Top Source Countries Associated with a Specified Object

By default, the **Top Source Countries** panel presents top 10 source countries based on data collected from all ADS devices. You can specify a region, region IP group, ADS device or ADS-protected group, or IPv4 or IPv6 address to view its top 10 source countries ranked according to traffic dropped by all ADS devices in the last 30 seconds.

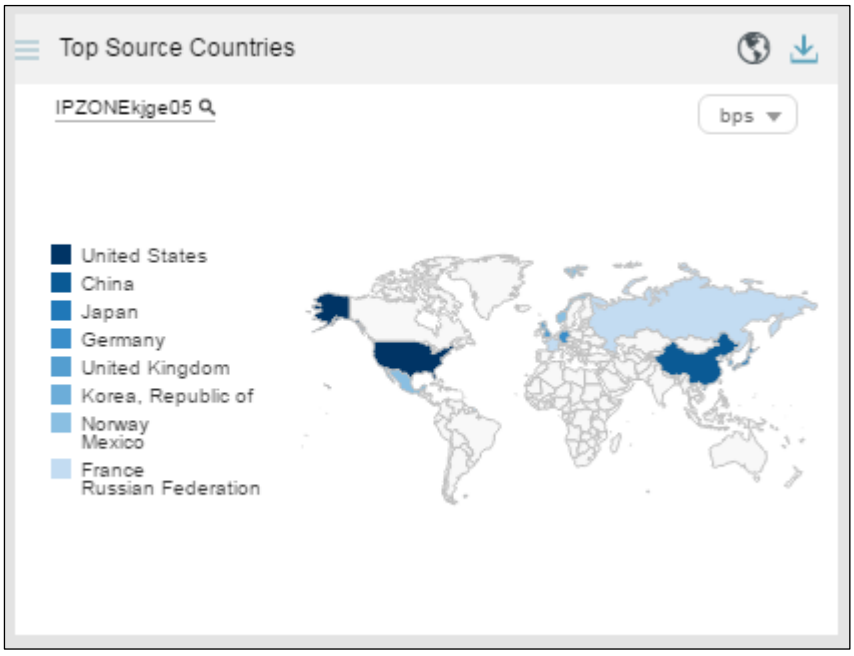
On the page shown in Figure 4-43, after you type a character string, the system displays all objects containing the typed character string.

Figure 4-43 Searching for a specific object



After you click a desired object, the panel displays the traffic of top source countries associated with the object.

Figure 4-44 Traffic of top source countries associated with a specific object



4.1.11.5 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Source Countries** panel to display traffic data in pps.

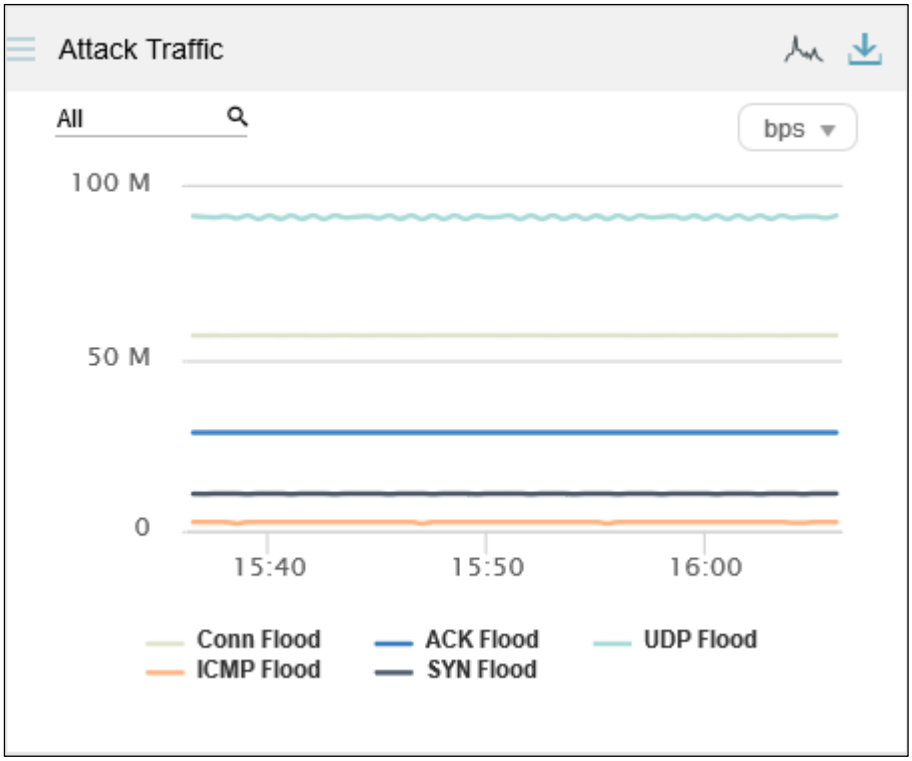
4.1.11.6 Downloading a Report

Click in the upper-right corner of the **Top Source Countries** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.12 Viewing Attack Traffic

The **Attack Traffic** panel shows the graph of attack traffic detected by ADS devices in the last 30 minutes. Data on this panel refreshes every 30 seconds.

Figure 4-45 Attack traffic



4.1.12.1 Understanding Data on the Panel

In the **Attack Traffic** graph,

- The x-axis indicates time, spanning 30 minutes.
- The y-axis indicates attack traffic. Various types of attack traffic are indicated by curves in different colors.

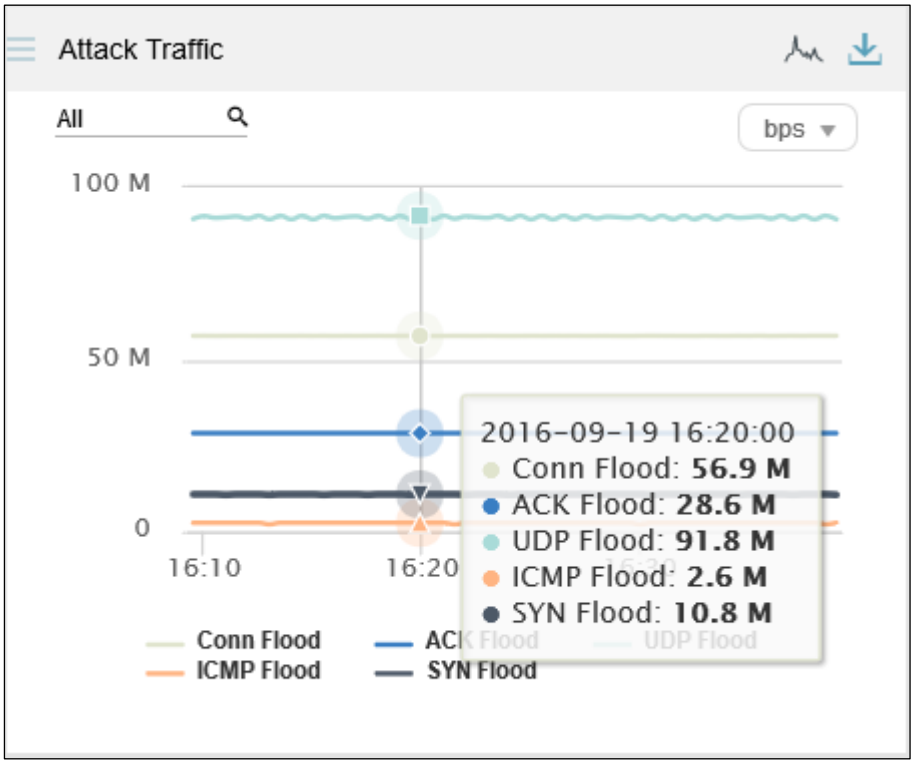
Table 4-2 Mappings between attack types and curve colors

Attack Type	Curve Color
ICMP flood attack	ICMP Flood
UDP flood attack	UDP Flood
Connection flood attack	Conn Flood
Others	Others
ACK flood attack	ACK Flood
SYN flood attack	SYN Flood

4.1.12.2 Viewing Traffic at a Specific Point of Time

Pointing to a specific time point displays the traffic of each attack type at this specific time point.

Figure 4-46 Traffic at a specific point of time



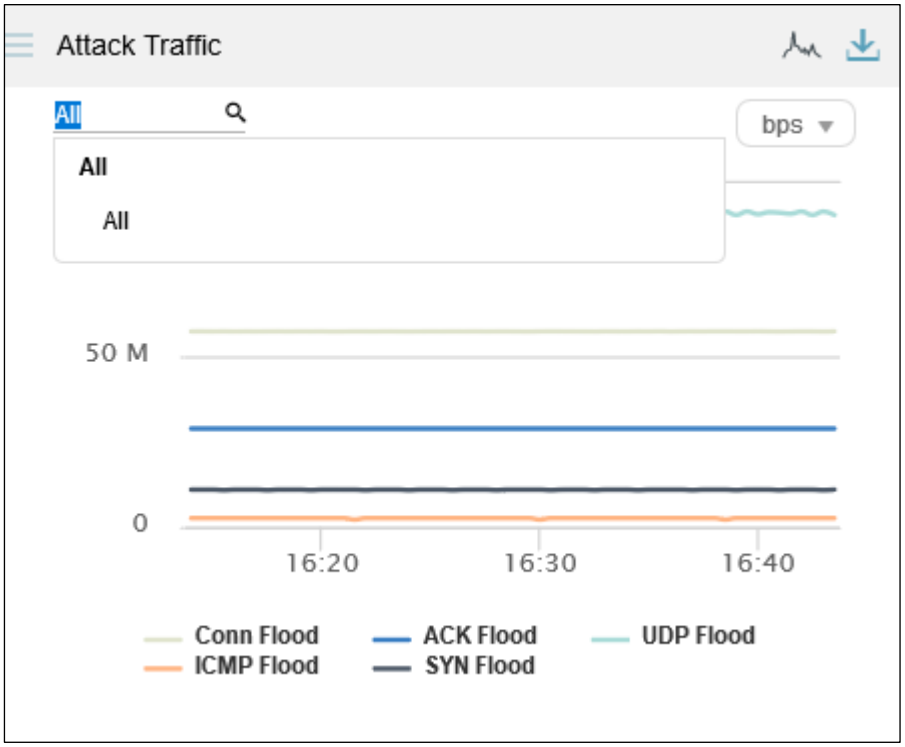
4.1.12.3 Viewing Attack Traffic of a Specified Object

By default, the **Attack Traffic** graph presents attack traffic trends detected by all ADS devices. You can specify a region, region IP group, ADS device, ADS-protected group, or IPv4 or IPv6 address to view its attack traffic trend in the last 30 minutes.

Step 1 On the page shown in Figure 4-46, type a character string.

The system displays all objects containing the typed character string.

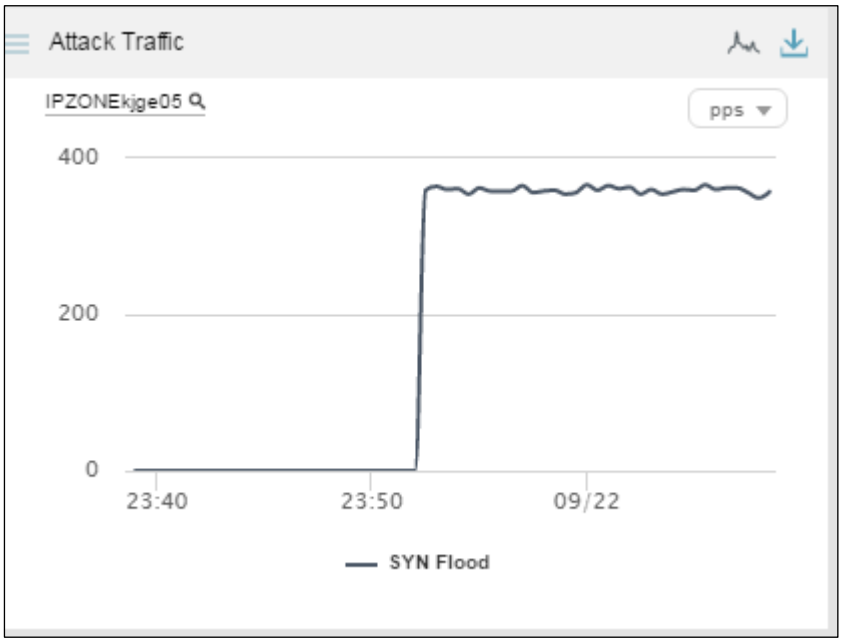
Figure 4-47 Searching for an object



Step 2 Click a desired object.

The panel displays the attack traffic trend of the object in the last 30 minutes.

Figure 4-48 Attack traffic trend of a specified object



----End

4.1.12.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic** panel to display traffic data in pps.

4.1.12.5 Downloading a Report

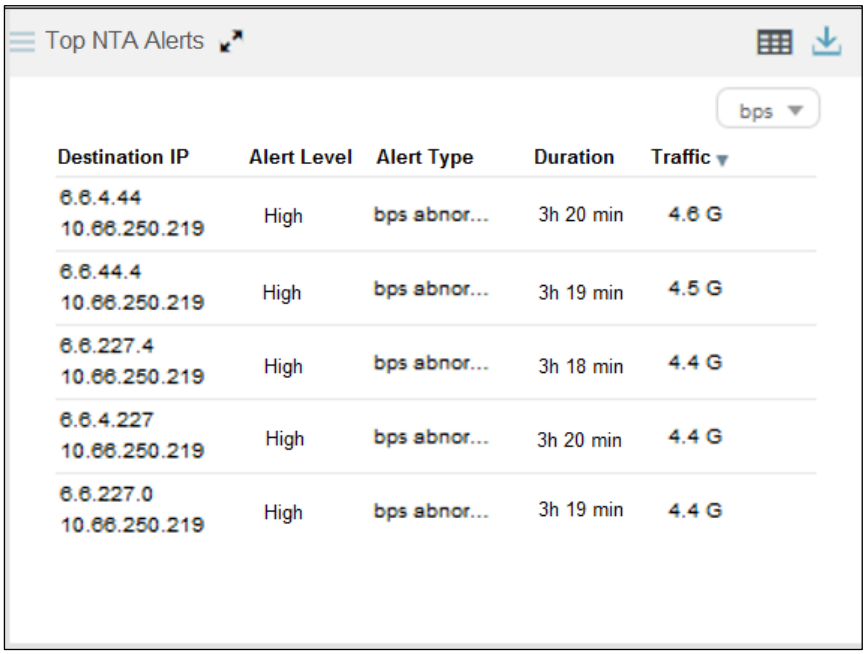
Click in the upper-right corner of the **Attack Traffic** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.13 Viewing Top Alerts Reported by NTA

The **Top NTA Alerts** panel shows top 5 traffic alerts reported by NTA devices in real time.

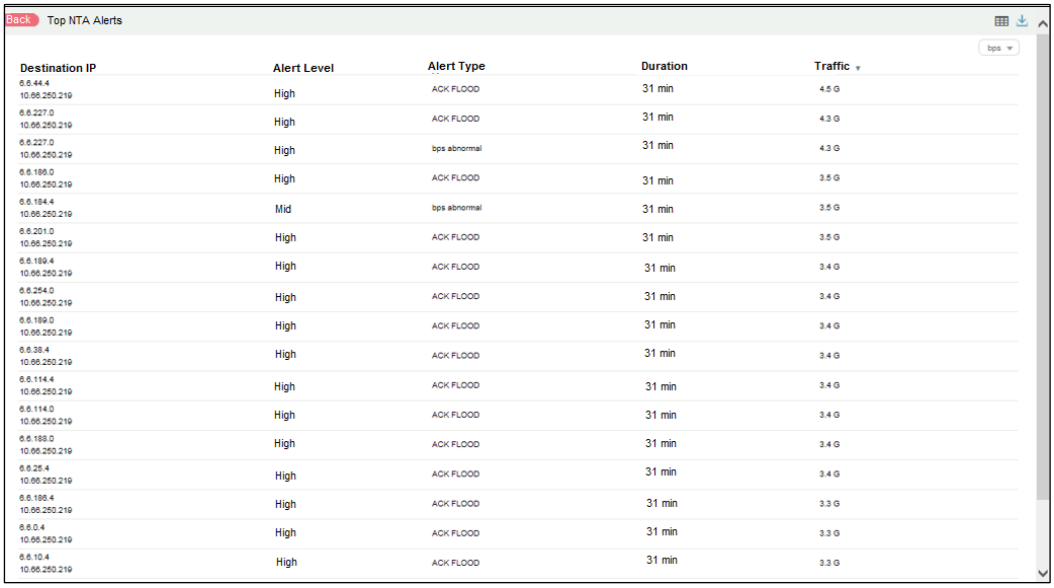
Data on this panel refreshes every 30 seconds.

Figure 4-49 Top alerts reported by NTA



Clicking displays more details about these alerts, as shown in Figure 4-50.

Figure 4-50 More details about alerts generated by NTA



4.1.13.1 Understanding Data on the Panel

The **Top NTA Alerts** panel shows top 5 alerts reported by NTA. The alert table contains the following information:

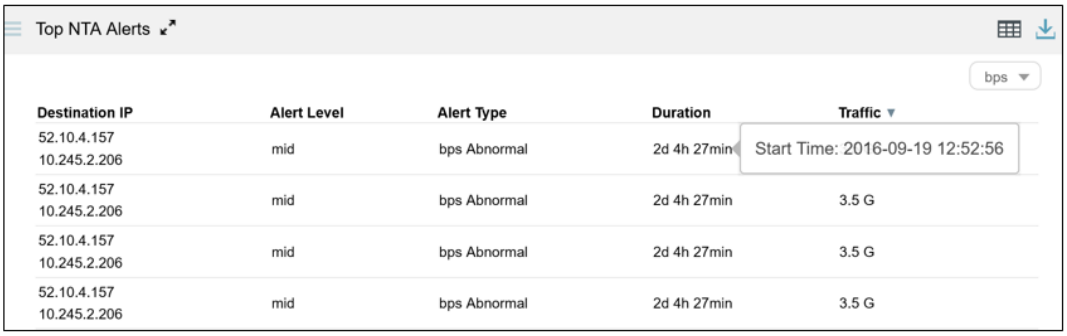
- **Destination IP**: shows the attacked destination IP address and the name of the NTA device that reports this alert.

- **Alert Level**: shows the alert level, which can be **High**, **Medium**, or **Low**. The alert level is determined by the deviation of the actual traffic value from the specified threshold. As thresholds vary with NTA devices, alert levels of these devices are determined by different deviations.
- **Alert Type**: shows the alert type, which can be one of the following:
  - **DDoS attack**: indicates that the alert is triggered when NTA detects a DDoS attack. The type of the DDoS attack is also displayed, for example, **SYN Flood**.
  - **Region traffic alert:** indicates that the alert is triggered by abnormal incoming or outgoing region traffic.
  - **IP group traffic alert**: indicates that the alert is triggered by abnormal traffic received or sent by an IP group.

Note	For details about alert levels and alert types of NTS, see the corresponding description in the *NSFOCUS NTA User Guide*.

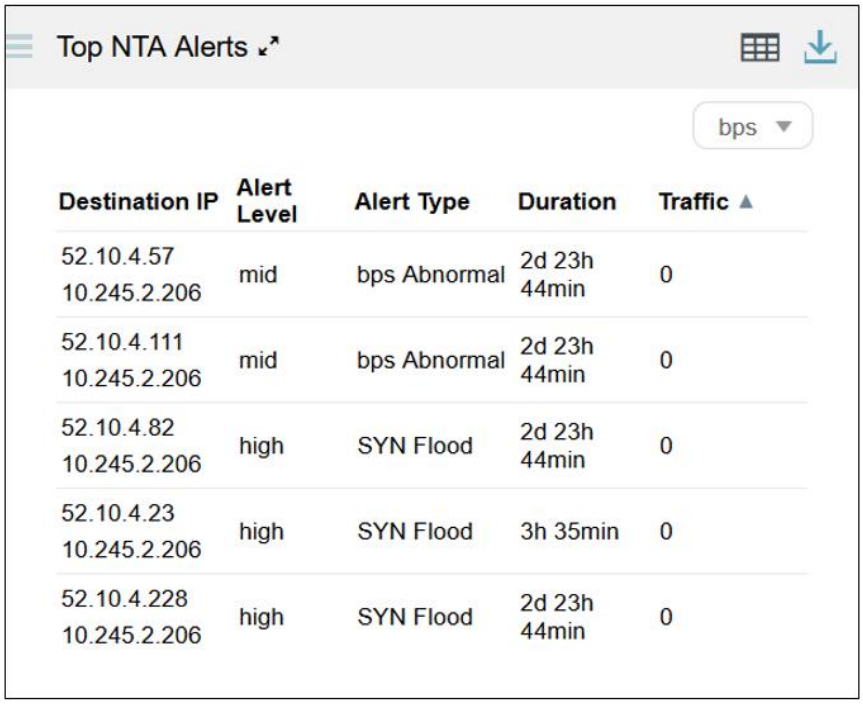
- **Duration**: shows the duration of the alert from the start time to current time. Pointing to a specific duration displays the start time of the attack against the destination IP address, as shown in Figure 4-51.

Figure 4-51 Start time of an alert reported by NTA



- **Traffic**: shows the traffic at the start time of the alert. By default, top alerts are ranked in descending order of largest traffic detected by ADS devices in the last 30 seconds. In this case, after you click **Traffic**, the ▲ icon is displayed and the top alerts are ranked in ascending order of smallest traffic detected by ADS devices in the last 30 seconds.

Figure 4-52 Top alerts reported by NTA in terms of smallest traffic



4.1.13.2 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top NTA Alerts** panel to display traffic data in pps.

4.1.13.3 Downloading a Report

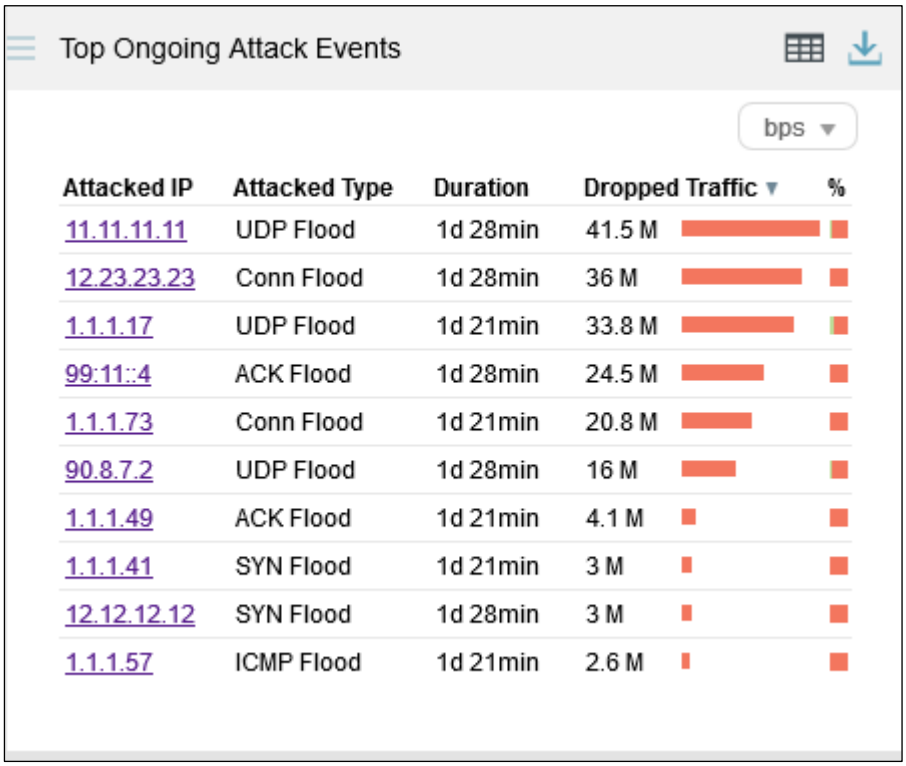
Click in the upper-right corner of the **Top NTA Alerts** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.14 Viewing Top Ongoing Attack Events

The **Top Ongoing Attack Events** panel shows top 10 ongoing attack events ranked according to attack traffic detected by all ADS devices in the last 30 seconds.

Data on this panel refreshes every 30 seconds.

Figure 4-53 Top ongoing attack events

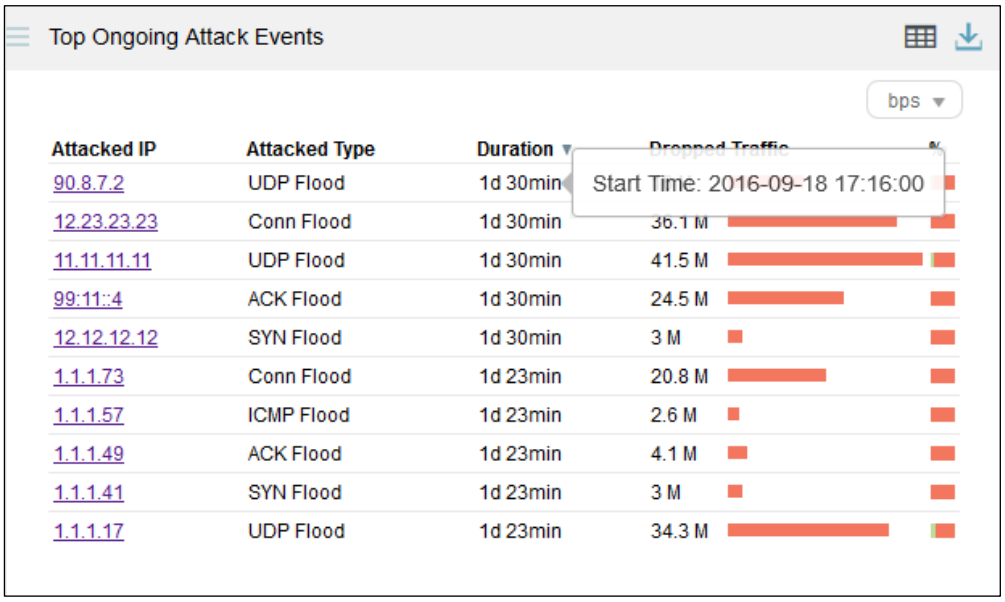


4.1.14.1 Understanding Data on the Panel

The **Top Ongoing Attack Events** panel shows top 10 ongoing attack events according to traffic dropped by ADS in the last 30 seconds. By default, these events are listed in descending order of dropped traffic.

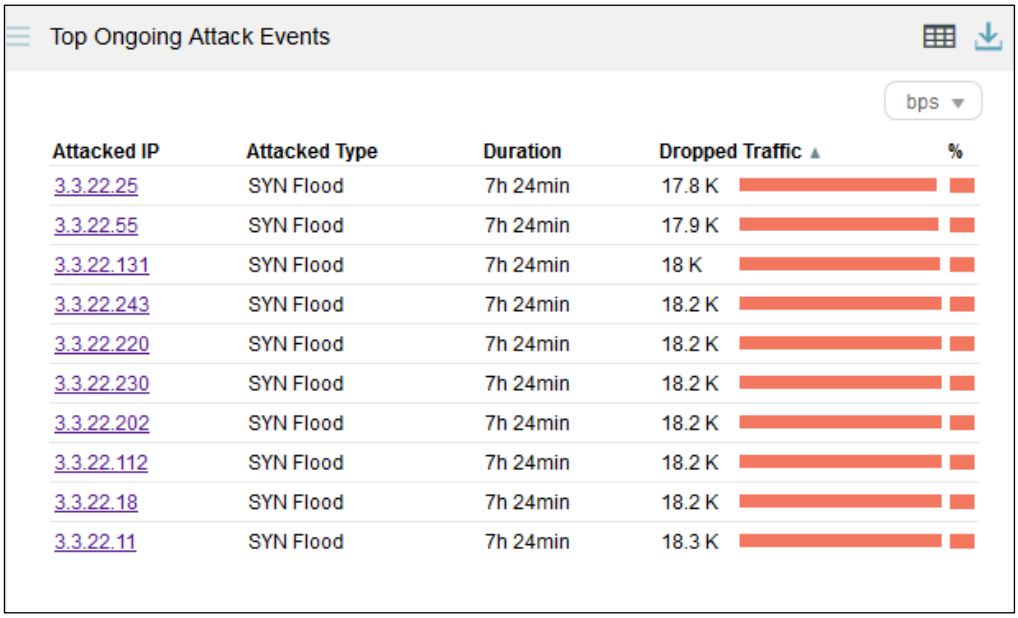
- **Attacked IP**: shows the attacked IP address. Clicking an IP address, you can view its detailed attack event information on an individual page. For details, see section 4.1.14.2 Viewing Attack Events Specific to an IP Address.
- **Attack Type**: shows the specific attack type.
- **Duration**: shows the duration from the time when an alert is triggered to the time when the data is refreshed. Pointing to a duration displays the attack start time of the IP address, as shown in Figure 4-54.

Figure 4-54 Start time of an ongoing attack event



- **Dropped Traffic**: By default, top 10 ongoing attack events are listed in descending order of traffic dropped by ADS. In this case, the ▼ icon is displayed to the right of **Dropped Traffic** and this column shows the total maximum traffic dropped by all ADS devices in the last 30 seconds. The red bar also indicates the total value. After you click **Dropped Traffic**, the ▲ icon is displayed and this column shows the total minimum traffic dropped by all ADS devices in the last 30 seconds.

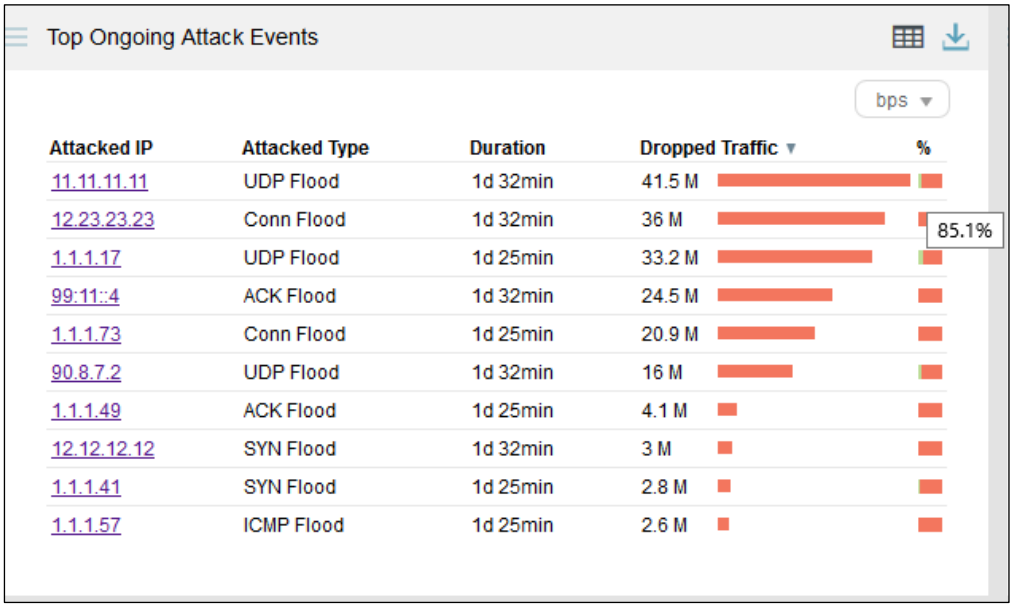
Figure 4-55 Top ongoing attack events by total minimum dropped traffic



- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. Pointing to a bar in this column displays the specific percentage. In a bar, green

indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-56, the percentage of dropped traffic for 11.11.11.11 is 85.1%.

Figure 4-56 Percentage of forwarded traffic in an ongoing attack event



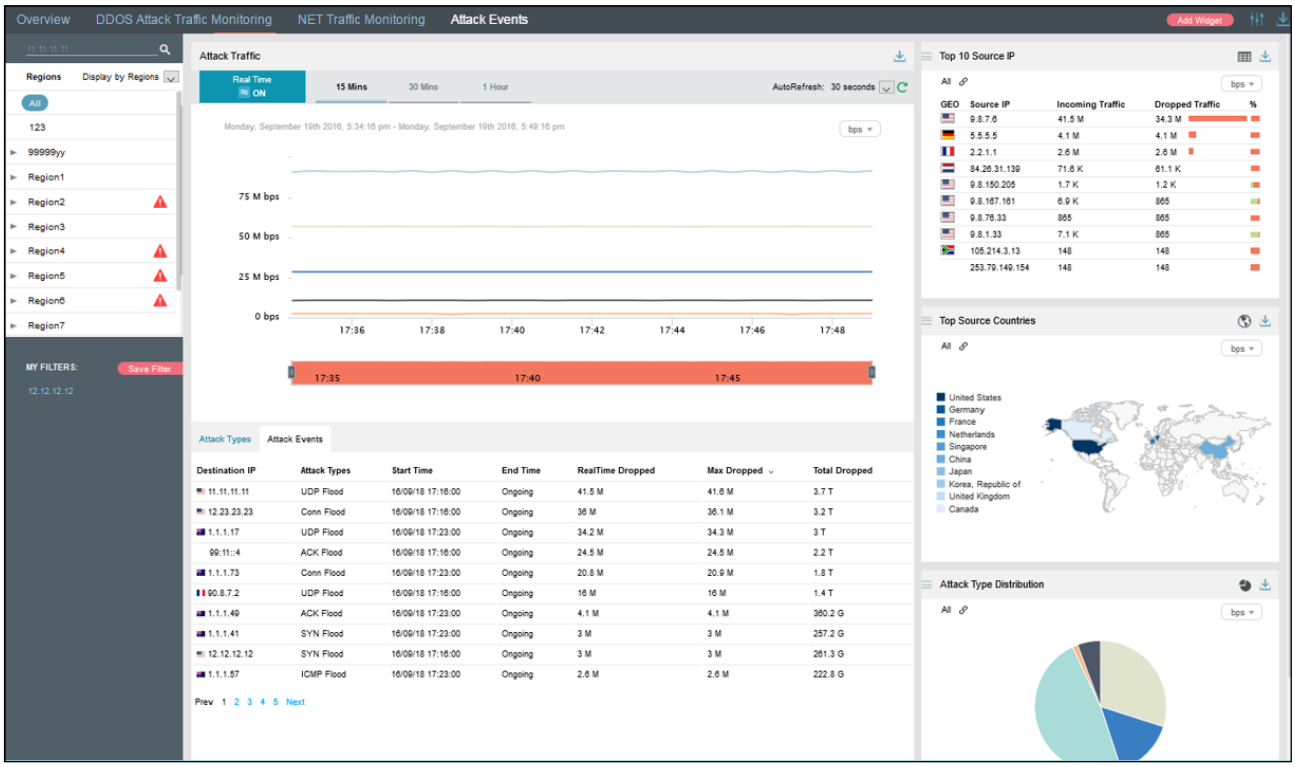
4.1.14.2 Viewing Attack Events Specific to an IP Address

You can conveniently view traffic of an IP address listed in the **Top Ongoing Attack Events** panel by performing the following steps:

Step 1 On the page shown in Figure 4-56, click an IP address, for example, 11.11.11.11.

The **Attack Events** page is displayed, with the IP address in question already in the search box in the left, as shown in Figure 4-57.

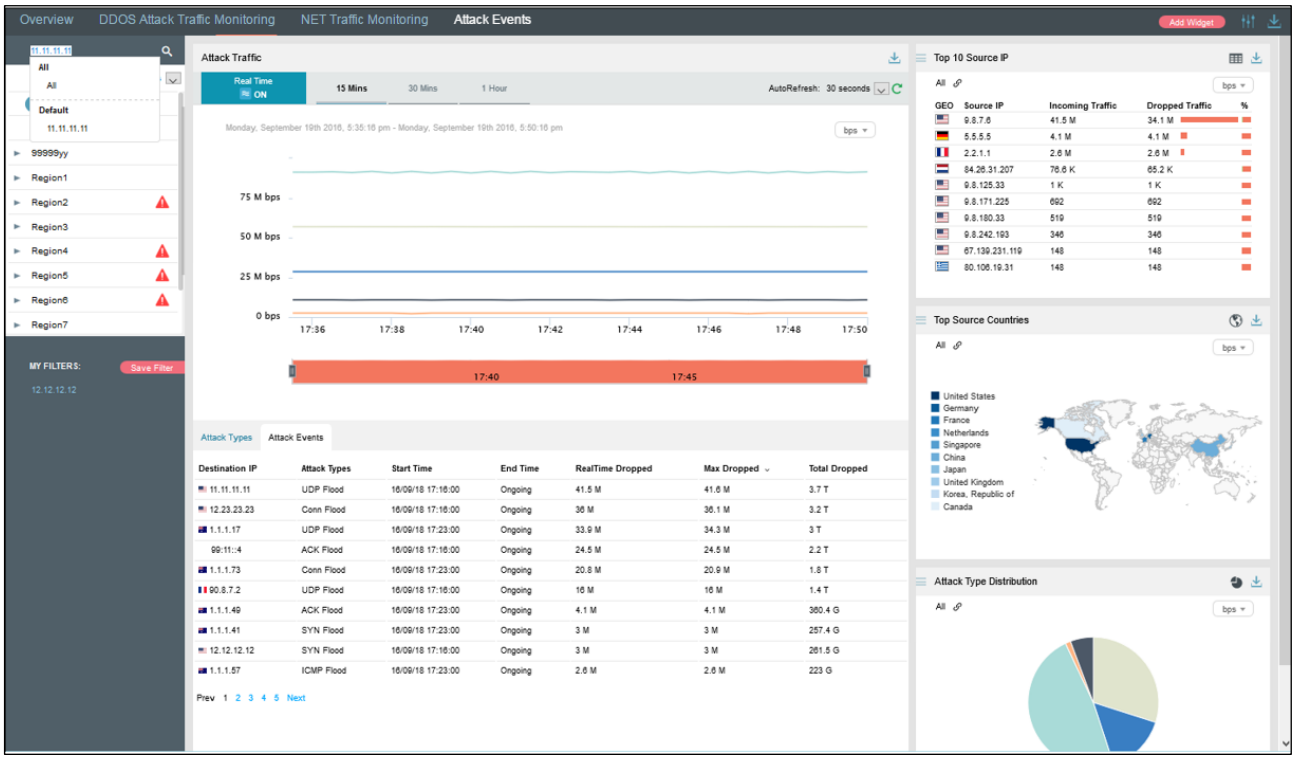
Figure 4-57 Attack traffic targeting an IP address



Step 2 Click in the search box.

The system displays all objects containing the current IP address.

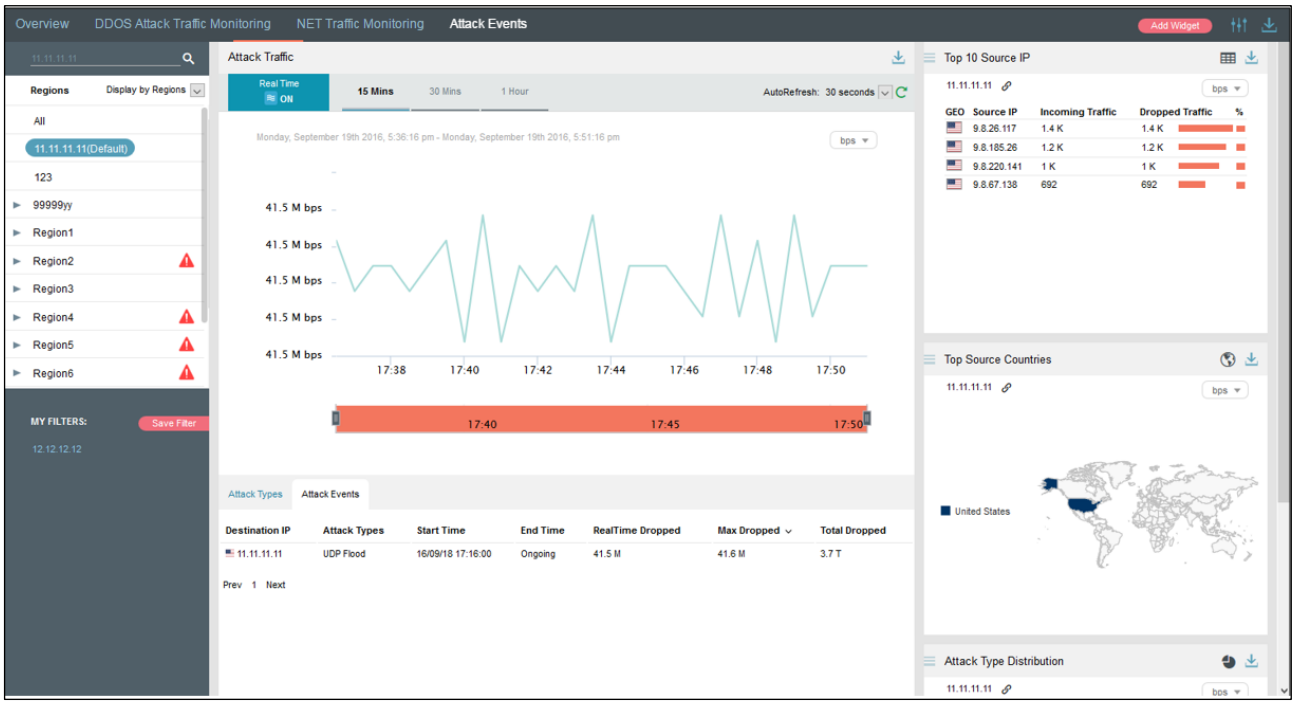
Figure 4-58 Searching for an IP address object



Step 3 Select the desired IP address object and then press **Enter**.

The attack event information of this IP address is displayed, as shown in Figure 4-59.

Figure 4-59 Attack event information of an IP address



4.1.14.3 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Ongoing Attack Events** panel to display traffic data in pps.

4.1.14.4 Downloading a Report

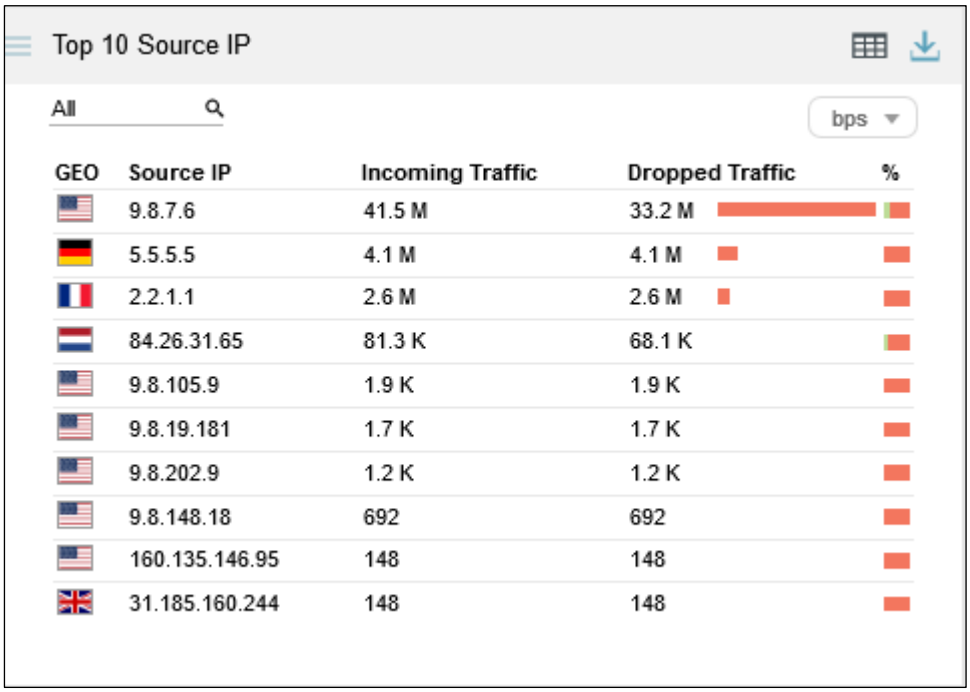
Click in the upper-right corner of the **Top Ongoing Attack Events** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.15 Viewing Top 10 Source IP Addresses

The **Top 10 Source IP Addresses** panel shows top 10 source IP addresses ranked according to traffic dropped by ADS in the last 30 seconds.

Data on this panel refreshes every 30 seconds.

Figure 4-60 Top 10 source IP addresses

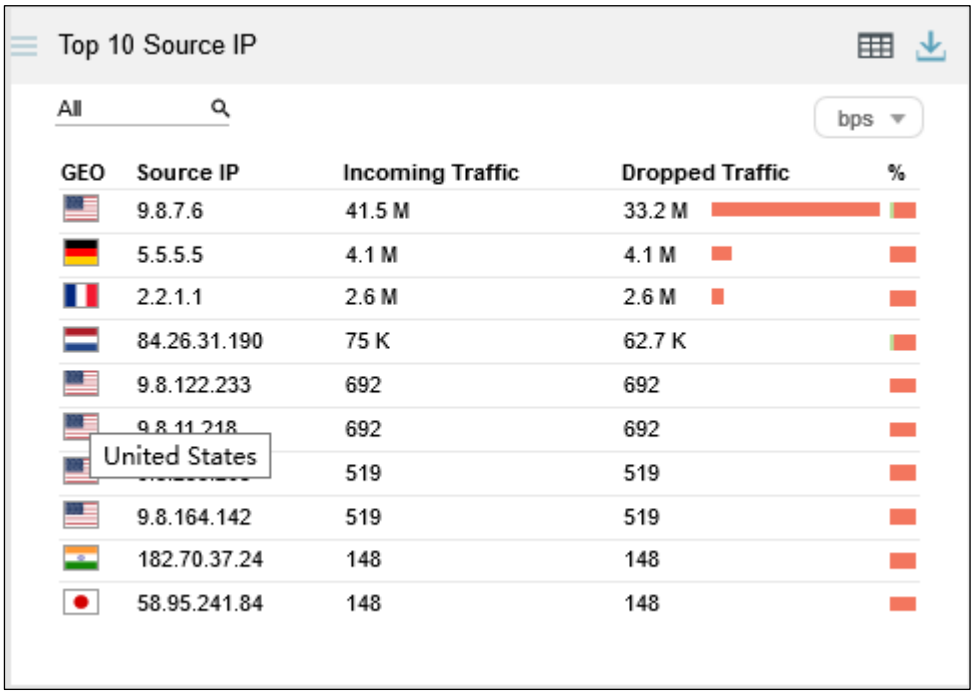


4.1.15.1 Understanding Data on the Panel

The table ranks top 10 source IP addresses according to traffic dropped by ADS in the last 30 seconds.

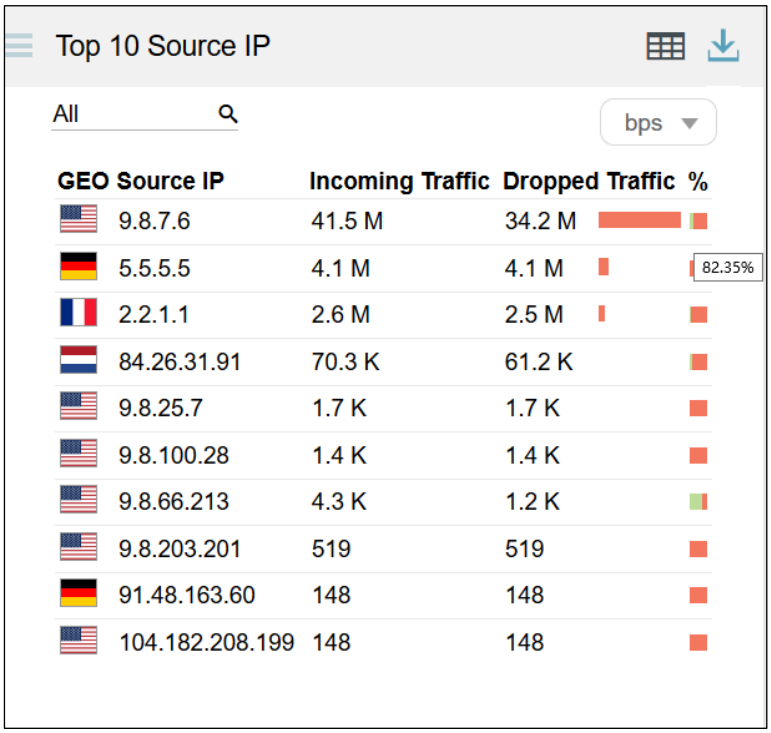
- **GEO**: shows the national flag icons. Pointing to an icon displays the country name, as shown in Figure 4-61.

Figure 4-61 Display of the country name



- **Source IP**: shows source IP addresses.
- **Incoming Traffic**: shows the total traffic received by ADS devices in the last 30 seconds.
- **Dropped Traffic**: shows the total maximum traffic dropped by all ADS devices in the last 30 seconds. The red bar to the right of the traffic value also indicates the maximum value. A longer bar indicates more traffic dropped.
- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. Pointing to a bar in this column displays the specific percentage. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-62, the percentage of dropped traffic for 9.8.7.6 is 82.35%.

Figure 4-62 Percentage of dropped traffic of a source IP address



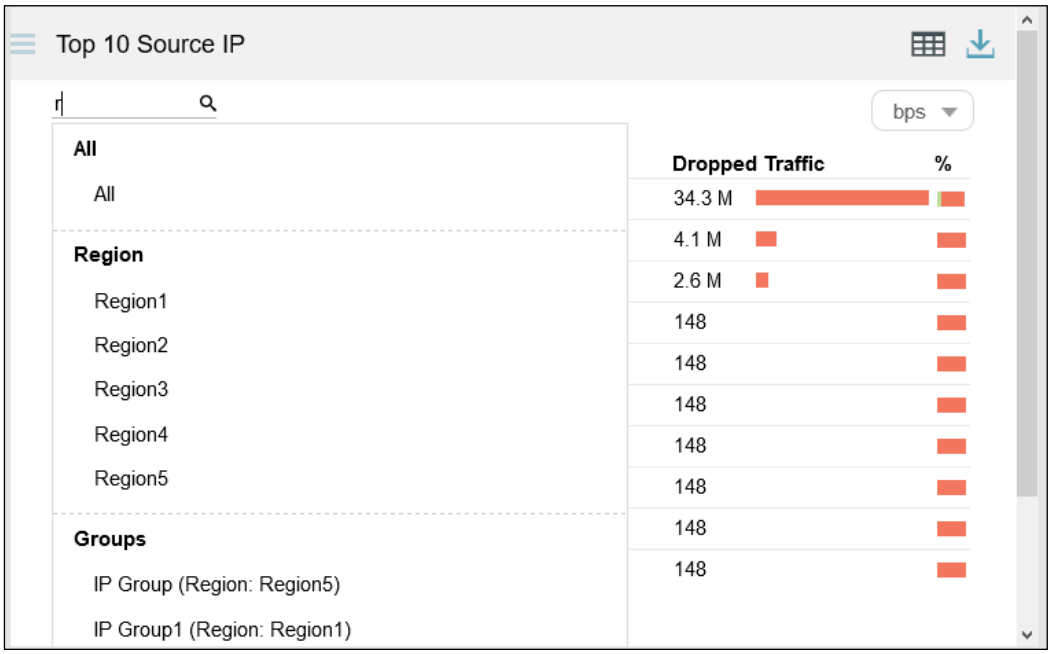
4.1.15.2 Viewing Traffic of a Specific Object

By default, the **Top 10 Source IP** panel presents top 10 source IP addresses based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, or ADS-protected group to view its top source IP addresses ranked according to traffic dropped in the last 30 minutes. You can also specify a source IPv4 or IPv6 address to view its traffic information in the last 30 minutes.

Step 1 On the page shown in Figure 4-62, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

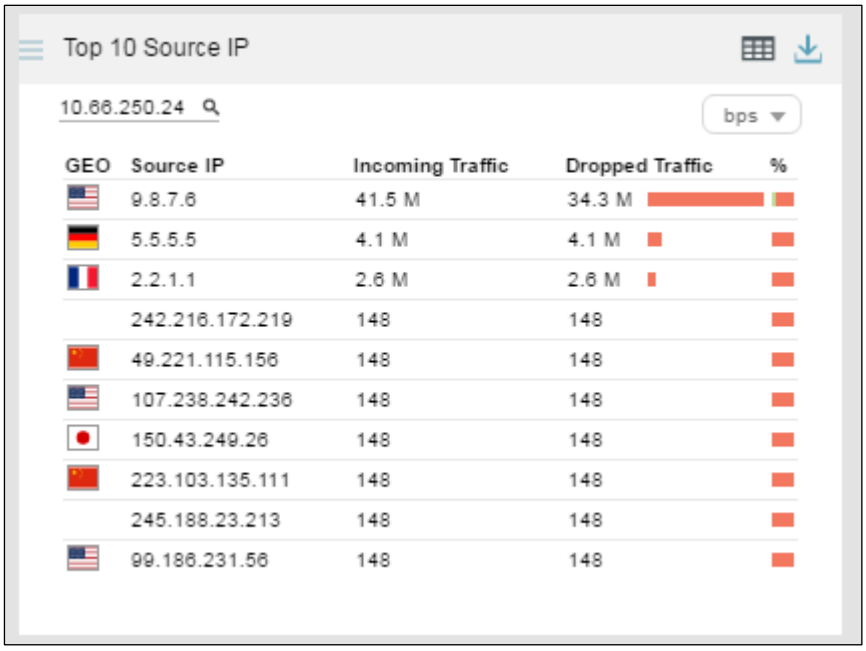
Figure 4-63 Searching for an object



Step 2 Select an object and press **Enter**.

Then source IP addresses associated with the specified object are listed in descending order of traffic handled by ADS in the last 30 minutes.

Figure 4-64 Traffic of top 10 source IP addresses associated with a specific object



4.1.15.3 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top 10 Source IP** panel to display traffic data in pps.

4.1.15.4 Downloading a Report

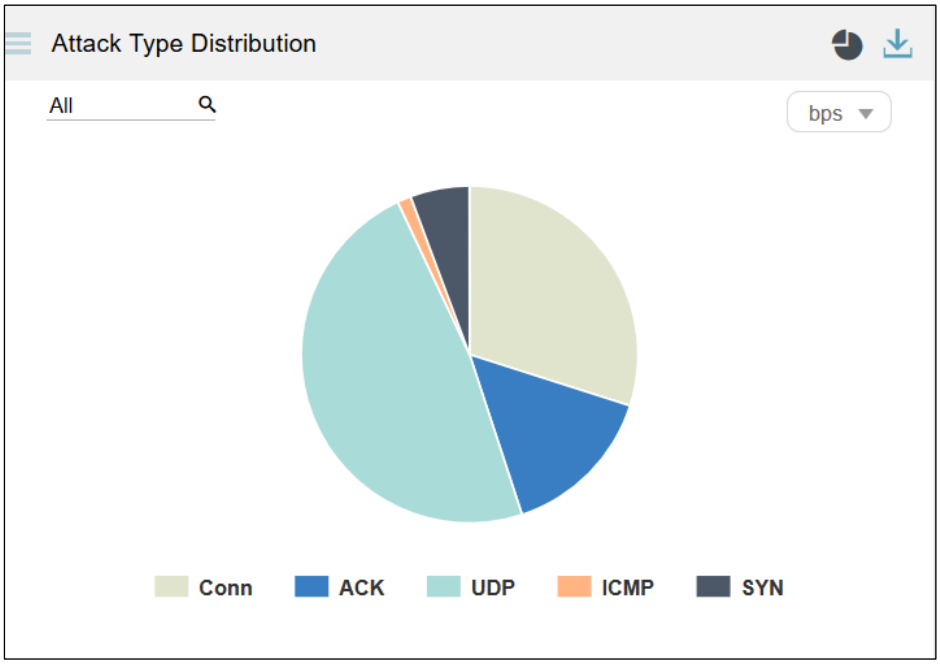
Click in the upper-right corner of the **Top 10 Source IP** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.16 Viewing Attack Type Distribution

The **Attack Type Distribution** panel shows the percentage of traffic of each attack type to the total traffic detected by ADS, as shown in Figure 4-65.

Data on this panel refreshes every 30 seconds.

Figure 4-65 Area representing traffic of an attack type separated from other areas



4.1.16.1 Understanding Data on the Panel

All attack types are displayed in a pie chart, with each indicated by a different color.

Table 4-3 Mappings between attack types and colors

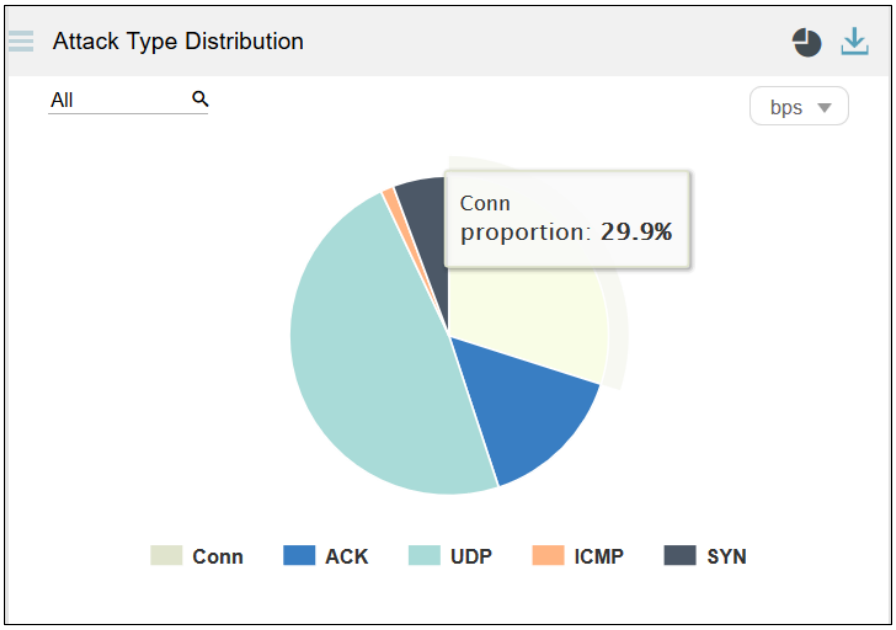
Attack Type	Color
Connection flood attack	Conn
ACK flood attack	ACK
UDP flood attack	UDP

Attack Type	Color
ICMP flood attack	ICMP
SYN flood attack	SYN

4.1.16.2 Viewing the Percentage of Traffic of an Attack Type

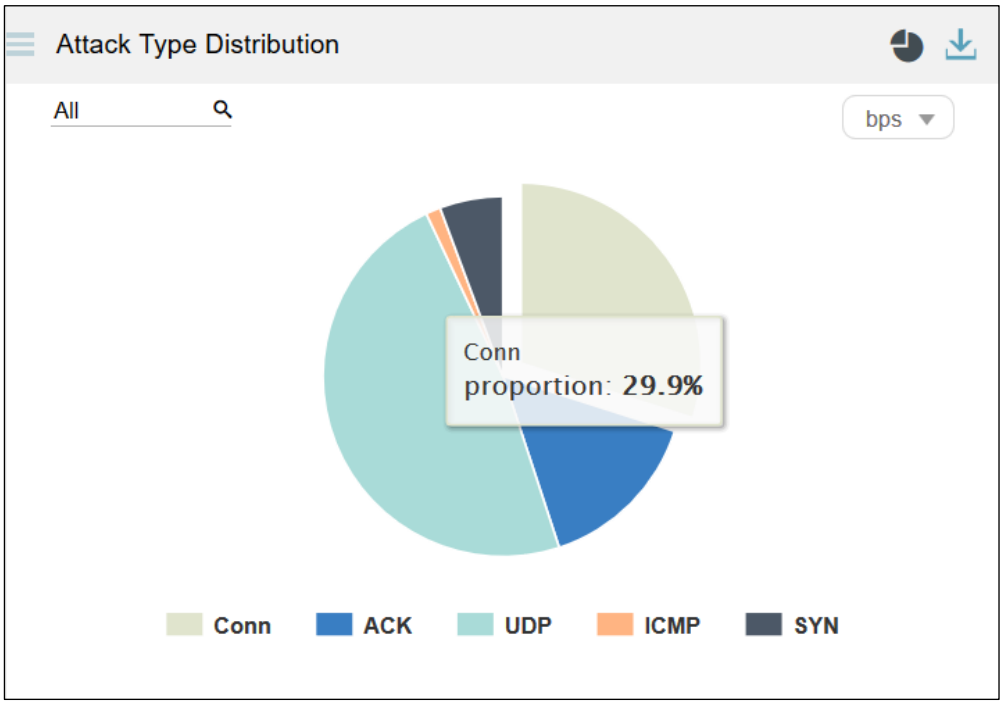
Pointing to the area of a specific attack type displays the percentage of traffic of this attack type to the total traffic, as shown in Figure 4-66.

Figure 4-66 Percentage of traffic of an attack type



Clicking in this area separates this area from other areas, as shown in Figure 4-67.

Figure 4-67 Separating the area of an attack type from other areas



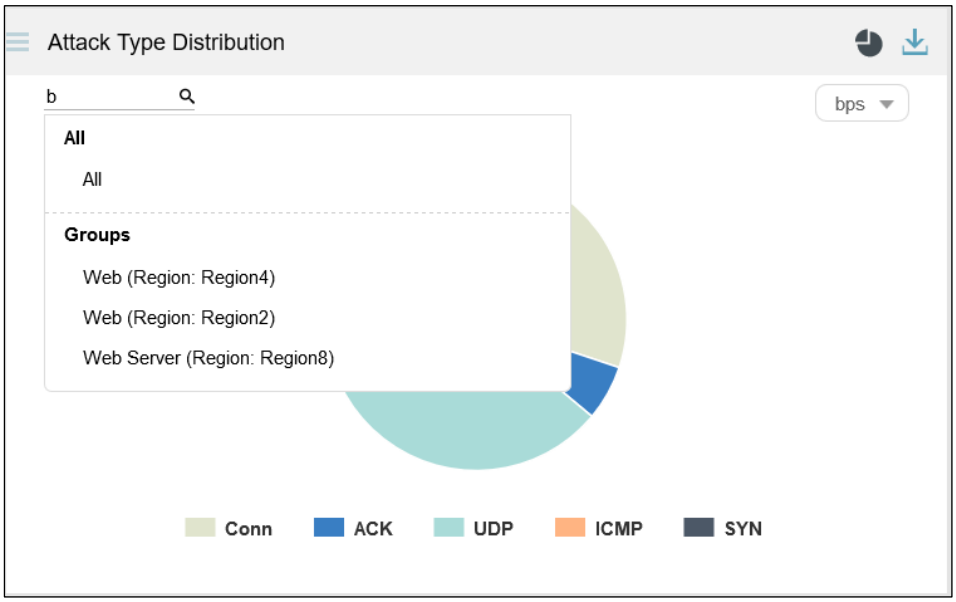
4.1.16.3 Viewing Attack Type Distribution of a Specified Object

By default, the **Attack Type Distribution** graph presents the distribution of attack types based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, ADS-protected group, or IPv4 or IPv6 address to view its attack type distribution in the last 30 minutes.

Step 1 On the page shown in Figure 4-65, type a character string.

The system displays all objects containing the typed character string, as shown in Figure 4-68.

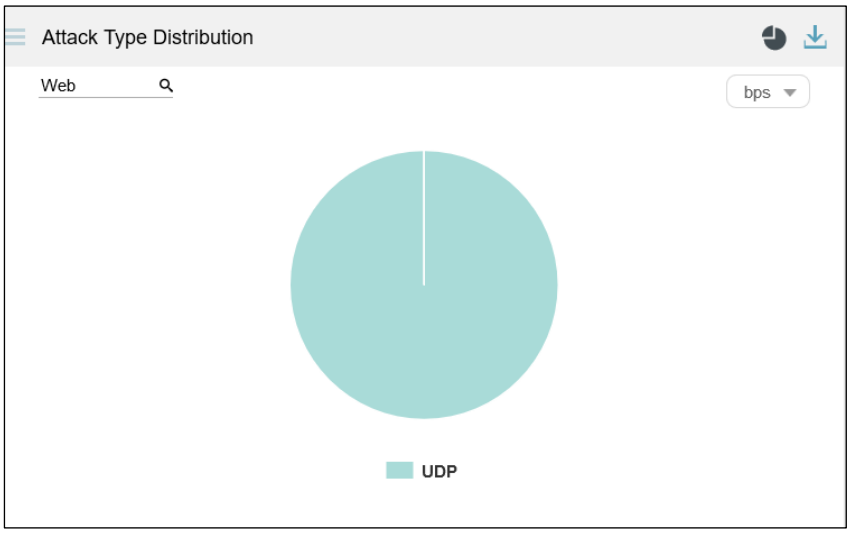
Figure 4-68 Searching for an object



Step 2 Select an object and press **Enter**.

Then the attack type distribution of a specified object in the last 30 minutes is displayed.

Figure 4-69 Attack type distribution of a specified object



4.1.16.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Attack Type Distribution** panel to display traffic data in pps.

4.1.16.5 Downloading a Report

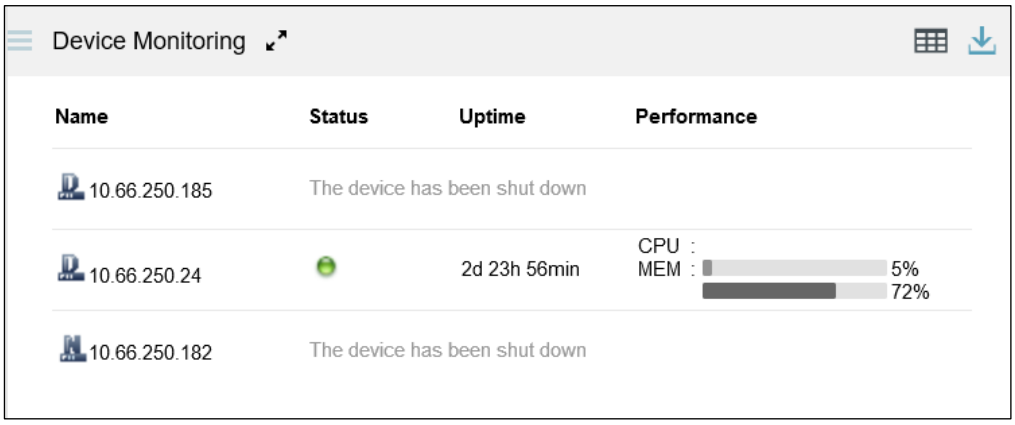
Click in the upper-right corner of the **Attack Type Distribution** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.17 Viewing Device Monitoring Information

The **Device Monitoring** panel shows the detailed monitoring information collected from ADS devices and NTA devices in the last 30 seconds, as shown in Figure 4-70.

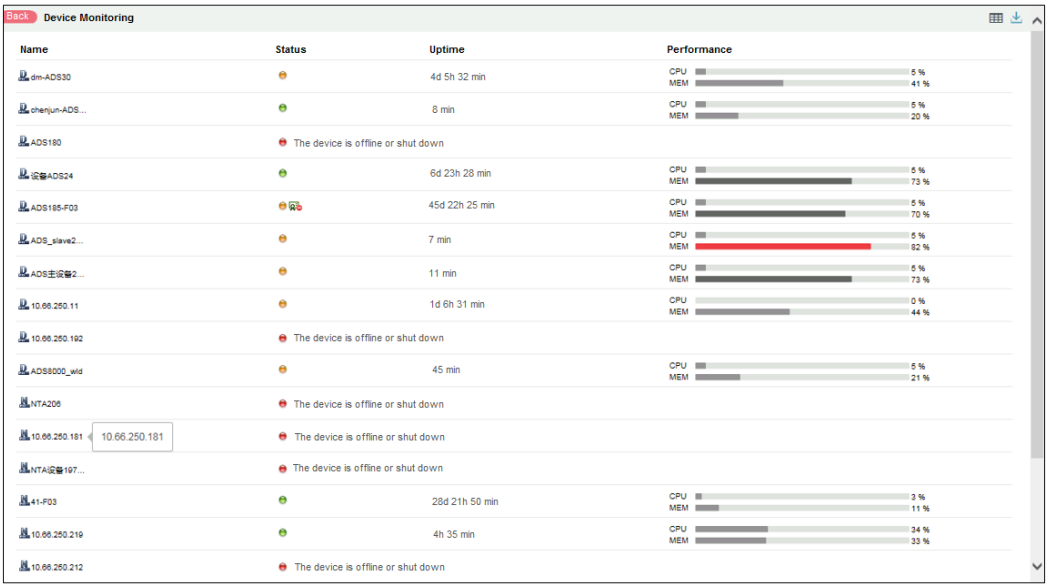
Data on this panel refreshes every 30 seconds.

Figure 4-70 Device monitoring information



Clicking displays more details about the monitored devices, as shown in Figure 4-71.

Figure 4-71 More details about the monitored devices

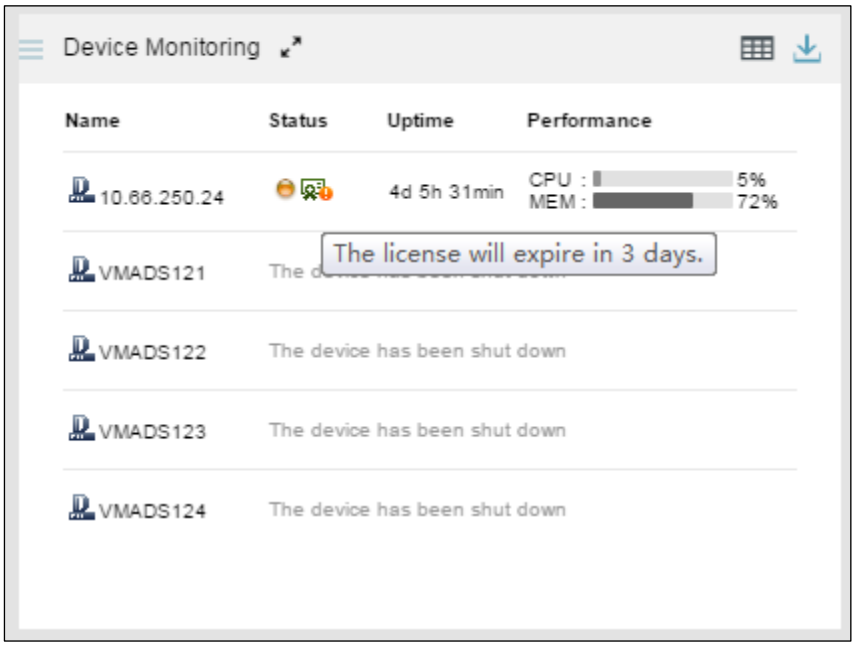


4.1.17.1 Understanding Data on the Panel

The **Device Monitoring** panel shows detailed monitoring information collected from all ADS devices and NTA devices.

- **Name**: shows the name of an NTA or ADS device.
- **Status**: shows whether the device is online.
  - When the device is online and properly connected, the icon is displayed.
  - When the device is offline, **The device has been shut down** is displayed in the **Status** column, but no status icon appears.
  - If the time of an online device is not synchronized with that of ADS M, the icon is displayed.
  - If the license of a device is about to expire, the icon is displayed. Pointing to this icon displays the license information.

Figure 4-72 License expiration reminder

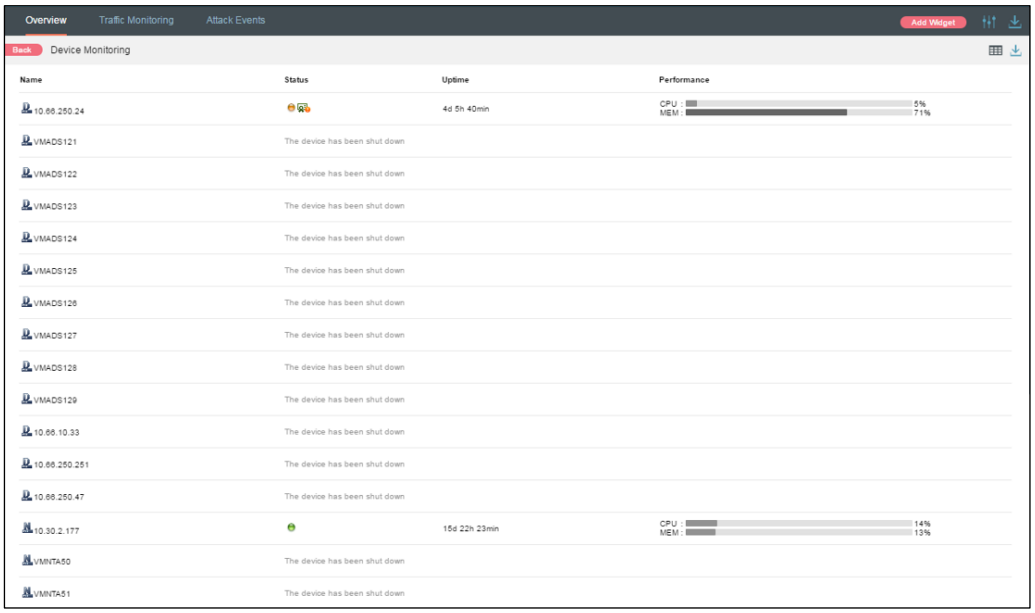


- **Uptime**: shows how long the system has been running continuously. The uptime is available only for online devices.
- **System Status**: shows the CPU/memory usage. Such information is available only to online devices.

  If the CPU or memory usage exceeds 80%, the bar turns red.

You can click to switch to the full screen mode, as shown in Figure 4-73.

Figure 4-73 Device monitoring information in full screen mode



You can click **Back** to return to the normal panel display mode.

4.1.17.2 Downloading a Report

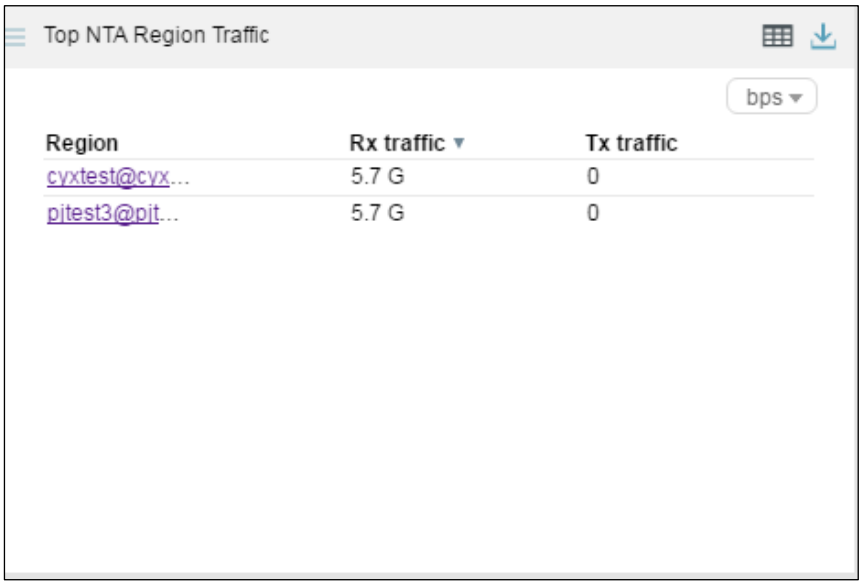
Click in the upper-right corner of the **Device Monitoring** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.18 Viewing Traffic of Top NTA's Regions

The **Top NTA Region Traffic** panel presents in real time top 10 NTA's regions with the largest network traffic in the last 30 seconds, as shown in Figure 4-74, making it convenient for users to learn which regions receive or transmit the largest network traffic.

Data on this panel refreshes every 30 seconds.

Figure 4-74 Top NTA Region Traffic panel

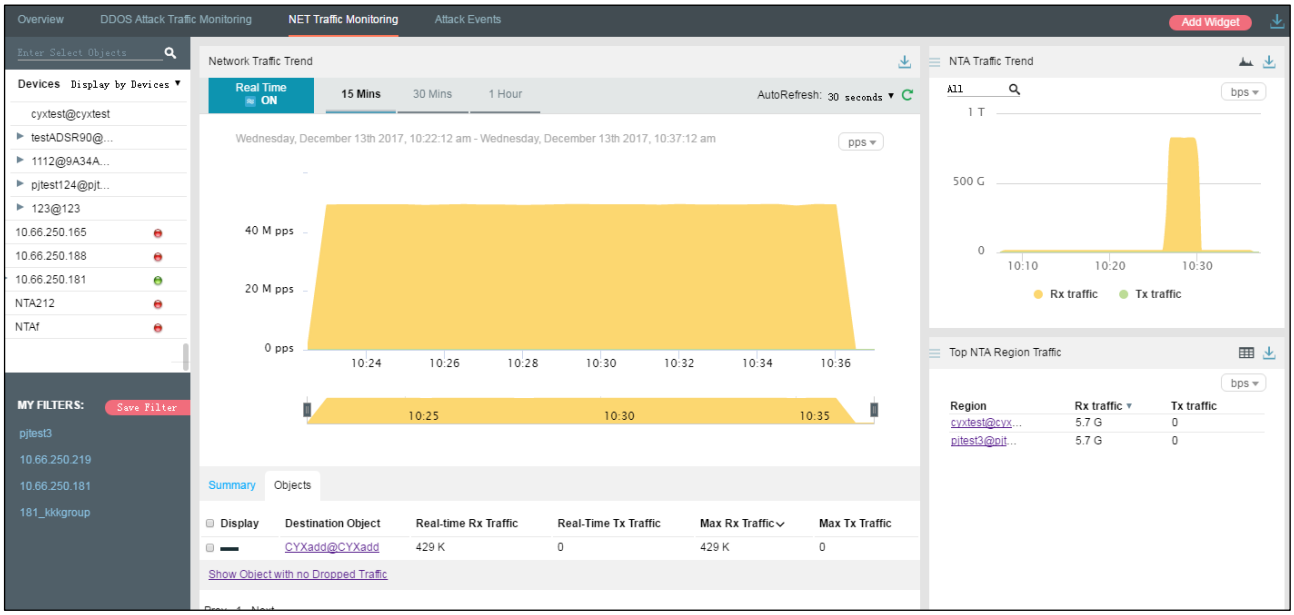


4.1.18.1 Understanding Data on the Panel

The list ranks top 10 NTA's regions according to network traffic generated in the last 30 seconds.

- **Region**: region that receives or transmits traffic. Clicking a region name opens the **NET Traffic Monitoring** tab page, where you can view more details about this region's traffic, as shown in Figure 4-75.

Figure 4-75 Traffic of a specific region



- **Rx traffic**: traffic received by NTA in the last 30 seconds

- **Tx traffic**: traffic transmitted by NTA in the last 30 seconds

4.1.18.2 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top NTA Region Traffic** panel to display traffic data in pps.

4.1.18.3 Downloading a Report

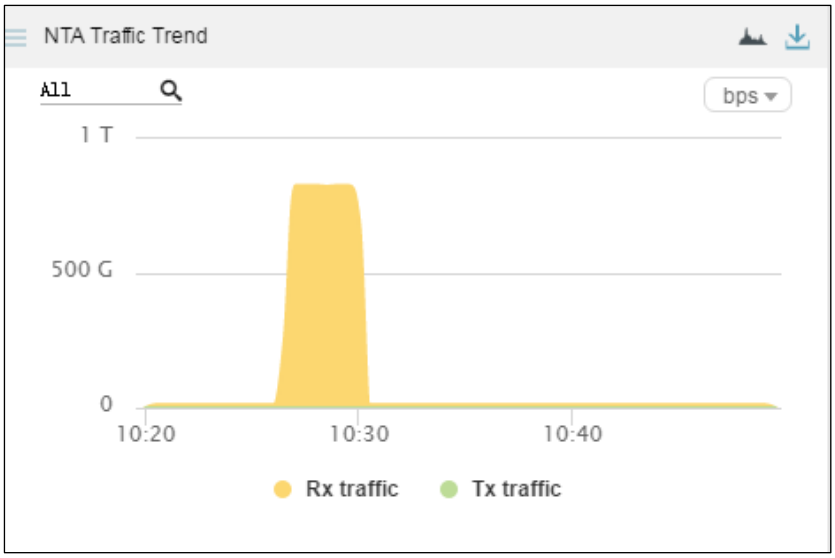
Click in the upper-right corner of the **Top NTA Region Traffic** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.1.19 Viewing Trends of Traffic on NTA

The **NTA Traffic Trend** panel shows trends of traffic received and transmitted in the last 30 minutes by NTA under monitoring of ADS M, as shown in Figure 4-76.

Data on this panel refreshes every 30 seconds.

Figure 4-76 NTA Traffic Trend panel



4.1.19.1 Understanding Data on the Panel

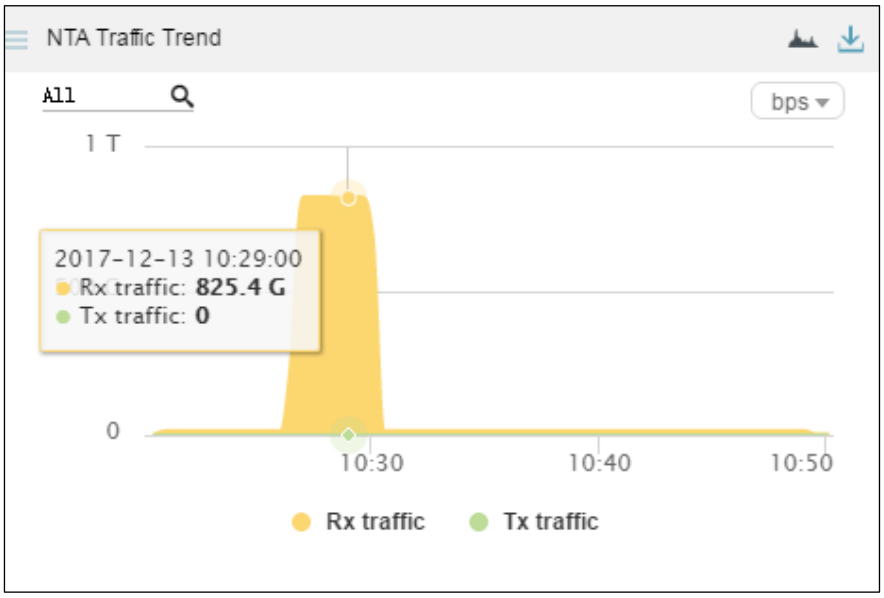
In the **NTA Traffic Trend** graph,

- The x-axis indicates time, spanning the last 30 minutes.
- The y-axis indicates traffic:
  - The yellow area represents the total traffic received.
  - The green area represents the total traffic transmitted.

4.1.19.2 Viewing Traffic at a Random Point of Time

Pointing to a random point in the **NTA Traffic Trend** graph displays the specific time, incoming traffic, outgoing traffic, and dropped traffic, as shown in Figure 4-77.

Figure 4-77 Detailed traffic information at a specific point of time



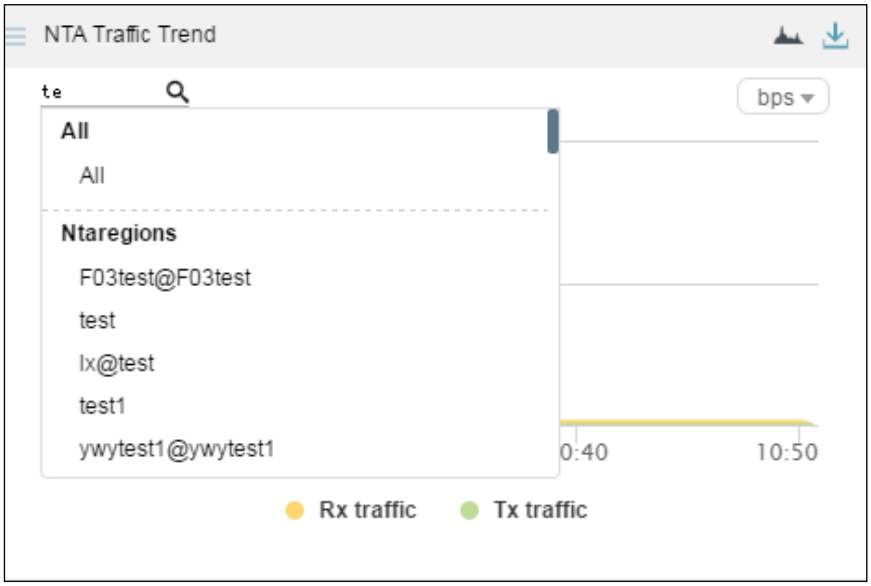
4.1.19.3 Viewing Traffic of a Specified Object

By default, the **NTA Traffic Trend** graph presents trends of traffic handled by all NTA devices under monitoring of ADS M. You can view real-time traffic trends of a specified region, regional IP group, and NTA device.

Step 1 On the page shown in Figure 4-77, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-78.

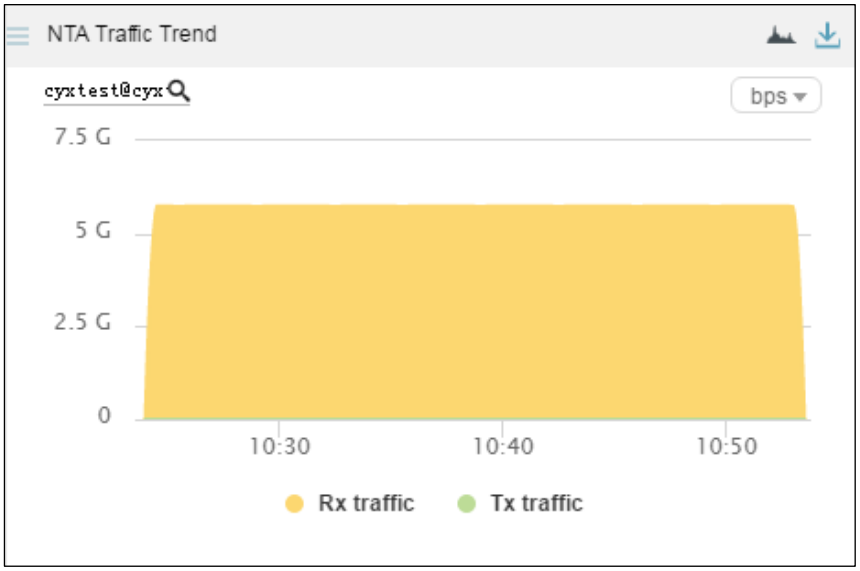
Figure 4-78 Searching for an object



Step 2 Select an object and press **Enter**.

Traffic trends of the specified object are displayed, as shown in Figure 4-79.

Figure 4-79 Real-time traffic trends of a specified object

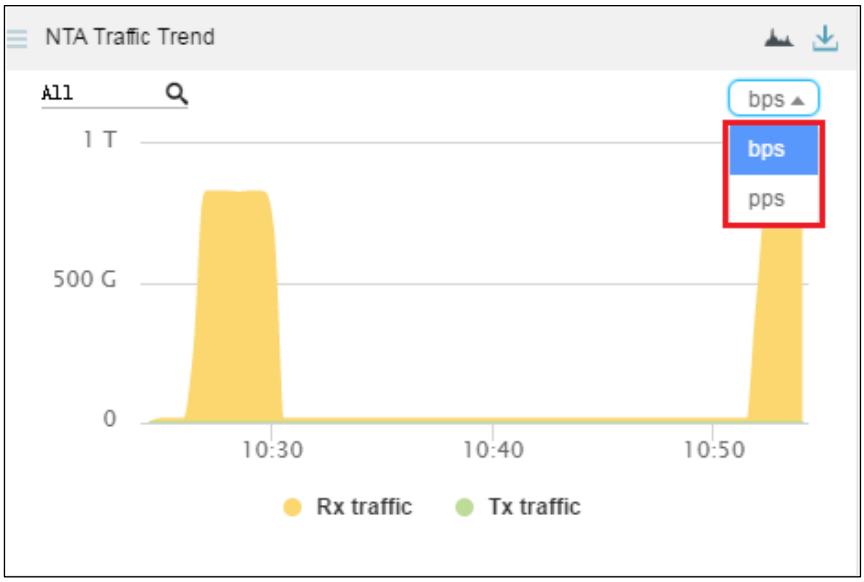


----End

4.1.19.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **NTA Traffic Trend** panel to display traffic data in pps, as shown in Figure 4-80.

Figure 4-80 Switching the traffic unit



4.1.19.5 Downloading a Report

Click in the upper-right corner of the **NTA Traffic Trend** panel and then data of this panel will be exported as a report. For details, see section 4.1.4 Downloading a Report.

4.2 DDoS Attack Traffic Monitoring

Note	ADS M presents attack traffic based on data uploaded by ADS devices.

Under **Traffic monitoring > DDOS Attack Traffic Monitoring**, you can do as follows:

- View real-time and historical attack traffic trends of all objects or a specified region, regional IP group, ADS device, ADS-protected group, or IP address
- View or add panels.
- Configure filters.

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view attack traffic information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

Attack traffic information includes real-time traffic information and historical traffic information. By default, attack traffic information is displayed by region.

4.2.1 Viewing Real-Time Attack Traffic Information

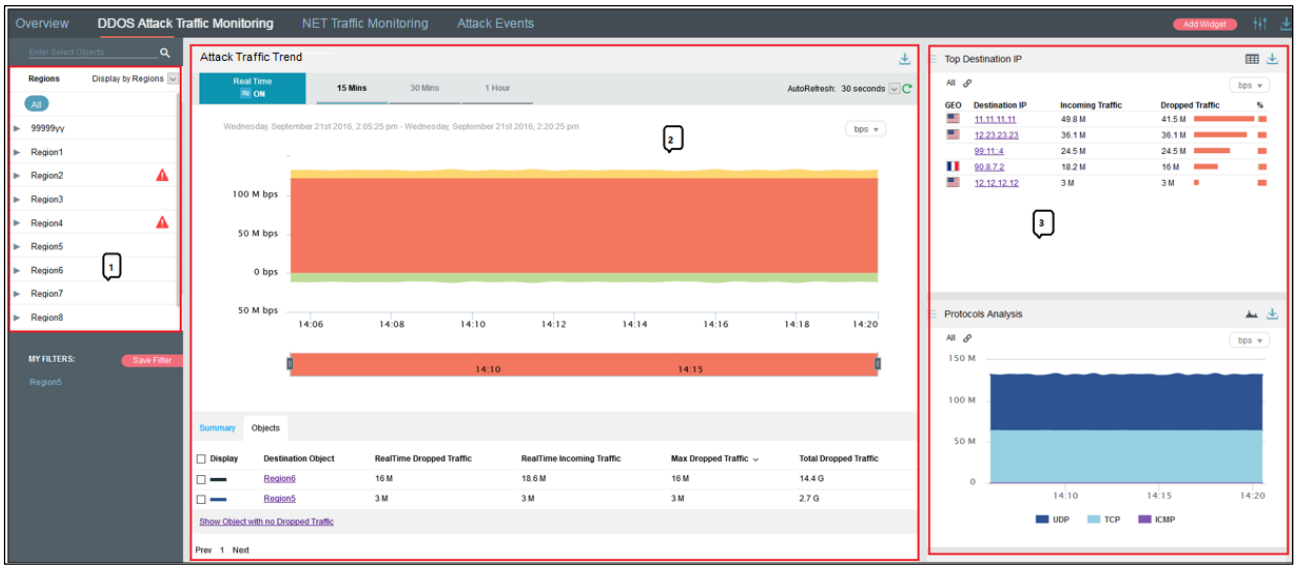
To view real-time attack traffic information, follow these steps:

Step 1 Choose **Traffic monitoring > DDOS Attack Traffic Monitoring**.

Real-time attack traffic information of all objects is displayed by default, including **Attack Traffic Trend**, and **Top Destination IP** and **Protocols Analysis** panels.

In real-time mode, trends of traffic in the last 15 minutes is displayed by default. You can click **30 Mins** or **1 Hour** to view the attack traffic trend of the last 30 minutes or last hour.

Figure 4-81 Attack traffic information of all objects



① List of objects ② Traffic trend ③ Panels

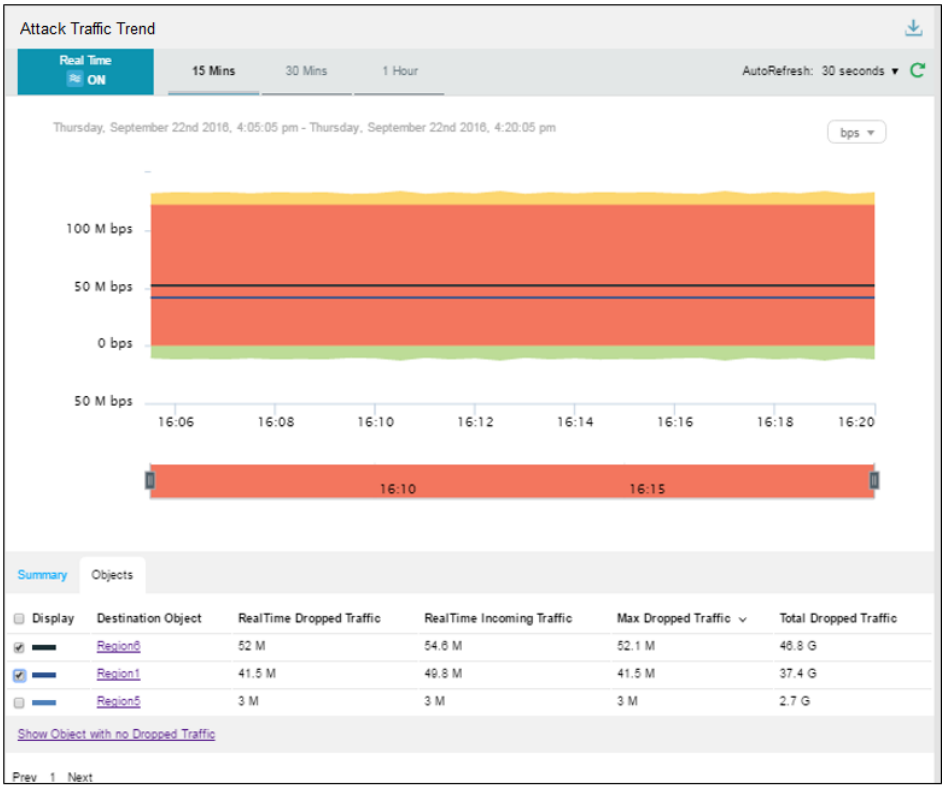
On the **DDOS Attack Traffic Monitoring** page, the **Objects** tab page ranks regions in descending order of traffic dropped by ADS.

Table 4-4 Real-time attack traffic trend – parameters on the Objects tab page

Parameter	Description
Display	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.
Destination Object	Indicates the traffic monitoring object.
RealTime Dropped Traffic	Indicates traffic (in bps or pps) dropped by ADS for the object.
RealTime Incoming Traffic	Indicates traffic (in bps or pps) received by the object in real time.
Max Dropped Traffic	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Total Dropped Traffic	Indicates the total traffic (in bits) dropped by ADS for the object in the statistical period. The traffic unit is bit.

Step 2 On the **Objects** tab page shown in Figure 4-81, select one or more objects to view traffic dropped by ADS for them. See Figure 4-82.

Figure 4-82 Real-time traffic trend graph of a specified object

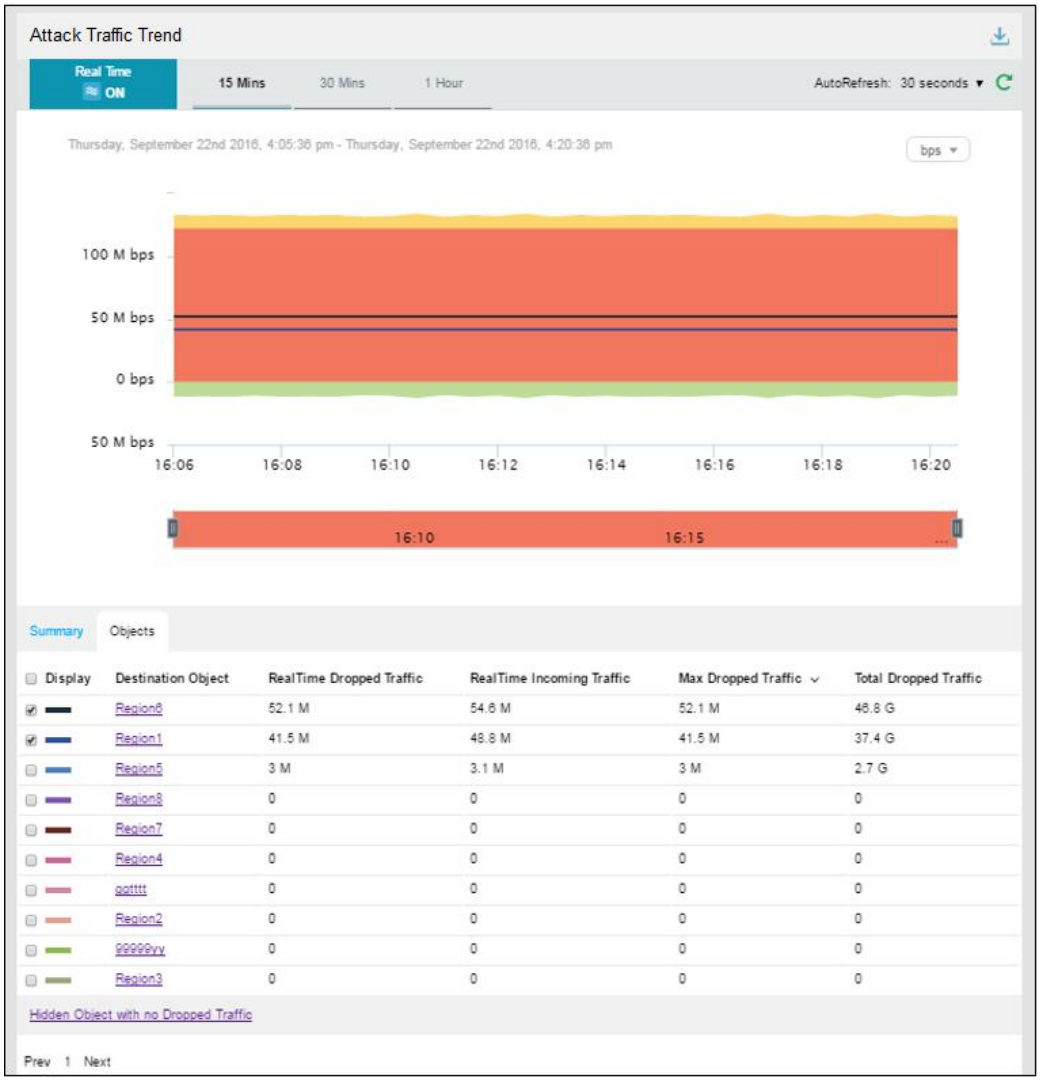


By default, only the objects with traffic dropped by ADS are displayed.

Step 3 Click the **Show Object with no Dropped Traffic** link to show all objects, as shown in Figure 4-83.

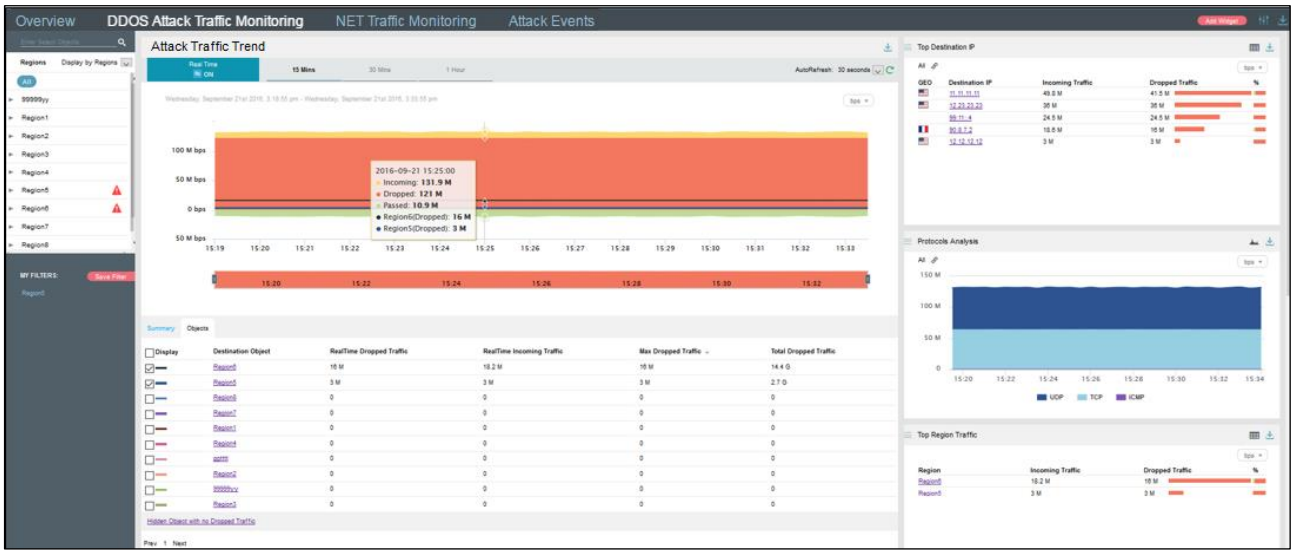
Clicking the **Hidden Object with no Dropped Traffic** link displays only objects with traffic dropped by ADS, but hides objects with no traffic dropped.

Figure 4-83 Real-time attack traffic trend graph of all objects



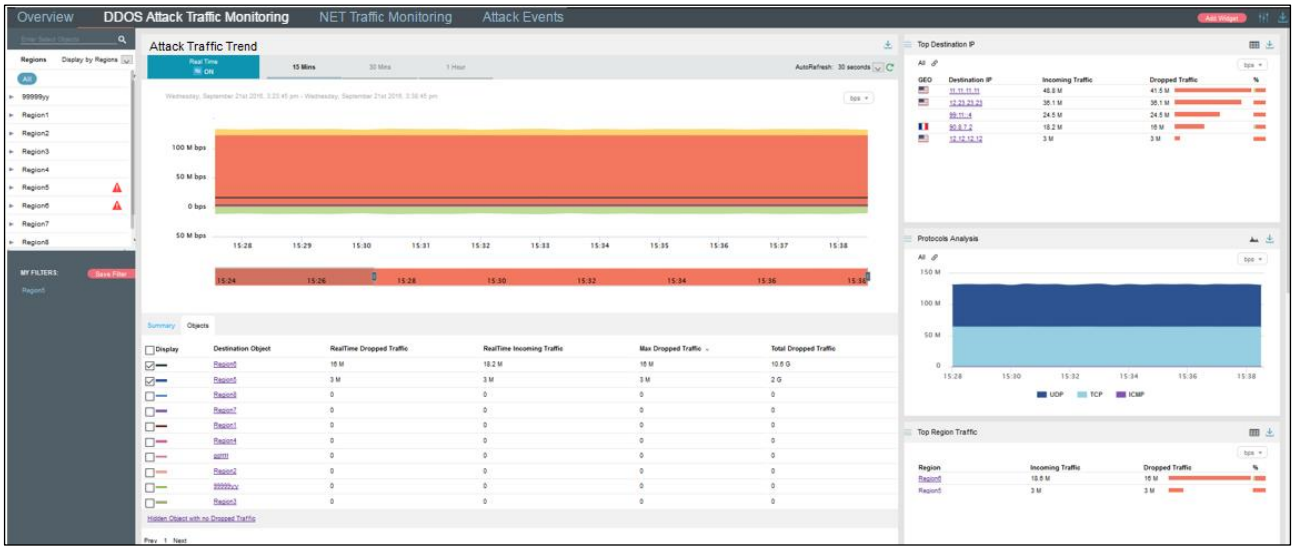
Step 4 Point to a random point in the attack traffic trend graph to display the total traffic received, forwarded, and dropped by ADS at a specific point of time for specified objects, as shown in Figure 4-84.

Figure 4-84 DDoS attack traffic information at a specific time



Step 5 Below the attack traffic trend graph, drag to view a finer-granularity traffic trend.

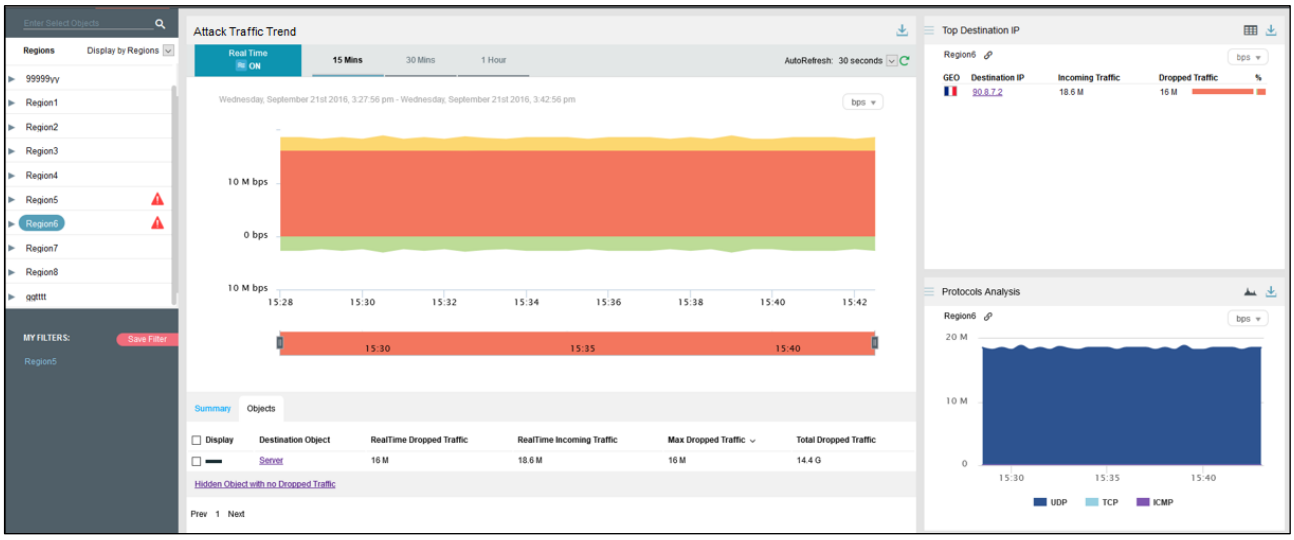
Figure 4-85 Finer-granularity traffic information



Step 6 Click a link of a region or IP group in the **Destination Object** column.

Traffic information of IP addresses in the region or IP group is displayed, including the **Attack Traffic Trend**, and **Top Destination IP** and **Protocols Analysis** panels.

Figure 4-86 Traffic information of a specific region



Step 7 On the page shown in Figure 4-81, click **Summary**.

The average and total are displayed for dropped traffic, outgoing traffic, and incoming traffic in the statistical period.

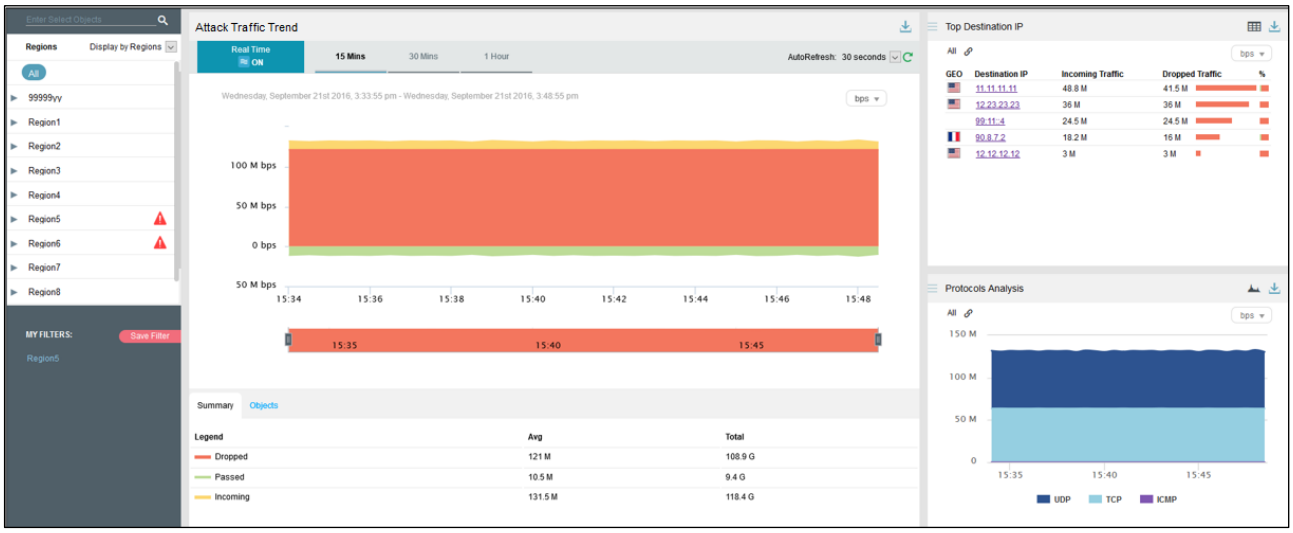
Clicking the bar or text in the **Legend** column hides or displays the corresponding traffic in the attack traffic trend graph. By default, all three types of traffic are displayed. A dimmed legend indicates that this type of traffic is hidden.

Table 4-5 describes parameters on the **Summary** tab page.

Table 4-5 Real-time traffic trend – parameters on the Summary tab page

Parameter	Description
Legend	Legends for dropped traffic, outgoing traffic, and incoming traffic.
Avg	Average of the dropped traffic, ongoing traffic, or incoming traffic. The traffic unit is bps or pps.
Total	Total value of the dropped traffic, ongoing traffic, or incoming traffic. The traffic unit is bit.

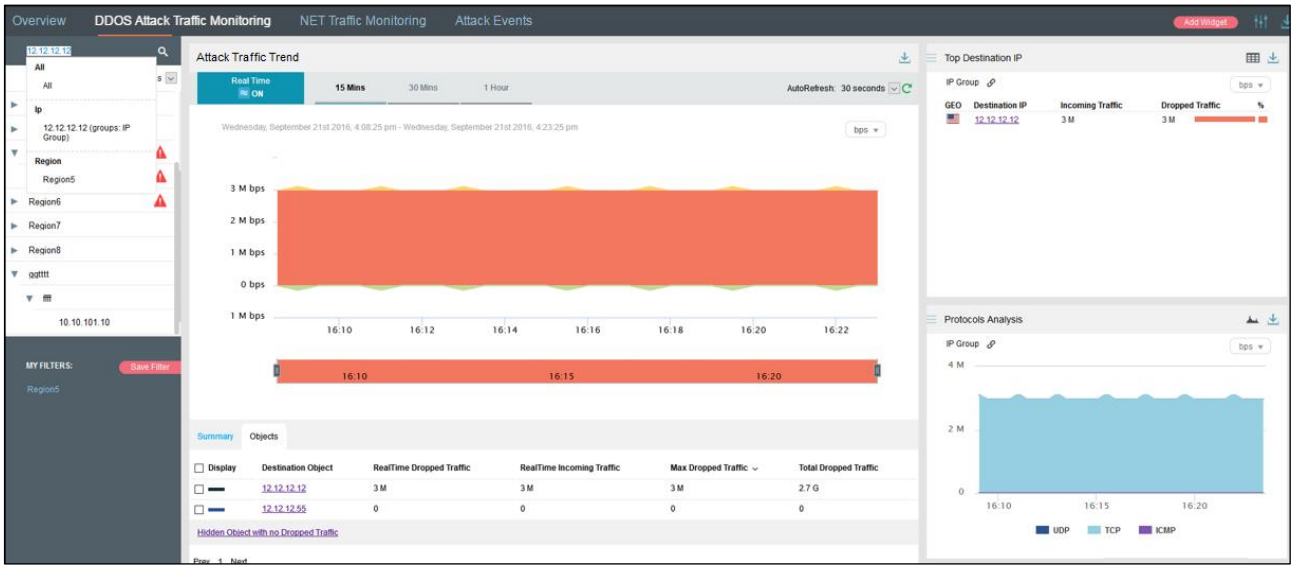
Figure 4-87 Summary of real-time attack traffic monitoring



Step 8 Click an IP address in the **Destination Object** column on the **Objects** tab page.

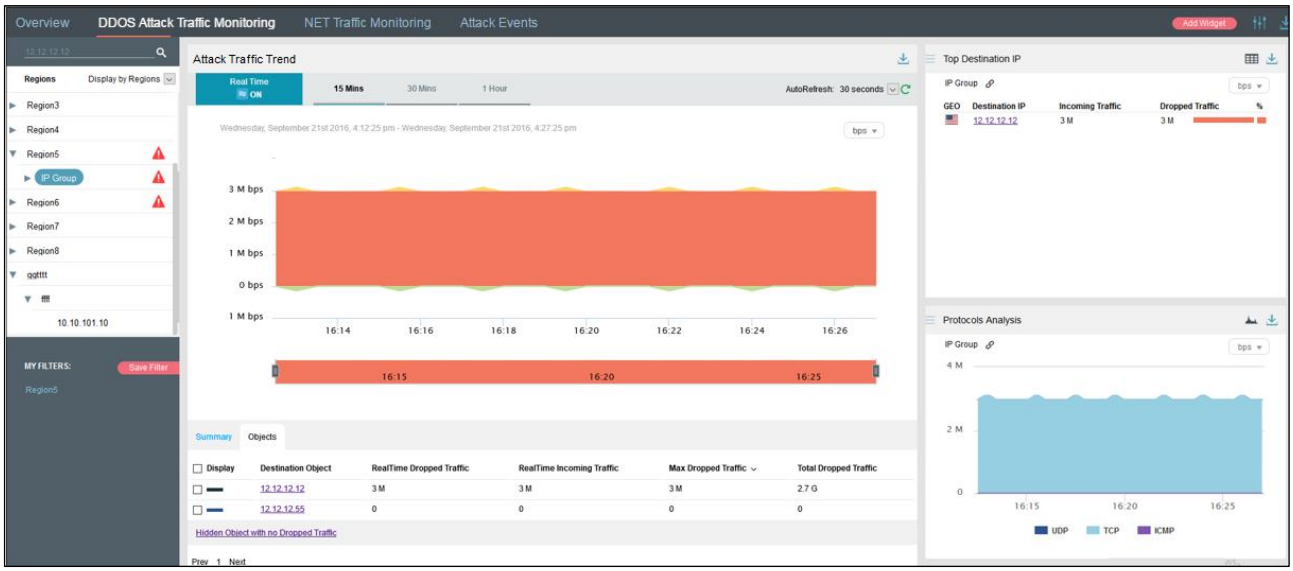
Then the search bar in the upper-left corner of the **DDOS Attack Traffic Monitoring** page shows the region to which the IP address in question belongs.

Figure 4-88 Searching for information associated with an IP address



The **Attack Traffic Trend** and **Top Destination IP** and **Protocols Analysis** panels concerning the IP address are displayed, as shown in Figure 4-89.

Figure 4-89 Real-time traffic monitoring of an IP address

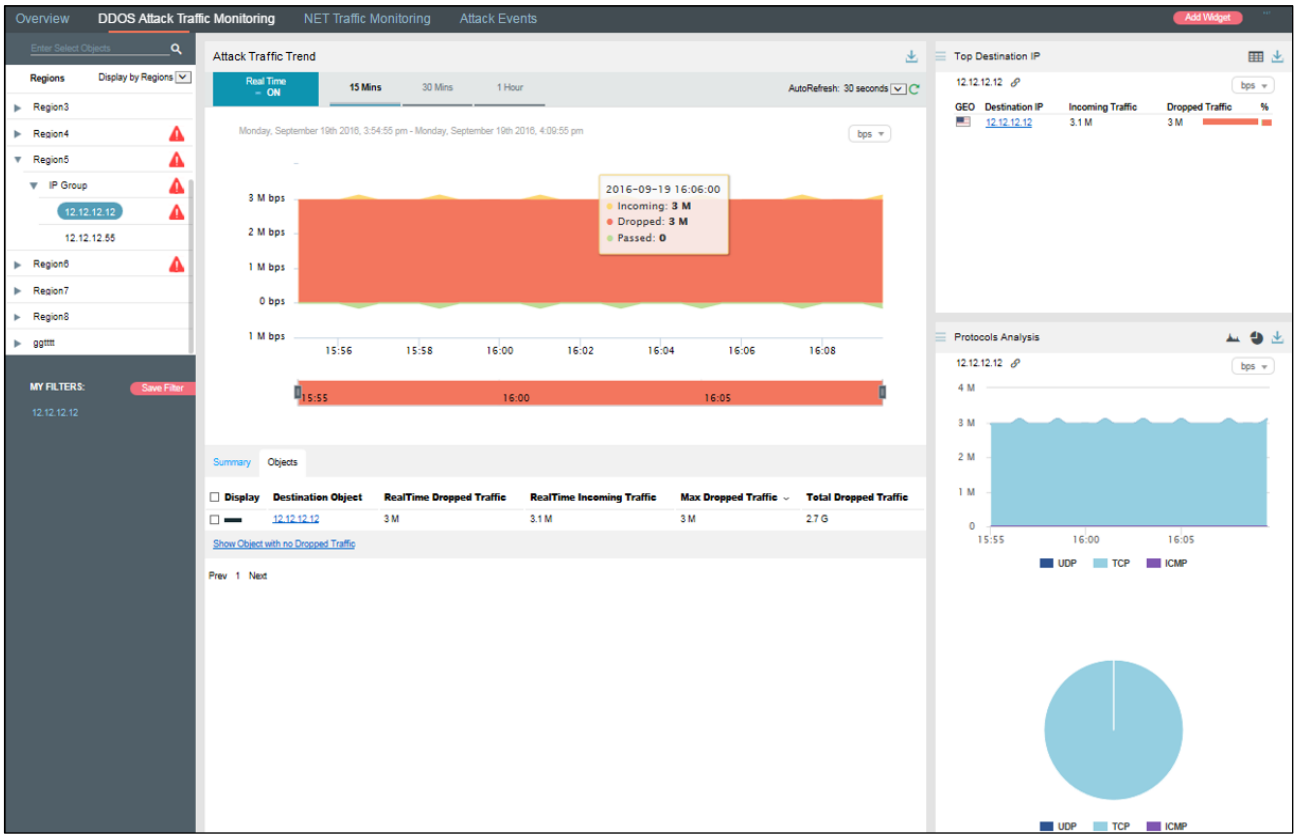


----End

4.2.2 Viewing Region-Specific Traffic Information

On the page shown in Figure 4-81, clicking a region in the left pane displays traffic information of the region and of all IP groups and IP addresses in this region. You can further view historical and real-time traffic trends and panels of a selected region, IP group under a region, or IP address. For example, you can choose **Region5 > IP Group > 12.12.12.12** to view traffic information of IP address **12.12.12.12**.

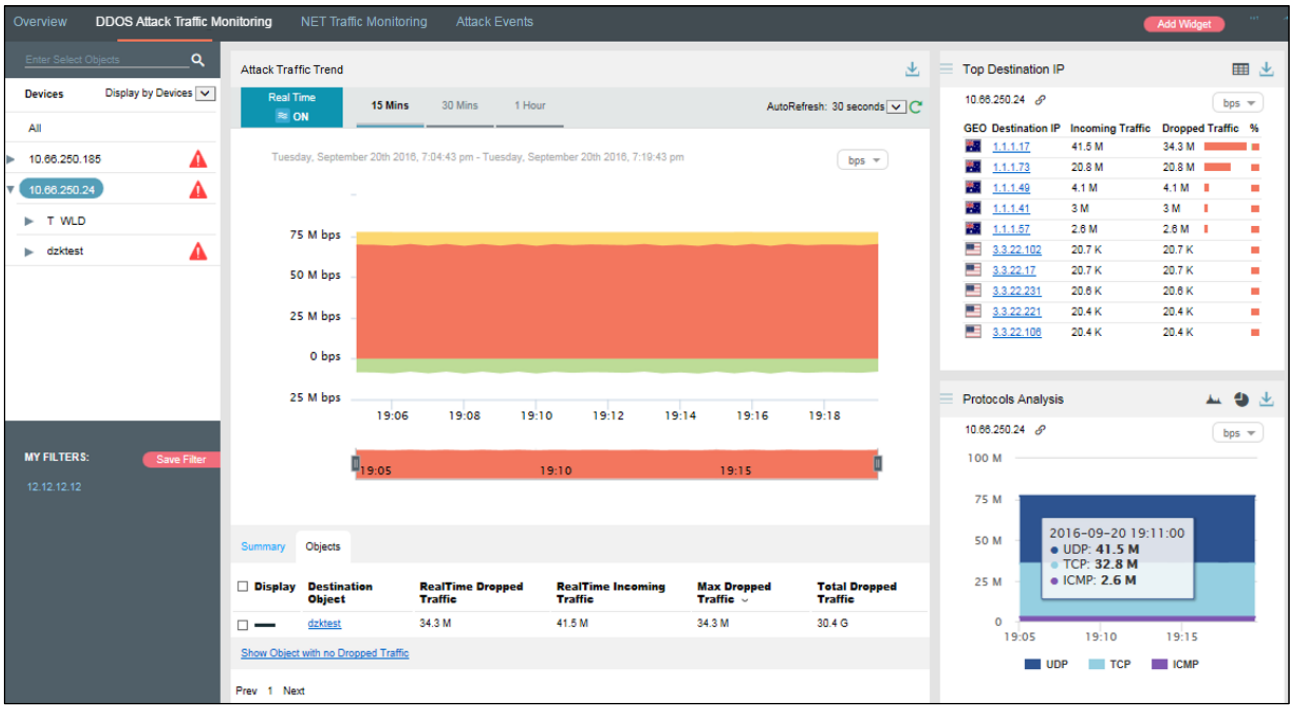
Figure 4-90 Traffic Monitoring page



4.2.3 Viewing Device-Specific Traffic Information

On the page shown in Figure 4-81, you can select **Display by Devices** from the drop-down list in the left pane and then select a device to view real-time attack traffic information of an ADS device, ADS-protected group, and specific IP addresses under a protection group. You can view historical and real-time attack traffic trends and panels of a selected ADS, ADS-protected group, and IP address under a protection group. For example, you can choose **10.66.250.24 > dzktest** to view traffic information of group **dzktest** protected by device 10.66.250.45.

Figure 4-91 Device-specific traffic information



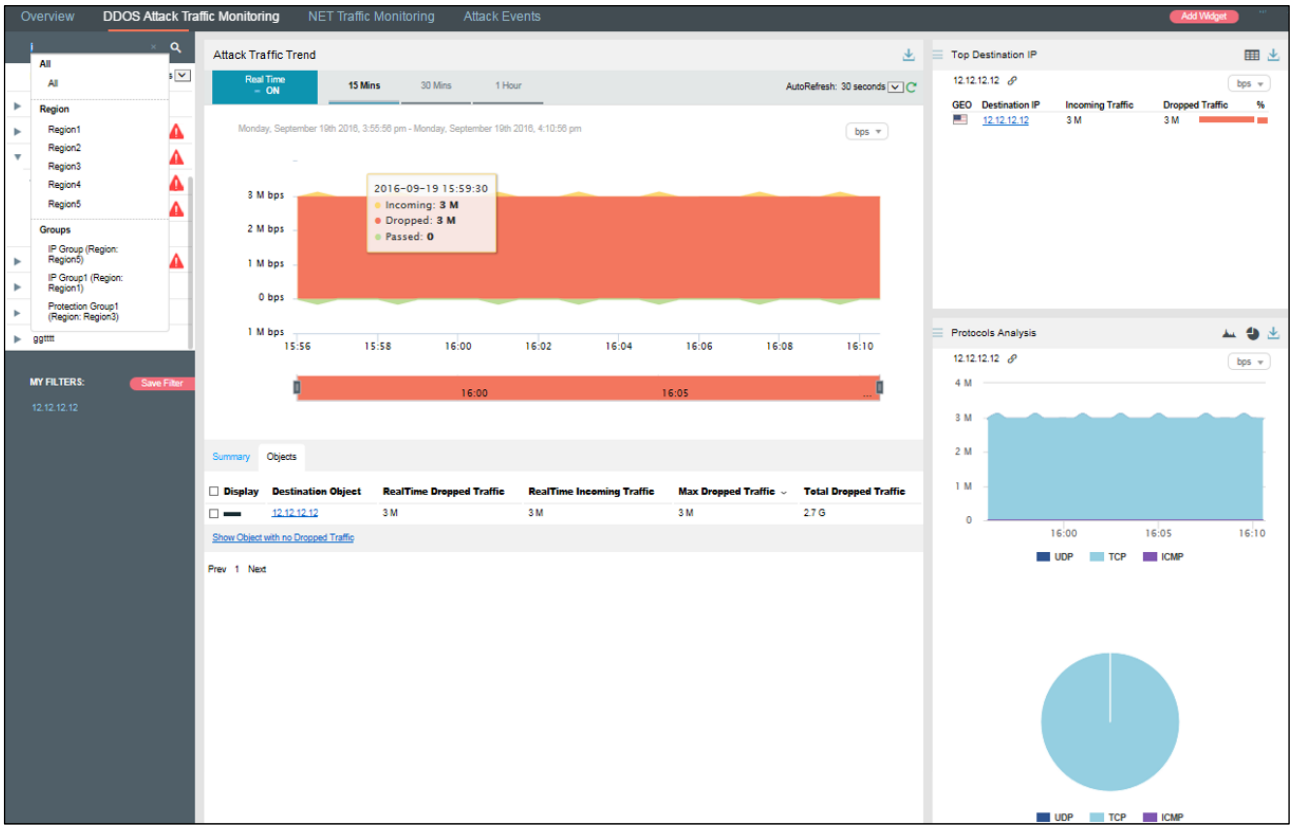
4.2.4 Viewing Object-Specific Traffic Information

By default, the **Attack Traffic Trend** graph displays attack traffic trends of all ADS devices monitored by ADS M. You can view the real-time attack traffic trends of a specified region, region IP group, ADS device, ADS-protected group, or IP address.

Step 1 On the page shown in Figure 4-81, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

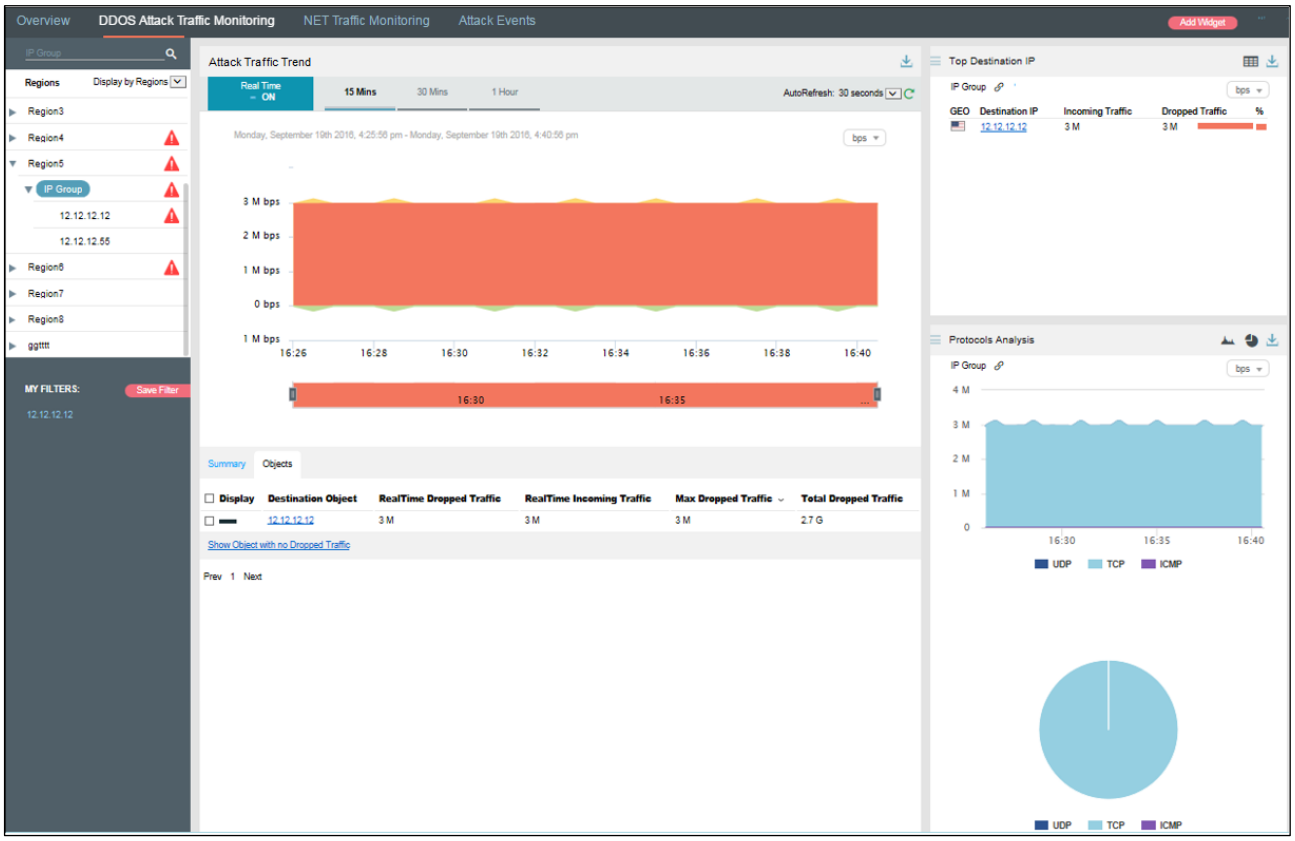
Figure 4-92 Searching for a traffic monitoring object



Step 2 Select an object to be queried, such as **IP Group (Group: Regions)**, and then press **Enter**.

Traffic information of the selected object is displayed.

Figure 4-93 Traffic information of a specified object



----End

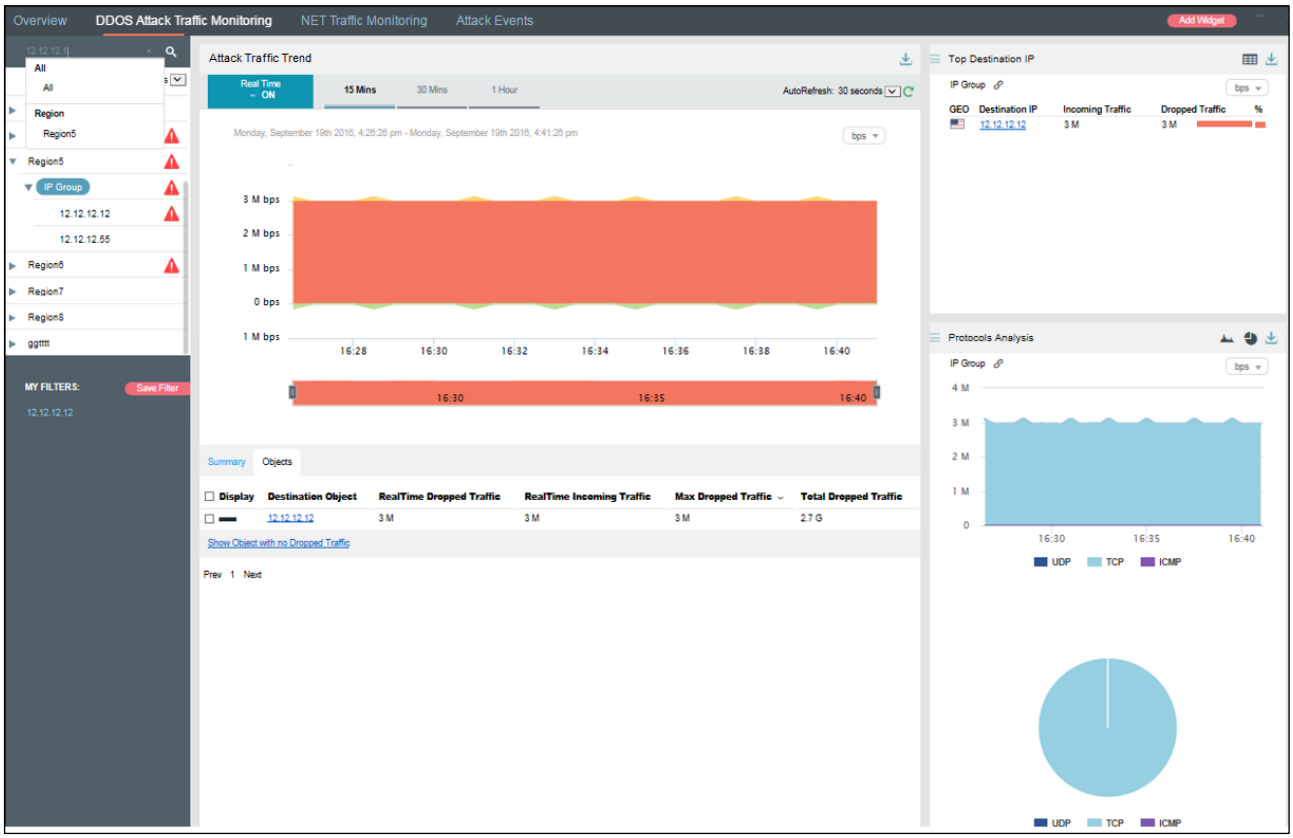
4.2.5 Viewing Traffic Information of an IP Address in the Default Protection Group

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view traffic information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

Step 1 On the page shown in Figure 4-81, type an IP address (such as 12.12.12.12) and then press **Enter**.

The system displays all objects containing this IP address.

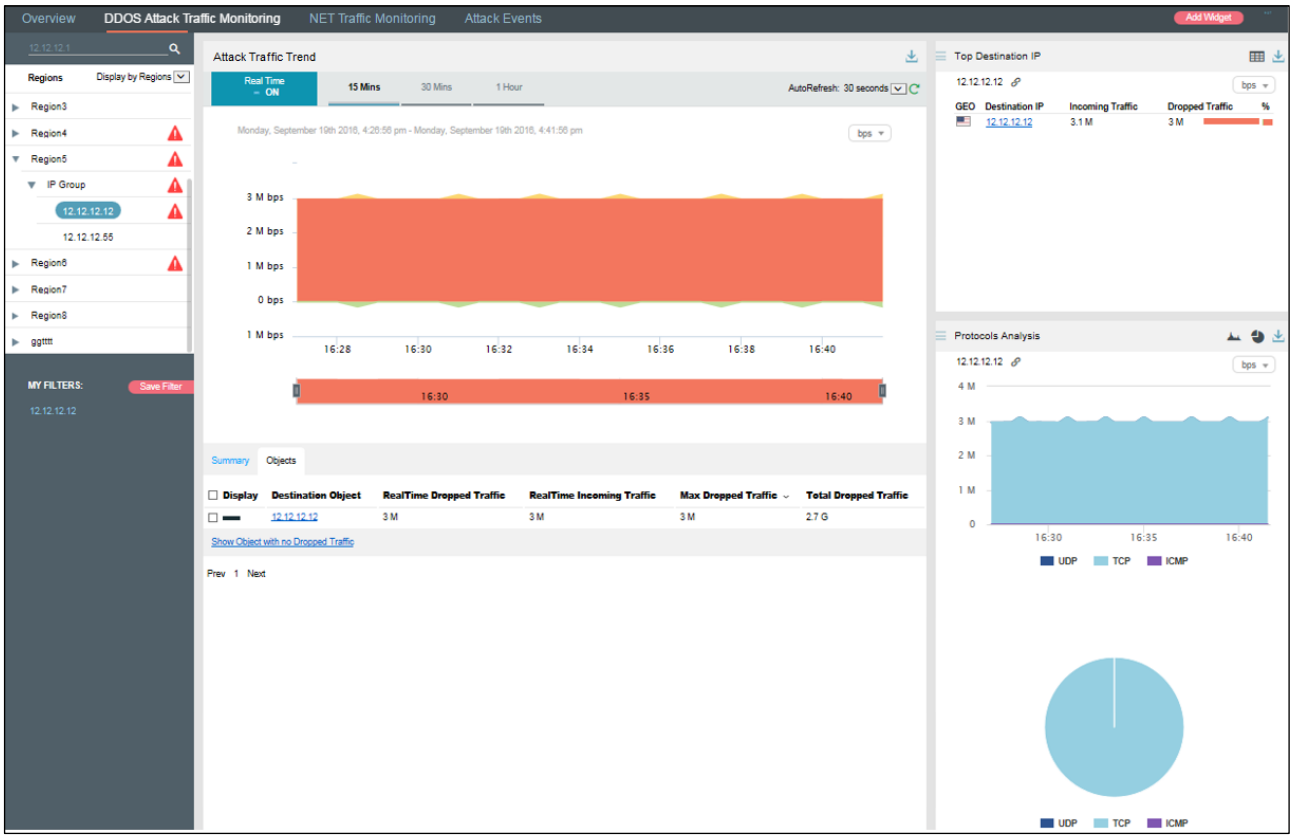
Figure 4-94 Searching for a traffic monitoring object



Step 2 Select the object to be queried and then press **Enter**.

Attack traffic information of this IP address is displayed.

Figure 4-95 Attack traffic information of an IP address in the default protection group



----End

4.2.6 Viewing Historical Attack Traffic Trends

To view historical attack traffic trends, follow these steps:

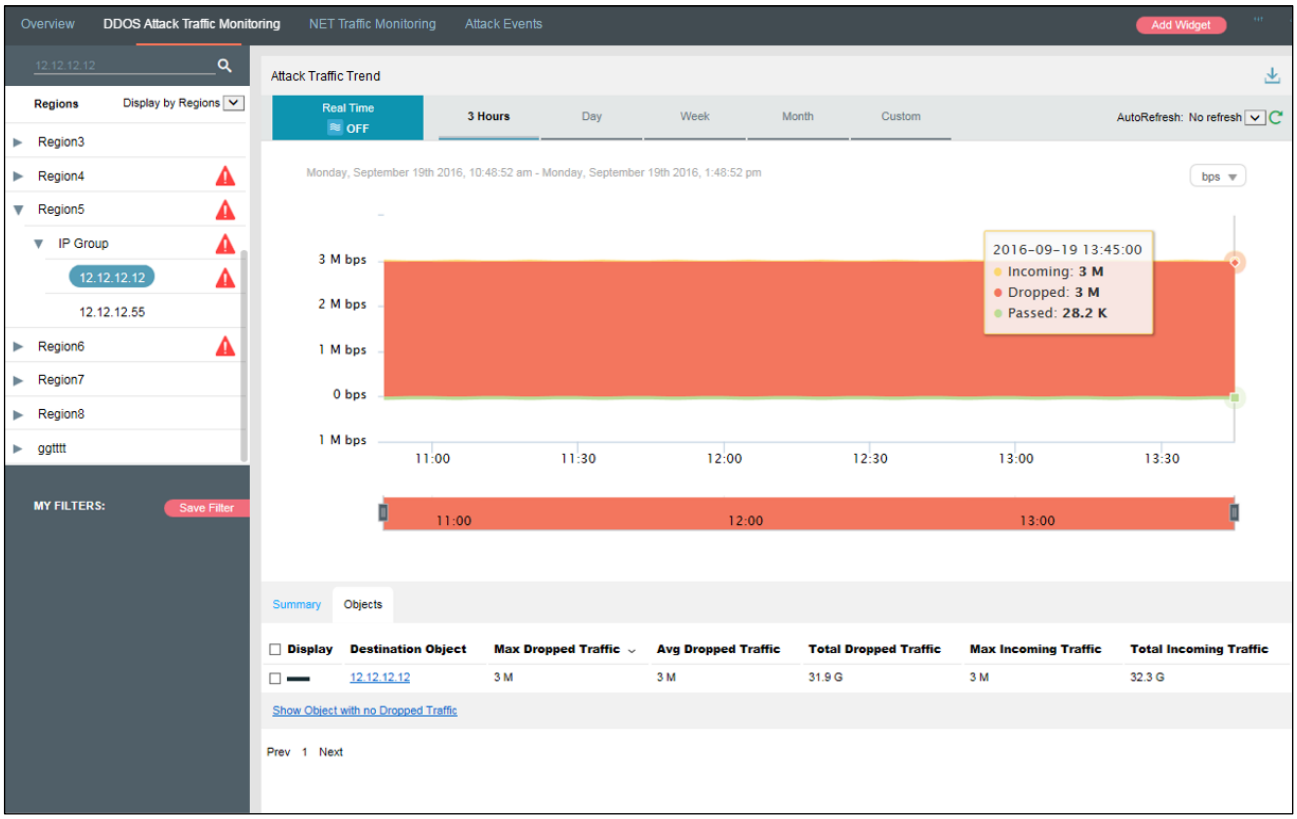
Step 1 On the page shown in Figure 4-81, click **ON** for **Real Time** in the **Attack Traffic Trend** area to disable the real-time mode and enable the historical mode.

Clicking **OFF** for **Real Time** enables the real-time mode again.

In historical mode, attack traffic trend graphs and panels with the icon display historical data

By default, the traffic attack trend graph displays traffic data in the last 3 hours. Clicking **Day**, **Week**, **Month**, or **Custom** displays attack traffic trend graphs in the last day, week, month, or a custom period.

Figure 4-96 Historical attack traffic – objects



The object list shows region names and detailed traffic information in descending order of dropped traffic volume.

Table 4-6 Historical attack traffic trend – parameters on the Objects tab page

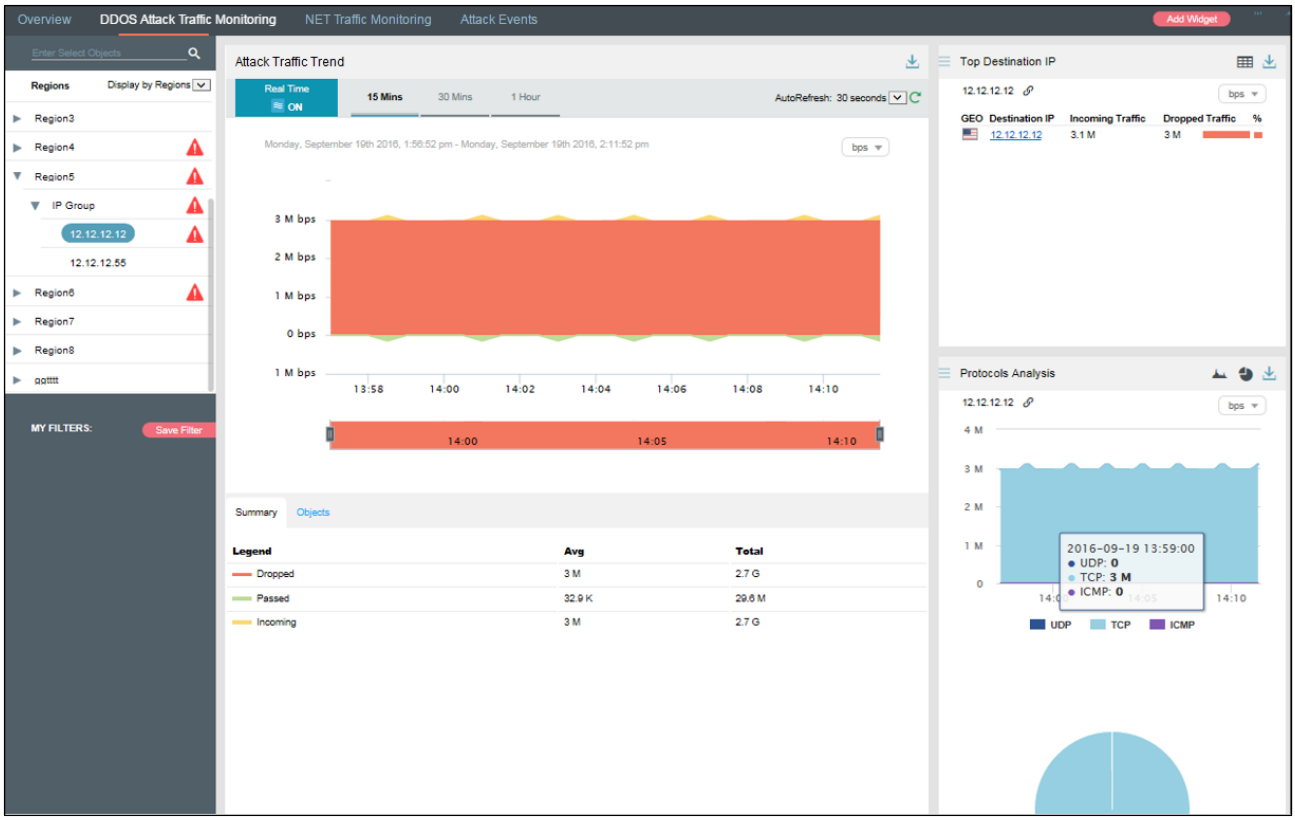
Parameter	Description
Display	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.
Destination Object	Indicates the traffic monitoring object.
Max Dropped Traffic	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Avg Dropped Traffic	Indicates the average traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Total Dropped Traffic	Indicates the total traffic (in bits) dropped by ADS for the object in the statistical period.
Max Incoming Traffic	Indicates the maximum traffic (in bps or pps) received by ADS for the object in the statistical period.
Total Incoming Traffic	Indicates the total traffic (in bits) received by ADS for the object in the statistical period.

Step 2 On the page shown in Figure 4-96, click **Summary**.

The summary of the historical attack traffic trend graph is displayed, including the average and total dropped, forwarded, and received traffic in the statistical period.

Clicking the bar or text in the **Legend** column hides or displays this type of traffic in the attack traffic trend graph. By default, all types of traffic are displayed. A dimmed color indicates that this type of traffic is not displayed. Otherwise, the traffic is displayed.

Figure 4-97 Historical attack traffic – summary



----End

4.2.7 Switching the Traffic Unit

By default, traffic is expressed in bps in the attack traffic trend graph. On the page shown in Figure 4-81, you can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic Trend** panel to display traffic data in pps.

4.2.8 Refreshing the Attack Traffic Trend Graph

By default, the attack traffic trend graph automatically refreshes every 30 seconds in real time mode. On the page shown in Figure 4-81, you can select **No refresh** from the **AutoRefresh** drop-down list in the upper-right corner of the **Attack Traffic Trend** panel. In this case, the attack traffic trend graph can be refreshed only by clicking .

By default, the attack traffic trend graph does not automatically refresh in historical mode. On the page shown in Figure 4-81, you can select **5 minutes** from the **AutoRefresh** drop-down

list in the upper-right corner of the **Attack Traffic Trend** panel. In this case, the attack traffic trend graph will refresh every 5 minutes.

4.2.9 Downloading a Traffic Trend Report

On the page shown in Figure 4-81, you can click in the upper-right corner to export the current data of the attack traffic trend graph as a report. For details, see 4.1.4 Downloading a Report.

4.2.10 Managing Filters

Filters are provided for users to define objects of their concern, so that they can find monitored objects more conveniently. After being created, filters are displayed in the filter list. You can click a filter to view traffic information of the object specified by the filter.

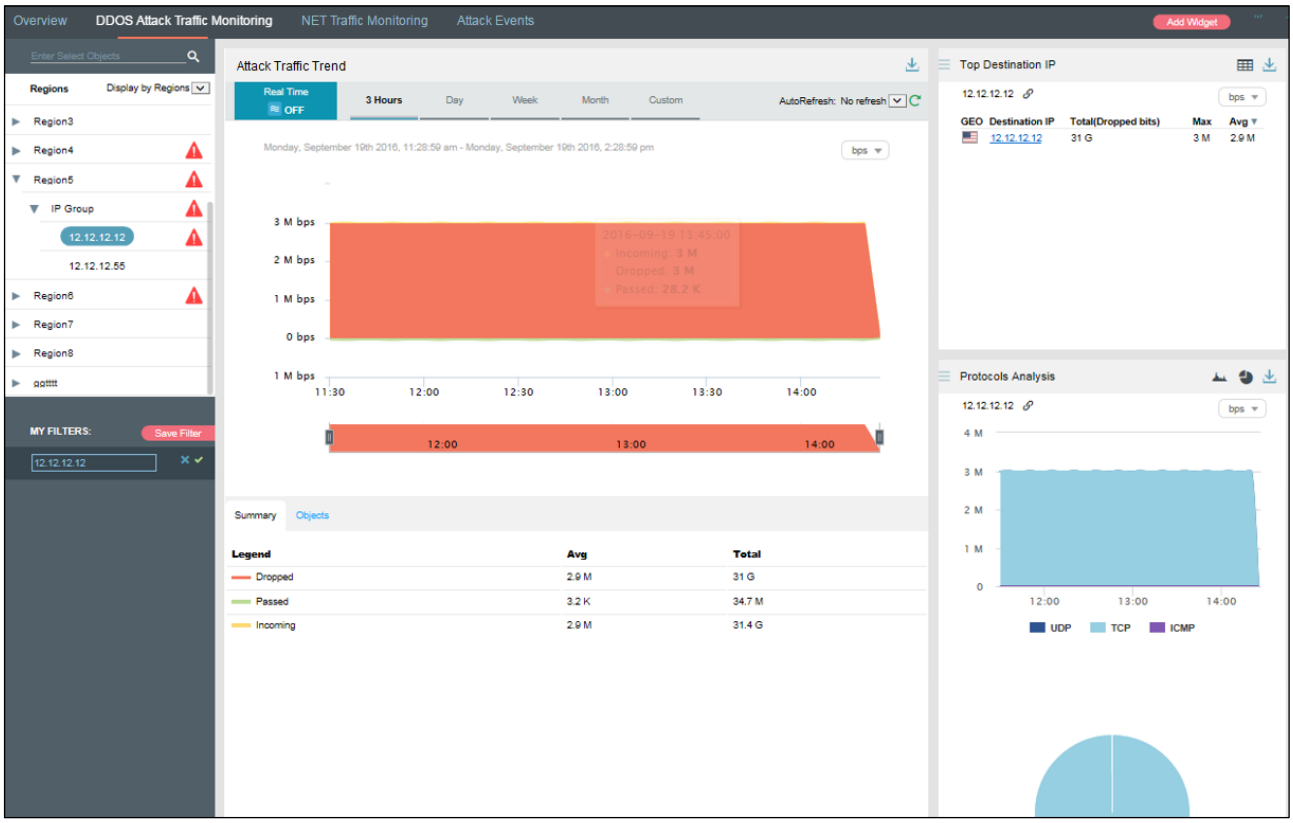
Any queried objects, such as a region, region IP group, ADS device, ADS-protected group, or IP address can be configured as a filter. But **All** and **Default IP (Default)** cannot be configured as a filter. You can configure multiple filters.

4.2.10.1 Configuring a Filter

To configure a filter, follow these steps:

Step 1 On the page shown in Figure 4-81, select an object from the left pane, such as 12.12.12.12, and then click **Save Filter**.

Figure 4-98 Adding a filter



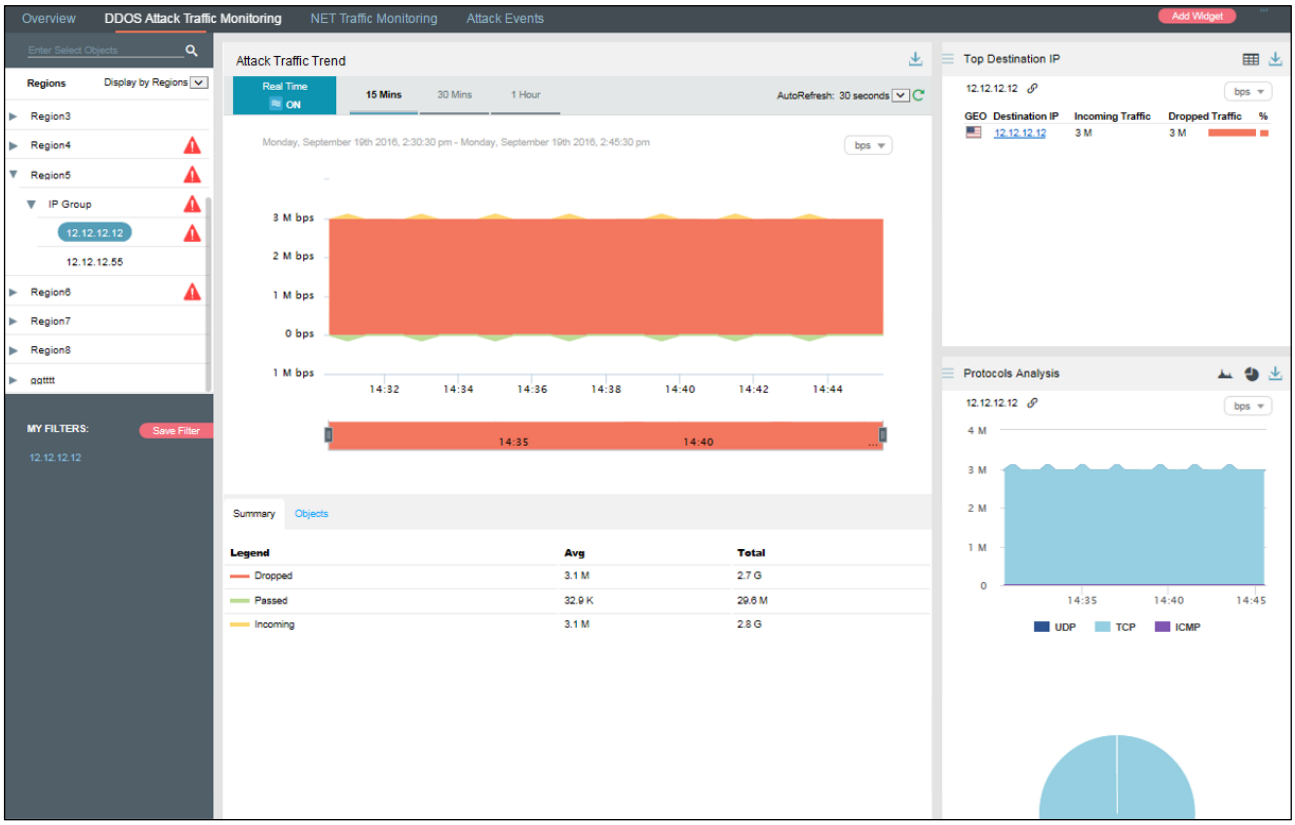
Step 2 Type the filter name.

By default, the object name is displayed as the filter name. You can use the default name or type a new one.

Step 3 Click and click **Confirm** in the dialog box that appears.

Step 4 Click **12.12.12.12** in the filter list to view its traffic information.

Figure 4-99 Viewing a filter



----End

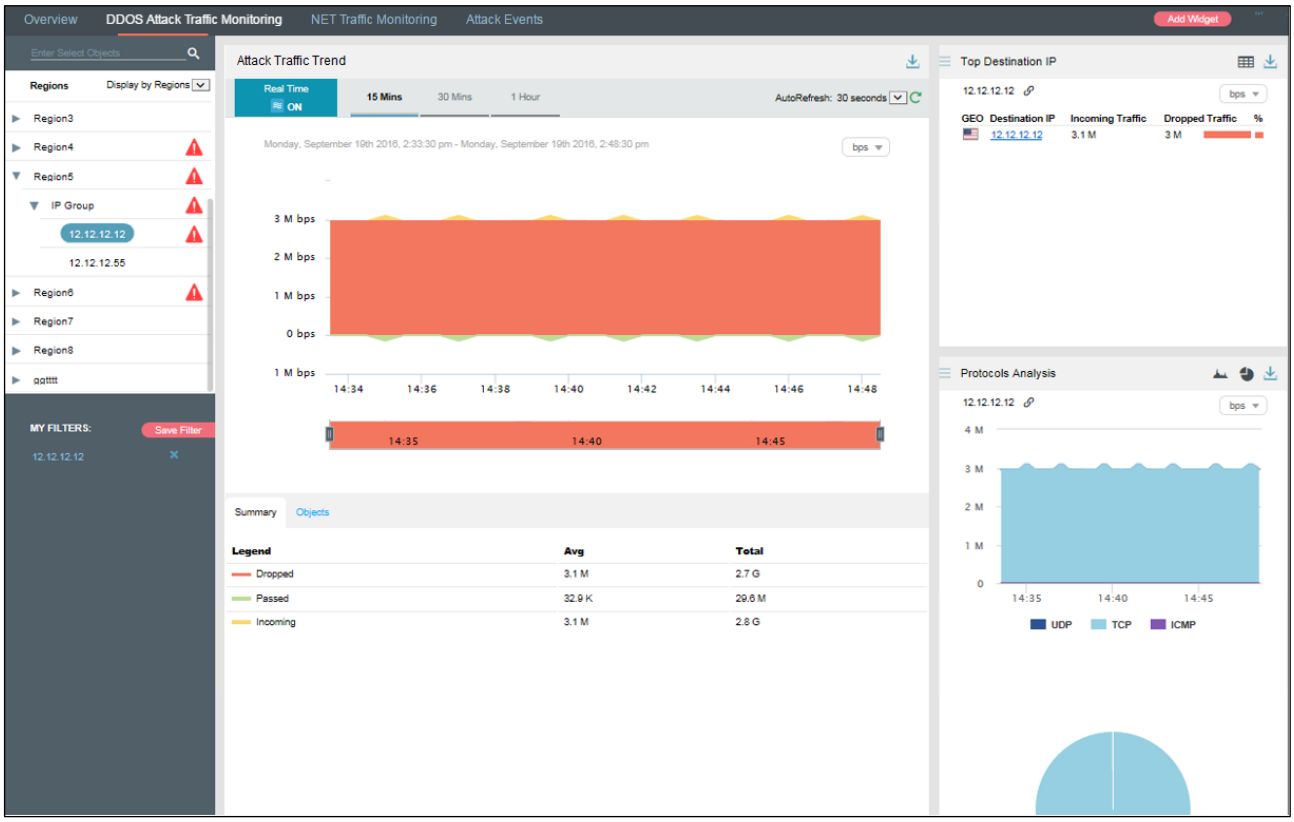
4.2.10.2 Deleting a Filter

To delete a filter, follow these steps:

Step 1 On the page shown in Figure 4-99, point to a filter name

The icon appears.

Figure 4-100 Deleting a filter



Step 2 Click and then **Confirm** in the dialog box that appears.

----End

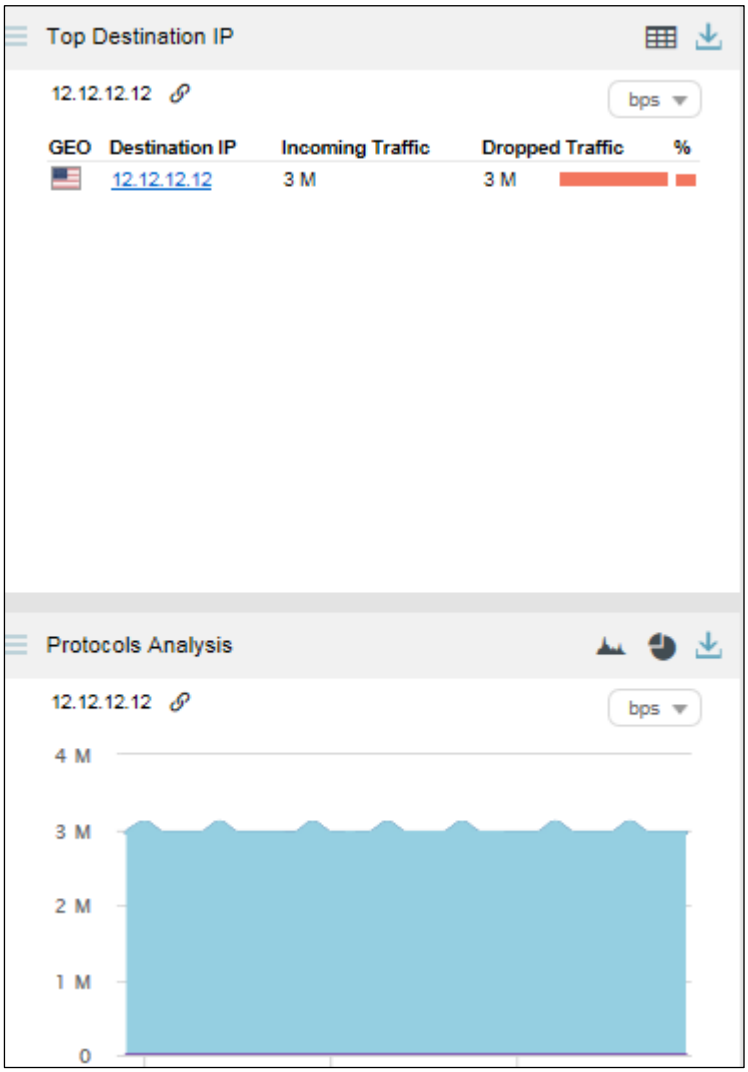
4.2.11 Managing Panels

By default, **Top Destination IP** and **Protocols Analysis** panels are displayed under **Traffic monitoring > DDOS Attack Traffic Monitoring**, as shown in Figure 4-101.

A panel with the icon indicates that when the selected object and statistical period change, the object and statistical period of this panel will change accordingly. A panel without the icon indicates the opposite.

You can add panels as required. For how to add, edit, and delete panels, see section 4.1 Overview.

Figure 4-101 Default panels on the DDOS Attack Traffic Monitoring page



4.3 Network Traffic Monitoring

Note	ADS M presents network traffic based on data uploaded by NTA devices.

Under **Traffic monitoring > NET Traffic Monitoring**, you can do as follows:

- View real-time and historical network traffic trends of all objects or a specified region, regional IP group, NTA device, or IP address.
- View or add panels.
- Configure filters.

IP addresses under the default protection group do not belong to any regions or IP groups. To view network traffic information of such an IP address, you need to expressly specify the IP address before the system displays its information.

Network traffic information includes real-time traffic information and historical traffic information. By default, network traffic information is displayed by region.

4.3.1 Viewing Real-Time Network Traffic Information

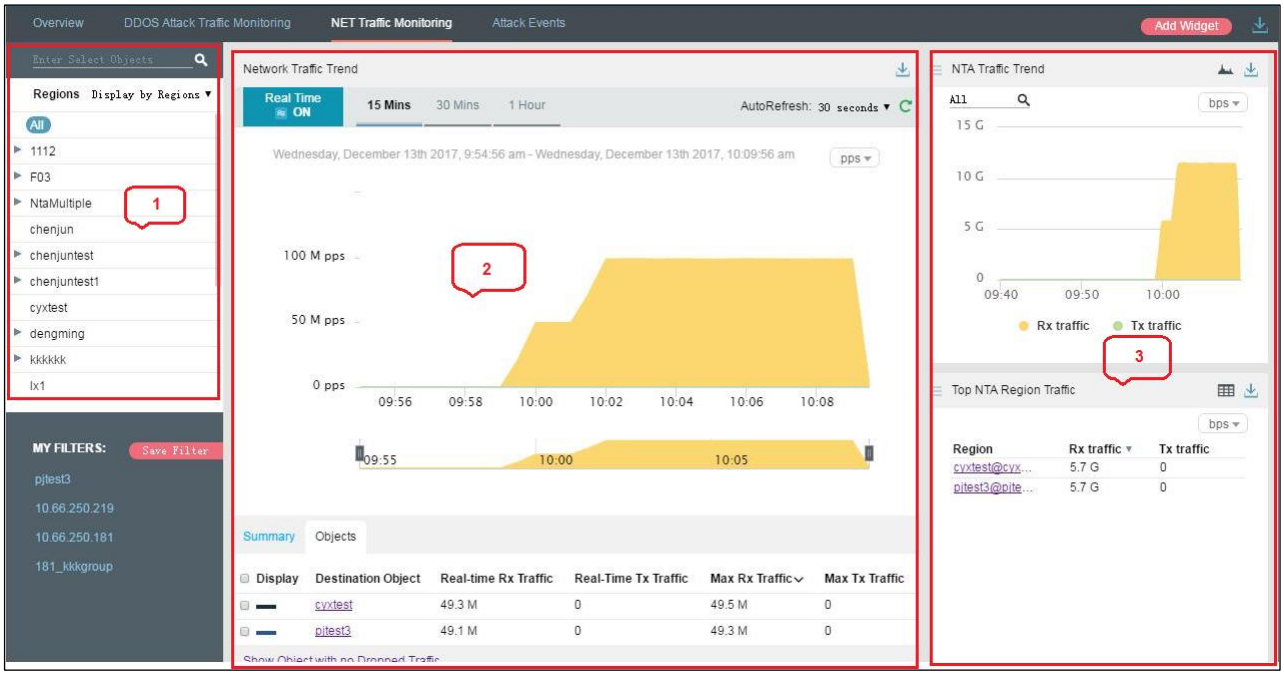
To view real-time network traffic information, follow these steps:

Step 1 Choose **Traffic monitoring > NET Traffic Monitoring**.

By default, real-time network traffic information of all monitoring objects is displayed, including **Network Traffic Trend**, and **NTA Traffic Trend** and **Top NTA Region Traffic** panels, as shown in Figure 4-102.

In real-time mode, the network traffic trend in the last 15 minutes is displayed by default. You can click **30 Mins** or **1 Hour** to view the network traffic trend of the last 30 minutes or last hour.

Figure 4-102 Network traffic information of all objects



① List of objects ② Traffic trend ③ Panels

On the **NET Traffic Monitoring** page, the **Objects** list ranks regions in descending order of real-time network traffic detected.

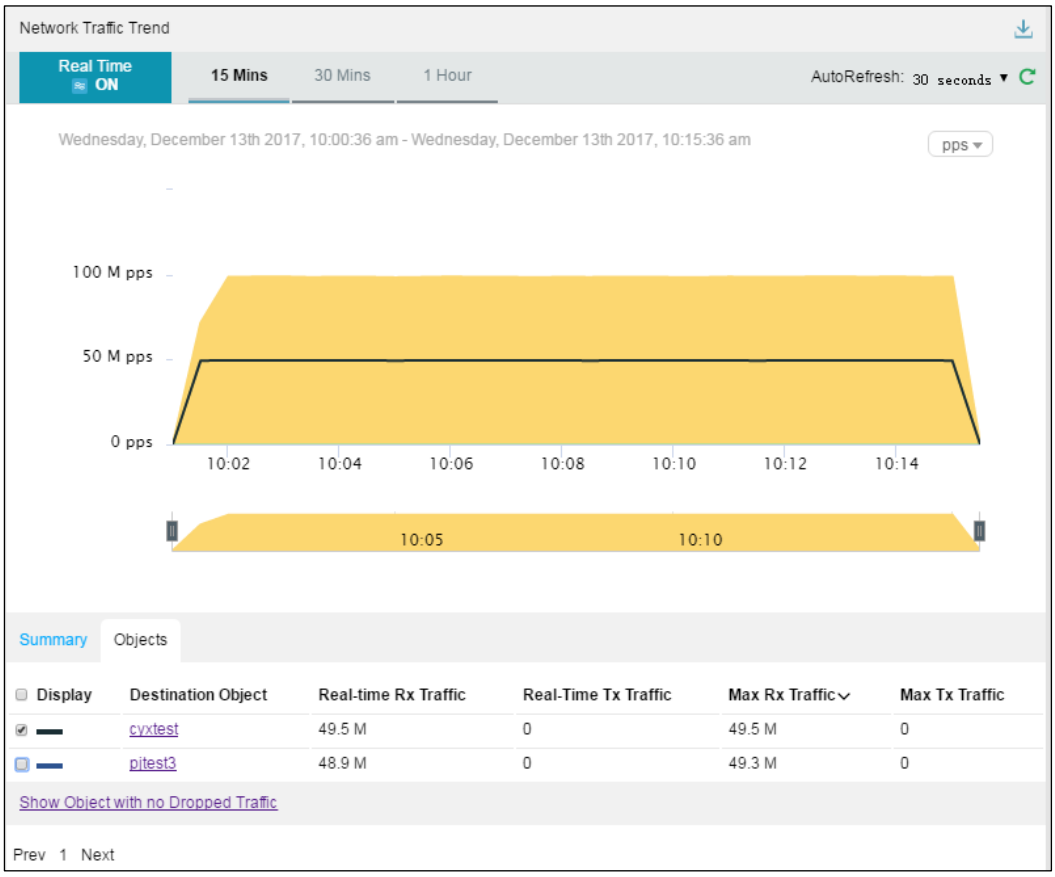
Table 4-7 Real-time network traffic trend – parameters on the Objects tab page

Parameter	Description
Display	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.

Parameter	Description
Destination Object	Indicates the traffic monitoring object.
Real-Time Rx Traffic	Indicates traffic (in bps or pps) received by the object in real time.
Real-Time Tx Traffic	Indicates traffic (in bps or pps) transmitted by the object in real time.
Max Rx Traffic	Indicates the maximum traffic (in bps or pps) received by the object in the statistical period.
Max Tx Traffic	Indicates the maximum traffic (in bps or pps) transmitted by the object in the statistical period.

Step 2 On the **Objects** tab page shown in Figure 4-102, select one or more objects to view its or their real-time network traffic. See Figure 4-103.

Figure 4-103 Real-time network traffic trend graph of a specified object

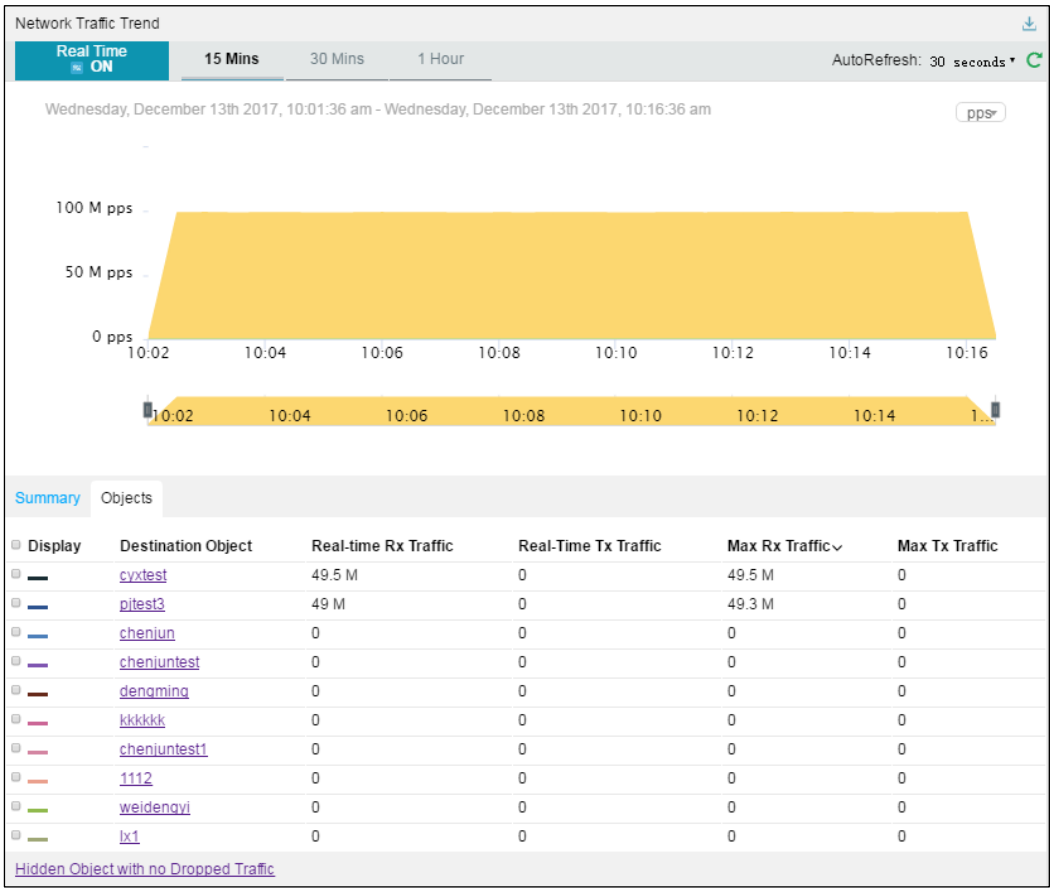


By default, only the objects with traffic dropped by ADS are displayed.

Step 3 Click the **Show Object with no Dropped Traffic** link to show all objects. See Figure 4-104.

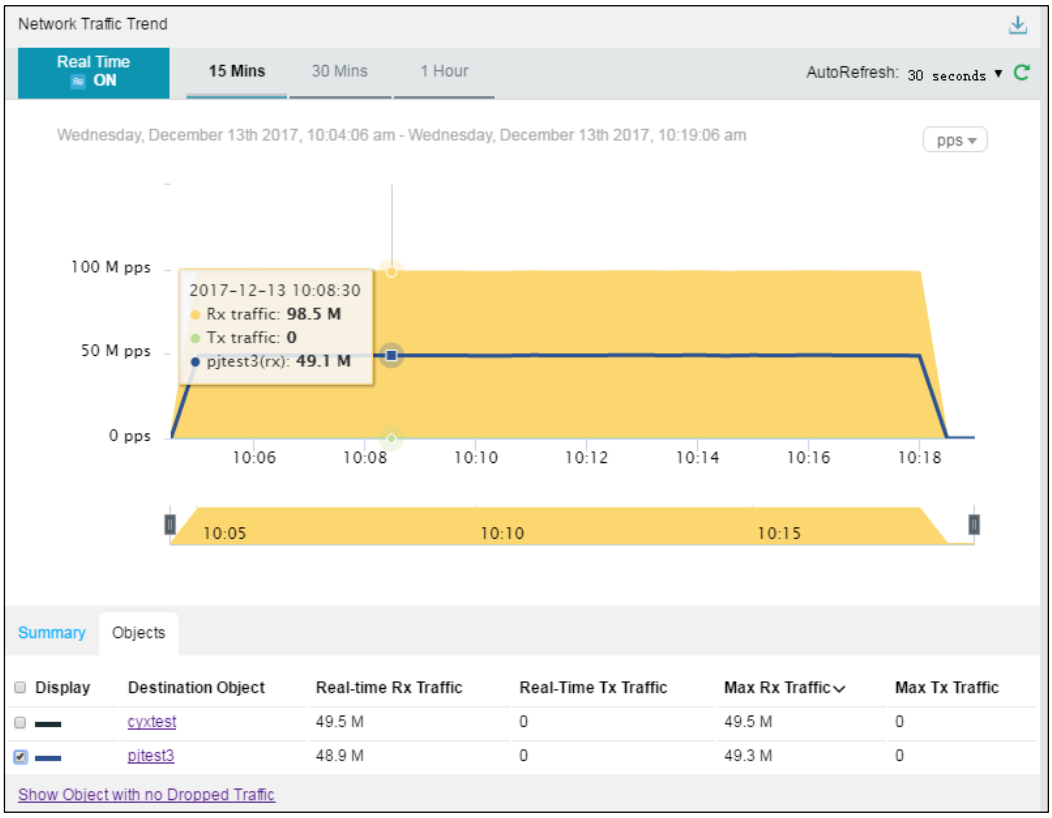
Clicking the **Hidden Object with no Dropped Traffic** link displays only objects with traffic dropped by ADS, but hides objects with no traffic dropped.

Figure 4-104 Real-time network traffic trend graph of all objects



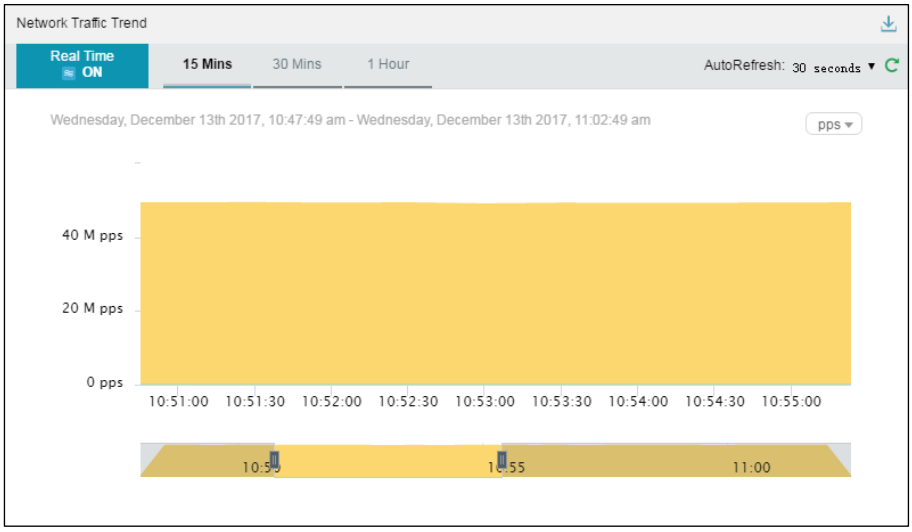
Step 4 Point to a random point in the network traffic trend graph to view the incoming traffic, outgoing traffic, and dropped traffic at the specific point of time, as well as real-time traffic dropped for the specified object. See Figure 4-105.

Figure 4-105 Network traffic information at a specific time



Step 5 Below the network traffic trend graph, drag to view a finer-granularity network traffic trend.

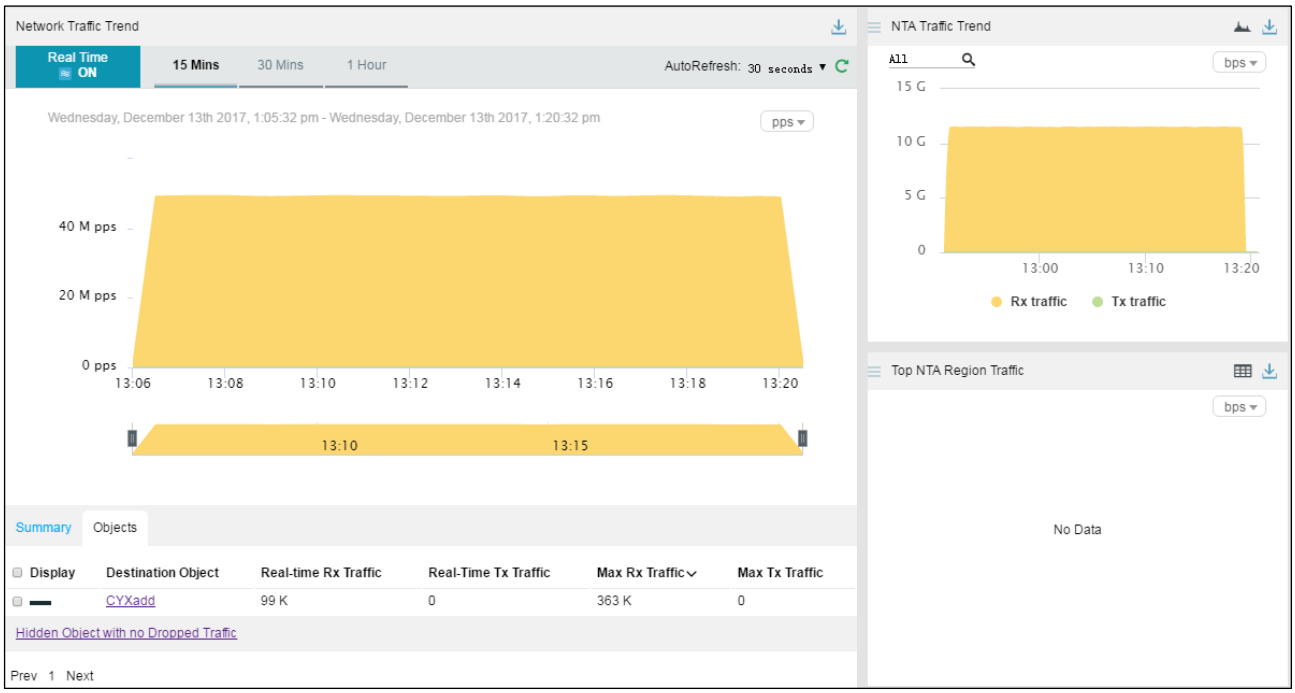
Figure 4-106 Finer-granularity network traffic information



Step 6 Click the link of a region or regional IP group in the **Destination Object** column.

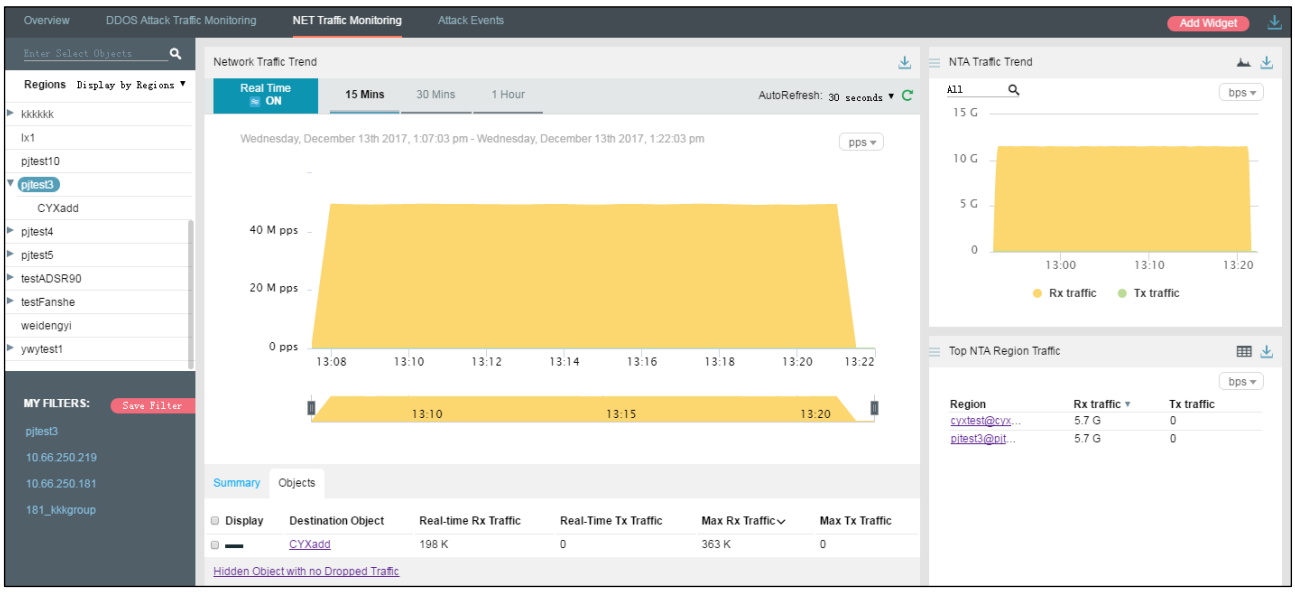
Traffic information of this region or regional IP group is displayed, including the network traffic trend graph, top NTA's regions by traffic, and NTA traffic trend, as shown in Figure 4-107.

Figure 4-107 Network traffic of a specific region



In addition, associated region information will be displayed in the left search pane, as shown in Figure 4-108.

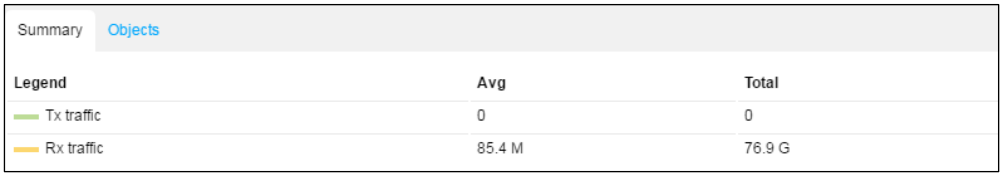
Figure 4-108 Associated region information displayed



Step 7 On the page shown in Figure 4-107, click **Summary**.

The average and total traffic received and transmitted in the statistical period are displayed, as shown in Figure 4-109.

Figure 4-109 Summary of network traffic monitoring information



Clicking the bar or text in the **Legend** column hides or displays this type of traffic in the traffic trend graph. By default, all types of traffic are displayed. A dimmed color indicates that this type of traffic is not displayed. Otherwise, the traffic is displayed.

Table 4-8 describes parameters on the **Summary** tab page.

Table 4-8 Real-time network traffic trend – parameters on the Summary tab page

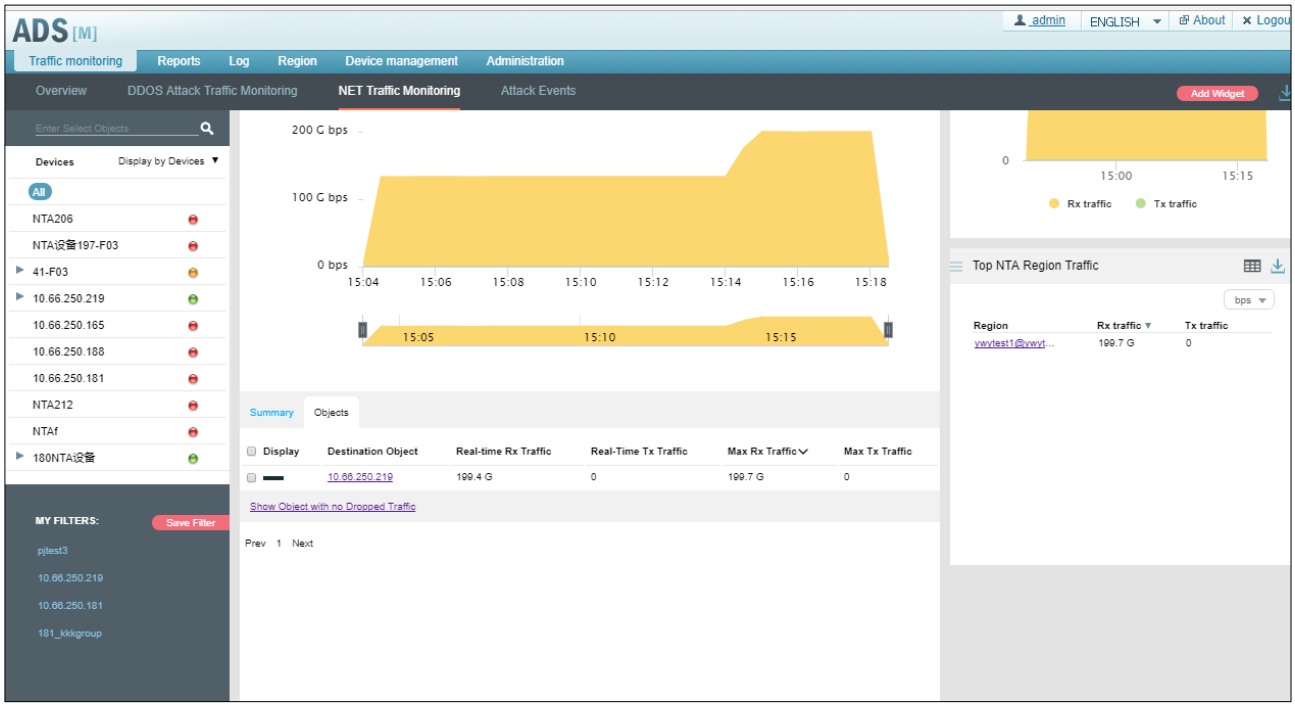
Parameter	Description
Legend	Colors representing transmitted and received traffic
Avg	Average traffic transmitted and received by the object
Total	Total traffic transmitted and received by the object

----End

4.3.2 Viewing Device-Specific Network Traffic Information

In the left pane of the **NET Traffic Monitoring** page, select **Display by Devices**. Then all NTA devices and regions and regional IP groups configured on these devices are listed. indicates that time of this device is not synchronized. indicates that this device is offline. indicates that this device is online. You can select an NTA device or a region/regional IP group under an NTA device to view its real-time and historical network traffic trends and panels. For example, select **10.66.250.219 > pjtest3@pjtest3**. Then network traffic information of region pjtest3 under device 10.66.250.219 is displayed, as shown in Figure 4-110.

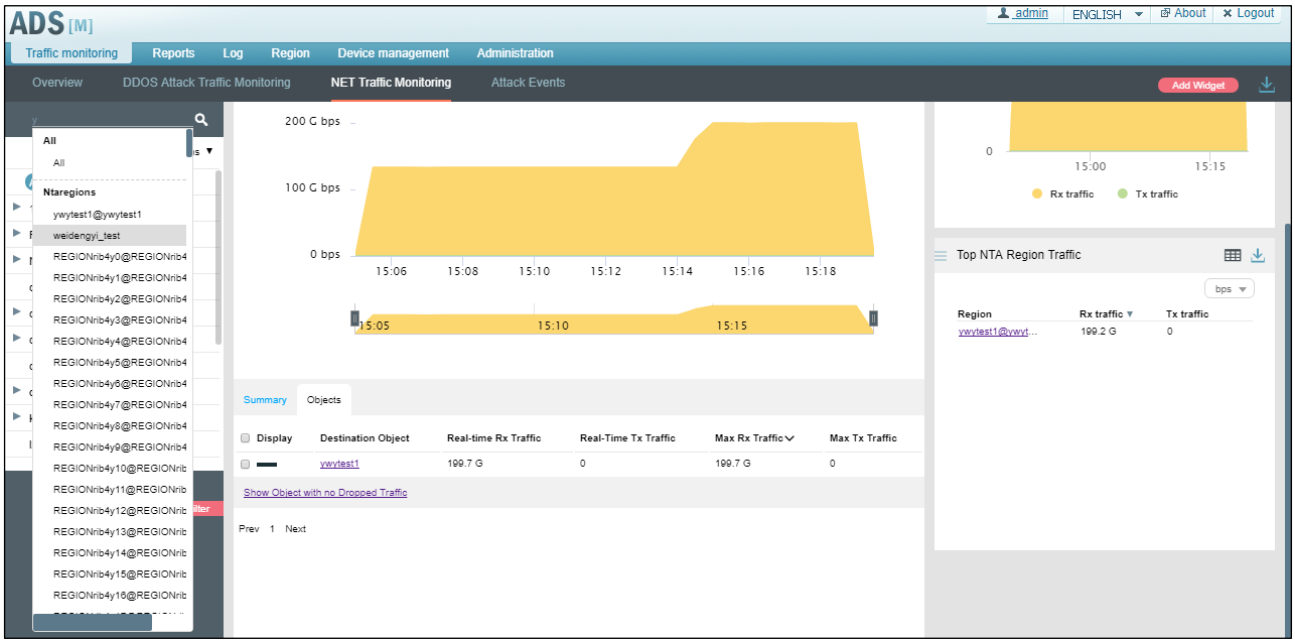
Figure 4-110 Device-specific network traffic information



4.3.3 Viewing Region-Specific Network Traffic Information

In the left pane of the **NET Traffic Monitoring** page, select **Display by Regions**. Then all regions and IP groups and IP addresses in these regions are displayed. You can select a region, an IP group, or an IP address to view its real-time and historical network traffic trends and panels. For example, select **pjtest3**. Then network traffic information of region pjtest3 is displayed, as shown in Figure 4-111.

Figure 4-111 Region-specific network traffic information



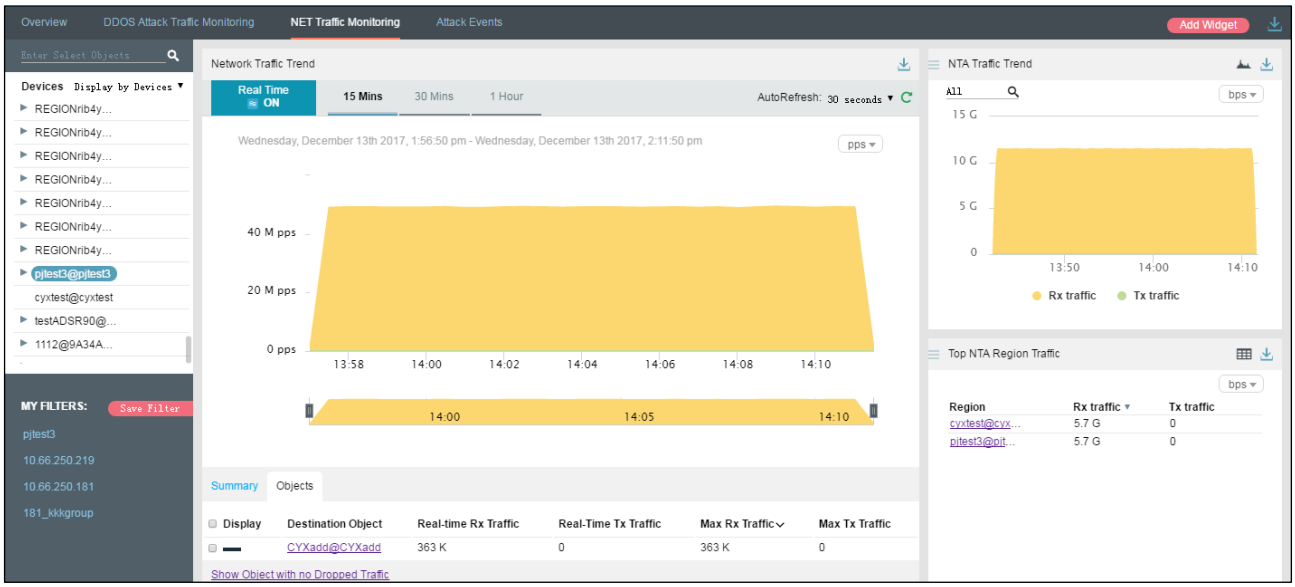
4.3.4 Viewing IP Group-Specific Network Traffic Information

Step 1 In the left pane of the NET Traffic Monitoring page, select Display by Devices.

Step 2 From the device list displayed, select an IP group under an NTA device.

Then real-time network traffic information of this IP group is displayed, as shown in Figure 4-112.

Figure 4-112 IP group-specific network traffic information



----End

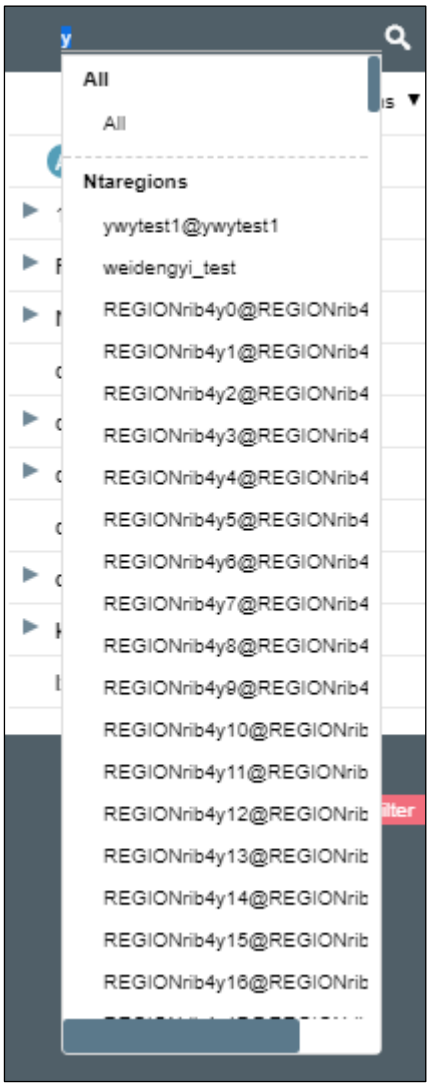
4.3.5 Viewing Object-Specific Network Traffic Information

By default, the **Attack Traffic Trend** graph displays network traffic trends of all NTA devices monitored by ADS M. You can specify an object, namely a region, regional IP group, or NTA device, to view its real-time network traffic trends.

Step 1 In the left pane, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-113.

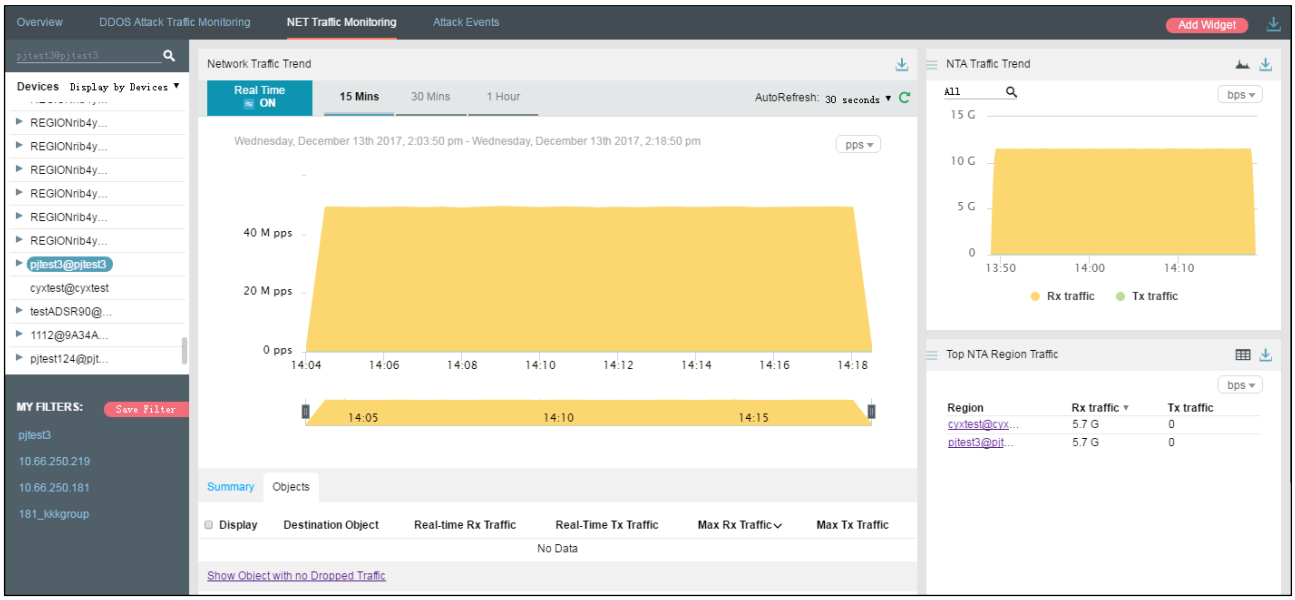
Figure 4-113 Searching for a network traffic monitoring object



Step 2 Select an object to be queried, such as **pjtest3@pjtest3**, and then press **Enter**.

Network traffic information of the selected object is displayed, as shown in Figure 4-114.

Figure 4-114 Object-specific network traffic information



----End

4.3.6 Viewing Historical Network Traffic Trends

To view historical network traffic trends, follow these steps:

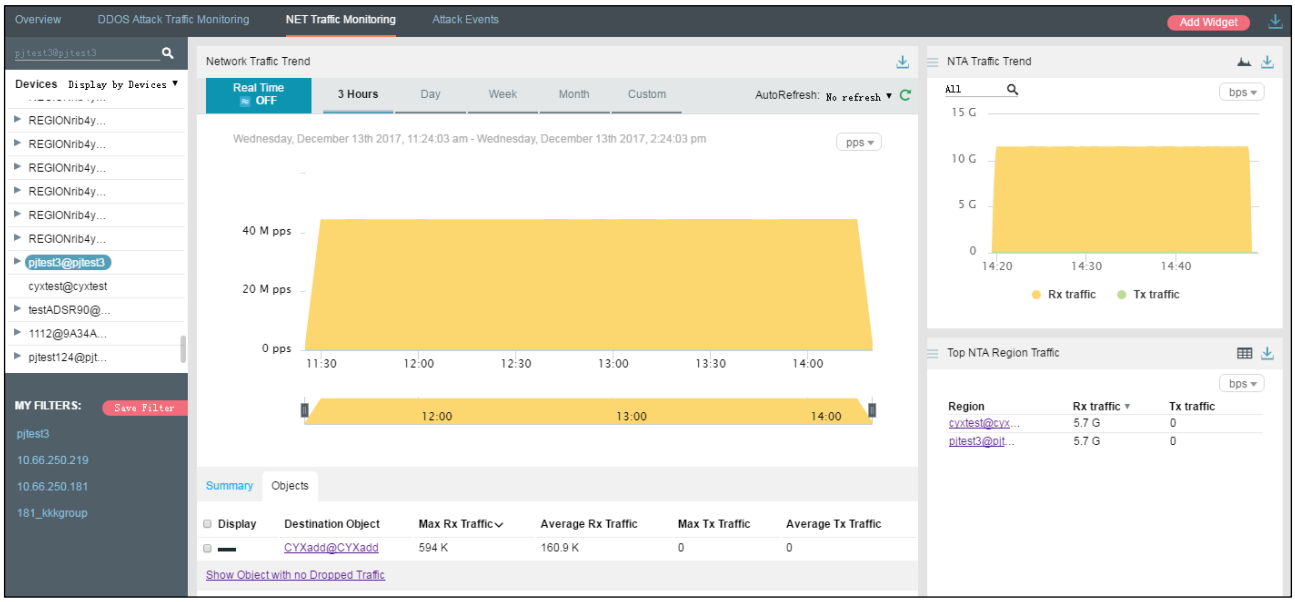
Step 1 On the **NET Traffic Monitoring** page, click **ON** for **Real Time** in the **Network Traffic Trend** area to disable the real-time mode and enable the historical mode. See Figure 4-115.

Clicking **OFF** for **Real Time** enables the real-time mode again.

In historical mode, both the network traffic trend graph and panels with the icon display historical data.

By default, the network traffic trend graph displays network traffic data in the last 3 hours. Clicking **Day**, **Week**, **Month**, or **Custom** displays the network traffic trend in the last day, week, month, or a custom period.

Figure 4-115 Historical network traffic – objects



The **Objects** tab page provides detailed network traffic information of regions, which are ranked in descending order of traffic volume.

Table 4-9 Historical network traffic trend – parameters on the Objects tab page

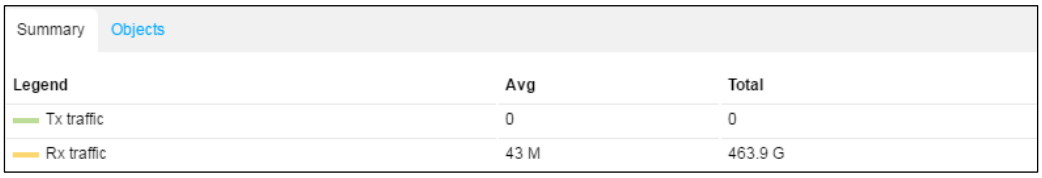
Parameter	Description
Display	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.
Destination Object	Indicates the traffic monitoring object.
Max Rx Traffic	Indicates the maximum traffic (in bps or pps) received by the object in the statistical period.
Average Rx Traffic	Indicates the average traffic (in bps or pps) received by the object in the statistical period.
Max Tx Traffic	Indicates the maximum traffic (in bps or pps) transmitted by the object in the statistical period.
Average Tx Traffic	Indicates the average traffic (in bps or pps) transmitted by the object in the statistical period.

Step 2 On the page shown in Figure 4-115, click **Summary**.

The average and total traffic received and transmitted in the statistical period are displayed, as shown in Figure 4-116.

Clicking the bar or text in the **Legend** column hides or displays this type of traffic in the network traffic trend graph. By default, all types of network traffic are displayed. A dimmed color indicates that this type of traffic is not displayed. Otherwise, the traffic is displayed. Table 4-8 describes parameters on the **Summary** tab page.

Figure 4-116 Historical network traffic – summary



----End

4.3.7 Switching the Traffic Unit

By default, traffic is expressed in bps in network traffic trend graphs. You can select **pps** from the drop-down list in the upper-right corner of the **Network Traffic Trend** area to display traffic in pps.

4.3.8 Refreshing the Traffic Trend Graph

By default, the network traffic trend graph automatically refreshes every 30 seconds in real-time mode. On the **NET Traffic Monitoring** page, you can select **No refresh** from the **AutoRefresh** drop-down list in the upper-right corner of the **Network Traffic Trend** panel. In this case, the network traffic trend graph does not refresh unless you click .

By default, the network traffic trend graph is not refreshed in historical mode. On the **NET Traffic Monitoring** page, you can select **5 minutes** from the **AutoRefresh** drop-down list in the upper-right corner of the **Network Traffic Trend** panel. In this case, the network traffic trend graph will automatically refresh every 5 minutes.

4.3.9 Downloading a Traffic Trend Report

On the **NET Traffic Monitoring** page, you can click in the upper-right corner of the **Network Traffic Trend** graph to download the current data of the network traffic trend graph as a report. For details, see section 4.1.4 Downloading a Report.

4.3.10 Managing Filters

Filters are provided for users to define objects of their concern, so that they can find monitored objects more conveniently. After being created, filters are displayed in the filter list. You can click a filter to view traffic information of the object specified by the filter.

Any queried object, such as a region, regional IP group, or NTA device, can be configured as a filter. But **All** and **Default IP (Default)** cannot be configured as a filter. You can configure multiple filters.

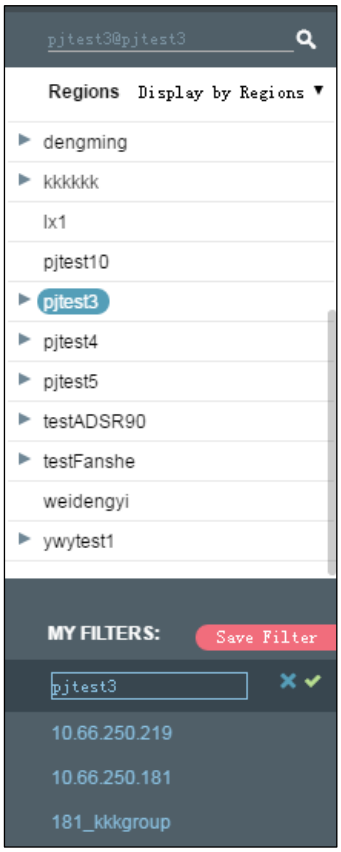
4.3.10.1 Configuring a Filter

To configure a filter, follow these steps:

Step 1 On the **NET Traffic Monitoring** page, select an object from the left pane, such as **pjtest3**, and then click **Save Filter**.

Then **pjtest3** appears in the filter list, as shown in Figure 4-117.

Figure 4-117 Creating a filter



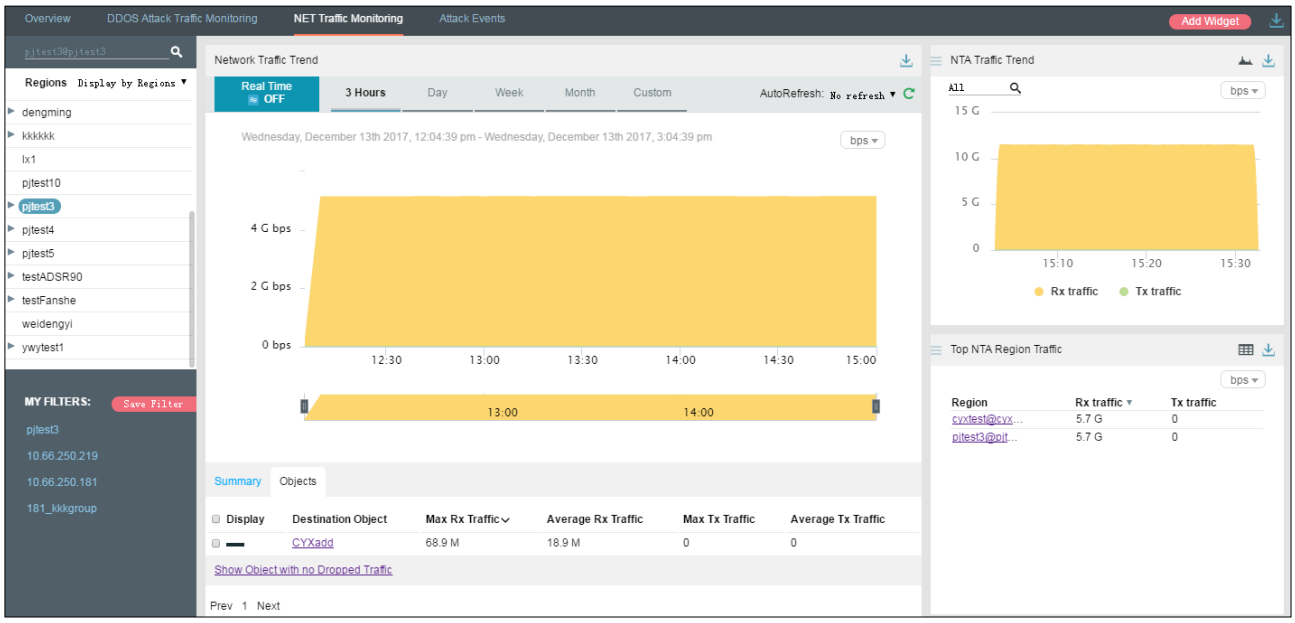
Step 2 Type the filter name.

By default, the object name is displayed as the filter name. You can use the default name or type a new one.

Step 3 Click and click **Confirm** in the dialog box that appears.

Step 4 Click **pjtest3** in the filter list to view its traffic information. See Figure 4-118.

Figure 4-118 Filtered network traffic information



----End

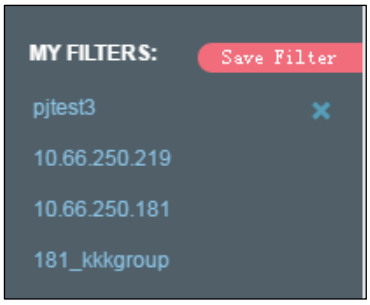
4.3.10.2 Deleting a Filter

To delete a filter, follow these steps:

Step 1 On the page shown in Figure 4-118, point to a filter name.

The icon appears, as shown in Figure 4-119.

Figure 4-119 Deleting a filter



Step 2 Click and then **Confirm** in the dialog box that appears.

----End

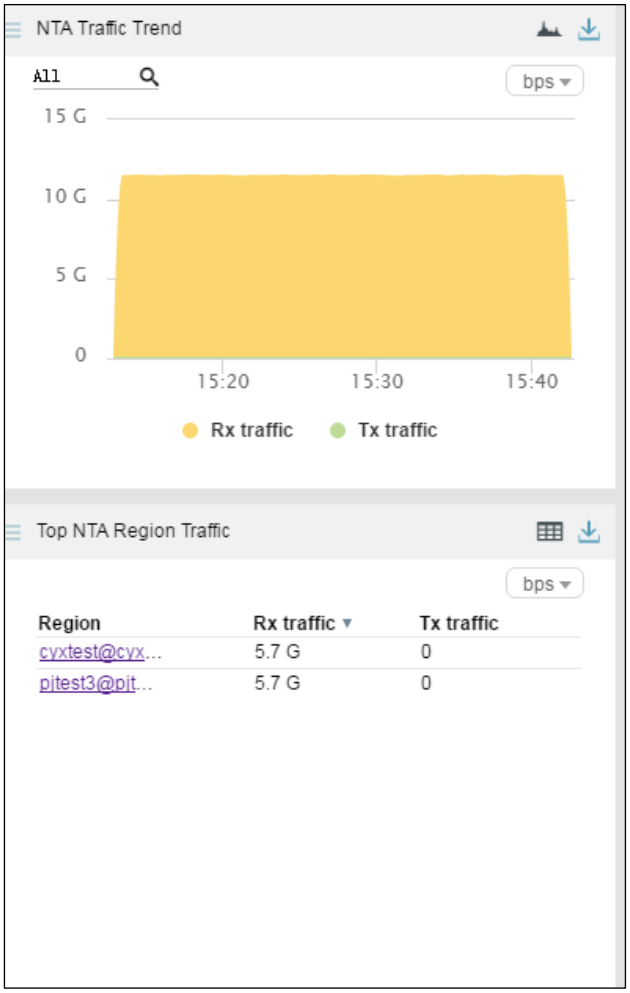
4.3.11 Managing Panels

On the **NET Traffic Monitoring** page, **NTA Traffic Trend** and **Top NTA Region Traffic** panels are displayed by default, as shown in Figure 4-120.

A panel with the icon indicates that when the selected object and statistical period change, the object and statistical period of this panel will change accordingly. A panel without the icon indicates the opposite.

You can add panels as required. For details about how to add, edit, and delete a panel, see section 4.1 Overview.

Figure 4-120 Default panels displayed on the NET Traffic Monitoring page



4.4 Attack Events

Under **Traffic monitoring > Attack Events**, you can do as follows:

- View real-time and historical attack events of all objects or a specified region, region IP group, ADS device, ADS-protected group, or IP address.
- View or add panels.
- Configure filters.

By default, when **Display by Regions** is selected, attack event information of all monitored regions is displayed in real time mode.

4.4.1 Viewing Attack Events in Real Time Mode

To view attack events in real time mode, follow these steps:

Step 1 Choose **Traffic monitoring > Attack Events**.

By default, attack traffic information of all monitored objects is displayed in real time mode, including top source countries, top 10 source IP addresses, and attack type distribution, as shown in Figure 4-121.

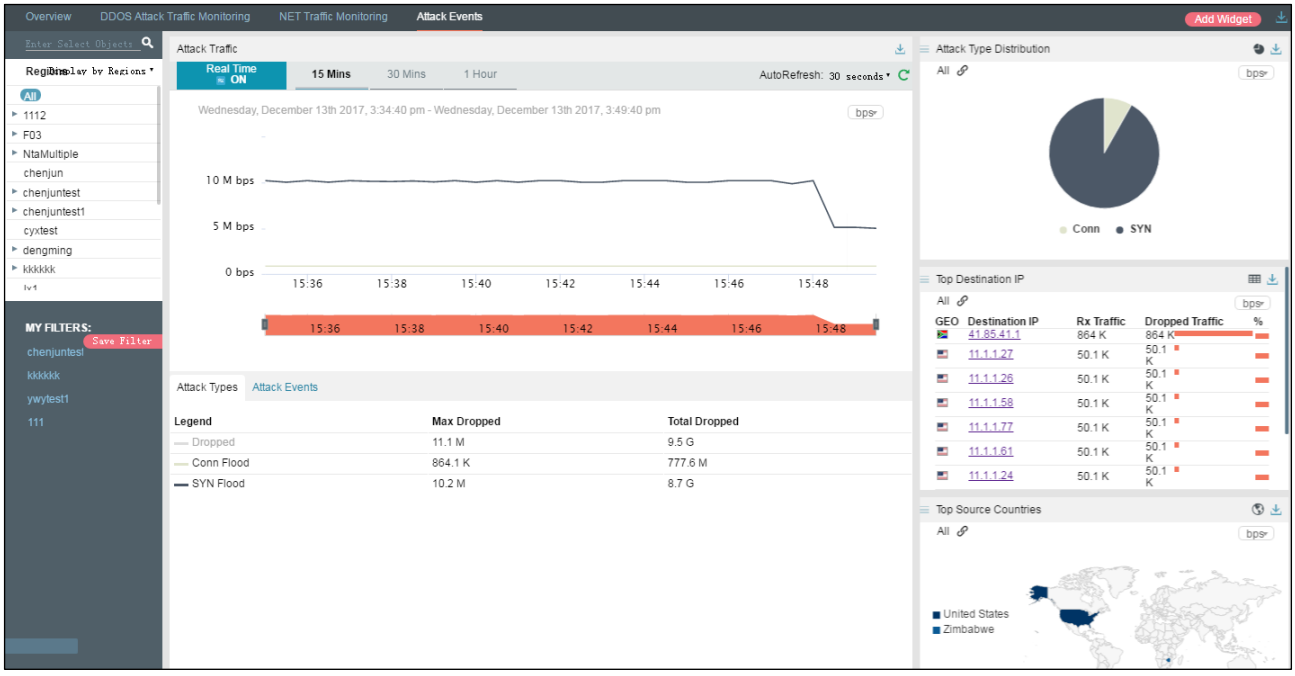
On the **Attack Types** tab page, attack type names and information of dropped traffic are displayed.

Clicking the bar or text in the **Legend** column hides or displays such type of attack traffic in the attack traffic trend graph. By default, all types of attack traffic are displayed. A dimmed color indicates that this type of attack traffic is not displayed. Otherwise, the attack traffic is displayed.

Table 4-10 Attack type parameters

Parameter	Description
Legend	Shows various colors, indicating different attack types, which correspond to those displayed in the attack traffic trend graph.
Max Dropped	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Total Dropped	Indicates the total traffic (in bits) dropped by ADS for the object in the statistical period.

Figure 4-121 Attack Events page – Attack Types panel



Step 2 Point to the attack traffic trend graph.

Detailed information about the time, real-time total dropped traffic, and real-time dropped traffic of a specific attack type is displayed, as shown in Figure 4-122.

Figure 4-122 Attack traffic information of a specific time

Step 3 Below the attack traffic trend graph, drag to view a finer-granularity traffic trend.

Figure 4-123 Finer-granularity traffic monitoring information

Step 4 On the page shown in Figure 4-121, click **Attack Events** below the attack traffic trend graph.

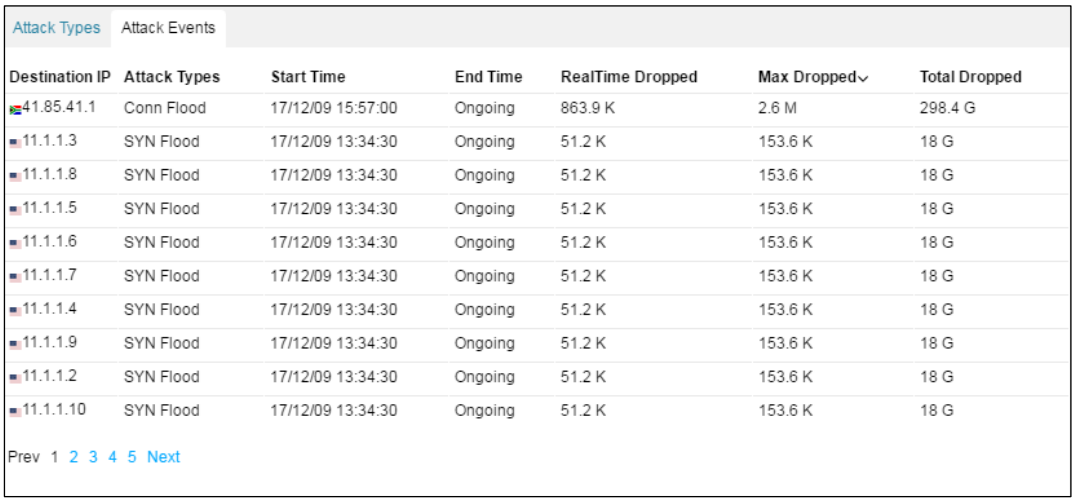
The ongoing attack events and their details are displayed, as shown in Figure 4-124.

On the attack event list, attack events are displayed in descending order of dropped traffic volume.

Table 4-11 Attack event parameters

Parameter	Description
Destination IP	Indicates the attacked IP address.
Attack Types	Indicates the type of the attack.
Start Time	Indicates the time when the attack begins.
End Time	Indicates the time when the attack ends.
RealTime Dropped	Indicates the traffic (in bps or pps) dropped by ADS for the object.
Max Dropped	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object.
Total Dropped	Indicates the total traffic (in bits) dropped by ADS for the object.

Figure 4-124 Attack traffic – attack events

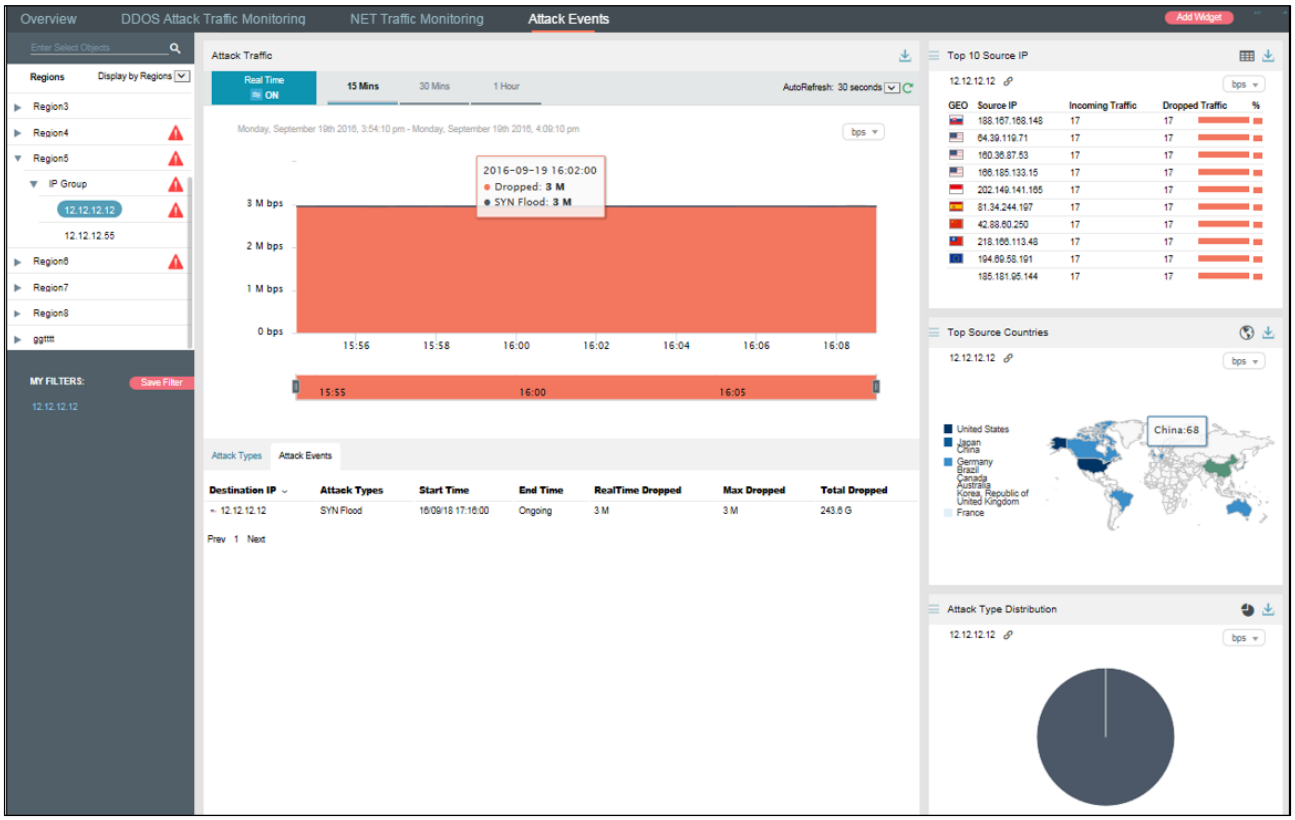


----End

4.4.2 Viewing Region-Specific Attack Events

On the page shown in Figure 4-121, clicking a region in the left pane displays attack traffic information of the region and of all IP groups and IP addresses in this region. You can further view historical and real-time attack traffic trends and panels of a selected region, IP group under a region, or IP address. For example, if you choose **Region5 > IP Group > 12.12.12.12**, you can view attack events of IP address 12.12.12.12.

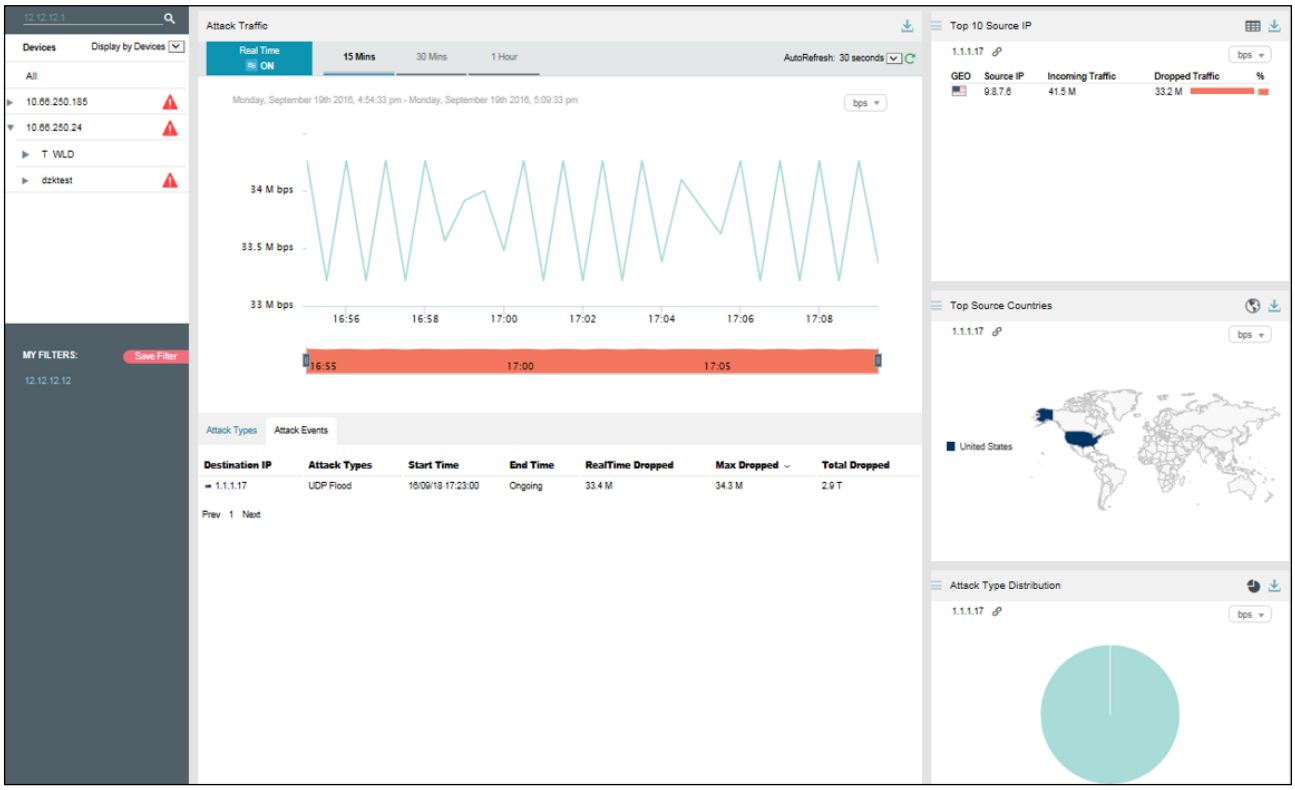
Figure 4-125 Region-specific attack events



4.4.3 Viewing Device-Specific Attack Events

On the page shown in Figure 4-121, you can select **Display by Devices** from the drop-down list in the left pane and then select a device to view real-time attack events of this ADS device, ADS-protected groups, and specific IP addresses under a protection group. You can view real-time and attack traffic trends and panels of a selected ADS, ADS-protected group, and IP address under a protection group. For example, you can choose **10.66.250.24 > dzktest** to view attack event information of group **dzktest** under device 10.66.250.45.

Figure 4-126 Device-specific attack events



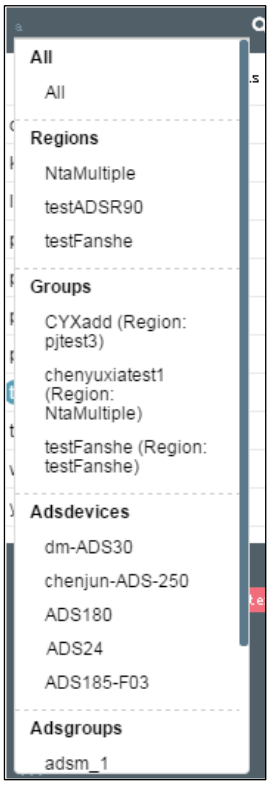
4.4.4 Viewing Object-Specific Attack Events

By default, the **Attack Events** tab page displays attack traffic trends of all ADS devices monitored by ADS M. You can view the real-time traffic trends of a specified region, regional IP group, ADS device, ADS-protected group, or IP address.

Step 1 On the page shown in Figure 4-121, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-127.

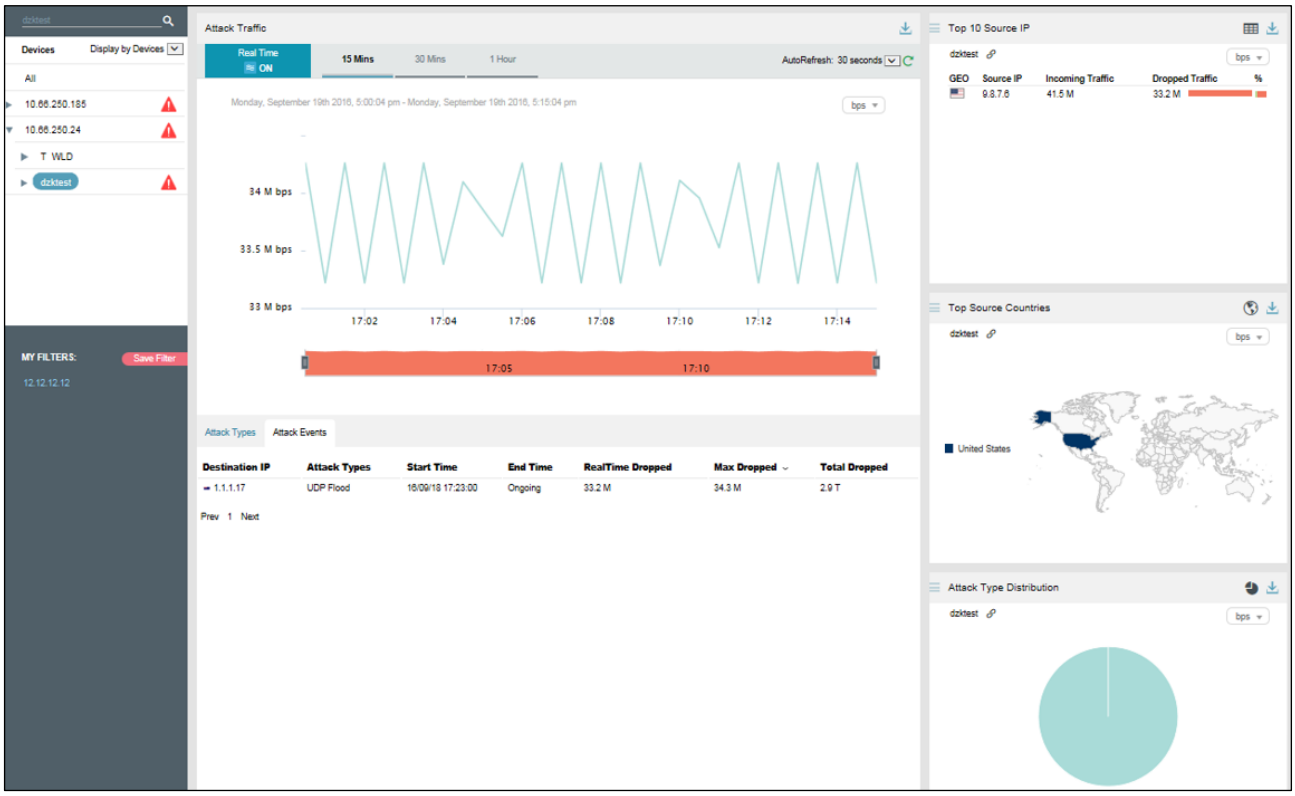
Figure 4-127 Searching for attack event objects



Step 2 Select an object to be queried, such as **dzktest**, and then press **Enter**.

Traffic information of the selected object is displayed, as shown in Figure 4-128.

Figure 4-128 Object-specific attack event information



----End

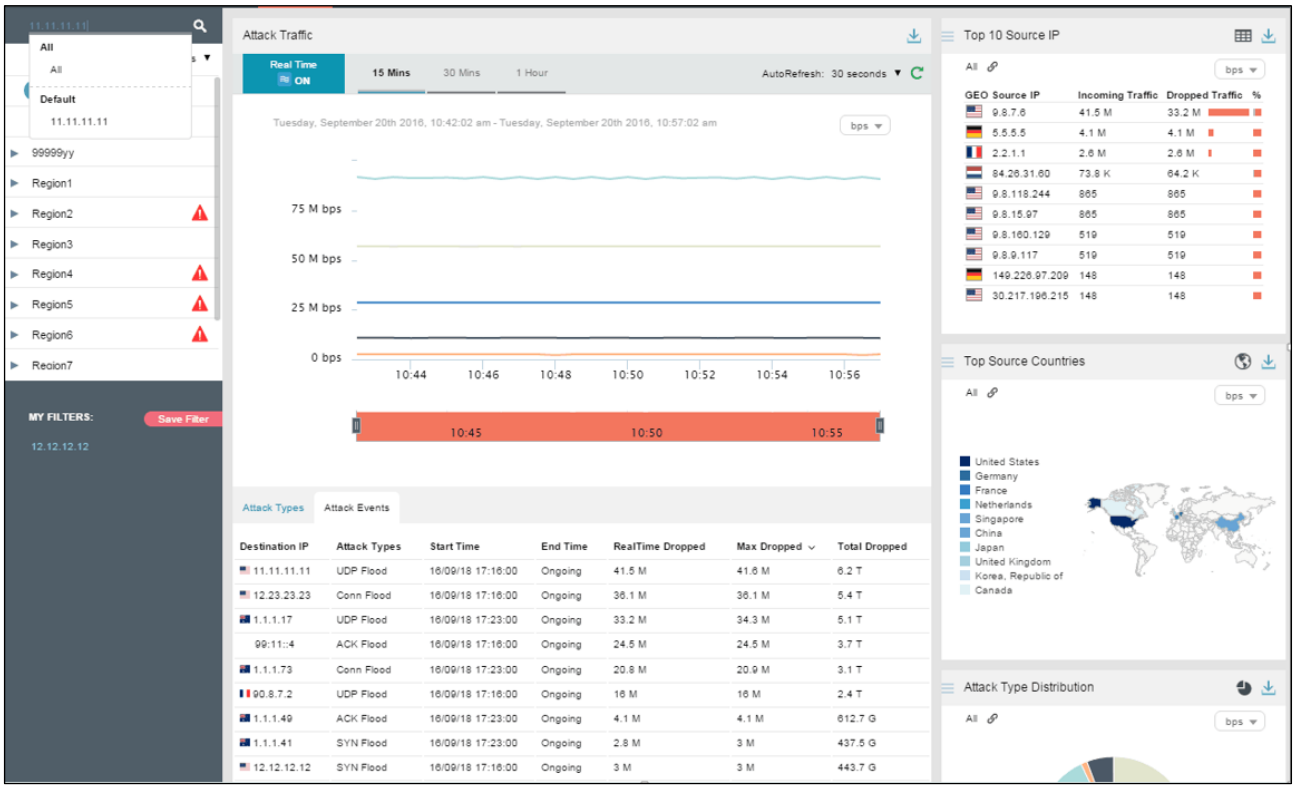
4.4.5 Viewing Attack Event Information of an IP Address in the Default Protection Group

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view attack traffic monitoring information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

Step 1 On the page shown in Figure 4-121, type an IP address (such as 11.11.11.11) and then press **Enter**.

The system displays all objects containing this IP address, as shown in Figure 4-129.

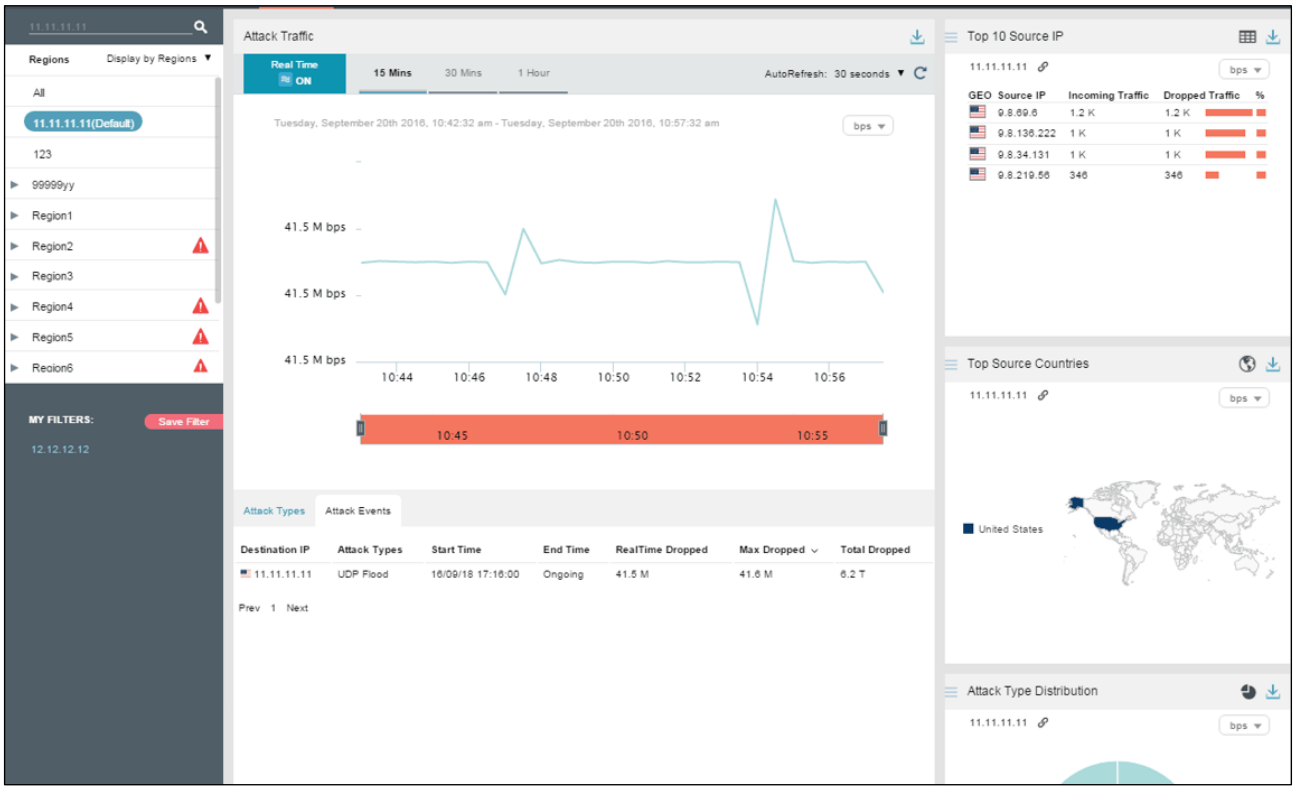
Figure 4-129 Searching for attack event objects



Step 2 Select the object to be queried and then press **Enter**.

Traffic monitoring information of this IP address is displayed, as shown in Figure 4-130.

Figure 4-130 Attack event information of an IP address in the default protection group



----End

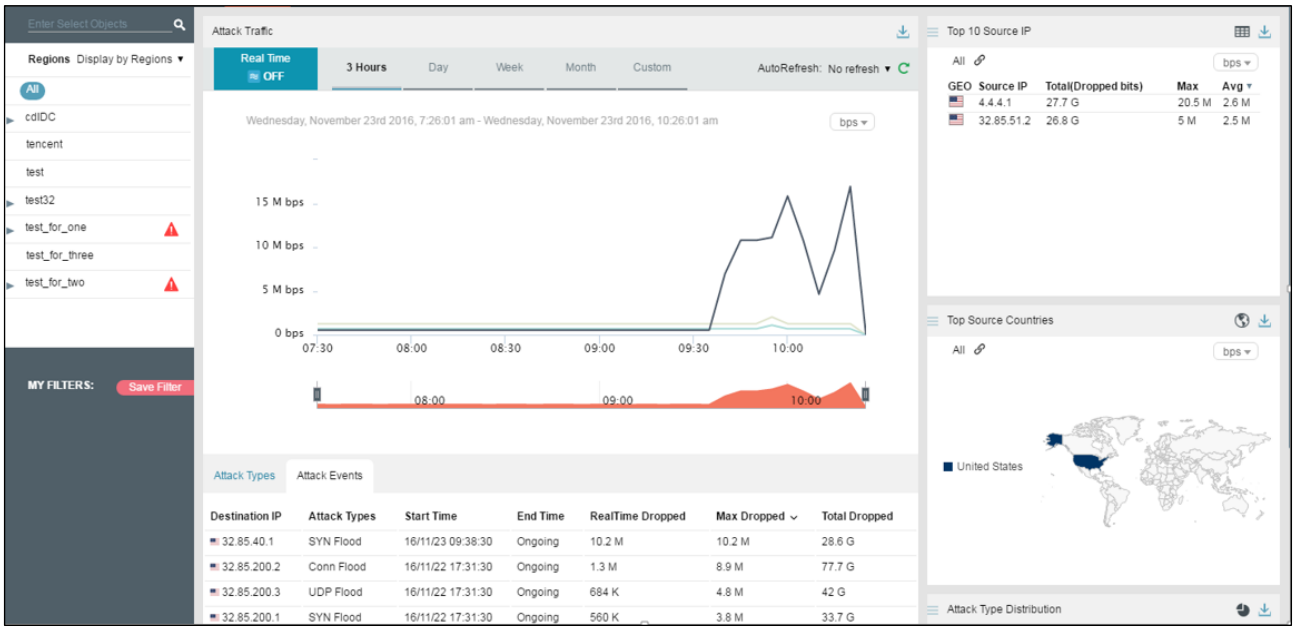
4.4.6 Viewing Attack Events in Historical Mode

On the page shown in Figure 4-121, clicking **ON** for **Real Time** in the **Attack Traffic** area disables the real-time mode and enables the historical mode. Clicking **OFF** for **Real Time** enables the real-time mode again.

In historical mode, attack traffic trend graphs and panels with the icon display historical data.

By default, the attack traffic trend graph displays attack traffic data in the last 3 hours. Clicking **Day**, **Week**, **Month**, or **Custom** displays attack traffic trend graphs in the last day, week, month, or a custom period.

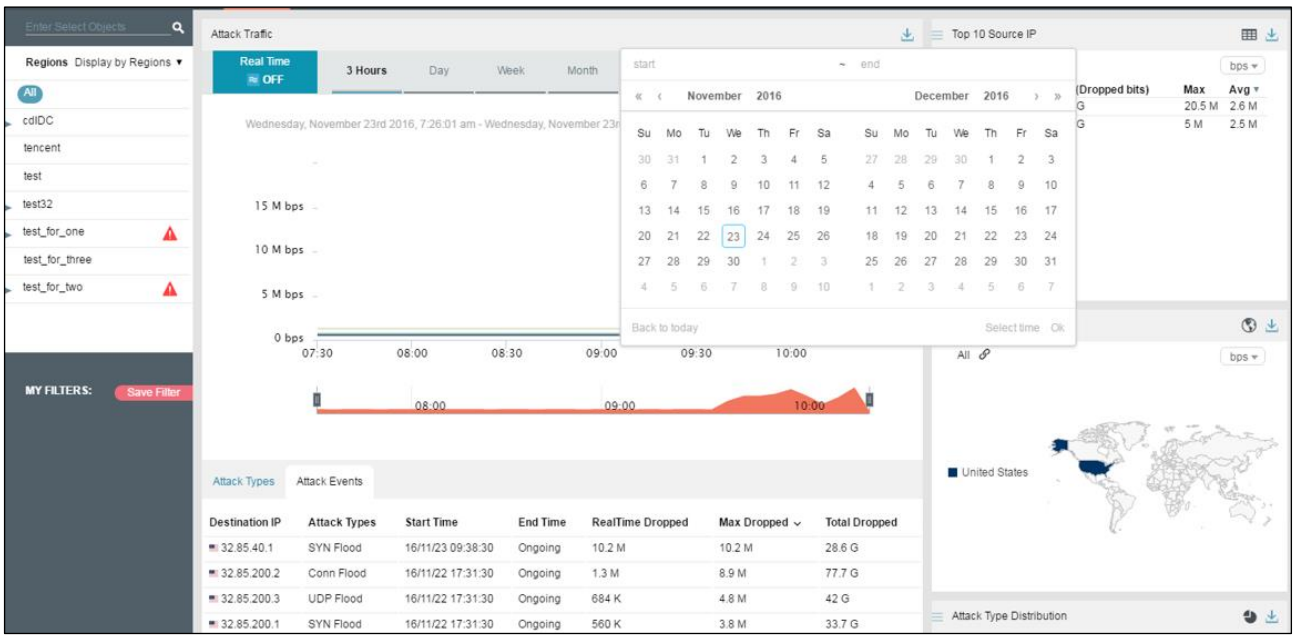
Figure 4-131 Historical attack traffic trend



On the page shown in Figure 4-131, click **Custom** above the attack traffic graph.

You can select the start time and end time of the attack traffic graph as required, as shown in Figure 4-132. The unit is the day.

Figure 4-132 Customization of the attack traffic trend graph



4.4.7 Switching the Traffic Unit

By default, traffic is expressed in bps in attack traffic trend graphs. On the page shown in Figure 4-121, you can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic** area to display traffic data in pps.

4.4.8 Refreshing the Attack Traffic Trend Graph

By default, the attack traffic trend graph automatically refreshes every 30 seconds in real time mode. On the page shown in Figure 4-121, you can select **No refresh** from the **AutoRefresh** drop-down list in the upper-right corner of the **Attack Traffic** area. In this case, the attack traffic trend graph does not refresh unless you click .

By default, the attack traffic trend graph does not automatically refresh in historical mode. On the page shown in Figure 4-121, you can select **5 minutes** from the **AutoRefresh** drop-down list in the upper-right corner of the **Attack Traffic** area. In this case, the attack traffic trend graph will automatically refresh every 5 minutes.

4.4.9 Downloading an Attack Traffic Trend Report

On the page shown in Figure 4-121, you can click in the upper-right corner to export the current data of the attack traffic trend graph as a report. For details, see section 4.1.4 Downloading a Report.

4.4.10 Managing Filters

Filters are provided for users to define objects of their concern, so that they can find detected attack events more conveniently. After being created, filters are displayed in the filter list. You can click a filter to view attack event information of the object specified by the filter.

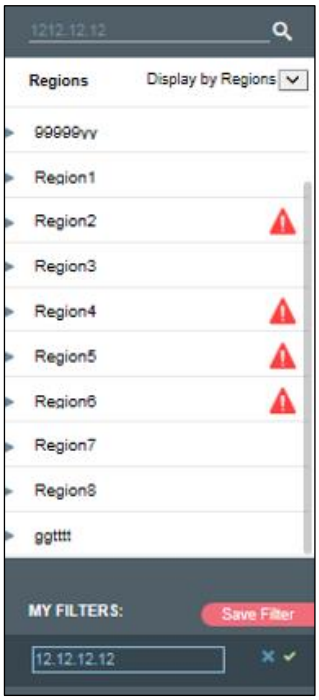
Any queried objects, such as a region, region IP group, ADS device, ADS-protected group, or IP address can be configured as a filter. But **All** and **Default IP (Default)** cannot be configured as a filter. You can configure multiple filters.

4.4.10.1 Configuring a Filter

To configure a filter, follow these steps:

Step 1 On the page shown in Figure 4-121, select an object from the left pane, such as 12.12.12.12, and then click **Save Filter**.

Figure 4-133 Creating a filter



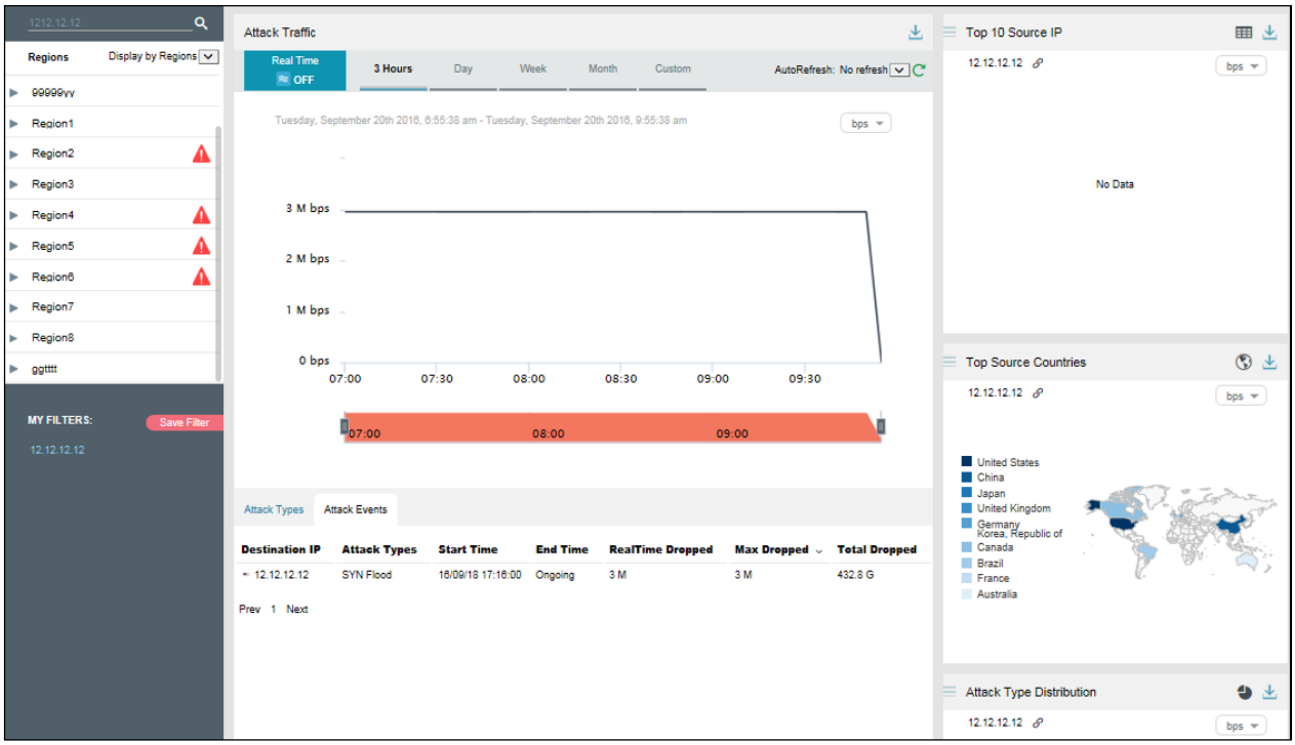
Step 2 Type the filter name.

By default, the object name is displayed as the filter name. You can use the default name or type a new one.

Step 3 Click and then click **Confirm** in the dialog box that appears.

Step 4 Click **12.12.12.12** in the filter list to view its attack traffic information.

Figure 4-134 Viewing a filter



----End

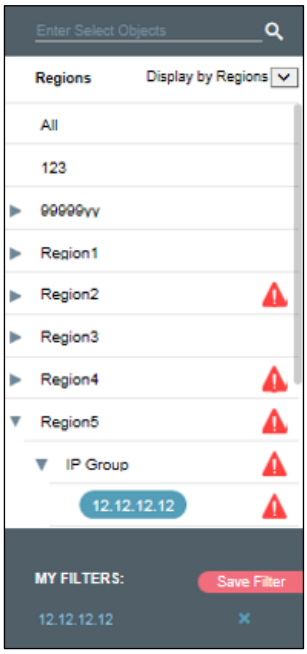
4.4.10.2 Deleting a Filter

To delete a filter, follow these steps:

Step 1 On the page shown in Figure 4-134, point to a filter name

The icon appears, as shown in Figure 4-135.

Figure 4-135 Deleting a filter



Step 2 Click ✕ and then **Confirm** in the dialog box that appears.

----End

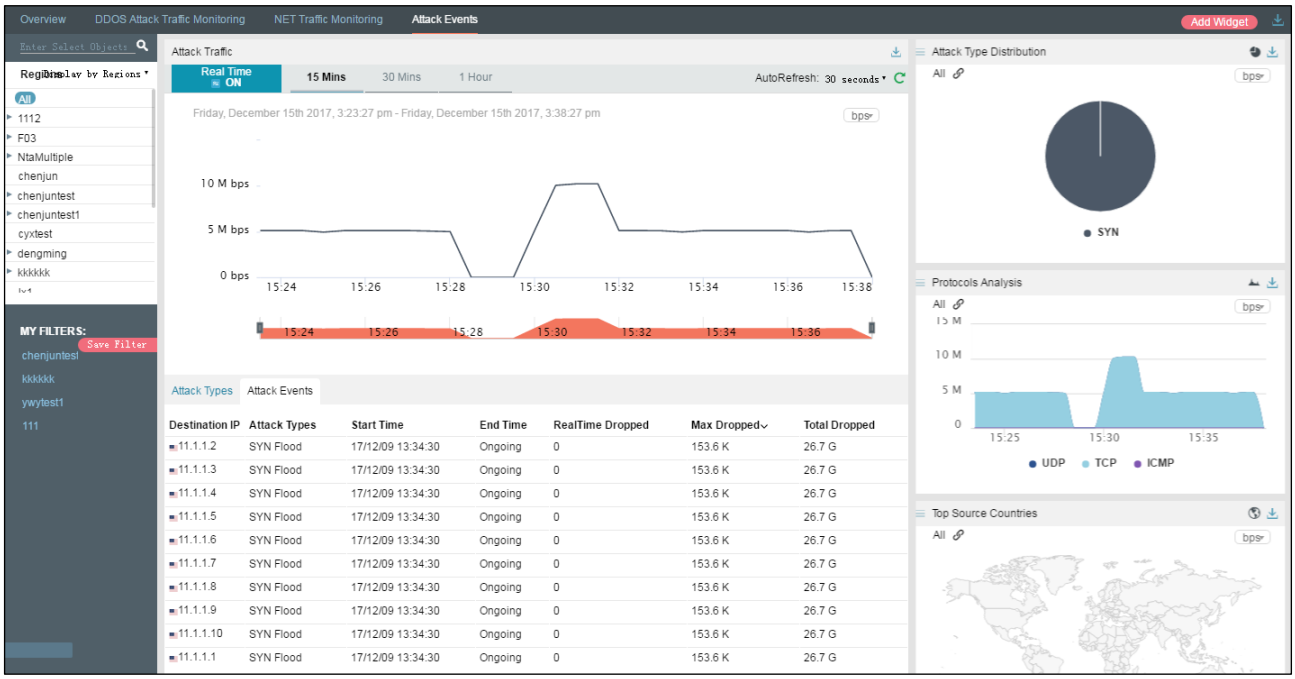
4.4.11 Managing Panels

By default, **Top 10 Source IP**, **Top Source Countries**, and **Attack Type Distribution** are displayed under **Traffic monitoring > Attack Events**, as shown in Figure 4-136.

A panel with the icon 🔗 indicates that when the selected object and statistical period change, the object and statistical period of this panel will change accordingly. A panel without the icon 🔗 indicates the opposite.

You can add panels as required. For how to add, edit, and delete panels, see section 4.1 Overview.

Figure 4-136 Default panels on the Attack Events page



5 Reports

You can view the following types of reports on ADS M:

- Built-in reports: include network traffic reports and DDoS attack reports.
- Custom reports: refer to the reports customized by users.

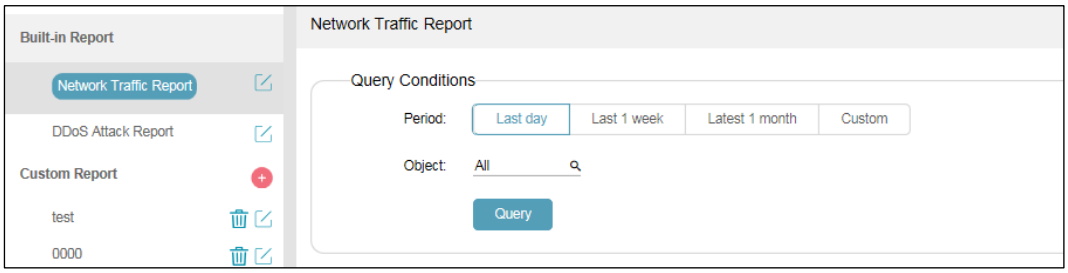
In addition to viewing reports, you can also configure ADS M to send reports via email and customize the report logo.

5.1 Built-in Reports

You can query built-in reports and edit the logo image displayed in built-in reports.

Choose **Reports > Built-in Report > Network Traffic Report**.

Figure 5-1 Network Traffic Report page



Querying a Report

After selecting a report type, you can query such type of reports in a specified period, which can be set to **Last day**, **Last 1 week**, **Last 1 month**, and **Custom**.

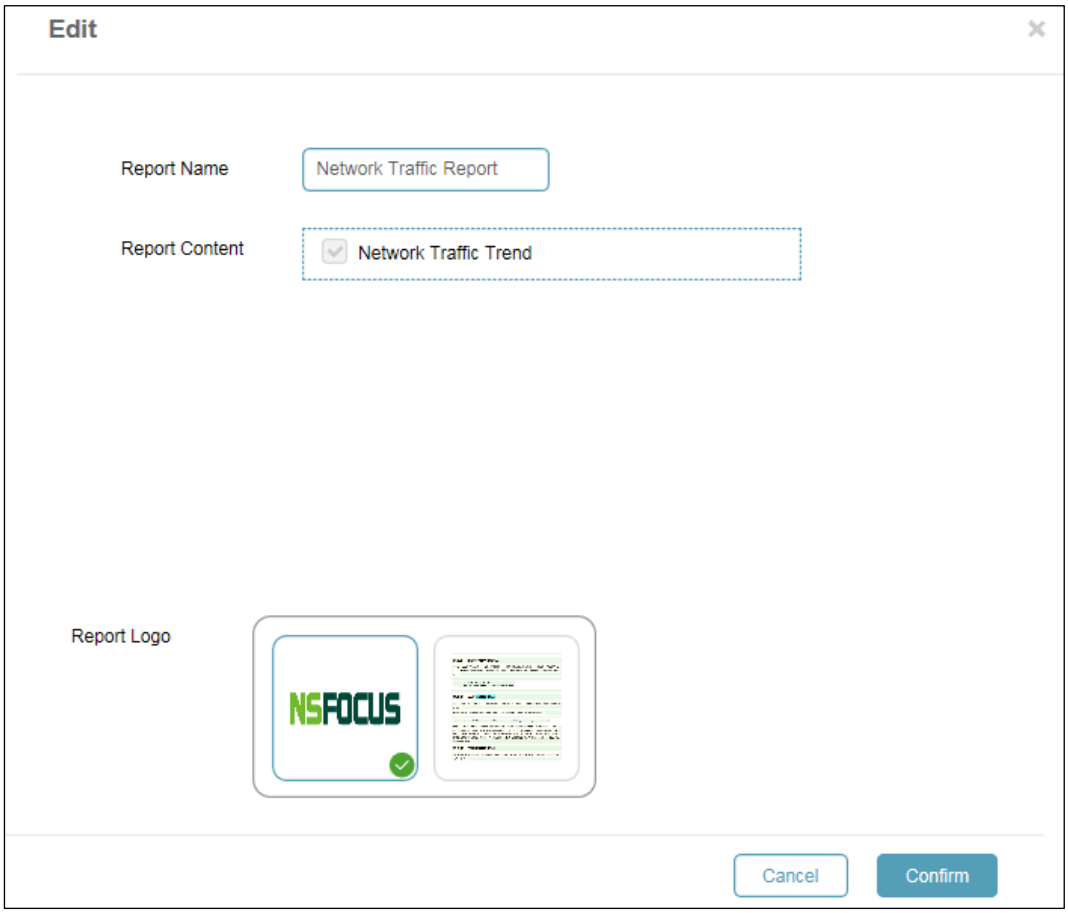
After setting **Period** and **Object**, click **Query**.

Reports meeting query conditions are displayed.

Editing a Report

You can edit the logo displayed in built-in reports. Clicking next to **Network Traffic Report** displays the dialog box shown in Figure 5-2.

Figure 5-2 Editing a report



Pointing to the logo image displays the icon . You click to view the big logo image.

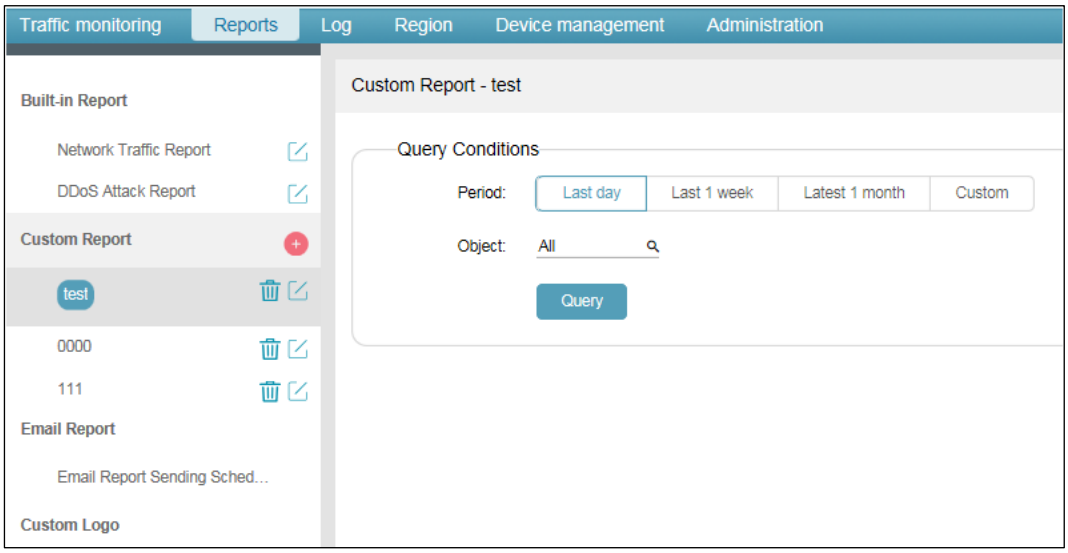
You can select a logo image and then click **Confirm** to save the setting.

5.2 Custom Reports

You can create, query, edit, and delete custom reports.

Choose **Reports > Custom Report**.

Figure 5-3 Custom Report page

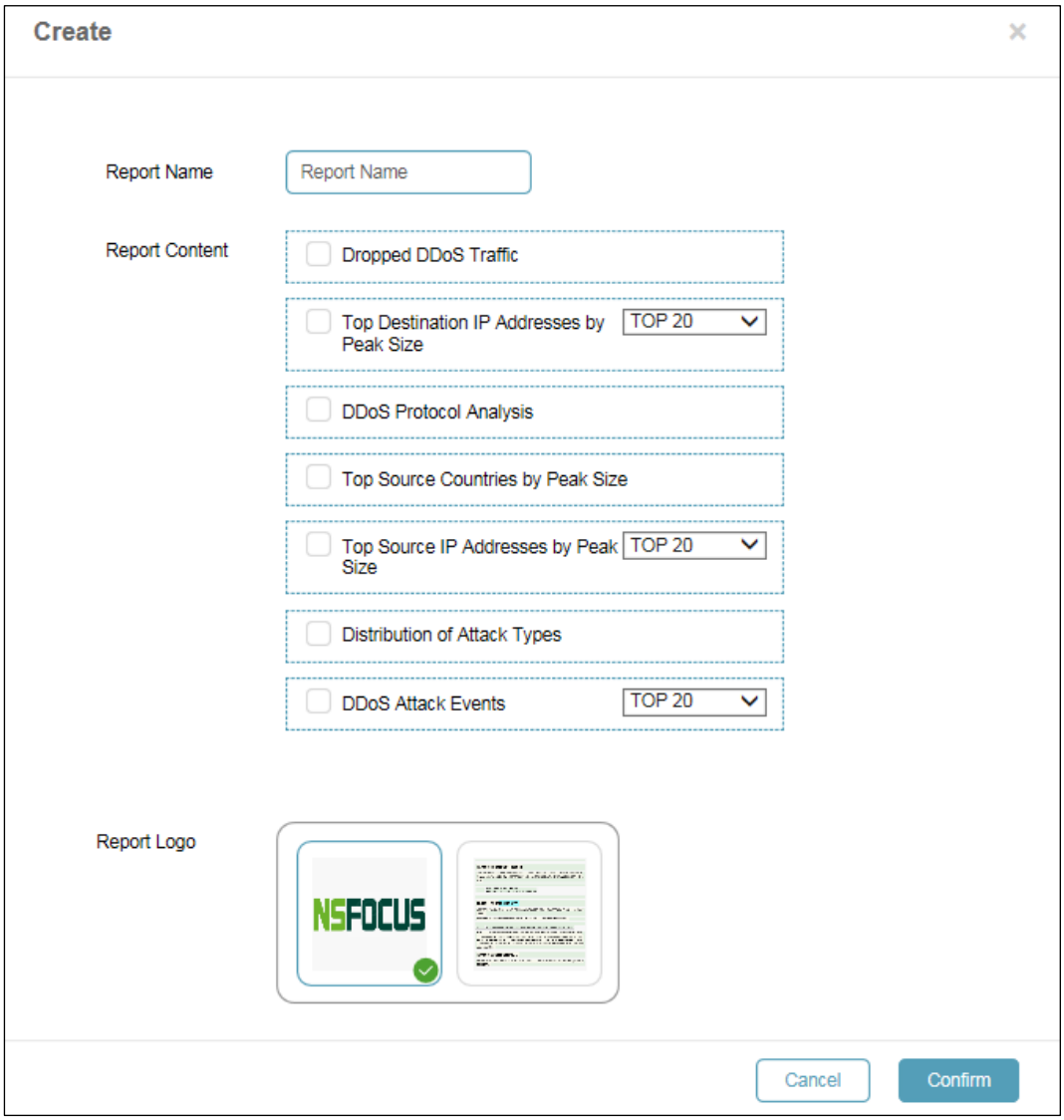


Creating a Custom Report

To create a custom report, follow these steps:

Step 1 Click next to **Custom Report**.

Figure 5-4 Creating a custom report



Step 2 In the dialog box, set the parameters.

- Set the report name.
- Select report contents.
- Select a report logo.

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

----End

Querying a Custom Report

After selecting a custom report type, you can query such type of reports in a specified period, which can be set to **Last day**, **Last 1 week**, **Last 1 month**, and **Custom**.

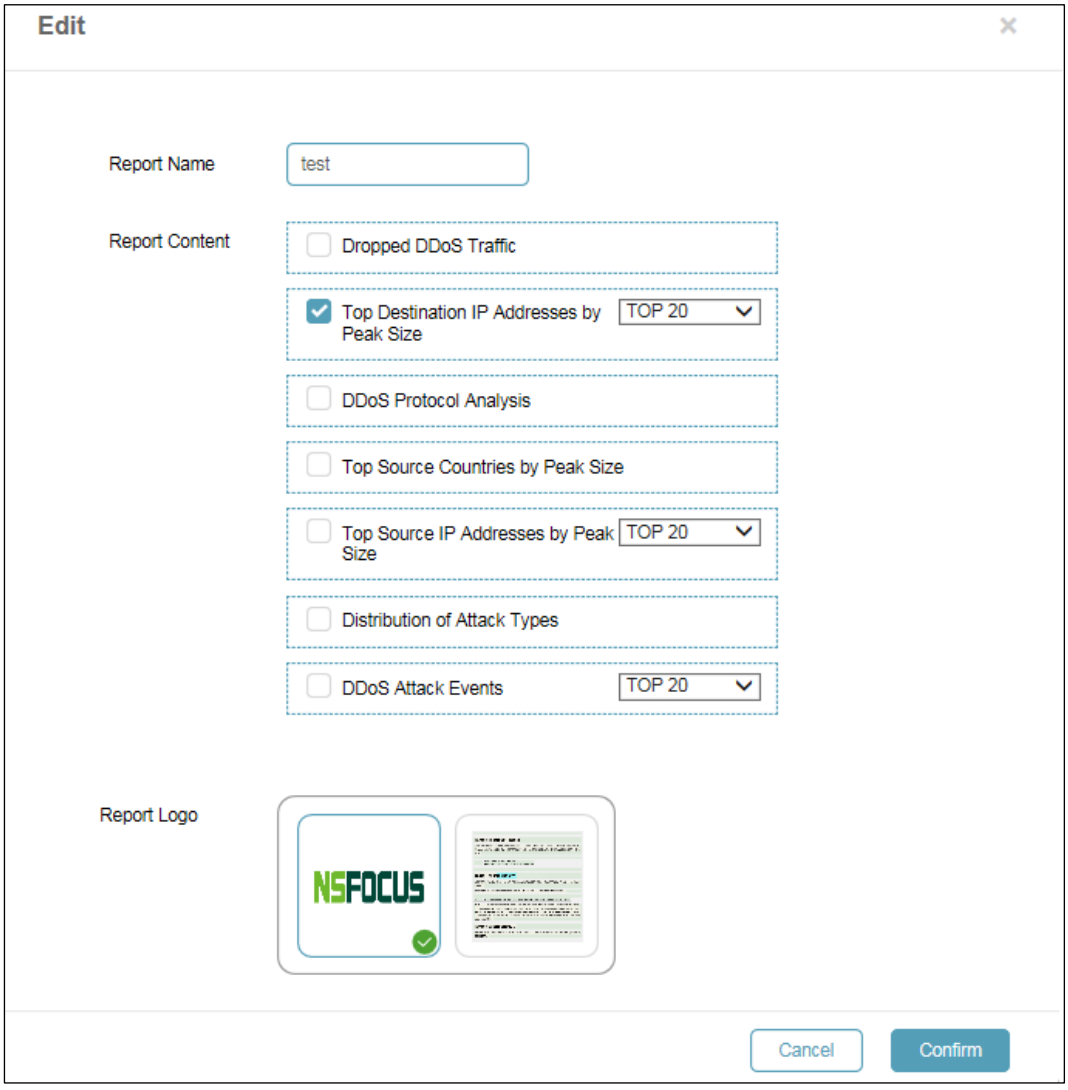
After setting **Period** and **Object**, click **Query**.

Reports meeting query conditions are displayed.

Editing a Custom Report

You can edit the name, module, and logo of custom reports. Clicking next to a custom report displays the dialog box shown in Figure 5-5.

Figure 5-5 Editing a custom report



After editing the report name, report contents, and report log, click **Confirm** to save the settings.

Deleting a Custom Report

You can click next to a custom report and then click **Confirm** in the confirmation dialog box to delete this custom report.

5.3 Email Report

Note	Before configuring an email report, you must configure the SMTP server under **Administration > Third-Party Interface > SMTP Server Configuration**. For details, see section 3.3.1 SNMP Configuration.

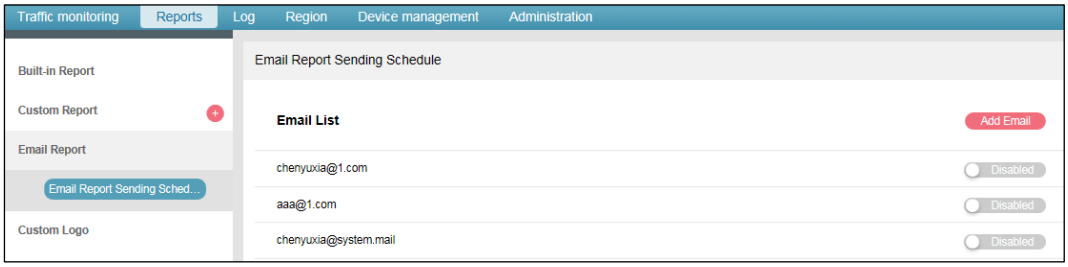
Configuring an email report sending schedule includes configuration of **Email Addresses**, **Report**, **Report Language**, and **Report Type**.

You can create, edit, enable/disable, and delete email report sending schedules.

Creating an Email Report Sending Schedule

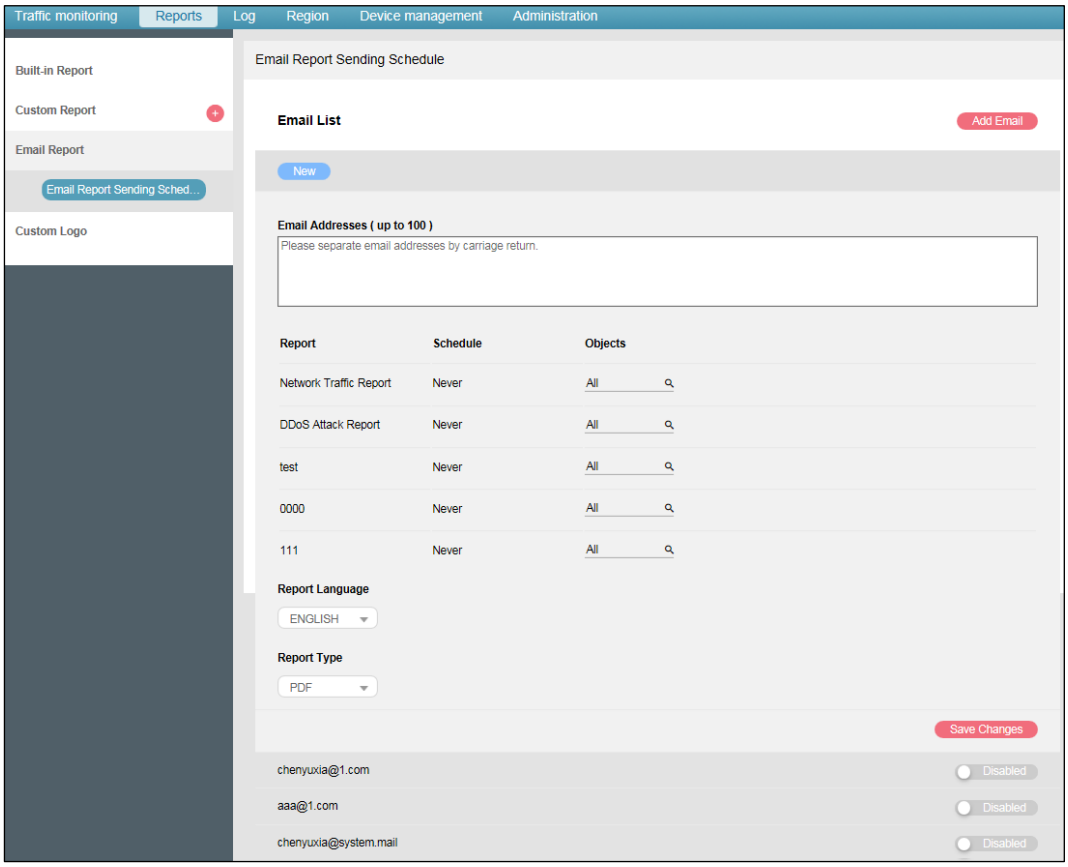
Step 1 Choose **Reports > Email Report > Email Report Sending Schedule**.

Figure 5-6 Email Report Sending Schedule page



Step 2 Click **Add Email**.

Figure 5-7 Creating an email report sending schedule



Step 3 Configure parameters.

Table 5-1 Parameters for configuring an email report sending schedule

Parameter	Description
Email Addresses	Specifies the email addresses to which reports will be sent.
Report	You can set **Schedule** and **Objects** to specify how reports will be sent. • **Schedule**: specifies the interval at which reports are sent. Options include **Daily**, **Weekly**, **Monthly**, and **Never**. • **Objects**: For traffic monitoring reports and attack event reports, data of all objects is collected by default. If you want reports to provide data regarding only a specific object, you must specify this object by doing as follows: Type a string under **Objects** and then select the desired one from the objects containing the string.
Report Language	Specifies the language of reports to be sent, which can be English, Simplified Chinese, and Japanese.
Report Type	Specifies the format of reports to be sent, which can be **PDF**, **HTML**, and **WORD**.

Step 4 Click **Save Changes** to save the settings.

The newly created email sending schedule will be displayed in the email list and is enabled by default.

----End

Editing an Email Report Sending Schedule

In Figure 5-6, clicking an email address in the email list expands the email report sending schedule. You can edit parameters as required (for parameter description, see Table 5-1) and then click **Save Changes** to save the settings.

Enabling/Disabling an Email Report Sending Schedule

In Figure 5-6, you can click Disabled / Enabled in the row of an email address to enable/disable this email report sending schedule.**Deleting an Email Report Sending Schedule**In Figure 5-6, clicking an email address in the email list expands the email report sending schedule. You can click **Delete Email** to delete this email report sending schedule.

5.4 Custom Logo

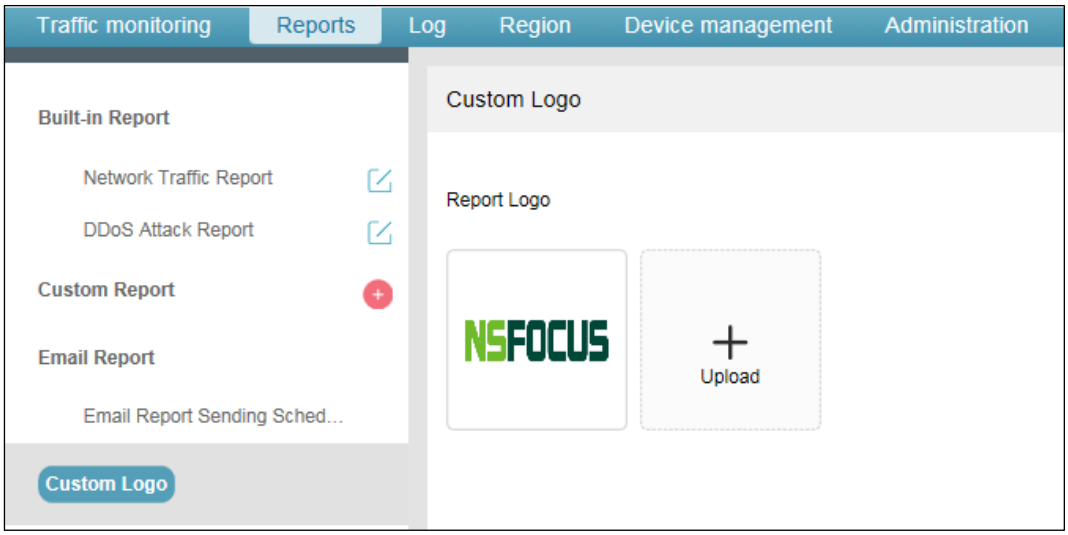
You can upload, view, and delete custom logos.

Uploading a Custom Logo

You can upload a logo image for use in the generated reports.

Step 1 Choose **Reports > Custom Logo**.

Figure 5-8 Custom Logo page



Step 2 Click + and then select the logo image to be uploaded.

----End

Viewing a Custom Logo

Pointing to the logo image displays the icon . You can click to view the big logo image.

Deleting a Custom Logo

You can delete uploaded logo images but not the built-in one.

Pointing to a custom logo displays . You can click and then **Confirm** in the confirmation dialog box to delete this custom logo.

6 Logs

Device logs include attack summary logs, login logs, operation logs, link status logs, performance logs, diversion logs, running alert log, HA logs, traffic alert logs, and cloud authentication logs. You can set query conditions to view logs online and export logs.

- Querying logs

  After setting query conditions, click **Search** to generate desired logs.
- Exporting logs

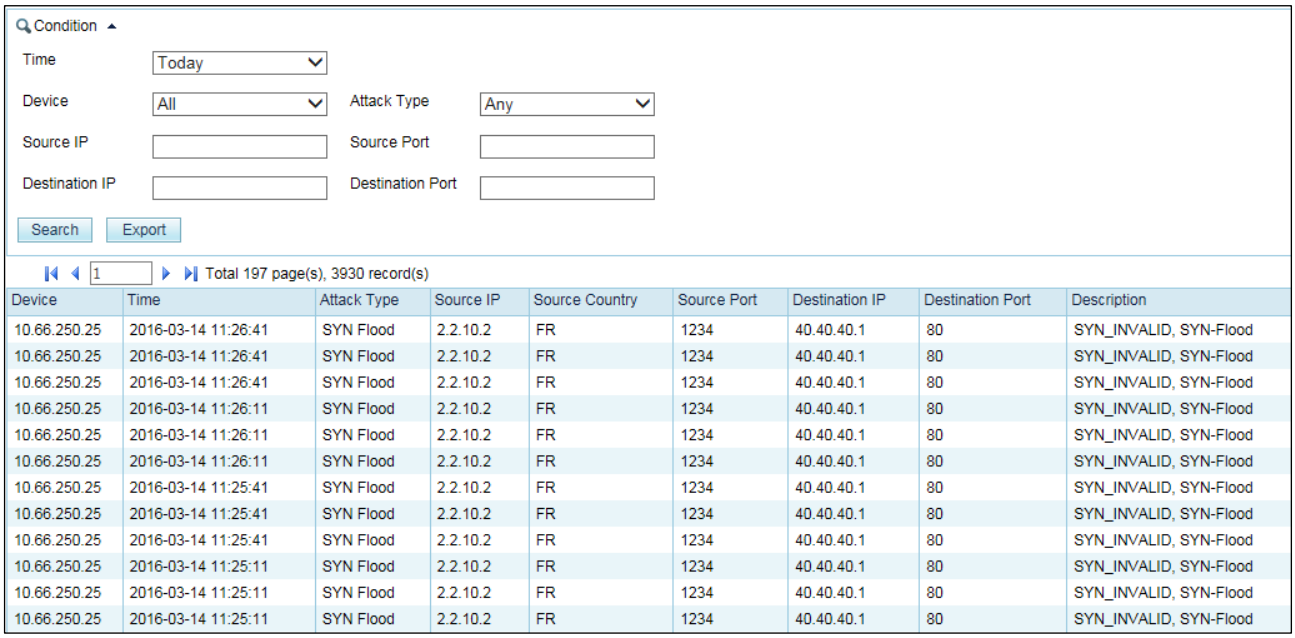
  After setting log export conditions, click **Export** to save logs to the local host.

6.1 Attack Summary Log

Choose **Log** > **Attack Summary Log**. The **Attack Summary Log** page appears, as shown in Figure 6-1.

You can set specific conditions to query or export logs of attacks detected and defended against by all devices in the device list.

Figure 6-1 Attack summary logs



Device	Time	Attack Type	Source IP	Source Country	Source Port	Destination IP	Destination Port	Description
10.66.250.25	2016-03-14 11:26:41	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:26:41	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:26:41	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:26:11	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:26:11	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:26:11	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:25:41	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:25:41	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:25:41	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:25:11	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:25:11	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood
10.66.250.25	2016-03-14 11:25:11	SYN Flood	2.2.10.2	FR	1234	40.40.40.1	80	SYN_INVALID, SYN-Flood

Table 6-1 describes parameters of attack summary logs.

Table 6-1 Parameters of attack summary logs

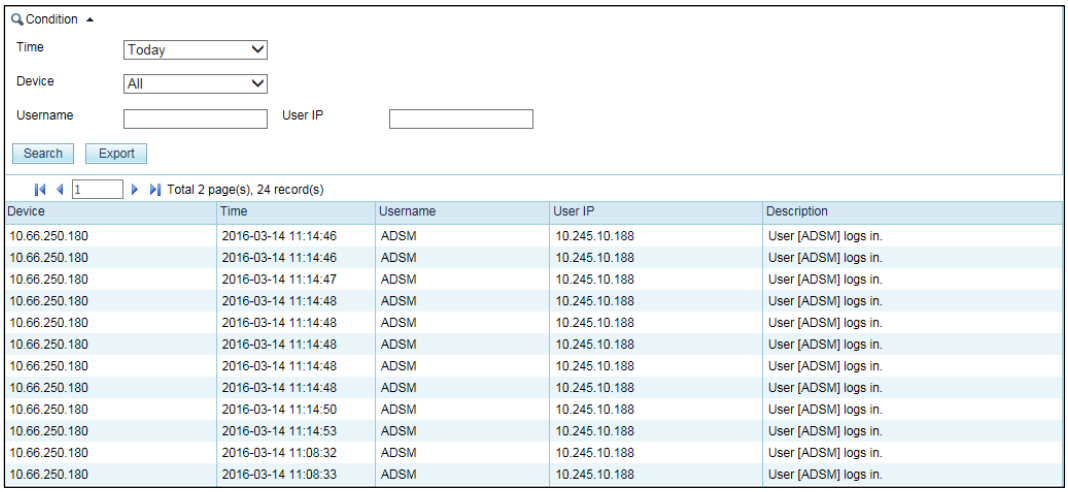
Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Specifies the device whose logs are queried. **All** indicates that logs on all devices are queried.
Attack Type	Specifies the attack type of logs to be queried. If you cannot determine what the attack type is, select **Any**.
Source IP	Specifies the IP address of the attack source.
Source Port	Specifies the port where attacks occur.
Destination IP	Specifies the IP address that suffers attacks.
Destination Port	Specifies the port that suffers attacks.

6.2 Login Log

Choose **Log** > **Login Log**. The **Login Log** page appears, as shown in Figure 6-2.

You can set specific conditions to query or export login logs of all devices in the device list.

Figure 6-2 Login logs



Device	Time	Username	User IP	Description
10.66.250.180	2016-03-14 11:14:46	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:46	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:47	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:50	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:14:53	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:08:32	ADSM	10.245.10.188	User [ADSM] logs in.
10.66.250.180	2016-03-14 11:08:33	ADSM	10.245.10.188	User [ADSM] logs in.

Table 6-2 describes parameters of login logs.

Table 6-2 Parameters of login logs

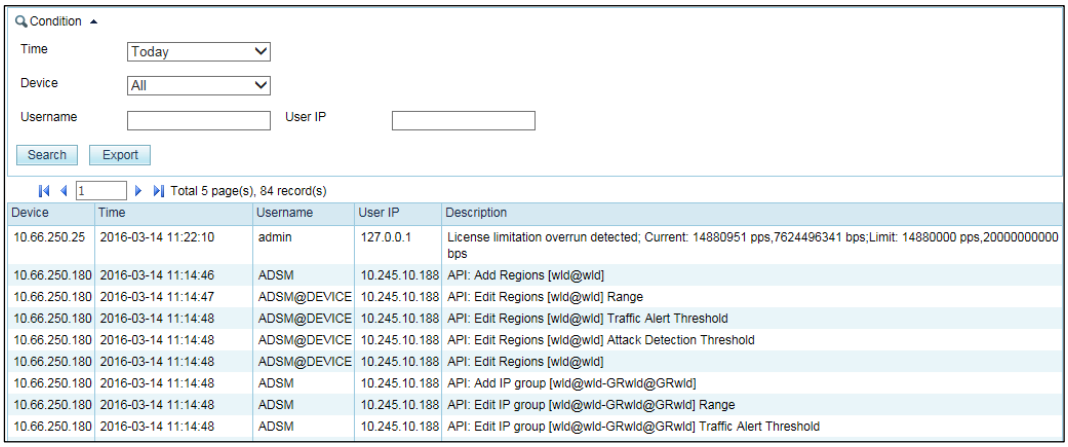
Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Specifies the device whose logs are queried. **All** indicates that logs on all devices are queried.
Username	Specifies the login user name. The full user name is required because fuzzy query is not allowed here.
User IP	Specifies the IP address of the user device. The full IP address is required because fuzzy query is not allowed here.

6.3 Operation Log

Choose **Log** > **Operation Log**. The **Operation Log** page appears, as shown in Figure 6-3.

You can set specific conditions to query or export operation logs of all devices in the device list.

Figure 6-3 Operation logs



Device	Time	Username	User IP	Description
10.66.250.25	2016-03-14 11:22:10	admin	127.0.0.1	License limitation overrun detected; Current: 14880951 pps,7624496341 bps;Limit: 14880000 pps,20000000000 bps
10.66.250.180	2016-03-14 11:14:46	ADSM	10.245.10.188	API: Add Regions [wld@wld]
10.66.250.180	2016-03-14 11:14:47	ADSM@DEVICE	10.245.10.188	API: Edit Regions [wld@wld] Range
10.66.250.180	2016-03-14 11:14:48	ADSM@DEVICE	10.245.10.188	API: Edit Regions [wld@wld] Traffic Alert Threshold
10.66.250.180	2016-03-14 11:14:48	ADSM@DEVICE	10.245.10.188	API: Edit Regions [wld@wld] Attack Detection Threshold
10.66.250.180	2016-03-14 11:14:48	ADSM@DEVICE	10.245.10.188	API: Edit Regions [wld@wld]
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	API: Add IP group [wld@wld-GRwld@GRwld]
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	API: Edit IP group [wld@wld-GRwld@GRwld] Range
10.66.250.180	2016-03-14 11:14:48	ADSM	10.245.10.188	API: Edit IP group [wld@wld-GRwld@GRwld] Traffic Alert Threshold

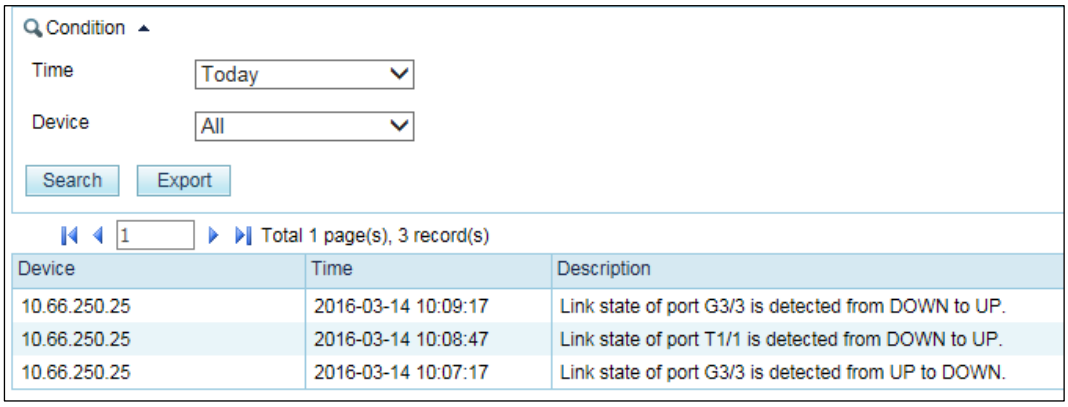
6.4 Link Status Log

Link status logs refer to connection and disconnection state logs at the interface of ADS M, that is, the records of states from Up to Down or from Down to Up.

Choose **Log** > **Link Status Log**. The **Link Status Log** page appears, as shown in Figure 6-4.

You can set specific conditions to query or export all link status logs of all devices in the device list.

Figure 6-4 Link status logs



Device	Time	Description
10.66.250.25	2016-03-14 10:09:17	Link state of port G3/3 is detected from DOWN to UP.
10.66.250.25	2016-03-14 10:08:47	Link state of port T1/1 is detected from DOWN to UP.
10.66.250.25	2016-03-14 10:07:17	Link state of port G3/3 is detected from UP to DOWN.

6.5 Diversion Log

Traffic diversion is logged only after you configure ADS diversion parameters.

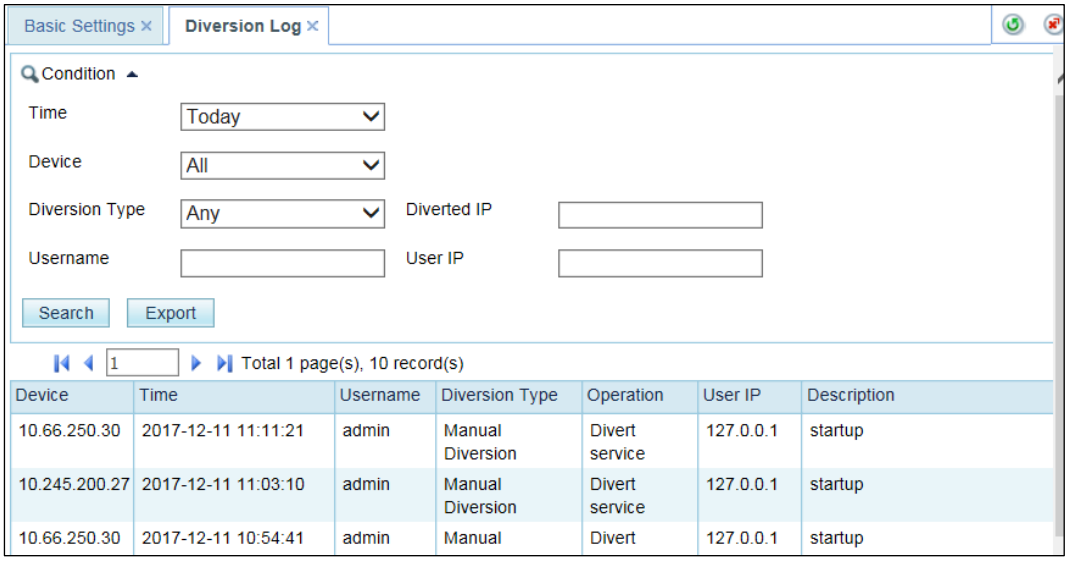
Choose **Log** > **Diversion Log**. The **Diversion Log** page appears, as shown in Figure 6-5.

You can set specific conditions to query or export all diversion information of all devices in the device list. The log information includes:

- Automatic diversion information
- Manual diversion information

- Diversion information generated during hierarchical coordination of ADS devices

Figure 6-5 Diversion logs



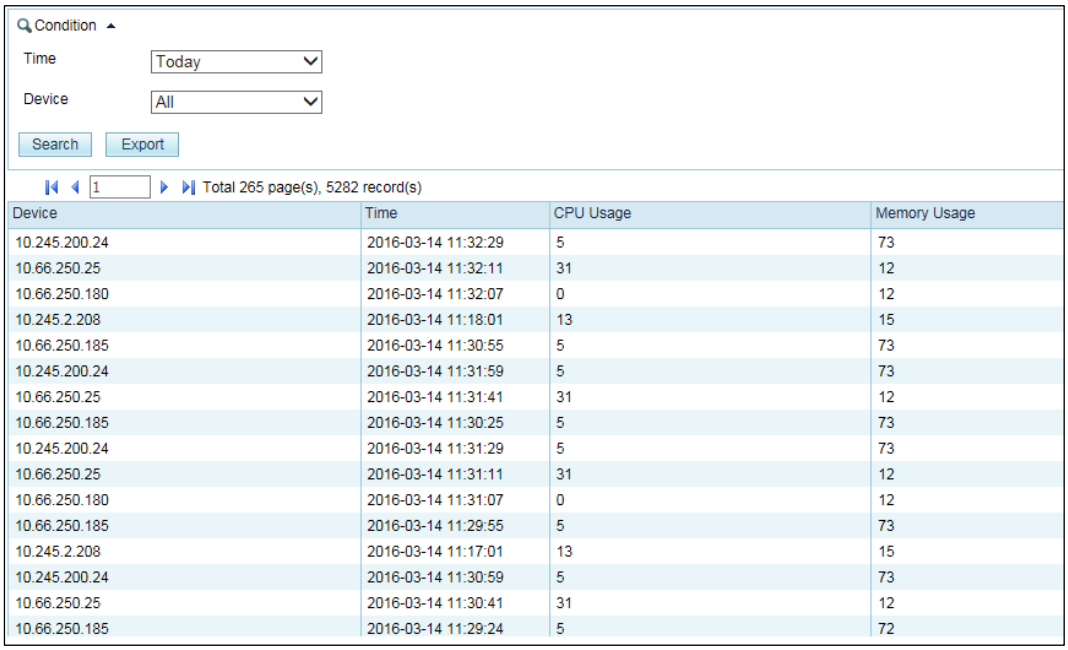
6.6 Performance Log

Choose **Log** > **Performance Log**. The **Performance Log** page appears, as shown in Figure 6-6.

You can set specific conditions to query or export all performance logs of all devices in the device list. The log information includes:

- Device name
- Generation time
- CPU usage
- Memory usage

Figure 6-6 Performance logs



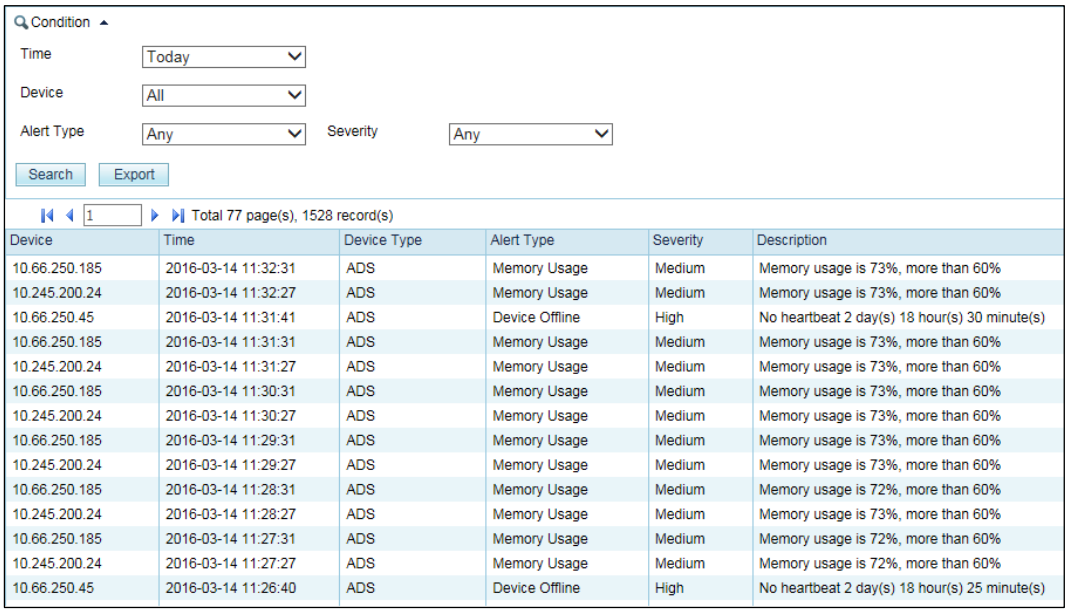
Device	Time	CPU Usage	Memory Usage
10.245.200.24	2016-03-14 11:32:29	5	73
10.66.250.25	2016-03-14 11:32:11	31	12
10.66.250.180	2016-03-14 11:32:07	0	12
10.245.2.208	2016-03-14 11:18:01	13	15
10.66.250.185	2016-03-14 11:30:55	5	73
10.245.200.24	2016-03-14 11:31:59	5	73
10.66.250.25	2016-03-14 11:31:41	31	12
10.66.250.185	2016-03-14 11:30:25	5	73
10.245.200.24	2016-03-14 11:31:29	5	73
10.66.250.25	2016-03-14 11:31:11	31	12
10.66.250.180	2016-03-14 11:31:07	0	12
10.66.250.185	2016-03-14 11:29:55	5	73
10.245.2.208	2016-03-14 11:17:01	13	15
10.245.200.24	2016-03-14 11:30:59	5	73
10.66.250.25	2016-03-14 11:30:41	31	12
10.66.250.185	2016-03-14 11:29:24	5	72

6.7 Performance Alert Log

Choose **Log > Performance Alert Log**. The **Performance Alert Log** page appears, as shown in Figure 6-7. You can set specific conditions to query or export performance alert logs reported by ADS M and managed ADS and NTA devices. The alerts include CPU usage alerts, memory usage alerts, ADS/NTA device offline alerts, and ADS M's HA alerts. The log information includes:

- Alert ID
- Generation time
- Device type
- Alert type
- Severity
- Description

Figure 6-7 Performance alert logs



Device	Time	Device Type	Alert Type	Severity	Description
10.66.250.185	2016-03-14 11:32:31	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.245.200.24	2016-03-14 11:32:27	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.66.250.45	2016-03-14 11:31:41	ADS	Device Offline	High	No heartbeat 2 day(s) 18 hour(s) 30 minute(s)
10.66.250.185	2016-03-14 11:31:31	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.245.200.24	2016-03-14 11:31:27	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.66.250.185	2016-03-14 11:30:31	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.245.200.24	2016-03-14 11:30:27	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.66.250.185	2016-03-14 11:29:31	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.245.200.24	2016-03-14 11:29:27	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.66.250.185	2016-03-14 11:28:31	ADS	Memory Usage	Medium	Memory usage is 72%, more than 60%
10.245.200.24	2016-03-14 11:28:27	ADS	Memory Usage	Medium	Memory usage is 73%, more than 60%
10.66.250.185	2016-03-14 11:27:31	ADS	Memory Usage	Medium	Memory usage is 72%, more than 60%
10.245.200.24	2016-03-14 11:27:27	ADS	Memory Usage	Medium	Memory usage is 72%, more than 60%
10.66.250.45	2016-03-14 11:26:40	ADS	Device Offline	High	No heartbeat 2 day(s) 18 hour(s) 25 minute(s)

Table 6-3 describes parameters of performance alert logs.

Table 6-3 Parameters of performance alert logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Device whose logs are queried. **All** indicates that logs on all devices are queried.
Alert Type	Alert type, which could be **Any**, **CPU Usage**, **Memory Usage**, **Device Offline**, or **HA Alert**. **Any** indicates that alerts of all types are queried.
Severity	Alert severity, which could be **Any**, **High**, **Medium**, or **Low**. **Any** indicates that alerts of all severities are queried.

6.8 HA Log

When the master and slave devices synchronize information such as configuration files and engine exceptions, ADS M will record such synchronization in HA logs, for further analysis and conclusion.

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

Figure 6-8 HA logs

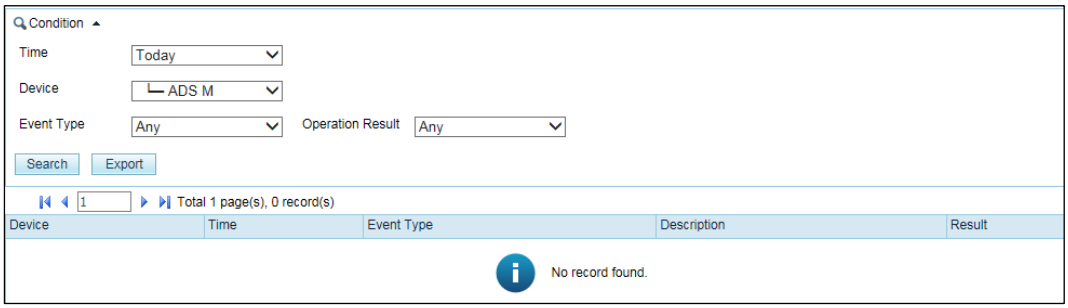


Table 6-4 describes parameters of HA logs.

Table 6-4 Parameters of HA logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Type of devices, which can be **ADS M** or **ADS**, indicating that HA logs on ADS M or ADS devices will be displayed.
Event Type	HA event type, which could be **Any**, **HA Start**, **HA Stop**, **Synchronize Configuration File**, **Update HA Configuration**, or **Exception**. **Any** indicates that logs of all event types are queried.
Operation Result	Operation result, which could be one of the following: • **Succeeded**: indicates that all logs about succeeded operations are queried. • **Failed**: indicates that all logs about failed operations are queried. • **Any**: indicates that logs with any results are queried.

6.9 Traffic Alert Log

The **Traffic Alert Log** page can be displayed only when **Detection Mode** is set to **NTA** on the **Basic Settings** page. For the configuration of the detection mode, see section 3.1.1 Basic Settings.

Choose **Log** > **Traffic Alert Log**. The **Traffic Alert Log** page appears, as shown in Figure 6-9.

You can set specific conditions to query or export all traffic alert logs of all NTA devices. The log information includes:

- Alert ID
- Alert type
- Severity
- Attacked IP address
- Region

- Attack time (such as start time, end time, or duration)
- Description

  The description is usually instantaneous traffic in the unit of pps and bps when the alert is generated. If the traffic of the attacked IP address is being diverted or filtered, words such as being diverted or being filtered will be displayed in the **Description** column.

Figure 6-9 Traffic alert logs

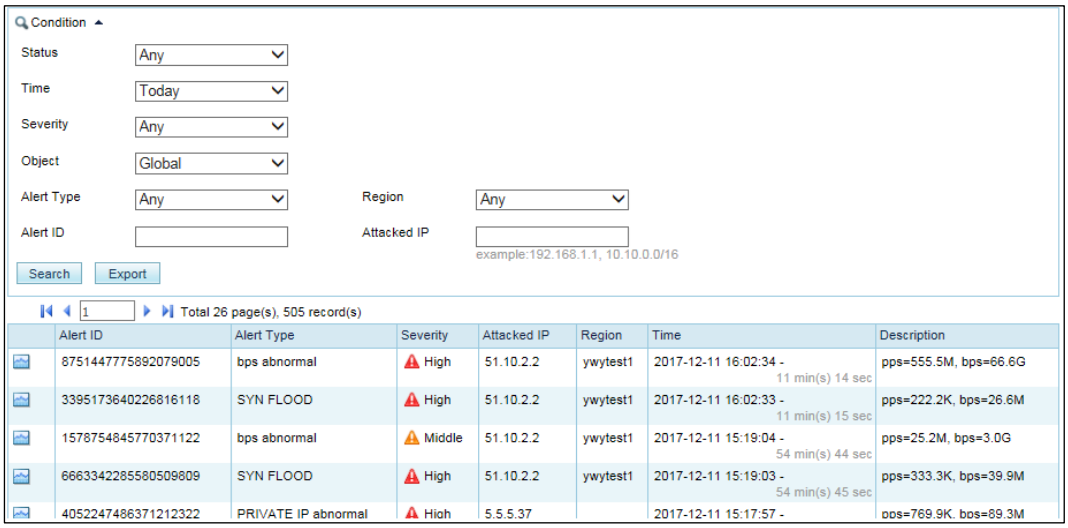


Table 6-5 describes parameters of traffic alert logs.

Table 6-5 Parameters of traffic alert logs

Parameter	Description
Status	Specifies the status of alerts to be queried, which can be set to one of the following: • **Ongoing**: indicates alerts that are occurring. • **Ended**: indicates alerts that are over. • **Any**: indicates all generated alerts.
Time	Specifies the query time range. The default value is **Today**, that is, logs of the current day are queried. In addition, you can query logs monthly, on a specified day, or in a custom period. For **Custom**, you need to set the start time and end time.
Severity	Specifies the alert severity, which can be set to **High**, **Medium**, and **Low**. **Any** indicates that alerts of all severities are queried.
Object	• **Global** indicates that alerts generated by all NTA devices are queried. • **By device** indicates that alerts generated by an NTA device are queried.
Device (Optional)	This option is available only when **Object** is set to **By device**. NTA devices added on ADS M will be displayed here. For NTA configuration, see section 8.3 Managing NTA Devices.
Alert Type	Specifies the type of alert events that can be reported by NTA devices to ADS M. **Any** indicates that alerts of all types are queried.
Region	Specifies the region where alerts are queried.

Parameter	Description
	New regions on ADS M are also displayed here. For region configuration, see section 7.3 Configuring a Region. **Any** indicates that alerts in all regions are queried.
Alert ID	Specifies the alert ID. The alert ID is reported by the NTA device to ADS M. This alert ID is the same as that on the NTA.
Attacked IP	Specifies the IP address that suffers attacks.

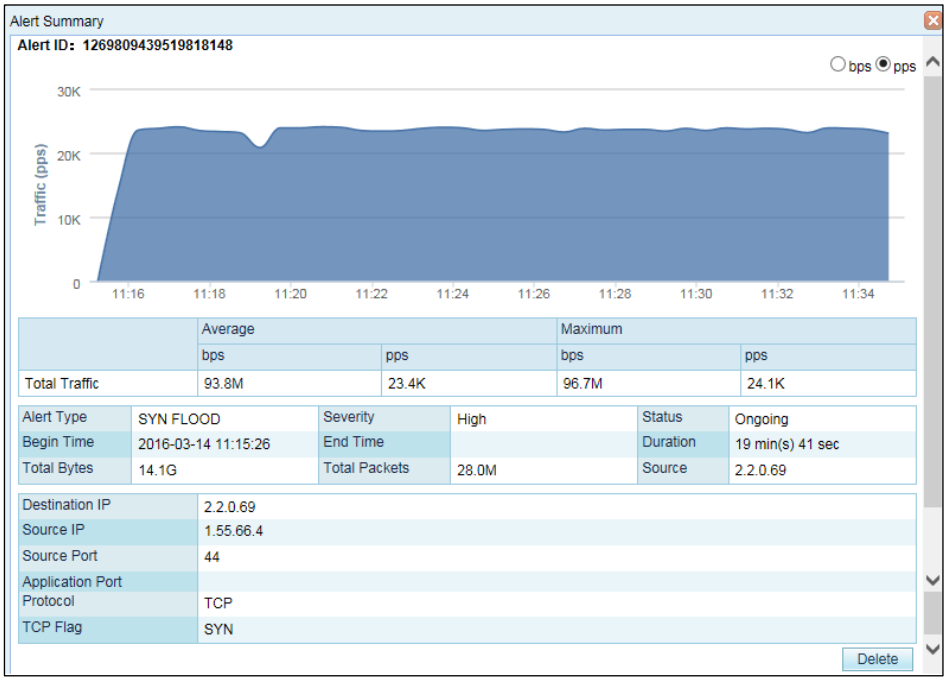
Click in the query results to open the **Alert Summary** page, as shown in Figure 6-10. This page displays detailed information of this alert, including:

- Traffic trend graph
- Average total traffic
- Maximum total traffic
- Other alert information

If the query time range is over three hours, the system displays the traffic trend only in three hours. You can select **bps** or **pps** to view the trend of abnormal traffic in pps or bps or click **Delete** in the lower-right corner of this page to delete this alert record.

Caution	After you click **Delete**, the alert record is deleted from the database, and cannot be restored. Please perform this operation with caution.

Figure 6-10 Alert summary



6.10 Cloud Authentication Logs

The **Cloud Authentication Logs** page is available only when an ADS M virtual machine is used. For how to configure cloud authentication, see section 3.1.2 License Management.

Choose **Log > Cloud Authentication Logs**. The **Cloud Authentication Logs** page appears.

Figure 6-11 Cloud Authentication Logs page

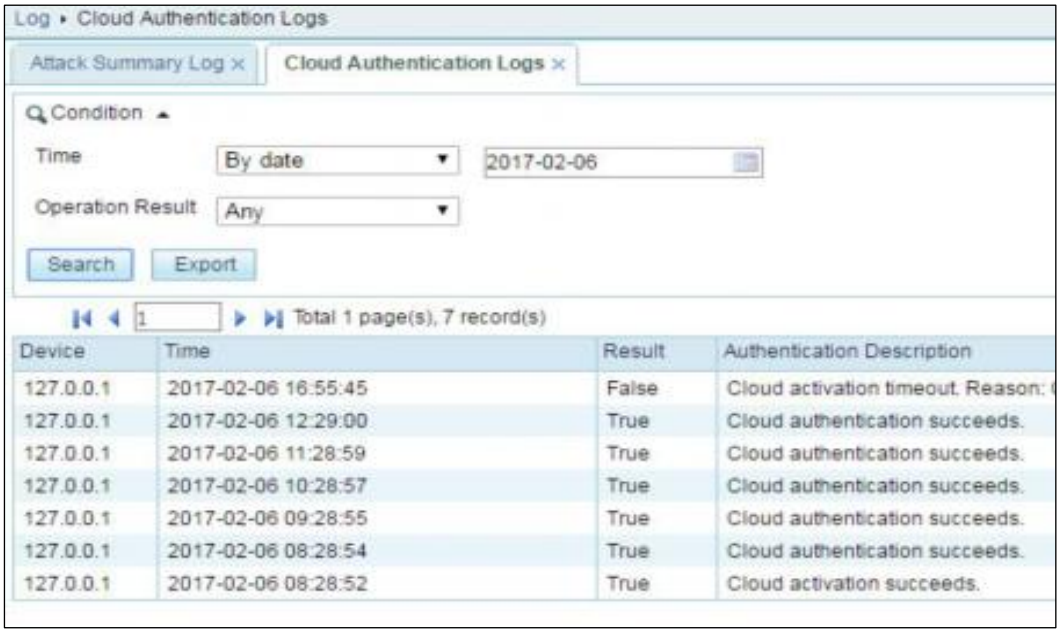


Table 6-6 describes parameters for querying cloud authentication logs.

Table 6-6 Parameters for querying cloud authentication logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Other options include **By Date**, **By Month**, and **Custom**. **Custom** indicates that you can query logs in a specified time range.
Operation Result	• **Successful** indicates that logs of successful activation or authentication are queried. • **Failed** indicates that logs of failed authentication are queried. • **Any** indicates that all logs are queried.

7 Region Management

A region is a collection of one or more ADS-protected hosts that work at the same geographical region or have some characteristics in common. Traffic of hosts in a region is displayed as a whole. Region management enables the administrator to perform corresponding deployment and management tailored to different requirements.

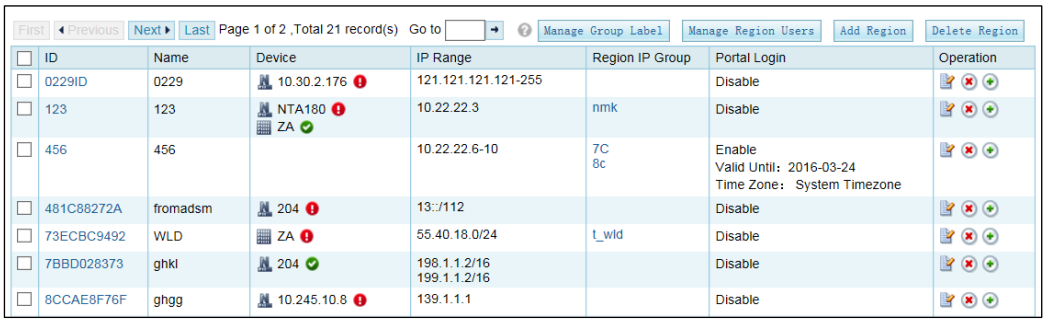
7.1 Managing Group Labels

ADS M supports grouped management of regions. A group label identifies one or more regions, facilitating region classification.

Choose **Region** > **Region Management**.

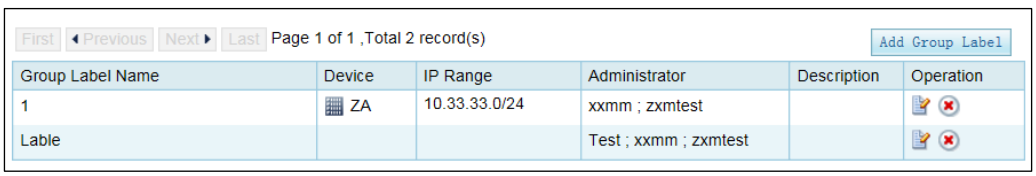
The **Region List** page appears, as shown in Figure 7-1.

Figure 7-1 Region list



Click **Manage Group Label**. The group label management page appears, as shown in Figure 7-2.

Figure 7-2 Group label management page



You can create, edit, and delete a group label.

7.1.1 Creating a Group Label

Click **Add Group Label** on the page shown in Figure 7-2. The dialog box for creating a group label appears, as shown in Figure 7-3.

Figure 7-3 Creating a group label

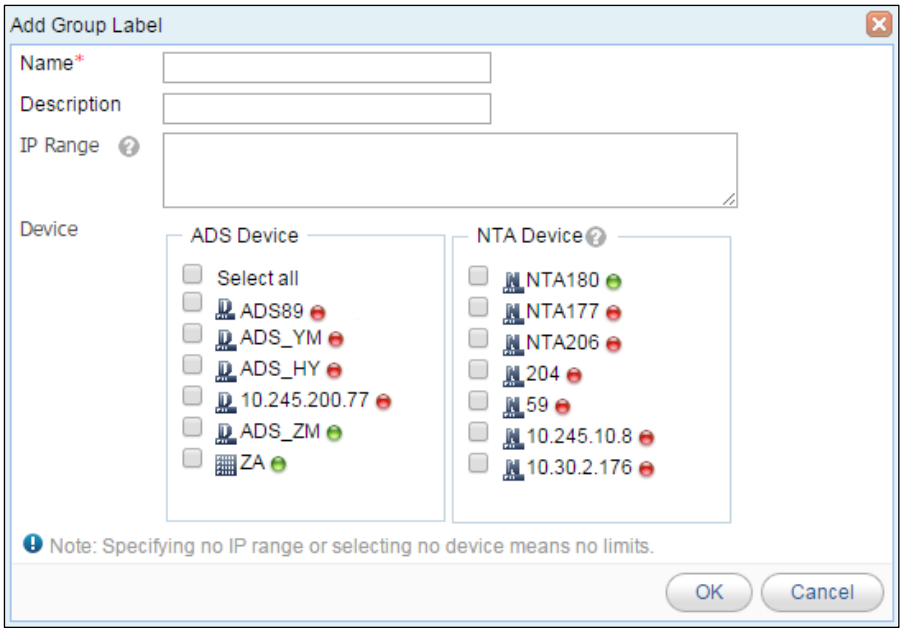


Table 7-1 describes parameters for creating a group label.

Table 7-1 Parameters for creating a group label

Parameter	Description
Name	Name of the group label, which cannot be the same as an existing one or the name of a region.
Description	Brief description of the group label.
IP Range	IP address range under this group label. Both IPv4 and IPv6 addresses are accepted. You can type one or more IP addresses, IP address ranges, and IP segments, with each in a separate line. A maximum of 4096 entries are allowed.
Device	ADS and NTA devices that are assigned this group label. Only devices that are managed by ADS M are available for you to select.

7.1.2 Editing a Group Label

In the group label list, click in the **Operation** column to edit a group label.

7.1.3 Deleting a Group Label

In the group label list, click in the **Operation** column to delete a group label.

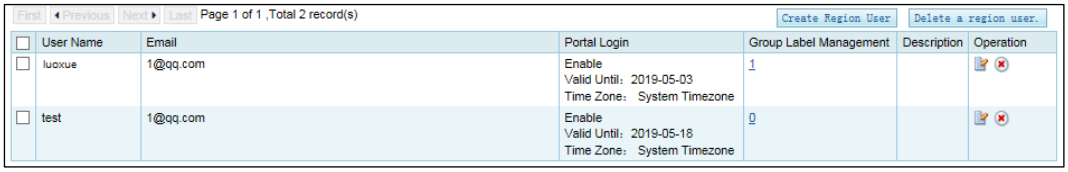
Caution	Deleting a group label will delete the region that references this label and all IP groups in the region. Also, this operation will make it impossible for a region user to log in to the enabled Portal system.

7.2 Managing Region Managers

A region manager for whom the Portal is enabled can create or edit regions on the Portal.

On the **Region List** page shown in Figure 7-1, click **Manage Region Users** in the upper-right corner. The list of region managers appears.

Figure 7-4 List of region managers



A system administrator can create, edit, or delete region managers.

7.2.1 Creating a Region Manager

On the **Manage Region Users** page shown in Figure 7-4, click **Create Region User** in the upper-right corner to create a region manager.

As long as the Portal is enabled (under **Administration > Third-Party Interface > Portal Configuration**), Portal-related settings appear when you create or edit a manager for this region. You can determine whether to enable the Portal for this manager. If the Portal is enabled, you also need to set the Portal login password, validity period, and time zone.

Only the region manager with Portal enabled and assigned a group label can log in to the Portal client for region management. For details about the Portal, see *NSFOCUS ADS Portal User Guide*.

Figure 7-5 Creating a region manager

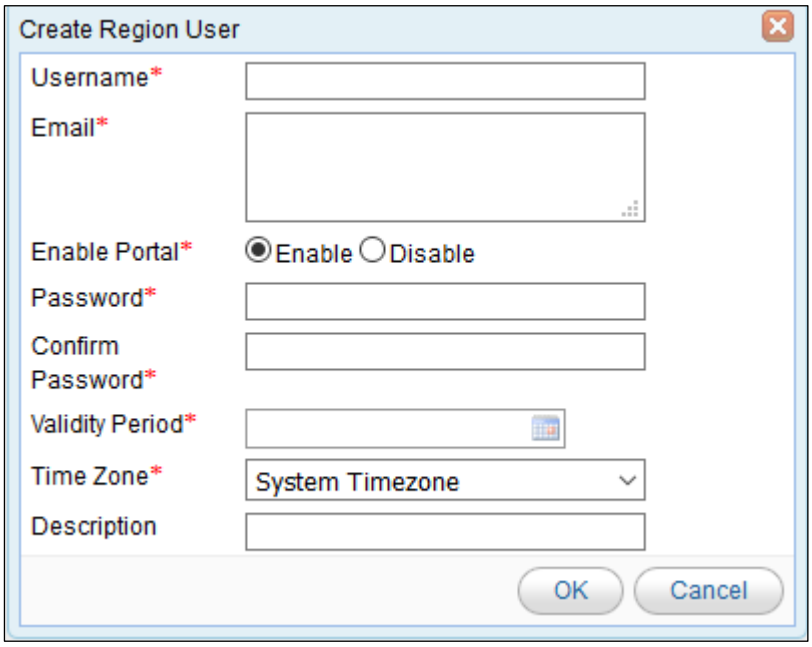


Table 7-2 describes parameters for creating a region manager.

Table 7-2 Parameters for creating a region manager

Parameter	Description
Username	Account name of this region manager. It cannot be the same as an existing region manager account name or region ID.
Email	Email address of this region manager.
Description	Brief description of this region manager.

7.2.2 Configuring Permissions of a Region Manager

On the **Manage Region Users** page shown in Figure 7-4, you can click a figure in the **Group Label Management** column of the region manager list to configure permissions of a region manager.

Figure 7-6 Configuring permissions of a region manager

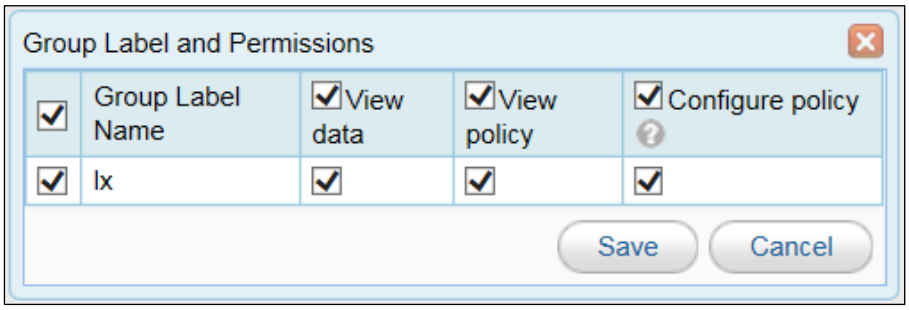


Table 7-3 describes parameters for configuring permissions of a region manager.

Table 7-3 Parameters for configuring permissions of a region manager

Parameter	Description
Group Label Name	Group label under which the region manager can manage settings of devices.
View data	Permission of viewing data of devices under the specified group label.
View policy	Permission of viewing policies applied to devices under the specified group label.
Configure policy	Permission of configuring policies for devices under the specified group label.

7.2.3 Editing a Region Manager

On the region manager list, click in the **Operation** column to edit settings of a region manager.

7.2.4 Deleting a Region Manager

- On the region manager list, click in the **Operation** column to delete a manager.
- On the region manager list, select one or more region managers and click **Delete a region user** to delete the selected managers.

7.3 Configuring a Region

This section details the configuration method of all regions managed by ADS M, including how to create, modify and delete a region.

The method of configuring IP groups varies with the detection mode of ADS M (for the configuration of the detection mode, see section 3.1.1 Basic Settings):

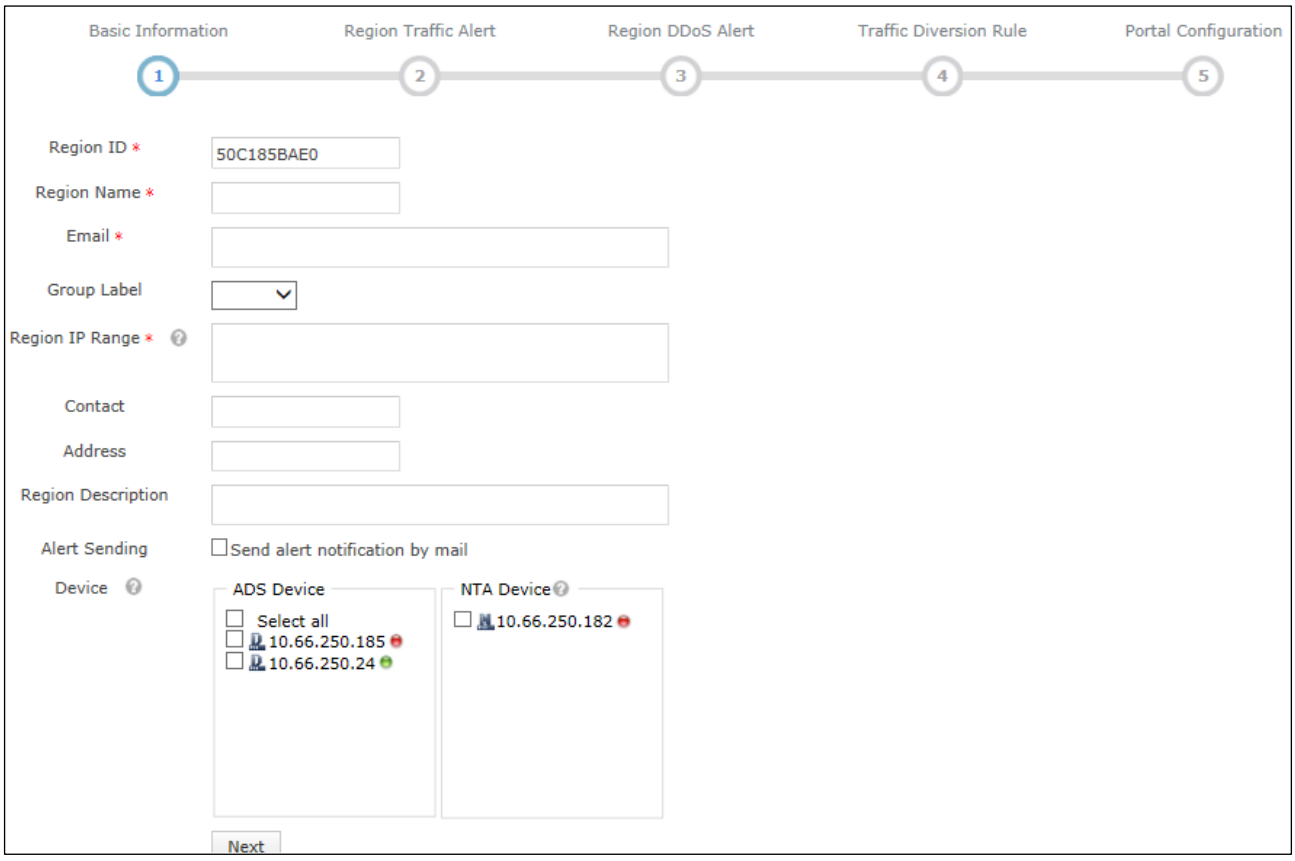
- For the detection mode of **NTA**, you need to configure basic information, region traffic alert parameters, region DDoS alert parameters, and traffic diversion rules.
- For the detection mode of **None** or **Local**, you need to configure only basic information.

7.3.1 Creating a Region

For ADS M whose detection mode is set to **NTA**, follow these steps to create a region:

Step 1 Click **Add Region** in the upper-right corner of the **Region List** page.

Figure 7-7 Configuring basic information of a region



Step 2 Configure basic information.

Table 7-4 Parameters for configuring basic information

Parameter	Description
Region ID	Uniquely identifies a region. It is automatically generated by the system and can be manually changed (note that you cannot change it when editing a region and it cannot be the same as an existing region ID or region user name) when you add a region. The region ID should be a string of 1 to 100 characters, consisting of English letters, digits, and/or underscores.
Region Name	Name of the region, which should be a string of 1 to 50 characters, consisting of English letters, digits, and/or underscores. The new region name cannot be the same as an existing one or the group label.
Email	Email address of the contact person of the region. You can type multiple email addresses, separated with the semicolon (;).

Parameter	Description
	Note Only the first 10 email address will be delivered to NTA devices. After **Send alert notification by mail** is selected, ADS M will periodically send region alerts to the email address of the contact person. For details about scheduling the sending of region alerts , see section 3.3.4 Mail Alert Settings.
Group Label	Specifies the label of the group to which the region belongs. Regions are displayed in hierarchical mode in the region tree in the left pane. Note You can also drag a region to a specific group label in the region tree in the left pane.
Region IP Range	Specifies the IP address range in the region monitored and protected by ADS M. Both IPv4 and IPv6 addresses are accepted. You can type one or more IP addresses, IP subnets, and IP segments, with each in a separate line. A maximum of 4096 entries are allowed. • IPv4 address format: 192.168.0.1, 192.168.0.1/24, or 192.168.0.1–254 • IPv6 address format: 2001::1-ffffe, 2001::1-ffffe/126, or 2001::1 An IP subnet can be a class B or class C IP subnet, containing up to 65,536 IP addresses. The prefix length of IPv4 addresses can be 16–32 and that of IPv6 addresses can be 1–128. Note For the addition of a region, ADS M does not support defining of the region based on router interfaces currently.
Contact	Contact person of the region.
Address	Fixed-line phone or mobile phone number of the contact person.
Region Description	Briefly describes service information of the region.
Alert Sending	Specifies the method of sending host alerts regarding the region. For details about scheduling the sending of region alerts or reports, see section 3.3.4 Mail Alert Settings.
Device	Specifies ADS and NTA devices for the region. Only devices that are managed by ADS M are available for you to select. Region information cannot be dispatched to ADS V4.5R89 and NTA V4.5R89.

Step 3 Configure region traffic alert parameters.

After configuring basic information, click **Next** to open the **Region Traffic Alert** page.

Figure 7-8 Configuring region traffic alert parameters

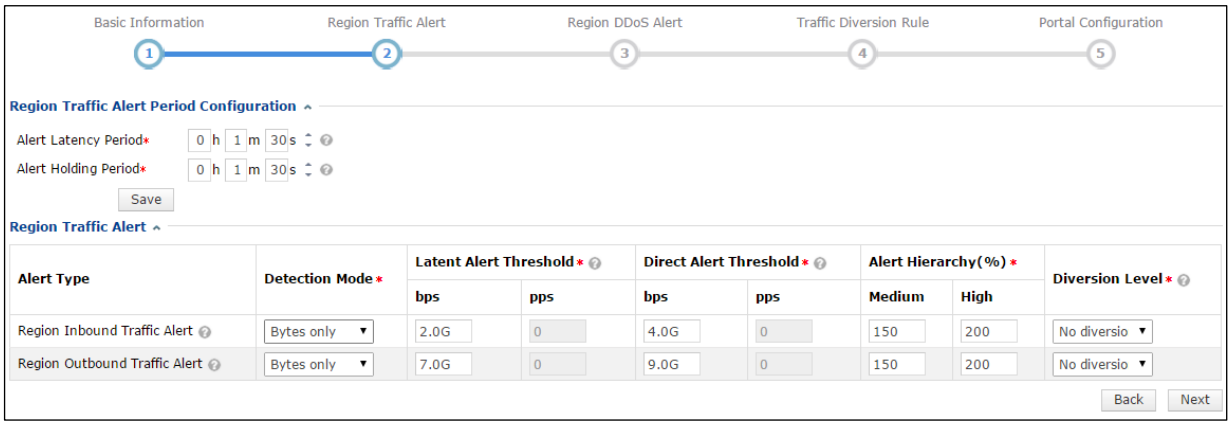


Table 7-5 describes region traffic alert parameters.

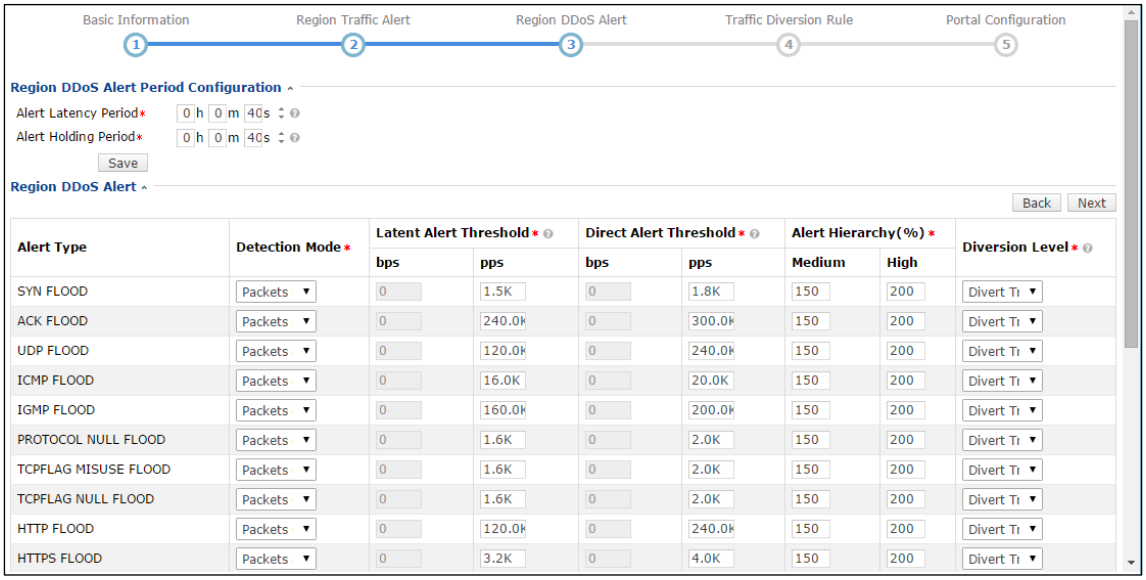
Table 7-5 Region traffic alert parameters

Parameter	Description
Alert Latency Period	Specifies the maximum duration NTA must wait to generate an alert for the traffic between the value of **Latent Alert Threshold** and that of **Direct Alert Threshold**. The value ranges are 0–23 for the hour (**h**), 0–59 for the minute (**m**), and 0–59 for the second (**s**).
Alert Holding Period	Specifies the time when an alert persists after the traffic rate falls below the value of **Direct Alert Threshold**, which indicates that the attack ends. This parameter is valid only for latent alerts. The value ranges are 0–23 for the hour (**h**), 0–59 for the minute (**m**), and 0–59 for the second (**s**).
Alert Type	Specifies the type of region traffic alerts, which can be either of the following: • **Region Inbound Traffic Alert**: checks the total inbound traffic of the region. • **Region Outbound Traffic Alert**: checks the total outbound traffic of the region.
Detection Mode	Specifies a detection mode, which can be **Not detect**, **Packets only**, **Bytes only**, **Both packets and bytes**, and **Either packets or bytes**.
Latent Alert Threshold	Specifies the threshold that triggers NTA to enter the latent period. If the traffic stays below the direct alert threshold but above the latent alert threshold for a certain period (which is called "latency period"), the system generates an alert. The proper use of the latent alert threshold can reduce false positives due to traffic jitter.
Alert Hierarchy	Specifies the hierarchy of traffic alerts and DDoS alerts.
Direct Alert Threshold	Specifies the threshold that triggers NTA to generate an alert.
Diversion Level	Specifies the level of traffic diversion conducted after a region traffic alert is triggered. There are three diversion levels (low, medium, and high), corresponding to three alert levels (low, medium, and high).

Step 4 Configure region DDoS alert parameters.

After configuring region traffic alert parameters, click **Next** to open the **Region DDoS Alert** page.

Figure 7-9 Configuring region DDoS alert parameters



For the description of parameters on this page, see Table 7-5.

Step 5 Configure region traffic diversion rules.

After configuring region alert hierarchy parameters, click **Next** to open the **Traffic Diversion Rule** page.

Figure 7-10 Configuring traffic diversion rules

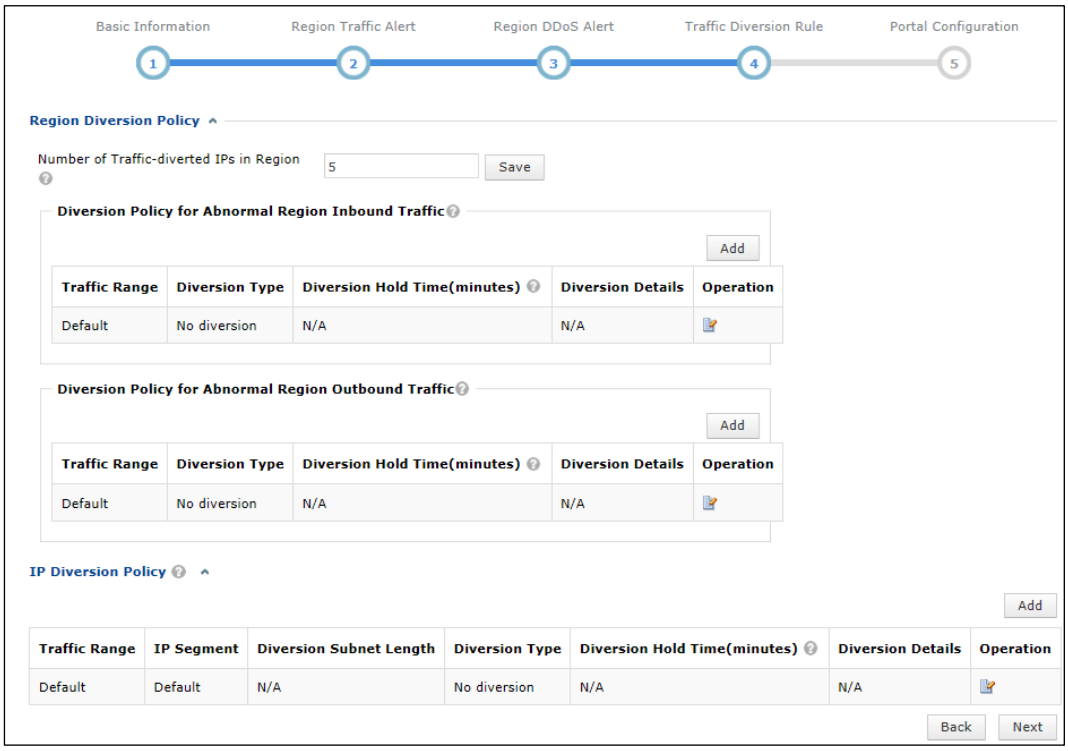


Table 7-6 describes parameters for configuring traffic diversion rules.

Table 7-6 Parameters for configuring traffic diversion rules

Parameter		Description
Region Diversion Policy	Number of Traffic-diverted IPs in Region	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 200. When **Diversion Policy for Abnormal Region Inbound/Outbound Traffic** is triggered, NTA can perform null route diversion for top N IP addresses.
	Diversion Policy for Abnormal Region Inbound Traffic	Specifies the diversion policy for inbound traffic of top N IP addresses when the inbound traffic alert is triggered. • The **Diversion Policy for Abnormal Region Inbound Traffic** can be triggered together with the **Diversion Policy for Abnormal Outbound Region Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** and create new diversion policies.
	Diversion Policy for Abnormal	Specifies the diversion policy for outbound traffic of top N IP addresses when the outbound traffic alert is triggered.

Parameter		Description
	Region Outbound Traffic	• The **Diversion Policy for Abnormal Region Outbound Traffic** can be triggered together with the **Diversion Policy for Abnormal Region Inbound Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** and create new diversion policies.
IP Diversion Policy		Specifies the diversion policy for IP addresses in a specific IP group when the DDoS alert is triggered. • The **IP Diversion Policy** can be triggered together with the **Diversion Policy for Abnormal Inbound IP Group Traffic** and **Diversion Policy for Abnormal Outbound IP Group Traffic**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. • You can click **Add** and create new diversion policies.

Step 6 Configuring the Portal.

After configuring traffic diversion rules, click **Next** to open the **Portal Configuration** page.

Figure 7-11 Configuring the Portal

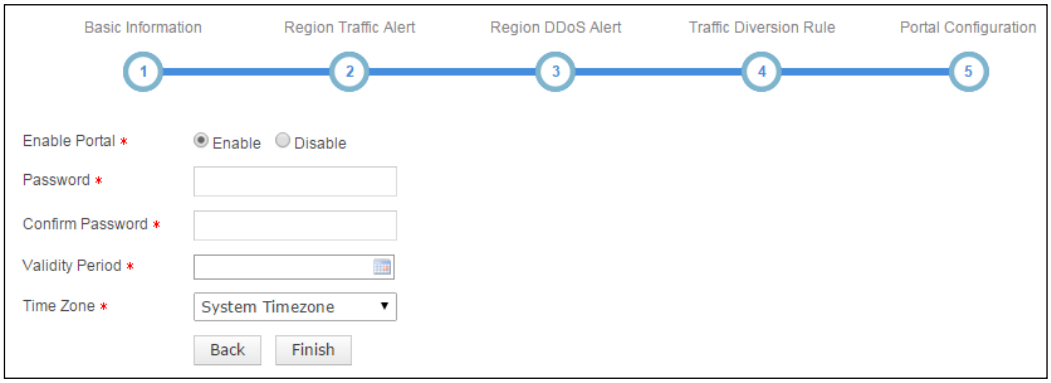


Table 7-7 describes the parameters for configuring the Portal.

Table 7-7 Parameters for configuring the Portal

Parameter	Description
Enable Portal	Controls whether to allow access to the Portal.
Password	Specifies the password for login to the web-based manager of the Portal.

Parameter	Description
	Note The password strength must be consistent with that specified in ADS M.
Confirm Password	Requires you to type the password again. The password you typed here must be the same as that you typed for **Password**.
Validity Period	Specifies how long the Portal account will be available. After the validity period expires, this Portal account will be invalid.
Time Zone	Specifies the time zone that the Portal account belongs to. Note The time zone configured on ADS M for the region takes effect and is displayed on the Portal only after the Portal user logs out and then logs in again. If a user directly configures the time zone on the Portal, the configuration takes effect immediately.

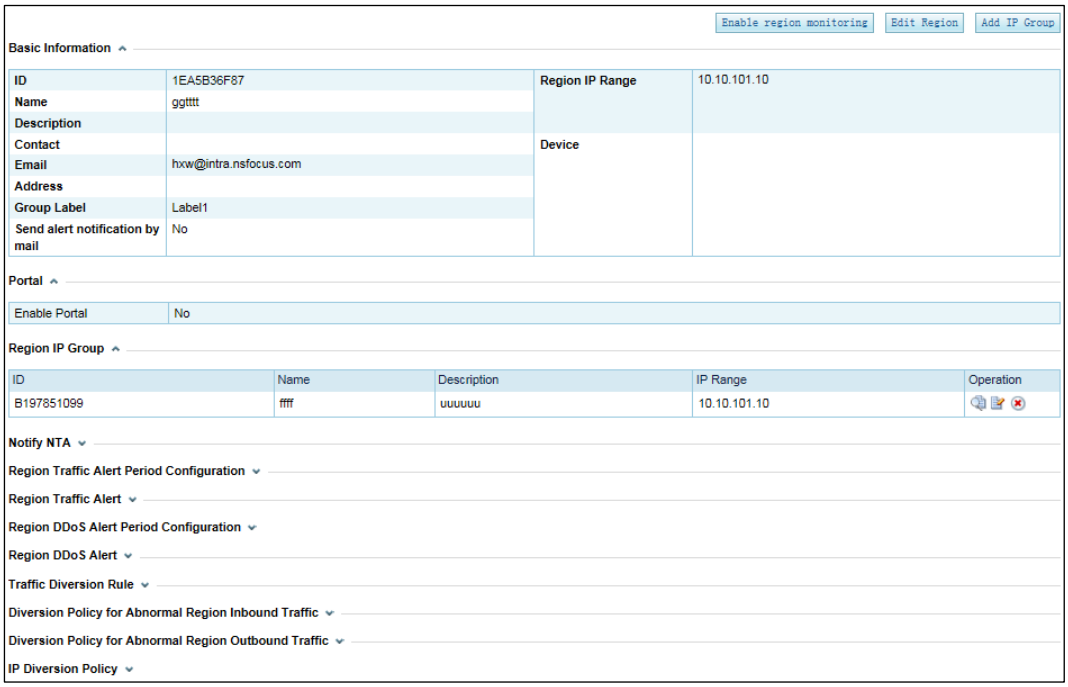
Step 7 After configuring traffic diversion rules, click **Finish**.

----End

7.3.2 Viewing Details of a Region

Choose **Region > Region Management** and select a region from the left region tree or click the ID of a region on the **Region List** page, as shown in Figure 7-12. Then details of the selected region appear.

Figure 7-12 Details of a region



7.3.3 Editing a Region

On the region list, click in the **Operation** column to modify settings of a region. Alternatively, click a region ID on the region list and then click **Edit Region** to open the region editing page.

Note	For a region dispatched by ADS M to NTA, it can be modified only on ADS M. Modifications made on NTA cannot be synchronized to ADS M.

7.3.4 Deleting a Region

On the region list, click in the **Operation** column to delete a region.

Caution	• Deleting a region stops you from continuing to view the opened monitoring page, configuration page, or other pages related to this region. • If NTA devices are offline when you delete a region or the management password is different for ADS M and NTA devices, the deletion of this region removes the region only from ADS M rather than from NTA devices.

7.4 Configuring a Regional IP Group

You can add a regional IP group for an existing region.

The method of configuring IP groups varies with the detection mode of ADS M (for the configuration of the detection mode, see section 3.1.1 Basic Settings):

- For the detection mode of **NTA**, you need to configure basic information, IP group traffic alert parameters, IP group DDoS alert parameters, IP group alert hierarchy parameters, traffic diversion rules, protection policies, and URL rule.
- For the detection mode of **None**, you need to configure basic information, protection policies, and URL rule.

7.4.1 Adding a Regional IP Group

7.4.1.1 NTA Detection Mode

Step 1 On the **Region List** page shown in Figure 7-1, click in the **Operation** column to add an IP group for a region.

Alternatively, you can click **Add IP Group** on the page shown in Figure 7-12.

Figure 7-13 Adding an IP group in NTA detection mode

Step 2 Configure basic information of the IP group.

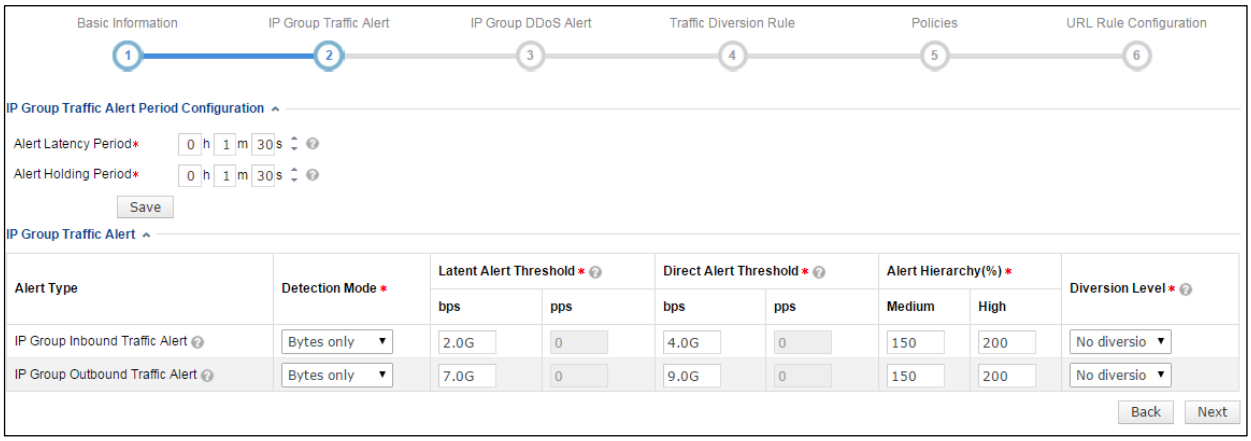
Table 7-8 Parameters for configuring basic information of an IP group

Parameter	Description
IP Group ID	Uniquely identifies an IP group. It is automatically generated by the system and can be manually changed (note that you cannot change it when editing an IP group and it cannot be the same as an existing one) when you add an IP group. The IP group ID should be a string of 1 to 50 characters, consisting of English letters, digits, and/or underscores.
IP Group Name	Name of the IP group, which should be a string of 1 to 50 characters, consisting of English letters, digits, and/or underscores.
IP Group IP Range	IP address range monitored and protected by ADS M. The IP address range can include one or more IP addresses, IP subnets, and IP segments. Each IP address or IP segment should be in a separate line. You can add up to 1024 entries. IP addresses in an IP group must be covered by the IP address range of the region. Otherwise, the system prompts you to change the range. Different IP groups in a region must contain different IP addresses. Otherwise, the system prompts you to change the range. When you type IP addresses, the IP range of the region to which the IP group belongs is dynamically displayed below the text box. **Note** A region can have a maximum of 64 IP groups, each of which can contain a maximum of 1024 entries.
IP Group Description	Brief description of the IP group.
Notify NTA	Controls whether to send NTA diversion notifications, alert notifications, or SNMP trap messages.

Step 3 Configure IP group traffic alert parameters.

After configuring basic information, click **Next** to open the **IP Group Traffic Alert** page.

Figure 7-14 Configuring IP group traffic alert parameters

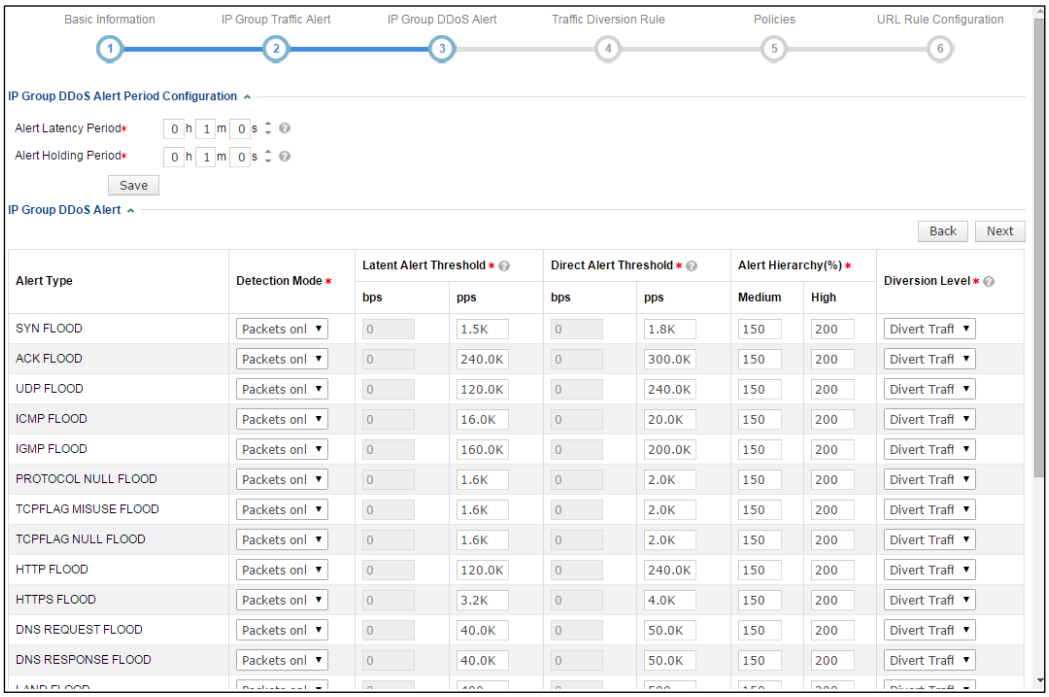


Parameter configuration here is the similar to that for a region. For the description of parameters, see Table 7-5.

Step 4 Configure IP group DDoS alert parameters.

After configuring IP group traffic alert parameters, click **Next** to open the **IP Group DDoS Alert** page.

Figure 7-15 Configuring IP group DDoS alert parameters



For the description of parameters on this page, see Table 7-5.

Step 5 Configure IP group traffic diversion rules.

After configuring IP group alert hierarchy parameters, click **Next** to open the **Traffic Diversion Rule** page.

Figure 7-16 Configuring IP group traffic diversion rules

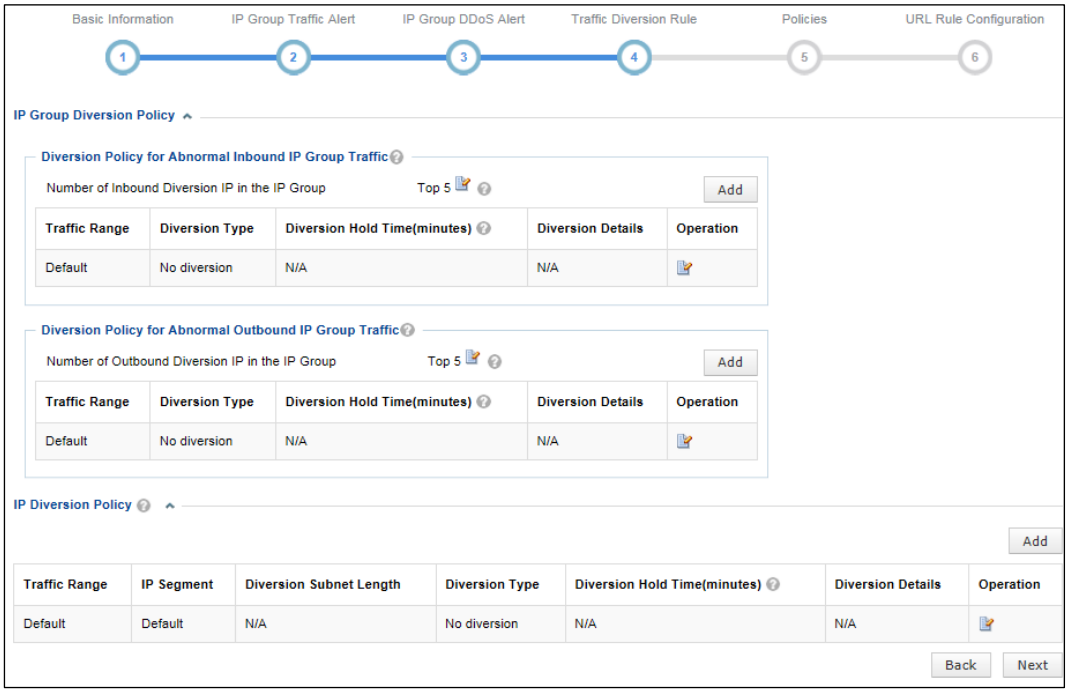


Table 7-9 describes parameters for configuring traffic diversion rules for an IP group.

Table 7-9 Parameters for configuring diversion rules for an IP group

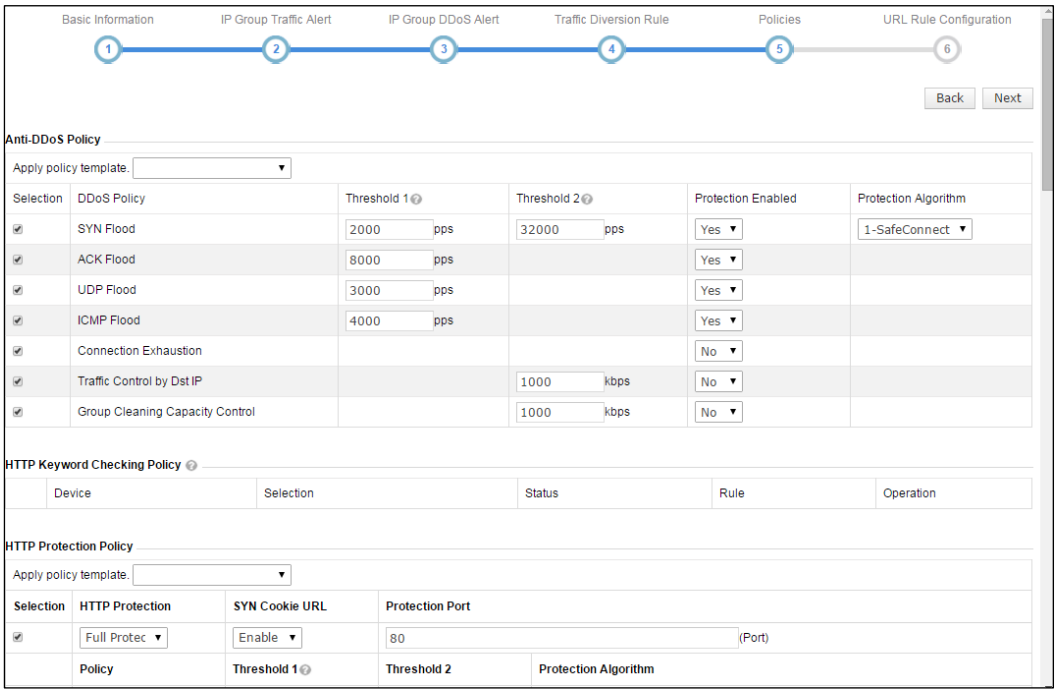
Parameter		Description
IP Group Diversion Policy	Diversion Policy for Abnormal Inbound IP Group Traffic	Specifies the diversion policy for inbound traffic of top N IP addresses or all IP addresses (**Any**) in an IP group when the inbound traffic alert is triggered. • The **Diversion Policy for Abnormal Inbound IP Group Traffic** can be triggered together with the **Diversion Policy for Abnormal Outbound IP Group Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. **Note** The diversion policy for a region has a lower priority than that for an IP group. • When the **Diversion Policy for Abnormal Inbound IP Group Traffic** is triggered, NTA can perform null route diversion for the top N IP addresses or all IP addresses (**Any**) in an IP group. N stands for a variable ranging from 1 to 200. The system sorts top N IP addresses every 5 minutes. • You can click **Add** and add new diversion policies.

Parameter		Description
	Diversion Policy for Abnormal Outbound IP Group Traffic	Specifies the diversion policy for outbound traffic of top N IP addresses in an IP group when the outbound traffic alert is triggered. • The **Diversion Policy for Abnormal Inbound IP Group Traffic** can be triggered together with the **Diversion Policy for Abnormal Outbound IP Group Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • When **Diversion Policy for Abnormal Region Outbound Traffic** is triggered, NTA can perform null route diversion for top N IP addresses. N stands for a variable ranging from 1 to 200. The system sorts top N IP addresses every 5 minutes. • You can click **Add** and add new diversion policies.
IP Diversion Policy		Specifies the diversion policy for IP addresses in a region when the DDoS alert is triggered. • **IP Diversion Policy** can be triggered together with the **Diversion Policy for Abnormal Inbound Region Traffic** and **Diversion Policy for Abnormal Outbound Region Traffic**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. • You can click **Add** and add new diversion policies.

Step 6 Configure IP group protection policies.

After configuring traffic diversion rules, click **Next** to open the **Policies** page.

Figure 7-17 Configuring IP group protection policies

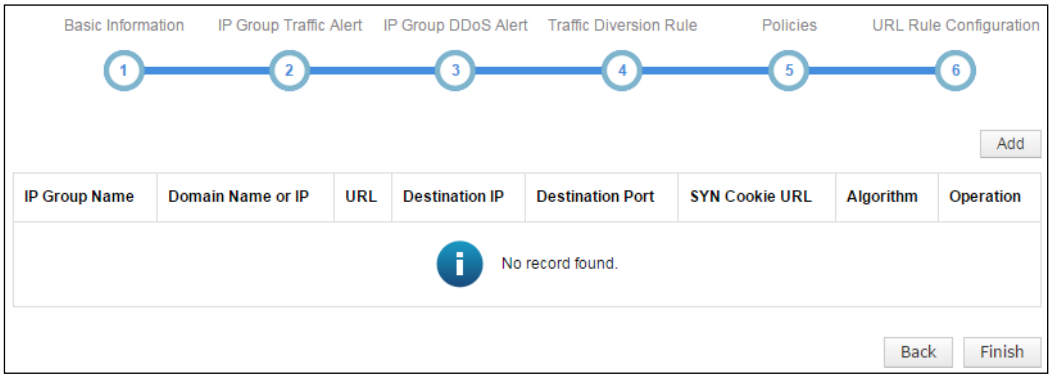


To edit protection policies, you can directly modify default settings or use policy templates. The method of configuring policies on ADS M is the same as that for policies on ADS devices. For details, see *NSFOCUS ADS User Guide*.

Step 7 Configure URL rules.

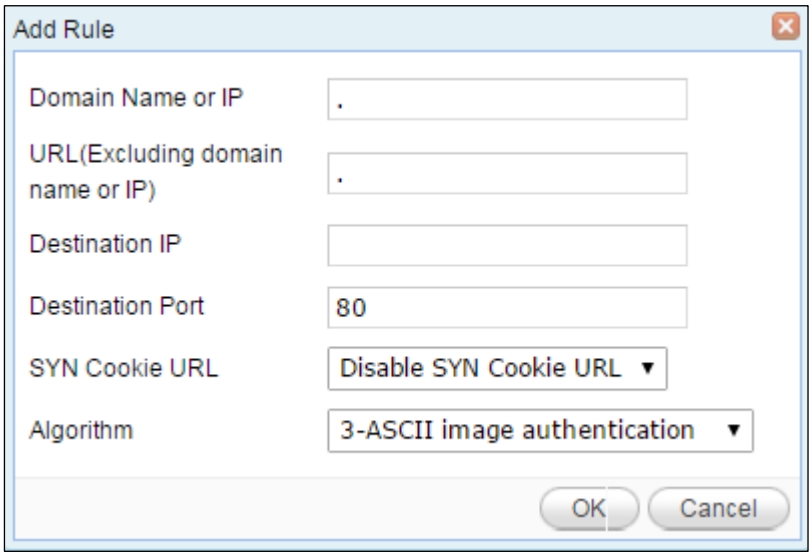
After configuring policies, click **Next** to open the **URL Rule Configuration** page.

Figure 7-18 Configuring a URL rule



a. Click **Add**.

Figure 7-19 Adding a URL rule



b. In the **Add Rule** dialog box, configure URL rule parameters.

Table 7-10 URL rule parameters

Parameter	Description
Domain Name or IP	Domain name or IP address of the server. The dot (.) indicates that this rule is valid for all domain names or IP addresses.
URL(Excluding domain name or IP)	Specifies the URL of a page on the server, with the domain name or IP address excluded. The dot (.) 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	Port of the server.
SYN Cookie URL	Controls whether to enable **SYN Cookie URL**.
Algorithm	Algorithm of the URL rule. Nine algorithms are available for you to select.

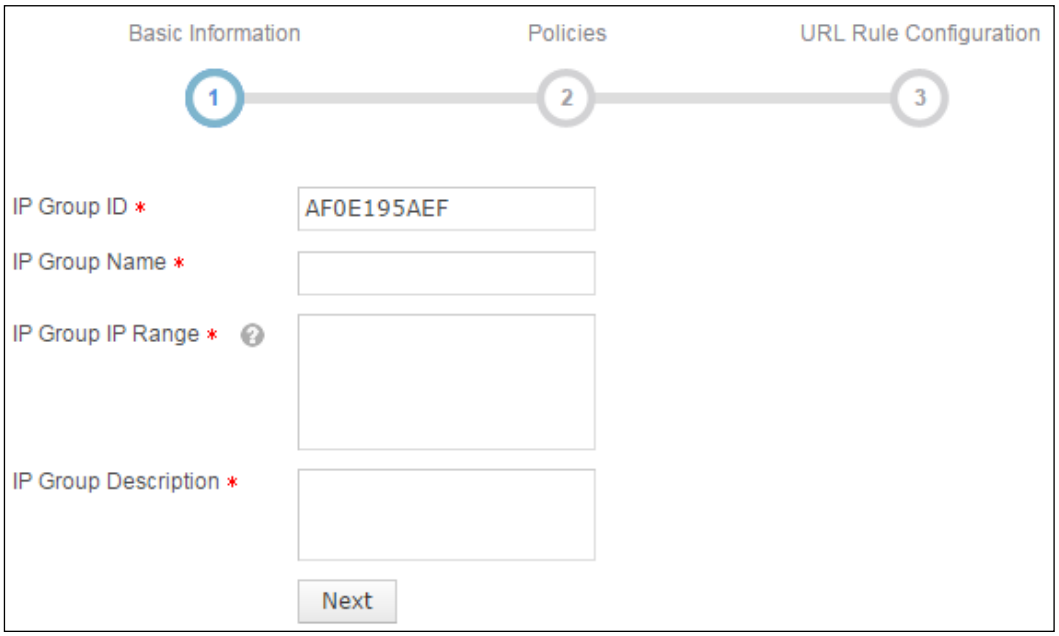
Step 8 After configuring the URL rule, click **Finish**.

----End

7.4.1.2 "None" Detection Mode

Step 1 Click **Add IP Group** on the page shown in Figure 7-12.

Figure 7-20 Adding an IP group in "None" detection mode



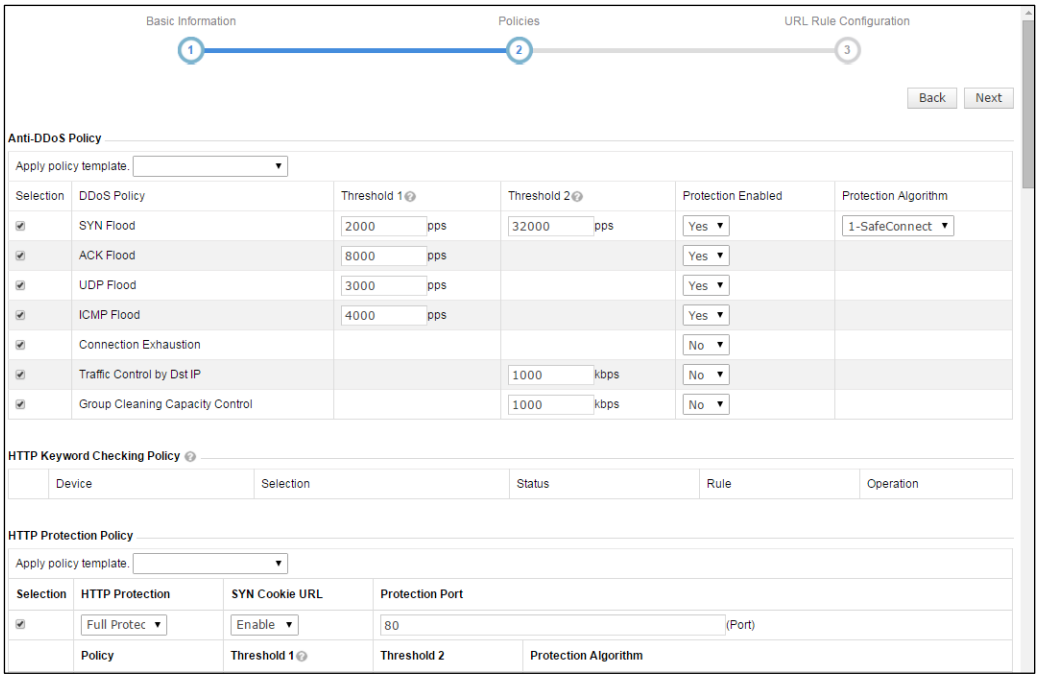
Step 2 Configure basic information for adding an IP group.

For the description of parameters for configuring basic information, see Table 7-8.

Step 3 Configure IP group protection policies.

After configuring basic information, click **Next** to open the **Policies** page.

Figure 7-21 Configuring IP group protection policies in "None" detection mode

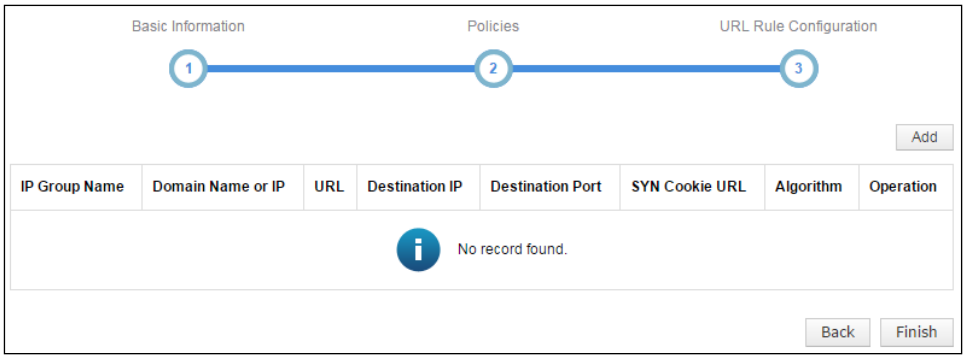


To edit protection policies, you can directly modify default settings or use policy templates. The method of configuring policies on ADS M is the same as that for policies on ADS devices. For details, see *NSFOCUS ADS User Guide*.

Step 4 Configure URL rules.

After configuring policies, click **Next** to open the **URL Rule Configuration** page.

Figure 7-22 Configuring URL rules in "None" detection mode



For details about configuring a URL rule, see Step 7 in section 7.4.1.1 NTA Detection Mode.

Step 5 After configuring the URL rule, click **Finish**.

----End

7.4.2 Modifying a Regional IP Group

On the regional IP group list, click in the row of a regional IP group to modify parameters (except the IP group ID) of the regional IP group.

Note	For regional IP groups dispatched by ADS M to ADS or NTA, they can be modified only from ADS M, but not on ADS or NTA. Even if you modify such IP groups on ADS or NTA, the modifications cannot be synchronized to ADS M.

7.4.3 Deleting a Regional IP Group

On the regional IP group list, click in the row of a regional IP group to delete the IP group.

Caution	• Deleting a regional IP group stops you from continuing to view the opened monitoring page, configuration page, or other pages related to this group. • If ADS or NTA devices are offline when you delete an IP group, the management password is different for ADS M and NTA devices, or the IP group is undergoing traffic diversion, the deletion of this IP group removes the group only from ADS M rather than from ADS or NTA devices.

7.4.4 Viewing Configuration Information of a Regional IP Group

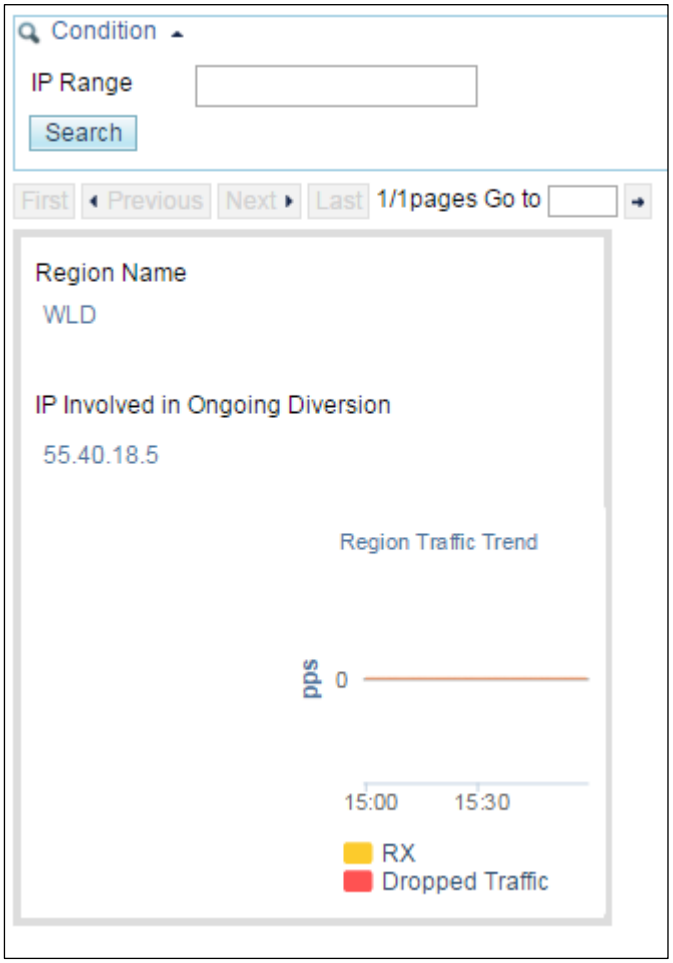
On the regional IP group list, click in the row of a regional IP group to view the configuration information of the IP group.

7.5 Configuring Traffic Diversion for a Region

You can check the ongoing traffic diversion and IP addresses whose traffic can be diverted in the region, and also manually divert the traffic of certain IP addresses.

Choose **Region > Traffic Diversion**. The page shown in Figure 7-23 displays the IP address under traffic diversion and the traffic trend of the region to which this IP address belongs. If no traffic diversion is happening currently, the system displays "No region is involved in traffic diversion."

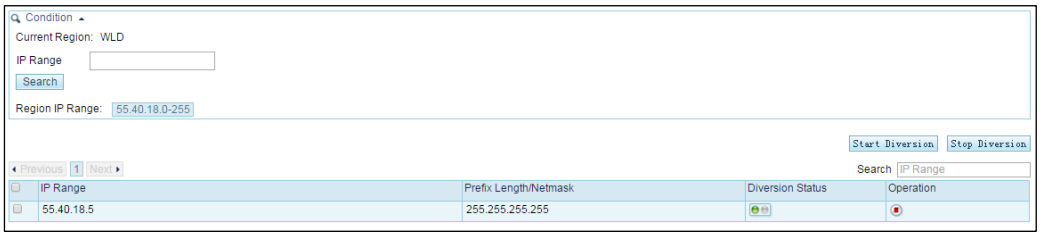
Figure 7-23 Region traffic diversion



7.5.1 Viewing the Region Under Traffic Diversion

You can click the region name on the page shown in Figure 7-23 to view the IP address range of this region and the IP address under traffic diversion, as shown in Figure 7-24. Note that only the IP addresses within this region in question can be retrieved.

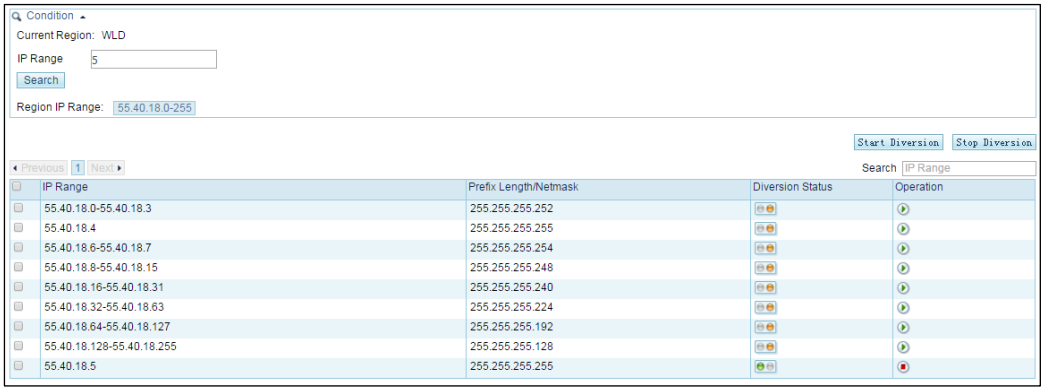
Figure 7-24 Viewing the region under traffic diversion



7.5.2 Configuring IP Addresses for Diversion

On the page shown in Figure 7-24, you can type an IP address range for query. Fuzzy query is supported. For example, if you type 5, all IP addresses starting with this digit will be displayed.

Figure 7-25 Searching for IP addresses whose traffic can be diverted



- Icons in the **Diversion Status** column are described as follows:
  - : Traffic diversion is not supported.
  - : Traffic diversion is ongoing.
  - : Traffic diversion is supported, but no traffic is being diverted.
- Icons in the **Operation** column are described as follows:
  - : starts traffic diversion.
  - : stops traffic diversion.

Also, you can select multiple IP addresses and click **Start Diversion** to start traffic diversion for them, or click **Stop Diversion** to stop traffic diversion.

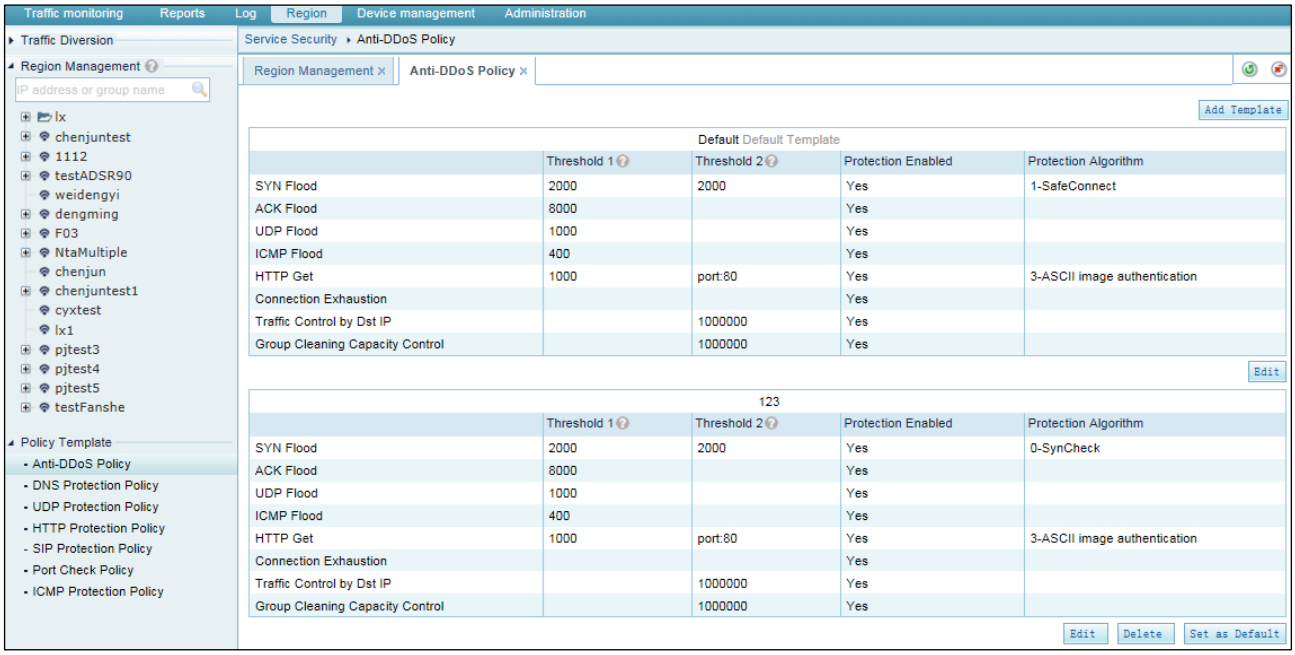
Note	To ensure successful traffic diversion, before starting diversion for an IP address on this page, make sure that the following items are properly configured for this IP address: routing daemon, IP route assignment, injection route, injection interface, and diversion filtering rule.

7.6 Configuring an ADS Protection Policy Template

The protection policies of ADS are used to detect and prevent DDoS attacks on devices under centralized management. ADS M provides various policy templates and allows users to configure their own according to their particular business needs. A policy template can be assigned to multiple ADS devices.

Step 1 Choose **Region > Policy Template > Anti-DDoS Policy**.

Figure 7-26 Anti-DDoS policy template



You can edit the following policy templates:

- Anti-DDoS policy
- DNS protection policy
- UDP protection policy
- HTTP protection policy
- SIP protection policy
- Port check policy
- ICMP protection policyFor detailed configuration operations, see the *NSFOCUS ADS User Guide*.

Note	By default, a new protection group and regional IP group adopt the default anti-DDoS policy template. For details about anti-DDoS policy parameters, see appendix A Parameters.

8 Device Management

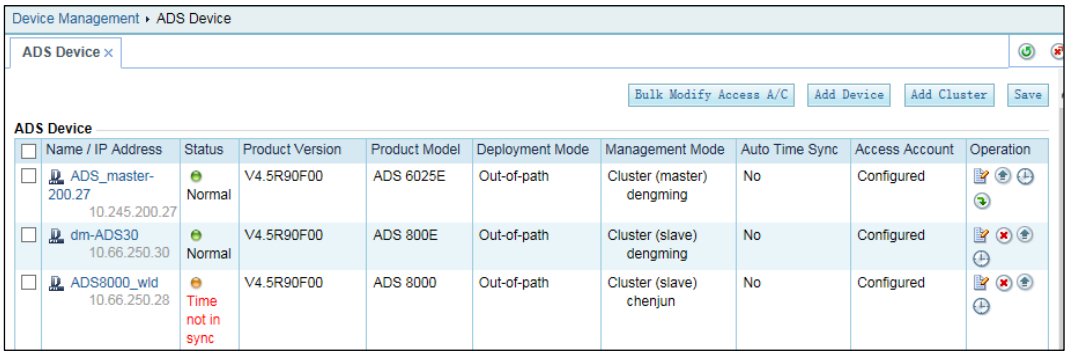
This chapter describes in detail the configuration methods of devices under ADS M, including how to add, modify and delete an ADS device, ADS cluster, and NTA device.

8.1 Managing ADS Devices

Click **Device Management > ADS Device**.

The **ADS Device** page appears, as shown in Figure 8-1.

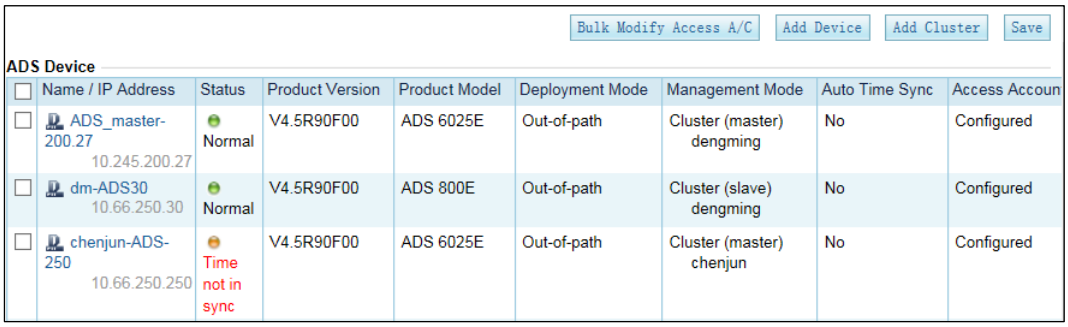
Figure 8-1 ADS Device page



The ADS device list consists of ADS devices and clusters, as shown in Figure 8-2. Initially, the device list is empty and you need to add devices or clusters manually. Clicking a device name opens the page for configuring protection policies.

When ADS is in the packet forwarding state, the state is also indicated in the **Device Monitoring** area on the **System Overview** page. If the license of ADS is about to expire in less than seven days, the system displays a message indicating that the license will expire in X days. When the license validity period is displayed as 0 days, the system displays a message indicating that the license is invalid or expires.

Figure 8-2 ADS devices



Prior to adding an ADS device, you need to log in to the web-based manager of this device to verify that this device is subordinate to ADS M (**System** > **Local Settings** > **Management Mode**) and type the IP address of ADS M**.** For details, see *NSFOCUS ADS User Guide***.**

After you complete the configuration and properly connect the two devices, this ADS device is subordinate to ADS M and appears in the treelike structure of monitoring objects.

8.1.1 Adding an ADS Device

To add an ADS device, follow these steps:

Step 1 Click **Add Device** in the upper-right corner of the **ADS Device** page shown in Figure 8-1.

The dialog box for adding an ADS device appears, as shown in Figure 8-3.

Figure 8-3 Adding an ADS device

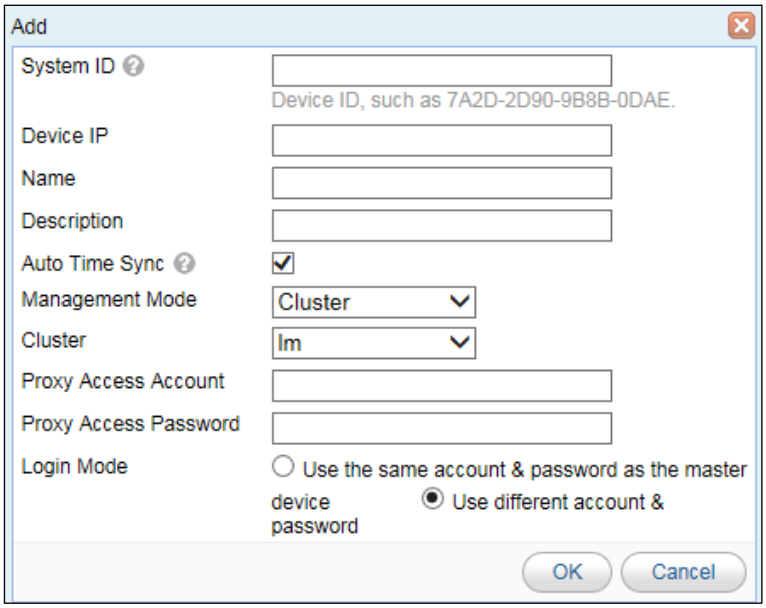


Table 8-1 describes parameters of an ADS device.

Table 8-1 Parameters of an ADS device

Parameter	Description
System ID	Specifies the system ID of the ADS device. It is required.
Device IP	Specifies the IP address of the device. Either an IPv4 or IPv6 address is accepted. It is required.
Name	Specifies the device name. It must be 1 to 20 characters long and cannot contain invalid characters such as angle brackets (<, or >), quotation marks (" or '), and slashes (/). The device name is mandatory and must be unique.
Description	Specifies the brief description of this ADS device such as the use of the device.
Auto Time Sync	Controls whether to automatically synchronize the system time of the device with that of ADS M. By default, this option is selected.
Management Mode	Specifies the device management mode, which can be **Standalone** or **Cluster**. • **Standalone**: indicates that the ADS device is independently deployed and does not accpet centralized management of ADS M. • **Cluster**: indicates that the ADS device accepts centralized management of ADS M. After an ADS device is successfully added, ADS M automatically obtains the ADS deployment mode.
Cluster	Specifies the cluster to which the ADS device belongs. This parameter is required when **Management Mode** is set to **Cluster**.
Group Label	Specifies the label of the group to which the device belongs. The device tree in the left part displays devices by groups. This parameter is required when **Management Mode** is set to **Standalone**.
Proxy Access Account	Specifies the account of the proxy ADS device. After the proxy access account and password are configured, ADS M can directly log in to the corresponding ADS device.
Proxy Access Password	Specifies the password of the proxy ADS device. After the proxy access account and password are configured, ADS M can directly log in to the corresponding ADS device.
Login Mode	• **Use the same account & password as the master device**: indicates that ADS M can use the same account and password to access both the ADS device and the master device. • **Use different account & password**: indicates that ADS M can use the configured account and password to access the ADS device. This parameter is required when **Management Mode** is set to **Cluster**.

Step 2 Set the parameters in the dialog box, and click **OK.**

----End

8.1.2 Editing ADS Device Settings

On the **ADS Device** page, click in the **Operation** column of an ADS device to modify information about the device, except device ID.

8.1.3 Deleting an ADS Device

On the **ADS Device** page, click in the **Operation** column of an ADS device to delete the device. Once an ADS device is deleted, it is no longer subject to management of ADS M and so will not upload its device information to ADS M.

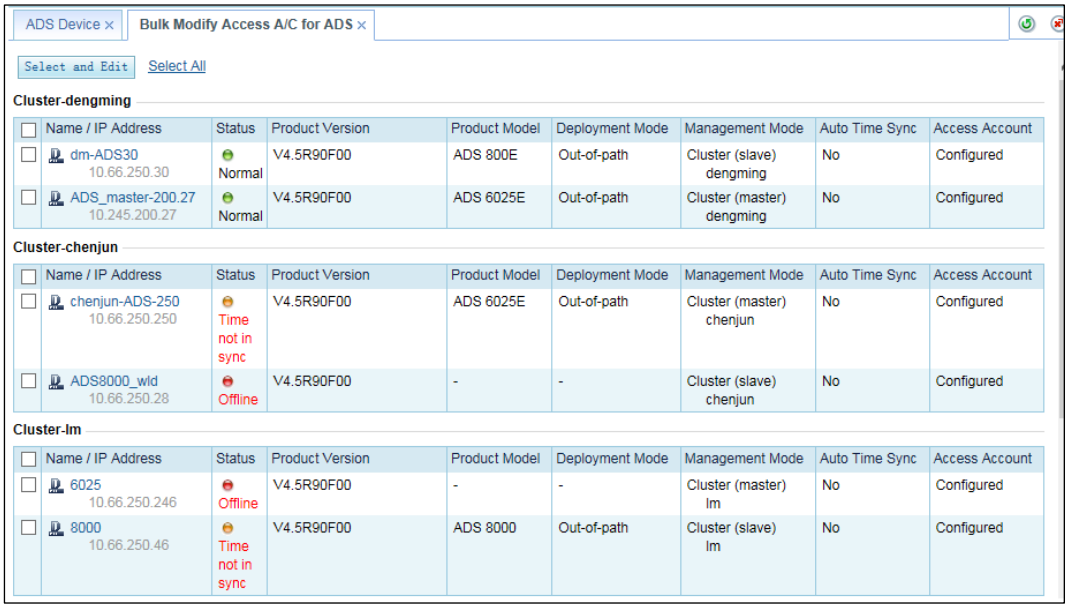
Caution	Once a device is deleted, you cannot continue to view monitoring pages, configuration pages, and other pages related to this device even if these pages were previously opened. In a cluster, the master device cannot be deleted unless the cluster has only one device.

8.1.4 Modifying Access Accounts in Batches

You can modify access account passwords in batches by following these steps:

Step 1 In the ADS device list shown in Figure 8-1, click **Bulk Modify Access A/C**.

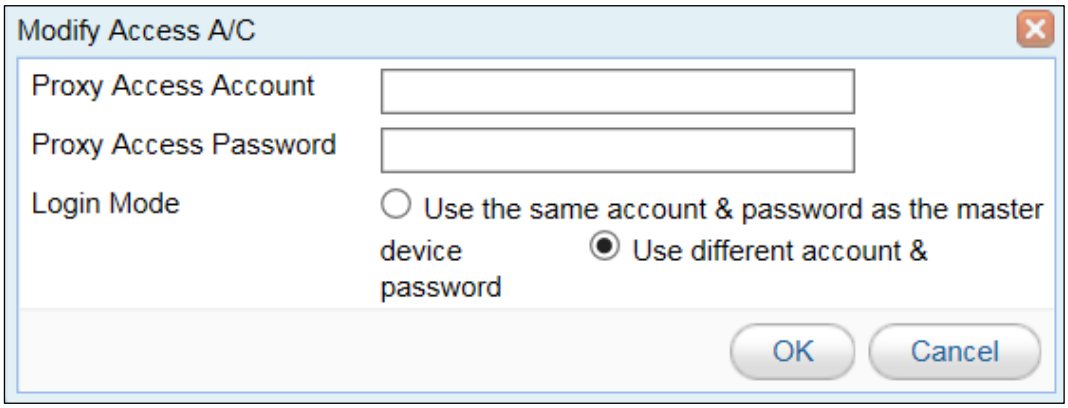
Figure 8-4 Modifying access accounts in batches



Step 2 Click multiple check boxes and then click **Select and Edit**.

You can click **Select All** to select all devices and then configure parameters.

Figure 8-5 Modifying access accounts



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

----End

8.1.5 Synchronizing Time

On the **ADS Device page**, click in the row of an ADS device to synchronize system time between the device and ADS M.

Note	• If system time is inconsistent between an ADS device and ADS M, the status icon of the device turns orange, notifying you of time inconsistency. • Inconsistent system time between two devices may impair the accuracy of statistical reports and device logs. • You are advised to ensure consistent time between ADS devices and the ADS M device through the NTP service.

8.1.6 Manually Synchronizing Configurations

Only the master device has the manual synchronization function.

In the ADS device list shown in Figure 8-1, click to synchronize the settings of the master device to slave devices.

8.1.7 Saving the Configuration

After the ADS device configuration is complete, click in the row of an ADS device save the settings. You can click **Save** in the upper-right corner of the page shown in Figure 8-1 to save the settings of selected devices.

Caution	Pay attention to the followings when saving the configuration:

	• Time synchronization and configuration saving can be performed on online ADS devices only. • If you save the configuration, the configuration information is still valid after the ADS device is restarted; if you do not write to the firmware, the ADS device is restored to the state before it is edited once the device is restarted.

8.1.8 Configuring an ADS Device

After an ADS device is added, you can click its name/IP address to access its web-based manager for configuration. For how to configure an ADS device, see the *NSFOCUS ADS User Guide*.

8.2 Managing ADS Clusters

ADS cluster (that is, device group) facilitates centralized management and configuration of multiple ADS devices. In ADS cluster mode, after the administrator configures protection parameters of the master device, slave devices automatically synchronize the configurations of protection groups configured on the master device. You can determine which configuration items need to be synchronized.

8.2.1 Adding an ADS Cluster

To add an ADS cluster, follow these steps:

Step 1 Click **Add Cluster** in the upper-right corner of the **ADS Device** page shown in Figure 8-1.

The **ADS Cluster** dialog box appears, as shown in Figure 8-6.

Figure 8-6 Adding an ADS cluster

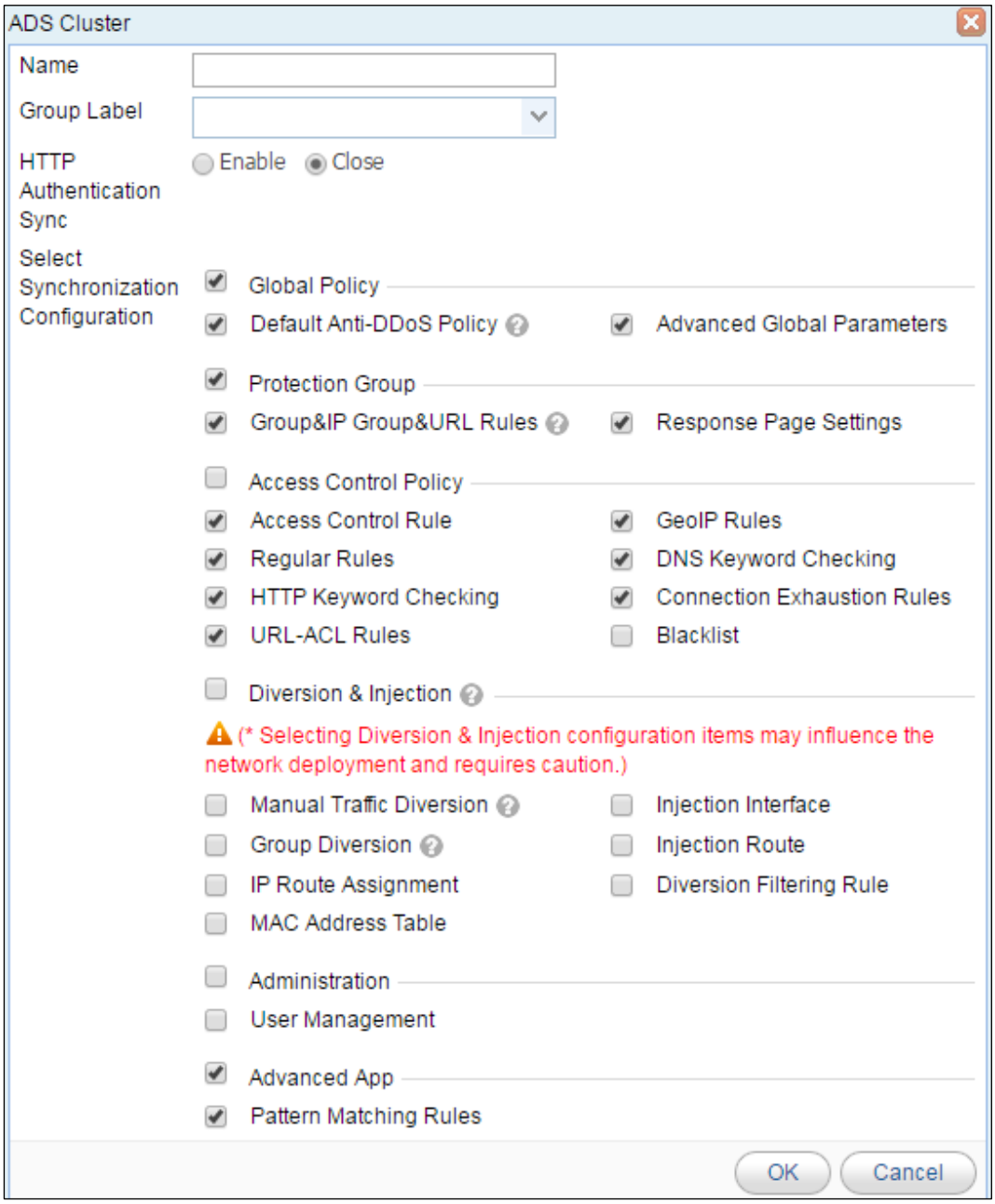


Table 8-2 describes parameters of an ADS cluster.

Table 8-2 ADS cluster parameters

Parameter	Description
Name	Specifies the ADS cluster name. It must be 1 to 20 characters long and cannot contain angle brackets (<, or >), quotation marks (" or '), or slashes (/). The ADS cluster name is mandatory and must be unique.

Parameter		Description
Group Label		Specifies the group label for an ADS cluster The device tree in the left part displays ADS clusters by groups.
HTTP Authentication Sync		Controls whether to enable HTTP authentication synchronization.
Select Synchronization Configuration	Global Policy	Lists global settings that can be synchronized.
	Protection Group	Lists protection group settings that can be synchronized
	Access Control Policy	Lists access control rules that can be synchronized.
	Diversion & Injection	Lists diversion and injection settings that can be synchronized. Synchronizing such items may influence the network deployment. Therefore, handle with care.
	Administration	Controls whether to synchronize user settings.
	Advanced App	Controls whether to synchronize pattern matching rules.

Note	Currently, packet capture can be conducted in a centralized way in an ADS cluster. In other words, when packets are captured on the master device in a cluster, the system prompts whether to capture packets on slave devices.

Step 2 Set parameters in the dialog box and click **OK**.

Then, the new ADS cluster is displayed on the treelike device list.

----End

8.2.2 Configuring a Cluster Blacklist

The cluster blacklist is used to block specified IP addresses. After the blacklist function is enabled, ADS devices in the cluster will block packets from IP addresses on the blacklist permanently or for a specified period, depending on the configuration.

You must manually add IP addresses to the blacklist or import a blacklist file.

Note	To use the cluster blacklist, you must select the **Blacklist** check box under **Select Synchronization Configuration** when creating an ADS cluster.

8.2.2.1 Enabling/Disabling the Blacklist

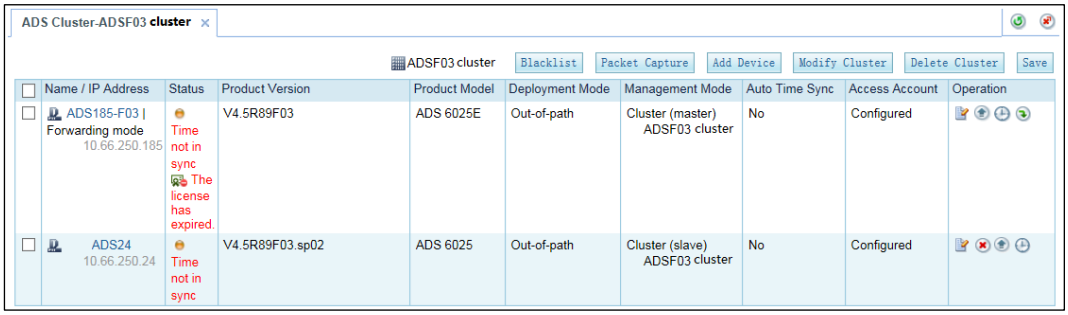
This section describes how to enable and disable the blacklist.

Enabling the Blacklist

To enable the blacklist, follow these steps:

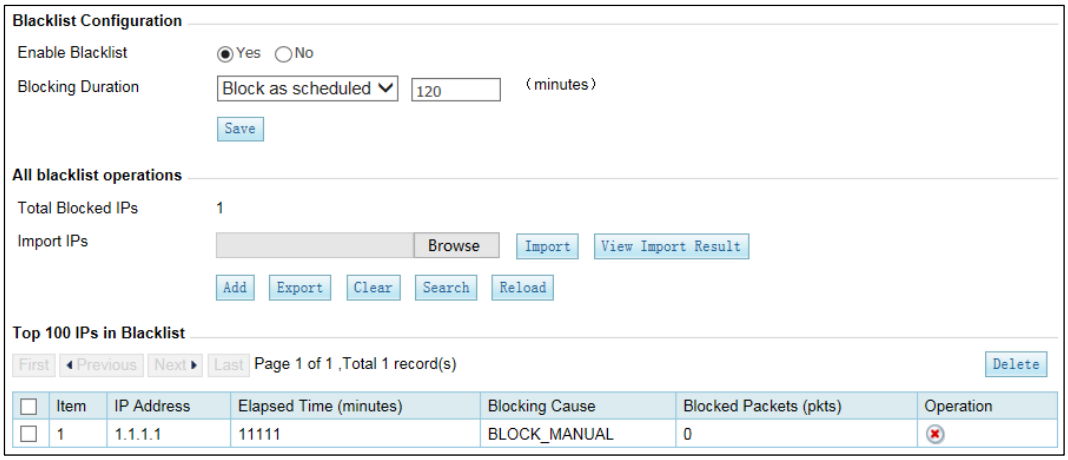
Step 1 After adding an ADS cluster, click its name on the treelike device list in the left pane to open the ADS cluster configuration page.

Figure 8-7 Configuring an ADS cluster



Step 2 Click **Blacklist** in the upper-right of the page.

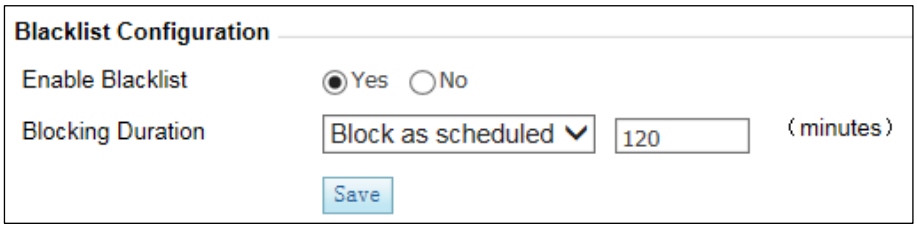
Figure 8-8 Blacklist Configuration page



Step 3 Set **Enable Blacklist** to **Yes**.

The blocking duration refers to the length of time that a blacklisted IP address is blocked. The option **Block as scheduled** 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 8-9 Blacklist configuration



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

----End

Disabling the Blacklist

To disable the blacklist, follow these steps:

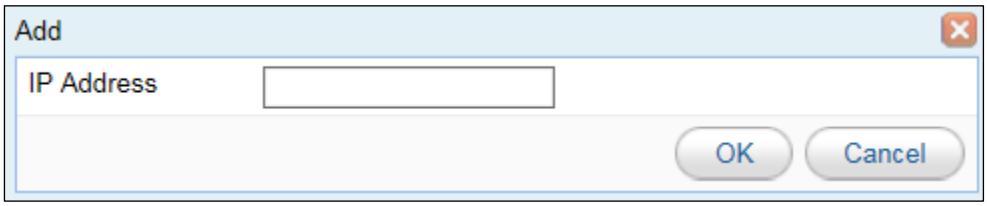
On the page shown in Figure 8-9, set **Enable Blacklist** to **No**.

8.2.2.2 Adding a Blacklist

To manually add a blacklist, follow these steps:

Step 1 In the **All blacklist operations** area shown in Figure 8-8, click **Add**.

Figure 8-10 Adding a blacklist



Step 2 Type the IP address of packets to be blocked (only IPv4 addresses are supported) and then click **OK**.

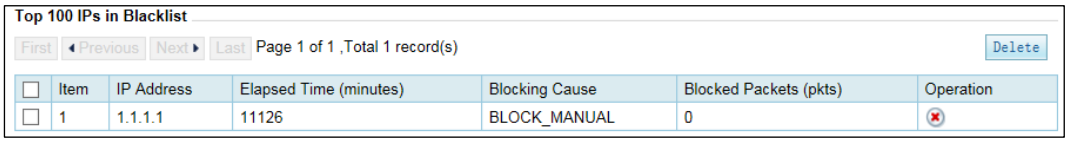
----End

8.2.2.3 Viewing the Blacklist

In the **Top 100 IPs in Blacklist** area shown in Figure 8-8, the system displays a maximum of the most recent 100 blacklisted IP addresses.

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 8-11 Viewing blacklist entries



8.2.2.4 Delete Blacklist Entries

You can delete blacklist entries one by one or in batches.

Deleting Blacklist Entries One by One

In the area shown in Figure 8-11, click in the **Operation** column of a blacklist entry and then click **OK** in the confirmation dialog box to delete this blacklist entry.

Deleting Blacklist Entries in Batches

Step 1 In the area shown in Figure 8-11, select one or more blacklist entries and then click **Delete**.

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

----End

8.2.2.5 Importing a Blacklist Configuration File

To import a blacklist configuration file, follow these steps:

Step 1 In the **All blacklist operations** area shown in Figure 8-8, click **Browse**.

Step 2 Select the blacklist configuration file and click **Open** to return to the blacklist configuration page.

Step 3 Click **Import**.

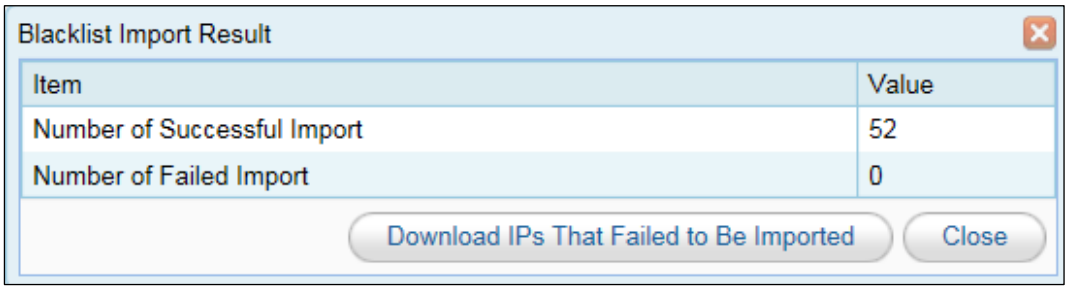
----End

8.2.2.6 Viewing the Import Result

To view the blacklist import result, follow these steps:

Step 1 In the **All blacklist operations** area shown in Figure 8-8, click **View Import Result**. The number of IP addresses successfully imported and that of IP addresses failing to be imported are displayed, as shown in Step 1.

Figure 8-12 Blacklist import result



Step 2 For IP addresses failing to be imported, click **Download IPs That Failed to Be Imported** to import them to a local disk drive.

Step 3 Click **Close** to return to the blacklist configuration page.

----End

8.2.2.7 Exporting a Blacklist Configuration File

In the **All blacklist operations** area shown in Figure 8-8, click **Export** to download all blacklist configuration files of the current cluster to a local disk drive.

8.2.2.8 Clearing Blacklist Entries

Step 1 In the **All blacklist operations** area shown in Figure 8-8, click **Clear**.

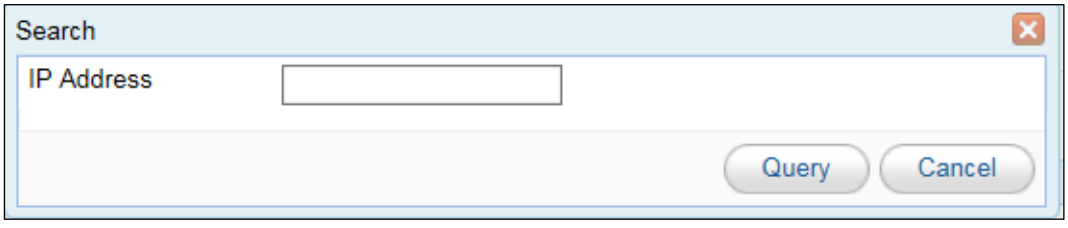
Step 2 In the confirmation dialog box, click **OK** to clear all blacklist entries, including all entries displayed in the **Top 100 IPs in Blacklist** area.

----End

8.2.2.9 Querying a Blacklist Entry

Step 1 In the **All blacklist operations** area shown in Figure 8-8, click **Search**.

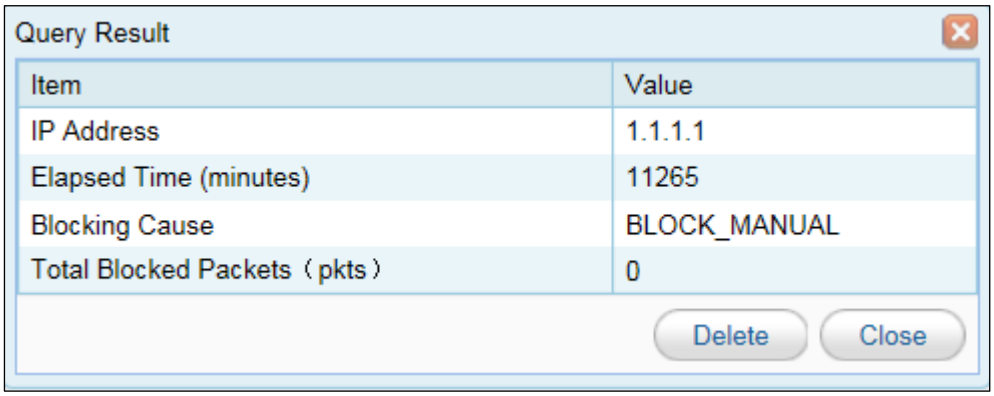
Figure 8-13 Querying a blacklist entry



Step 2 Type the IP address to be queried and then click **Query**.

The query result is displayed, as shown in Figure 8-14.

Figure 8-14 Query result



----End

8.2.3 Cluster Packet Capture

Cluster packet capture is to capture network packets from master and slave devices according to the configured conditions. Packets can be captured manually and automatically.

8.2.3.1 Configuring Manual Packet Capture

Creating a Manual Packet Capture Task

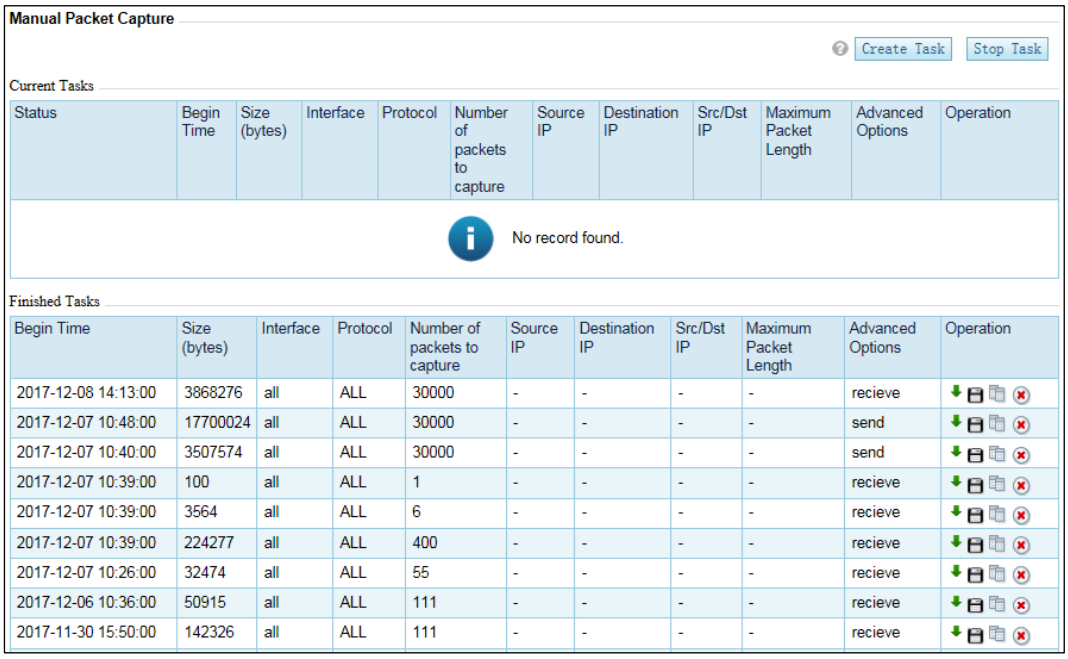
To create a manual packet capture task, follow these steps:

Step 1 On the page shown in Figure 8-7, click **Packet Capture**.

The packet capture configuration page appears. Figure 8-15 shows the **Manual Packet Capture** area.

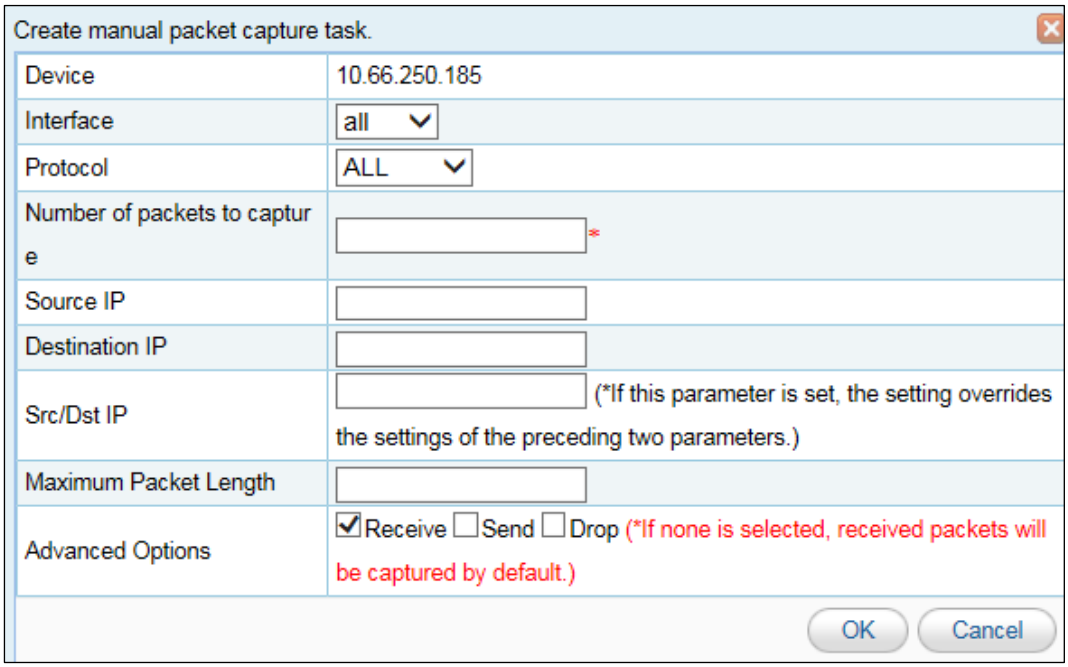
In the upper part of the **Manual Packet Capture** area, the status of packet capture tasks is displayed. When the packet capture task is in progress, **Status** is displayed as **Ongoing**. When the packet capture task is manually stopped, **Status** is displayed as **Stopped**.

Figure 8-15 Manual Packet Capture area



Step 2 Click **Create Task**.

Figure 8-16 Creating a manual packet capture task



Step 3 Configure manual packet capture parameters.

Table 8-3 Parameters for creating a manual packet capture task

Parameter	Description
Device	Device object of this task, which cannot be modified.
Interface	Interface on which packets are captured for this task. **All** indicates that packets on all interfaces are captured.
Protocol	Specifies a protocol. Packets using the specified protocol will be captured. The value can be **All**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**, with **All** as the default value.
Number of packets to capture	Number of the packets to be captured. The value ranges from 1 to 30000.
Source IP	Specifies the source IP address of this task. This parameter is optional. Leaving this parameter empty indicates that packets from any IP address will be captured. Note The source IP address can be an IPv4 or IPv6 address.
Destination IP	Specifies the destination IP address of this task. This parameter is optional. Leaving this parameter empty indicates that packets to any IP address will be captured. Note The destination IP address can be an IPv4 or IPv6 address.
Src/Dst IP	Specifies the source or destination IP address of this task. This parameter is optional. If you set this parameter, ignore **Source IP** and **Destination IP**. Note Both IPv4 and IPv6 addresses are allowed.
Maximum Packet Length	Specifies the maximum length of the packets to be captured. The value ranges from 64 to 1518.
Advanced Options	This parameter is optional. Options include **Receive**, **Send**, and **Drop**. • **Receive** indicates that ADS captures received packets. • **Send** indicates that ADS captures packets that are sent. • **Drop** indicates that ADS captures dropped packets. If none is selected, received packets will be captured by default.

Step 4 Click **OK**.

The new manual packet task starts immediately after being added and the status is displayed in the current task list.

----End

Stopping a Manual Packet Capture Task

You can stop a manual packet capture task in either of the following ways:

Method 1: In the current task list shown in Figure 8-15, click in the **Operation** column of a manual packet capture task to stop this task immediately.

Method 2: In Figure 8-15, click **Stop Task** in the upper-right corner of the page to immediately stop manual packet capture tasks that are in progress.

Downloading a Master's Manual Packet Capture File

In the current task list shown in Figure 8-15, click in the **Operation** column of a manual packet capture task to download the master's manual packet capture file to a local disk drive.

Download a Cluster Manual Packet Capture File

In the current task list shown in Figure 8-15, click in the **Operation** column of a manual packet capture task to download the cluster's (including both master and slave devices') manual packet capture file to a local disk drive.

Duplicating a Manual Packet Capture Task

To duplicate a manual packet capture task, follow these steps:

Step 1 In the current task list shown in Figure 8-15, click in the **Operation** column of a manual packet capture task to copy this task and edit its parameters.

Step 2 After editing parameters, click **OK** to start this manual packet capture task immediately.

----End

Deleting a Manual Packet Capture Task

In the finished task list shown in Figure 8-15, click in the **Operation** column of a manual packet capture task and then click **OK** in the confirmation dialog box to delete this task.

8.2.3.2 Configuring Automatic Packet Capture

Creating an Automatic Packet Capture Task

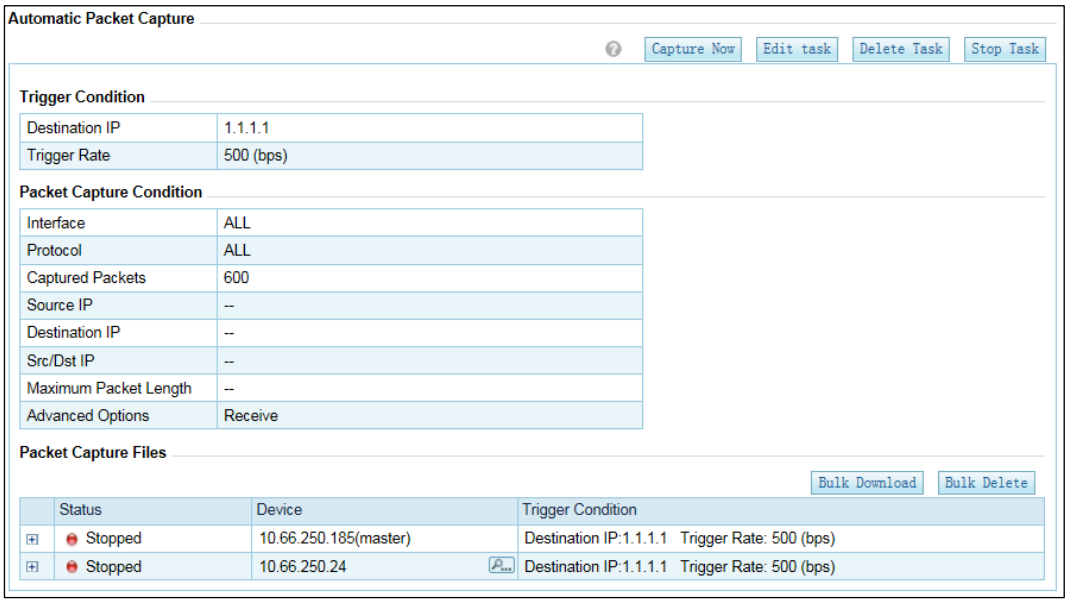
To configure an automatic packet capture task, follow these steps:

Step 1 In Figure 8-7, click **Packet Capture**.

The packet capture configuration page appears. Figure 8-17 shows the **Automatic Packet Capture** area.

In the upper part of the **Automatic Packet Capture** area, the status of packet capture tasks is displayed. When the packet capture task is in progress, **Status** is displayed as **Ongoing**. When the packet capture task is manually stopped, **Status** is displayed as **Stopped**.

Figure 8-17 Automatic Packet Capture area



Step 2 Click **Create Task**.

Figure 8-18 Creating an automatic packet capture task

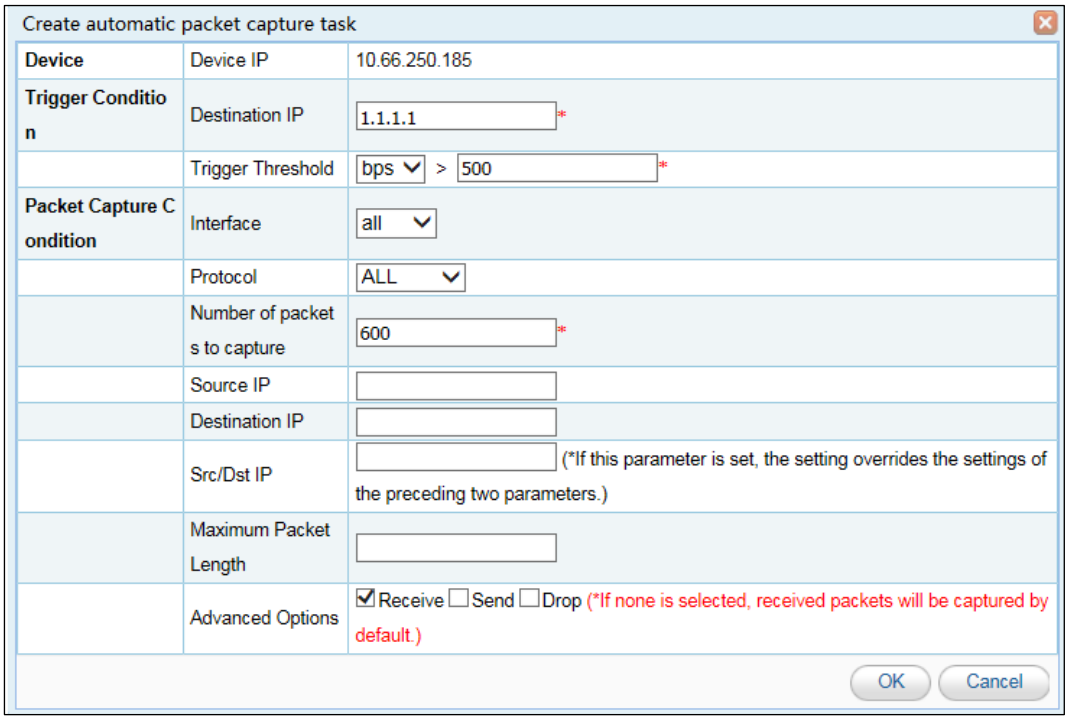


Table 8-4 describes some parameters for creating an automatic packet capture task. For details, see Table 8-3.

Table 8-4 Parameters for creating an automatic packet capture task

Parameter	Description
Device IP	Device object of this task, which cannot be modified.
Destination IP	Specifies the destination IP address for this packet capture task.
Triggering Threshold	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 Click **OK** to complete the configuration.

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

----End

Stopping an Automatic Packet Capture Task

After an automatic packet capture task is created, click **Stop Task** in the upper-right of the **Automatic Packet Capture** area shown in Figure 8-17 to stop this task immediately.

After the automatic packet capture task is stopped, **Status** is displayed as **Stopped**.

Starting an Automatic Packet Capture Task

Stopped automatic packet capture tasks can be manually started.

In Figure 8-17, click **Capture Now** in the upper-right corner to start the automatic packet capture task immediately.

When the packet capture task is in progress, **Status** is displayed as **Ongoing**.

Editing an Automatic Packet Capture Task

To edit an automatic packet capture task, follow these steps:

Step 1 In Figure 8-17, click **Edit Task** in the upper-right corner.

Step 2 After editing parameters, click **OK** to save the settings.

----End

Deleting Automatic Packet Capture Files

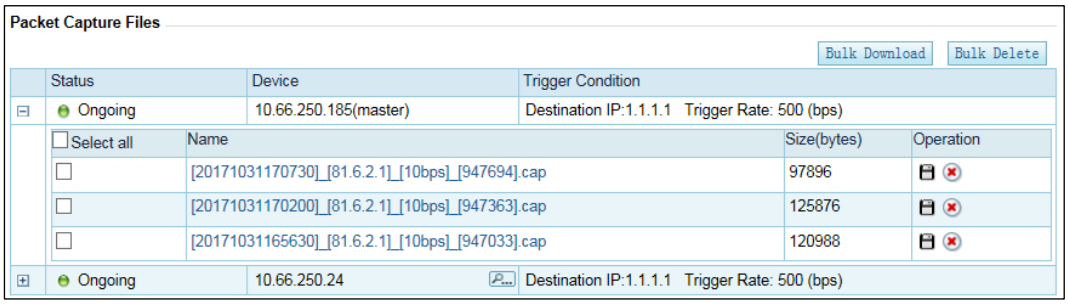
You can delete automatic packet capture files one by one or in batches.

Deleting Automatic Packet Capture Files One by One

To delete automatic packet capture files one by one, follow these steps:

Step 1 In the **Packet Capture Files** area shown in Figure 8-17, click to expand the automatic packet capture file list.

Figure 8-19 Packet capture files



Step 2 Click in the **Operation** column of a packet capture file and then click **OK** in the confirmation dialog box.

----End

Deleting Automatic Packet Capture Files in Batches

Step 3 In Figure 8-19, select the check boxes of one or more automatic packet capture files and then click **Bulk Delete**.

Step 4 Click **OK** in the confirmation dialog box.

----End

Viewing an Automatic Packet Capture File

In Figure 8-19, click the name of an automatic packet capture file to view its details.

Downloading an Automatic Packet Capture File

You can download automatic packet capture files one by one or in batches.

Downloading Automatic Packet Capture Files One by One

In Figure 8-19, click in the **Operation** column of an automatic packet capture file to download this file to a local disk drive.

Downloading Automatic Packet Capture Files in Batches

In Figure 8-19, select the check boxes of one or more automatic packet capture files and then click **Bulk Download** to download these files to a local disk drive.

8.2.4 Adding an ADS Device to the Cluster

To add an ADS device to the cluster, follow these steps:

Step 1 In Figure 8-7, click **Add Device** to add an ADS device to the cluster.

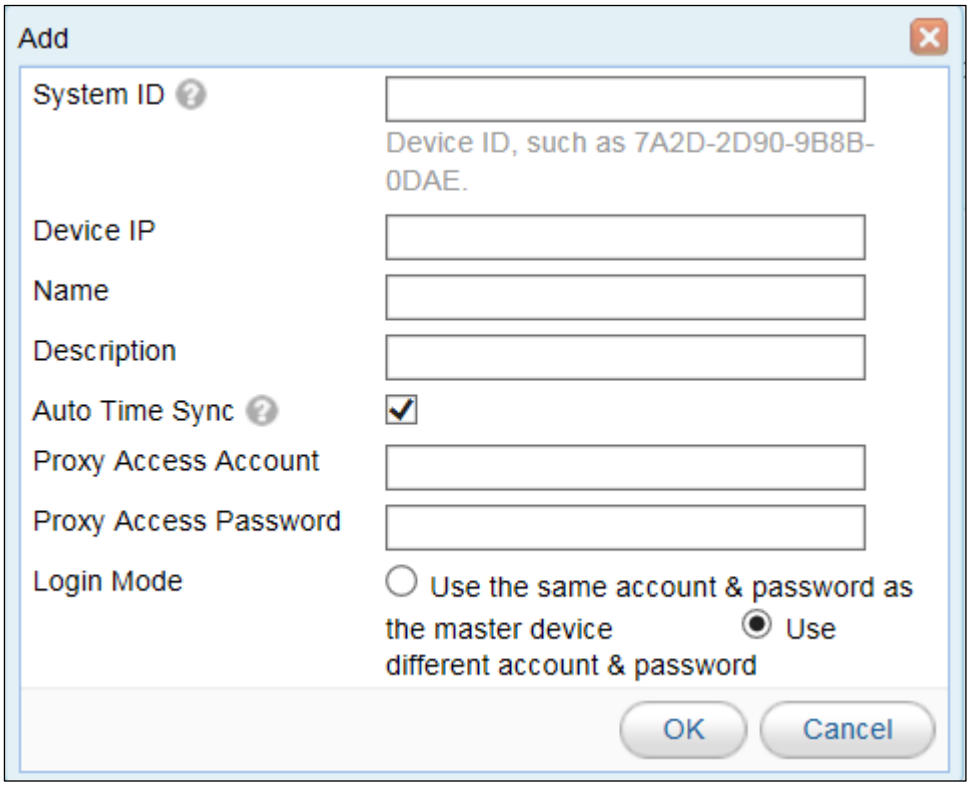
For description of parameters for adding an ADS device, see Table 8-1.

In addition to adding a device, you can perform the following operations on the cluster configuration page:

- Editing a device
- Deleting a device
- Synchronizing time
- Manually synchronizing configurations
- Saving the configuration

For details, see section 8.1 Managing ADS Devices.

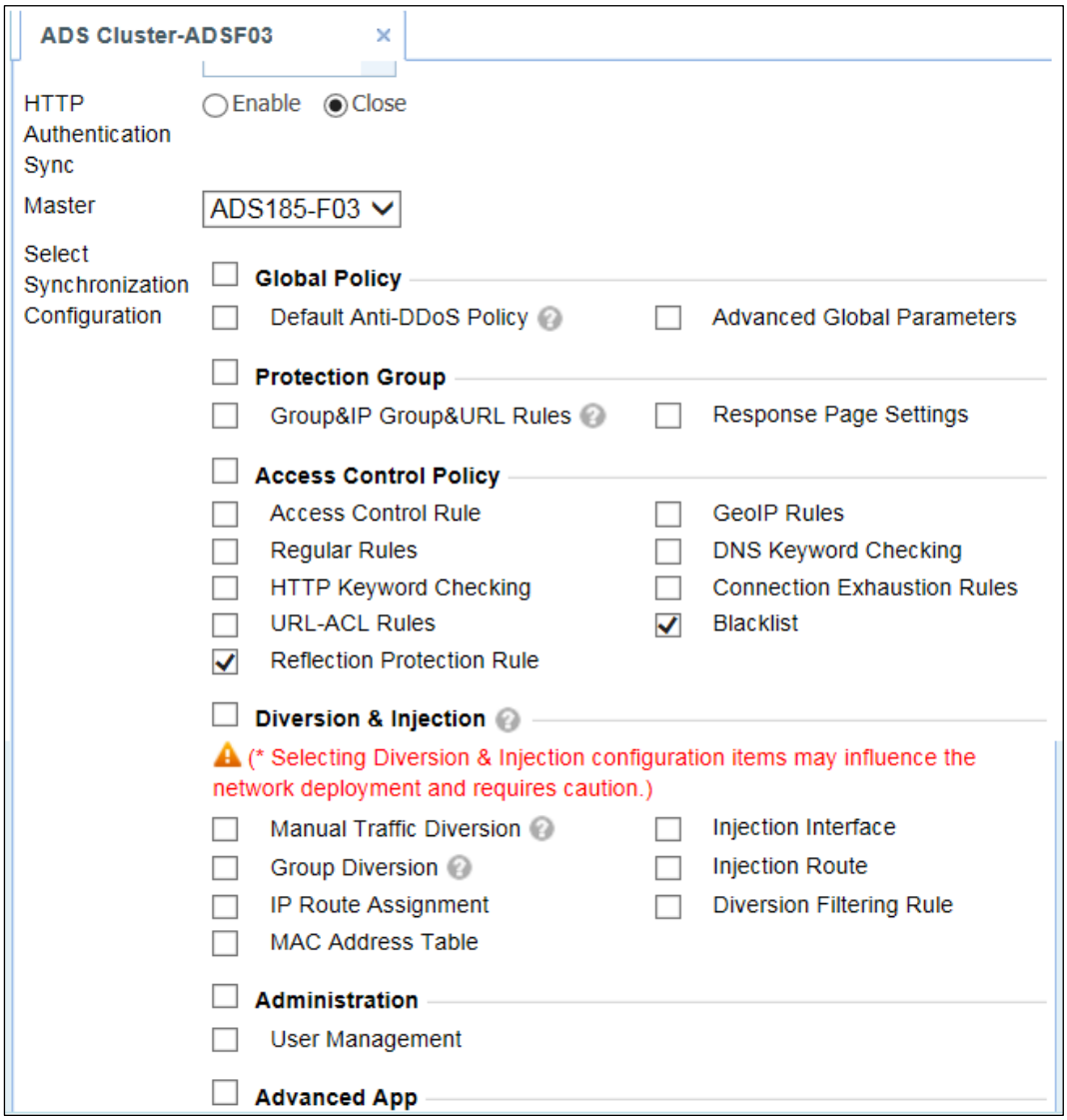
Figure 8-20 Adding an device to the cluster



8.2.5 Modifying a Cluster

In Figure 8-7, click an ADS cluster name on the left treelike device list and then click **Modify Cluster** on the ADS cluster configuration page to modify settings of this cluster. See Figure 8-21.

Figure 8-21 Modifying an ADS cluster



Note

- When a cluster includes one or more ADS devices, you can configure a master device and edit its settings. A cluster can have only one master device.
- ADS clusters without a master device are not displayed on the device list under **Region**. You cannot perform any operations on devices in such clusters.

8.2.6 Deleting a Cluster

In Figure 8-7, click an ADS cluster name on the left treelike device list and then click **Delete Cluster** on the ADS cluster configuration page to delete the cluster. As an ADS cluster is deleted, ADS devices in this cluster will not be deleted but automatically switch to the standalone mode.

Caution	• Once an ADS cluster is deleted, you cannot continue to view opened monitoring page, configuration page, or other pages that relate to this cluster. • In a cluster, the master device cannot be deleted except that the cluster has only one device.

8.2.7 Saving the Configuration

In Figure 8-7, select the check boxes of one or more devices and then click **Save** in the upper-right corner to save the configuration of the selected device(s).

Caution	Note the following when saving the configuration: • Time synchronization and configuration saving can be performed only on online ADS devices. • If you save the configuration, the configuration information remains valid after the ADS device is restarted; if you do not save the configuration, the ADS device is restored to the state before it is edited once the device is restarted.

8.3 Managing NTA Devices

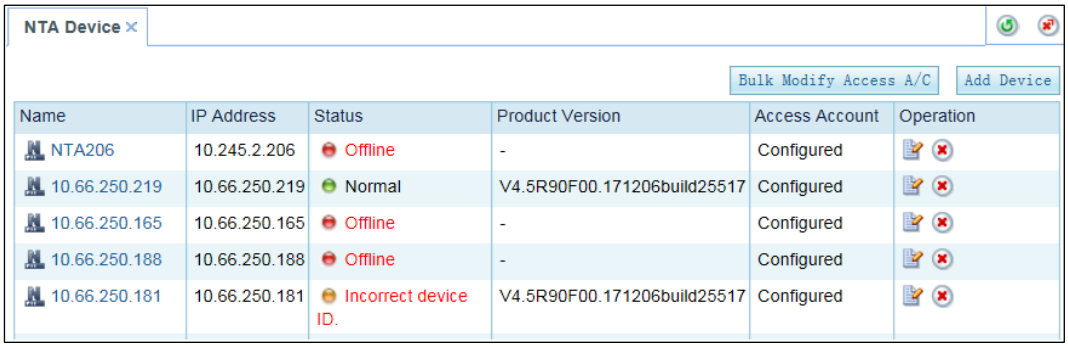
To configure an NTA device, follow these steps:

Step 1 Click **NTA Device** under **Device Management**.

The **NTA Device** page appears, as shown in Figure 8-22. Initially, the device list is empty and you need to add a device manually.

If the license of NTA is about to expire in less than seven days, the system displays a message indicating that the license will expire in X days. When the license validity period is displayed as 0 days, the system displays a message indicating that the license is invalid or expires.

Figure 8-22 NTA Device page



Step 2 Click a device to reconfigure its settings.

Prior to adding an NTA device, you need to log in to the web-based manager of this **device to** verify that this device is subordinate to ADS M (**Administration > Third-Party Interface > Management Mode**) and type the IP address of ADS M**.** For details, see *NSFOCUS NTA*

User Guide. After you complete the configuration and properly connect the two devices, this NTA device is subordinate to ADS M and appears in the tree structure of monitoring objects.

----End

8.3.1 Adding an NTA Device

To add an NTA device, follow these steps:

Step 1 Click **Add Device** in the upper-right corner of the **NTA Device** page.

A dialog box for adding an NTA device is displayed. See Figure 8-23.

Figure 8-23 Adding an NTA device

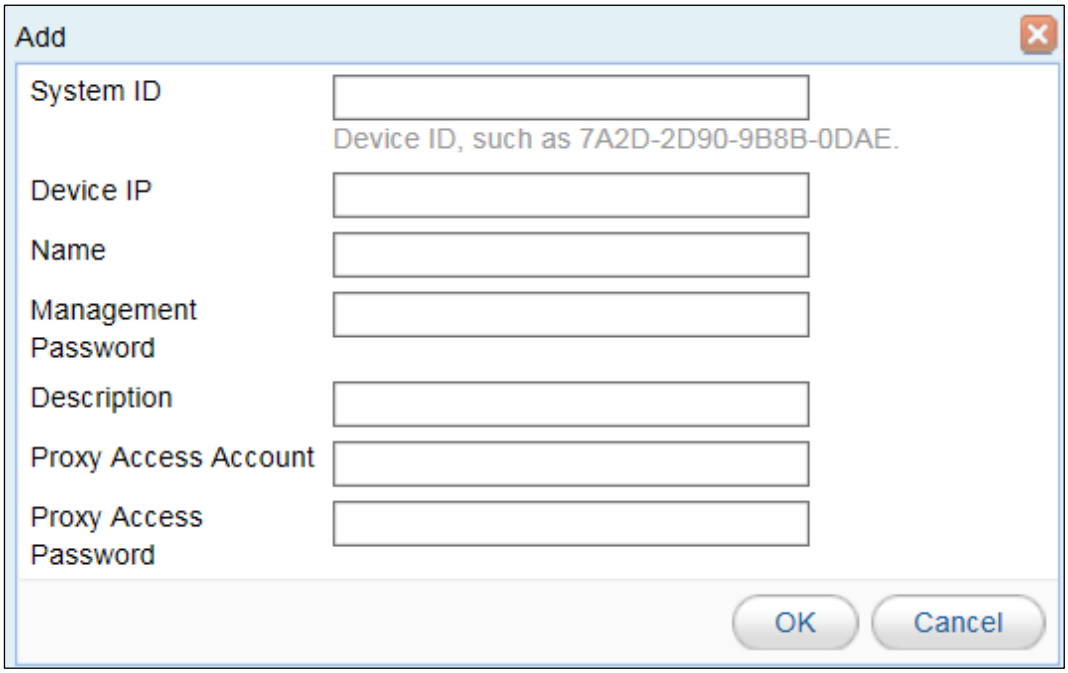


Table 8-5 describes parameters of an NTA device.

Table 8-5 NTA device parameters

Parameter	Description
System ID	Specifies the system ID of an NTA device. This parameter is mandatory.
Device IP	Specifies the IP address of an NTA device. Either an IPv4 or IPv6 address is acceptable. This parameter is mandatory.
Name	Specifies the name of an NTA device. The name should be 1 to 20 characters long and cannot contain angle brackets (<, or >), quotation marks (" or '), or slashes (/). A new name cannot duplicate that of an existing device. This parameter is mandatory.
Management Password	Specifies the management password of NTA V4.5R90F00. It must be the same as the authorization key configured on the web-based

Parameter	Description
	manager (**Administration > Third-Party Interface > Management Mode**) of NTA. NTA V4.5.61.2 does not require the management password.
Description	Specifies the brief description of an NTA device, for example, device usage.
Proxy Access Account	Specifies the account of the proxy NTA device. After the proxy access account and password are configured, ADS M can directly logs in to the corresponding NTA device.
Proxy Access Password	Specifies the password of the proxy NTA device. After the proxy access account and password are configured, ADS M can directly logs in to the corresponding NTA device.

Step 2 Set parameters in the dialog box and click **OK**.

----End

8.3.2 Modifying NTA Device Settings

On the **NTA Device** page, click in the row of an NTA device to modify the information about the device. Note that the device ID cannot be edited.

8.3.3 Deleting an NTA Device

On the **NTA Device** page, click in the row of an NTA device to delete the device. After an NTA device is deleted, it is no longer subject to management of ADS M, nor will it upload the information to ADS M.

Note	Once an NTA device is deleted, you cannot continue to view the opened monitoring page, configuration page, or other pages that relate to this device.

After adding an NTA device, you need to configure traffic diversion settings before the interaction between ADS and NTA devices. For details, see the *NSFOCUS NTA User Guide*.

8.3.4 Modifying Access Accounts in Batches

You can modify NTA access account passwords in batches in the same way as ADS access accounts. For details, see section 8.1.4 Modifying Access Accounts in Batches.

8.3.5 Configuring an NTA Device

After an NTA device is added, you can click its name to access its web-based manager for configuration. For how to configure an NTA device, see the *NSFOCUS NTA User Guide*.

9 Console-based System Management

9.1 Overview

Using console port connections, you can access the console management interface to perform operations such as restoration of initial configuration, status detection, and system restoration, which cannot be conducted on the web-based manager.

9.2 Login to the Console

For details about console login, refer to the *NSFOCUS ADS M Installation Guide*.

After login, if you remain inactive on the console within 20 minutes, the system logs you out of the console unconditionally. To continue your operation, you must log in again.

9.3 Console Configuration

After a successful login, the main menu is displayed, as shown in Figure 9-1. Type a sequence number as prompted and press **Enter** to open a menu.

If you log in to the console with the default password, the system reminds you to change the password. You are advised to change a new password. For how to change the password, see section 9.3.6 Changing the Console Password.

Figure 9-1 Main menu of the console

```
 Welcome to Nsfocus ADS M
=======================================
      s)  Display system status
      setup
        1)  Network
        2)  Datetime
        3)  Timezone
        4)  Locale
        5)  Console password(Initial password being used. Please change it immediately.)
        6)  Reset web admin password
        7)  Factory default
        8)  Recover database
        9)  Set web server port
      r)  Restart system services
      b)  Reboot
      h)  Shutdown
      x)  Logout
=======================================
Input your selection:
```

9.3.1 Checking System Status

On the main menu, type **s** and press **Enter** to view the system status. As shown in Figure 9-2, the displayed screen shows the hard disk mount status, system status, network status, and route status, from which you can determine the system operating condition.

Figure 9-2 Checking system status

```
================ Hard Disk ==================
Filesystem            Size  Used Avail Use% Mounted on
rootfs                754M  404M  312M  57% /
/dev/mapper/root      754M  404M  312M  57% /
tmpfs                1007M  516K 1007M   1% /var
tmpfs                1007M  276M  732M  28% /tmp
none                  4.0G     0  4.0G   0% /dev/shm
/dev/sda1              94M   12M   77M  14% /boot
/dev/sdb1             4.6G  285M  4.1G   7% /var/log
/dev/sdb5             4.6G  129M  4.3G   3% /usr/data/adsm
/dev/sdb6              19G  734M   17G   5% /usr/data/files
/dev/sdb7             9.2G 1013M  7.8G  12% /usr/data/pgsql/data
/dev/sdb8              19G  608M   17G   4% /usr/data/pgsql/tablespaces/snapspace
/dev/sdb9             156G  515M  148G   1% /usr/data/pgsql/tablespaces/floworigin
/dev/sdb10             37G  812M   35G   3% /usr/data/pgsql/tablespaces/attackorigin
/dev/sdb11             28G  134M   26G   1% /usr/data/pgsql/tablespaces/devorigin
/dev/sdb12             92G  129M   87G   1% /usr/data/probe
Press any key to continue...
```

9.3.2 Configuring Network Settings

On the main menu, type **1** and press **Enter** to access the network setting menu, as shown in Figure 9-3. On this menu, you can type **0** and press **Enter** to return to the main menu.

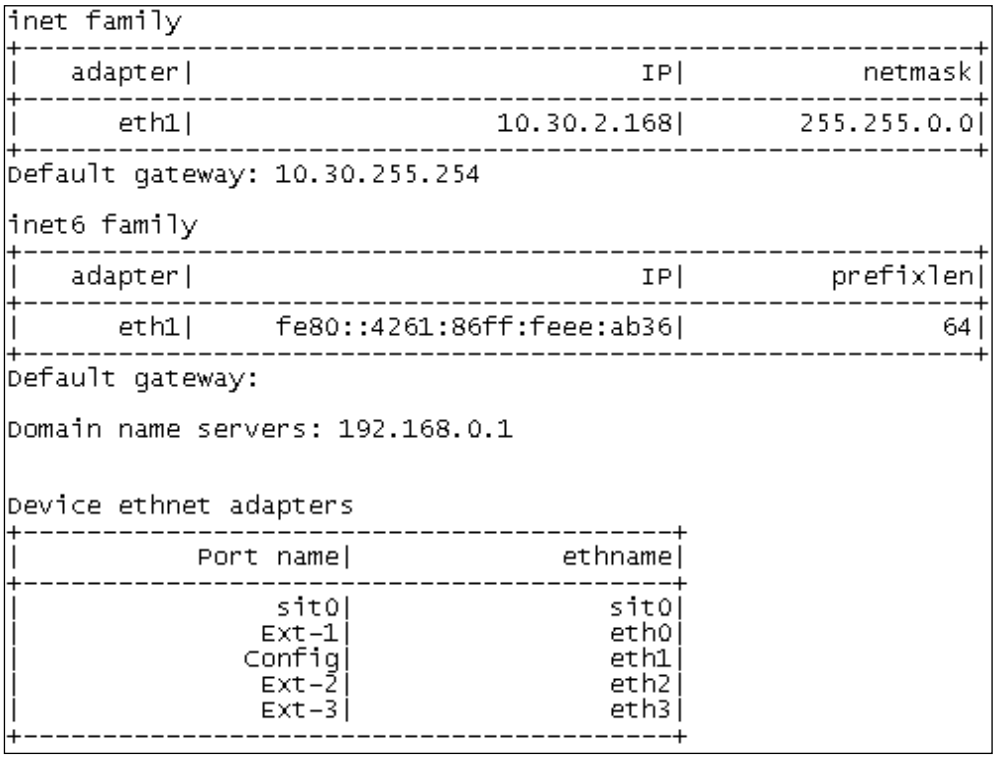
Figure 9-3 Network setting menu

```
Please select an operation:
  1) Display network settings
  2) Add an address
  3) Delete an address
  4) Setup default gateway
  5) Add a route
  6) Delete a route
  7) Setup domain name server
  8) Set to Default
  0) Escape
>
```

Viewing Network Settings

On the network setting menu, type **1** and press **Enter** to view network settings, as shown in Figure 9-4. The following screen displays network settings of the current system interface.

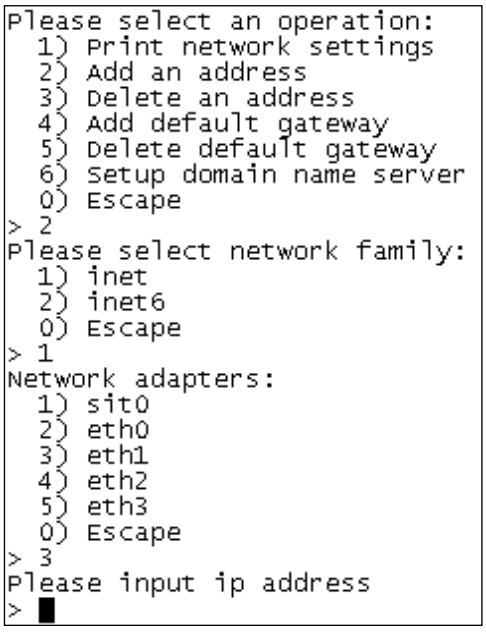
Figure 9-4 Viewing network settings



Adding an IP Address

On the network setting menu, type **2** and press **Enter** to configure an IP address of the system management interface. Type the IP address and subnet mask of the network interface, and press **Enter**. Then the system displays the settings and return to the network setting menu, as shown in Figure 9-5.

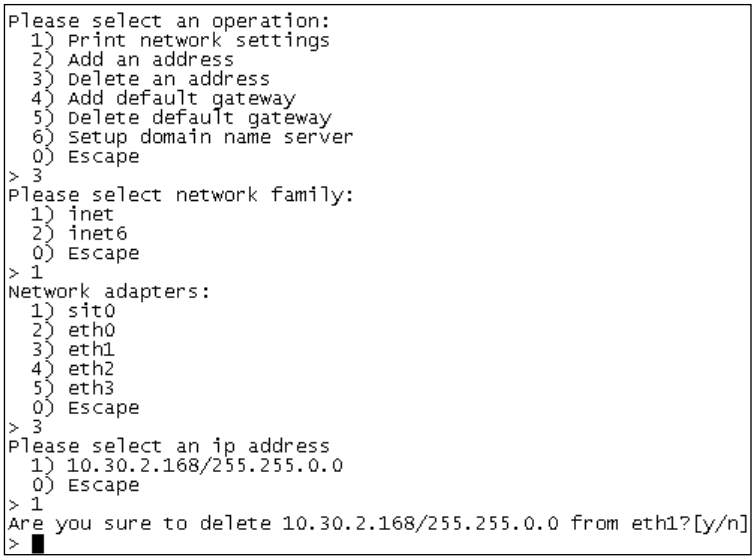
Figure 9-5 Adding an IP address



Deleting an IP Address

On the network setting menu, type **3** and press **Enter** to delete an IP address. Select the IP address to be deleted, type **y** and press **Enter** to delete it and return to the network setting menu, as shown in Figure 9-6.

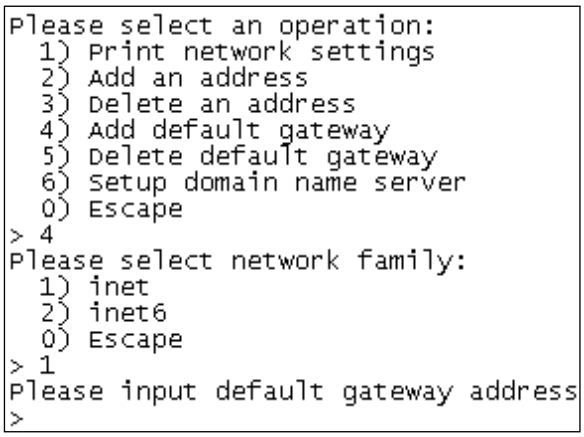
Figure 9-6 Deleting an IP address



Adding a Default Gateway

On the network setting menu, type **4** and press **Enter** to add a default gateway. Type the IP address of the gateway as prompted, and press **Enter**. Then the system displays the settings and return to the network setting menu, as shown in Figure 9-7.

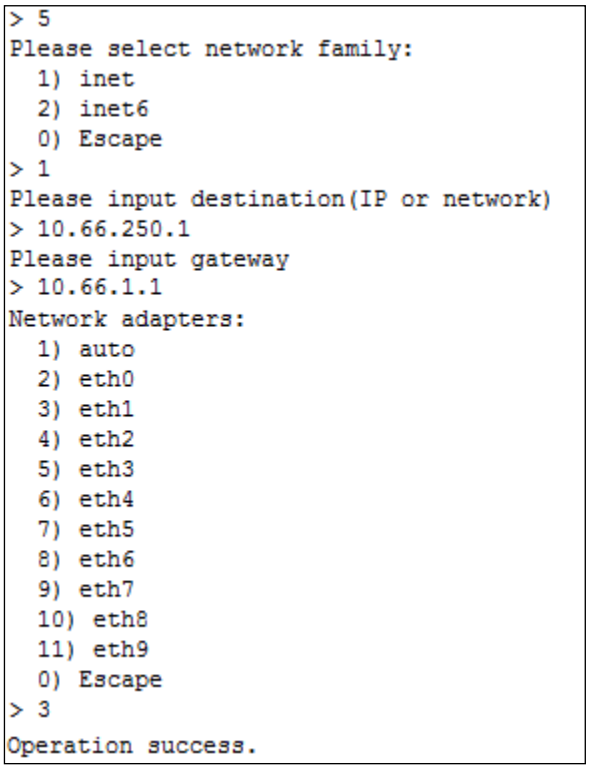
Figure 9-7 Adding a default gateway



Adding a Route

On the networking menu, type **5** and press **Enter** to add a route. Type the IP address and gateway address as prompted, select an interface, and press **Enter**. Then the system displays the configured route and returns to the networking menu, as shown in Figure 9-8.

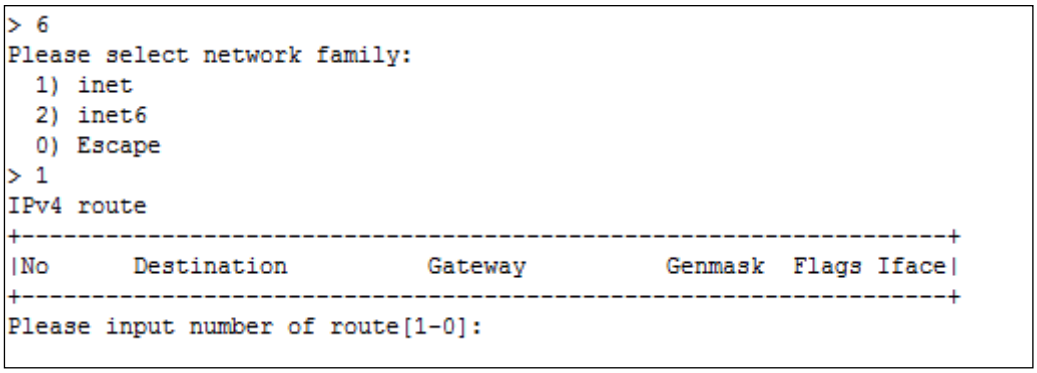
Figure 9-8 Adding a route



Deleting a Route

On the network setting menu, type **6** and press **Enter** to delete a route. Select a desired route, type **y** and press **Enter** to delete it and return to the network setting menu, as shown in Figure 9-9.

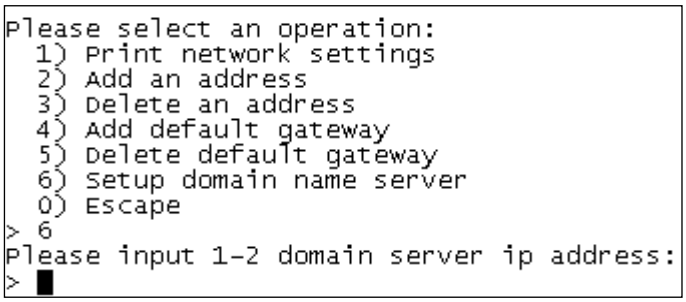
Figure 9-9 Deleting a route



Configuring a DNS Server

On the network setting menu, type **6** and press **Enter** to configure a DNS server. Type the IP address of the DNS as prompted, and press **Enter** to save the setting and return to the network setting menu, as shown in Figure 9-10.

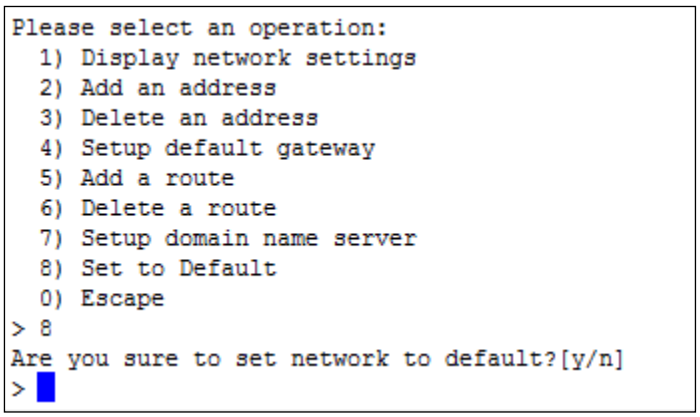
Figure 9-10 Configuring the DNS server



Restore Default Network Settings

On the network setting menu, type **8** and press **Enter** to enter the network restore menu. Type **y** and press **Enter**. Then the system will reset all network settings to factory settings and returns to the networking menu, as shown in Figure 9-11.

Figure 9-11 Restoring default network settings



9.3.3 Setting System Time

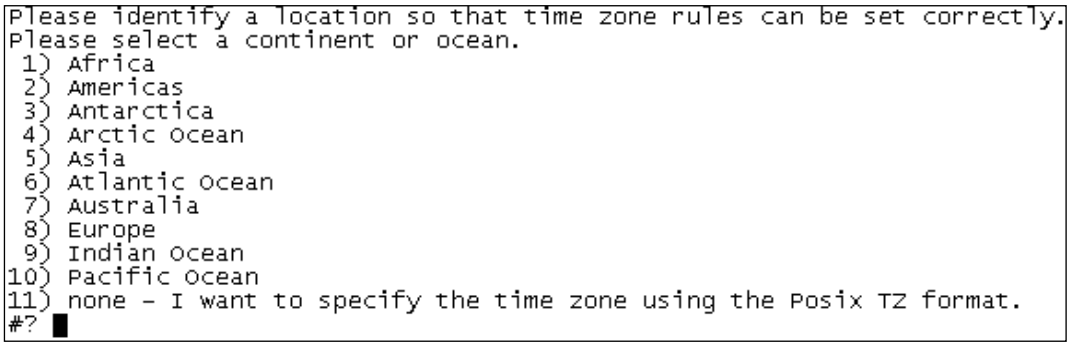
On the main menu, type **2** and press **Enter** to set the current system date and time, as shown in Figure 9-12. Type system date and time, such as 2012-03-19 15:18:55, and press **Enter** to save the settings. Then press any key to return to the main menu.

Figure 9-12 Console management – Setting system time

9.3.4 Setting the System Time Zone

On the main menu, type **3** and press **Enter** to set the system time zone, as shown in Figure 9-13. Select the time zone as prompted, and press **Enter** to save the setting. Then press any key to return to the main menu.

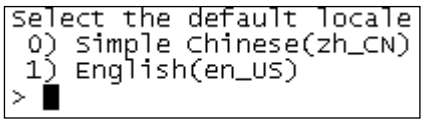
Figure 9-13 Console management – setting system time zone



9.3.5 Setting the System Language

On the main menu, type **4** and press **Enter** to set the language of the web-based manager, as shown in Figure 9-14. You can select Simplified Chinese or English, and press **Enter** to save the setting. Then press any key to return to the main menu.

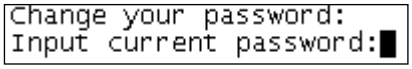
Figure 9-14 Console management – Setting system language



9.3.6 Changing the Console Password

On the main menu, type **5** and press **Enter** to change the console login password, as shown in Figure 9-15. First type the current password, then the new password, and press **Enter**. The new password must contain a minimum of 6 characters. The system will display a message notifying whether the password is changed.

Figure 9-15 Console management – changing console password

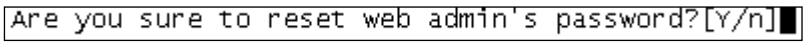


Note	As prompted, the console password must be at least six characters long. See appendix B Default Parameters for the initial account of the console.

9.3.7 Resetting the Web Administrator's Password

On the main menu, type **6** and press **Enter** to open the menu for resetting the password used by the administrator **admin** to log in to the web-based manager, as shown in Figure 9-16. First type **y** and press **Enter** to restore the initial password used by the administrator **admin** for login to the web-based manager. The system will display a message notifying whether the initial password is restored.

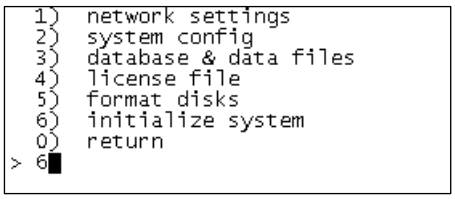
Figure 9-16 Console management – resetting the administrator's password



9.3.8 Restoring Factory Settings

On the main menu, type **7** and press **Enter** to restore factory settings, as shown in Figure 9-17 On this menu, you can type **0** and press **Enter** to return to the main menu.

Figure 9-17 Restoring factory settings



Restoring Network Settings

On the factory setting restoration menu, type **1** and press **Enter** to restore network settings. Type **y** and press **Enter** to restore initial network settings. This operation restores the IP address, subnet mask, and gateway address of a network interface to the initial state. System reboot is not required after restoration.

Restoring System Settings

On the factory setting restoration menu, type **2** and press **Enter** to conduct system restoration. Type **y** and press **Enter** to restore initial system settings, including the password. After restoration, the system is rebooted automatically.

Database Restoration

On the factory setting restoration menu, type **3** and press **Enter** to conduct database restoration. Type **y** and press **Enter** to clear the system database.

System log reports are cleared as you clear the database. Therefore, back up vital data before this operation.

Deleting the License

On the factory setting restoration menu, type **4** and press **Enter** to open the page of deleting the license. Type **y** and press **Enter** to delete the imported license.

Formatting the Hard Disk

On the factory setting restoration menu, type **5** and press **Enter** to open the page for formatting the hard disk. Type **y** and press **Enter** to format the hard disk. After the hard disk is formatted, all data is deleted.

Initializing the System

On the factory setting restoration menu, type **6** and press **Enter** to open the page for initializing the system. Type **y** and press **Enter** to initialize all the system settings.

9.3.9 Restoring the Database

On the main menu, type **8** and press **Enter** to restore the backup database to ADS M.

You can successfully restore the backup only after database backup is configured in the **Data Backup and Restore** area under **Administration > Local Settings > Data Storage**.

9.3.10 Setting the Web Service Port

On the main menu, type **9** and press **Enter** to set the port via which you can log in to ADS M. The port number can be **80**, **443**, or an integer ranging from 10000 to 65534. Assume that the IP address of ADS M is https://192.168.1.100. If the port number is changed to **80**, you need to type https://192.168.1.100:80 in the address bar of the browser.

9.3.11 Restarting System Services

On the main menu, type **r** and press **Enter** to restart system services.

9.3.12 Rebooting the System

On the main menu, type **b** and press **Enter** to reboot the system.

9.3.13 Shutting Down the System

On the main menu, type **h** and press **Enter** to shut down the system.

9.3.14 Exiting the System

On the main menu, type **x** and press **Enter** to log out of the console management interface.

A Parameters

A.1 Anti-DDoS Policy

- SYN Flood

  Threshold 1: 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.

  Threshold 2: The rate at which ADS sends reverse detection packets in response to SYN packets, after SYN flood protection is triggered. A greater value means a better protection effect and a higher load on ADS M.

  You are advised to set threshold 1 to 80% of the maximum traffic carried by the user server and threshold 2 to 15,000,000 pps.

- ACK Flood

  Threshold 1: 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. Under most application environments, you are advised use the default value.

- UDP Flood

  Threshold 1: 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. Under most application environments, you are advised use the default value.

- ICMP Flood

  Threshold 1: 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. Under most application environments, you are advised use the default value.

- Connection Exhaustion Prevention

  Currently, ADS M provides only the option of whether to enable connection exhaustion protection in the anti-DDoS policy. Further configurations need to be performed on the web-based manager of ADS.

A.2 UDP Policy Parameters

- Drop UDP Fragment

  Selecting **Drop UDP Fragment** indicates that ADS M drops received UDP fragments.

- Max UDP Packet Length

ADS M drops UDP packets with the length over the specified value. RFC specifies that the default maximum length of UDP packets is 65535.

- Bandwidth Coefficient of Source IP

  It limits the number of UDP packets transmitted from each source IP address per second.

A.3 Diversion Filtering Rules

- Allow Diversion by Default

  A checkmark in the **Allow Diversion by Default** checkbox indicates that the diversion filtering rule applied by ADS M to protected hosts allows diversion by default.

- IP Address/Netmask

  IP address/subnet mask of the diversion filtering rule.

- Allow Diversion

  A checkmark in the **Diversion** checkbox indicates that the traffic of the IP address/subnet mask can be diverted.

- Enable Diversion Filtering Rules

  Selecting the **Enable** checkbox indicates that the manual diversion policy takes effect on ADS M.

B Default Parameters

B.1 Default Parameters of the Communication Interface

For ADS NX3-M600A/M1600A:

Management Interface	1.1.1.1
Subnet Mask	255.255.255.0

For ADS NX3-M1600E:

Management Interface	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

B.2 Default Account of the Web Administrator

User Name	admin
Password	nsfocus

B.3 Default Account of the Console Administrator

User Name	admin
Password	nsfocus

B.4 Communication Parameters of the Console Port

Baud Rate	115200
Data Bits	8

B.5 Default Account of the Web Administrator

Baud Rate	115200
Data Bits	8