NSFOCUS NTA
User Guide

Version: V4.5R90F03 (2021-08-30)

Confidentiality: RESTRICTED

©2021 NSFOCUS

■ Copyright © 2021 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

1 Product Overview 4

1.1 Product Characteristics 4

1.2 Typical Deployment 5

1.2.1 Typical Deployment Mode for a Carrier's Network 5

1.2.2 Typical Deployment Mode for an Enterprise's Office Network 6

1.2.3 Typical Deployment Mode for a Campus Network 7

1.3 Configuration Process 8

2 Initial Configuration 10

2.1 Logging In to the Console 10

2.2 Configuring the IP Address of the Management Interface 15

2.3 Logging In to the Web-based Manager 16

2.4 Importing a License 19

3 Login Management 23

3.1 Web-based Manager 23

3.1.1 Users 23

3.1.2 Login 24

3.1.3 Forced Password Change 24

3.1.4 Page Layout 25

3.1.5 Common Buttons and Their Functions 26

3.2 Console User Interface 27

3.2.1 Console User 27

3.2.2 Login 27

3.3 SSH 28

4 Administration 29

4.1 System Configuration 29

4.1.1 Basic Configuration 30

4.1.2 Website Customization 35

4.1.3 SSL Certificate Import 36

4.1.4 Remote Assistance 36

4.2 Network Configuration 38

4.2.1 Configuring a Local Interface 38

4.2.2 Configuring a Route 41
4.2.3 Configuring a DNS Server 42
4.2.4 Configuring a Bond 43
4.3 Third-Party Interface 43
4.3.1 Email Service 44
4.3.2 SNMP Service 50
4.3.3 Syslog Service 55
4.3.4 SFTP Service 57
4.3.5 Cloud Platform 58
4.3.6 Third-Party Cloud Platform 59
4.3.7 Cloud Cleaning Platform 61
4.3.8 BSA Configuration 62
4.3.9 Management Mode 63
4.3.10 NTA-ATM 64
4.4 Diagnosis 65
4.4.1 Ping 66
4.4.2 Traceroute 66
4.4.3 Snmpwalk 67
4.4.4 Tcpdump 68
4.4.5 Telnet 71
4.4.6 Fault Diagnosis 71
4.5 Data Management 73
4.6 User Management 75
4.6.1 Managing User Accounts 75
4.6.2 Configuring Security Settings 77
4.6.3 Configuring Authentication 79
4.6.4 Configuring Whitelist for NTA Access via Web API 81
4.6.5 Managing the HTTP Host Whitelist 82
4.6.6 Managing the Current User by Using the Shortcut Button 83
4.7 Hot Standby 84
4.7.1 Getting to Know VRRP 84
4.7.2 Configuring Hot Standby 86
4.8 License 90
4.9 System Upgrade 92
4.9.1 Upgrading System Software 92
4.9.2 Upgrading Detection Rules 95
4.9.3 Upgrading Threat Intelligence 98
4.10 Alert Whitelist 100
4.11 Access Control 101
4.11.1 Enabling Access Control 102
4.11.2 Allowing Access from Specified IP Addresses 102
4.11.3 Denying Access from Specified IP Addresses 104

5 Configuration 106
5.1 Objects 106
5.1.1 Router 106
5.1.2 Router Interface Group 119
5.1.3 Region 122
5.2 Alert Templates 155
5.2.1 Router Alert Template 156
5.2.2 Region Alert Template 158
5.2.3 IP Group Alert Template 164
5.3 Global Alert Settings 169
5.3.1 Default DDoS Attack Detection Thresholds 170
5.3.2 Alert Parameters 171
5.3.3 Alert Plug-in Management 172
5.3.4 Auto-learning Baseline Parameters 177
5.3.5 Traffic Statistics 179
5.4 Global Diversion Settings 179
5.4.1 Default Diversion Configuration 180
5.4.2 BGP Configuration 182
5.4.3 Protection Device Configuration 188
5.4.4 BGP FlowSpec Configuration 189
5.5 Flow Data Collection and Forwarding 195
5.6 Detection of Bogus Source IP Addresses 197
5.7 NTI 198
5.8 Data Dictionary 200
5.8.1 Application Ports 201
5.8.2 Autonomous Systems 202
5.9 Bulk Configuration 204
5.9.1 Bulk Configuring Regions 204
5.9.2 Bulk Configuring IP Groups 206
5.9.3 Bulk Configuring Auto-Learning 207
6 Log Management 209
6.1 Log Query 209
6.2 Log Parameters 210
6.2.1 Diversion Log 211
6.2.2 Audit Log 212
6.2.3 Running Log 212
6.2.4 FlowSpec Diversion Log 213
7 Report Management 215
7.1 Overview 215
7.2 Traffic Report 216
7.3 DDoS Attack Report 221

7.4 Bogus Source IP Report 225
7.5 Traffic Comparison Report 227
7.6 Email Sending Configuration 229
8 Alert Management 231
8.1 Overview 231
8.1.1 Viewing Overall Alert Statistics 231
8.1.2 Viewing Information About Specified Alerts 234
8.2 Alert Query 241
9 Monitoring 245
9.1 View Management 245
9.1.1 Adding a View 246
9.1.2 Editing a View 247
9.1.3 Switching to a Desired View 251
9.1.4 Setting a View as Default 251
9.2 Overall Monitoring Statistics 251
9.3 Regions 254
9.3.1 Viewing Alert and Traffic Statistics of All Regions 254
9.3.2 Viewing Monitoring Information of a Specific Region 254
9.4 Routers 257
9.4.1 Viewing Overall Statistics of Routers 257
9.4.2 Viewing Monitoring Information of Interfaces on a Specific Router 262
9.5 Router Interface Groups 266
9.6 IP Addresses 268
9.7 Diversion Routing Table 270
9.7.1 IP Diversion 270
9.7.2 FlowSpec Diversion 273
9.7.3 Group Diversion 274
9.7.4 Manual Traffic Diversion 277
9.7.5 FlowSpec Manual Traffic Diversion 279
9.8 Traffic Auto-learning 282
9.9 Local Status 285
10 Console-based Management 290
10.1 Configuring the Network 291
10.1.1 Viewing Network Settings 292
10.1.2 Adding an Interface IP Address 292
10.1.3 Configuring a Route 294
10.1.4 Configuring DNS Servers 295
10.2 Viewing or Configuring System Time 295
10.3 Controlling System Engines 296
10.4 Configuring the ACL 296
10.5 Resetting the Console Password 296

10.6 Viewing System Configurations 297
10.7 Controlling the Web Service 297
10.8 Performing System Management 297
10.8.1 Configuring One-Click Fault Collection 298
10.8.2 Restoring Factory Settings 299
10.9 Enabling/Disabling PPPoE Interfaces 299
10.10 Restarting the Device 300
10.11 Powering Off the Device 300
10.12 Exiting the Privileged Mode 301
10.13 Exiting the Console 301
10.14 Viewing the Help Information of the Console 302
10.15 Enabling/Disabling Cloud-based Authentication 302
10.16 Viewing System Logs 303
10.17 Viewing Resources Consumed by Processes 303
A Abbreviations 304
B Default Parameters 305
B.1 Default Network Settings 305
B.1.1 Default Settings of Local Interfaces 305
B.1.2 Default Route Settings 305
B.2 Default Administrator Accounts 305
B.2.1 Web Operator 305
B.2.2 Web Auditor 305
B.2.3 Console Administrator 306
B.2.4 SSH Administrator 306
B.3 Communication Parameters of the Console Port 306
B.4 Flow Collecting and Forwarding 306
C IPv4/IPv6 Support 307

Figures

Figure 1-1 Typical deployment on a carrier's network 6
Figure 1-2 Typical deployment on an enterprise's office network 7
Figure 1-3 Typical deployment on a campus network 8
Figure 1-4 NTA configuration flow chart 9
Figure 2-1 Configuring a quick connection 11
Figure 2-2 Login window 12
Figure 2-3 Changing the login password 12
Figure 2-4 Commands available in unprivileged mode 12
Figure 2-5 Accessing the privileged mode 13
Figure 2-6 Commands available in privileged mode 13
Figure 2-7 Configuring the IP address of the management interface 15
Figure 2-8 Configuring the network gateway of the management interface 16
Figure 2-9 Security alert 17
Figure 2-10 Login page 17
Figure 2-11 Setting the system language 18
Figure 2-12 Setting the country/region and time zone 18
Figure 2-13 Changing the initial password 19
Figure 2-14 License page 20
Figure 2-15 License preview 21
Figure 2-16 Importing the license successfully 21
Figure 3-1 Changing the password 25
Figure 3-2 Page layout 25
Figure 4-1 Basic Information area 30
Figure 4-2 Exporting configuration files 31
Figure 4-3 Importing a configuration file 32
Figure 4-4 Configurations that can be imported 33
Figure 4-5 Remote Management area 34

Figure 4-6 System Engine area 35
Figure 4-7 Website Customization page 36
Figure 4-8 SSL Certificate Import page 36
Figure 4-9 Remote assistance 37
Figure 4-10 Configuring remote assistance 37
Figure 4-11 Configuring remote assistance 38
Figure 4-12 Local Interface page 39
Figure 4-13 Interface attributes 39
Figure 4-14 Adding an IPv4 address 40
Figure 4-15 Adding an IPv6 address 40
Figure 4-16 Route page 41
Figure 4-17 Adding a static route 41
Figure 4-18 DNS Server page 42
Figure 4-19 Creating a bond 43
Figure 4-20 Creating a bond 43
Figure 4-21 Mail Configuration page 45
Figure 4-22 Log sending configuration area 45
Figure 4-23 Email Template page 47
Figure 4-24 Modified email template 48
Figure 4-25 SMTP Server page 49
Figure 4-26 Configuring an SMTP server 49
Figure 4-27 Send Test Mail dialog box 50
Figure 4-28 Configuring the SNMP v1/v2c service 51
Figure 4-29 Configuring the SNMPv3 service 52
Figure 4-30 Configuring account-based authentication parameters 52
Figure 4-31 Configuring private key-based authentication parameters 53
Figure 4-32 Network Management Station area 54
Figure 4-33 Configuring a trusted NMS 55
Figure 4-34 Syslog Service page 56
Figure 4-35 Configuring a syslog server 56
Figure 4-36 SFTP Service Configuration page 57
Figure 4-37 Cloud Platform page 58
Figure 4-38 Third-party cloud platform page 59

Figure 4-39 Adding a third-party cloud platform 60
Figure 4-40 Cloud Cleaning Platform page 61
Figure 4-41 Adding a cloud cleaning platform 61
Figure 4-42 BSA Configuration page 62
Figure 4-43 ADS M list 63
Figure 4-44 Configuring the management mode 63
Figure 4-45 Page for configuring real-time synchronization with NTA-ATM 64
Figure 4-46 Page for configuring scheduled synchronization with NTA-ATM 65
Figure 4-47 ping page 66
Figure 4-48 traceroute page 67
Figure 4-49 snmpwalk page 68
Figure 4-50 tcpdump page 68
Figure 4-51 Selection of pattern 1 69
Figure 4-52 Selection of pattern 2 70
Figure 4-53 Telnet page 71
Figure 4-54 Fault diagnosis page 72
Figure 4-55 Fault collection progress 72
Figure 4-56 Message prompting the completion of fault collection 72
Figure 4-57 Saving the fault diagnosis file 73
Figure 4-58 Refreshed list of fault diagnosis files 73
Figure 4-59 Data Partition Usage page 74
Figure 4-60 Viewing details about the partition usage 74
Figure 4-61 Displaying only used space of data partitions 75
Figure 4-62 Account Configuration page 76
Figure 4-63 Creating a system administrator account 76
Figure 4-64 Security Configuration page 78
Figure 4-65 Local authentication configuration page 80
Figure 4-66 Radius authentication configuration page 80
Figure 4-67 Web API Whitelist page 81
Figure 4-68 Enabling the HTTP host whitelist 82
Figure 4-69 Adding an entry to the HTTP host whitelist 83
Figure 4-70 Editing personal information 84
Figure 4-71 VRRP networking diagram 85

Figure 4-72 Hot Standby page 87
Figure 4-73 Configuring hot standby parameters 88
Figure 4-74 Configuring VRRP backup groups 89
Figure 4-75 License information 90
Figure 4-76 System Upgrade page 93
Figure 4-77 System Upgrade page after an upgrade file is selected 93
Figure 4-78 Upgrade confirmation dialog box 94
Figure 4-79 Upgrade notes 95
Figure 4-80 Detection Rule Upgrade page 96
Figure 4-81 Local Upgrade area after an upgrade file is selected 96
Figure 4-82 Upgrade confirmation 96
Figure 4-83 Auto Sync area 97
Figure 4-84 Threat Intelligence Upgrade area 98
Figure 4-85 Local Upgrade area after an upgrade file is selected 98
Figure 4-86 Upgrade confirmation 99
Figure 4-87 Auto Sync area 100
Figure 4-88 Alert Whitelist page 101
Figure 4-89 Alert whitelist enabled 101
Figure 4-90 Access Control page 102
Figure 4-91 Enabling access control 102
Figure 4-92 Disabling external access 102
Figure 4-93 Local IP address added to the whitelist 103
Figure 4-94 Specifying IP addresses that should be allowed to access NTA 103
Figure 4-95 IP addresses allowed access to NTA 104
Figure 4-96 Specifying IP addresses that should be denied access to NTA 104
Figure 5-1 Routers page 107
Figure 5-2 Query of routers 108
Figure 5-3 Basic information configuration 109
Figure 5-4 Flow configuration 109
Figure 5-5 SNMP configuration 111
Figure 5-6 Router alert configuration 113
Figure 5-7 Traffic statistics configuration 114
Figure 5-8 Router settings 115

Figure 5-9 Interface List page 116
Figure 5-10 Router interface topology 118
Figure 5-11 Configuring the interface type 118
Figure 5-12 Setting interface query conditions 119
Figure 5-13 Query result 119
Figure 5-14 Router Interface Groups page 120
Figure 5-15 Adding an interface group 120
Figure 5-16 List of interfaces to be included in the group 121
Figure 5-17 Interfaces included in the group 121
Figure 5-18 Region list 123
Figure 5-19 Adding a region 124
Figure 5-20 Region settings 125
Figure 5-21 Configuring basic information 126
Figure 5-22 Area for specifying IP address ranges 127
Figure 5-23 Area for specifying router interfaces 128
Figure 5-24 Selecting router interfaces 128
Figure 5-25 Viewing router interfaces included in a region 129
Figure 5-26 Configuring region traffic alert policies 130
Figure 5-27 Configuring DDoS attack detection policies 133
Figure 5-28 Configuring traffic statistics parameters 135
Figure 5-29 Configuring traffic diversion rules 136
Figure 5-30 Changing the number of traffic-diverted IP addresses 137
Figure 5-31 Adding a region-specific diversion policy 137
Figure 5-32 Adding an IP address-specific diversion policy 139
Figure 5-33 Traffic diversion policies sorted in descending order of priority 141
Figure 5-34 Region list 142
Figure 5-35 Basic Information page for adding an IP group 143
Figure 5-36 Range page for adding an IP group 144
Figure 5-37 Traffic alert policies of the added IP group 145
Figure 5-38 IP Group DDoS Attack Alert configuration page 146
Figure 5-39 Traffic statistics configuration page 147
Figure 5-40 Traffic Diversion Rule configuration page 148
Figure 5-41 IP groups included in a region 148

Figure 5-42 Settings of an IP group 149
Figure 5-43 IP groups included in a region 150
Figure 5-44 Edit IP Group Auto-learning Baseline page 151
Figure 5-45 Configuring traffic auto-learning 152
Figure 5-46 Auto-learning in progress 153
Figure 5-47 Method of handling learning results 153
Figure 5-48 Baseline data obtained through auto-learning 154
Figure 5-49 Operations that can be performed on the learning result 154
Figure 5-50 Edit Threshold page 155
Figure 5-51 Router Alert Template page 156
Figure 5-52 Adding a router alert template 157
Figure 5-53 Region Alert Template page 158
Figure 5-54 Basic information configuration page 158
Figure 5-55 Configuring region traffic alert policies 159
Figure 5-56 Configuring region DDoS attack alert parameters 160
Figure 5-57 Configuring traffic statistics parameters for the region 161
Figure 5-58 Configuring region traffic diversion rules 161
Figure 5-59 Edit Region Template page 162
Figure 5-60 Region alert template settings displayed on one page 163
Figure 5-61 Specifying regions to be covered by the edited template 164
Figure 5-62 IP Group Alert Template page 165
Figure 5-63 Configuring an alert template for an IP group 165
Figure 5-64 Configuring IP group traffic alert policies 166
Figure 5-65 Configuring DDoS attack alerts for an IP group 167
Figure 5-66 Configuring traffic statistics parameters for an IP group 168
Figure 5-67 Configuring traffic diversion rules for an IP group 168
Figure 5-68 Specifying IP groups to be covered by the edited template 169
Figure 5-69 Default DDoS Attack Alert Threshold page 170
Figure 5-70 Alert Parameters page 171
Figure 5-71 Alert Plug-in Management page 173
Figure 5-72 Adding an alert type 173
Figure 5-73 Custom Attack Alerts list 174
Figure 5-74 Add Feature page 175

Figure 5-75 Viewing fields of an attack alert plug-in 176
Figure 5-76 Configuring UDP reflection alert detection 176
Figure 5-77 Auto-learning Baseline Parameters page 177
Figure 5-78 Changing the direct alert threshold growth rate 177
Figure 5-79 Adding a traffic auto-learning policy 178
Figure 5-80 Changing the time granularity 178
Figure 5-81 Traffic Statistics page 179
Figure 5-82 Default Diversion Configuration page 180
Figure 5-83 Adding an IP address-specific diversion policy 181
Figure 5-84 Traffic diversion policies sorted in descending order of priority 181
Figure 5-85 BGP Configuration page 182
Figure 5-86 Add BGP Session page 183
Figure 5-87 Message indicating that the BGP entry is in use 185
Figure 5-88 Confirmation dialog box for deleting a BGP entry 185
Figure 5-89 Referencing of a BGP session 186
Figure 5-90 Routing entries 186
Figure 5-91 Query of the BGP neighbor status 187
Figure 5-92 BGP neighbor status query result 187
Figure 5-93 List of protection devices 188
Figure 5-94 Adding a protection device 188
Figure 5-95 Objects that have used the device 189
Figure 5-96 FlowSpec BGP page 190
Figure 5-97 Adding a BGP FlowSpec entry 190
Figure 5-98 Message indicating that the current BGP FlowSpec entry is in use 192
Figure 5-99 Confirmation dialog box for deleting a BGP FlowSpec entry 192
Figure 5-100 Referencing of a BGP FlowSpec entry 193
Figure 5-101 Viewing routing entries 194
Figure 5-102 BGP FlowSpec neighbor displayed 194
Figure 5-103 Neighbor status query result 195
Figure 5-104 Flow Settings page 196
Figure 5-105 Bogus source IP address detection rules 197
Figure 5-106 Creating a bogus source IP address detection rule 198
Figure 5-107 Threat Intelligence page 199

Figure 5-108 Threat intelligence query result 200
Figure 5-109 Application Port page 201
Figure 5-110 Adding an application 202
Figure 5-111 AS page 203
Figure 5-112 Adding an AS 203
Figure 6-1 Diversion Log page 209
Figure 6-2 Search result 210
Figure 7-1 Traffic Report page 216
Figure 7-2 Traffic report 218
Figure 7-3 Detailed statistical data in a traffic report 219
Figure 7-4 Exporting a report 220
Figure 7-5 DDoS Attack Report page 221
Figure 7-6 DDoS attack report 223
Figure 7-7 Detailed statistical data in a DDoS report 224
Figure 7-8 Exporting a report 225
Figure 7-9 Search area of bogus source IP reports 226
Figure 7-10 Bogus source IP report 227
Figure 7-11 Search area of traffic comparison reports 228
Figure 7-12 Report for comparing traffic data of the same router 229
Figure 7-13 Email sending configuration 230
Figure 7-14 Creating an email sending rule 230
Figure 8-1 Overview of alerts 232
Figure 8-2 Viewing detailed alert information 232
Figure 8-3 Page displaying details about an alert 235
Figure 8-4 Information about the diversion triggered by the alert 236
Figure 8-5 Configuring manual diversion 236
Figure 8-6 Prompt message 237
Figure 8-7 Viewing traffic details 237
Figure 8-8 Traffic details 238
Figure 8-9 Viewing alert details 238
Figure 8-10 Viewing details about a source IP address 239
Figure 8-11 Exporting a report 239
Figure 8-12 Top 5 source IP addresses of DDoS attack alerts 240

Figure 8-13 Searching for alerts 241
Figure 8-14 Alert search result 243
Figure 8-15 Exporting the alert list 244
Figure 9-1 Monitoring overview 246
Figure 9-2 Adding a view 246
Figure 9-3 New view named alert 247
Figure 9-4 Editing the view name 248
Figure 9-5 View with the new name 248
Figure 9-6 Confirmation dialog box for deleting a pane 249
Figure 9-7 Adding a pane 249
Figure 9-8 Editing pane properties 250
Figure 9-9 Modified pane 250
Figure 9-10 Confirmation dialog box for deleting a view 251
Figure 9-11 Overall monitoring statistics 252
Figure 9-12 Alert and traffic statistics of regions 254
Figure 9-13 Detailed monitoring information of a region 255
Figure 9-14 Router monitoring 257
Figure 9-15 Top routers with the heaviest traffic 258
Figure 9-16 Statistics of all routers under monitoring 258
Figure 9-17 Searching for a specific router 259
Figure 9-18 Detailed monitoring information of a router 260
Figure 9-19 Switching to the monitoring page of another router 262
Figure 9-20 Monitoring statistics of routers 262
Figure 9-21 Page showing interface monitoring information 263
Figure 9-22 Monitoring information of a specific interface 264
Figure 9-23 Monitoring information of router interface groups 266
Figure 9-24 Detailed monitoring information of a specific router interface group 267
Figure 9-25 Switching to the monitoring page of another router interface group 268
Figure 9-26 IP traffic query 269
Figure 9-27 Monitoring information of the specified IP address 269
Figure 9-28 IP diversion routes 271
Figure 9-29 Conditions for searching for IP diversion routes 272
Figure 9-30 FlowSpec Diversion page 273

Figure 9-31 Group diversion routes 275
Figure 9-32 Query result of group diversion routes 276
Figure 9-33 Manual diversion routes 277
Figure 9-34 Adding a manual diversion route 277
Figure 9-35 FlowSpec Manual Traffic Diversion page 279
Figure 9-36 Adding a FlowSpec manual diversion route 280
Figure 9-37 Monitoring of traffic auto-learning results 282
Figure 9-38 Viewing auto-learning results of all IP groups 283
Figure 9-39 Viewing auto-learning results of IP groups in a specific learning state 283
Figure 9-40 Checking search results 284
Figure 9-41 Viewing DDoS attack alerts of an IP group 284
Figure 9-42 Editing auto-learning baseline settings of an IP group 285
Figure 9-43 Machine Status page 286
Figure 9-44 Left chart in the System Status area 287
Figure 9-45 Local interface status 288
Figure 9-46 More system information 289
Figure 10-1 Network configuration menu 291
Figure 10-2 Existing network settings 292
Figure 10-3 Configuring an IPv4 address of an interface 293
Figure 10-4 Deleting an interface IP address 294
Figure 10-5 Configuring a default IPv4 route in privileged mode 294
Figure 10-6 Configuring a default IPv6 route in privileged mode 295
Figure 10-7 Configuring DNS servers in privileged mode 295
Figure 10-8 Configuring system time 296
Figure 10-9 Controlling system engines 296
Figure 10-10 Configuring the ACL 296
Figure 10-11 Resetting the login password of the console user interface 297
Figure 10-12 Viewing system configuration 297
Figure 10-13 Controlling the web service 297
Figure 10-14 Performing system management 297
Figure 10-15 Configuring one-click fault collection 298
Figure 10-16 Restoring factory settings 299
Figure 10-18 Restarting the system. 300

Figure 10-19 Powering off the device 301
Figure 10-20 Exiting the privileged mode 301
Figure 10-21 Exiting the console user interface 302
Figure 10-22 Viewing the help information of the console 302
Figure 10-23 Enabling/disabling cloud-based authentication 303
Figure 10-24 Viewing system logs 303
Figure 10-25 Viewing NTA resources consumed by processes 303

Tables

Table 2-1 Commands available in unprivileged mode 13
Table 2-2 Commands available in privileged mode 13
Table 2-3 Meanings of keys 14
Table 3-1 Permissions of different roles 24
Table 3-2 Page layout 26
Table 3-3 Common buttons and their functions 26
Table 4-1 Parameters for configuring basic information 30
Table 4-2 Interface attributes 39
Table 4-3 Parameters for configuring a static route 42
Table 4-4 Log sending parameters 46
Table 4-5 Parameters for configuring an SMTP server 49
Table 4-6 SNMPv3 service configuration parameters 53
Table 4-7 Parameters for configuring a trusted NMS 55
Table 4-8 Parameters for configuring a syslog server 57
Table 4-9 Parameters for configuring the SFTP service 58
Table 4-10 Parameters for configuring a cloud platform 58
Table 4-11 Parameters for configuring a third-party cloud platform 60
Table 4-12 Parameters for configuring a cloud cleaning platform 61
Table 4-13 BSA configuration parameter 62
Table 4-14 Parameters for configuring ADS M 64
Table 4-15 Paramters for configuring real-time synchronization with NTA-ATM 64
Table 4-16 Parameters for packet capture pattern 1 69
Table 4-17 Parameters for packet capture pattern 2 70
Table 4-18 Parameters for configuring an account 76
Table 4-19 Login parameters 78
Table 4-20 Radius authentication parameters 80
Table 4-21 Parameters on the License page 91

Table 4-22 Automatic synchronization parameters 97
Table 4-23 Automatic synchronization parameters 100
Table 5-1 Parameters in the router list 108
Table 5-2 Parameters for configuring basic information of a router 109
Table 5-3 Flow configuration parameters 110
Table 5-4 SNMP configuration parameters 111
Table 5-5 Router alert parameters 113
Table 5-6 Parameters in the interface list 116
Table 5-7 Parameters in the region list 123
Table 5-8 Parameters for configuring basic information of a region 126
Table 5-9 Parameters for configuring traffic alert policies 130
Table 5-10 DDoS attack alert parameters 133
Table 5-11 Parameters for configuring a region-specific diversion policy 138
Table 5-12 Parameters for configuring an IP address-specific diversion policy 139
Table 5-13 Parameters for configuring basic information of an IP group 143
Table 5-14 Parameters for configuring traffic auto-learning 152
Table 5-15 Parameters for configuring a router alert template 157
Table 5-16 Global alert parameters 171
Table 5-17 BGP configuration parameters 183
Table 5-18 BGP FlowSpec configuration parameters 190
Table 5-19 Parameters of flow settings 196
Table 5-20 Parameters for configuring a bogus source IP address detection rule 198
Table 5-21 Parameters for configuring NTA to collaborate with NTI 199
Table 5-22 Parameters for adding an AS 204
Table 6-1 Parameters of the diversion log 211
Table 6-2 Parameters of the audit log 212
Table 6-3 Parameters of the running log 212
Table 6-4 Parameters of the FlowSpec diversion log 213
Table 7-1 Conditions for querying traffic reports 216
Table 7-2 Parameters for exporting traffic reports 220
Table 7-3 Conditions for querying DDoS attack reports 221
Table 7-4 Parameters for querying a bogus source IP report 226
Table 7-5 Parameters for querying a traffic comparison report 228

Table 8-1 Parameters in the alert list 233
Table 8-2 Basic alert parameters 235
Table 8-3 Parameters for exporting a report 240
Table 8-4 Parameters for querying alerts 241
Table 8-5 Parameters for exporting the alert list 244
Table 9-1 Monitoring pane description 252
Table 9-2 Monitoring pane description 255
Table 9-3 Parameters of performance and traffic statistics 259
Table 9-4 Monitoring pane description 260
Table 9-5 Parameters in the router interface list 263
Table 9-6 Monitoring pane description 265
Table 9-7 Parameters in the router interface group list 266
Table 9-8 Monitoring pane description 267
Table 9-9 Parameters for querying traffic statistics of an IP address 269
Table 9-10 Parameters of IP diversion routes 271
Table 9-11 FlowSpec diversion route parameters 273
Table 9-12 Parameters of group diversion routes 275
Table 9-13 Parameters for adding a manual diversion route 277
Table 9-14 Parameters for configuring a FlowSpec manual diversion route 280
Table 9-15 Basic NTA information. 287
Table 10-1 Parameters in the sys diagnose start command 298

Preface

Scope

This document presents main functions and usage of the web-based manager and console user interface of NSFOCUS Network Traffic Analyzer NX3-HD2100/HD2200 ("NTA" for short).

This document is provided for reference only. It may slightly differ from the actual product due to version upgrade or other reasons.

Audience

This document is intended for the following users:

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

This document assumes that you have knowledge in the following areas:

- Linux and Windows operating systems
- TCP/IP protocols
- Network security

Organization

Chapter	Description
1 Product Overview	Describes the characteristics, major functions, typical deployment modes, and configuration process of NTA.
2 Initial Configuration	Describes the initial configurations to be completed before the initial login to NTA.
3 Login Management	Describes how to log in to and manage NTA.
4 Administration	Describes how to configure basic settings, network connections, and interfaces to third-party software, how to use diagnosis and analysis tools, and how to manage data and user accounts, import the license, and upgrade the system.
5 Configuration	Describes how to configure monitoring objects, alert templates, global alert parameters, global diversion settings, flow data collection and forwarding, and the data dictionary.
6 Log Management	Describes how and what to view about various logs.

Chapter	Description
7 Report Management	Describes how and what to view about various reports generated in real time.
8 Alert Management	Describes how to view alert statistics and details of each log.
9 Monitoring	Describes how to view monitoring information, including regions, IP groups, routers, router interface groups, diversion routing tables, and local status of NTA.
10 Console-based Management	Describes how to log in to and manage NTA via the console user interface.
A Abbreviations	Describes acronyms and abbreviations used in this document.
B Default Parameters	Describes default settings of NTA.
C IPv4/IPv6 Support	Describes NTA support for IPv4/IPv6.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
	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

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

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

1 Product Overview

Section	Description
Product Characteristics	Describes outstanding characteristics of NTA.
Typical Deployment	Describes typical deployment modes of NTA.
Configuration Process	Describes the recommended process for configuring NTA.

1.1 Product Characteristics

With the rapid development of Internet technologies, it becomes more and more difficult to monitor a network due to the following factors:

- Increasing complexity of networks
- Evolution from the Internet Protocol version 4 (IPv4) to the Internet Protocol version 6 (IPv6)
- Constant emergence of new applications
- Bandwidth expansion

In this context, network security becomes an urgent issue that cannot be ignored. Various network anomalies, such as distributed denial-of-service (DDoS) attacks, pose a great threat to data centers, carriers, and other enterprises. Traditional network management tools cannot monitor carrier-class networks with heavy traffic or analyze packet types and traffic trends in complex network environments. For increasingly prevalent DDoS attacks, they cannot rapidly identify attack sources, targets, or types.

Based on flow technologies, NTA is a traffic monitoring and analysis product intended for carriers and data centers. NTA can monitor bandwidth usage of carrier-class networks. It can also detect DDoS attacks and generate corresponding alerts in real time, effectively reducing the additional operation and maintenance (O&M) workload caused by network complexity, thanks to its following characteristics:

- Industry-leading capability of abnormal traffic detection
- Various analysis and detection mechanisms
- Flexible deployment modes

In addition, NTA provides diverse statistical and analytic functions. The multidimensional traffic analysis and collection results can serve as a reference for network planning and business planning.

NTA has the following characteristics:

- Real-time monitoring of network status: Through network traffic collection and analysis, you can monitor the network status in real time. Based on such data, a network administrator can gain a network-wide perspective, taking a panoramic view of traffic status and trends and having a good grasp of network load and network resource usage.
- Accurate and exhaustive traffic analysis: Based on years of experience in flow data detection and analysis, NSFOCUS continuously optimizes flow data analysis algorithms, guaranteeing accurate analytic results even for complex network environments.
- Powerful anomaly detection capability: NTA implements detection based on built-in signatures and custom signatures, covering all threats to the backbone network. The proprietary intelligent detection system monitors bidirectional network traffic and discriminates between inbound and outbound attack traffic intelligently. This ensures the security of both the intranet and the extranet.
- Support for IPv4/IPv6 dual-stack analysis and detection: NTA supports traffic analysis and attack detection for the IPv4/IPv6 dual stack, leaving nothing to chance.
- Flexible report display: NTA has a flexible report system, which can generate various reports based on the combination of different conditions. The system provides real-time and historical reports, supporting viewing of reports for the last 1/7/30 days, by day/week/month, or for a specified period. In other words, NTA provides not only real-time monitoring reports but also historical reports for future reference and forensics. A report can be displayed as a pie chart, bar chart, or trend chart, or in a custom manner (area chart or broken-line chart).
- Complete solution: As one of the important product series of NSFOCUS and an integral part of the complete anti-DDoS solution, NTA works with NSFOCUS Anti-DDoS System (ADS) and NSFOCUS ADS Management (ADS M) to effectively protect a network against DDoS attacks.

1.2 Typical Deployment

NTA can be deployed flexibly. The following typical deployment modes are available to adapt to different network topologies and structures as well as different requirements for traffic analysis:

- Typical Deployment Mode for a Carrier's Network
- Typical Deployment Mode for an Enterprise's Office Network
- Typical Deployment Mode for a Campus Network

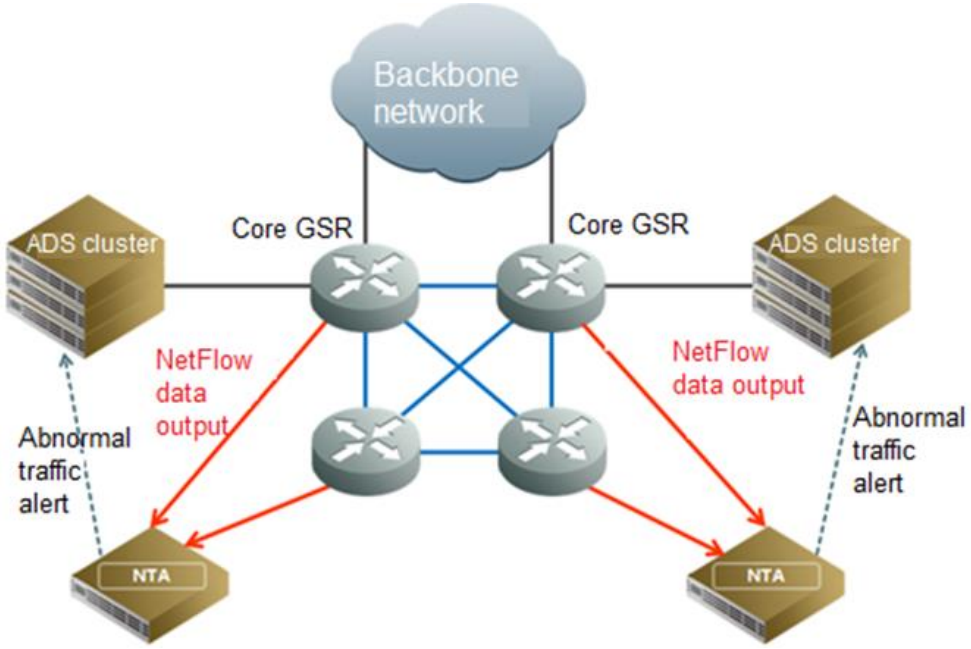
1.2.1 Typical Deployment Mode for a Carrier's Network

This deployment mode, as shown in Figure 1-1, applies to various metropolitan area networks (MANs) and private networks. The four egress routers in this figure are connected in full mesh, indicated with blue lines. To avoid repeated collection of flow data, do not enable NetFlow or sFlow on the ports of routers for mutual connection. Enable NetFlow or sFlow on the router ports for uplink or downlink connection instead.

On some small-scale networks, there may be only two egress routers. In this case, the preceding principle also applies. That is to say, do not enable NetFlow or sFlow on the ports of routers for mutual connection. You can deploy only one NTA device if its performance is strong enough.

In the network environment of a carrier, NTA NX3-HD2100/HD2200 are usually deployed with ADS clusters.

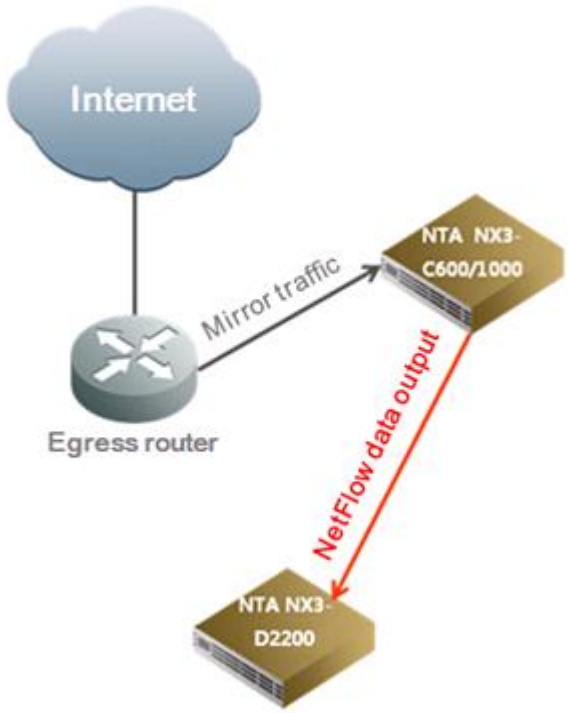
Figure 1-1 Typical deployment on a carrier's network



1.2.2 Typical Deployment Mode for an Enterprise's Office Network

On an enterprise's office network, the customer's network elements (NEs) may or may not support NetFlow and sFlow. In the former case, NTA can be deployed in the same way as that for a carrier's network. In the latter case, one NTA NX3-C1000 or NX3-C600 device must be added.

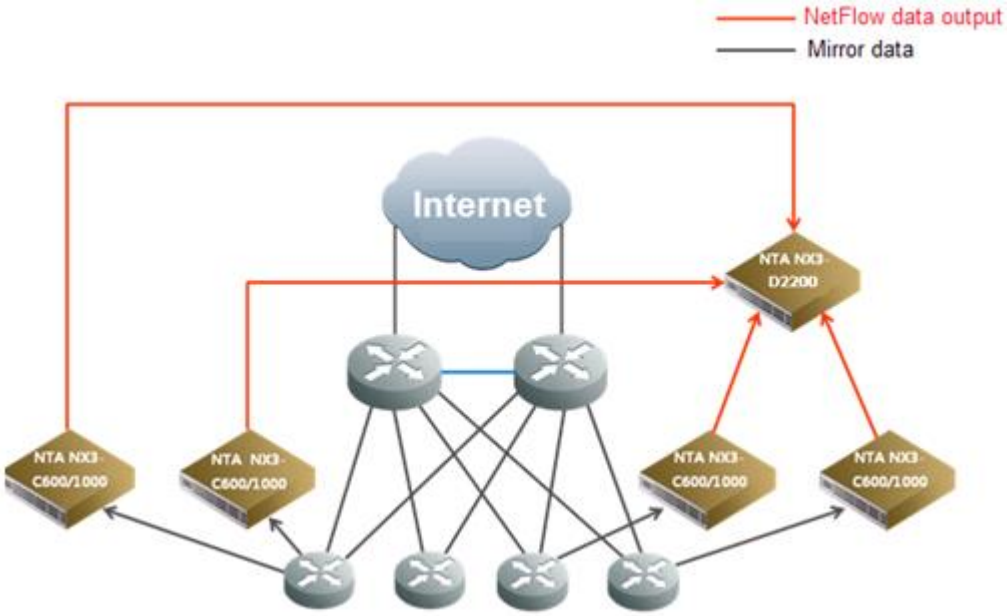
Figure 1-2 Typical deployment on an enterprise's office network



1.2.3 Typical Deployment Mode for a Campus Network

For a campus network, the customer may be concerned about traffic between subnets. Distribution-layer devices on such a network may not support NetFlow or sFlow. In this case, traffic on the uplink port of each access-layer router must be mirrored to NTA NX3-C1000 or NX3-C600 devices, which convert traffic to NetFlow or sFlow data and then send such data to the NTA NX3-HD2100/HD2200 device. If distribution-layer devices support NetFlow and sFlow, you do not need to deploy NTA NX3-C1000 or NX3-C600 devices. You can just enable NetFlow or sFlow on access-layer routers, which can directly send NetFlow or sFlow data to the NTA NX3-HD2100/HD2200 device.

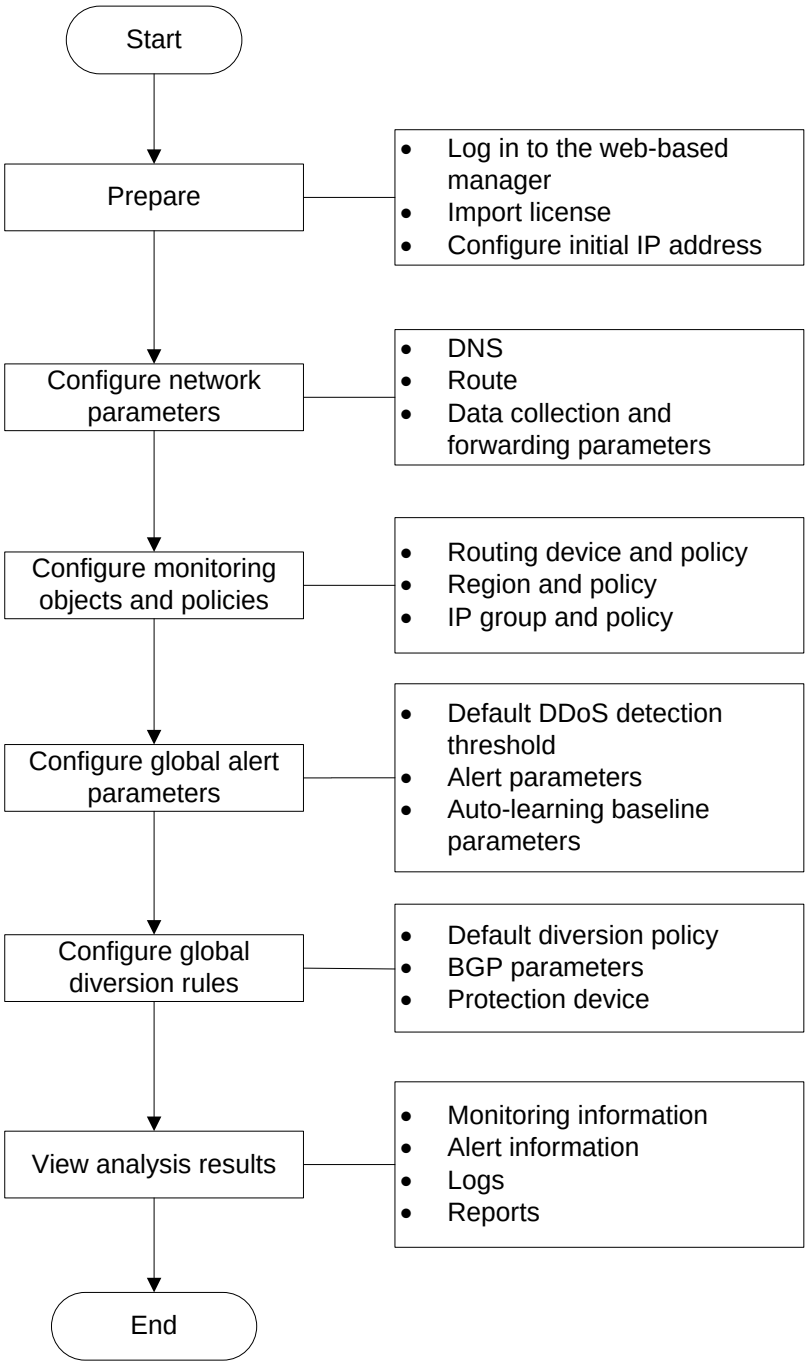
Figure 1-3 Typical deployment on a campus network



1.3 Configuration Process

Figure 1-4 shows the configuration process of NTA.

Figure 1-4 NTA configuration flow chart



2 Initial Configuration

To use the web-based manager, you must complete the following configurations upon your first login:

1. Log in to the console.
2. Configure the IP address and subnet mask of the management interface of the device.
3. Log in to the web-based manager to change the initial password.
4. Import a valid license file.

This chapter contains the following sections:

Section	Description
Logging In to the Console	Describes how to log in to the console by using a tool.
Configuring the IP Address of the Management Interface	Describes how to configure the IP address of the management interface of NTA.
Logging In to the Web-based Manager	Describes how to log in to the web-based manager of NTA.
Importing a License	Describes how to import a license.

2.1 Logging In to the Console

For initial use, you need to log in to the console to change the IP address of the management interface.

Before logging in to the console, prepare the following:

- One PC
- One serial cable shipped in the accessory kit
- Terminal software that can connect to the console port, such as SecureCRT.
- NTA connected to the PC with the serial cable

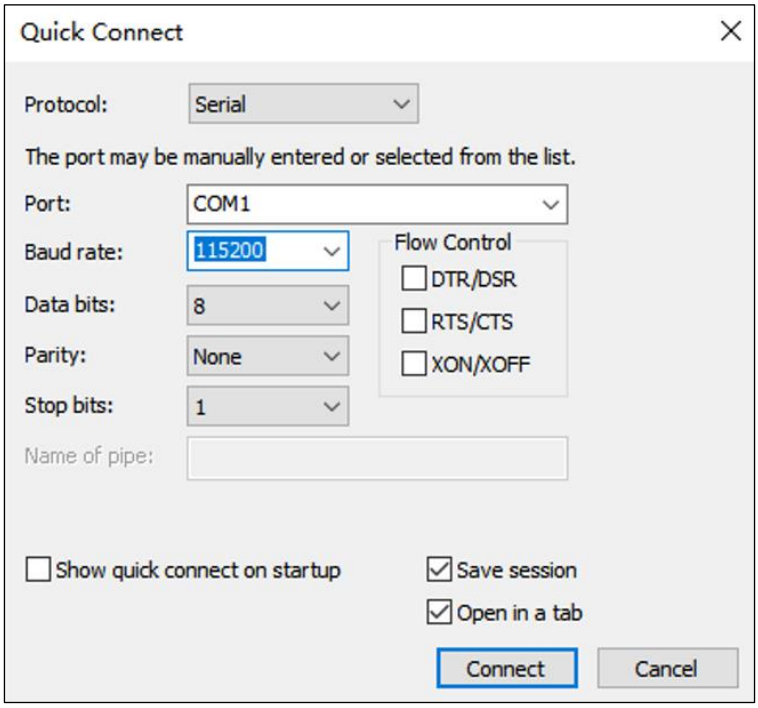
The following takes SecureCRT as an example to describe how to log in to the console user interface of NTA:

Step 1 Click **SecureCRT.exe** to open SecureCRT.

Step 2 Configure quick connection parameters.

Set **Protocol** to **Serial**, **Port** to **COM1**, **Baud rate** to **115200**, and **Data bits** to **8**, and leave other parameters at their default settings.

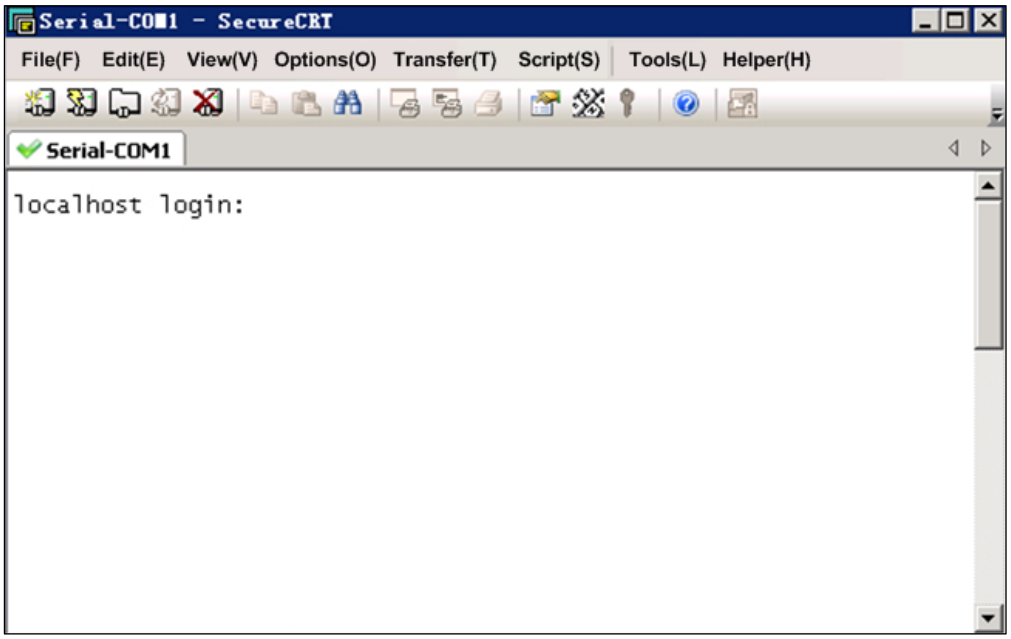
Figure 2-1 Configuring a quick connection



Step 3 Click **Connect**.

The console login window appears.

Figure 2-2 Login window



Step 4 Type the default user name and password (both are **admin**) to log in to the console.

Figure 2-3 Changing the login password

```
localhost login: admin
Password:
account use default password, Strongly recommended to change the password
Change it?(Y/N)n
NTA>
```

Step 5 Change the login password.

Press **Y** and type the new password. The password should consist of at least digits and English letters.

Step 6 Access the unprivileged mode.

For login to NTA via the console port, you are permitted nonprivileged access by default, as shown in Figure 2-4. In this mode, you can use only some of the commands.

Figure 2-4 Commands available in unprivileged mode

```
NTA>
  enable    Enable privileged commands
  ethtool   Display ethernet card settings
  exit      Exit and logout
  help      Description of the interactive help system
  tcpdump   Dump traffic on a network
```

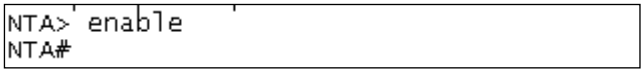
Table 2-1 lists the commands available in nonprivileged mode.

Table 2-1 Commands available in unprivileged mode

Command	Description
enable	Enables the privileged mode.
ethtool	Queries and configures Ethernet card settings.
tcpdump	Prints contents of network packets for fast network diagnosis.
help	Displays help information about the use of command lines.
exit	Exits the console user interface.

Step 7 Type **enable** at the command prompt to gain privileged access.

Figure 2-5 Accessing the privileged mode



To view commands available in privileged mode, press **?**. Figure 2-6 shows these commands.

Figure 2-6 Commands available in privileged mode

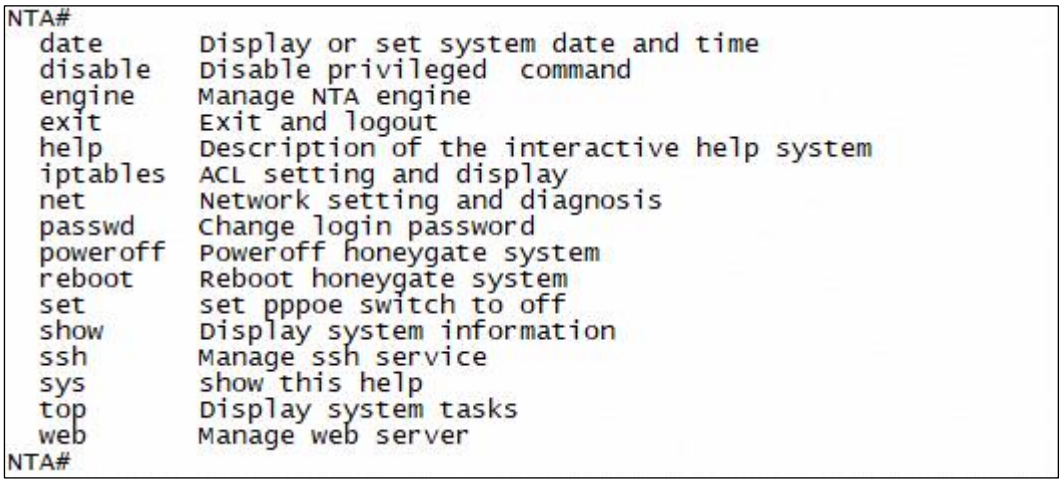


Table 2-2 shows the commands available in privileged mode.

Table 2-2 Commands available in privileged mode

Command	Description
date	Configures the system date and time.
disable	Exits the privileged mode.
engine	Enables or disables the system engine.
exit	Exits the console user interface.
help	Displays help information.

Command	Description
net	Displays and configures network settings, including the interface IP address, route, and DNS server.
passwd	Changes the password for access to the console user interface.
poweroff	Shuts down the system power.
reboot	Restarts the system.
show	Displays system configurations.
ssh	Enables or disables the SSH service.
sys	Displays system configurations.
top	Displays system tasks.
web	Manages the web service.

Step 8 Type **disable** in the command line interface to exit the privileged mode.

Step 9 Type **exit** in the command line interface to exit the console user interface.

----End

In the console user interface, you can only perform operations with the keyboard. Table 2-3 describes meanings of the frequently used keys.

Table 2-3 Meanings of keys

Key	Meaning
↑	(1) Switches to the input box; (2) Moves up.
↓	(1) Switches to **OK**; (2) Moves down.
←	(1) Switches to **OK**; (2) Moves left.
→	(1) Switches to **Cancel**; (2) Moves right.
Esc	Cancels an operation.
Enter	Confirms an operation.
Tab	Switches between an input box, the **OK** button, and the **Cancel** button.
BackSpace	Deletes the character to the left of the cursor.

For how to manage NTA through menus in the console user interface and the meanings of menu commands, see chapter 10 Console-based Management.

2.2 Configuring the IP Address of the Management Interface

After successful login to the console user interface, you can configure the IPv4 address, subnet mask, and gateway address for the management interface, as shown in Figure 2-7. After the configuration is complete, you can log in to the web-based manager.

Figure 2-7 Configuring the IP address of the management interface

```
NTA> en
NTA# net

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
> 2
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Network adapters:
  1) eth0
  2) eth1
  0) Escape
> 1
Please input ip address
> 10.245.2.206
Please input netmask
> 255.255.0.0
```

Configure the default network gateway of the management interface.

Figure 2-8 Configuring the network gateway of the management interface

```
NTA> en
NTA# net

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
> 4
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Please input default gateway address
> 10.245.255.254
Operation success.
```

2.3 Logging In to the Web-based Manager

Note	· Before login, check whether the options of blocking pop-ups and disabling JavaScript are selected in the browser. If yes, cancel the selections. · You are advised to use the latest Firefox, Internet Explorer (IE) 10.0, or Chrome browser and set the screen resolution to 1024x768 or higher.

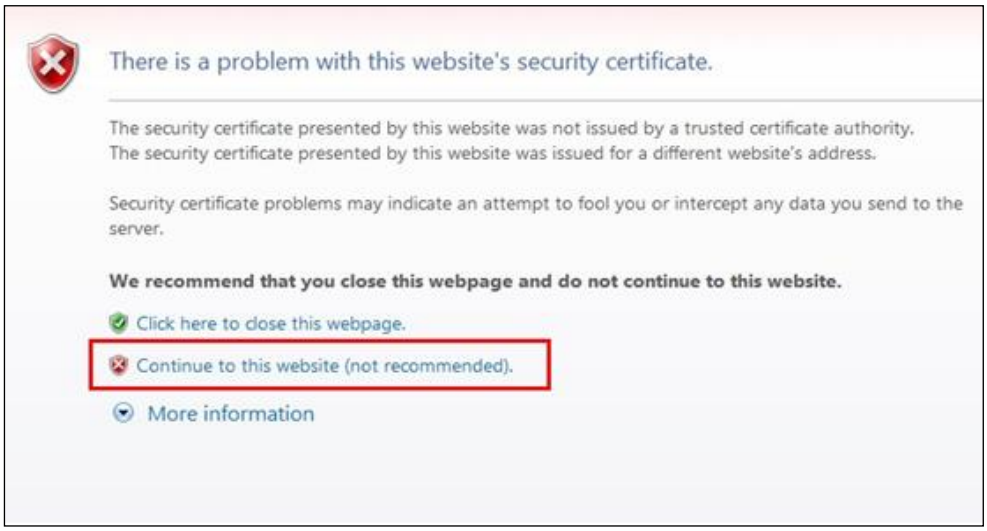
To log in to the web-based manager of NTA, perform the following steps:

Step 1 Make sure that the client communicates properly with NTA (open port 443 if the traffic needs to go through a firewall).

Step 2 Open a browser (Internet Explorer is used here) and connect to the management IP address of NTA over HTTPS, for example, enter **https://10.30.2.204** in the address bar.

After you press **Enter**, a security alert appears.

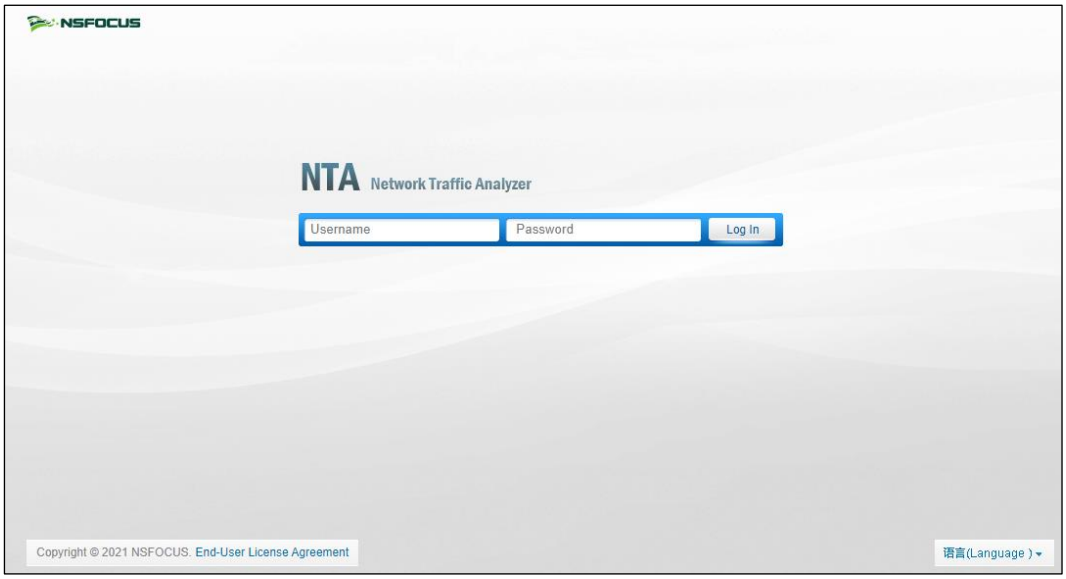
Figure 2-9 Security alert



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

The login page shown in Figure 2-10 appears.

Figure 2-10 Login page



Step 4 Type the initial user name and password (both are **admin**), and then click **Log In**.

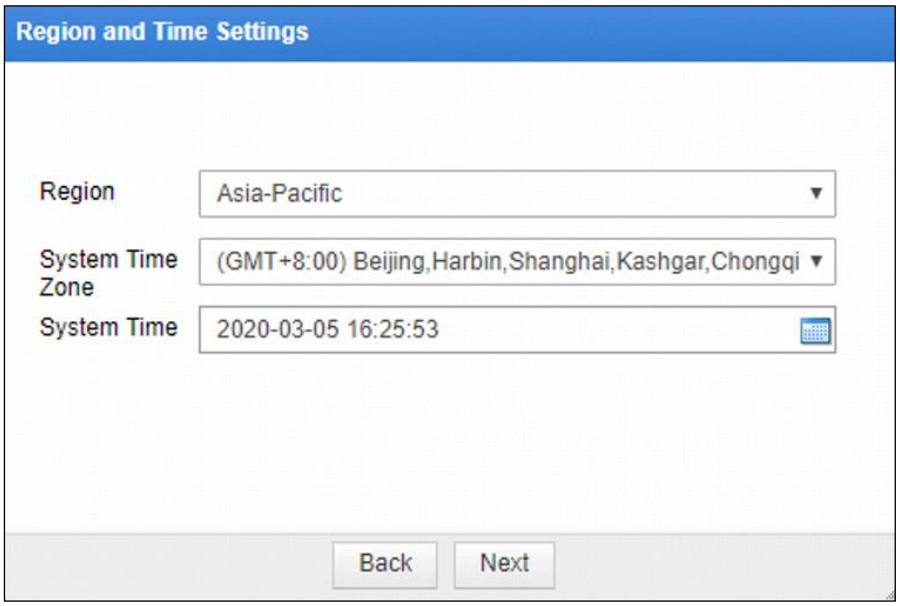
A window shown in Figure 2-11 appears, asking you to select a system language.

Note	During the first login to NTA that has just been upgraded to V4.5R90F00 or later, you need to set the locality, system time zone, and system time, but do not need to change the initial password.

Figure 2-11 Setting the system language

Step 5 Select a language. After the system directs you to the page shown in Figure 2-12, set the locality of the device, time zone, and system time. Then click **Next**.

Figure 2-12 Setting the country/region and time zone

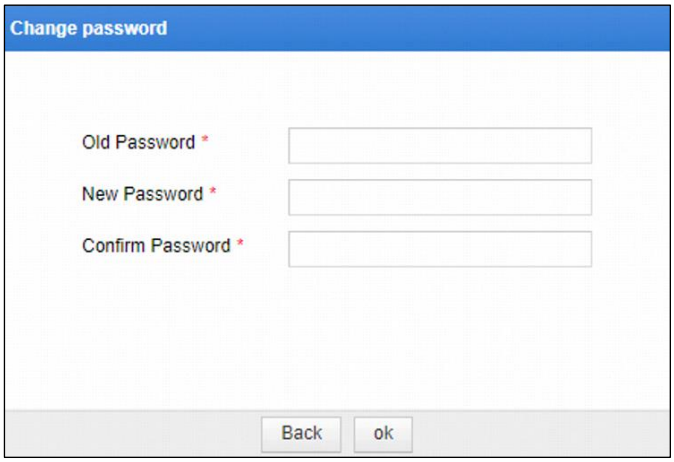


Step 6 Change the initial password.

The page for changing the initial password appears.

The new password must be a string of no less than 8 characters and contain at least two of the following character types: English letters, digits, and special characters.

Figure 2-13 Changing the initial password



Step 7 After changing the initial password, click **Submit** to make the settings take effect.

Then you successfully log in to the web-based manager.

----End

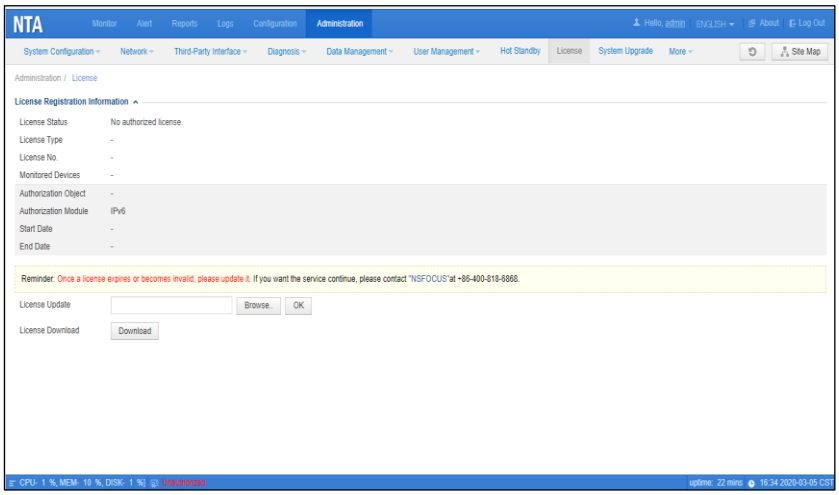
2.4 Importing a License

After logging in to an NTA device, you must import a license before using it.

To import a license, perform the following steps:

Step 1 Choose **Administration** > **License**.

Figure 2-14 License page



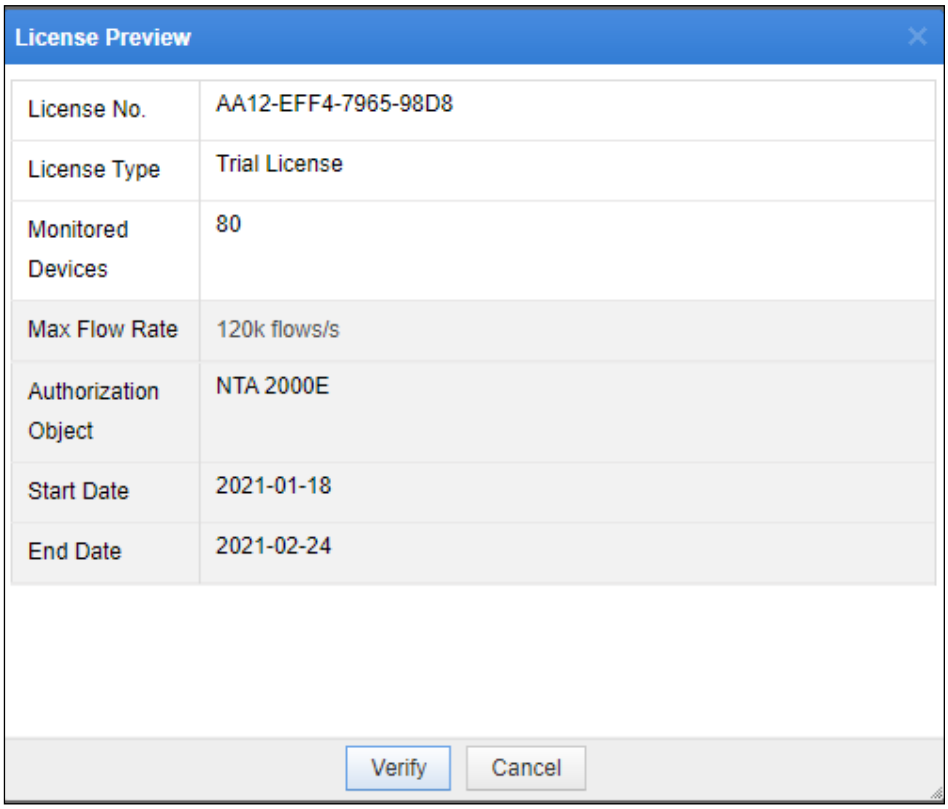
Step 2 Browse to the NTA license file and click **Open**.

Note	To get the NTA license file, please contact NSFOCUS technical support.

Step 3 Click **OK**.

The license preview page appears, as shown in Figure 2-15.

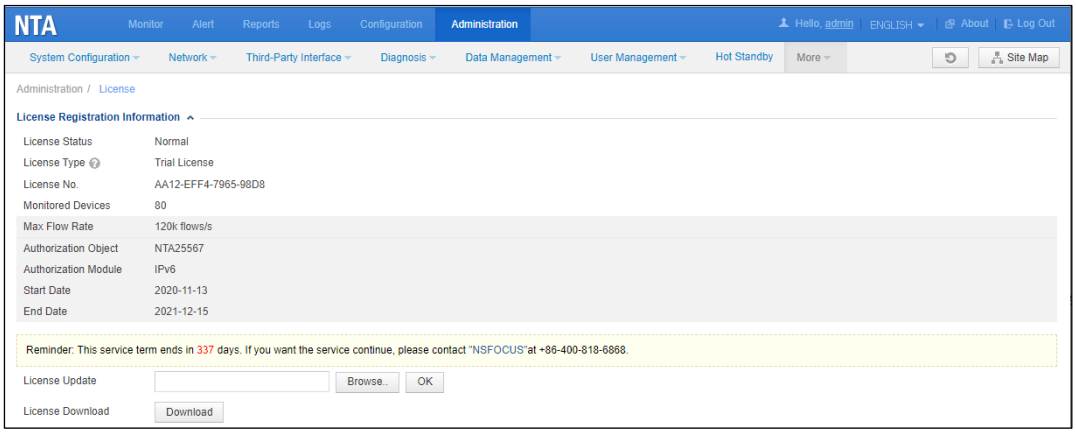
Figure 2-15 License preview



Step 4 Click **Verify** to import the license file.

The page after an import success is as shown in Figure 2-16.

Figure 2-16 Importing the license successfully



Note	**Max Flow Rate** limits the number of flows that can be processed by NTA per second. The value varies with the device model.

	Flows per second are limited to 120,000 for both NTA NX3-2000E and NX3-HD2200,60,000 for NTA NX3-1000E, 60,000/100,000 for NTA NX3-HD2100, 120,000/180,000/240,000 for NTA NX3-HD2200, and 60,000/120,000/180,000/240,000/300,000 for vNTA. For details, contact NSFOCUS technical support.

----End

3 Login Management

This chapter describes three login management modes of NTA, containing the following sections:

Section	Description
Web-based Manager	Describes management through the web-based manager, whose intuitive human-machine interfaces (HMIs) provide all necessary management functions. NTA supports Internet Explorer 10.0, Firefox, and Chrome browsers.
Console User Interface	Describes how to configure and manage NTA using command lines via the console.
SSH	Describes how to manage NTA from a remote management client supporting the Secure Shell protocol (SSH).

Note	All NSFOCUS products support web-based management and console-based management, but some may not support management via SSH or other means.

3.1 Web-based Manager

The web-based manager of NTA provides intuitive HMIs for users to manage and configure NTA. The following sections describe the users, login method, and page layout of, and common operations on the web-based manager.

3.1.1 Users

The web-based manager of NTA has two types of users:

- System administrator

  A system administrator has permissions of managing and configuring the web-based manager. **admin** is the default system administrator account.
- Audit administrator

  An audit administrator has permissions of viewing system logs. **auditor** is the default auditor account.

On NTA, different roles have different permissions, as shown in Table 3-1.

Table 3-1 Permissions of different roles

Role		Permission
System administrator	Super administrator (**admin**)	Has the highest permissions and can add system administrators, change the password of **auditor**, and perform other configurations. The default password is **admin**.
	System administrator	Has almost the same permissions as **admin**, but can only add configuration administrators and common users. This administrator cannot modify information of built-in accounts (**admin** and **auditor**) and other administrator accounts.
	Configuration administrator	Has permissions of configuring business-related settings, such as routers, regions, and policies. Unlike a system administrator, a configuration administrator cannot perform the following operations: • Configure the NTA system, that is, access the Administration module. • View audit logs. • Configure alert templates and data dictionaries.
	Common user	Unlike a system administrator, a common user cannot: • View routing tables in the Monitor module. • View audit logs in the Logs module. • Configure any settings in the Configuration module. • Configure any settings in the Administration module.
Auditor	**auditor** (default)	Can only view the local monitoring status and audit logs. The default password of the default auditor account, **auditor**, is **auditor**. This type of accounts can be added.

3.1.2 Login

For details on login to the web-based manager, see section 2.3 Logging In to the Web-based Manager.

Upon your first login, import a license for proper use of the system. For how to import a license, see section 2.4 Importing a License.

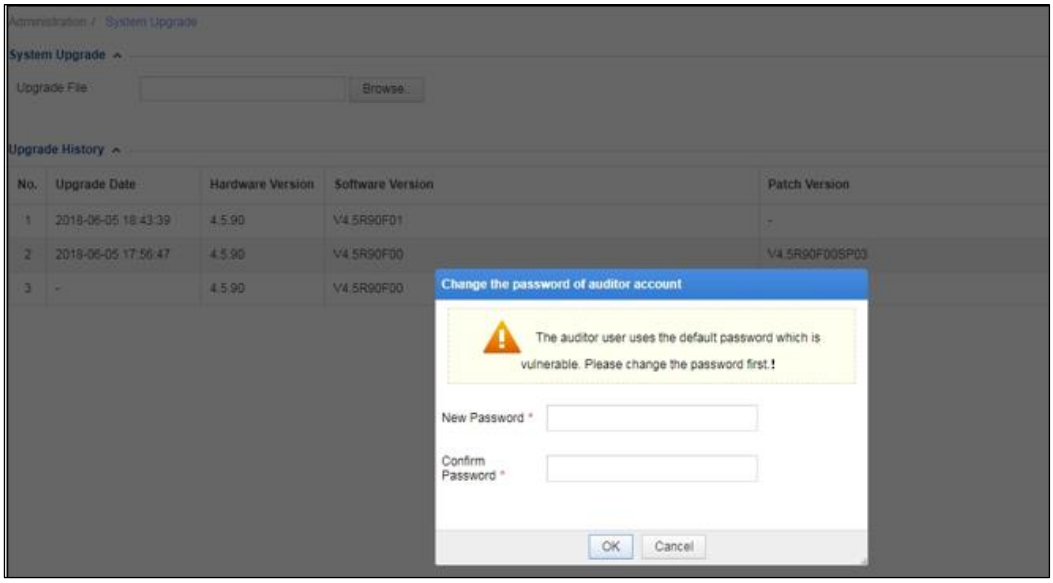
- After remaining inactive for over 10 minutes after login, you must log in again to continue using the system.
- The possible cause for a login failure may be (1) incorrect user name; (2) incorrect password; (3) upper/lower case confusion; or (4) account disabled or deleted.

3.1.3 Forced Password Change

During an upgrade to this version, the system automatically checks whether the **auditor** account uses the default password. If yes, once the **admin** user logs in, the system forces him or her to change the default password of the **auditor** account, as shown in Figure 3-1.

The **admin** user needs to type the new password twice and click **OK**.

Figure 3-1 Changing the password



3.1.4 Page Layout

The **admin** user accesses the system after successful login. Figure 3-2 shows the general layout of the page.

Figure 3-2 Page layout

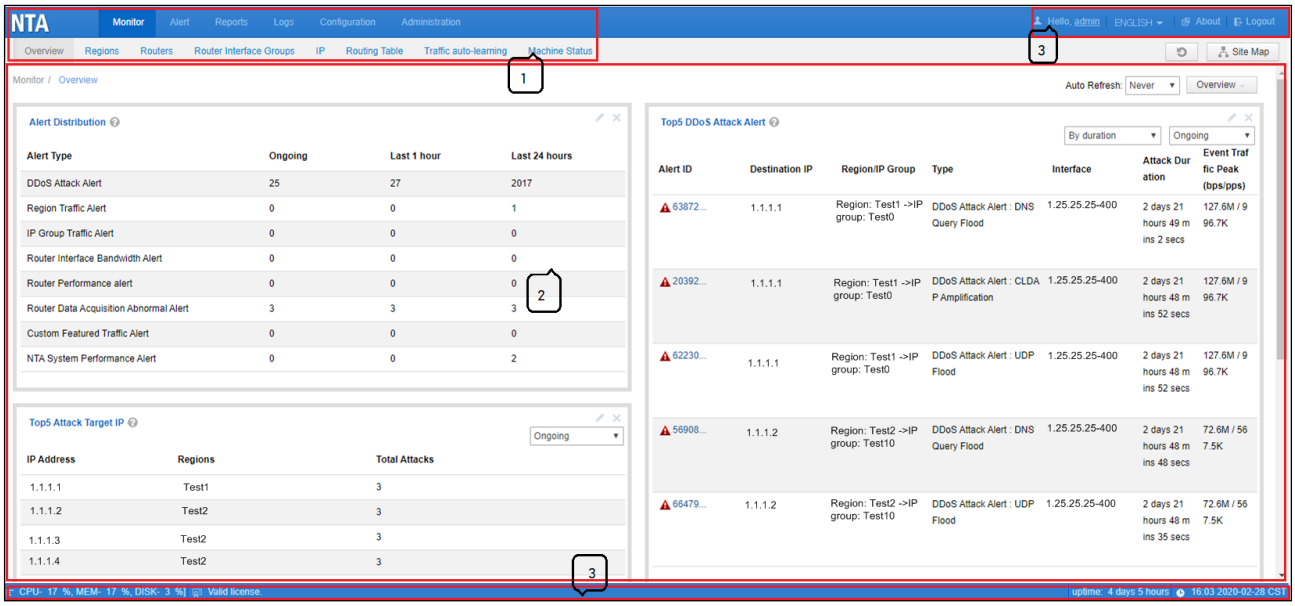


Table 3-2 describes the page layout.

Table 3-2 Page layout

No.	Area	Description
1	Navigation bar	Area where menus and related submenus are provided to help you locate system functions. Clicking **Site Map**, you can quickly find the desired module.
2	Work area	Area where you can perform configurations and operations and view data.
3	Quick access bar	Area providing the following common buttons of the system: • Hello, admin: modifies the password of the current account. • ENGLISH: switches the language. • About: presents information about NTA. • Logout: logs you out of the web-based manager. • CPU- 16 %, MEM- 16 %, DISK- 3 %: presents the hardware resource usage of the system. • Valid license.: presents license details. • uptime: 4 days 6 hours: presents the system uptime. • 16:54 2020-02-28 CST: presents the system time and its time zone. Note For the sake of security, you are advised to click Logout to log out of the system.

Note	The menus and work areas vary with user permissions.

3.1.5 Common Buttons and Their Functions

Table 3-3 describes common buttons and their functions.

Table 3-3 Common buttons and their functions

Button	Function
	Edits the current item.
	Deletes the current item. Note • Predefined items, such as the **admin** account in **User Management**, cannot be deleted.

Button	Function
	• Referenced items cannot be deleted.
	Refreshes the current page.
	Starts an operation.
	Stops an ongoing operation.
	Moves up/down a policy in a list.
	Enables/Disables a policy.
	Copies the current item.
	Exports a report as an .xml or .csv file.
	Prints logs or a report.
	Returns the query result according to the conditions you have set.
	Displays monitoring information of an interface or referencing of an object.
	Deletes a diversion route.
	Displays brief information about the item.

Pointing to a button displays the description of what the button does.

3.2 Console User Interface

Through a console port, you can access the console user interface of NTA, which provides certain functions such as initial system configuration, status detection, and restoration of the initial configurations. Functions that cannot be managed on the web-based manager can be managed via the console. The following sections describe how a console user accesses the console user interface of NTA over a serial connection.

3.2.1 Console User

The default console user of NTA is **admin**, with **admin** as the default password.

3.2.2 Login

For details on login to the console user interface, see section 2.1 Logging In to the Console.

3.3 SSH

In addition to the web-based manager and console, NTA can be remotely managed via software that supports SSH, such as secureCRT or PuTTY. You can type the correct user name, password, and port number (respectively **conadmin**, k@eT!23i, and **50022** by default) for SSH login. For the first use, you will be forced to change the default password.

Note	To implement SSH-based management, make sure that the SSH service has been enabled on the system. For details, see section 4.1.1.2 Configuring Remote Assistance.

4 Administration

This chapter describes common operations and methods for system maintenance, containing the following sections:

Section	Description
System Configuration	Describes how to configure the system time and default language and how to enable or disable various services in the system.
Network Configuration	Describes how to configure a physical interface, static route, and DNS server.
Third-Party Interface	Describes how to configure interfaces for interworking with the SMTP server, SNMP server, syslog server, and NSFOCUS ESPP.
Diagnosis	Describes how to use NTA and network fault diagnosis tools.
Data Management	Describes how to configure automatic disk cleaning and view the usage of each data partition.
User Management	Describes how to configure user accounts, security settings, and authentication settings.
Hot Standby	Describes how to configure the hot standby function based on VRRP.
License	Describes how to view the license status and import the license file.
System Upgrade	Describes how to upgrade the system software, detection rule library, and threat intelligence database online.
Alert Whitelist	Describes how to configure an alert whitelist.
Access Control	Describes how to configure access control.

4.1 System Configuration

System configuration consists of the following:

- Basic Configuration
- Website Customization
- SSL Certificate Import
- Remote Assistance

4.1.1 Basic Configuration

This section describes how to configure the system time and default language and how to enable or disable services in the system. You can directly shut down or restart the system or restart all services in the system at one click on the **Basic Information** page.

This section covers the following topics:

- Configuring Basic Information: describes how to configure the system time and NTP server, and import and export system settings.
- Configuring Remote Assistance: describes how to enable or disable the SSH service and configure the service port.
- Configuring System Engines: describes how to enable or disable key services on NTA.

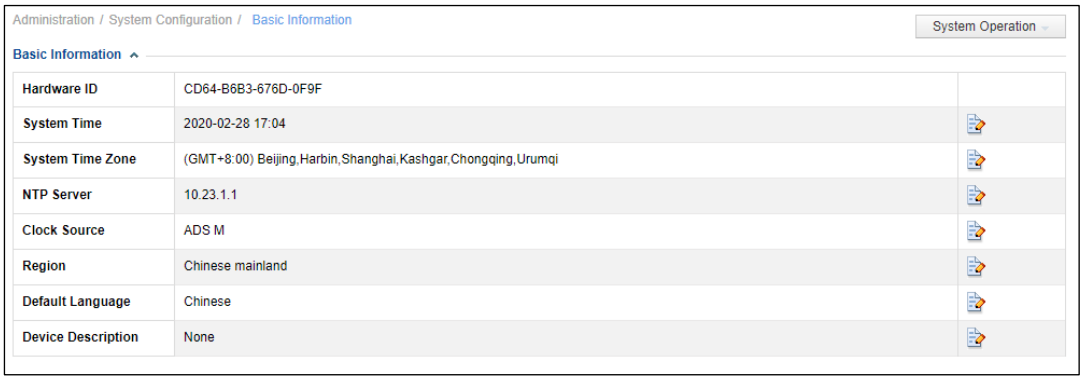
4.1.1.1 Configuring Basic Information

To configure basic information of the system, follow these steps:

Step 1 Choose **Administration > System Configuration > Basic Information**.

Figure 4-1 shows the **Basic Information** area.

Figure 4-1 Basic Information area



Step 2 Configure basic information.

Table 4-1 Parameters for configuring basic information

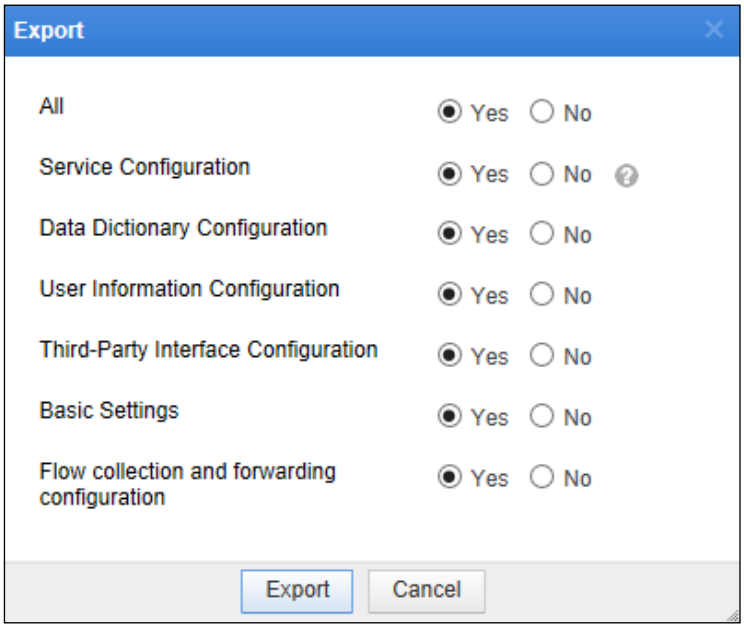
Parameter	Description
Hardware ID	Indicates the unique identifier of the system, which cannot be edited.
System Time	Specifies the current system time of the built-in clock. You can click to change the time according to your geographical location. After you confirm the change, the system time is changed.
System Time Zone	Specifies the time zone of the built-in clock. You can click to change the time zone according to your geographical location. After you confirm the change, the time zone is changed.
Clock Source	Specifies the reference clock source for time synchronization of NTA, which can be **NTP Server** or **ADS M**.
NTP Server	Specifies the domain name of the current NTP server. The NTP server can

Parameter	Description
	synchronize system clocks to ensure that the time on all devices on the network is the same. You can click to change the NTP server. After you confirm the change, the NTP server is changed.
Region	For the selection of **Chinese mainland**: • The default NTI server address is **nti.nsfocus.com**. • The cloud authorization server based in China is used for vNTA (virtualized version of NTA). For the selection of other regions: • The default NTI server address is **nti.nsfocusglobal.com**. • The international cloud authorization server is used for vNTA.
Default Language	Specifies the default language of logs. The web-based manager supports Simplified Chinese and English. The default language is **English**. You can click to change the default language of the system. After you confirm the change, the default language is changed.
Device Description	Provides descriptive information of the device to make it easier to identify the device.

Step 3 Export the settings.

a. Click **System Operation** and choose **Export Config** from the drop-down list. The **Export** dialog box appears, as shown in Figure 4-2.

Figure 4-2 Exporting configuration files



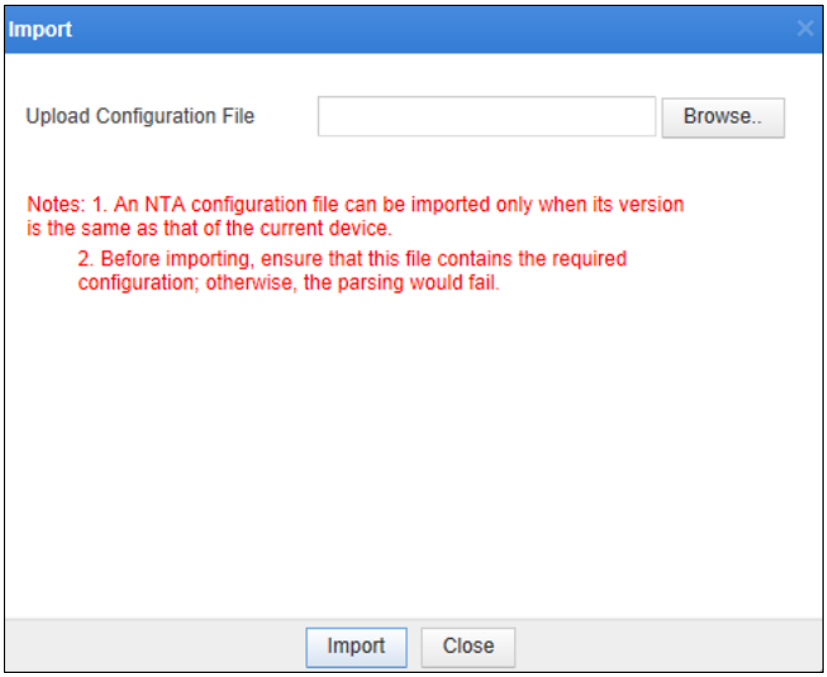
Service Configuration covers region configuration, IP group configuration, routing device configuration, interface group configuration, global diversion configuration, and global alert configuration.

b. Click **Yes** for the configurations you want to export and then click **Export**. After you select a path, the selected configuration files are exported as backups.

Step 4 Import the settings.

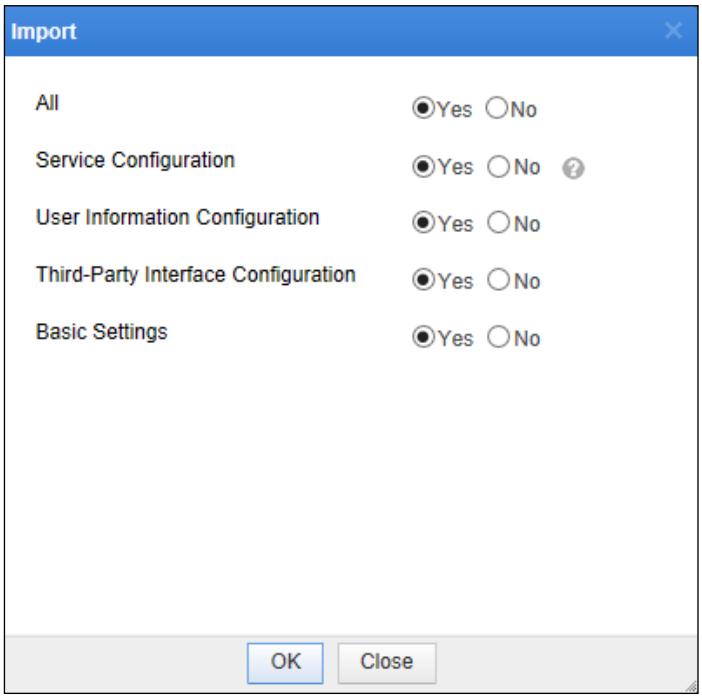
a. Click **System Operation** and choose **Import Config** from the drop-down list. The **Import** dialog box appears, as shown in Figure 4-3.

Figure 4-3 Importing a configuration file



b. Click **Browse** and select a file, and then click **Import** to import the previously exported configuration file into the NTA system. After you click **Import**, a dialog box appears, showing which configuration files are available for import, as shown in Figure 4-4.

Figure 4-4 Configurations that can be imported



c. Click **OK** to complete the import or click **Close** to cancel the import.

Tip	• The imported configuration file can take effect only when its NTA version is the same as the current one. • The imported configuration file will overwrite the current settings of the system and the engines will automatically restart in the process. Therefore, traffic auto-learning and alerting will also stop functioning. • Auto-learning data of users can be imported and exported, but the "Learning failed" and "Learning" states will be changed to the "Not learned" state.

----End

4.1.1.2 Configuring Remote Assistance

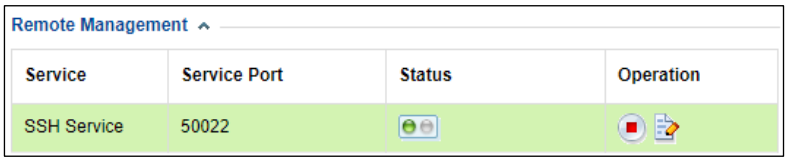
NTA can be remotely managed via SSH. You can control whether to enable the SSH service and specify the port number of the SSH service.

To configure remote assistance, follow these steps:

Step 1 Choose **Administration > System Configuration > Basic Information**.

Figure 4-5 shows the **Remote Management** area.

Figure 4-5 Remote Management area



Step 2 Stop or start the SSH service.

- The status indicators indicate that the service has been started. To stop the service, click in the **Operation** column. After that, you cannot remotely log in to and configure the current device via SSH.
- The status indicators indicate that the service has been disabled. To start the service, click in the **Operation** column.

Step 3 Change the SSH service port.

The **Service Port** column displays the number of the port on NTA for providing the SSH service. The default port is **50022**. To change the port, click in the **Operation** column. After the change, the system automatically restarts the SSH service to commit the change.

Step 4 Click **Reboot** on the **System Operation** drop-down list to restart the NTA hardware system from the web-based manager.

Step 5 Click **Shutdown** on the **System Operation** drop-down list to shut down the NTA hardware system from the web-based manager.

----End

4.1.1.3 Configuring System Engines

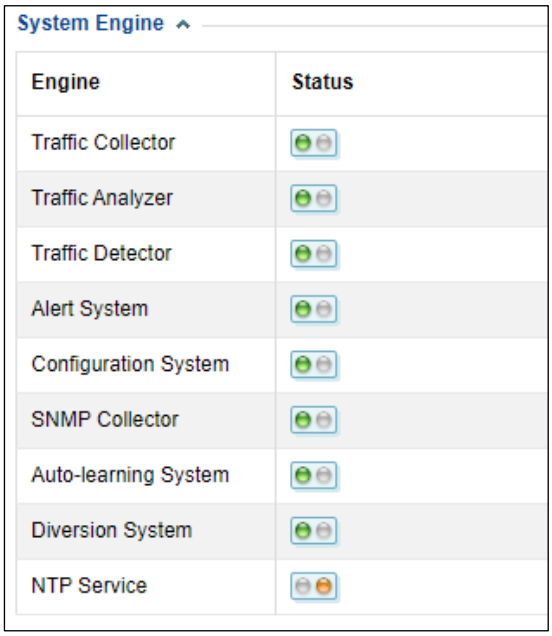
NTA provides traffic collection, traffic analysis, traffic detection, alert management, SNMP collection, auto-learning, and diversion control services. You can check whether a service runs properly and enable or disable a service. However, as these services are essential for NTA to run properly, you are advised not to disable any of them.

To view the system engine status, follow these steps:

Step 1 Choose **Administration > System Configuration > Basic Information**.

Figure 4-6 shows the **System Engine** area.

Figure 4-6 System Engine area



Step 2 Stop or start a service.

- The status indicators indicate that the service has been started.
- The status indicators indicate that the service has been disabled.

To restart all engines, click **System Operation** and choose **Restart Engine** from the drop-down list.

Step 3 Restart the web server.

After modifying system settings, generally, you are prompted to restart the web server to commit the changes. You can click **No** in the dialog box to not restart the web server immediately. To restart the web server later, click **System Operation** and choose **Restart web server** from the drop-down list.

----End

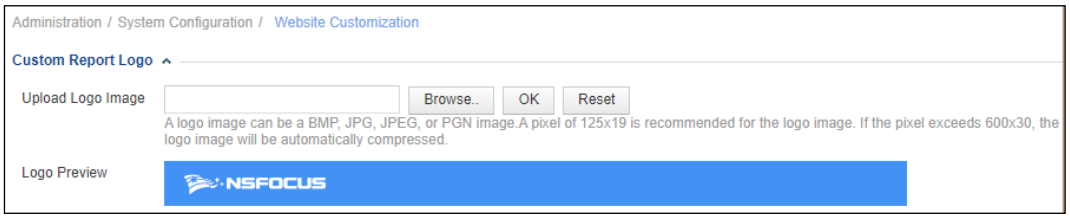
4.1.2 Website Customization

On the **Website Customization** page, you can upload an image as the logo above the title in reports, including traffic reports and DDoS attack reports.

To upload a logo image, follow these steps:

Step 1 Choose **Administration > System Configuration > Website Customization**.

Figure 4-7 Website Customization page



Step 2 Click **Browse** and select the image to be uploaded.

Make sure that the format and size of the image meet the requirements.

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

You can preview the logo that is uploaded.

----End

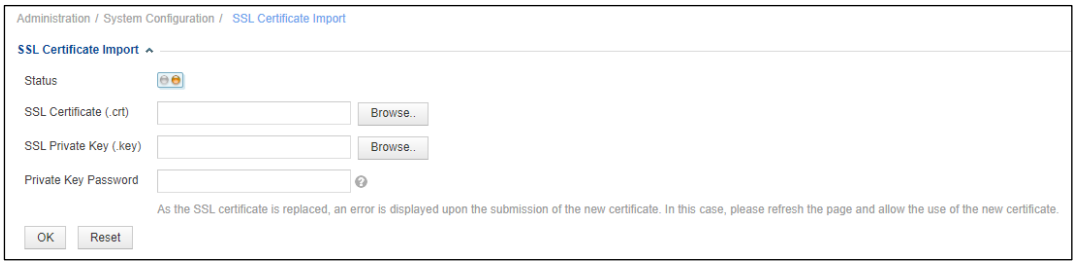
4.1.3 SSL Certificate Import

On the **SSL Certificate Import** page, you can upload an SSL certificate.

To configure an SSL certificate, follow these steps:

Step 1 Choose **Adminisdtration > System Configuration > SSL Certificate Import**.

Figure 4-8 SSL Certificate Import page



Step 2 Click **Browse** to select the desired SSL certificate and private key.

Step 3 Configure a private key password and click **OK**.

----End

4.1.4 Remote Assistance

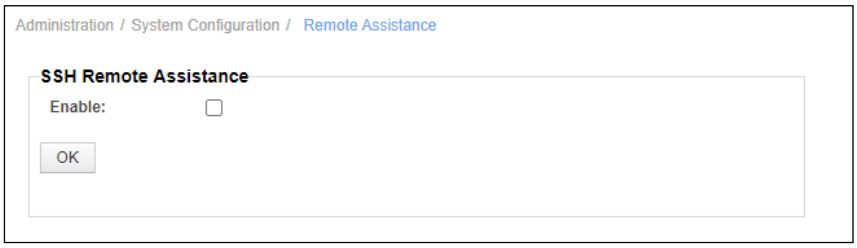
When NTA becomes faulty, you can enable the remote assistance function, allowing NSFOCUS technical support to provide remote support.

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

To enable the remote assistance function, follow these steps:

Step 1 Choose **Administration > System Configuration > Remote Assistance**.

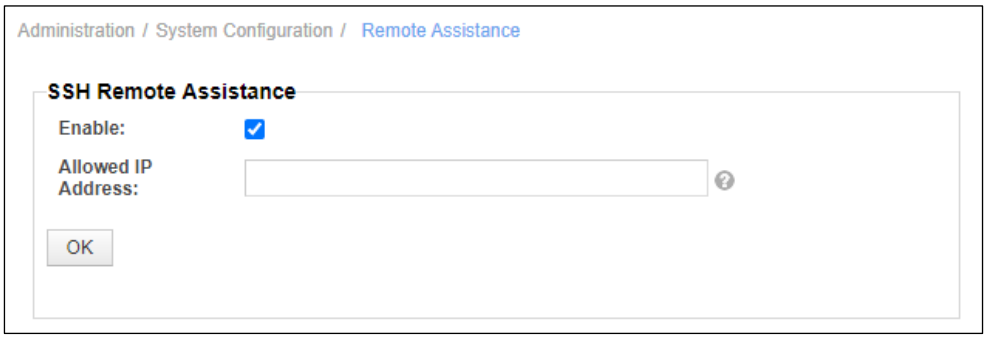
Figure 4-9 Remote assistance



Step 2 Select **Enable** and configure the IP address for remote assistance.

You can configure at most three IP addresses separated by the colon.

Figure 4-10 Configuring remote assistance



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

Then the login key used by the specified IP address for remote access to NTA and its QR code are displayed below, as shown in Figure 4-11.

Figure 4-11 Configuring remote assistance

----End

4.2 Network Configuration

The Network module allows you to configure parameters for NTA to connect to other network devices and the Internet by performing the following operations:

- Configuring a Local Interface
- Configuring a Route
- Configuring a DNS Server
- Configuring a Bond

4.2.1 Configuring a Local Interface

You can configure the IP address of the network interface on NTA. NTA supports IPv4/IPv6 dual stack. As a dual-stack node, NTA allows you to configure both IPv4 and IPv6 addresses. It uses the IPv4 protocol stack for communication with IPv4 nodes and the IPv6 protocol stack for communication with IPv6 nodes. For an interface connecting to a dual-stack network, you must configure both IPv4 and IPv6 addresses.

Note	The dual-stack technology is an effective IPv4-to-IPv6 transition technology. Dual-stack network nodes support both IPv4 and IPv6 protocol stacks. A source node chooses a protocol stack according to the protocol supported by the destination node and a network device does so according to the protocol type of packets when processing and forwarding packets.

Step 1 Choose **Administration > Network > Local Interface**.

Figure 4-12 Local Interface page

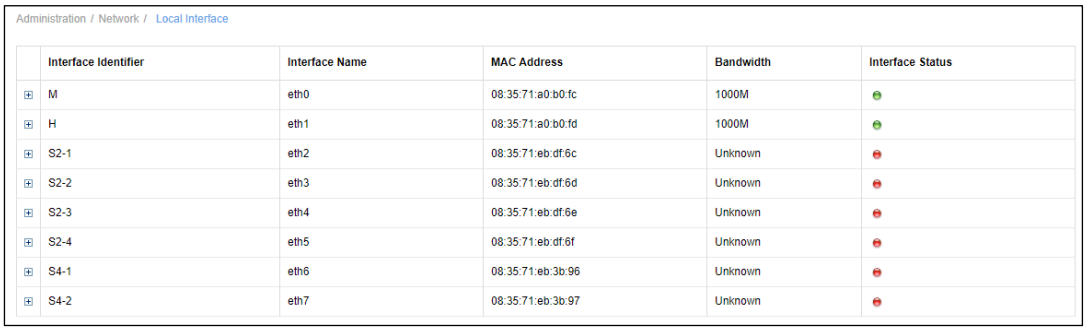


Table 4-2 describes parameters on this page.

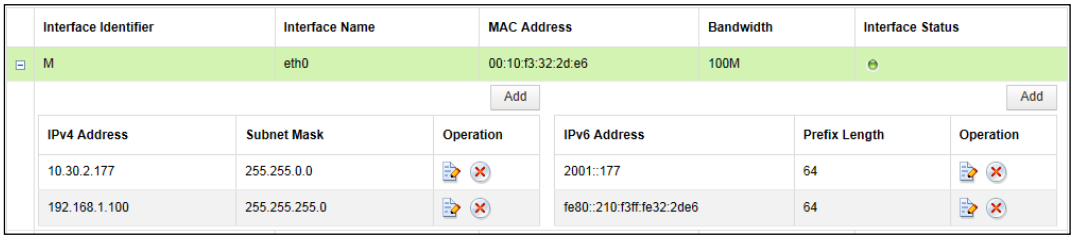
Table 4-2 Interface attributes

Parameter	Description
Interface Identifier	Indicates the type of an interface, which can be an expansion interface or a configuration interface. The configuration interface is indicated with H or M. The expansion interface is indicated with Sa-b, representing the bth interface on the ath expansion board.
Interface Name	Indicates the name of each physical interface of NTA.
MAC Address	Indicates the MAC address of the physical interface.
Bandwidth	Indicates the maximum physical bandwidth of each interface. When the network connection of an interface is down, its bandwidth is displayed as **Unknown**.
Interface Status	Indicates the status of each interface: • indicates that the network connection of the interface is up. • indicates that the network connection of the interface is down.

Step 2 Configure interface attributes.

Clicking on the left of the interface name displays all IP addresses that have been configured, as shown in Figure 4-13.

Figure 4-13 Interface attributes

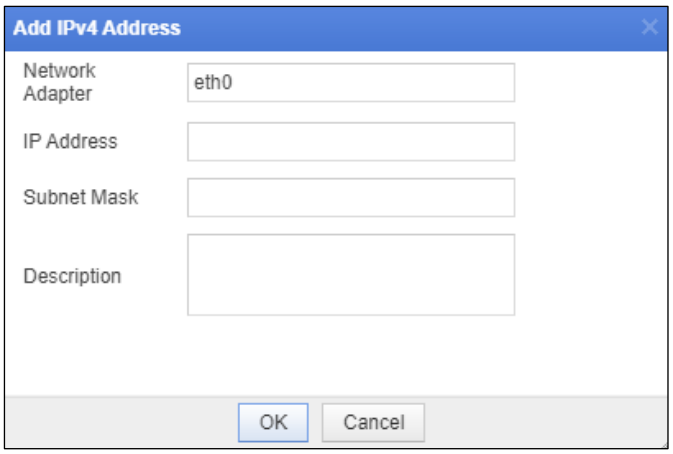


Multiple IPv4 and IPv6 addresses can be configured for each interface.

Step 3 Add an IPv4 address for the local interface.

a. Click **Add** in the IPv4 address area.

Figure 4-14 Adding an IPv4 address

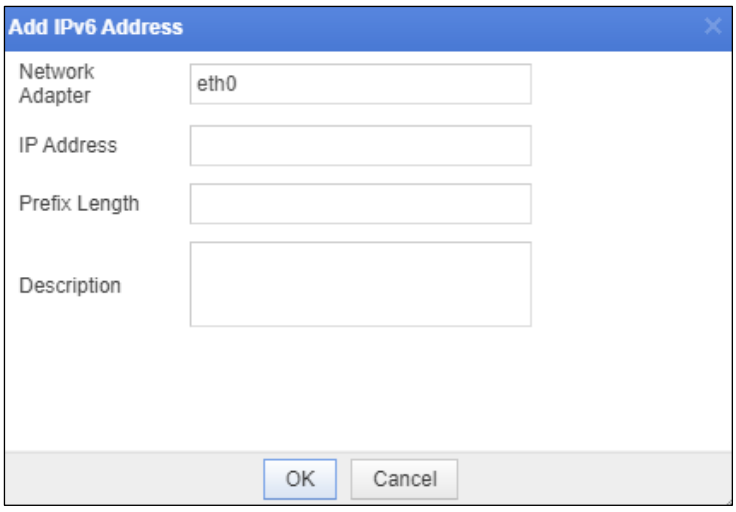


b. In the **Add IPv4 Address** dialog box, type an IPv4 address, the subnet mask, and the description. Click **OK** to save the settings.

Step 4 Add an IPv6 address for the local interface.

a. Click **Add** in the IPv6 address area.

Figure 4-15 Adding an IPv6 address



b. In the **Add IPv6 Address** dialog box, type an IPv6 address, the prefix length, and the description. Click **OK** to save the settings.

----End

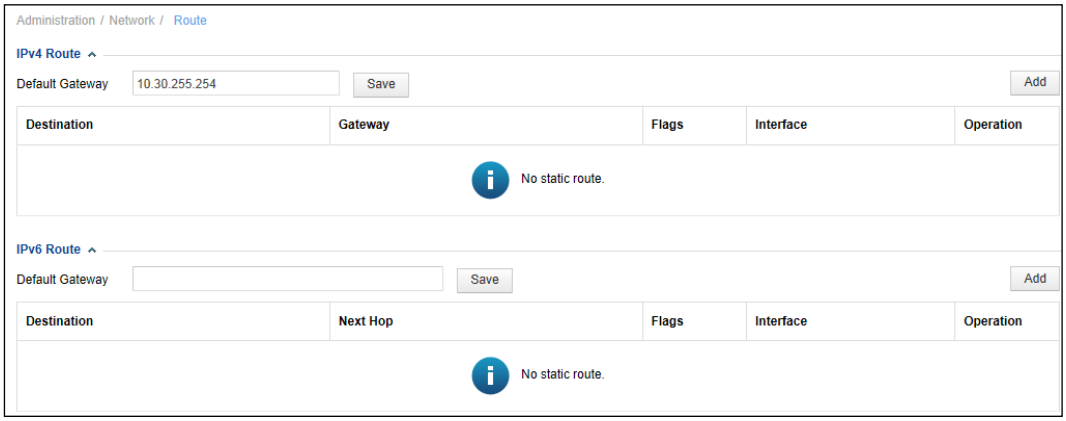
4.2.2 Configuring a Route

NTA forwards packets through a static route and default gateway. For this purpose, you must configure a static route and default gateway in advance.

The procedure is as follows:

Step 1 Choose **Administration** > **Network** > **Route**.

Figure 4-16 Route page



Step 2 Configure a default gateway.

A default gateway is the node that NTA uses to forward packets when an IP address does not match any other routes in the routing table.

Type an IPv4 or IPv6 address in the **Default Gateway** field and then click **Save**.

Step 3 Configure a static route.

Click **Add** and configure a static route in the dialog box shown in Figure 4-17.

Figure 4-17 Adding a static route

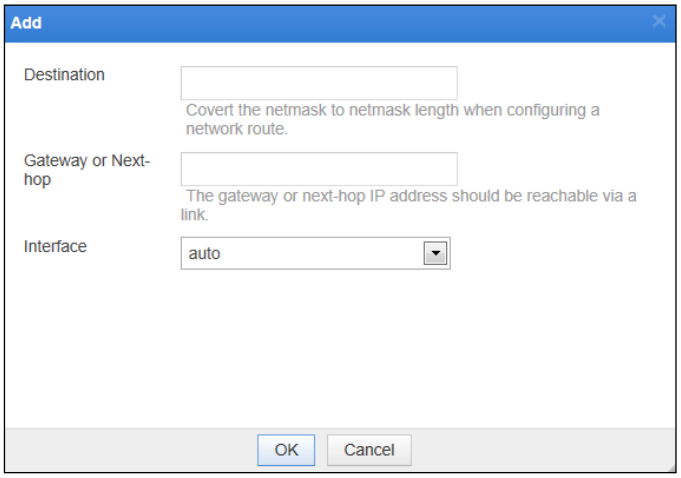


Table 4-3 describes parameters for configuring a static route.

Table 4-3 Parameters for configuring a static route

Parameter	Description
Destination	Specifies the destination address or network of IP packets. You can type an IPv4 address and its subnet mask for an IPv4 route or an IPv6 address and its prefix for an IPv6 route. Note If you want to configure a static route for a network segment, you need to convert the subnet mask into a subnet length, such as 10.20.0.0/24.
Gateway or Next-hop	Specifies the gateway for the static route, usually, the local IP address of the next-hop device.
Interface	Specifies the egress interface of the static route.

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

----End

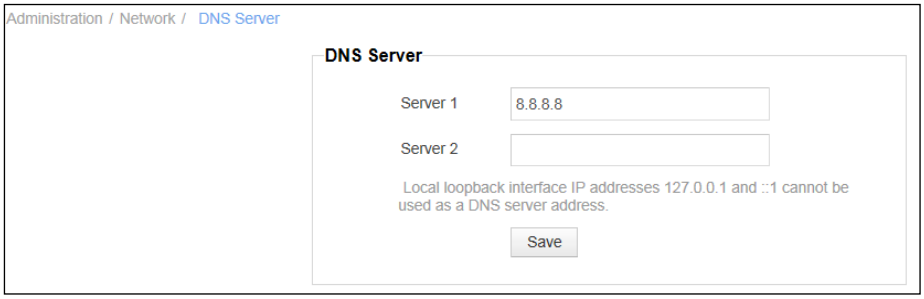
4.2.3 Configuring a DNS Server

As an essential and fundamental service on the Internet, the Domain Name System (DNS) service is used to determine the mapping between domain names and IP addresses. As a DNS client, NTA can request the domain name resolution service from a specified DNS server.

To configure the DNS server, follow these steps:

Step 1 Choose **Administration** > **Network** > **DNS Server**.

Figure 4-18 DNS Server page



Step 2 Type an IPv4 or IPv6 address.

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

----End

4.2.4 Configuring a Bond

Bond is a method of grouping two or more physical NICs into a logical device with an Ethernet interface that uses an unified IP address.
To create a bond, follow these steps:

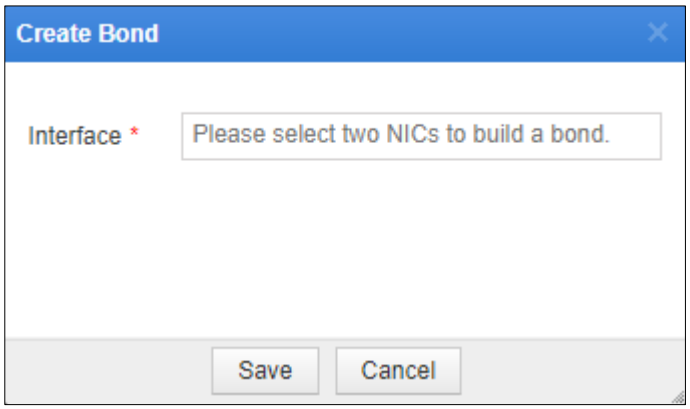
Step 1 Choose **Administration > Network > Bond Configuration**.

Figure 4-19 Creating a bond

Step 2 Create a bond.

Click **Add** and configure parameters in the dialog box shown in Figure 4-20.

Figure 4-20 Creating a bond



Step 3 Select two interfaces to form a bond.

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

----End

4.3 Third-Party Interface

The Third-Party Interface module allows you to configure interfaces for communication with other devices.

This section covers the following topics:

- Email Service: describes how to configure a Simple Mail Transfer Protocol (SMTP) server to send alert messages by email.
- SNMP Service: describes how to configure NTA to be managed via SNMP.
- Syslog Service: describes how to configure NTA to dump logs and alerts to a third-party syslog server.

- SFTP Service: describes how NTA dumps status information to a third-party SFTP server.
- Cloud Platform: describes how to configure NTA to collaborate with NSFOCUS ESPP for reports of the latest threats to the latter.
- Third-Party Cloud Platform: describes how to configure NTA to report the latest threats to the configured third-party cloud platform.
- Cloud Cleaning Platform: describes how to configure NTA to report latest threats to the NSFOCUS cloud cleaning platform.
- BSA Configuration: describes how to configure NTA to collaborate with BSA.
- Management Mode: describes how to configure NTA to be managed by ADS M.
- NTA-ATM: describes how to configure NTA to collaborate with NTA-ATM.

4.3.1 Email Service

To configure the email service, you must perform the following tasks:

- Configuring Mail Settings: Configure parameters for sending logs, alerts, and scheduled reports by email.
- Configuring the Email Template: Configure the header and content of the alert email template.
- Configuring an SMTP Server: Configure an SMTP server for sending email messages.

4.3.1.1 Configuring Mail Settings

This involves the following sub-tasks:

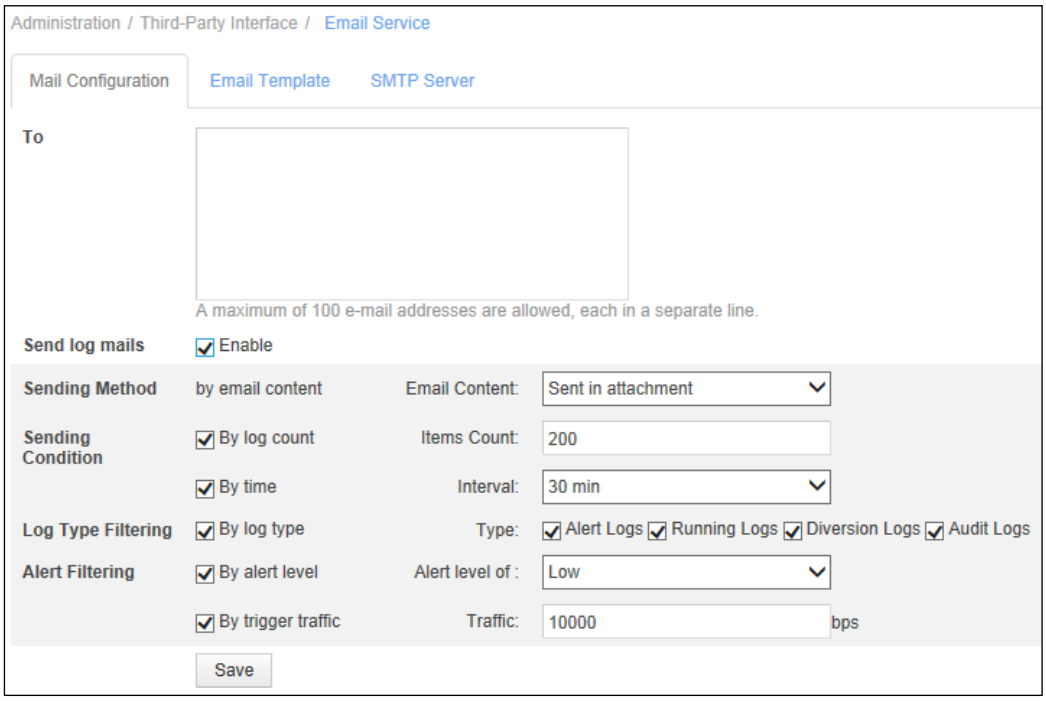
- Email alert configuration: configuration of email addresses to which alerts will be sent
- Log sending configuration: configuration of log sending conditions and alert filtering conditions
- Scheduled alerting configuration: configuration of parameters for generating and sending alerts in a scheduled manner

The procedure is as follows:

Step 1 Choose **Administration** > **Third-Party Interface** > **Email Service**.

The **Mail Configuration** page appears, as shown in Figure 4-21.

Figure 4-21 Mail Configuration page



Step 2 Configure email alert settings.

In the **To** text box, type email addresses to which alerts, logs, and global diversion notifications will be sent.

Step 3 Configure log sending parameters.

Configure log sending conditions and alert filtering conditions in the area shown in Figure 4-22.

Figure 4-22 Log sending configuration area

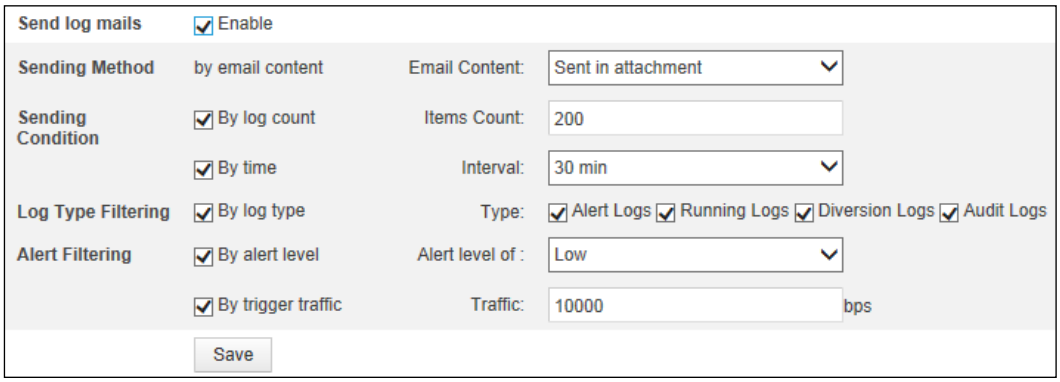


Table 4-4 describes log sending parameters.

Table 4-4 Log sending parameters

Parameter	Description
Send log mails	Controls whether to enable the function of sending logs that meet specified conditions.
Sending Method	Specifies how log contents are sent. It has the following options: • **Sent in the body**: indicates that logs are sent in the body of the email message. • **Sent in attachment**: indicates that logs are sent in the attachment of the email message. • **Sent in both the body and attachment**: indicates that logs are sent in both the body and attachment of the email message.
By log count	Specifies that logs are sent to the specified email addresses when the number of logs generated reaches the specified value of **Items Count**, which is **200** by default.
By time	Specifies that logs are sent at an interval to the specified email addresses. The interval can be **5 min**, **15 min**, **30 min** (default), **1 hr**, **3 hr**, **6 hr**, **12 hr**, or **1 day**.
By log type	Specifies that only logs of the selected types will be sent by email. If this option is disabled, all types of logs will be sent.
By alert level	Specifies that only alerts of the specified level or above will be sent by email. For example, when **Medium** is specified, events of only medium- and high-level risks will be sent.
By trigger traffic	Specifies that alerts are sent to the specified email addresses only when the traffic reaches the specified threshold in bps.

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

----End

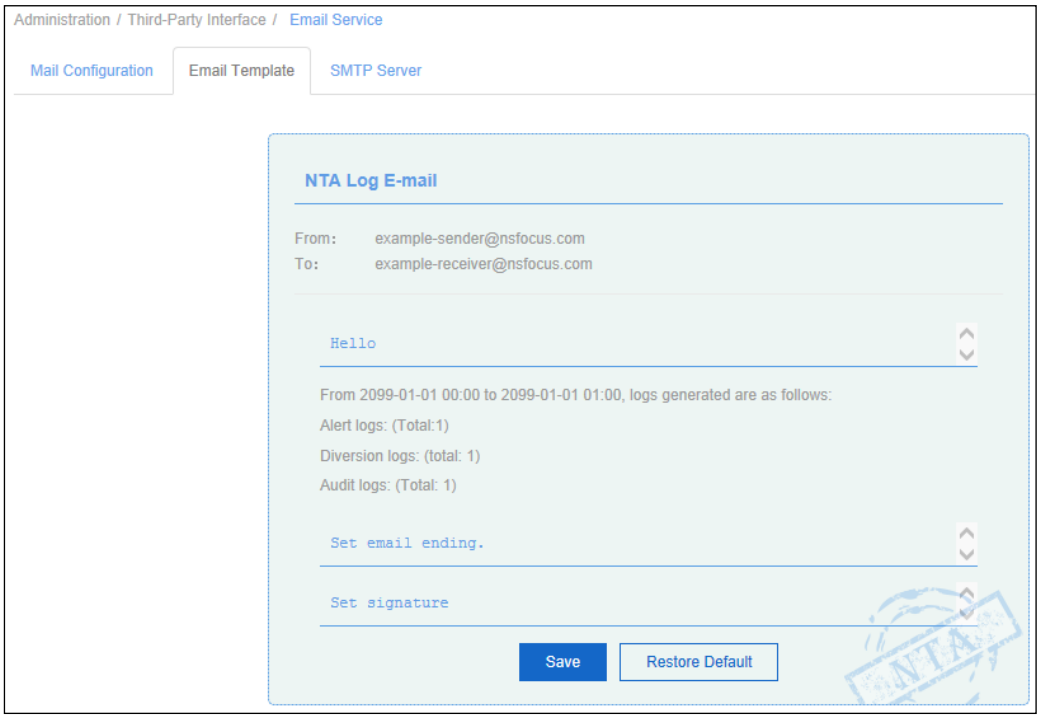
4.3.1.2 Configuring the Email Template

The email template is used to configure the format of alert messages sent by email to the administrator. NTA comes with a default email template, which can be modified as required.

To configure the email template, follow these steps:

Step 1 Choose **Administration** > **Third-Party Interface** > **Email Service** and click **Email Template**.

Figure 4-23 Email Template page



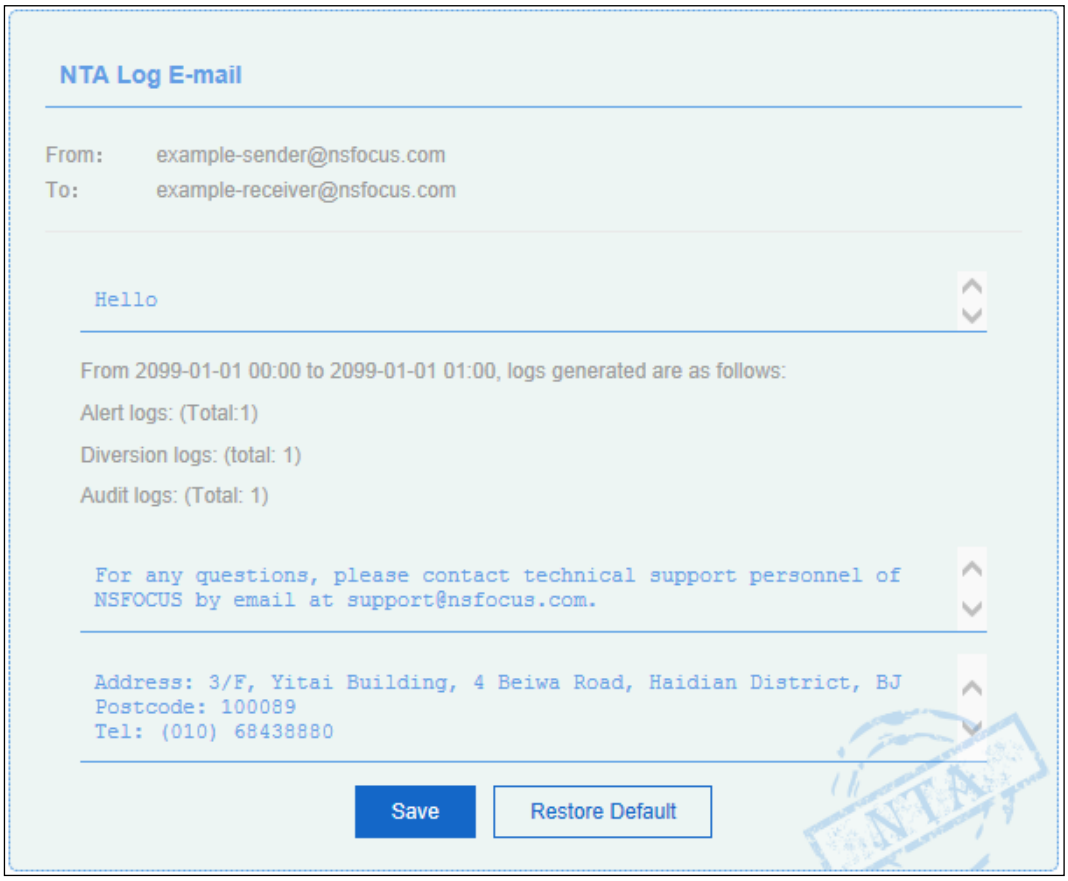
Step 2 Modify the email template.

Information that can be modified is displayed in blue, including:

- Message header: a header that applies to all email messages sent by NTA, which is **NTA Log E-mail** by default
- First line of the email body: generally for salutation, which is **Hello** by default
- Last line of the email body: generally for contact information
- Signature: generally for sender information

After the operation, click **Save**. Figure 4-24 shows the modified email template.

Figure 4-24 Modified email template



Clicking **Restore Default** restores the template to the default one.

----End

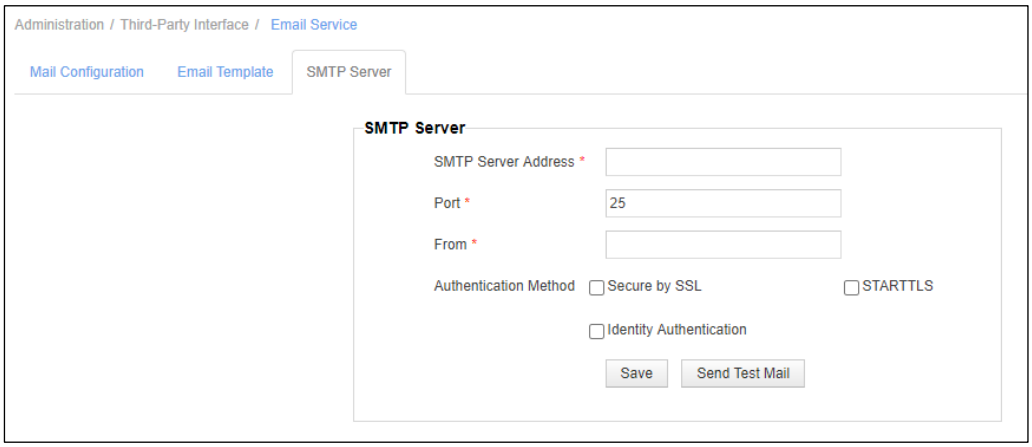
4.3.1.3 Configuring an SMTP Server

An SMTP server can be used for sending alerts by email. To have an SMTP server in place, you must configure the server address, port number, and email address of the sender.

The procedure is as follows:

Step 1 Choose **Administration** > **Third-Party Interface** > **Email Service** and click **SMTP Server**.

Figure 4-25 SMTP Server page



Step 2 Configure parameters.

Figure 4-26 Configuring an SMTP server

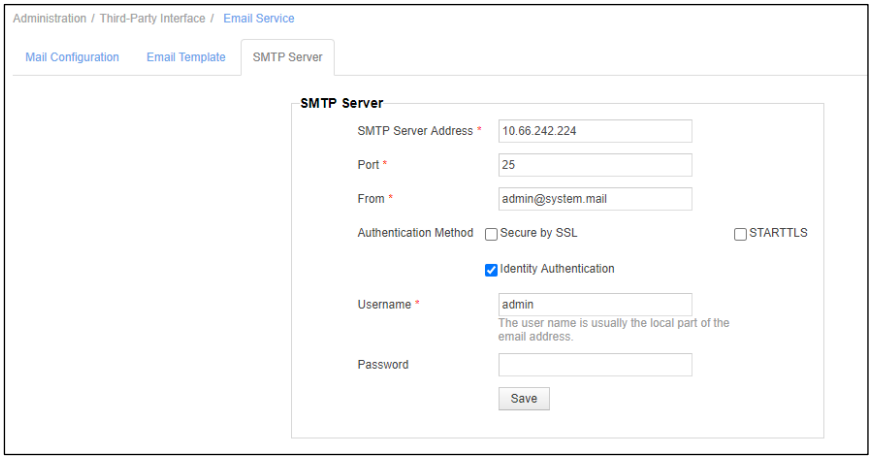


Table 4-5 describes parameters for configuring an SMTP server.

Table 4-5 Parameters for configuring an SMTP server

Parameter	Description
SMTP Server Address	Specifies the IP address or domain name of the server for sending email messages. For IP addresses, you can type either an IPv4 or IPv6 address. This field is mandatory.
Port	Specifies the port number of the SMTP server for sending email messages. The default port is **25**. When **Secure by SSL** is selected, this value automatically changes to **465**. This field is mandatory.
From	Specifies the email address from which logs are sent. This field is mandatory.
Authentication Method	Specifies the authentication method, which can be one of the following:

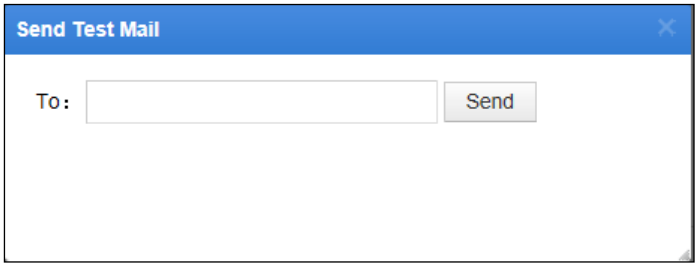
Parameter	Description
	• **Secure by SSL**: If this option is selected, SMTP sessions are encrypted via SSL. This field is available only when you select **Identity Authentication**. • **STARTTLS**: If this option is selected, emails are sent via StartTLS. **Identity Authentication**: If this option is selected, you need to configure the user name and password for sending email messages.
Username/Password	Specifies the user name and password for sending email messages. These two fields are available only when you select **Identity Authentication**.

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

Step 4 Test parameter settings.

a. After the SMTP server is configured, with **Identity Authentication** unchecked, you can click **Send Test Mail** to check whether parameter settings are correct. In the dialog box shown in Figure 4-27, type the email addresses for receiving the test mail.

Figure 4-27 Send Test Mail dialog box



b. Click **Send**. NTA will send the test mail to all the specified email addresses and to the address typed in the **From** field as well if the parameters are correctly set.

Tip	When SMTP server settings are being edited, you are not allowed to send a test mail. The **Send Test Mail** button is available only after you complete the editing and save the changes.

----End

4.3.2 SNMP Service

The Simple Network Management Protocol (SNMP) service is used to configure related parameters for NTA to accept management by third-party SNMP software (network management station, NMS). SNMP configuration involves the following sub-tasks:

- Enable and configure the SNMP service on NTA.
- Download the MIB library from NTA and import it to NMSs.
- Configure trusted NMSs.

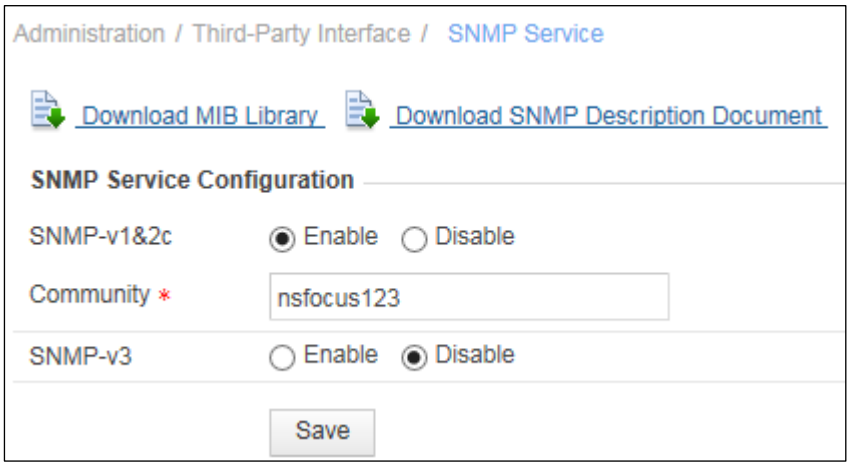
To configure the SNMP service, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > SNMP Service**.

Step 2 Configure the SNMP service.

NTA can be managed and monitored through SNMPv1, SNMPv2c, or SNMPv3.

Figure 4-28 Configuring the SNMP v1/v2c service



a. Enable SNMPv1/v2c by selecting **Enable** for **SNMP-v1&2c**, as shown in Figure 4-28.

   By default, SNMPv1/v2c-based traffic monitoring is enabled on NTA. You can enable or disable this function as required.

   After SNMPv1/v2c is enabled, you must configure **Community**. The community string configured here must be the same as the read-only community string on the NMS; otherwise, NTA could not communicate with NMS. The default value is **public**.

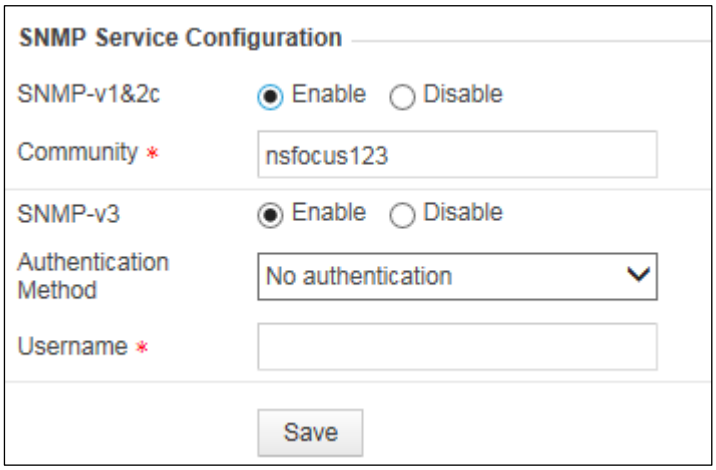
   Set parameters and click **Save** to commit the settings.

b. Alternatively, enable SNMPv3 by selecting **Enable** for **SNMP-v3**.

   By default, SNMPv3-based traffic monitoring is disabled on NTA, as shown in Figure 4-28. You can enable or disable this function as required.

Figure 4-29 shows the area displayed after SNMPv3 is enabled.

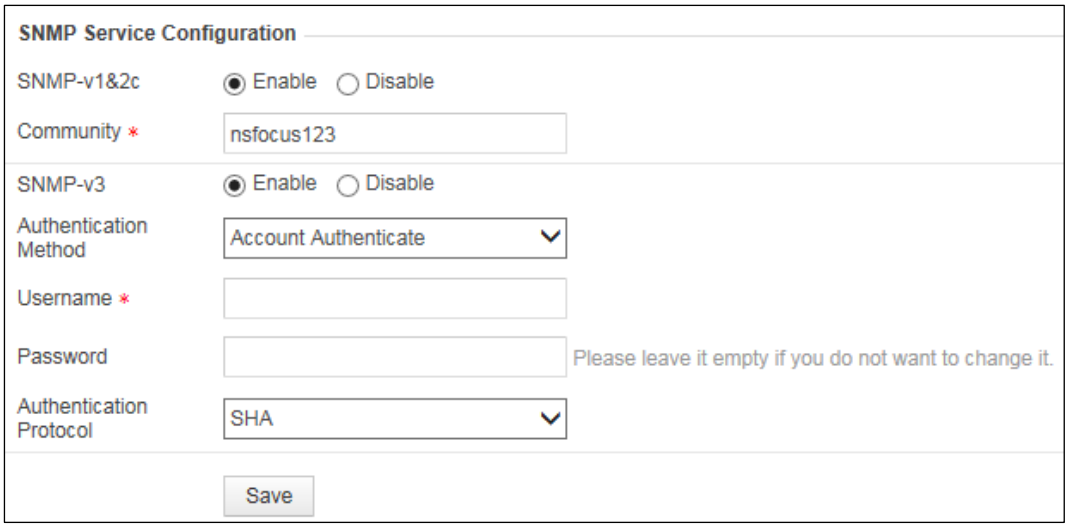
Figure 4-29 Configuring the SNMPv3 service



SNMPv3 supports three authentication methods: **No authentication**, **Account Authenticate**, and **Private Key Authenticate**. The default value is **No authentication**. Parameters vary with the authentication method.

- **No authentication**: indicates that no authentication is performed. In this case, authentication and encryption functions are unavailable. As shown in Figure 4-29, you need to type only the user name for this method.
- **Account Authenticate**: indicates that authentication based on HMAC-MD5 or HMAC-SHA is adopted. In this case, the encryption function is still unavailable. As shown in Figure 4-30, you need to select an authentication protocol and type the user name and password for this method.

Figure 4-30 Configuring account-based authentication parameters



- **Private Key Authenticate**: indicates that private key-based authentication is adopted. In this case, data is also encrypted with the Data Encryption Standard (DES) algorithm for transmission, ensuring the privacy of data. As shown in Figure 4-31, you need to type the user name and password and specify the private key password for this method.

Figure 4-31 Configuring private key-based authentication parameters

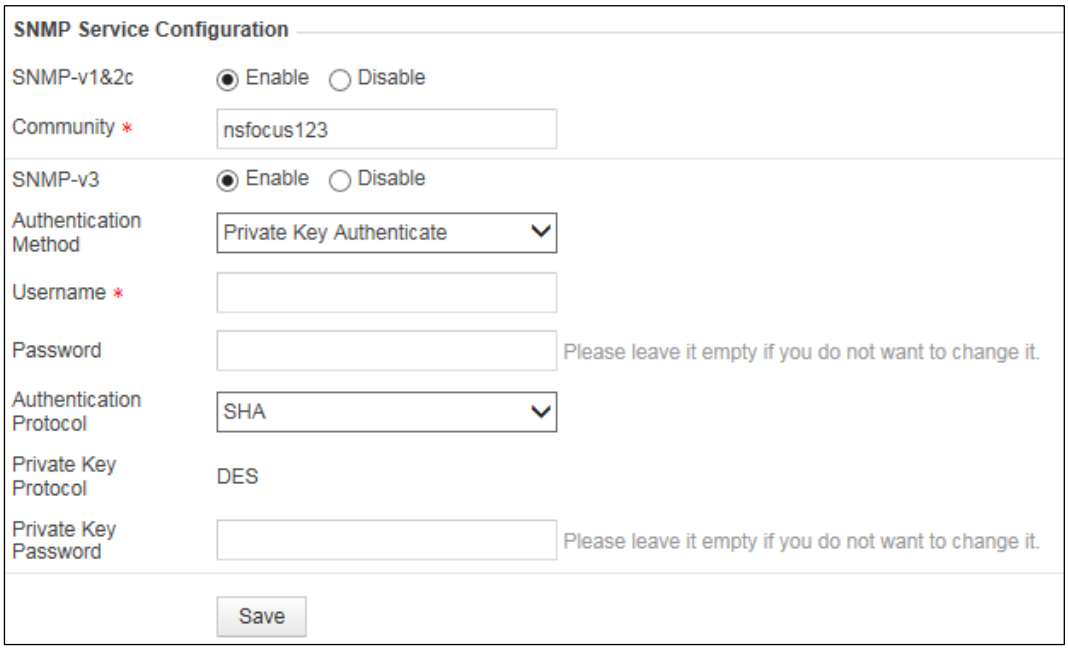


Table 4-6 describes parameters for the three authentication methods of SNMPv3.

Table 4-6 SNMPv3 service configuration parameters

Parameter	Description
Authentication Method	Specifies an authentication method. It has the following values: • **No authentication**: no authentication required • **Account Authenticate**: only authentication required • **Private Key Authenticate**: authentication and encryption required The default authentication method is **No authentication**.
Username	Specifies the user name of the SNMP service user.
Password	Specifies the password for generating the authentication key.
Authentication Protocol	Specifies the authentication protocol, which can be **MD5** or **SHA**. This parameter is available when you select **Account Authenticate** or **Private Key Authenticate** for **Authentication Method**.
Private Key Protocol	Specifies an encryption protocol. Currently, NTA supports only the DES symmetric encryption algorithm. This parameter is available when you select **Private Key Authenticate** for **Authentication Method**.
Private Key Password	Specifies the password for generating a private key for encryption and decryption protocols. This parameter is available when you select **Private Key Authenticate** for **Authentication Method**.

Set parameters and click **Save** to commit the settings.

Step 3 Download the MIB library.

On the page shown in Figure 4-28, you can click **Download MIB Library** and **Download SNMP Description Document** to download the corresponding document to a local disk drive.

Step 4 To manage and monitor NTA, you must download the MIB library from NTA and then import it to NMS configured in step 4.Configure a trusted NMS.

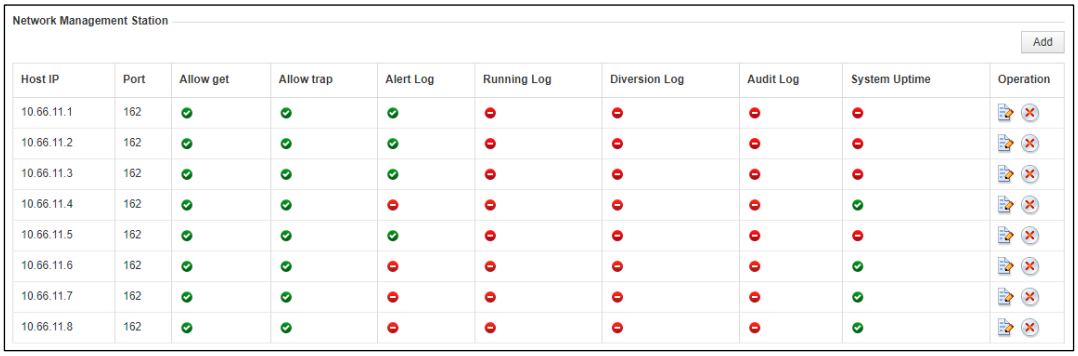
After the SNMP service is enabled on NTA, it does not mean NTA will accept management from all NMSs. Actually, NTA accepts management only from trusted NMSs. For this purpose, you need to configure a list of trusted NMSs to:

- Put NTA under management of these NMSs
- Allow or not allow NTA to send trap messages to a specified NMS
- Allow or not allow NTA to accept GET requests from a specified NMS

Note	You also need to import the MIB library of NTA to NMSs so that NMSs can obtain NTA basic information via the GET method and receive Trap messages from NTA.

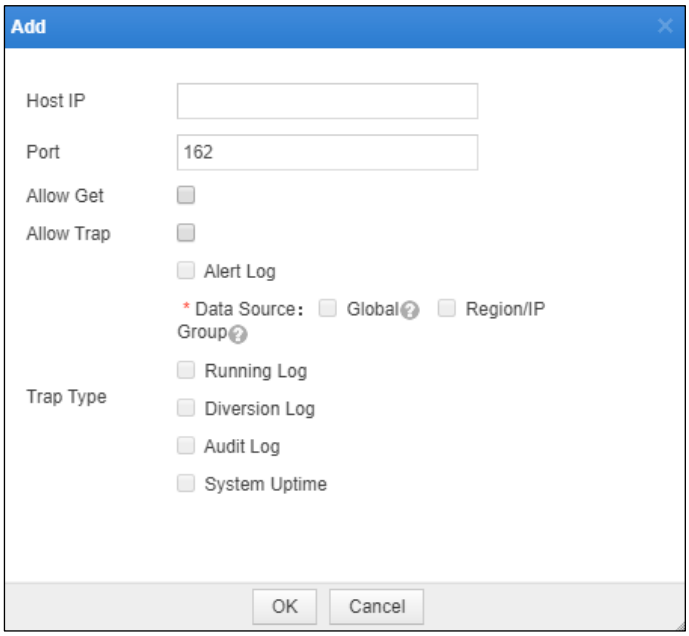
Figure 4-32 shows the area for configuring a trusted NMS.

Figure 4-32 Network Management Station area



a. Click **Add**.

Figure 4-33 Configuring a trusted NMS



b. In the **Add** dialog box, configure parameters.

Table 4-7 Parameters for configuring a trusted NMS

Parameter	Description
Host IP	Specifies the IP address of the trusted NMS.
Port	Specifies the port of the trusted NMS. The value range is 1–65535.
Allow Get	Controls whether to allow this NMS to obtain product information and performance information, such as CPU usage, memory usage, and disk usage, of NTA by using the GET method. If you need to use the OID value of NTA, contact NSFOCUS technical support.
Allow Trap	Controls whether NTA automatically sends trap messages to NMS. After this is enabled, NTA automatically sends a trap message when a log is generated.
Trap Type	Specifies the types of logs that NTA sends to NMS via trap messages. After it is enabled, NTA automatically sends a trap message when a log of a specified type is generated. This field is available only when the **Allow Trap** check box is selected.

c. Click **OK**.

----End

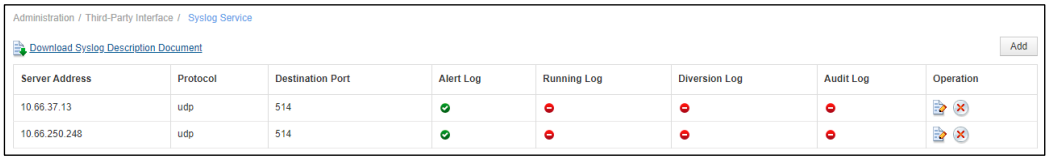
4.3.3 Syslog Service

On NTA, certain logs can be dumped to a syslog server. For this purpose, you must configure a syslog server and specify the types of logs to be dumped in advance.

The procedure is as follows:

Step 1 Choose **Administration > Third-Party Interface > Syslog Service**.

Figure 4-34 Syslog Service page



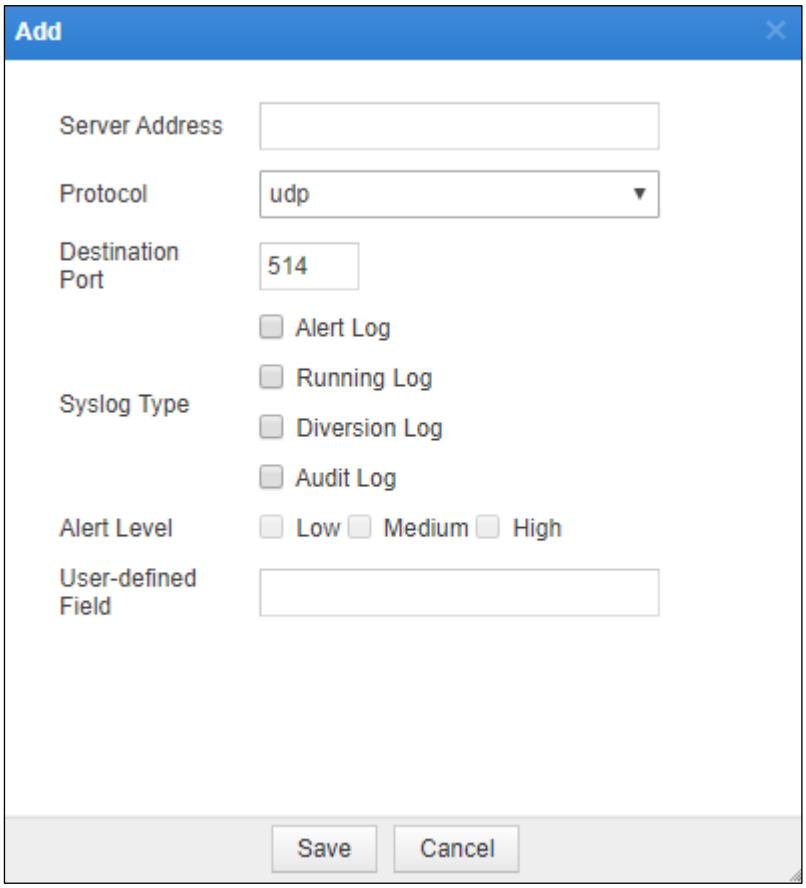
Step 2 Download the syslog description document.

On the page shown in Figure 4-34, you can click **Download Syslog Description Document** to download the corresponding document to a local disk drive for reference in the case of adding a syslog server.

Step 3 Configure a syslog server.

a. Click **Add**.

Figure 4-35 Configuring a syslog server



b. In the **Add** dialog box, configure parameters.

Table 4-8 Parameters for configuring a syslog server

Parameter	Description
Server Address	Specifies the IP address of the syslog server.
Protocol	Specifies the protocol type that the syslog server uses to provide the service, which can be **udp** or **tcp**.
Destination Port	Specifies a port for the syslog server to receive logs. The default port is **514**.
Syslog Type	Specifies the types of logs to be dumped to the syslog server. You must select at least one type.
Alert Level	Specifies which levels of alert will be sent to the syslog server. This field is available only when **Syslog Type** is set to **Alert Logs**.
User-defined Field	Specifies the custom contents to be sent to the syslog server.

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

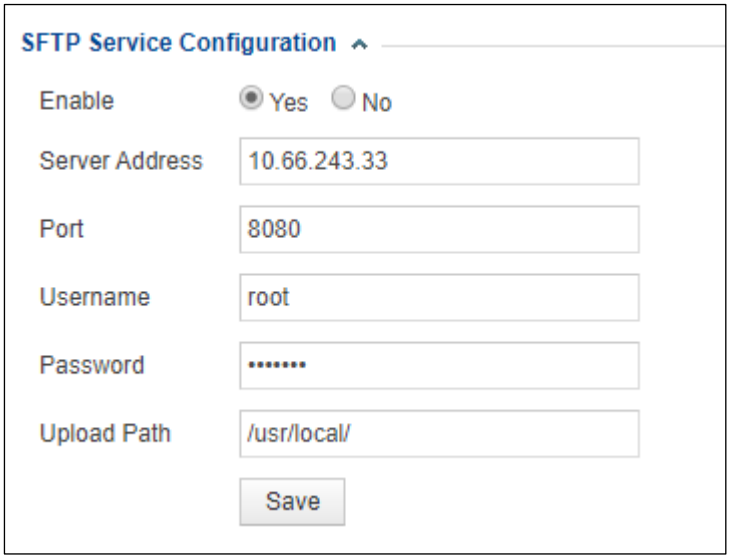
----End

4.3.4 SFTP Service

After the SFTP service is configured and enabled, the background program of NTA will automatically send status information to the specified SFTP server.
To configure the SFTP service, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > SFTP Service**.

Figure 4-36 SFTP Service Configuration page



Step 2 Configure SFTP service parameters.

Table 4-9 Parameters for configuring the SFTP service

Parameter	Description
Enable	Determines whether to enable the SFTP service.
Server Address	Specifies the IP address of the SFTP server. Only IPv4 addresses are allowed here.
Port	Specifies the port used by the SFTP server to receive status information.
Username/Password	Specifies the user name and password used for login to the SFTP server. This account must have the read/write access to the SFTP server.
Upload Path	Specifies the directory on the SFTP server where the received status information is stored. If the root directory is used to save logs, type /.

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

----End

4.3.5 Cloud Platform

After the cloud platform is enabled and NSFOCUS ESPP is configured, the background program of NTA will automatically upload log files (including alerts and performance information) to NSFOCUS ESPP as long as NTA can properly connect to the latter. Upon detection of a problem with NTA, NSFOCUS ESPP immediately notifies the technical support personnel, thereby guaranteeing the security of customers' networks.

To configure a cloud platform, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > Cloud Platform**.

Figure 4-37 Cloud Platform page

Step 2 Configure parameters.

Table 4-10 Parameters for configuring a cloud platform

Parameter	Description
Enable	Controls whether to enable NTA to connect to NSFOCUS ESPP.

Parameter	Description
ESPP Address *X*	Specifies the IP address of NSFOCUS ESPP that can properly communicate with NTA. For the IP address of NSFOCUS ESPP, contact NSFOCUS technical support.

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

When NTA properly connects to the configured cloud platform, the indicator on the right of the IP address is green; otherwise, it is red.

----End

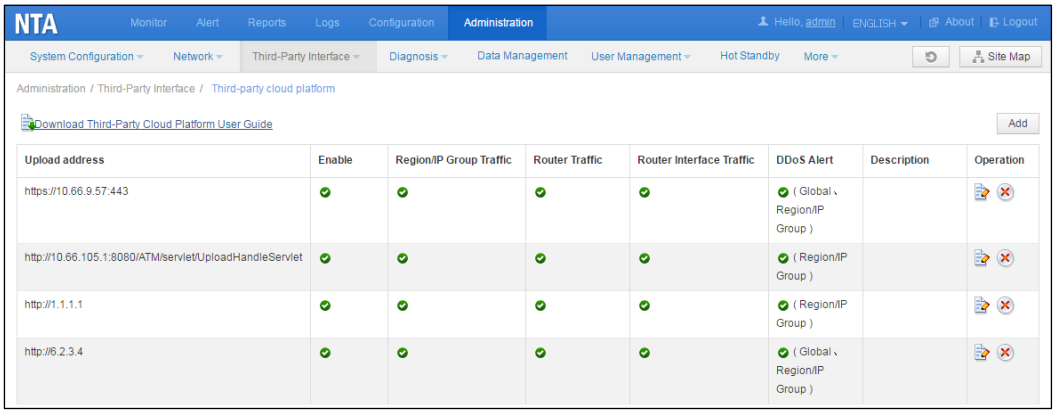
4.3.6 Third-Party Cloud Platform

After the third-party cloud platform is configured and enabled, the background program of NTA will automatically uploads log files (including alert and performance information) and traffic data to the third-party cloud platform only if NTA properly connects to this platform.

To configure a third-party cloud platform, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > Third-Party Cloud Platform**.

Figure 4-38 Third-party cloud platform page



To delete a connection, click in the **Operation** column.

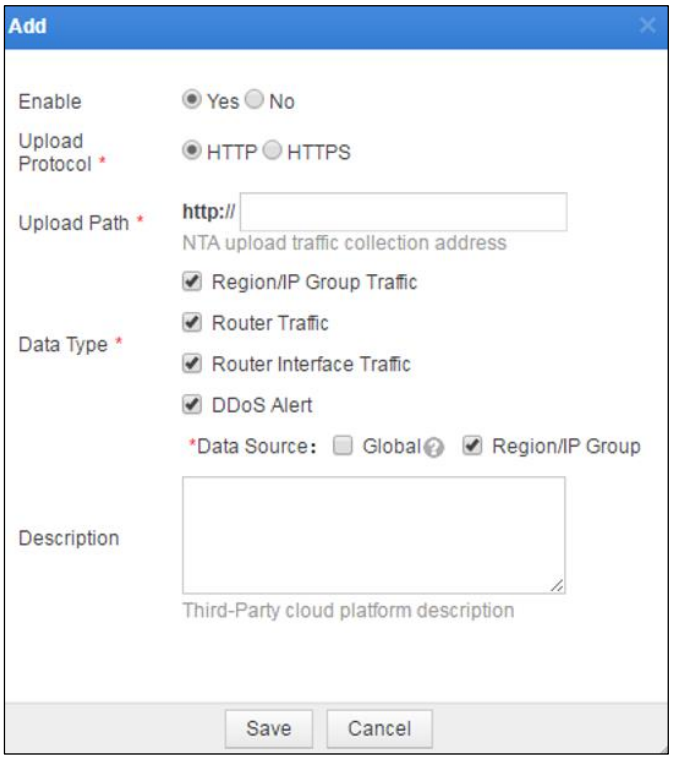
To modify a connection, click in the **Operation** column.

Step 2 Download the third-party cloud platform user guide.

On the page shown in Figure 4-38, you can click **Download Third-Party Cloud Platform User Guide** to download the corresponding document to a local disk drive for reference in the case of adding a third-party cloud platform.

Step 3 Click **Add** in the upper-right corner of the page.

Figure 4-39 Adding a third-party cloud platform



Step 4 Configure parameters in the **Add** dialog box.

Table 4-11 Parameters for configuring a third-party cloud platform

Parameter	Description
Enable	Controls whether to enable NTA to connect to the third-party cloud platform.
Upload Protocol	Specifies the protocol for uploading data.
Upload Path	Specifies the URL of the third-party cloud platform.
Data Type	Specifies the type of data to be uploaded to the third-party cloud platform.
Data Source	Specifies data sources of DDoS alerts. It has the following values: • **Global**: uploads DDoS alerts from all possible sources. • **Region/IP Group**: uploads DDoS alerts only from regions and IP groups. **Note** Use of global sources may overload the third-party system with too much data.
Description	Brief description of the third-party cloud platform.

Step 5 Click **Save** to commit the settings.

----End

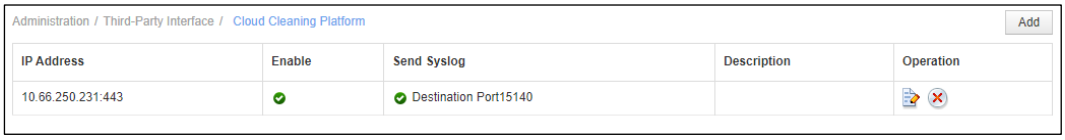
4.3.7 Cloud Cleaning Platform

After the cloud cleaning platform is configured and enabled, the background program of NTA will automatically uploads log files (including alert and performance information) and traffic data to the cloud cleaning platform only if NTA properly connects to this platform.

To configure a cloud cleaning platform, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > Cloud Cleaning Platform**.

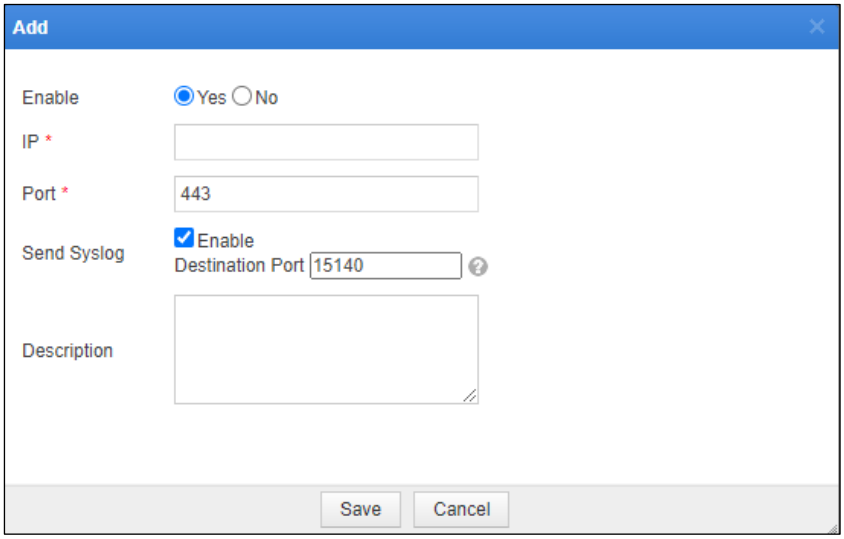
Figure 4-40 Cloud Cleaning Platform page



- To delete a connection, click in the **Operation** column.
- To modify a connection, click in the **Operation** column.

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

Figure 4-41 Adding a cloud cleaning platform



Step 3 Configure parameters in the **Add** dialog box.

Table 4-12 Parameters for configuring a cloud cleaning platform

Parameter	Description
Enable	Controls whether to enable NTA to connect to the cloud cleaning platform.
IP	Specifies the IP address used by the cloud cleaning platform to communicate with NTA. For the IP address of the cloud cleaning platform, contact NSFOCUS technical support.

Parameter	Description
Port	Specifies the port used by the cloud cleaning platform to connect to NTA. The value range is 1–65535. For the port of the cloud cleaning platform, contact NSFOCUS technical support.
Send Syslog	Controls whether to send logs via syslog. This function is disabled by default. After it is enabled, the system regularly collects alerts and sends them to the cloud cleaning platform. The default destination port is **15140**.
Description	Brief description of the cloud cleaning platform.

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

----End

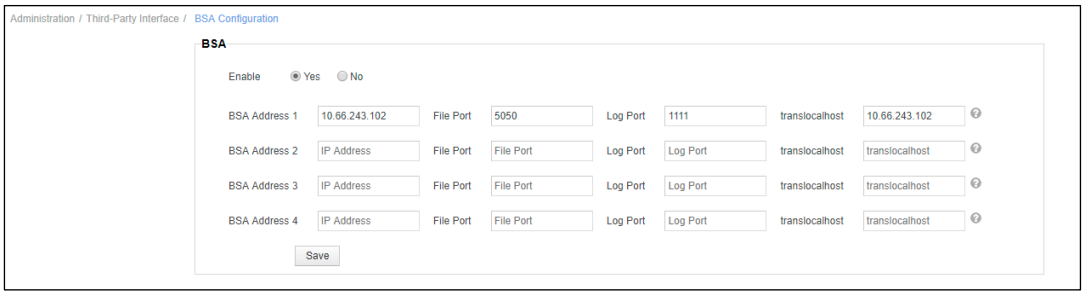
4.3.8 BSA Configuration

After BSA configuration is configured and enabled, the background program of NTA will automatically uploads log files (including alert and performance information) to BSA only if NTA properly connects to BSA.

To configure BSA, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > BSA Configuration**.

Figure 4-42 BSA Configuration page



Step 2 Configure parameters.

Table 4-13 BSA configuration parameter

Parameter	Description
Enable	Controls whether to enable NTA to connect to BSA.
BSA Address X	Specifies the IP address of BSA, making sure that NTA can properly communicate with BSA. For the IP address of BSA, contact NSFOCUS technical support.
File Port	Port for transmitting files to NTA.
Log Port	Port for transmitting logs to NTA.
translocalhost	When BSA works in a NAT environment, this parameter is set to **127.0.0.1**; otherwise, it is set to the IP address BSA uses to collaborate with NTA.

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

----End

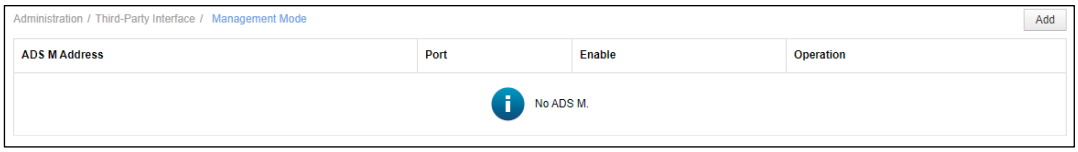
4.3.9 Management Mode

When used for abnormal traffic detection, NTA can be managed by NSFOCUS ADS M to provide real-time traffic monitoring for traffic cleaning objects. **At most five ADS M devices can be added.**

To enable NTA to be managed by NSFOCUS ADS M, follow these steps:

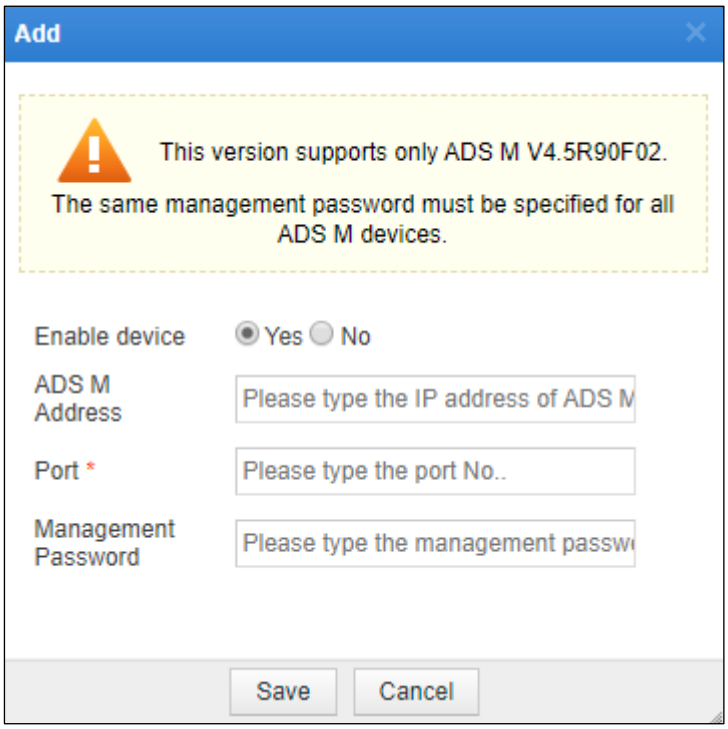
Step 1 Choose **Administration > Third-Party Interface > Management Mode**.

Figure 4-43 ADS M list



Step 2 Click **Add**.

Figure 4-44 Configuring the management mode



Step 3 In the **Add** dialog box, configure parameters.

Table 4-14 Parameters for configuring ADS M

Parameter	Description
Enable device	Controls whether to enable NTA to connect to ADS M. Initially, this is disabled. You need to click **Yes** to enable this function.
ADS M Address	Specifies the IP address of ADS M, which can be an IPv4 or IPv6 address.
Port	Specifies the port used by ADS M to connect NTA.
Management Password	Specifies a password for authentication of ADS M. This password must be the same on both sides.

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

----End

4.3.10 NTA-ATM

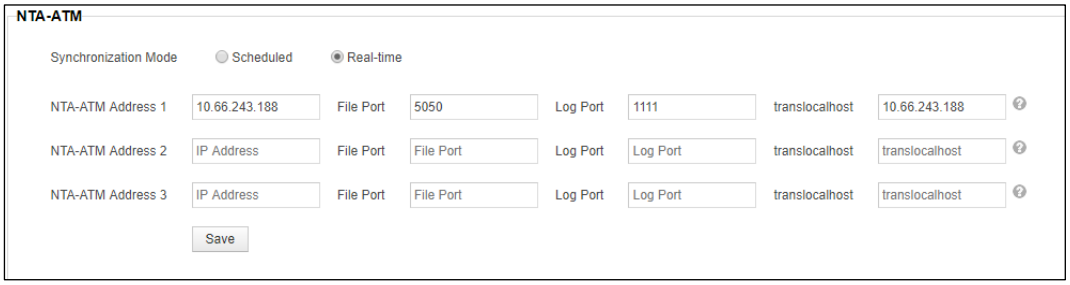
NTA-ATM stands for NSFOCUS Network Traffic Analyzer–Attack Trend Monitoring System. NTA can collaborate with NTA-ATM, which obtains data from NTA in an unsolicited manner to inform administrators of the attack situation in the network, making security O&M easy and convenient. For this purpose, you need to configure parameters on both NTA and NTA-ATM. Here only the method of configuring related parameters on NTA is described. For the configuration method on NTA-ATM, see the *NSFOCUS NTA-ATM User Guide*.

To configure the collaboration with NTA-ATM, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > NTA-ATM**.

a. For the synchronization mode, select **Real-time** to enable data to be synchronized from NTA to NTA-ATM every 30 seconds.

Figure 4-45 Page for configuring real-time synchronization with NTA-ATM



b. Configure parameters.

Table 4-15 Paramters for configuring real-time synchronization with NTA-ATM

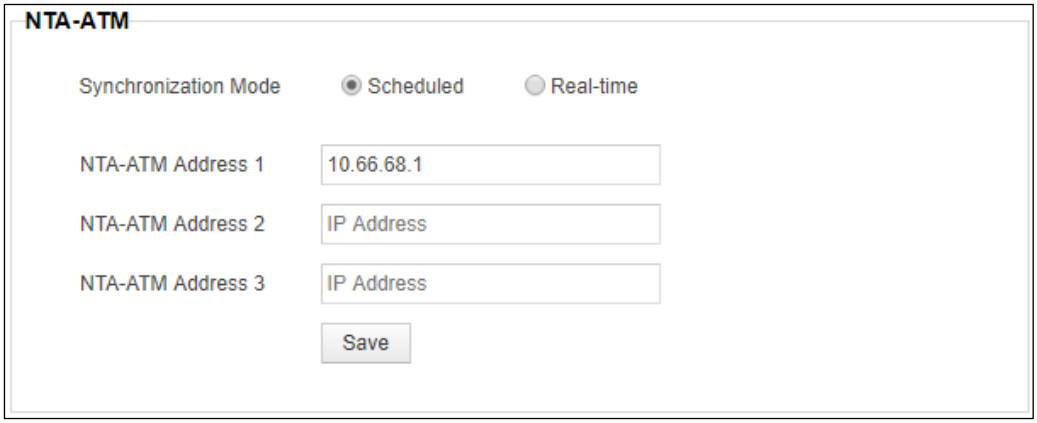
Parameter	Description
Synchronization Mode	Specifies the synchronization mode. Here **Real-time** should be selected.
NTA-ATM Address *X*	Specifies the IP address of NTA-ATM, which must be reachable for NTA.

Parameter	Description
	For the IP address of NTA-ATM, contact NSFOCUS technical support.
File Port	Specifies a port for transmission of files to NTA-ATM.
Log Port	Specifies a port for transmission of logs to NTA-ATM.
translocalhost	When NTA-ATM works in a NAT environment, this parameter should be set to **127.0.0.1**; otherwise, it should be the IP address of NTA-ATM.

c. (Optional) For scheduled synchronization, on the **NTA-ATM** page, select **Scheduled** as the synchronization mode.

In this mode, data is synchronized from NTA to NTA-ATM every 5 minutes.

Figure 4-46 Page for configuring scheduled synchronization with NTA-ATM



d. (Optional) Configure the IP address of NTA-ATM.

At most three can be configured.

Step 2 Click **Save** to commit the settings.

----End

4.4 Diagnosis

Choose **Administration > Diagnosis**. NTA provides the following tools:

- Ping
- Traceroute
- Snmpwalk
- Tcpdump
- Telnet
- Fault Diagnosis

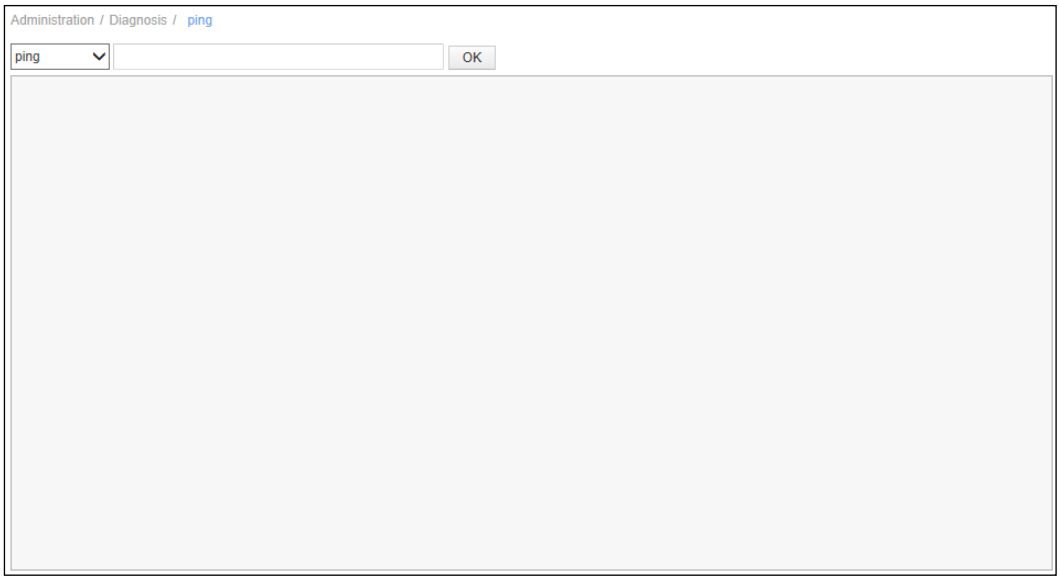
4.4.1 Ping

Ping is used to check whether a host is alive or connects to the network.

The procedure is as follows:

Step 1 Choose **Administration > Diagnosis > ping**.

Figure 4-47 ping page



Step 2 Select **ping** or **ping6** from the drop-down list, type a domain name or an IPv4/IPv6 address in the text box on the right, and then click **OK**.

The ping result is displayed in the text box below.

----End

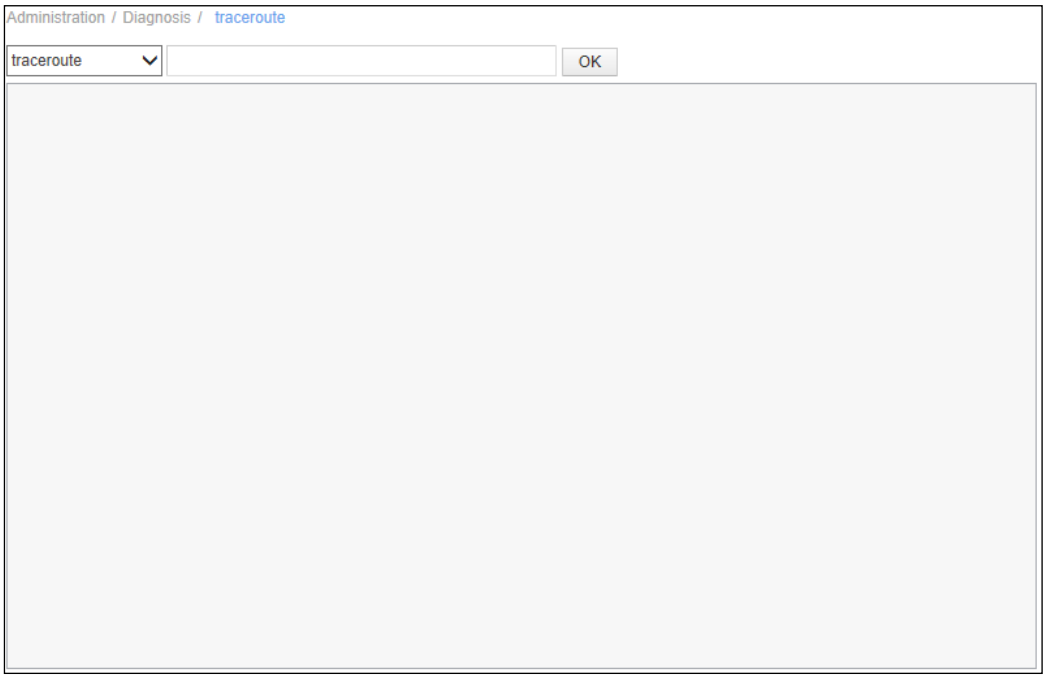
4.4.2 Traceroute

Traceroute is used to check network routing.

The procedure is as follows:

Step 1 Choose **Administration > Diagnosis > traceroute**.

Figure 4-48 traceroute page



Step 2 Select **traceroute** or **traceroute6** from the drop-down list, type an IPv4 or IPv6 address in the text box on the right, and then click **OK**.

The traceroute result is displayed in the text box below.

----End

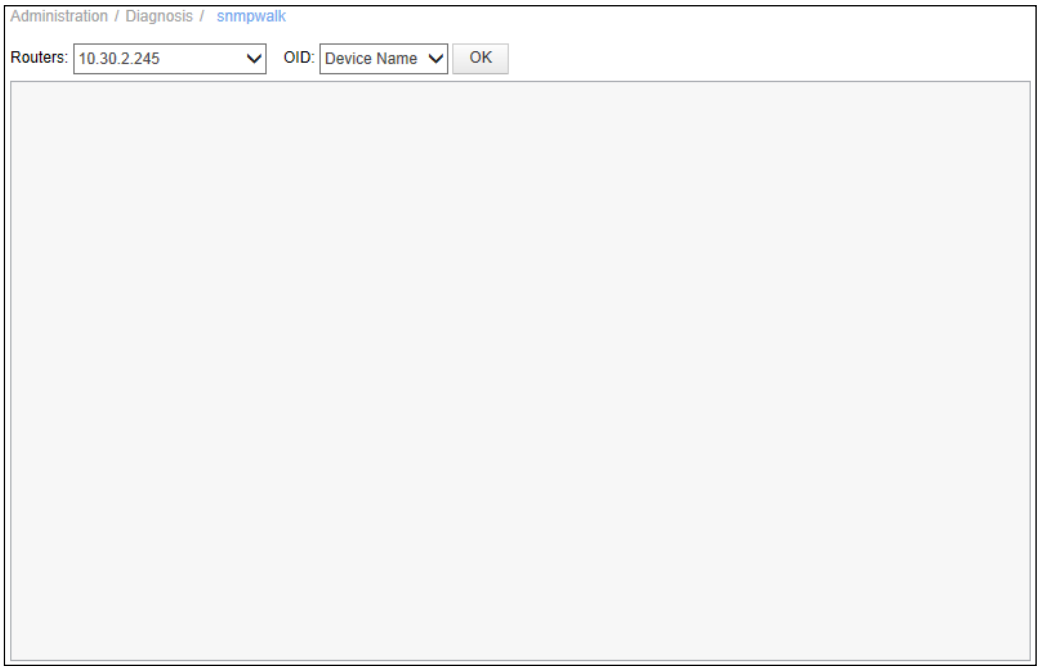
4.4.3 **Snmpwalk**

Snmpwalk is used to retrieve MIB object IDs (OIDs) on a routing device.

The procedure is as follows:

Step 1 Choose **Administration > Diagnosis > snmpwalk**.

Figure 4-49 snmpwalk page



Step 2 Select a router from the **Routers** drop-down list, select an OID, and then click **OK**.

The snmpwalk result is displayed in the text box below.

----End

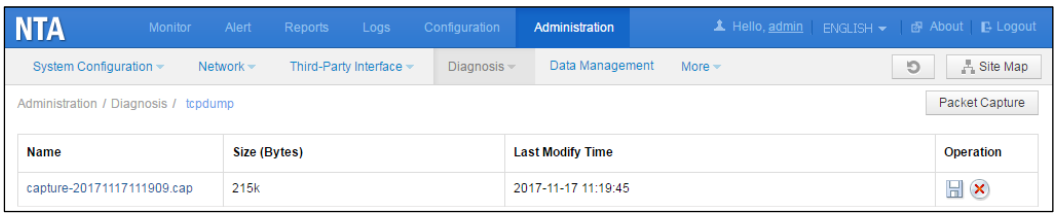
4.4.4 Tcpdump

Tcpdump is used to intercept and analyze packets being transmitted or received over a network as defined by a user. The user can check the status of and troubleshoot network interface cards (NICs) based on such analysis.

The procedure is as follows:

Step 1 Choose **Administration > Diagnosis > tcpdump**.

Figure 4-50 tcpdump page



Step 2 Capture packets.

a. Click **Packet Capture**. In the dialog box that appears, select **Pattern 1** or **Pattern 2**.

Figure 4-51 shows parameters for pattern 1.

Figure 4-51 Selection of pattern 1

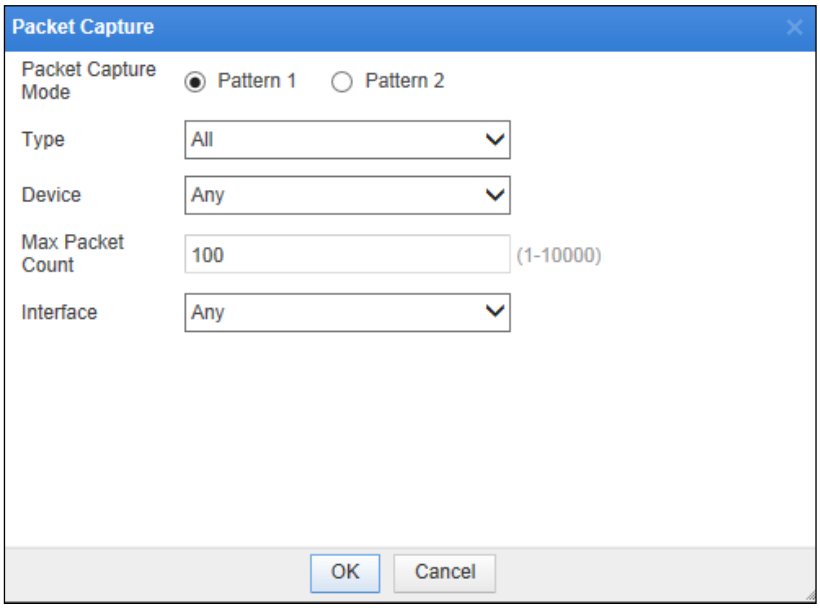


Table 4-16 describes parameters for packet capture pattern 1.

Table 4-16 Parameters for packet capture pattern 1

Parameter	Description
Type	Specifies the type of packets to be captured. You can select **All**, **Netflow**, **NetStream**, **sFlow**, **IPFIX**, **SNMP**, or **BGP**.
Device	Specifies the routing device from which packets will be captured.
Max Packet Count	Specifies the maximum number of packets to be captured. The value ranges from 1 to 10000.
Interface	Specifies the interface through which packets will be captured. You can select an enabled network interface from the drop-down list.

Figure 4-52 shows parameters for pattern 2.

Figure 4-52 Selection of pattern 2

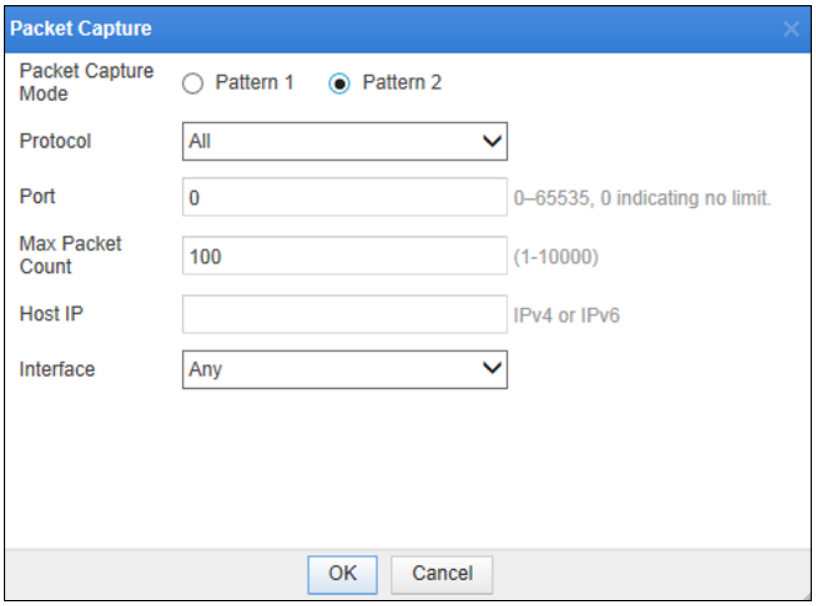


Table 4-17 describes parameters for packet capture pattern 2.

Table 4-17 Parameters for packet capture pattern 2

Parameter	Description
Protocol	Specifies a protocol so that packets transmitted by using this protocol will be captured. You can select **All**, **TCP**, **UDP**, or **ICMP**.
Port	Specifies the transport-layer port so that packets transmitted through this port will be captured.
Max Packet Count	Specifies the maximum number of packets to be captured. The value ranges from 1 to 10000.
Host IP	Specifies the destination IP address so that packets with this destination IP address will be captured. You can type either an IPv4 or IPv6 address. No value indicates all IP addresses.
Interface	Specifies the interface through which packets will be captured. You can select an enabled network interface from the drop-down list.

b. Configure parameters and click **OK**. The tool then captures packets as specified and saves them in a .cap file, which is displayed in the list.

Step 3 Download the packet capture file.

In the list, click the file name or click in the **Operation** column to download the file. This file can be opened with Ethereal or Wireshark.

Step 4 Delete the packet capture file.

In the list, click in the **Operation** column to delete the file.

Note	Packet capture files of ongoing tasks cannot be deleted.

----End

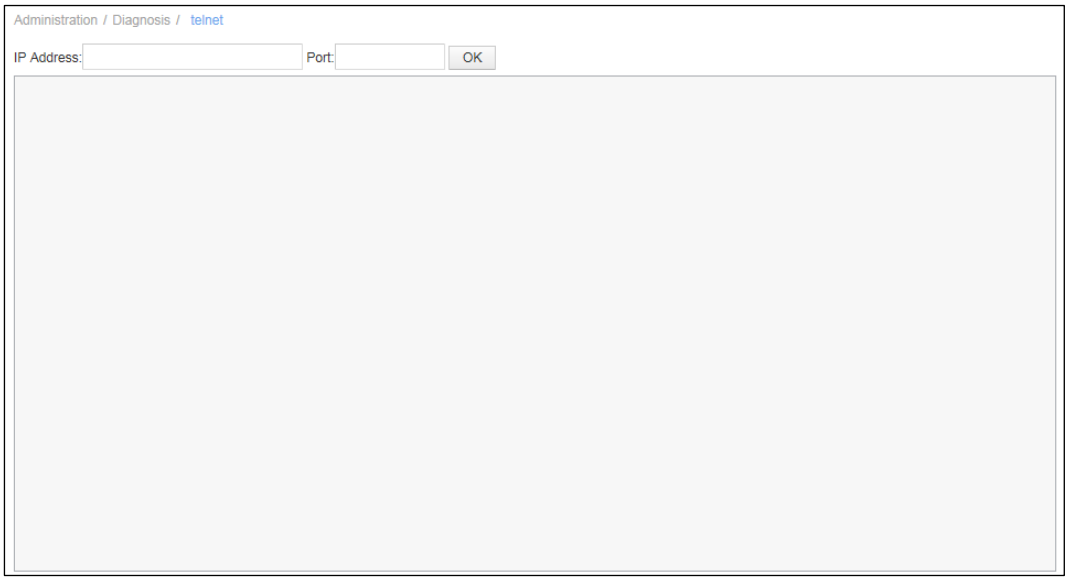
4.4.5 Telnet

When NTA collaborates with other devices or sends data to other devices, you can use Telnet to check whether the peer port is reachable, so as to verify whether a firewall is configured or whether certain services are disabled on the peer device.

To use this function, follow these steps:

Step 1 Choose **Administration > Diagnosis > telnet**.

Figure 4-53 Telnet page



Step 2 Type an IPv4 or IPv6 address and a port number, and then click **OK**.

The Telnet result is displayed in the text box below.

----End

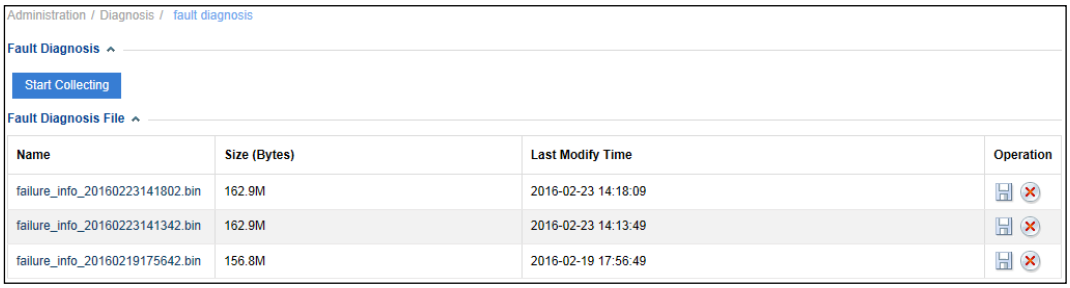
4.4.6 Fault Diagnosis

NTA provides such functions as one-click fault collection and upload of encrypted fault information. NSFOCUS technical support can locate and troubleshoot faults according to the collected data.

To use this function, follow these steps:

Step 1 Choose **Administration > Diagnosis > fault diagnosis**.

Figure 4-54 Fault diagnosis page

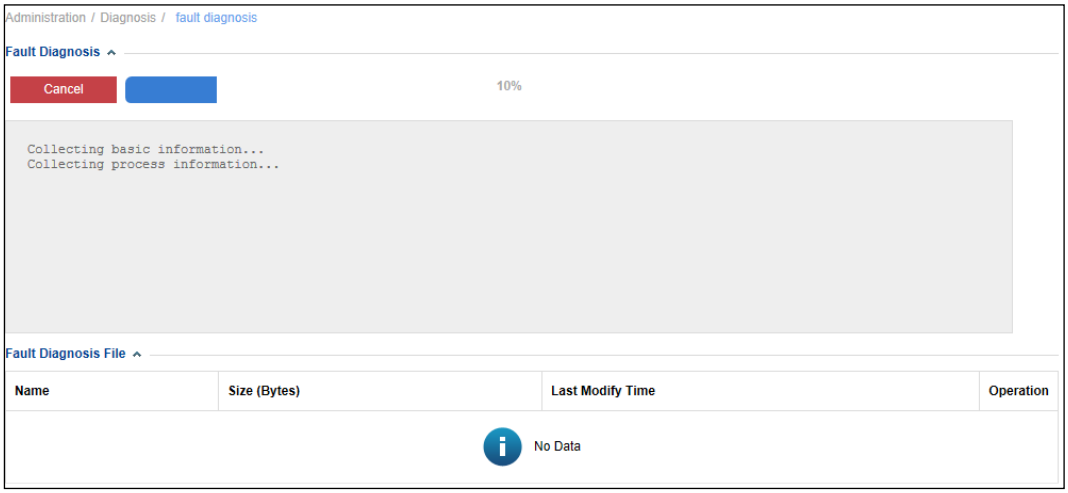


In the **Fault Diagnosis File** area, historical fault diagnosis files are listed. A maximum of three files can be saved. If there are already three fault diagnosis files, the new fault diagnosis file will overwrite the earliest one.

Step 2 Click **Start Collecting**.

The progress and details of fault collection are displayed, as shown in Figure 4-55.

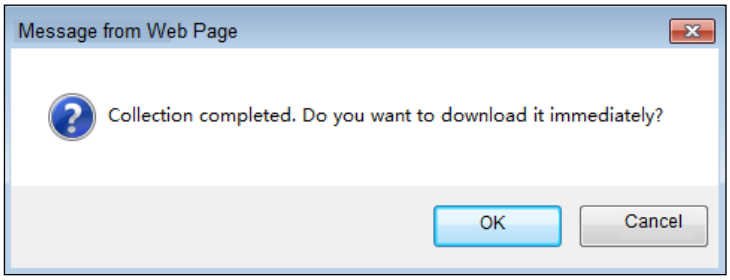
Figure 4-55 Fault collection progress



Step 3 Download fault collection information.

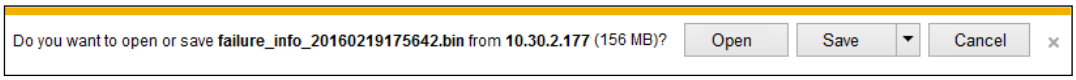
After fault collection is complete, the system prompts a message, as shown in Figure 4-56.

Figure 4-56 Message prompting the completion of fault collection



- Clicking **Cancel** returns you to the fault diagnosis page. In the **Fault Diagnosis File** area, click a file name or click in the **Operation** column. In the dialog box shown in Figure 4-57, specify a path to save the fault diagnosis file.
- Clicking **OK** displays a dialog box for saving the fault diagnosis file, as shown in Figure 4-57.

Figure 4-57 Saving the fault diagnosis file

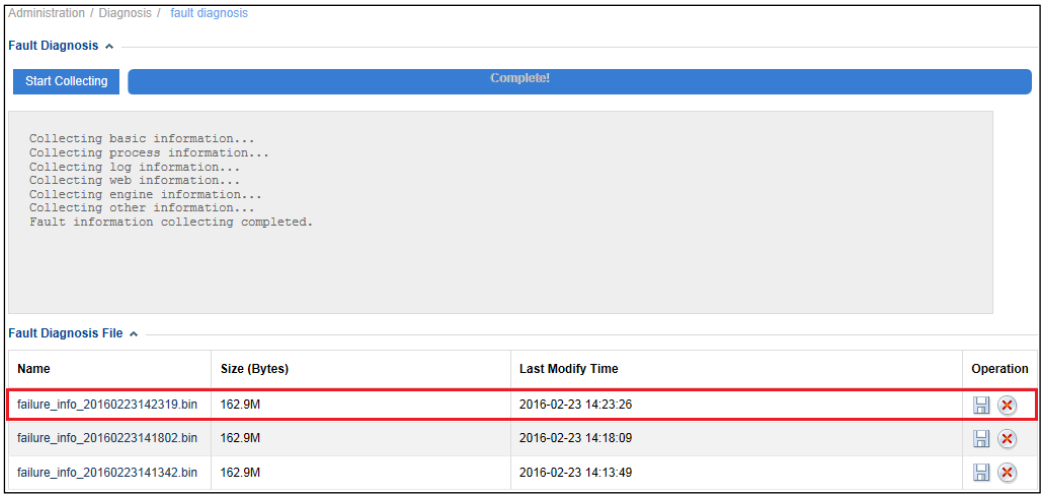


Click **Save** to save the fault diagnosis file to the default path. Alternatively, click the drop-down button on the right of **Save** and choose **Save As** to save the fault diagnosis file to a specified path.

Step 4 View fault diagnosis files.

After fault collection is complete, if there are already three fault diagnosis files, the new fault diagnosis file will overwrite the oldest one, as shown in Figure 4-58.

Figure 4-58 Refreshed list of fault diagnosis files



Step 5 Delete a fault diagnosis file.

Click in the **Operation** column to delete a fault diagnosis file.

----End

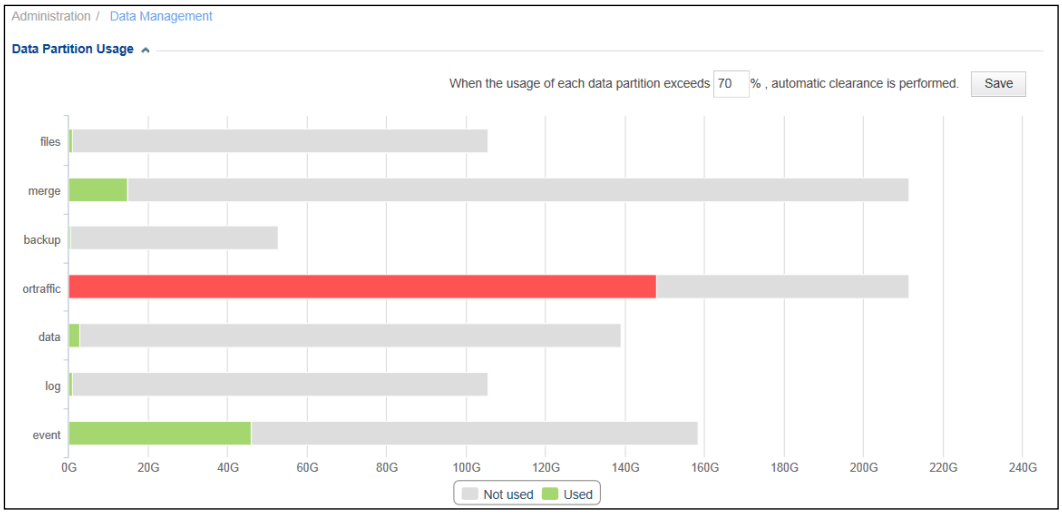
4.5 Data Management

The Data Management module allows you to learn the usage of data partitions in the NTA system in real time. You can specify a threshold for the partition usage. When the actual partition usage exceeds the threshold, NTA automatically cleans the disk. This effectively prevents data loss caused by insufficient disk space.

To set the usage threshold, follow these steps:

Step 1 Choose **Administration > Data Management**.

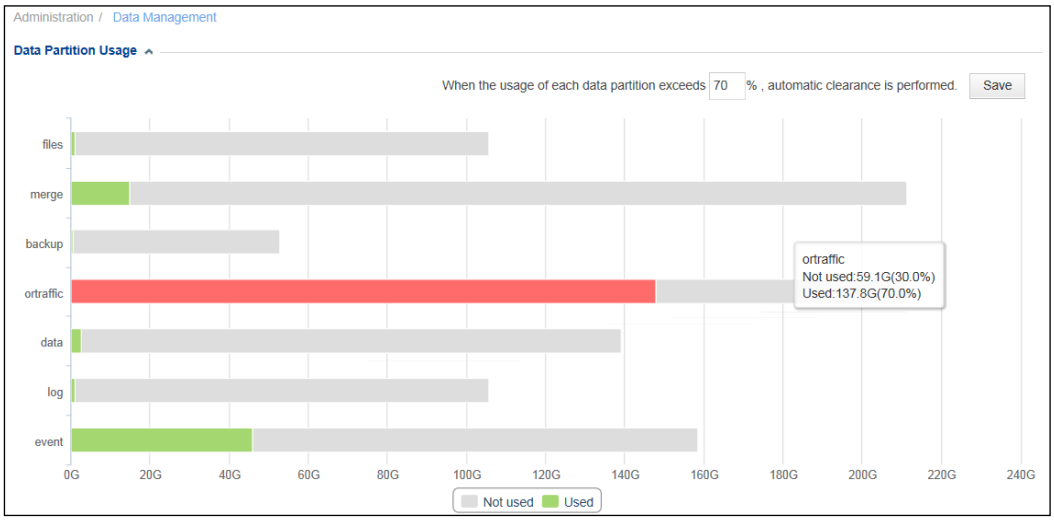
Figure 4-59 Data Partition Usage page



Step 2 View the data partition usage.

You can check the usage of all data partitions. Pointing to a bar displays details about the usage of the data partition represented by this bar, as shown in Figure 4-60.

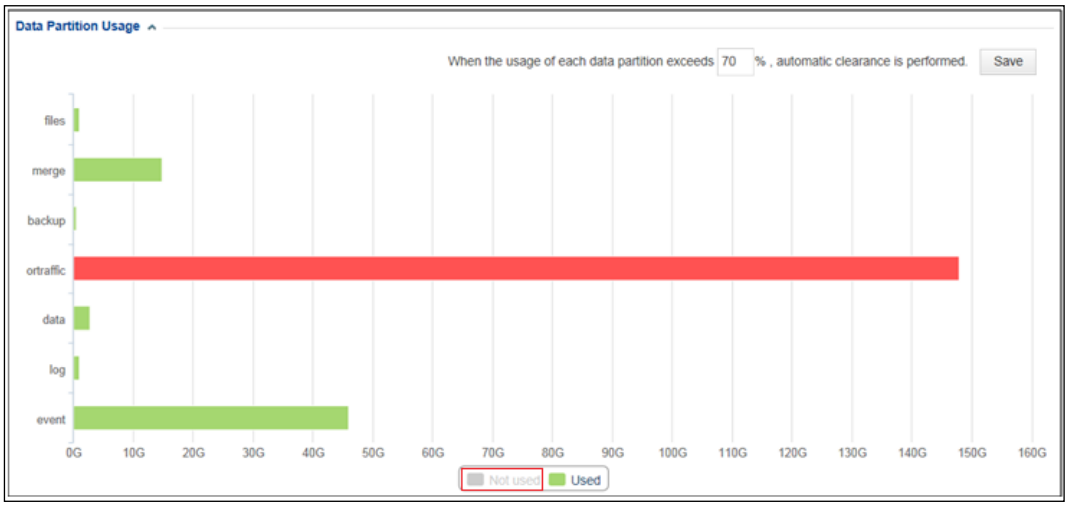
Figure 4-60 Viewing details about the partition usage



The used space and available space are both displayed by default. If the usage of a data partition is represented by a red bar, such as ortraffic in Figure 4-60, it indicates that the usage has exceeded the threshold.

You can click a curve name to remove the corresponding curve, and re-click the curve name to resume its display. The chart shown in Figure 4-61 displays only the used space of data partitions. In this case, **Not used** turns grey.

Figure 4-61 Displaying only used space of data partitions



Step 3 Set the automatic disk cleaning threshold.

At the upper right of the page, you can set a threshold for the partition usage. When the actual usage exceeds the threshold, the bar in the chart turns red and the system automatically cleans expired data. The default threshold is **70**%.

----End

4.6 User Management

In the User Management module, you can manage accounts and set login parameters.

User management involves the following sub-tasks:

- Managing User Accounts
- Configuring Security Settings
- Configuring Authentication
- Configuring Whitelist for NTA Access via Web API
- Managing the HTTP Host Whitelist
- Managing the Current User by Using the Shortcut Button

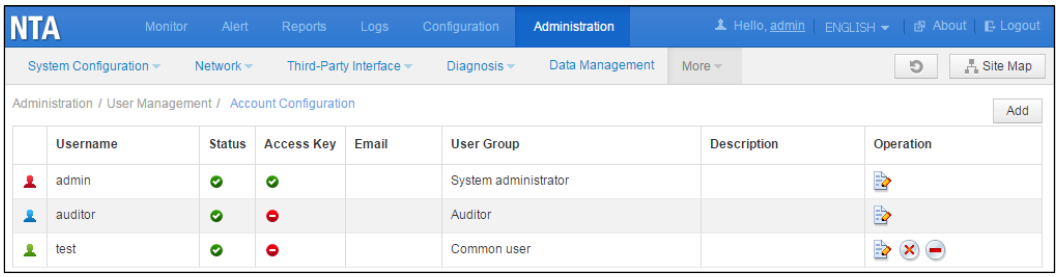
4.6.1 Managing User Accounts

NTA has two default accounts: **admin** and **auditor**. The user **admin** can create system administrator, configuration administrator, auditor, and common user accounts. For the description of permissions for different roles, see Table 3-1.

Creating an Account

Step 1 Choose **Administration > User Management > Account Configuration**.

Figure 4-62 Account Configuration page



Step 2 Create a system administrator account.

a. Click **Add**.

b. In the **Add** dialog box, configure parameters.

Figure 4-63 Creating a system administrator account

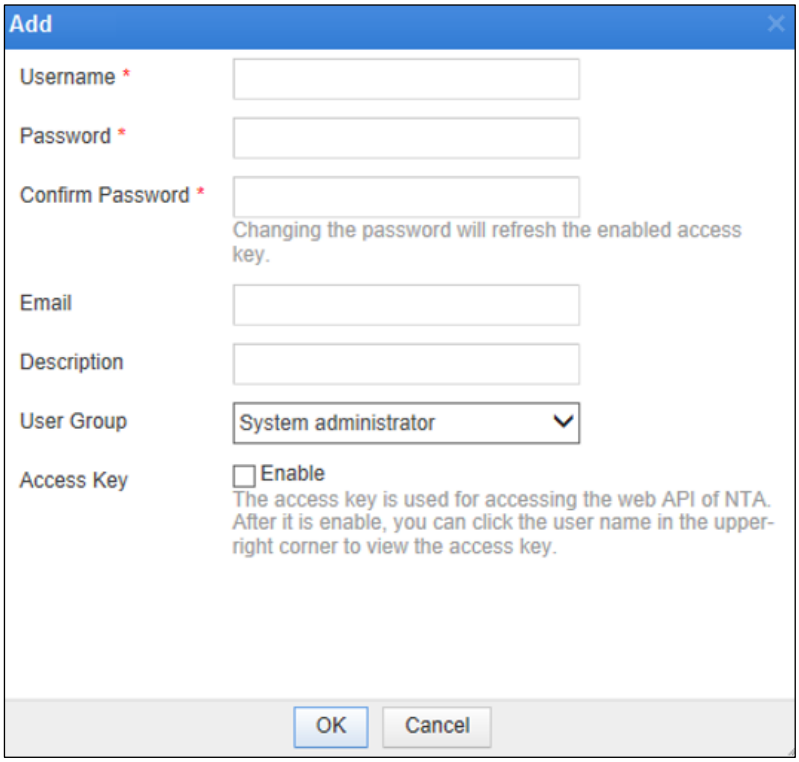


Table 4-18 describes parameters for configuring an account.

Table 4-18 Parameters for configuring an account

Parameter	Description
Username	User name of the new account, which must be a string of 4 to 20 English letters, digits, underscores and/or hyphens (-).
Password	Password of the new account, the minimum length of which depends on the **Minimum Length** value specified under **Administration > User Management > Security**

Parameter	Description
	Configuration.
Confirm Password	Specifies a repeat entry of the password for accuracy.
Email	Valid email address. It is an optional parameter.
Description	Brief description of the new account. It is an optional parameter.
User Group	Specifies a group to which the new account will belong to control the user permissions. Options include **System administrator**, **Configuration administrator**, **Auditor**, **Common user**, and **Custom-permission user**. The user **admin** can add any type of accounts, but a common system administrator can add only configuration administrators, auditors, and common users.
Access Key	Controls whether to enable the key for third-party access to NTA through the web API. After this is enabled, the user accessing the web-based manager of NTA with the new account can view the specific key after clicking in the quick access bar.

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

----End

Editing an Account

In the account list, click in the **Operation** column of an account to edit its information. Note that the user name cannot be changed.

Deleting an Account

In the account list, click in the **Operation** column of an account to delete this account. The default accounts **admin** and **auditor** cannot be deleted.

Disabling an Account

Default accounts cannot be disabled. Only newly created accounts can be disabled, which must be performed by **admin**. After being disabled, an account cannot be used for login to the web-based manager of NTA.

In the account list, click in the **Operation** column of an account to disable this account.

Enabling an Account

After disabling an account, **admin** can enable it again so that this account can be used for login to the web-based manager of NTA again.

In the account list, click in the **Operation** column of an account to enable this account.

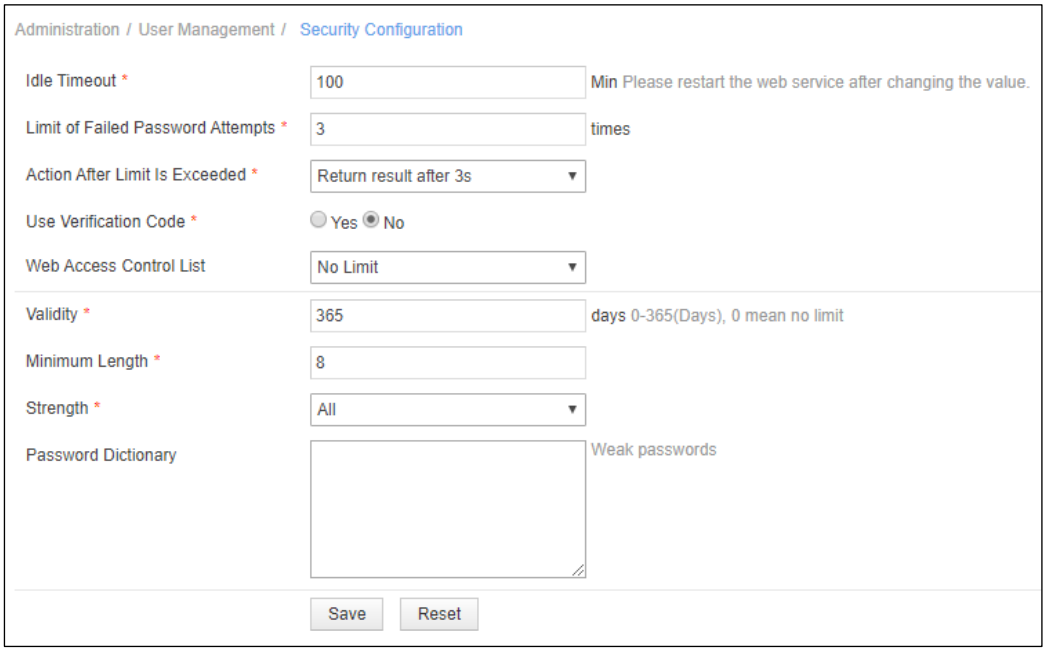
4.6.2 Configuring Security Settings

Security settings ensure the security of local accounts through login authentication. They do not take effect for Radius authentication, which is configured on the Radius server.

To configure account security settings, follow these steps:

Step 1 Choose **Administration** > **User Management** > **Security Configuration**.

Figure 4-64 Security Configuration page



Step 2 Configure login parameters.

Table 4-19 Login parameters

Parameter	Description
Idle Timeout	Specifies the time for NTA to keep the session alive in the absence of any operation before logging you out to ensure account security. The default value is **10** minutes.
Limit of Failed Password Attempts	Specifies the maximum number of consecutive login failures that are allowed before a specified action is taken against the account. The value is an integer in the range of 3–20, with **3** as the default value.
Action After Limit Is Exceeded	Specifies an action taken against the account after the **Limit of Failed Password Attempts** is exceeded. It has the following values: • **Return result after 3s**: returns error information. This is the default action. • **Lock client IP for 20 min**: locks the IP address of the client for 20 minutes before allowing users to log in again from this IP address. • **Lock account for 30 min**: locks the account for 30 minutes before allowing users to log in again with this account.
Use Verification Code	Controls whether to use verification codes to authenticate user login. • **Yes**: enables use of verification codes so that a user can successfully log in to NTA only after typing a correct verification code. • **No**: disables use of verification codes for login authentication.
Web Access Control List	Specifies IP addresses from which users are or are not allowed to access NTA. It has the following values:

Parameter	Description
	• **No Limit**: no limit to source IP addresses. • **Allow Access from the Following IP Addresses**: allows user access to NTA from the specified IP addresses. • **Block Access from the Following IP Addresses**: denies user access to NTA from the specified IP addresses. The default value is **No Limit**.
Validity	Specifies a period for a login password to remain valid before the system pops up a dialog box for you to change the password. The default value is **365** days.
Minimum Length	Specifies the minimum length of a login password. The default value is **8**.
Strength	Specifies the complexity of a login password. It has the following values: • **All**: no requirement for the setting of passwords. • **Necessary parts**: specifies what types of characters are contained in a password. You can select **Letters**, **Digit**, and/or **Special Characters**. The default value is **All**.
Password Dictionary	Specifies character strings that cannot be used as passwords. It is empty by default.

Step 3 Click **Save** to save the settings. To restore parameter settings to factory defaults, click **Reset**.

----End

4.6.3 Configuring Authentication

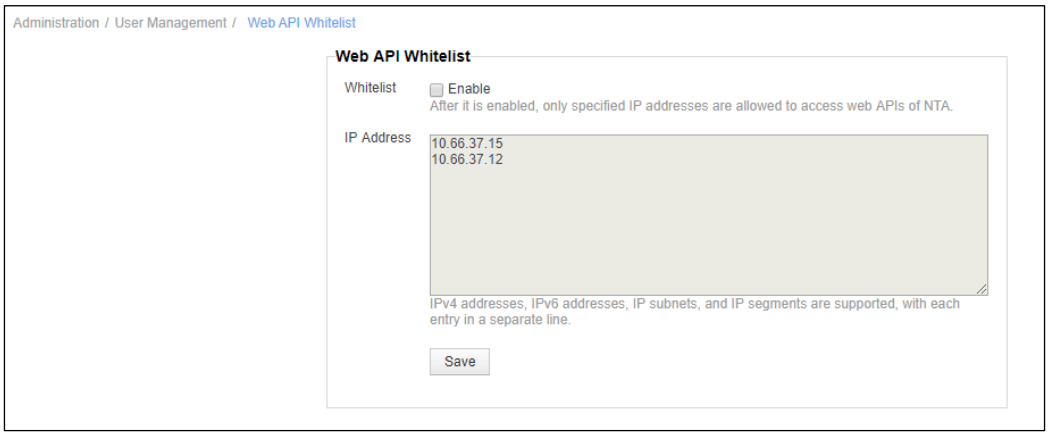
Accounts can be authenticated based on a local database or a third-party Radius authentication server.

No matter which authentication method is used, you need to configure a user account on NTA. When **Radius Authentication** is selected, the account created on NTA must have the same user name and passwords as those specified on the Radius server. For account configuration, see section 4.6.1 Managing User Accounts.

To configure account authentication, follow these steps:

Step 1 Choose **Administration** > **User Management** > **Authentication Configuration**.

Figure 4-65 Local authentication configuration page



Step 2 Select an authentication method.

- **Local Authentication**: This is the default authentication method, by which accounts are authenticated on NTA. To use this method, you only need to select it on the configuration page shown in Figure 4-65. Local authentication is unavailable for vNTA.
- **Radius Authentication**: authenticates accounts on the Radius server. On the page shown in Figure 4-66, select **Radius Authentication** and configure other parameters.

Figure 4-66 Radius authentication configuration page

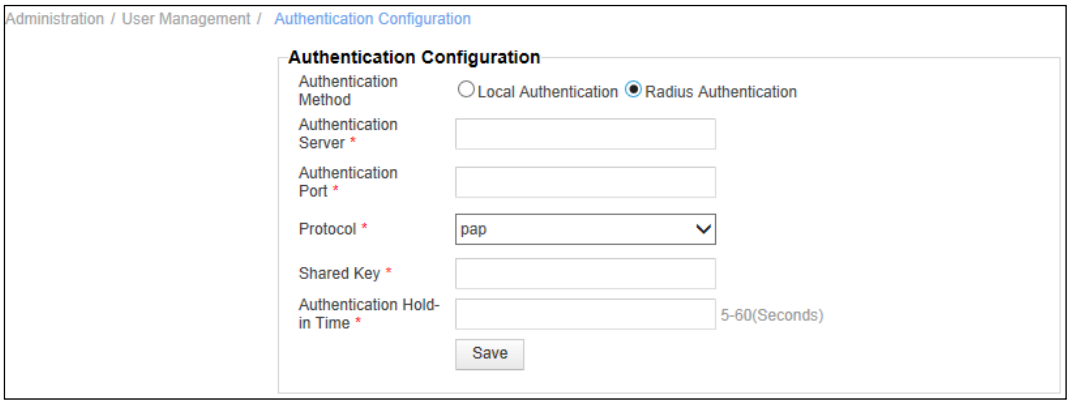


Table 4-20 describes parameters for configuring Radius authentication.

Table 4-20 Radius authentication parameters

Parameter	Description
Authentication Server	Specifies the IP address of the Radius server.
Authentication Port	Specifies the port that the Radius server uses to provide authentication.
Protocol	Specifies the protocol type used for authentication. It has the following values:

Parameter	Description
	• **pap**: Password Authentication Protocol • **chap**: Challenge-Handshake Authentication Protocol • **spap**: Shiva Password Authentication Protocol • **mschapv1**: Microsoft Challenge Handshake Authentication Protocol version 1 • **mschapv1**: Microsoft Challenge Handshake Authentication Protocol version 2
Shared Key	Specifies the password provided for NTA authentication for its access to the Radius server. NTA and the Radius server can receive packets from each other and respond accordingly only when the key configured here is the same as that on the Radius server.
Authentication Hold-in Time	Specifies the time for NTA to keep attempting to connect to the Radius server.

Step 3 Configure parameters and click **Save** to commit the settings.

----End

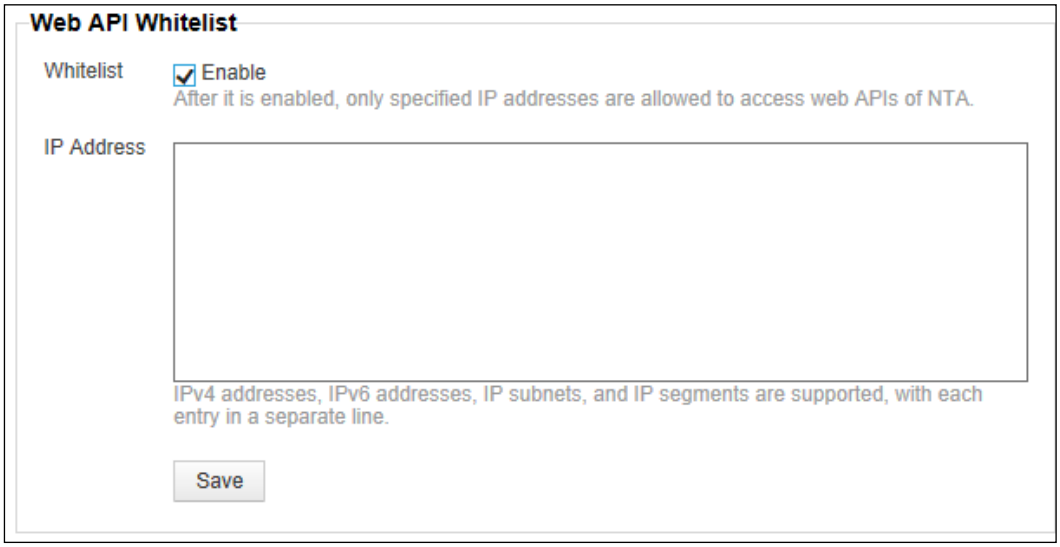
4.6.4 Configuring Whitelist for NTA Access via Web API

Third-party users can access NTA through the web API interface. If the web API whitelist is disabled, any IP addresses can be used for login to NTA with the access key. After the whitelist is enabled, only the IP addresses on the whitelist can be used for login to NTA with the access key.

To configure the web API whitelist, follow these steps:

Step 1 Choose **Administration > User Management > Web API Whitelist**.

Figure 4-67 Web API Whitelist page



Step 2 Select **Enable** for **Whitelist** and type IP addresses in the text box below.

You can type IPv4 or IPv6 addresses, IP subnets, or IP address segments, with one entry in each line.

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

----End

4.6.5 Managing the HTTP Host Whitelist

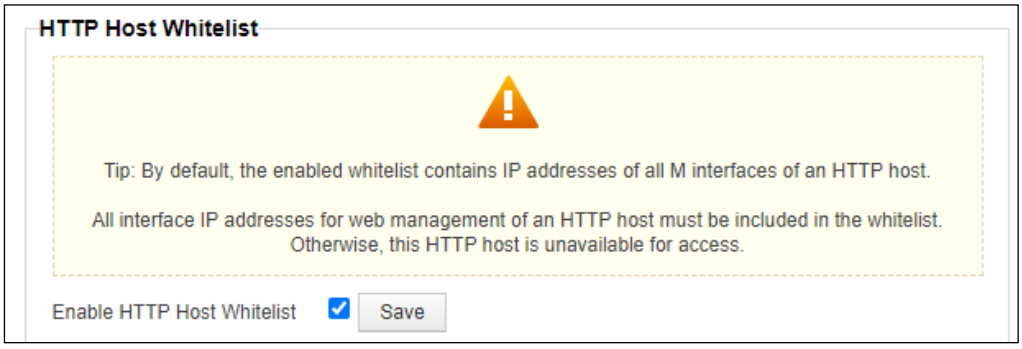
The HTTP host whitelist is disabled by default. After it is enabled, no HTTP host-related vulnerability will be reported regarding the system.

Note	The HTTP host whitelist applies to all management interfaces of an HTTP host by default. Therefore, after this function is enabled, you should add IP addresses of all interfaces used for web management to the whitelist; otherwise, this HTTP host would be unavailable for access.

To configure an HTTP host whitelist, follow these steps:

Step 1 Choose **Administration > User Management > HTTP Host Whitelist**.

Figure 4-68 Enabling the HTTP host whitelist

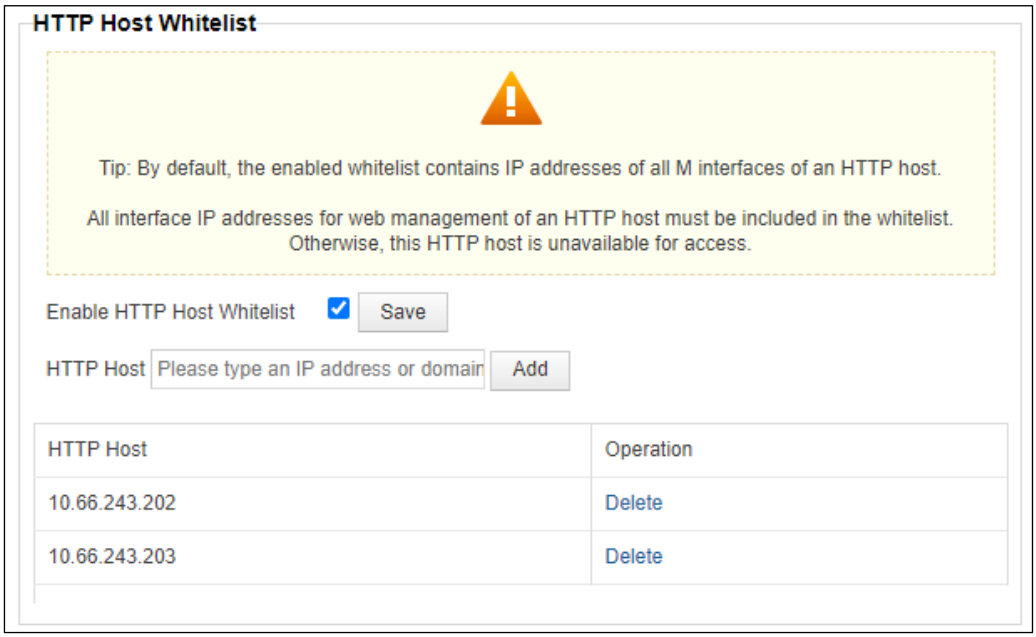


Step 2 Enable the HTTP host whitelist by selecting the check box.

Step 3 In the **HTTP Host** text box that appears, type an IP address or domain name and click **Add**.

You can add up to 10 IP addresses or domain names.

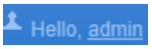
Figure 4-69 Adding an entry to the HTTP host whitelist



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

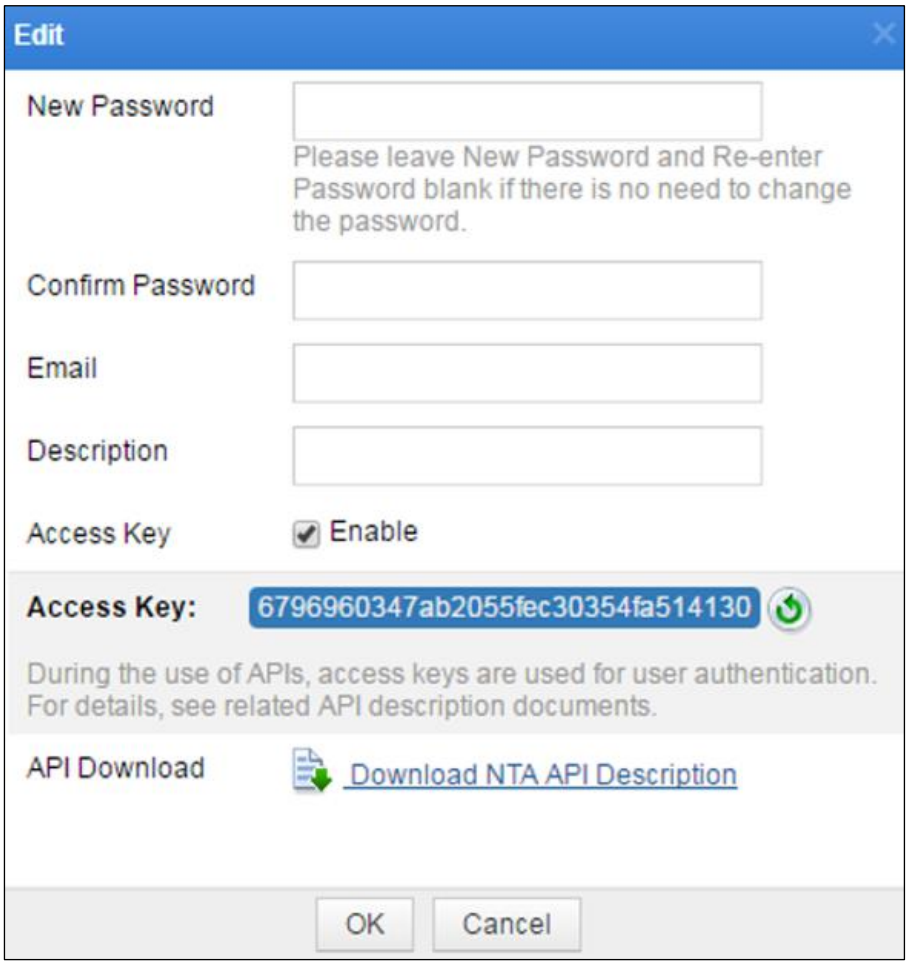
----End

4.6.6 Managing the Current User by Using the Shortcut Button

After login to NTA, you can click 

in the quick access bar in the upper-right corner of the web-based manager. The **Edit** dialog box appears, as shown in Figure 4-70. In this dialog box, you can edit information about the current user and disable the access key. If the web API interface is enabled, you can view its key. You can click to update the access key. After the access key is updated, third-party users can access NTA only by using the updated access key.

Figure 4-70 Editing personal information



4.7 Hot Standby

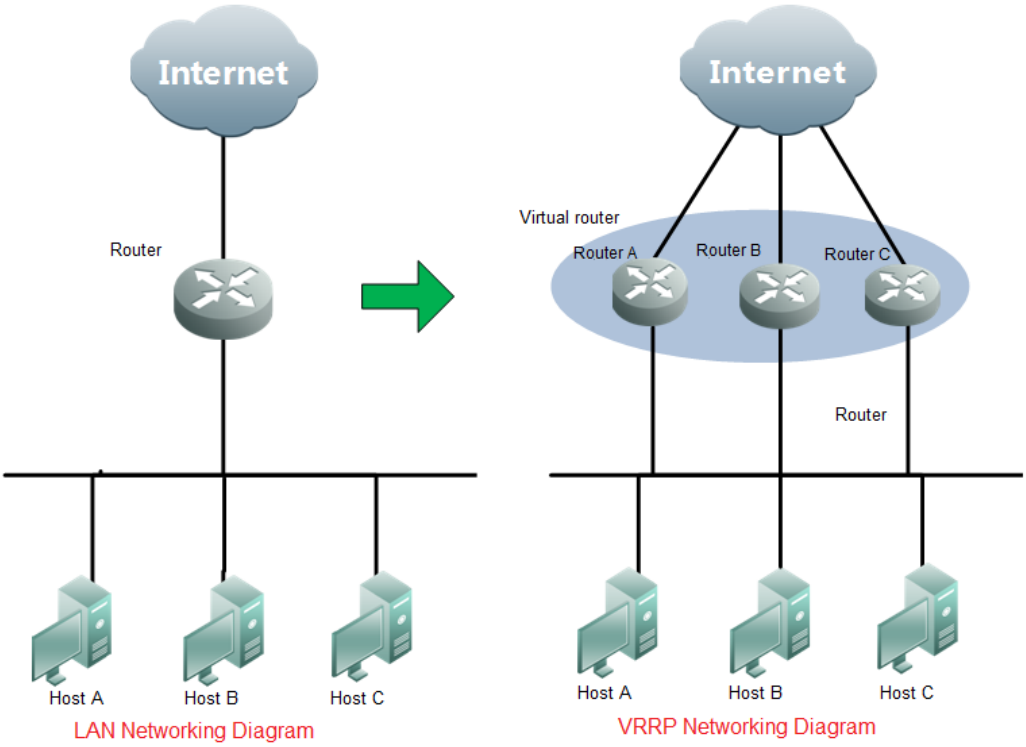
During data communication, any kind of software or hardware error may cause improper network connection or network interruption, which in turn will cause data transmission failure. The VRRP-based hot standby function provided by NTA can effectively prevent data communication interruptions caused by single point of failures (SPOFs) and enhance network reliability.

4.7.1 Getting to Know VRRP

Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol used to resolve network interruptions caused by gateway faults. As shown in Figure 4-71, several routers on a local area network (LAN) are grouped together to form a VRRP backup group. A backup group, which consists of a master router and multiple backup routers, functions as a virtual router.

Figure 4-71 VRRP networking diagram



Router A, router B, and router C constitute a virtual router. This virtual router has its own IP address and hosts on the LAN take it as their default gateway. Router A, router B, or router C, whichever has the highest priority, works as the master router assuming the responsibility of a gateway. The other two work as backup routers. When the master router becomes faulty, the backup ones automatically forward packets in lieu of the former, thereby ensuring the continuity and reliability of network communication.

VRRP Backup Group

A VRRP group has the following characteristics:

- Has the unique virtual router identifier (VRID).
- Has its own virtual IP address: Hosts on a LAN know only the IP address of the virtual router, with no need to distinguish the master router from backup routers.
- The master router and backup routers in the backup group each has its own IP address.
- The election mechanism of VRRP decides which router in the group assumes the forwarding responsibility. Hosts on a LAN need to only take the virtual router as the default gateway.

VRRP Advertisement Interval Timer

The master router in a VRRP backup group sends periodic VRRP advertisement messages, notifying other routers in the group that it is working properly.

Users can adjust the interval for the master router to send advertisement messages by setting a VRRP timer. A backup router, if failing to receive any VRRP advertisement message over a

period of three intervals, takes itself as the master router and sends VRRP advertisement messages, thereby starting reelection of the master router.

Working Mode of Routers in a Backup Group

Routers in a backup group work in either of the following modes:

- Non-preemption: In this mode, a backup router, even if it is configured with a higher priority, will not become the master one as long as the master router functions properly.
- Preemption: In this mode, the backup router sends VRRP advertisement messages when finding that it has a higher priority than the current master router. This leads to the reelection of the master router within the group to replace the original master one. Accordingly, the original master router will become a backup router.

4.7.2 Configuring Hot Standby

NTA supports the hot standby function implemented by only two NTA devices working in active/standby mode. One NTA works in active mode, handling all services and sending configurations to the standby device for backup. The other works in standby mode, not handling services and for backup purposes only.

Before enabling high availability (HA), you need to first specify the master and backup NTA devices and configure a VRRP backup group on the master device. Interfaces on the two devices with the same VRID back up each other. Interfaces on the master device in the VRRP backup group are all master ones and those on the backup device are all backup ones.

After the hot standby function is enabled, the master NTA synchronizes configuration information in real time to the backup device to ensure consistent configurations between the two. Configuration information that can be synchronized includes the following:

- Monitoring object settings
- Alert configuration templates
- Global alert settings
- Global diversion settings
- Flow collection and forwarding settings
- Data dictionary settings
- Basic system settings
- Third-party interface settings
- User management settings
- Auto-learning baseline thresholds

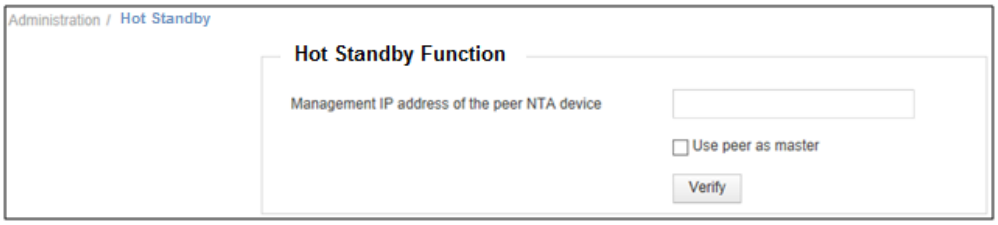
An active/standby switchover is triggered when any of the following occurs on the master device:

- Any interface in the VRRP group is down.
- The system restarts.
- The system engine is down.
- The system is power off.

To configure the hot standby function, follow these steps:

Step 1 Choose **Administration > Hot Standby**.

Figure 4-72 Hot Standby page



Step 2 Configure the interface for configuration synchronization and the HA role of the current device.

a. Type the IP address of the peer NTA for **Management IP address of the peer NTA device**. You are advised to use the IP address of the M interface.

b. Specify the HA role of the current NTA.

If the current NTA is a backup device, you must select the **Use peer as master** check box. If the current NTA is a master device, you do not need to select this check box.

After the HA role is specified, all roles in the VRRP group are the same as the HA role of the device.

- When the current device is the master, all interfaces on it are masters.
- When the current device is the backup, all interfaces on it are also backup ones.

c. Click **Verify** to check whether the current NTA properly connects to the peer NTA, whether their time zone configurations are the same, and whether their software versions are the same.

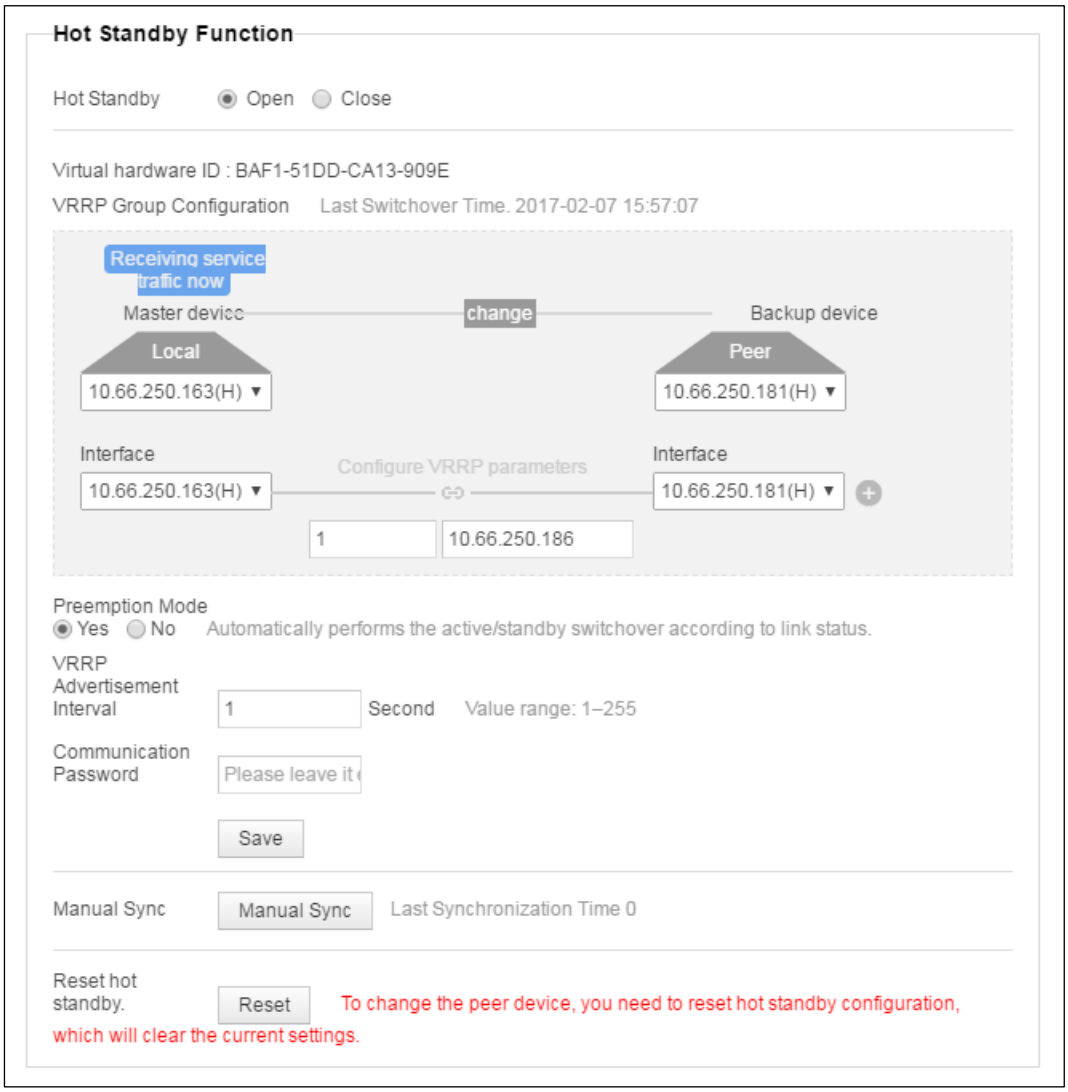
You can continue configuring related parameters only after the current NTA passes the verification.

Step 3 Enable the hot standby function.

Click **Enable** to enable the function or click **Disable** to disable the function.

Step 4 Configure related parameters on the page shown in Figure 4-73.

Figure 4-73 Configuring hot standby parameters

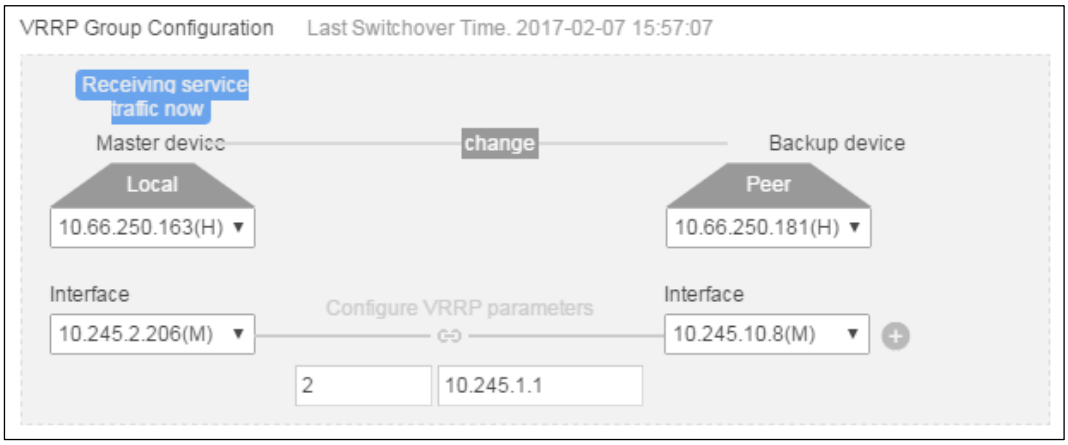


a. Check the role of the current device.

   In the upper part of the page, the roles of the current and peer devices in the backup group are displayed.

b. Configure VRRP backup groups. At most five can be configured.

Figure 4-74 Configuring VRRP backup groups



The **Interface** drop-down box is used to select interfaces that back up each other. The two interfaces in a group must have IP addresses on the same segment; otherwise, VRRP multicast packets for configuration synchronization cannot be received.

In the left text box below **Configure VRRP parameters**, specify a VRID to uniquely identify a VRRP group. The value must be an integer in the range of 1 to 255. Note the following when configuring a VRID:

- Usually, corresponding interfaces on the master and backup devices, such as the M interface on the master device and the M interface on the backup device, are assigned the same VRID. In this manner, they belong to the same VRRP group and can back up each other.
- The VRID of interfaces in the same VRRP group must be the same.
- Different interfaces on a device cannot be configured with the same VRID, that is, cannot be in the same VRRP group.

In the right text box below **Configure VRRP parameters**, configure the virtual IP address of the VRRP backup group. This IP address must be on the same network segment as the IP addresses of the two interfaces in the group and different from the IP address of any interface.

You can click to create a VRRP group or to delete one.

c. Configure the preemption mode.
   - If you click **Yes** for **Preemption Mode**, when the fault on the master device is fixed, this device preempts to become the master, forwarding data again.
   - If you click **No** for **Preemption Mode**, when the fault on the master device is fixed, this device does not preempt to become the master. In this case, services are not handed over back to it. That is to say, the original backup device still works in active state to forward data.

d. Configure a communication password.

   A communication password facilitates secure configuration synchronization. It must be a string of 8–20 characters. To configure such a password, you need to log in from a virtual IP address or log in to a master or backup device with the **admin** account, and then type the password on the **Hot Standby Function** page.

   For an NTA device with the hot standby function, after it is upgraded to V4.5R89F01CN or later, you must configure a communication password before properly using this function.

e. Configure synchronization settings.

NTA supports manual and automatic synchronization of all configurations on the master device to the backup device. This can take place only after you properly configure VRRP group parameters.

By default, when configurations on the master device change, such changes are synchronized to the backup device.

When the current device is the master, you can click **Manual Sync** to synchronize configurations on this device to the backup. When the current device is the backup, the **Manual Sync** button is unavailable.

f. Configure the VRRP advertisement interval.

The VRRP advertisement interval indicates the interval at which the device sends a heartbeat message in multicast mode to notify its own status. The default value is recommended. If the backup line interface fails to receive any multicast packet from the master line interface after the specified interval, the system deems that the master line is down. In this case, the backup line turns to active and begins to forward data.

The VRRP advertisement interval configured on the local device must be the same as that on the peer device.

Step 5 Click **Save** to commit the settings.

Step 6 If you need to reconfigure parameters, click **Reset** to clear the current settings.

----End

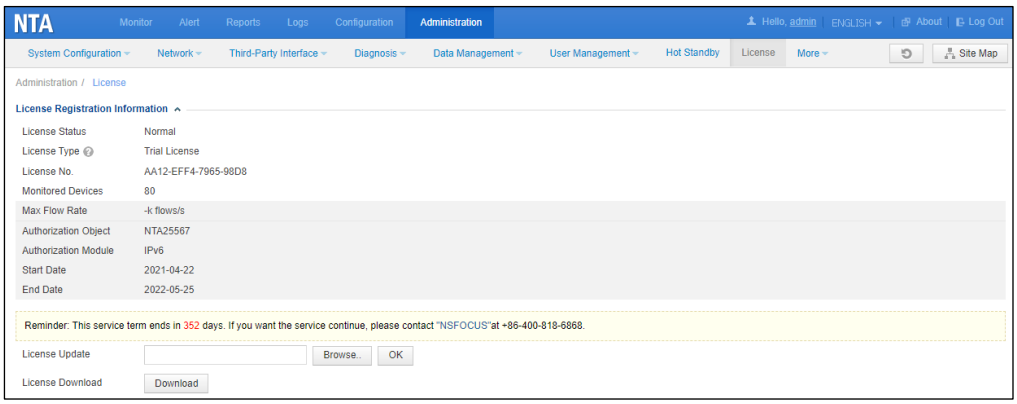
4.8 License

After an NTA device is installed, you must import the license before using it. Information about the license will be automatically displayed after the license is imported.

To manage the system license, follow these steps:

Step 1 Choose **Administration** > **License**.

Figure 4-75 License information



Note	The **License** page of vNTA has an additional area **Cloud Authorization**. For details about the related functions, please contact NSFOCUS technical support.

Table 4-21 describes parameters on this page.

Table 4-21 Parameters on the License page

Parameter	Description
License Status	Indicates whether the license status is normal.
License Type	Indicates the license type, which can be Trial, Interim, Formal, and Subscription. • **Trial**: license for products on trial. • **Interim**: license for devices for which a purchase contract is signed but the full payment is not made. • **Subscription**: license that is valid for devices for a certain period after the amount is paid in full. • **Formal**: license officially made available to the customer after all fees are paid.
License No.	Indicates the unique number of the license.
Max Flow Rate	Limits the number of flows that can be processed by NTA per second. Values vary with the device models: • NTA NX3-2000E/HD2200: 120k • NTA NX3-1000E: 60k • vNTA: depending on the license
Monitored Devices	Indicates the maximum number of devices that can be managed by the current NTA.
Authorization Object	Indicates the object to which this license is authorized.
Start Date	Indicates the date when the license begins to take effect for the current service. Note The current service refers to the license upgrade service.
End Date	Indicates the date when the license expires for the current service. • When a trial, interim, or subscription license expires, you cannot upgrade NTA, which will later stop all system services. • When a formal license expires, you cannot upgrade NTA, which will, however, still provide protection. Note The current service refers to the license upgrade service.

Step 2 Import the license.

In the lower part of the **License Registration Information** area, click **Browse** and select a license file from the local disk drive. Then click **OK**. The license preview page then appears. Click **Verify** to import the license.

Note	• To get a license file, please contact NSFOCUS technical support. • You are advised not to include special characters or Chinese characters in the license file name.

Step 3 Download the license.

In the lower part of the **License Registration Information** area, click **Download** to download the current license file to a local disk drive.

----End

4.9 System Upgrade

In the Upgrade module, you can perform the following operations:

- Upgrading System Software
- Upgrading Detection Rules
- Upgrading Threat Intelligence

4.9.1 Upgrading System Software

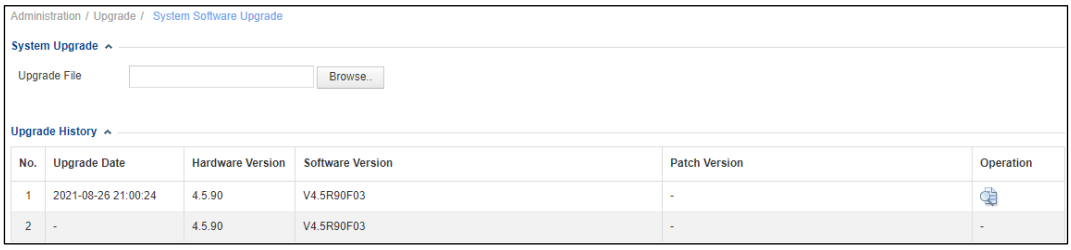
The system software of NTA can only be manually upgraded. The procedure is as follows:

Step 1 Contact NSFOCUS technical support for the NTA upgrade package. Make sure that the package applies to your product.

Note	For vNTA, you can obtain the upgrade package only after license verification: • On the page shown in Figure 4-75, download the license file of the current system to a local disk drive. • Log in to NSFOCUS's software upgrade page at http://update.nsfocus.com, click **Pure Software Device Upgrade**, and then upload the previously downloaded license file for verification. After the license is verified, you can download the mapping vNTA upgrade file. For details, contact NSFOCUS technical support.

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

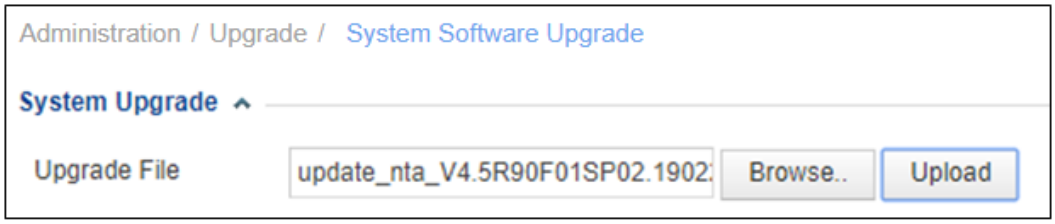
Figure 4-76 System Upgrade page



Step 3 Click **Browse**, select the upgrade package, and then click **Open**.

The **Upload** button appears, as shown in Figure 4-77.

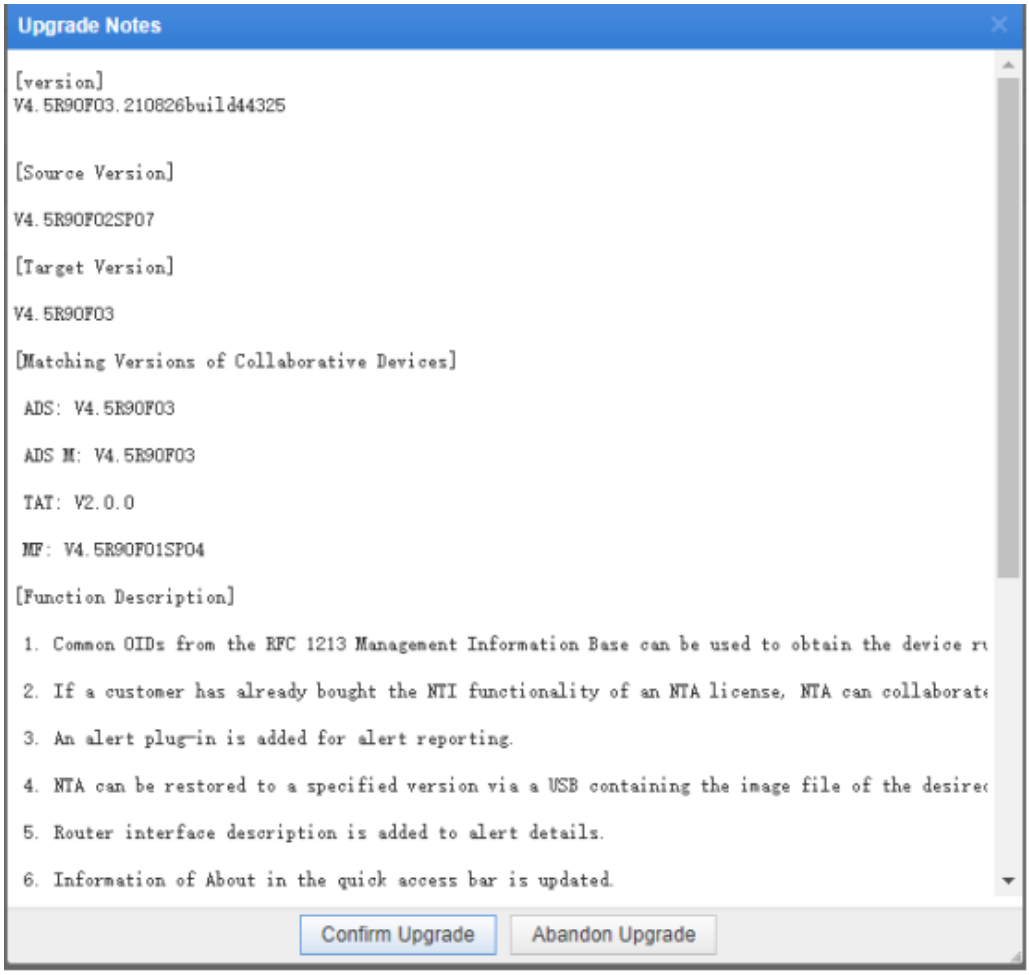
Figure 4-77 System Upgrade page after an upgrade file is selected



Step 4 Click **Upload**.

After the upgrade package is uploaded, the system displays the upgrade confirmation dialog box.

Figure 4-78 Upgrade confirmation dialog box



Step 5 Click **Confirm Upgrade** to start the upgrade immediately.

During the upgrade, NTA displays the progress. After the upgrade is complete, NTA automatically returns to the previous page.

Note	During the upgrade, you need to wait patiently until a message indicating successful upgrade appears.

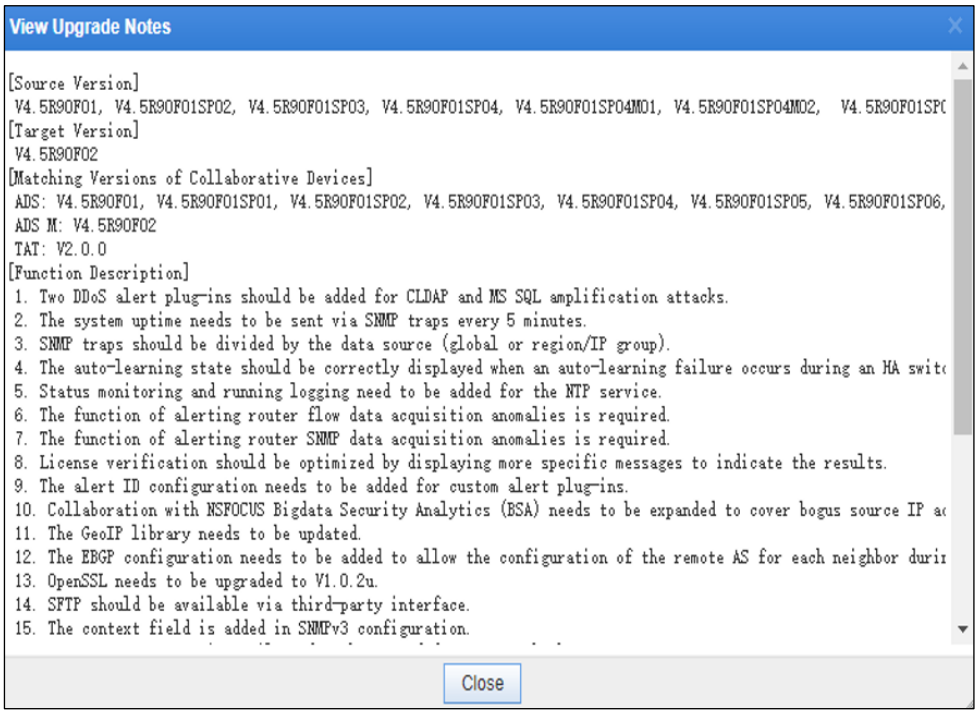
The system automatically restarts after the message prompting the upgrade success.

Step 6 Log in to the system and view the firmware version and upgrade date in the **Upgrade History** list to check whether the upgrade succeeded.

Step 7 View upgrade notes.

a. Click in the **Operation** column to view upgrade notes. The "-" sign in the **Operation** column indicates that it is the original software version.

Figure 4-79 Upgrade notes



b. Click **Close** to return to the **System Upgrade** page.

----End

4.9.2 Upgrading Detection Rules

You can upgrade NTA's detection rule library locally or remotely.

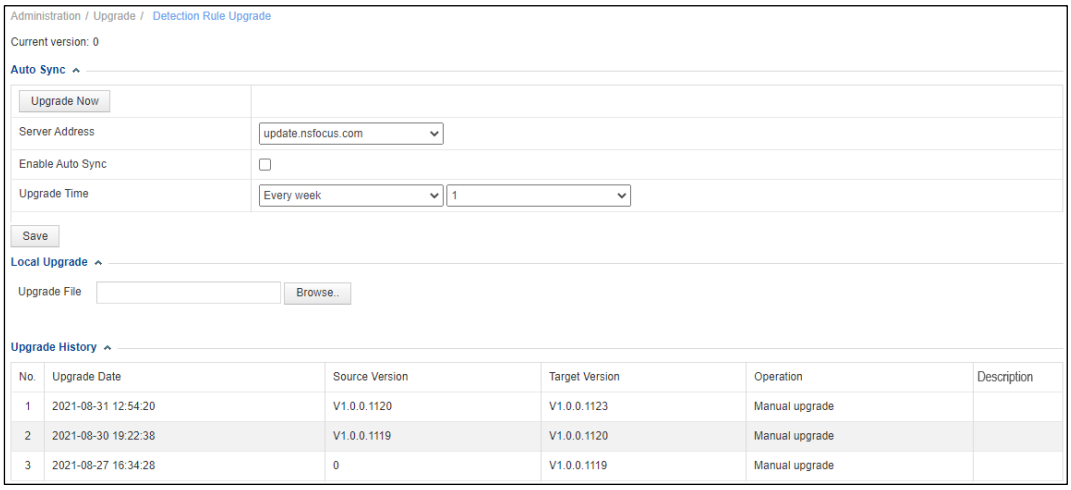
Local Upgrade

To upgrade the detection rule library locally, follow these steps:

Step 1 Contact NSFOCUS technical support for the upgrade package of the detection rule library. Make sure that the package matches the hardware model.

Step 2 Choose **Administration > Upgrade > Detection Rule Upgrade**.

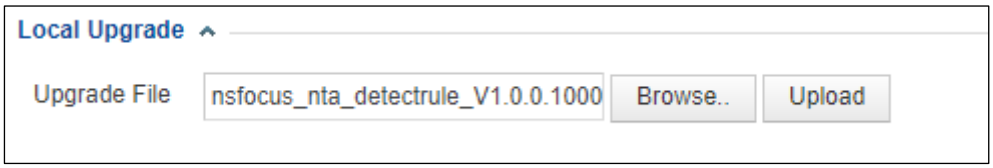
Figure 4-80 Detection Rule Upgrade page



Step 3 In the **Local Upgrade** area, click **Browse**, select the upgrade package, and then click **Open**.

The **Upload** button appears, as shown in Figure 4-81.

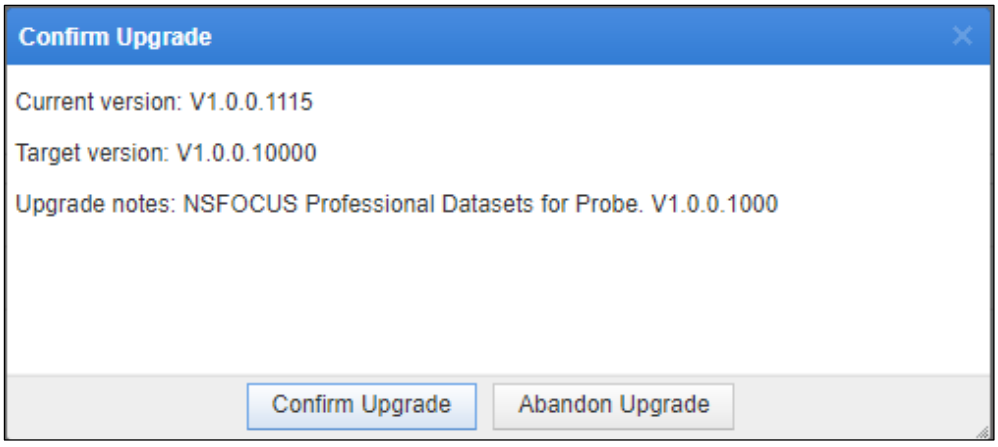
Figure 4-81 Local Upgrade area after an upgrade file is selected



Step 4 Click **Upload**.

After the upgrade package is uploaded, the system displays the upgrade confirmation dialog box.

Figure 4-82 Upgrade confirmation



Step 5 Click **Confirm Upgrade** to start the upgrade.

During the upgrade, NTA displays the progress. After the upgrade is complete, NTA automatically returns to the previous page.

Note	The system upgrade takes some time. Please be patient and wait until an upgrade success message is displayed.

Step 6 View the upgrade history.

View upgrade information in the **Upgrade History** list.

----End

Remote Upgrade

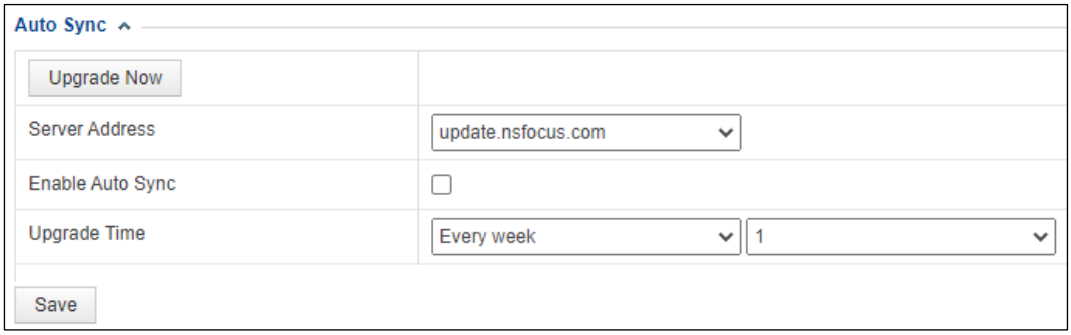
To upgrade the detection rule library remotely, follow these steps:

Step 1 Choose **Administration > Upgrade > Detection Rule Upgrade**.

Step 2 (Optional) Click **Upgrade Now** to upgrade the detection rule library instantly.

You can also configure NTA to automatically synchronize the rule library as required.

Figure 4-83 Auto Sync area



Step 3 In the **Auto Sync** area, configure automatic synchronization parameters.

Table 4-22 Automatic synchronization parameters

Parameter	Description
Server Address	Specifies the server address from which you can obtain the rule library upgrade file. The server address automatically displayed is a default one and can be directly used.
Enable Auto Sync	Contros whether to enable automtic synchronization. After this is enabled, the rule library will be automatically upgraded.
Upgrade Time	Specifies a time for the rule library to automatically upgrade.

Step 4 Click **Save**.

Then the system will automatically upgrade at the specified time.

Step 5 View the upgrade history.

View upgrade information in the **Upgrade History** list.

----End

4.9.3 Upgrading Threat Intelligence

You can upgrade NTA's threat intelligence database locally or remotely.

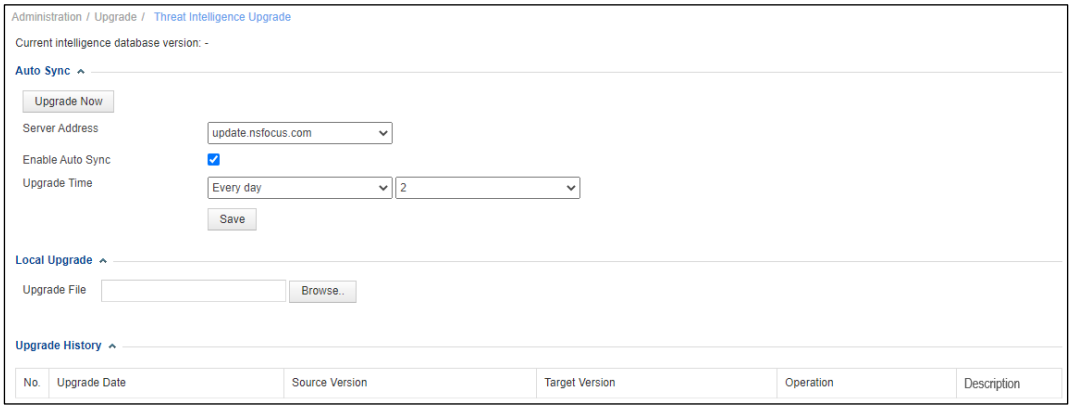
Local Upgrade

To upgrade the threat intelligence database locally, follow these steps:

Step 1 Contact NSFOCUS technical support for the upgrade package of the threat intelligence database. Make sure that the package matches the hardware model.

Step 2 Choose **Administration** > **Upgrade** > **Threat Intelligence Upgrade**.

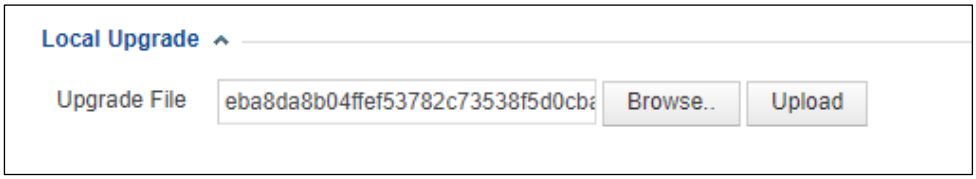
Figure 4-84 Threat Intelligence Upgrade area



Step 3 In the **Local Upgrade** area, click **Browse**, select the upgrade package, and then click **Open**.

The **Upload** button appears, as shown in Figure 4-85.

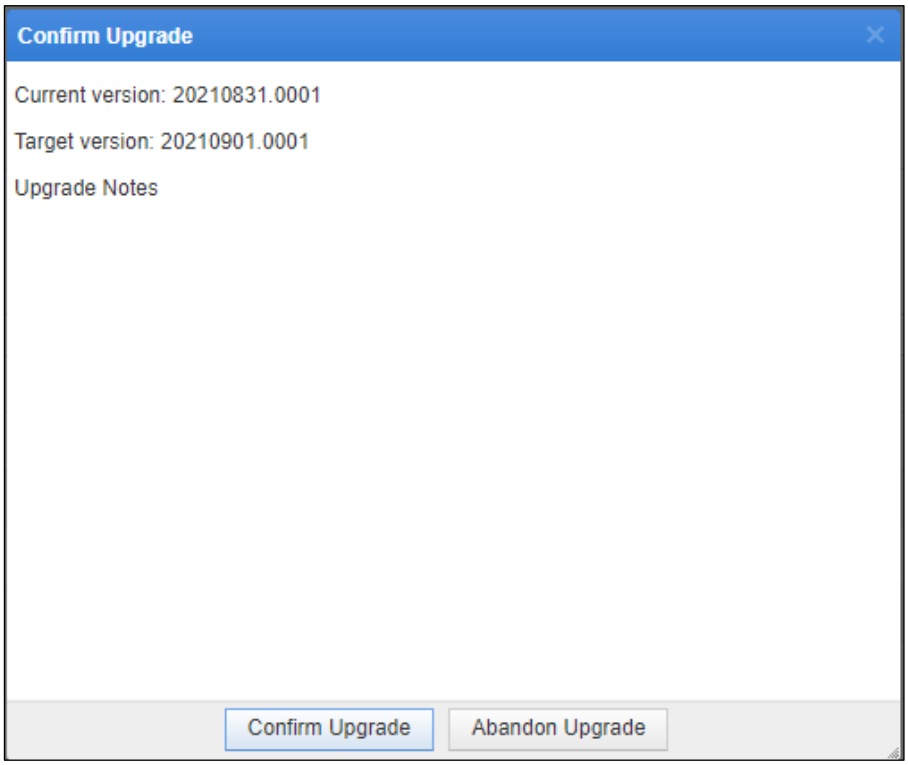
Figure 4-85 Local Upgrade area after an upgrade file is selected



Step 4 Click **Upload**.

After the upgrade package is uploaded, the system displays the upgrade confirmation dialog box.

Figure 4-86 Upgrade confirmation



Step 5 Click **Confirm Upgrade** to start the upgrade.

During the upgrade, NTA displays the progress. After the upgrade is complete, NTA automatically returns to the previous page.

Note	The system upgrade takes some time. Please be patient and wait until an upgrade success message is displayed.

Step 6 View the upgrade history.

View upgrade information in the **Upgrade History** list.

----End

Remote Upgrade

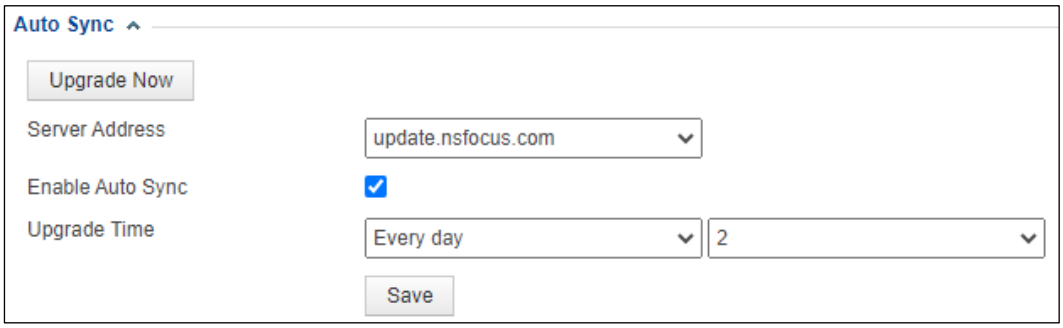
To upgrade the threat intelligence database remotely, follow these steps:

Step 1 Choose **Administration > Upgrade > Threat Intelligence Upgrade**.

Step 2 (Optional) Click **Upgrade Now** to upgrade the threat intelligence database instantly.

You can also configure NTA to automatically synchronize the threat intelligence database as required.

Figure 4-87 Auto Sync area



Step 3 In the **Auto Sync** area, configure automatic synchronization parameters.

Table 4-23 Automatic synchronization parameters

Parameter	Description
Server Address	Specifies the server address from which you can obtain the threat intelligence database upgrade file. The server address automatically displayed is a default one and can be directly used.
Enable Auto Sync	Contros whether to enable automtic synchronization. After this is enabled, the threat intelligence database will be automatically upgraded.
Upgrade Time	Specifies a time for the threat intelligence database to automatically upgrade.

Step 4 Click **Save**.

Then the system will automatically upgrade at the specified time.

Step 5 View the upgrade history.

View upgrade information in the **Upgrade History** list.

----End

4.10 Alert Whitelist

After the alert whitelist function is enabled, no alert will be generated about traffic to the IP addresses included in the whitelist.

To configure the whitelist, follow these steps:

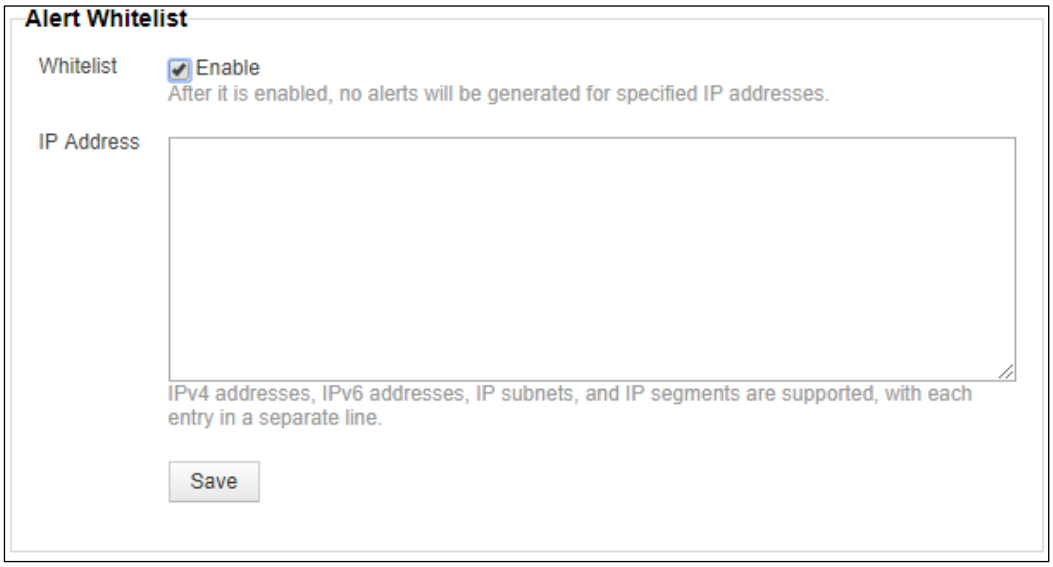
Step 1 Choose **Administration > Alert Whitelist**.

Figure 4-88 Alert Whitelist page

The alert whitelist function is disabled by default.

Step 2 Click **Enable** to enable the alert whitelist function.

Figure 4-89 Alert whitelist enabled



Step 3 Type IP addresses in the text box, with each in a separate line.

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

----End

4.11 Access Control

NTA supports access control. In other words, it can allow or deny access from one or more specified IP addresses.

4.11.1 Enabling Access Control

To enable access control, follow these steps:

Step 1 Choose **Administration** > **Access Control**.

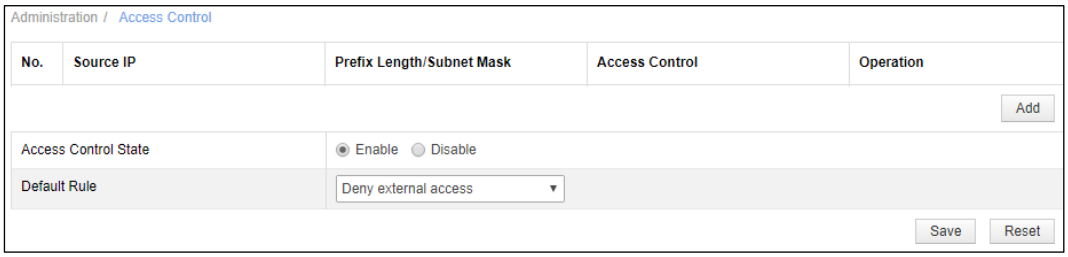
Figure 4-90 Access Control page

Access control is disabled by default.

Step 2 Click **Enable** and then **Save** to enable access control.

By default, all external IP addresses are allowed to access the device.

Figure 4-91 Enabling access control



----End

4.11.2 Allowing Access from Specified IP Addresses

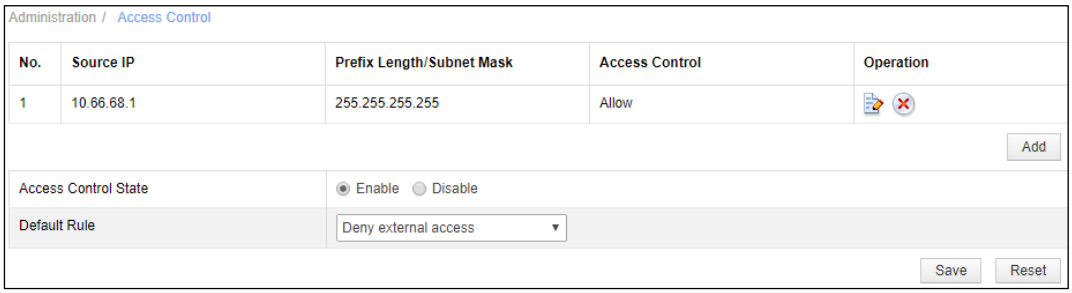
To allow access from specified IP addresses, follow these steps:

Step 1 On the page shown in Figure 4-91, select **Deny external access** as a default rule.

Figure 4-92 Disabling external access

Step 2 Click **Save** and then in the dialog box that appears, click **OK** to add the IP address of the local machine to the whitelist so that it can continue to access NTA.

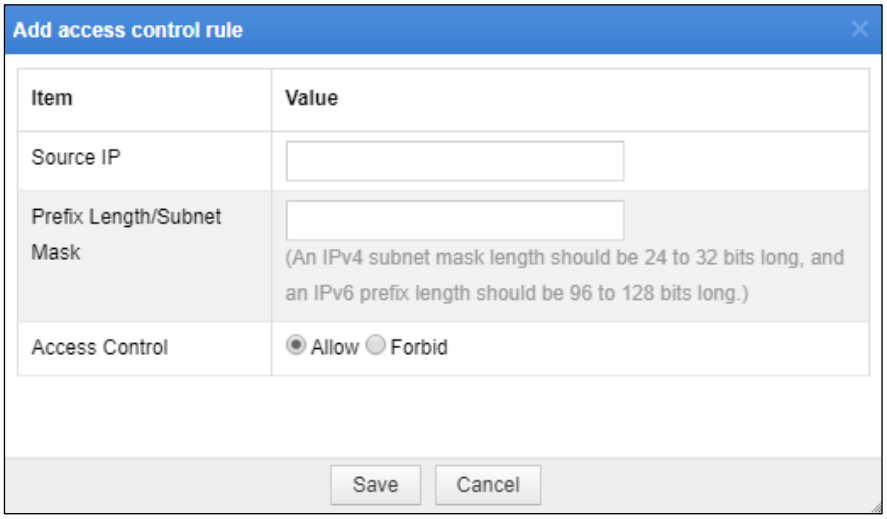
Figure 4-93 Local IP address added to the whitelist



Caution	If you fail to add the local IP address to the whitelist because of not understanding this function or deleting this IP address from the whitelist by mistake, you will be unable to log in to the web-based manager or the console user interface of NTA. To resolve this issue, you can log in to the console user interface to disable the access control function by running the **NTA# iptables off** command. For operations on the console user interface, see section 10.4 Configuring the ACL.

Step 3 To the lower right of the rule list, click **Add** to specify other IP addresses that should be allowed to access NTA.

Figure 4-94 Specifying IP addresses that should be allowed to access NTA



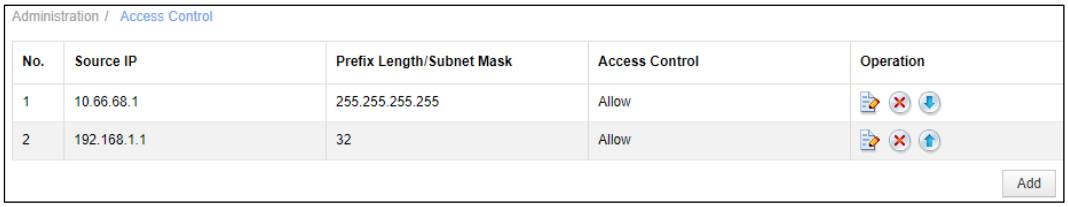
Step 4 Specify a source IP address and its prefix length or subnet mask, and then click **Allow** for **Access Control**.

Step 5 Click **Save**.

Now only the specified IP addresses can access NTA.

Note	Rules in the list are matched one by one from top to bottom. You can click or to move a rule up or down.

Figure 4-95 IP addresses allowed access to NTA



----End

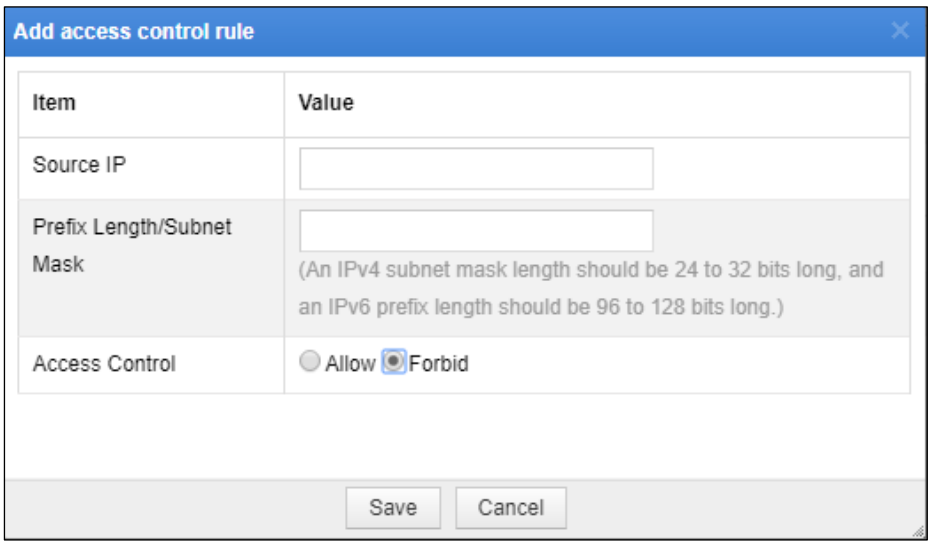
4.11.3 Denying Access from Specified IP Addresses

To deny access from specified IP addresses, follow these steps:

Step 1 On the page shown in Figure 4-91, select **Allow external access** as a default rule.

Step 2 To the lower right of the rule list, click **Add** to specify IP addresses that should be denied access to NTA.

Figure 4-96 Specifying IP addresses that should be denied access to NTA



Step 3 Specify a source IP address and its prefix length or subnet mask, and then click **Forbid** for **Access Control**.

Step 4 Click **Save**.

Now only the specified IP addresses are denied access to NTA.

----End

5 Configuration

This chapter presents core configurations of NTA, containing the following sections:

Section	Description
Objects	Describes how to configure objects monitored by NTA, including routers, router interface groups, and regions.
Alert Templates	Describes how to configure a router alert template, region alert template, and IP group alert template.
Global Alert Settings	Describes how to configure global alert settings, including default DDoS attack detection thresholds, global alert parameters, alert plug-in management, and traffic auto-learning parameters.
Global Diversion Settings	Describes how to configure default diversion policies, a BGP route for routing notification, a protection device, and FlowSpec BGP.
Flow Data Collection and Forwarding	Describes how to configure flow data collection and forwarding.
Detection of Bogus Source IP Addresses	Describes how to configure bogus source IP address detection rules.
NTI	Describes how to configure NTA to collaborate with NSFOCUS Threat Intelligence center (NTI).
Data Dictionary	Describes how to configure an application port and AS object.
Bulk Configuration	Describes how to configure regions and IP groups in batches.

5.1 Objects

The Objects module allows you to configure the following objects for NTA to monitor:

- Router
- Router Interface Group
- Region

5.1.1 Router

NTA can monitor NetFlow, sFlow, and NetStream data sent through a router. It can also monitor the CPU and memory usage as well as traffic on interfaces of the router on which the SNMP function is enabled.

By default, NTA does not monitor any devices. If you want NTA to monitor a device, you need to add this device manually.

Router configuration involves the following tasks:

- Configuring a Router
- Configuring Router Interfaces

5.1.1.1 Configuring a Router

NTA can detect and analyze traffic through a router. It can also monitor the resource usage and interface bandwidth usage of the router. For this purpose, you need to configure the router first, which involves the following:

- Basic information configuration: configuration of the device name, its IP address, whether to collect flow packets, and what alert template to use
- Flow configuration: configuration of parameters for receiving flow data from the router
- SNMP configuration: configuration of parameters for receiving data from the router via SNMP
- Router alert configuration: configuration of the interface bandwidth usage and performance alert thresholds
- Traffic statistics configuration: selection of statistical items of traffic

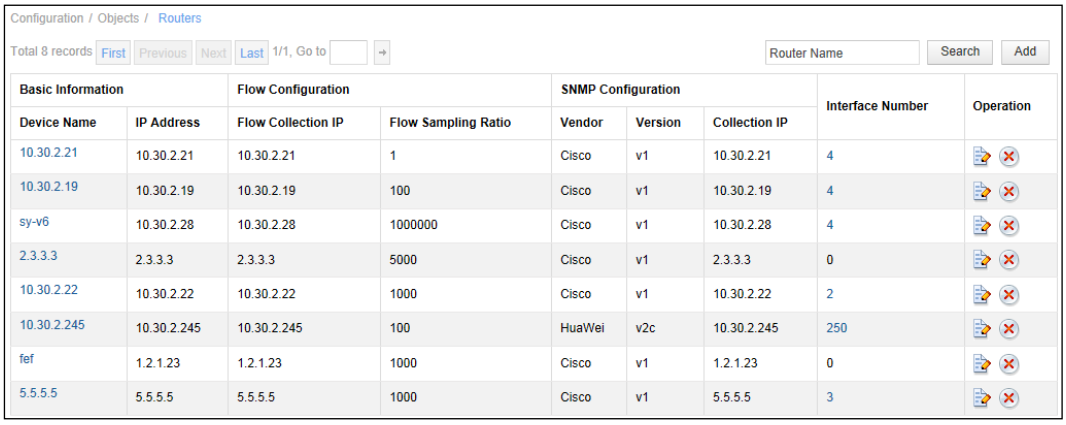
NTA monitors traffic through routers for attacks according to default DDoS attack alert thresholds. For details, see section 5.3.1 Default DDoS Attack Detection Thresholds.

To configure a router, follow these steps:

Step 1 Choose **Configuration > Objects > Routers**.

After you enable PPPoE interfaces in the console, you can view their number on the web-based manager. For how to enable PPPoE interfaces, see section 10.9 Enabling/Disabling PPPoE Interfaces.

Figure 5-1 Routers page



The preceding list displays routers that have been added. You can view brief information of these routers. Table 5-1 describes parameters in this list.

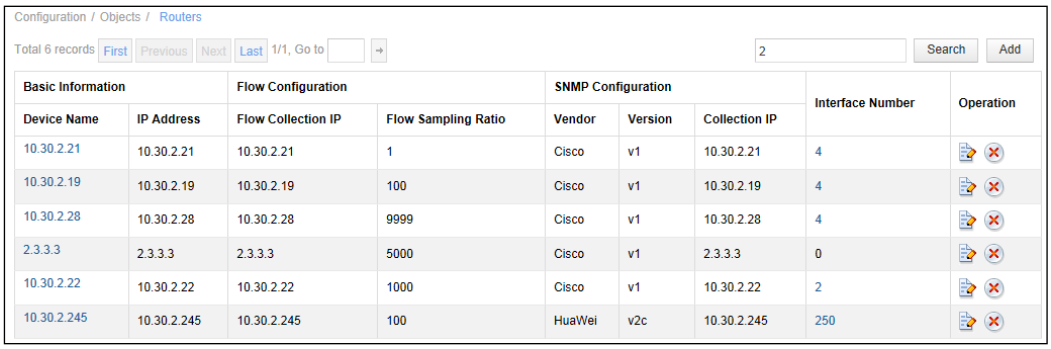
Table 5-1 Parameters in the router list

Parameter	Description
Device Name	Name of the router.
IP Address	IP address that identifies the router.
Flow Collection IP	IP address used by the router to send flow data to NTA.
Flow Sampling Ratio	Indicates the ratio of flow packets to be sampled to all the flow packets passing through the router.
Vendor	Vendor of the router.
Version	Version of the SNMP protocol.
Collection IP	IP address from which SNMP information will be collected
Interface Number	Number of router interfaces obtained via SNMP or flow data. Clicking the number in this column shows information of all monitored interfaces of the router, including basic settings, interface bandwidth usage, and inbound and outbound traffic.
Operation	Indicates operations that can be performed on the router. You can click the corresponding button to edit or delete the router.

Step 2 Find a router.

Fuzzy search is supported. Type a string in the **Router Name** text box and then click **Search**. Routers whose name contains the string will be displayed in the list below, as shown in Figure 5-2.

Figure 5-2 Query of routers



Step 3 Add a router.

Click **Add**.

a. Configure basic information on the page shown in Figure 5-3.

Figure 5-3 Basic information configuration

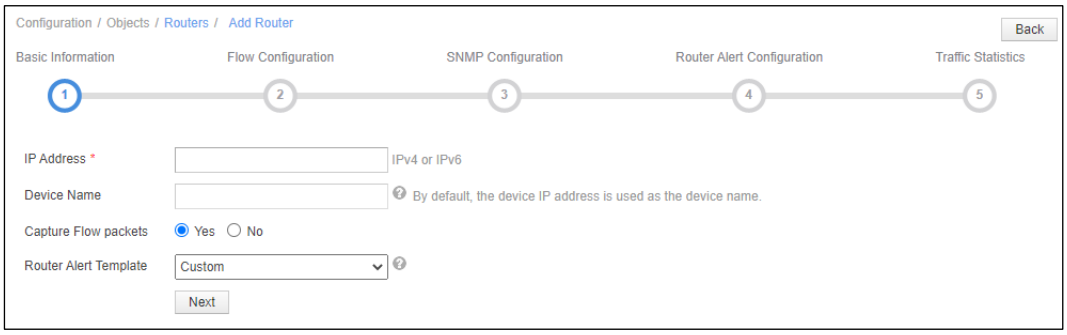


Table 5-2 describes parameters for configuring basic information of a router.

Table 5-2 Parameters for configuring basic information of a router

Parameter	Description
IP Address	Specifies the IP address of the monitored router. You can type either an IPv4 or IPv6 address. This parameter is mandatory.
Device Name	Specifies the name of the router (characters like () {} <> ' " and \ are not allowed in a device name). It is the IP address by default.
Capture Flow packets	Controls whether to collect flow data from this router. If you select **Yes**, NTA directs you to **Flow Configuration** after you click **Next** on the **Basic Information** page; otherwise, NTA directs you to **SNMP Configuration**, skipping **Flow Configuration**.
Router Alert Template	Specifies an alert template to configure alert parameters for this router. The drop-down list displays the existing alert templates. You can also select **Custom** and configure alert parameters on the **Router Alert Configuration** page. For the configuration of a router alert template, see section 5.2.1 Router Alert Template.

Click **Next**.

b. Configure flow settings on the page shown in Figure 5-4.

Figure 5-4 Flow configuration

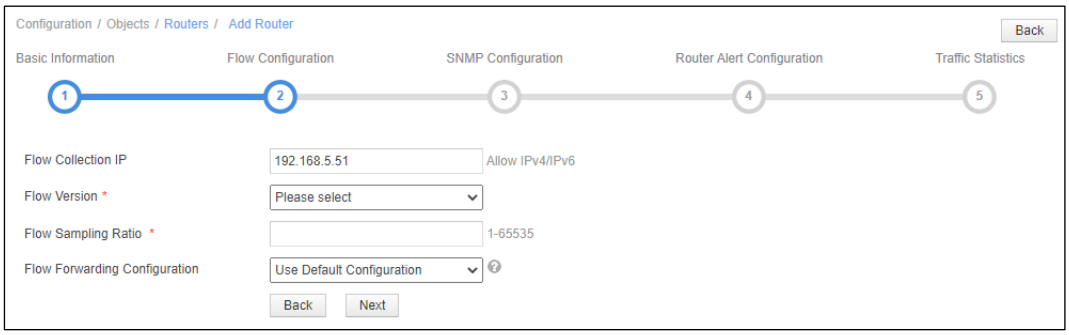


Table 5-3 describes parameters for configuring flow settings.

Table 5-3 Flow configuration parameters

Parameter	Description
Flow Collection IP	Specifies the IP address used by the router to send flow data to NTA. You can type either an IPv4 or IPv6 address.
Flow Version	Specifies the flow protocol type and version number. If **Flow Version** is set to **flexible netflow**, the flow protocol type can be NetFlow V5, NetFlow V9, or IPFIX.
Sampling Rate Adaption	Controls whether to configure the sampling ratio by means of adaption. This parameter is displayed when **Flow Version** is set to **sflow_v4** or **sflow_v5**.
Flow Sampling Ratio	Specifies the ratio of packets to be sampled to all packets passing through the router. This parameter is required when **Flow Version** is set to **sflow_v4** or **sflow_v5** and **Sampling Rate Adaption** is set to **No**, or when **Flow Version** is set to values other than **sflow_v4** and **sflow_v5**. Its value is an integer in the range of 1–1000000, which must be the same as that on the router.
Flow Forwarding Configuration	Specifies whether to forward collected flow data to other IP addresses. It has the following values: • **Use Default Configuration**: indicates the use of the global default settings. For details, see section 5.5 Flow Data Collection and Forwarding. • **Not Forward**: indicates that NTA does not forward received flow data. • **Custom**: requires you to type destination IP addresses in the text box below. You can type either IPv4 or IPv6 addresses.

Click **Next**.

To return to the **Basic Information** page, click **Back**.

c. On the **SNMP Configuration** page, configure parameters for NTA to receive the following router information via SNMP:

   – CPU and memory usage

   – Interface information and description

   – Brief information of interface traffic

   If SNMP collection is not configured here, only interface index information can be viewed from the interface list, but not other information such as the interface name, IP address, description, and bandwidth.

   Note that NTA can query information of a router only after parameters related to the SNMP server have been configured on the router.

Figure 5-5 shows the **SNMP Configuration** page.

Figure 5-5 SNMP configuration

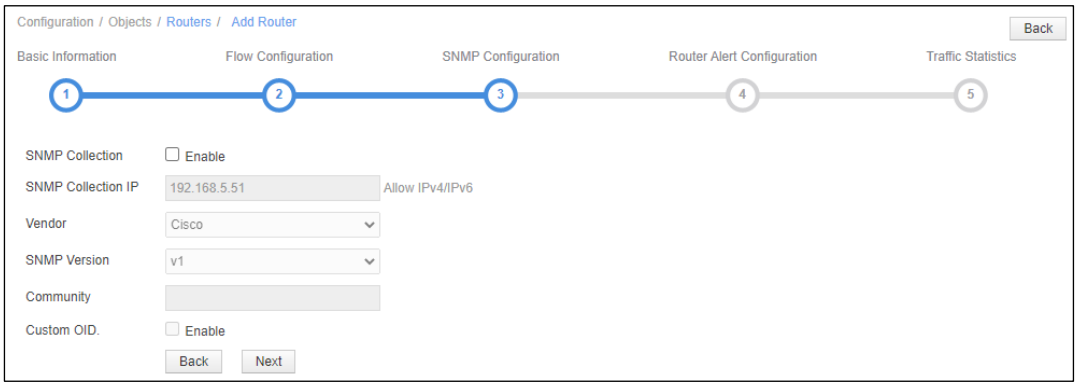


Table 5-4 describes parameters for configuring SNMP collection.

Table 5-4 SNMP configuration parameters

Parameter	Description
SNMP Collection	Controls whether to enable NTA to collect data from the router via SNMP. By default, it is not enabled.
SNMP Collection IP	Specifies the IP address from which SNMP information will be collected. The IP address here may be different from the source address of flow data. If you do not specify any IP address here, NTA uses the IP address of the router to collect SNMP information.
Vendor	Specifies the vendor of the router. Whether the CPU and memory OIDs will be collected and what algorithm will be adopted depend on the vendor. The value **Other** indicates that no CPU or memory information will be collected.
SNMP Version	Specifies the SNMP version. Currently, NTA supports data collection via SNMPv1, v2c, and v3.
context	Indicates the context of the router. This parameter is optional. It is available only when **v3** is selected for **SNMP Version**.
Community	Specifies the community string for access to the router's statistics. This parameter is available for SNMPv1 and SNMPv2c.
Username	Specifies the user name of the SNMP service user. This parameter is available for SNMPv3.
Password	This parameter must be configured when v3 is selected as the SNMP version.
Security Level	Specifies the authentication method. SNMPv3 supports three authentication methods: **No authentication**, **Account Authenticate**, and **Private Key Authenticate**. The default value is **No authentication**. Parameters vary with the authentication method. This parameter is available for SNMPv3.
Authentication Protocol	Specifies the authentication protocol, which can be **MD5** or **SHA**. This parameter is available when SNMPv3 is selected and the authentication method is **Account Authenticate** or **Private Key Authenticate**.
Private key encryption protocol	Specifies an encryption protocol. Currently, NTA supports DES and AES symmetric-key algorithms. This parameter is available when SNMPv3 is selected and the authentication method is **Private Key Authenticate**.
Private Key Password	Specifies the password for generating the authentication key. This parameter is available when SNMPv3 is selected and the authentication method is **Private Key**

Parameter	Description
	Authenticate.
Custom OID	Controls whether to enable custom OIDs. After selecting the **Enable** check box, you need to further configure related parameters.
CPU Usage OID	This is available only after custom OIDs are enabled. Specifies an OID for the CPU usage. After this is specified, the system directly uses it instead of obtaining the related OID from the attached OID document.
Memory Usage Computation Method	Specifies a method of calculating the memory usage OID, which can be either of the following: • **Usage OID**: calculates the memory usage based on the specified memory usage OID. For this method, you should specify an OID for the memory usage. • **Numerical OID**: calculates the memory usage based on multiple memory usage OIDs. For this method, you should configure at least two of the following: **Total Memory OID**, **OID of Used Memory**, and **OID of Idle Memory**.
Memory Usage OID	This parameter must be configured when custom OIDs are enabled and **Usage OID** is selected as the memory usage calculation method. Specifies an OID for the memory usage. After this is specified, the system directly uses it to calculate the memory usage instead of obtaining the related OID from the attached OID document.
Total Memory OID	This parameter must be configured when custom OIDs are enabled and **Numerical OID** is selected as the memory usage calculation method. Specifies an OID for the total memory space. After this is specified, the system directly uses it to calculate the total memory space instead of obtaining the related OID from the attached OID document.
OID of Used Memory	This parameter must be configured when custom OIDs are enabled and **Numerical OID** is selected as the memory usage calculation method. Specifies an OID for the used memory space. After this is specified, the system directly uses it to calculate the used memory space instead of obtaining the related OID from the attached OID document.
OID of Idle Memory	This parameter must be configured when custom OIDs are enabled and **Numerical OID** is selected as the memory usage calculation method. Specifies an OID for the idle memory space. After this is specified, the system directly uses it to calculate the idle memory space instead of obtaining the related OID from the attached OID document.

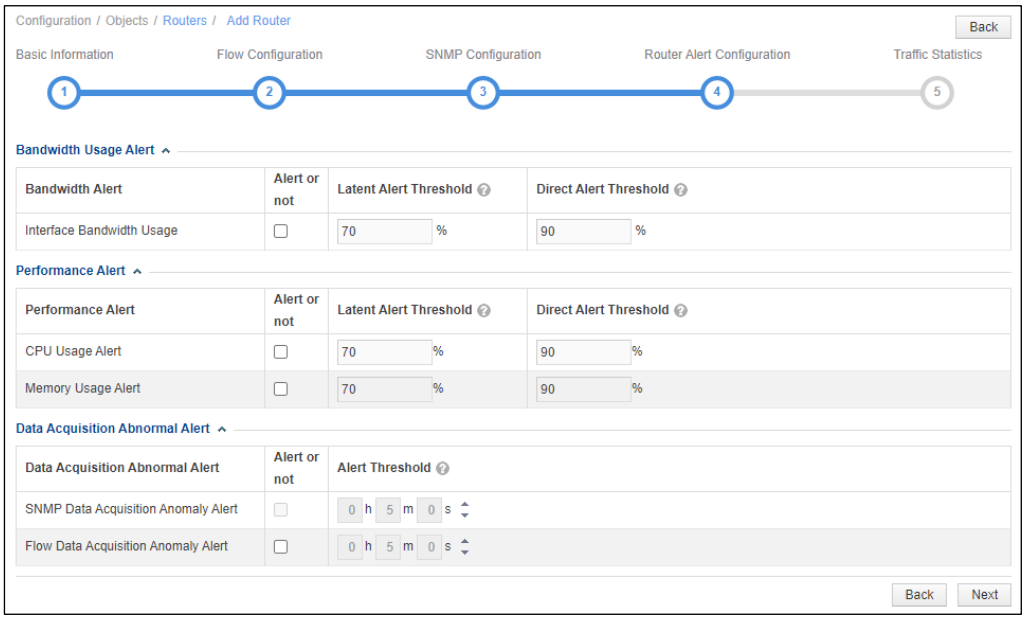
Click **Next**.

To return to the **Flow Configuration** page, click **Back**.

d. Configure router alert parameters on the page shown in Figure 5-6.

   If a router alert template is selected during the configuration of basic router information, the default settings of the template are displayed on this page. You can modify these default settings.

Figure 5-6 Router alert configuration



NTA supports alerting for abnormal bandwidth, CPU usage, and memory usage, as well as abnormal SNMP data acquisition and flow data acquisition. Here you can configure whether to enable the alerting function and alert thresholds. Table 5-5 describes router alert parameters.

Table 5-5 Router alert parameters

Parameter	Description
Alert or not	Controls whether to enable the alerting function.
Latent Alert Threshold	Specifies the bandwidth, CPU, or memory usage threshold that triggers NTA to generate an alert only after the usage stays at this level for some time (depending on **Alert Latency Period** under **Configuration > Global Alert Settings > Alert Parameters**). For the setting of **Alert Latency Period**, see section 5.3.2 Alert Parameters.
Direct Alert Threshold	Specifies the bandwidth, CPU, or memory usage threshold that triggers NTA to generate an immediate alert.
Alert Threshold	Specifies the threshold for the SNMP or flow data acquisition interruption duration, which triggers NTA to generate an immediate alert.

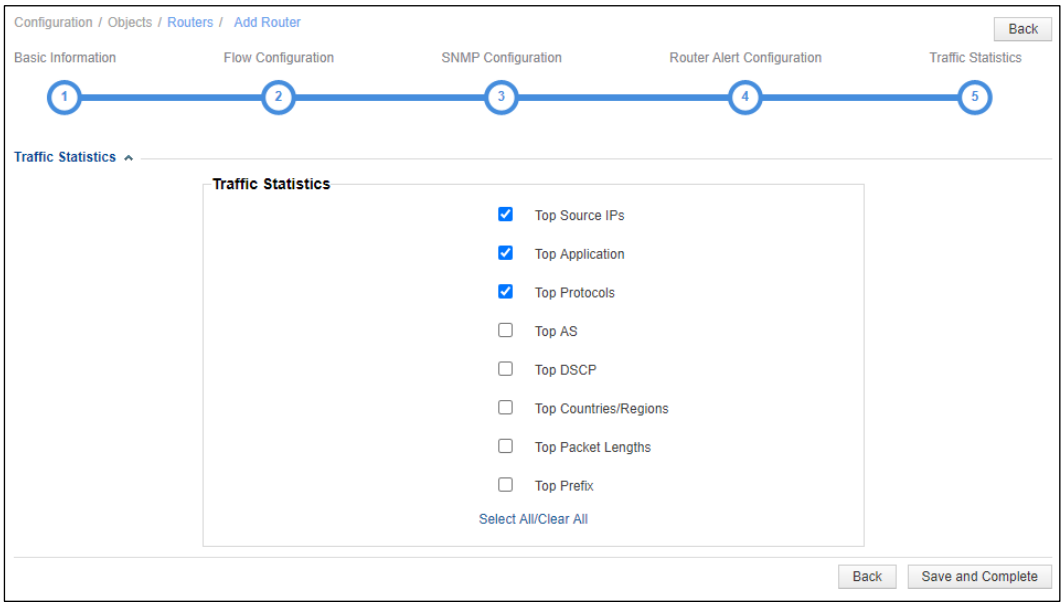
Click **Next**.

To return to the **SNMP Configuration** page, click **Back**.

e. Configure traffic statistics parameters on the page shown in Figure 5-7.

On the **Traffic Statistics** page, select statistical items of traffic.

Figure 5-7 Traffic statistics configuration



Click **Save and Complete** to commit the settings.

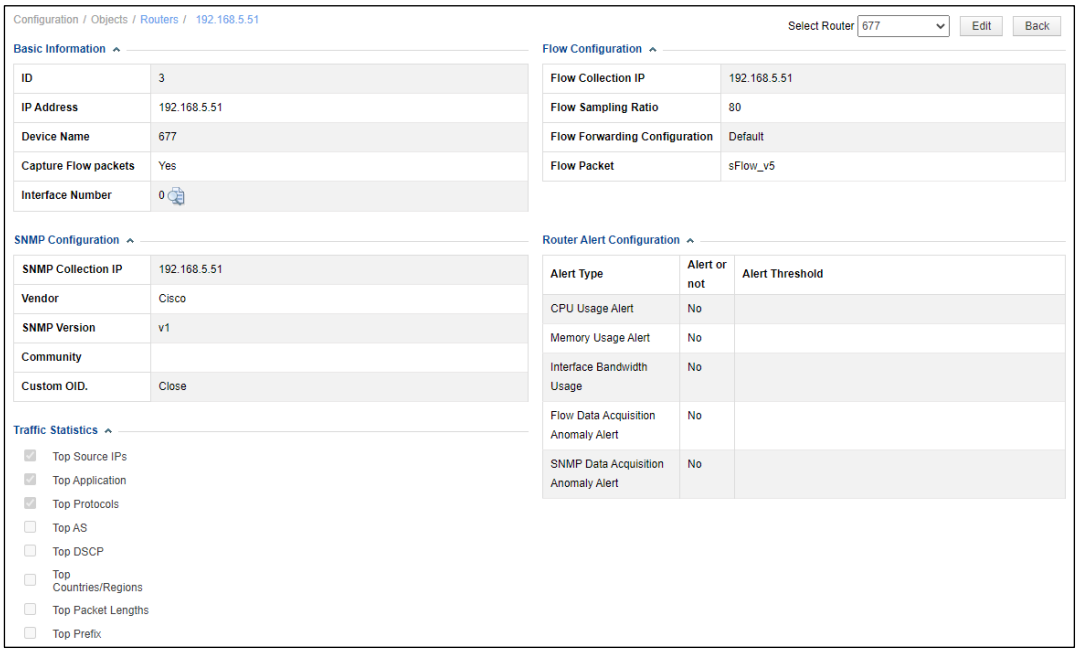
To return to the **Router Alert Configuration** page, click **Back**.

Step 4 View and modify router settings.

Clicking a device name in the router list displays all settings of the device on a page, as shown in Figure 5-8.

Alternatively, you can click in the **Operation** column. In this way, you can view and modify all settings at any step.

Figure 5-8 Router settings



- To view details about another router, select it from the **Select Router** drop-down list.
- To modify the settings, click **Edit**.
- To return to the router list page, click **Back**.
- To view the settings of all interfaces on this router, click next to the interface number. To stop monitoring an interface, click in the **Operation** column. For details, see section 5.1.1.2 Configuring Router Interfaces.

Step 5 Delete a router.

To delete a router, click in the **Operation** column.

----End

5.1.1.2 Configuring Router Interfaces

You can configure router interfaces as required, including:

- Enabling or disabling the monitoring function: After it is enabled for a router interface, NTA can monitor the traffic and bandwidth usage of this interface.
- Specifying the interface type: An interface connecting a router and the Internet is called an uplink interface, and an interface connecting a router and the server is called a downlink interface.
- Adding an interface to a router interface group: After a router interface group is configured, NTA can monitor the overall traffic of the group.

To configure router interfaces, follow these steps:

Step 1 Choose **Configuration > Objects > Routers**.

On the page shown in Figure 5-1, **Interface Number** shows the total number of interfaces, including physical interfaces and VLAN interfaces, on a router. Clicking the number displays the **Interface List** page.

Figure 5-9 Interface List page

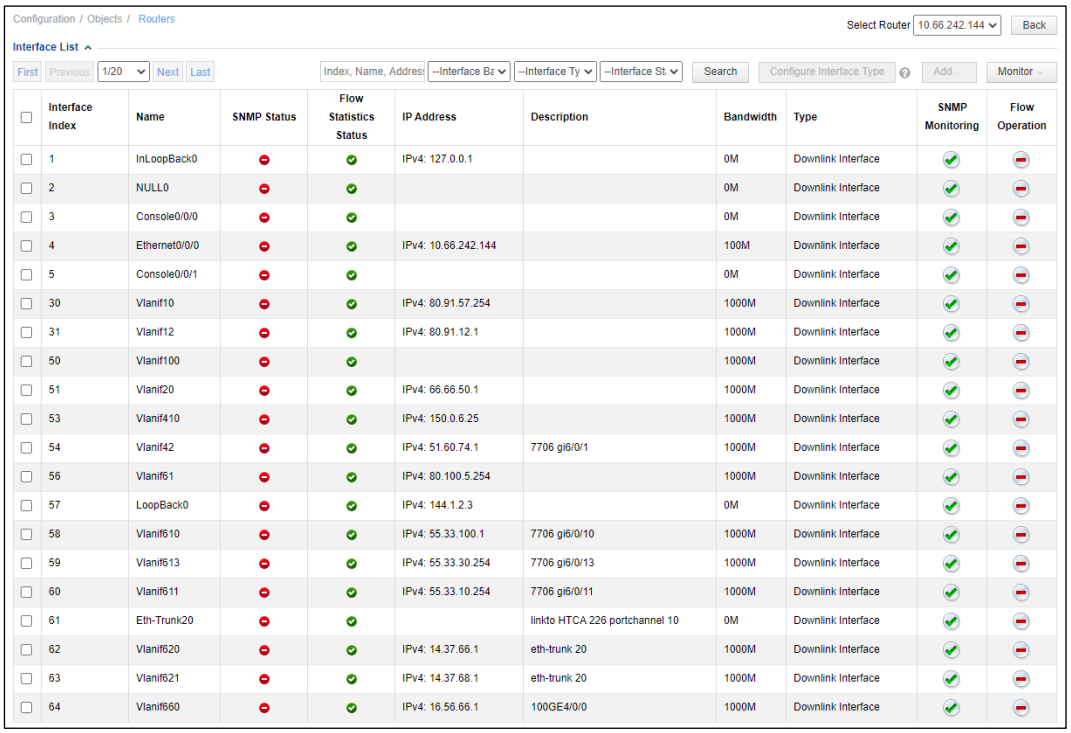


Table 5-6 describes parameters in the interface list.

Table 5-6 Parameters in the interface list

Parameter	Description
Interface Index	Indicates the interface index, which is obtained from flow data.
Name	Indicates the interface name, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, nothing is displayed here.
SNMP Status	Indicates whether SNMP is enabled to monitor traffic and bandwidth usage of the interface. indicates SNMP disabled and indicates SNMP enabled. In the former case, NTA cannot obtain traffic and bandwidth usage of the interface.
Flow Statistics Status	Indicates whether flow statistics are enabled ( ) to rank top N IP addresses, countries/regions, differentiated services code points (DSCPs) in terms of flows on the interface. After it is disabled ( ), such statistics are not collected.
IP Address	Indicates the IP address of the interface, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, or SNMP collection is enabled but no IP address is configured for this interface, nothing is displayed here.
Description	Indicates brief information about the interface, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, nothing is displayed here.
Bandwidth	Indicates the bandwidth configuration of the interface, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, **N/A** is displayed here.

Parameter	Description
Type	Indicates the interface type, which can be **Downlink Interface**, **Uplink Interface**, or **Interconnection**.
SNMP Monitoring	Indicates the SNMP operation that can be performed on the interface: enable or disable SNMP interface traffic monitoring. After this is enabled, SNMP traffic statistics are displayed under **Monitor > Routers**.
Flow Operation	Indicates the flow operation that can be performed on the interface: enable or disable flow monitoring on the interface. After this is enabled, related statistics are displayed under **Monitor > Routers**.

Step 2 Enable or disable SNMP-based monitoring.

The **SNMP Status** column shows whether SNMP is enabled for monitoring traffic and bandwidth usage of an interface.

- The icon indicates that SNMP-based monitoring is enabled. In this case, you can click in the **SNMP Operation** column to disable this function.
- The icon indicates that SNMP-based monitoring is disabled. In this case, you can click in the **SNMP Operation** column to enable this function.

Select one or more interfaces and then choose corresponding commands from the **Monitor** drop-down list to monitor or cancel monitoring on the specified interfaces. You can also choose **Monitor All** or **No Monitor** to monitor or cancel monitoring on all interfaces.

Step 3 Enable or disable flow statistics.

The **Flow Statistics Status** colomn shows whether flow statistics are enabled.

- The icon indicates that this function is enabled. In this case, you can click in the **Flow Operation** column to disable this function.
- The icon indicates that this function is enabled. In this case, you can click in the **Flow Operation** column to enable this function.

Select one or more interfaces and then choose corresponding commands from the **Monitor** drop-down list to monitor or cancel flow statistics on the specified interfaces. You can also choose **Monitor All** or **No Monitor** to monitor or cancel flow statistics on all interfaces.

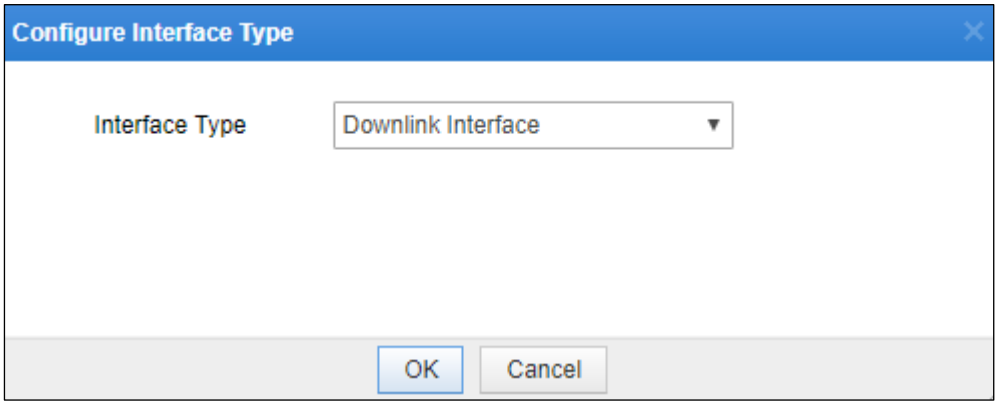
Step 4 Specify the interface type.

From the list shown in Figure 5-9, select one or more interfaces. Pointing to the question mark following **Configure Interface Type** displays the router interface topology, as shown in Figure 5-10.

Figure 5-10 Router interface topology

You can select one or more interfaces from the interface list shown in Figure 5-9 and click **Configure Interface Type**. Then the interface configuration dialog box appears, as shown in Figure 5-11.

Figure 5-11 Configuring the interface type



You can configure the specified interfaces as uplink, downlink, or interconnection interfaces. To distinguish between inbound and outbound traffic, you are advised to specify the interface type of a router as follows:

- The interface for connection to the Internet is an uplink interface.
- The interface for connection to the server is a downlink interface.
- Interfaces for connection to other routers are interconnection interfaces.

Step 5 Add interfaces to a router interface group.

Select interfaces from the interface list and click **Add**.

- If router interface groups are available, select one from the drop-down list. Then the selected interfaces are added to this group.
- If no router interface group is available or existing ones are not appropriate for the purpose, choose **Add Interface Group** to create a new group, to which the selected

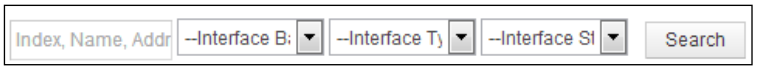
interfaces will be added. For the creation of a router interface group, see section 5.1.2 Router Interface Group.

Step 6 Query interfaces.

For a large number of interfaces, NTA displays them page by page. You can jump to the first page by clicking **First** or to the last page by clicking **Last**. You can also view these interfaces page by page by clicking **Previous** or **Next**. In addition, you can view a specific page by selecting a page number from the drop-down list.

You can set query conditions to find the desired interfaces, as shown in Figure 5-12.

Figure 5-12 Setting interface query conditions



Type the index, name, or IP address in the **Index**, **Name**, or **Address** text box. Then select the interface bandwidth, type, and/or monitoring status from the adjacent drop-down lists. Note that if SNMP-based monitoring is not enabled during router addition, **Interface Bandwidth** is unavailable.

Finally click **Search**. The qualified interfaces are listed below.

Assume that you select **8000M** for **Interface Bandwidth**. Clicking **Search** returns all interfaces with the bandwidth of 8000 Mbit/s, as shown in Figure 5-13.

Figure 5-13 Query result

Step 7 Switch to another router.

Select another router from the **Select Router** drop-down list to open the editing page of the specified router.

----End

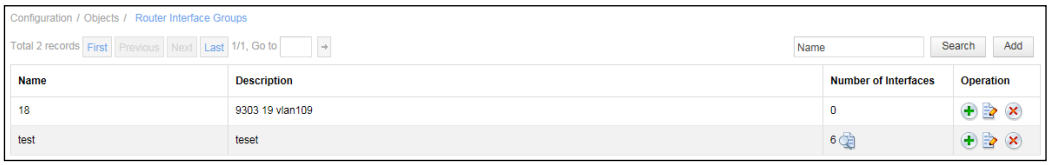
5.1.2 Router Interface Group

A router interface group is a set of interfaces on a router, used to define the network boundary. After configuration, you can monitor the overall traffic of this interface group.

To configure a router interface group, follow these steps:

Step 1 Choose **Configuration** > **Objects** > **Router Interface Groups**.

Figure 5-14 Router Interface Groups page

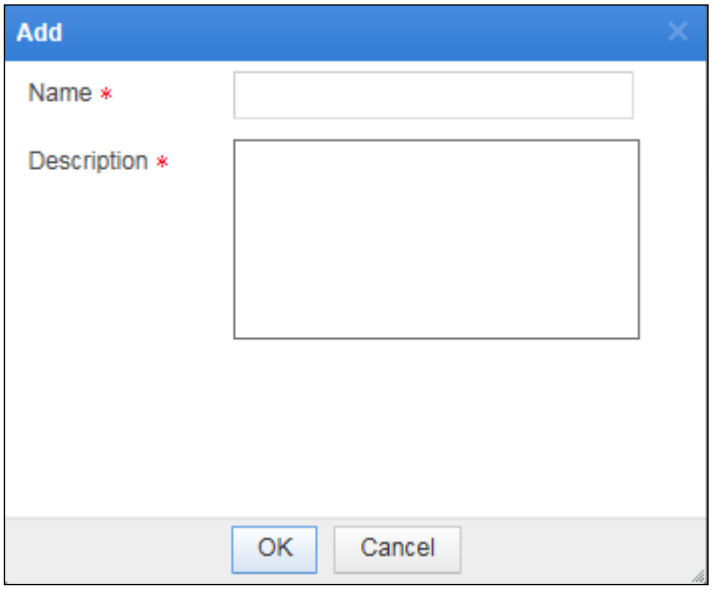


- To delete a router interface group, click in the **Operation** column.
- To change the group name and description, click in the **Operation** column.
- To add interfaces in a group, click in the **Operation** column.

Step 2 Add an interface group.

a. Click **Add**. The dialog box for adding an interface group appears, as shown in Figure 5-15.

Figure 5-15 Adding an interface group

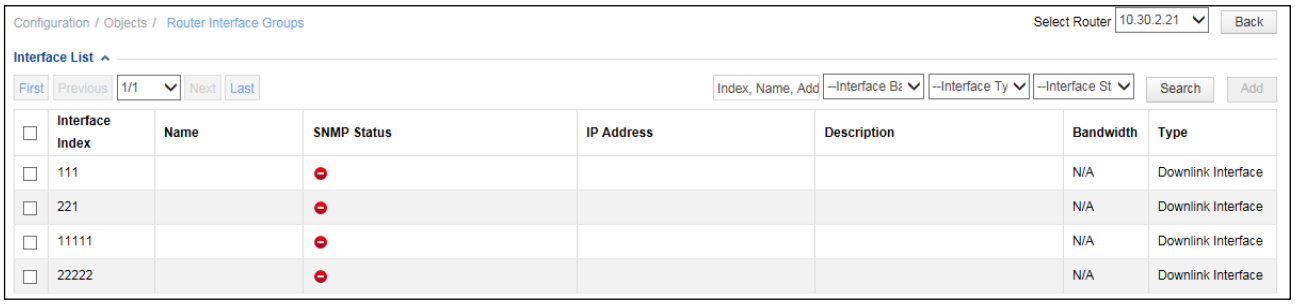


b. Enter the group name and description, and then click **OK**. The new group does not contain any interface. Therefore, **Number of Interfaces** is displayed as **0**.

Step 3 Specify interfaces to be included in the interface group.

a. Click in the **Operation** column to open the **Interface List** page.

Figure 5-16 List of interfaces to be included in the group



b. After selecting one or more interfaces, click **Add** to add them to the group.

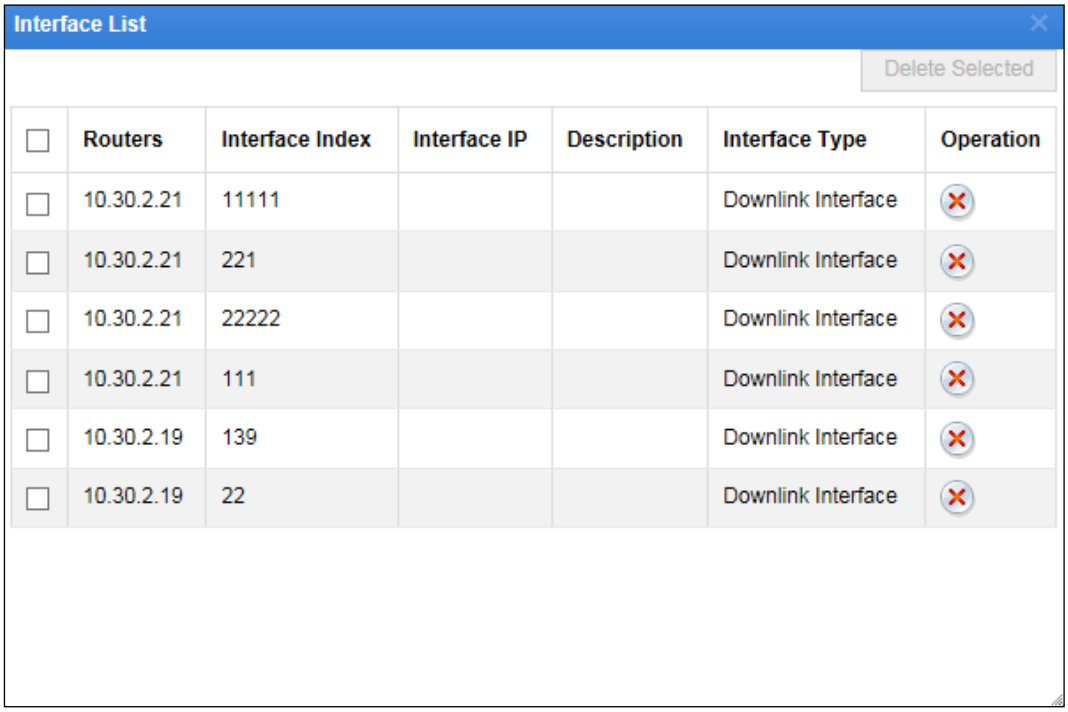
When interfaces are displayed page by page, you can specify a page to view interfaces on this page. You can also specify query conditions and then click **Search**. In this case, all desired interfaces will be listed.

Note that the **Add** button is available only after you select one or more interfaces.

Step 4 View interfaces included in an interface group.

Click next to the number of interfaces to display all interfaces in the group. See Figure 5-17.

Figure 5-17 Interfaces included in the group



To delete an interface, click in the **Operation** column. Alternatively, select one or more interfaces and then click **Delete Selected** to delete the specified interfaces.

----End

5.1.3 Region

A region is a collection of a user's or a company's businesses. On NTA, you can define a region based on IP address ranges or router interfaces to implement region-based centralized monitoring of traffic. You can further define an IP group for businesses of the same property in the region and define a traffic detection policy for this IP group.

Region configuration involves the following:

- Configuring Basic Information: configuration of such basic information as the region name and contact person
- Managing User Accounts: configuration of IP address ranges or router interfaces to be included in the region
- Configuring Traffic Alert Policies: configuration of monitoring policies for both inbound and outbound traffic of the region, including traffic alert policies, alert hierarchy policies, and alert diversion policies
- Configuring DDoS Attack Detection Policies: configuration of DDoS attack detection policies for all IP addresses in the region, including attack detection policies, alert hierarchy policies, and alert diversion policies
- Configuring Traffic Statistics: configuration of traffic statistics parameters for the region
- Configuring Traffic Diversion Rules: configuration of separate policies for diverting abnormal inbound and outbound traffic of the region, and policies for diverting traffic destined for devices encountering DDoS attacks
- Configuring an IP Group and Related Policies: configuration of an IP group for businesses of the same property in the region and configuration of a traffic detection policy for this IP group

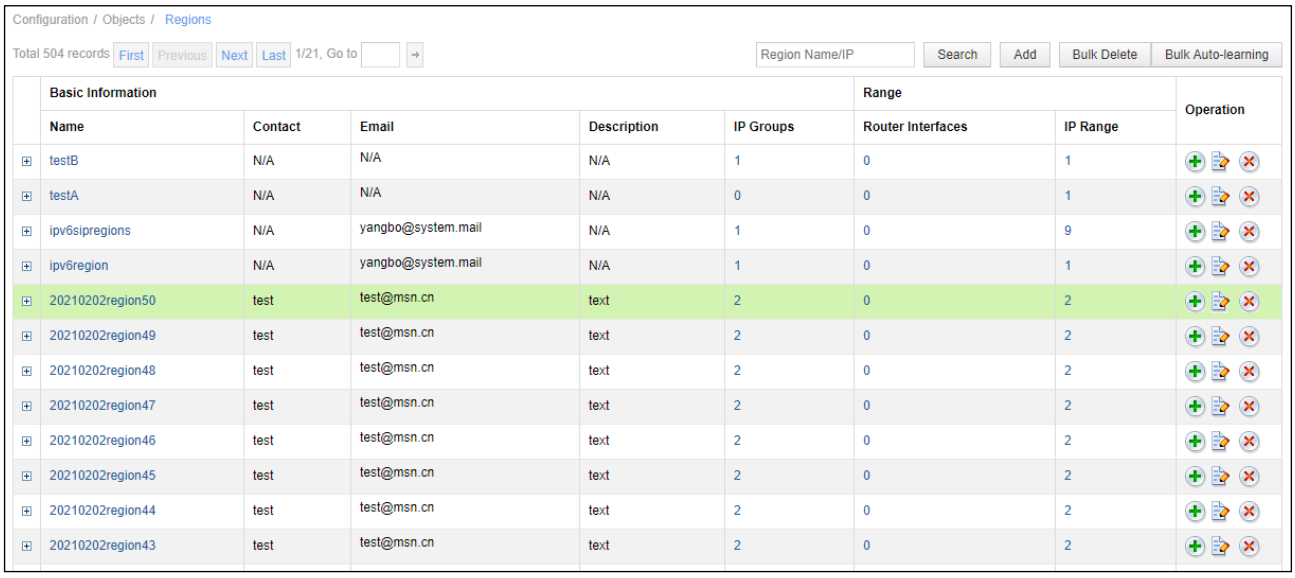
Note	• Region traffic is monitored based on traffic alert thresholds and traffic diversion rules. Traffic diversion can take place only when the traffic rate reaches the threshold and the traffic meets the diversion condition. • The policy for the IP group comes before the policy for the region when NTA implements abnormal traffic detection. When neither is hit, NTA will conduct abnormal traffic detection based on default policies.

You can configure regions one by one or in batches. This section describes how to configure a single region. For details about how to configure regions in batches, see section 5.9.1 Bulk Configuring Regions.

To configure a single region, follow these steps:

Step 1 Choose **Configuration > Objects > Regions**.

Figure 5-18 Region list



Basic information of all regions is displayed. Table 5-7 describes parameters in this list.

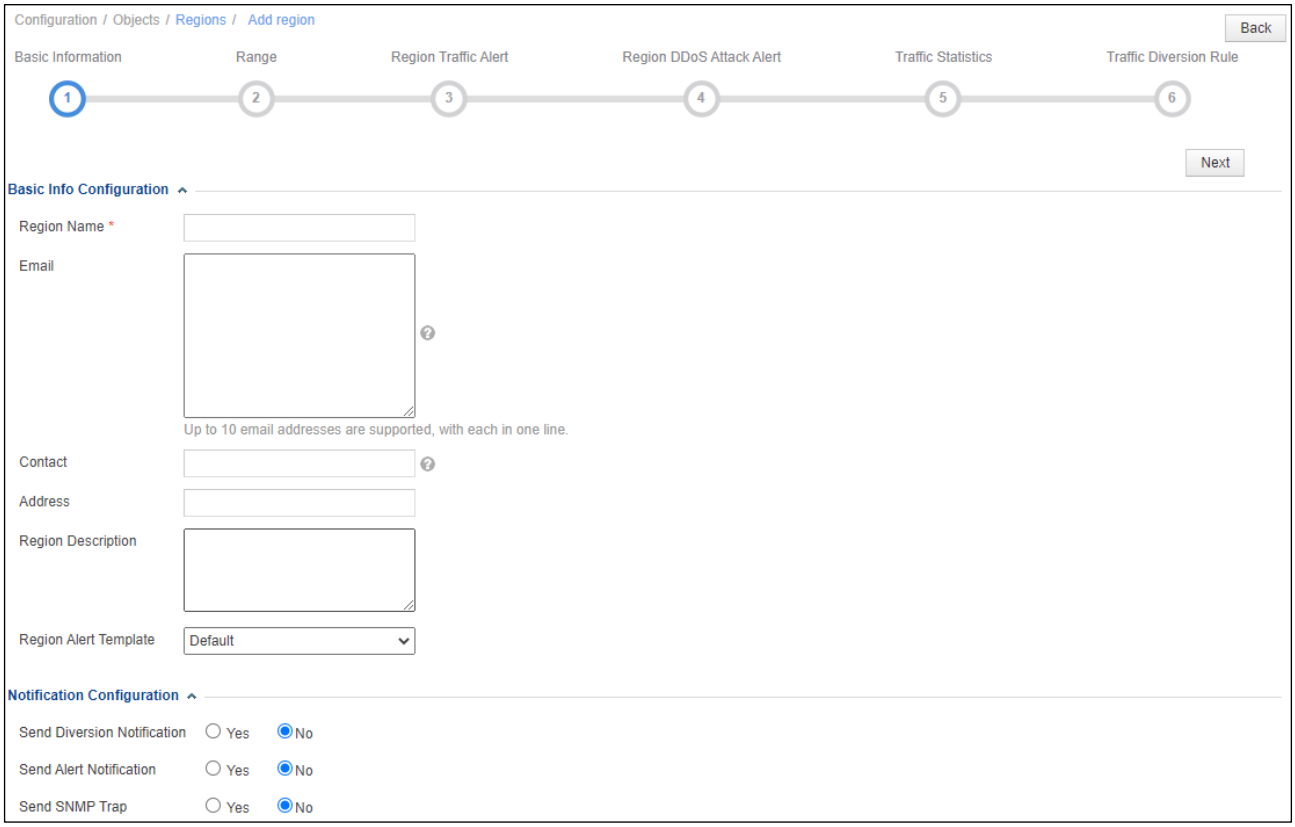
Table 5-7 Parameters in the region list

Parameter	Description
Name	Indicates the name of the region.
Contact	Specifies the name of the contact person for the region.
Email	Indicates the email address of the contact person. A maximum of 10 email addresses are allowed, with each in a separate line.
Description	Indicates the region description.
IP Group	Indicates the number of IP groups in the region. Clicking the number displays all included IP groups. Clicking ⊞ on the left of the region name displays the same information.
Router Interfaces	Indicates the number of router interfaces in the region. When the region is defined based on IP addresses, its value is displayed as **0**. Pointing to the number displays details about the interface.
IP Range	Indicates the number of IP address ranges in the region. When the region is defined based on router interfaces, its value is displayed as **0**. Pointing to the number displays details about the address ranges.
Operation	Indicates operations that can be performed for the region: • : adds an IP group. • : modifies region settings. • : deletes the region.

Step 2 Add a region.

Click **Add**. The page for adding a region appears, as shown in Figure 5-19.

Figure 5-19 Adding a region



To configure a region, you need to configure the following:

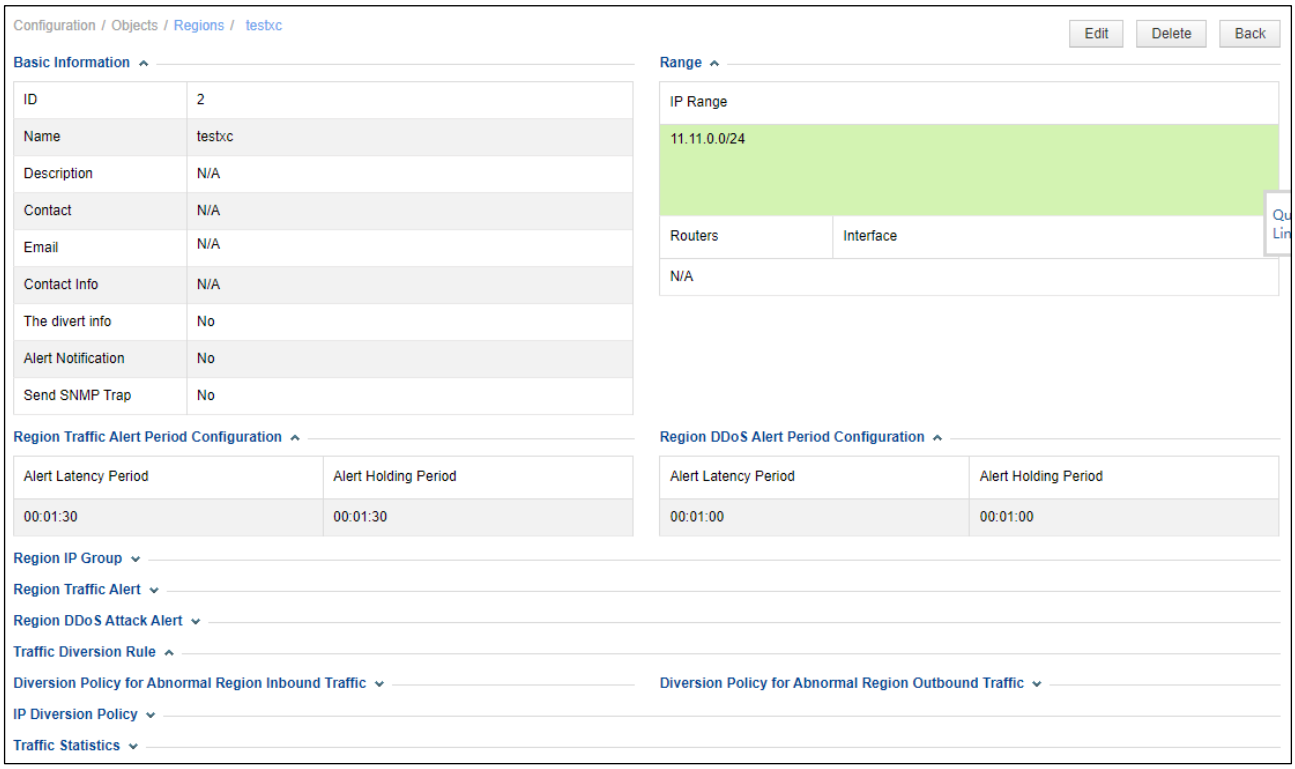
- Basic information
- Range
- Region traffic alert policies
- Region DDoS attack detection policies
- Traffic statistics parameters
- Traffic diversion rule

You can complete the configuration step by step. Alternatively, you can configure just basic information. To configure other parameters, you can modify region settings after clicking in the **Operation** column of this region.

Step 3 View and modify region settings.

Clicking the region name displays all settings of the region on one page, as shown in Figure 5-20.

Figure 5-20 Region settings



After clicking **Edit**, you can modify its settings. You can also click in the **Operation** column of the region list and then modify the settings.

A quick link is available on this page, so that you can quickly navigate to the desired area.

To return to the region list, click **Back**.

Step 4 Deleting a region.

- On the page shown in Figure 5-20, click **Delete** in the upper-right corner to delete the related region.
- On the region list shown in Figure 5-18, click in the **Operation** column of a region to delete the region.
- On the region list shown in Figure 5-18, select several regions and click **Bulk Delete** to delete them.

----End

5.1.3.1 Configuring Basic Information

To add a region, you must first configure basic information such as the region name and contact person. Figure 5-21 shows the page for configuring basic information.

Figure 5-21 Configuring basic information

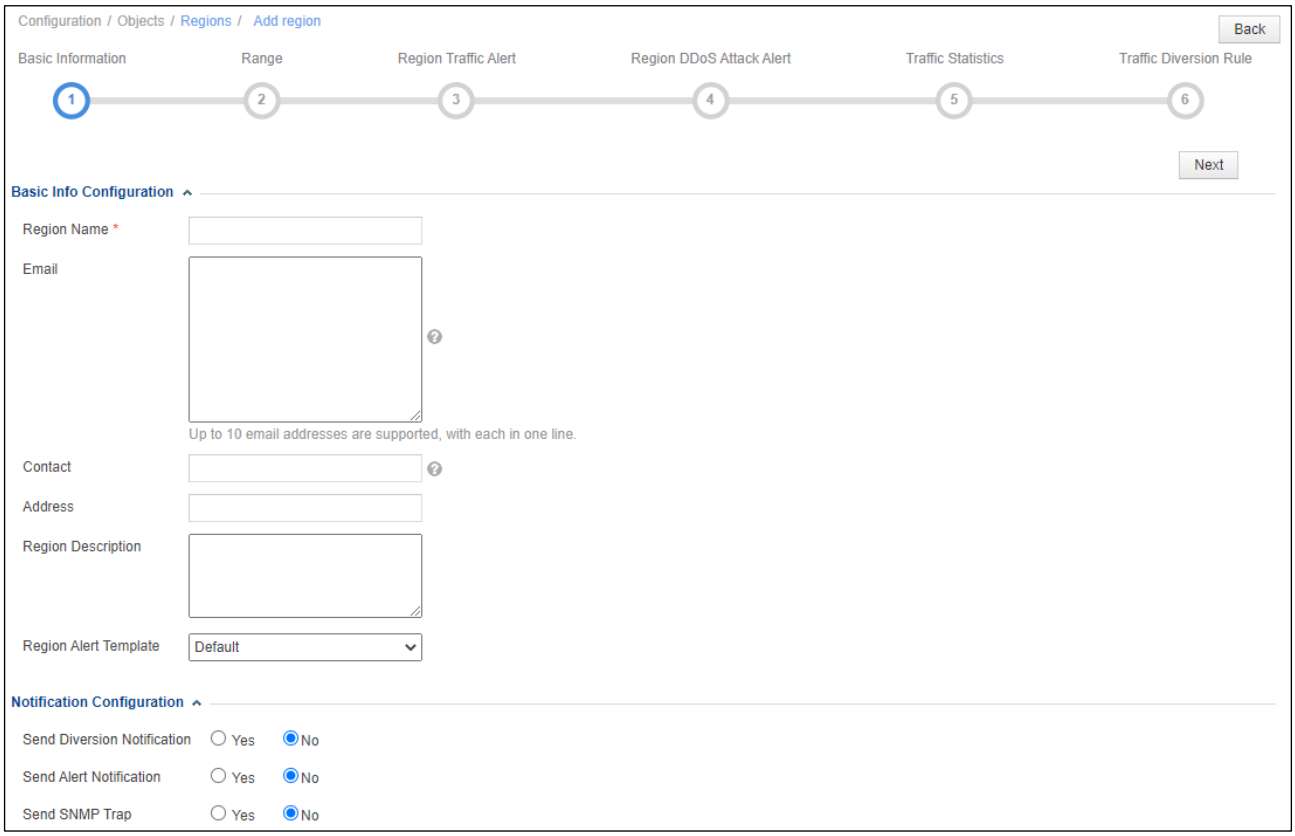


Table 5-8 describes parameters for configuring basic information of a region.

Table 5-8 Parameters for configuring basic information of a region

Parameter	Description
Region name	Specifies the name of the region to be monitored. This parameter is mandatory.
Email	Specifies the email address of the contact person. A maximum of 10 email addresses are allowed, with each in a separate line.
Contact	Specifies the name of the contact person for the region.
Address	Specifies the correspondence address of the contact person.
Region Description	Describes the region. A maximum of 50 characters are allowed.
Region Alert Template	Specifies an alert template to configure alert parameters for this region. The drop-down list displays the existing alert templates. For the configuration of a region alert template, see section 5.2.2 Region Alert Template.
Send Diversion Notification	If you select **Yes**, NTA sends a diversion notification email to the designated address of the contact when the diversion targeting a region or IP groups within a region starts and ends.
Send Alert Notification	If you select **Yes**, when an alert related to a region or IP groups within a region starts and ends, NTA sends an email to the designated address of the contact, including the destination IP address and the region or IP group to which the IP address belongs.

Parameter	Description
Send SNMP Trap	If you select **Yes**, NTA sends alerts and diversion logs about a region to the SNMP server.

After completing the configuration, click **Next**.

5.1.3.2 Configuring the IP Range

A region is a collection of the customer's businesses. You can define a region based on either of the following:

- IP address ranges: If you are clear about the IP addresses used by the customer, you can define this region based on IP address ranges. Moreover, you can define IP groups to subdivide the businesses and define different policies for these IP groups.
- Router interfaces: If you are not clear about the IP addresses used by the customer, you can define this region based on router interfaces involved in this region. In this case, no IP group can be configured.

Figure 5-22 shows the area for configuring the range.

Figure 5-22 Area for specifying IP address ranges

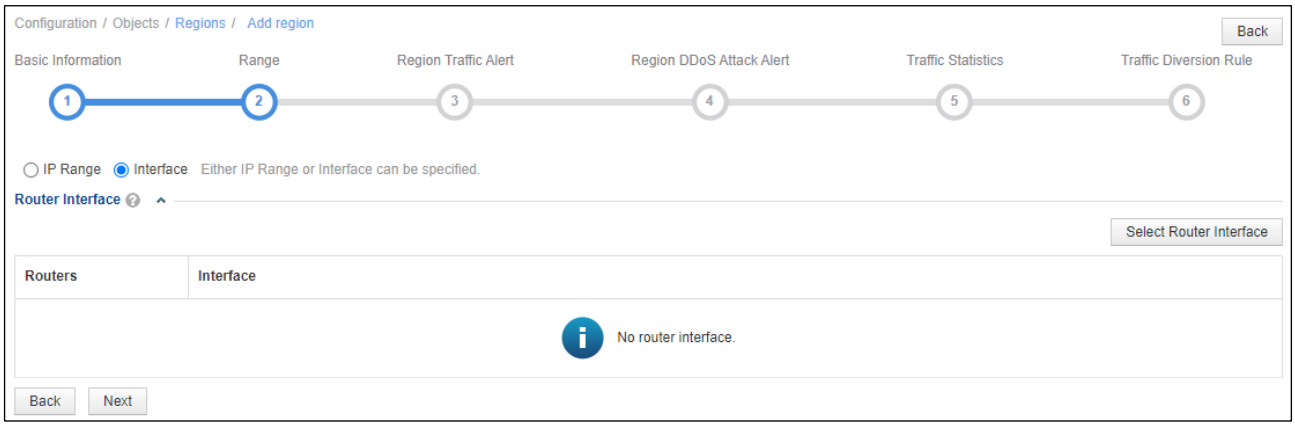
After **IP Range** is selected, you must enter IPv4 and/or IPv6 address ranges in the following formats:

- Range specified by a start IP address and an end IP address like 10.10.10.2-10.10.10.23 or 10.10.10.2-23.
- IP/mask: IPv4 address with a netmask ranging from 15 to 32 or IPv6 address with a netmask ranging from 1 to 128.
- Specific IPv4 or IPv6 address.

When the configured IP address conflicts with the existing IP address in a region, the system prompts a message indicating the region name and IP address or IP segment.

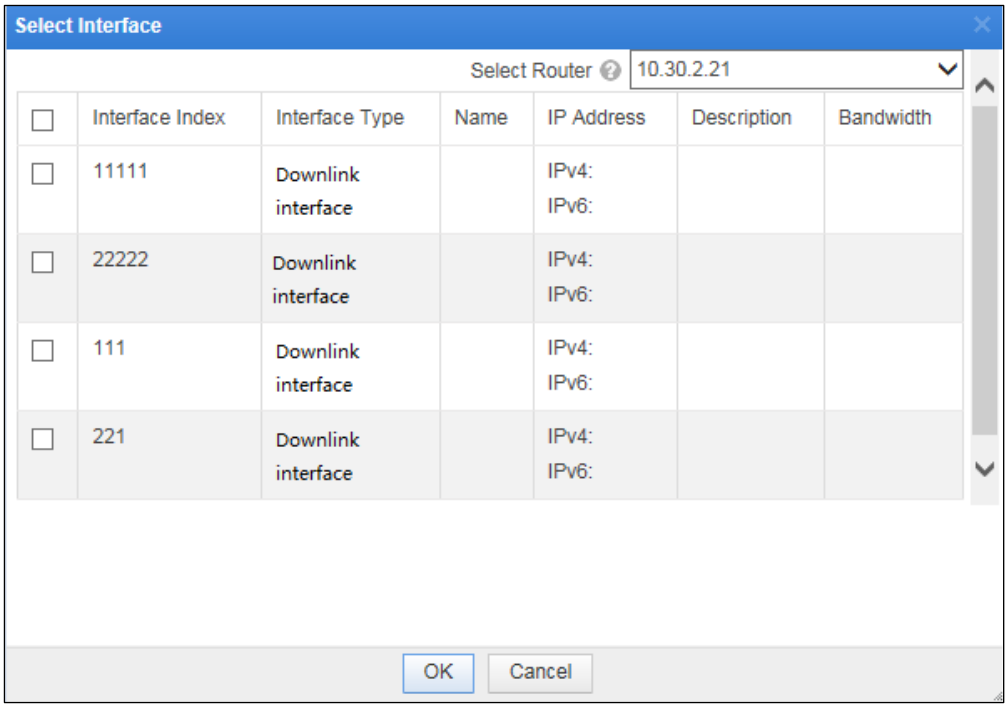
If you select **Interface**, an area shown in Figure 5-23 appears.

Figure 5-23 Area for specifying router interfaces



Click **Select Router Interface** and then select interfaces to be included in this region in the dialog box shown in Figure 5-24.

Figure 5-24 Selecting router interfaces



After you select a router from the drop-down box in the upper-right corner, all uplink and downlink interfaces of this router are then displayed in the list. For configuration of router interfaces, see section 5.1.1.2 Configuring Router Interfaces. Select one or more interfaces and then click **OK** to proceed to region traffic alert configuration.

You can click **Select Router Interface** and select interfaces for other routers. Figure 5-25 shows the configured range. A maximum of 16 interfaces can be selected for a region.

Figure 5-25 Viewing router interfaces included in a region

After completing the configuration, click **Next**.

5.1.3.3 Configuring Traffic Alert Policies

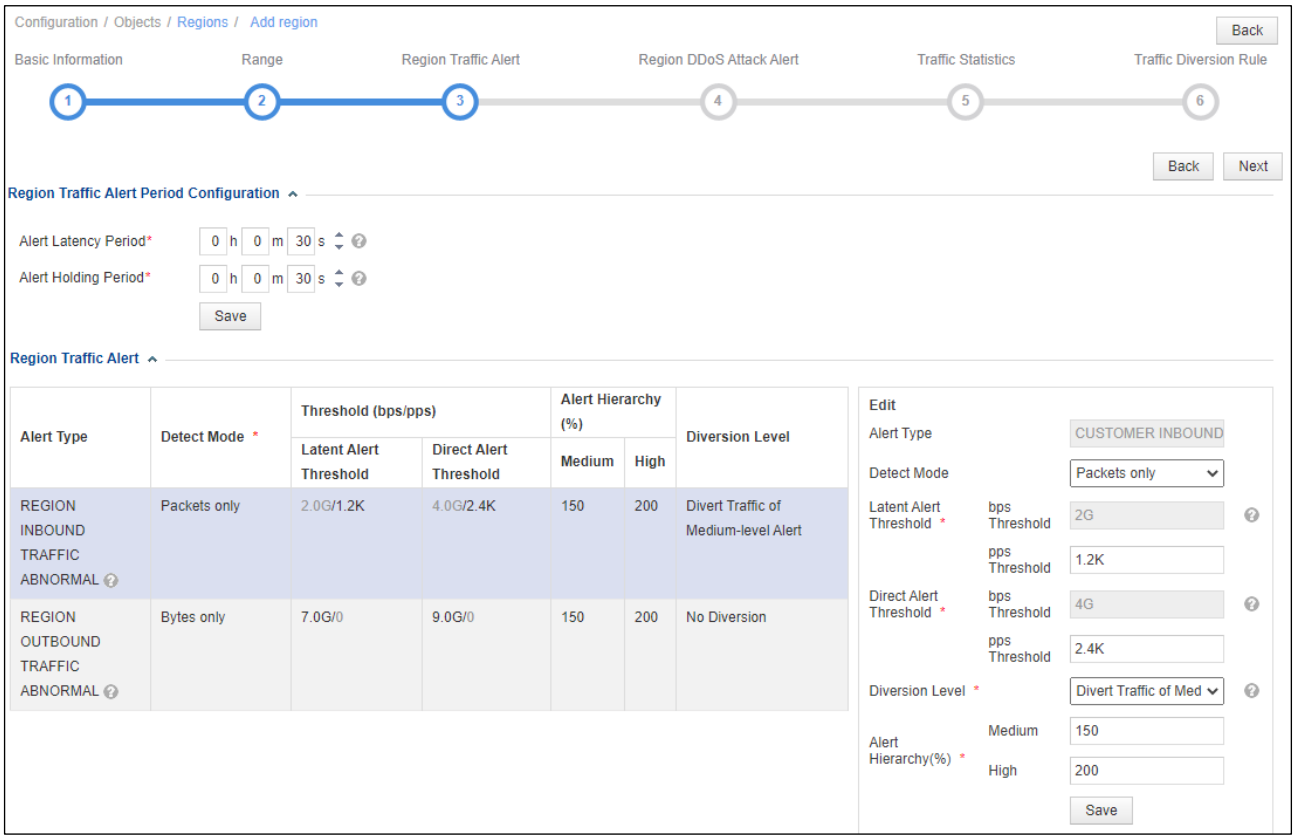
NTA can separately monitor the inbound and outbound traffic of a region after you configure traffic alert policies for the region. The traffic alert policies include the following:

- Traffic detection policies: check the inbound and outbound traffic of the entire region so that an alert can be generated when a threshold is exceeded.
- Alert hierarchy policies: set the alert hierarchy.
- Traffic diversion policies: specify which levels of alerts will trigger traffic diversion. If an alert reaches the diversion-triggering level, NTA will divert traffic as specified by the corresponding diversion policy.

When detecting abnormal traffic, NTA generates alerts at proper levels as specified by alert hierarchy policies, and divert traffic as specified by diversion policies.

Figure 5-26 shows the page for configuring traffic alert policies.

Figure 5-26 Configuring region traffic alert policies



In the **Region Traffic Alert Period Configuration** area, you can configure **Alert Latency Period** and **Alert Holding Period** for alerts triggered on abnormal traffic. For parameter description, see Table 5-16.

In the **Region Traffic Alert** area, you can configure region traffic alerts, which are divided into inbound traffic alerts and outbound traffic alerts.

When you click an alert type, the **Edit** area shows the alert type's parameters for you to edit.

Table 5-9 describes the parameters for configuring traffic alert policies.

Table 5-9 Parameters for configuring traffic alert policies

Parameter	Description
Detection Mode	Specifies the type of traffic based on which an alert is generated. It has the following values:

Parameter	Description
	• **No detection**: indicates that NTA does not check whether inbound or outbound traffic is abnormal. • **Packets only**: indicates that an alert is generated when the traffic rate in pps is found to exceed the threshold. • **Bytes only**: indicates that an alert is generated when the traffic rate in bps is found to exceed the threshold. • **Both packets and bytes**: indicates that an alert is generated when the traffic rate in pps and that in bps are both found to exceed the thresholds. • **Either packets or bytes**: indicates that an alert is generated when either the traffic rate in pps or that in bps is found to exceed the threshold.
Latent Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an alert only after the traffic rate stays at this level for some time. Note The latent alert threshold must be lower than the direct alert threshold. • **bps Threshold**: indicates a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: indicates a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Direct Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an immediate alert. Note The direct alert threshold should be greater than the latent alert threshold. • **bps Threshold**: indicates a threshold in bps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: indicates a threshold in pps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Alert Hierarchy	Specifies how to classify alert levels. **Latent Alert Threshold** is a basis for classifying alert levels and needs to be configured in advance. Alert levels are classified according to the ratio of actual traffic to the **Latent Alert Threshold** value: • **Low**: specifies the lowest ratio to trigger a low-level alert. The value is fixed to 100%. When the actual ratio is higher than the lowest ratio triggering a lower-level alert but lower than the lowest ratio triggering a medium-level alert, NTA generates a low-level alert. • **Medium**: specifies the ratio to trigger a medium-level alert. The default value is 150, and the maximum value is 10000. When the actual ratio is higher than the lowest ratio triggering a medium-level alert but lower than the lowest ratio triggering a high-level alert, NTA generates a medium-level alert. • **High**: specifies the ratio to trigger a high-level alert. The default value is 200, and the maximum value is 10000. When the actual ratio is higher than the lowest ratio triggering a high-level alert, NTA always generates a high-level alert. If the region alert hierarchy is not configured, NTA will detect traffic and send alerts according to the global alert hierarchy. For details, see section 5.3.2 Alert Parameters.

Parameter	Description
Diversion Level	Specifies the alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. For the definition of alert levels, see section 5.3.2 Alert Parameters. • **No Diversion**: indicates that no traffic diversion will take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.

After completing the configuration, click **Save** to apply the parameter settings and then click **Next** to proceed.

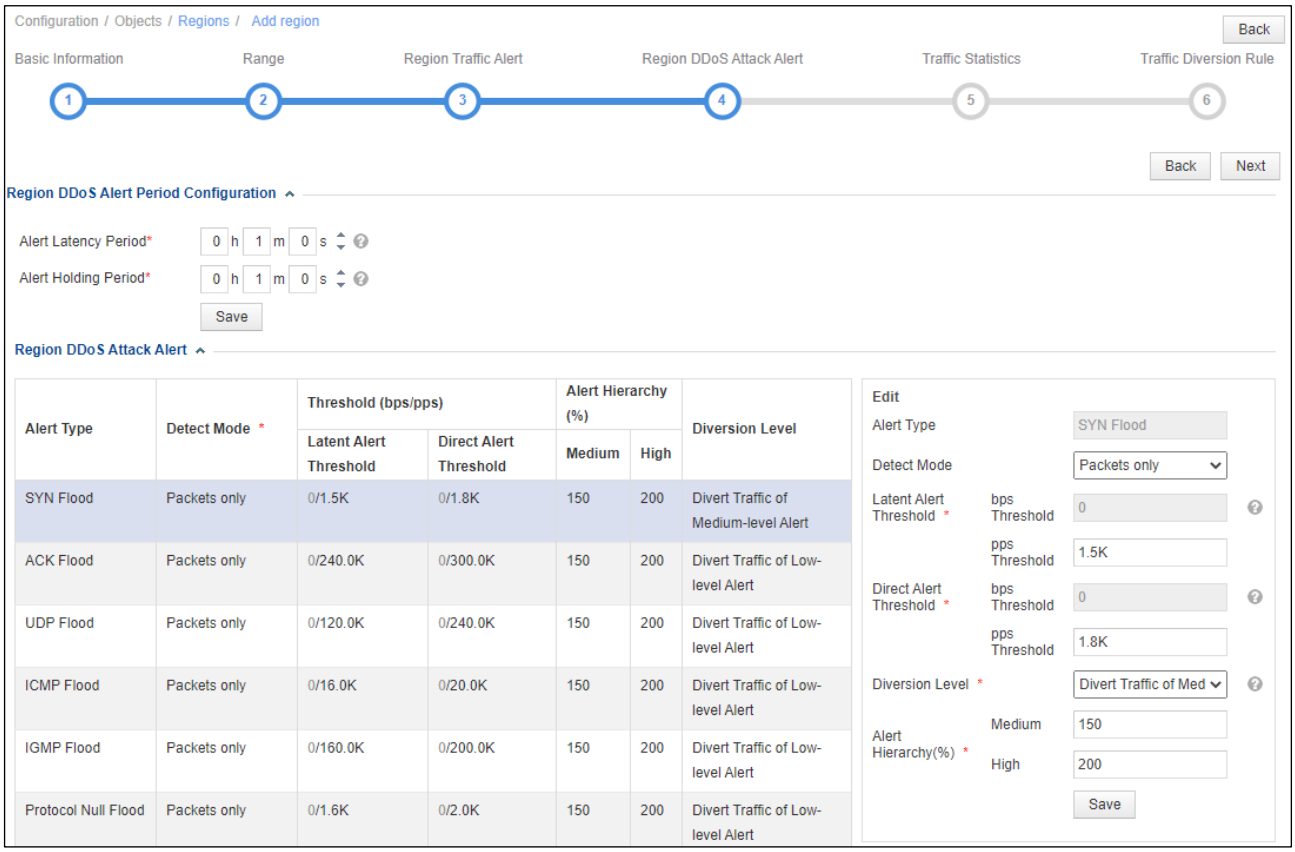
5.1.3.4 Configuring DDoS Attack Detection Policies

NTA can detect DDoS attacks for each IP address in the region. You can configure the following detection, alert, and diversion policies for various attack types:

- DDoS attack detection policies: check the traffic of each IP address. If attack signatures are matched, NTA generates alerts.
- Alert hierarchy policies: set the alert hierarchy.
- Traffic diversion policies: specify which levels of alerts will trigger traffic diversion. If an alert reaches the diversion-triggering level, NTA will divert traffic as specified by the corresponding diversion rule.

Figure 5-27 shows the page for configuring DDoS attack detection policies.

Figure 5-27 Configuring DDoS attack detection policies



In the **Region DDoS Alert Period Configuration** area, you can configure **Alert Latency Period** and **Alert Holding Period** for alerts triggerd on DDoS attacks. For parameter description, see Table 5-16.

The **Region DDoS Attack Alert** area displays all attack types that can be detected by NTA, including built-in attack types and custom ones. For adding custom attack types, see section 5.3.3 Alert Plug-in Management.

When you click an alert type, the **Edit** area shows the alert type's parameters for you to edit.

Table 5-10 describes the parameters for configuring DDoS alert policies.

Table 5-10 DDoS attack alert parameters

Parameter	Description
Detection Mode	Specifies the type of traffic based on which a DDoS attack alert is generated. It has the following values:

Parameter	Description
	• **No detection**: indicates that NTA does not check whether inbound or outbound traffic exceeds the specified threshold. • **Packets only**: indicates that an alert is generated when the traffic rate in pps is found to exceed the threshold. • **Bytes only**: indicates that an alert is generated when the traffic rate in bps is found to exceed the threshold. • **Both packets and bytes**: indicates that an alert is generated when the traffic rate in pps and that in bps are both found to exceed the thresholds. • **Either packets or bytes**: indicates that an alert is generated when either the traffic rate in pps or that in bps is found to exceed the threshold.
Latent Alert Threshold	Specifies the threshold for the aggregate inbound or outbound traffic per second of a region that matches an attack signature. When this threshold is exceeded, NTA does not generate an alert until the traffic rate stays at this level for some time (alert latency period). For the setting of **Alert Latency Period**, see section 5.3.2 Alert Parameters. Note The latent alert threshold must be lower than the direct alert threshold. The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: indicates a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: indicates a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Direct Alert Threshold	Specifies the threshold for the aggregate inbound or outbound traffic per second of a region. When this threshold is exceeded, NTA generates an immediate alert. Note The direct alert threshold must be greater than the latent alert threshold. The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: indicates a threshold in bps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: indicates a threshold in pps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Diversion Level	Specifies the alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. For the definition of alert levels, see section 5.3.2 Alert Parameters. • **No Diversion**: indicates that no traffic diversion will take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.
Alert Hierarchy	NTA supports the hierarchical structure of DDoS attack alerts and traffic anomaly alerts generated for each IP address.

Parameter	Description
	• **Low**: specifies the lowest ratio to trigger a low-level alert. The value is fixed to 100%. When the actual ratio is higher than the lowest ratio triggering a lower-level alert but lower than the lowest ratio triggering a medium-level alert, NTA generates a low-level alert. • **Medium**: specifies the ratio to trigger a medium-level alert. The default value is 150, and the maximum value is 10000. When the actual ratio is higher than the lowest ratio triggering a medium-level alert but lower than the lowest ratio triggering a high-level alert, NTA generates a medium-level alert. • **High**: specifies the ratio to trigger a high-level alert. The default value is 200, and the maximum value is 10000. When the actual ratio is higher than the lowest ratio triggering a high-level alert, NTA always generates a high-level alert.

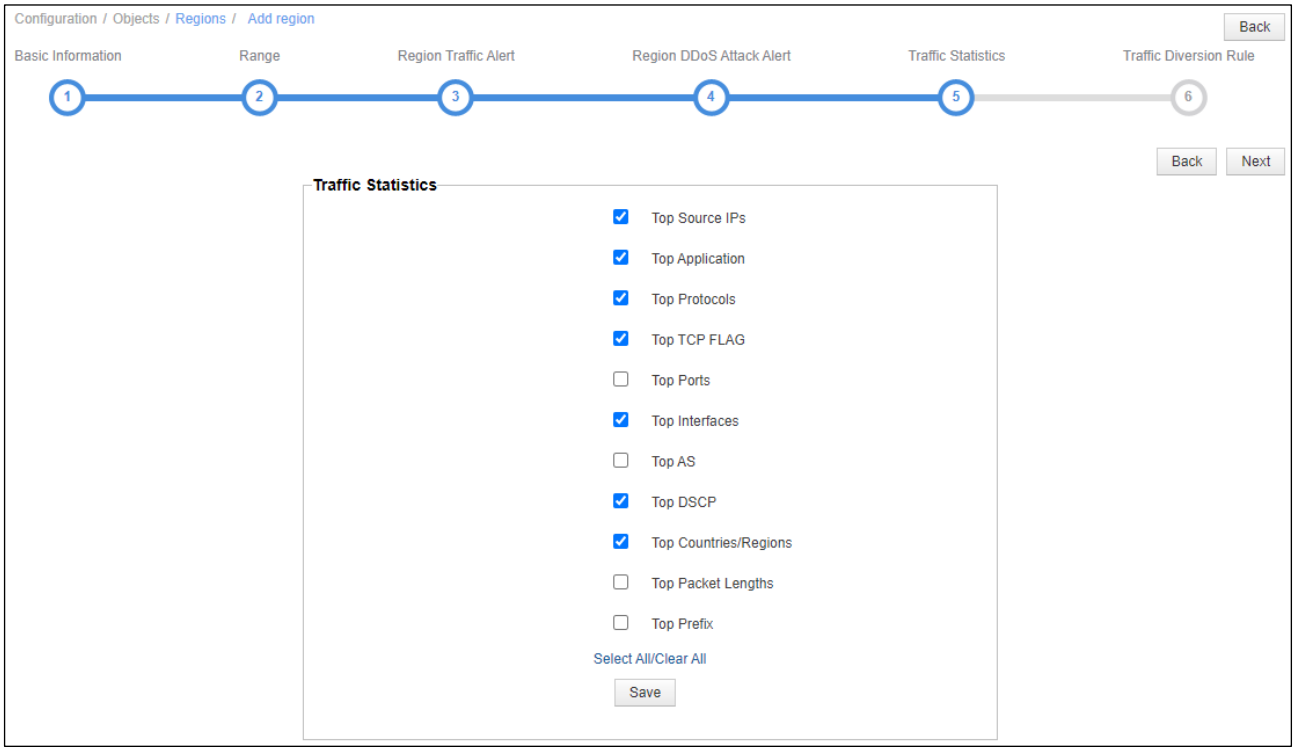
After completing the configuration, click **Save** to apply the parameter settings and then click **Next** to proceed.

5.1.3.5 Configuring Traffic Statistics

You can specify statistical items of traffic for the region.

Figure 5-28 shows the configuration page of traffic sdtatistics.

Figure 5-28 Configuring traffic statistics parameters



Select statistical items of traffic and click **Save**.

5.1.3.6 Configuring Traffic Diversion Rules

You can configure the following diversion policies to handle abnormal traffic and attack traffic of a region:

- Region-specific diversion policy

  When the inbound or outbound traffic of a region becomes so abnormal as to trigger an alert that reaches the diversion level, NTA will divert traffic to or from top n IP addresses in the region according to the diversion policy configured here.

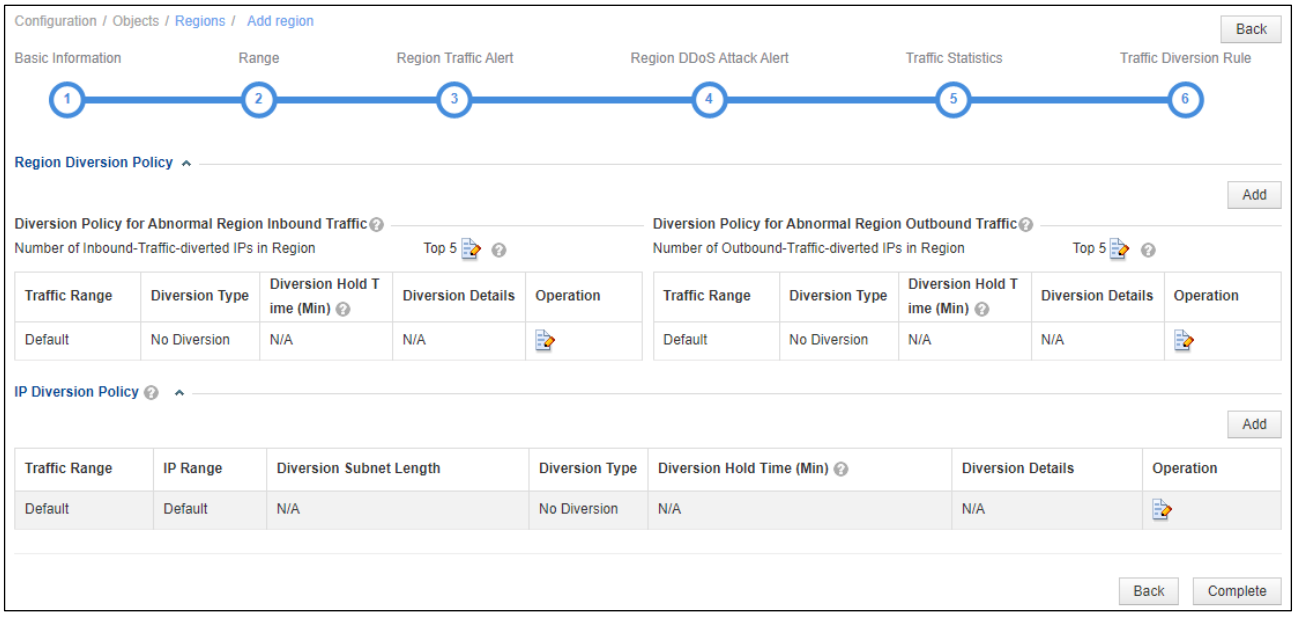
- IP address-specific diversion policy

  When traffic to or from an IP address in a region becomes so abnormal as to trigger a DDoS attack alert that reaches the diversion level, NTA will divert such traffic according to the diversion policy configured here.

Note	If no IP address-specific diversion policy is configured here, NTA will implement traffic diversion according to the default diversion policy. For how to configure diversion policies, see section 5.4.1 Default Diversion Configuration.

Figure 5-29 shows the page for configuring traffic diversion rules.

Figure 5-29 Configuring traffic diversion rules



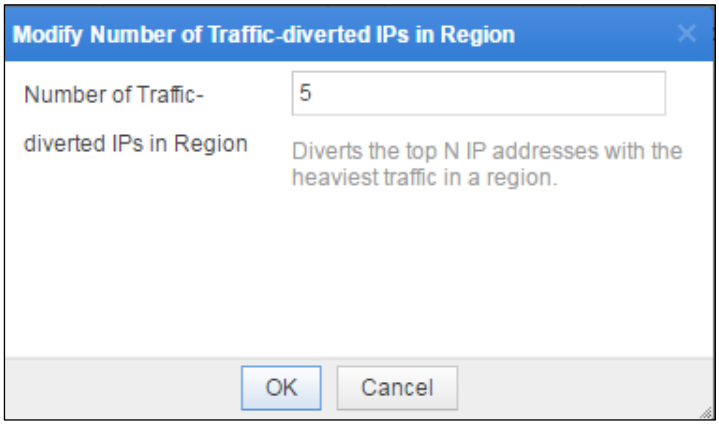
On this page, you can perform the following operations:

- Change the number of top n traffic-diverted IP addresses.

  After you specify **Number of Traffic-diverted IPs in Region**, traffic of top n addresses in the region will be diverted to a null route after the region's inbound or outbound traffic is so abnormal as to trigger the related diversion policy. The default value of **Number of Traffic-diverted IPs in Region** is **5**. You can click and then change the value to any

integer no greater than 300. Figure 5-30 shows the dialog box for changing the number of traffic-diverted IP addresses in a region.

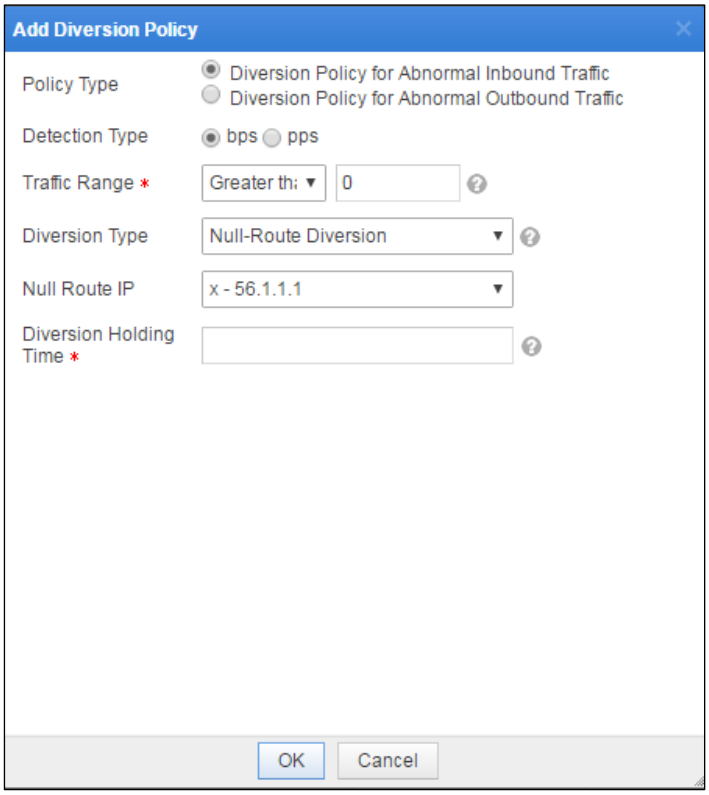
Figure 5-30 Changing the number of traffic-diverted IP addresses



- Add a region-specific diversion policy.

  Click **Add** in the upper-right corner of the **Region Diversion Policy** area. Then you can configure a diversion policy in the dialog box shown in Figure 5-31.

Figure 5-31 Adding a region-specific diversion policy



Select a policy type (for inbound or outbound traffic) and specify the traffic range.

Table 5-11 describes parameters for configuring a region-specific diversion policy.

Table 5-11 Parameters for configuring a region-specific diversion policy

Parameter	Description
Policy Type	Specifies whether the policy is for abnormal inbound or outbound traffic.
Detection Type	Specifies the traffic unit, which can be **bps** or **pps**.
Traffic Range	Specifies the traffic range, which is in the format of "number + K/M/G", such as 800M or 100K.
Diversion Type	Specifies a diversion type. It has the following values: • **No Diversion**: indicates that NTA will not divert abnormal traffic. • **BGP Diversion**: indicats that NTA will divert abnormal traffic to a third-party cleaning device. • **Null-Route Diversion**: indicates that NTA will drop abnormal traffic by diverting it to a null route.
Protection Device	Destination cleaning device for BGP diversion. This must be specified when **BGP Diversion** is selected for **Diversion Type**. A third-party device will be selected from the drop-down box for traffic cleaning. For how to configure a third-party cleaning device, see section 5.4.3 Protection Device Configuration.
Null Route IP	Destination IP address of the null route. This must be specified when **Null-Route Diversion** is selected for **Diversion Type**. For how to configure a null route IP address, see section 5.4.2 BGP Configuration.
Diversion Holding Time	Specifies how long a diversion route will remain valid. This must be specified when **BGP Diversion** or **Null-Route Diversion** is selected for **Diversion Type**. After sending a "BGP/Null-Route Diversion" notification to a device, NTA will start a countdown for the diversion when the attack traffic changes and matches a new diversion type. Once the diversion holding time expires, NTA revokes the diversion. **0** indicates immediate revocation of the diversion and no holding.

After completing the configuration, click **OK**.

- Add an IP address-specific diversion policy.

  You can configure IP address-specific policies to enable traffic diversion to be triggered by a DDoS attack alert. For different IP address ranges in a region, you can configure different diversion policies.

  Click **Add** in the upper-right corner of the **IP Diversion Policy** area. Then you can configure a diversion policy in the dialog box shown in Figure 5-32.

Figure 5-32 Adding an IP address-specific diversion policy

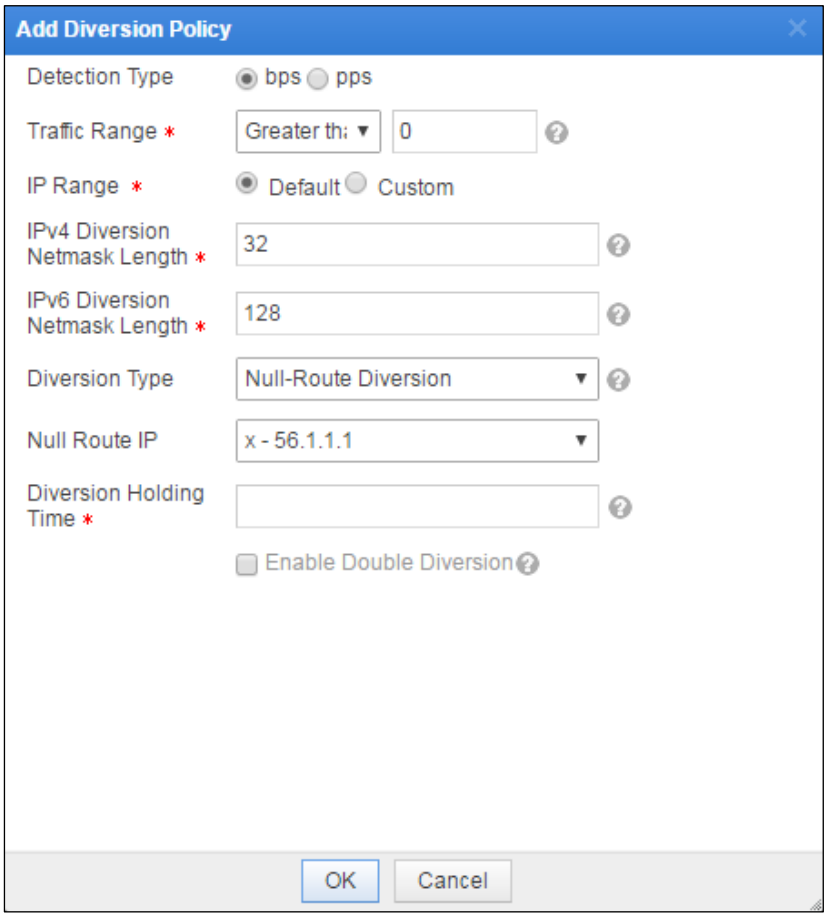


Table 5-12 describes parameters for configuring an IP address-specific diversion policy.

Table 5-12 Parameters for configuring an IP address-specific diversion policy

Parameter	Description
Detection Type	Specifies the traffic unit, which can be **bps** or **pps**.
Traffic Range	Specifies the traffic range, which is in the format of "number + K/M/G", such as 800M or 100K.
IP Range	Specifies an IP address or IP segment for which the traffic to be diverted is destined. It has the following values: • **Default**: indicates the diversion policy when no IP address or IP segment is matched. • **Custom**: indicates the diversion policy when the specified IP address segment is matched.
IPv4 Diversion Netmask Length	This parameter is available only when **Diversion Type** is set to **BGP Diversion**, **FlowSpec Diversion**, or **Null-Route Diversion**. The diversion prefix length is used to control the route netmask sent by NTA. For example, the value **32** indicates that NTA sends only one host route for diversion; the value **24** indicates that NTA sends a 24-bit netmask for diversion. The default value is **32**. The value range is 15–32.
IPv6 Diversion	This parameter is available only when **Diversion Type** is set to **BGP Diversion**, **FlowSpec Diversion**, or **Null-Route Diversion**. Specifies the diversion prefix length

Parameter	Description
Netmask Length	of the IPv6 address. The default value is **128**. The value range is 1–128.
Diversion Type	Specifies a diversion type. It has the following values: • **No Diversion**: indicates that NTA will not divert attack traffic. • **ADS Diversion**: indicates that the router forwards the traffic to ADS for cleaning upon receiving a routing notification from ADS which is notified by NTA of abnormal traffic. For how to specify such an ADS for this purpose, see section 5.4.3 Protection Device Configuration. • **BGP Diversion**: indicates that NTA sends a BGP routing notification to the router for traffic diversion. For this purpose, you need to select a configured third-party router. For details, see section 5.4.3 Protection Device Configuration. For how to configure BGP parameters for sending routing notifications, see section 5.4.2 BGP Configuration. • **Null-Route Diversion**: indicates that NTA will drop attack traffic by diverting it to a null route. For this purpose, you need to configure a null route IP address, that is, the destination IP address to which traffic will be diverted. For how to configure a null route IP address, see section 5.4.2 BGP Configuration. • **FlowSpec Diversion**: indicates that NTA will use FlowSpec to automatically divert traffic when detecting abnormal traffic.
Protection Device	Destination cleaning device for BGP diversion. This must be specified when **BGP Diversion** is selected for **Diversion Type**. A third-party device will be selected from the drop-down box for traffic cleaning. For how to configure a third-party cleaning device, see section 5.4.3 Protection Device Configuration.
Null Route IP	Destination IP address of the null route. This must be specified when **Null-Route Diversion** is selected for **Diversion Type**. For how to configure a null route IP address, see section 5.4.2 BGP Configuration.
Action	This parameter is available only when **Diversion Type** is set to **FlowSpec Diversion**. • **accept**: indicates that NTA will instruct the router to accept traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **discard**: indicates that NTA will instruct the router to drop traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **rate_limit**: indicates that NTA will instruct the router to limit the traffic rate by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **redirect**: indicates that NTA will instruct the router to redirect traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **traffic_marking**: indicates that NTA will instruct the router to mark traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration.
FlowSpec BGP	This parameter is available only when **Diversion Type** is set to **FlowSpec Diversion**. Specifies a BGP neighbor.
Diversion Holding Time	Specifies how long a diversion route will remain valid. This must be specified when **Null-Route/BGP/ADS/FlowSpec Diversion** is selected for **Diversion Type**. After sending a "Null-Route/BGP/ADS/FlowSpec Diversion" notification to a device, NTA will start a countdown for the diversion when the attack traffic changes and matches a new diversion type. Once the diversion holding time expires, NTA revokes the diversion. **0** indicates immediate revocation of the diversion and no holding.
Enable Double	Controls whether to enable double diversion. Double diversion indicates that two

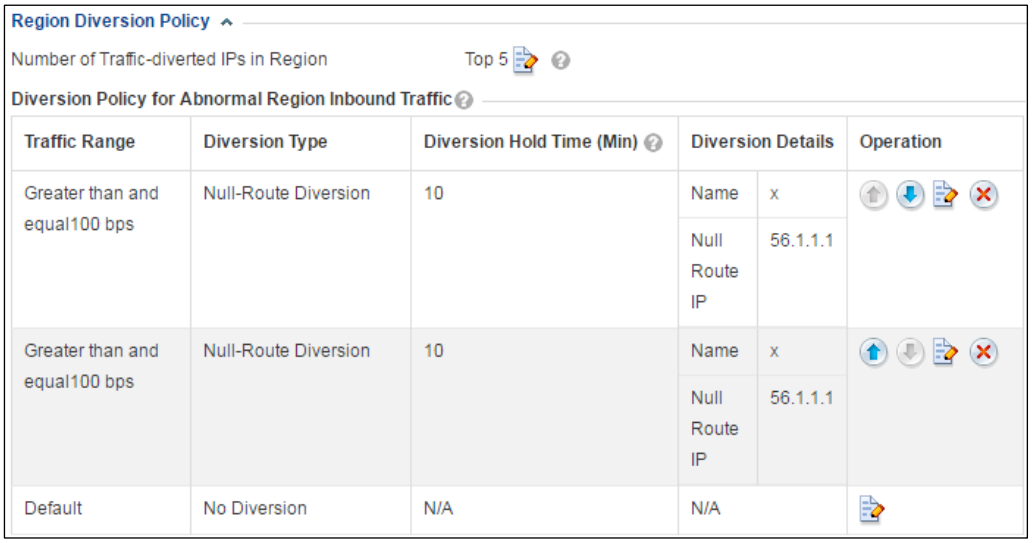
Parameter	Description
Diversion	diversion actions can be configured for a diversion rule. For the two diversion types, the IP range is the same, but the IPv4 or IPv6 diversion prefix length can be different. For example, if BGP1 and BGP2 diversion types are configured for a diversion policy, the IP range is the same, but the IPv4 or IPv6 diversion prefix lengths are /24 and /32 respectively.

After completing the configuration, click **OK**.

- Change the policy priority.

  When multiple diversion policies are available, they are displayed in descending order of priority, as shown in Figure 5-33. When a policy is hit, NTA diverts traffic according to this policy.

Figure 5-33 Traffic diversion policies sorted in descending order of priority



You can click in the **Operation** column to raise the priority or to lower the priority.

- Modify or delete a policy.

  You can click or in the **Operation** column to edit or delete a policy.

5.1.3.7 Configuring an IP Group and Related Policies

A region may contain different types of business. For example, a region may contain a web IP group, a game IP group, and a DNS IP group. For more accurate traffic detection, you can define an IP group for each of these groups and configure detection and diversion rules for each IP group.

IP group configuration involves the following tasks:

- Adding an IP Group and Related Policies
- Configuring the Auto-Learning Baseline: configuration of the function of dynamically learning DDoS attack traffic for determining baseline thresholds for an IP group.

Adding an IP Group and Related Policies

To add an IP group, you need to configure the following:

- Basic information: configuration of basic information such as the IP group name.
- Range: configuration of IP address ranges to be included in the IP group.
- Traffic alerting: configuration of inbound and outbound traffic alert thresholds, alert hierarchy policies, and diversion levels.
- DDoS attack alerting: configuration of DDoS attack detection policies, alert thresholds, and diversion policies for the entire IP group. If traffic auto-learning has been configured, NTA dynamically adjusts DDoS attack alert thresholds according to auto-learning results.
- Traffic diversion rule: configuration of policies for diverting abnormal traffic received or sent by the IP group and a policy for diverting DDoS attack traffic targeting a specific device IP address.

Note	If an IP address belongs to both an IP group and a region, the priority of traffic diversion policies is IP group policy > region policy > default policy. That is to say, NTA first checks traffic against the policy for the IP group and will handle the traffic accordingly if that policy is hit; otherwise, NTA uses the policy for the region and then the default policy to detect abnormal traffic.

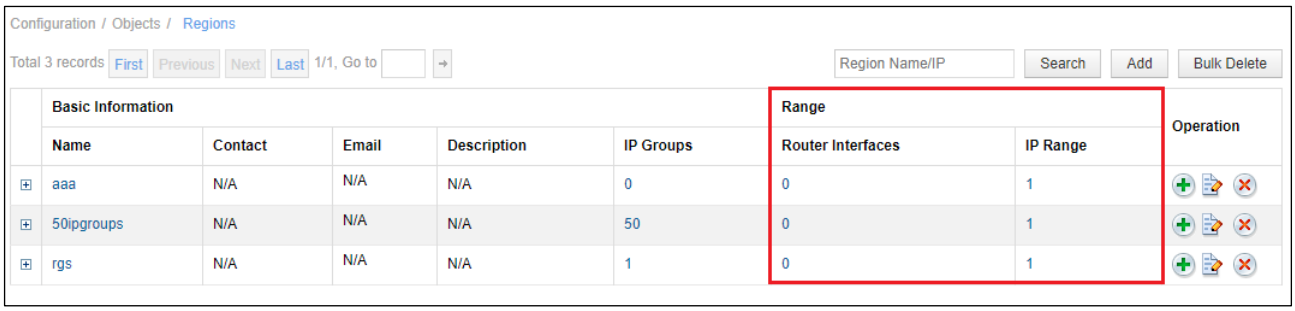
You can configure IP groups one by one or in batches. This section describes how to configure a single IP group. For details about how to configure IP groups in batches, see section 5.9.2 Bulk Configuring IP Groups.

To add a single IP group, follow these steps:

Step 1 Choose **Configuration > Objects > Regions**.

On the **Regions** page, you can see existing regions, as shown in Figure 5-34.

Figure 5-34 Region list



You can determine whether a region is configured based on router interfaces or IP address ranges from **Range**:

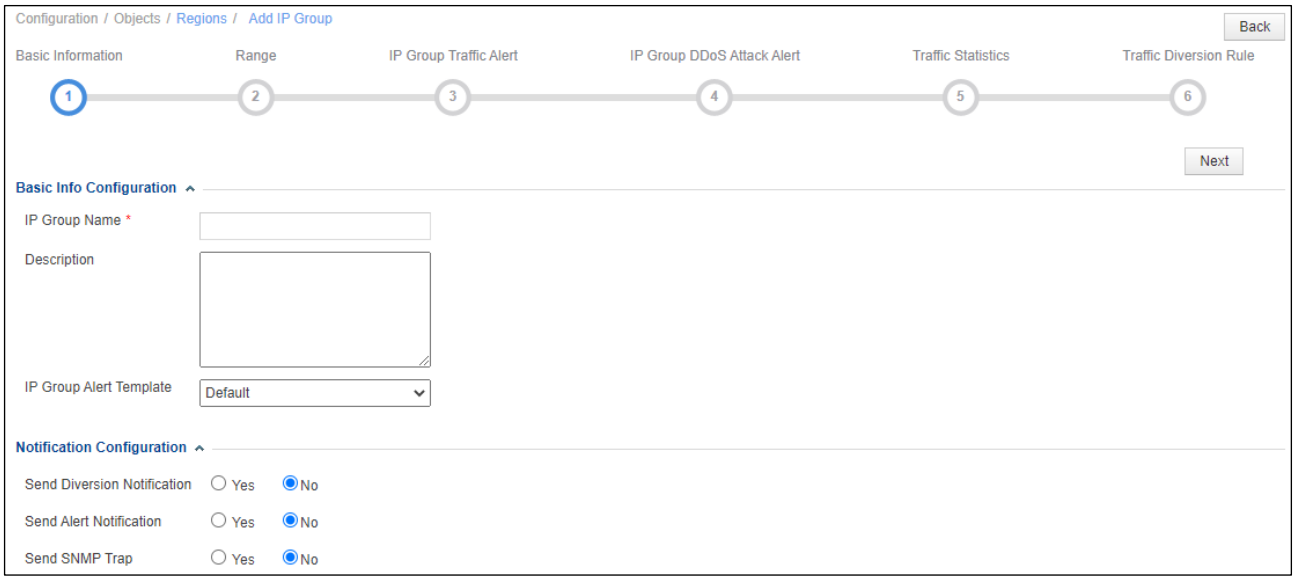
- If a region is configured based on router interfaces, the **Region IP Range** value is displayed as **0**. For this type of region, you cannot add IP groups.
- If a region is configured based on IP address ranges, the **Router Interfaces** value is displayed as **0**. For this type of region, you can add IP groups.

Step 2 Click in the **Operation** column to add an IP group.

To add an IP group, you must complete the following tasks:

a. Configure basic information such as the IP group name and notification parameters.

Figure 5-35 Basic Information page for adding an IP group



Enter the IP group name and, optionally, description. Then select an existing alert template or **Default** and choose whether to send various notifications.

Table 5-13 describes parameters for configuring an IP group.

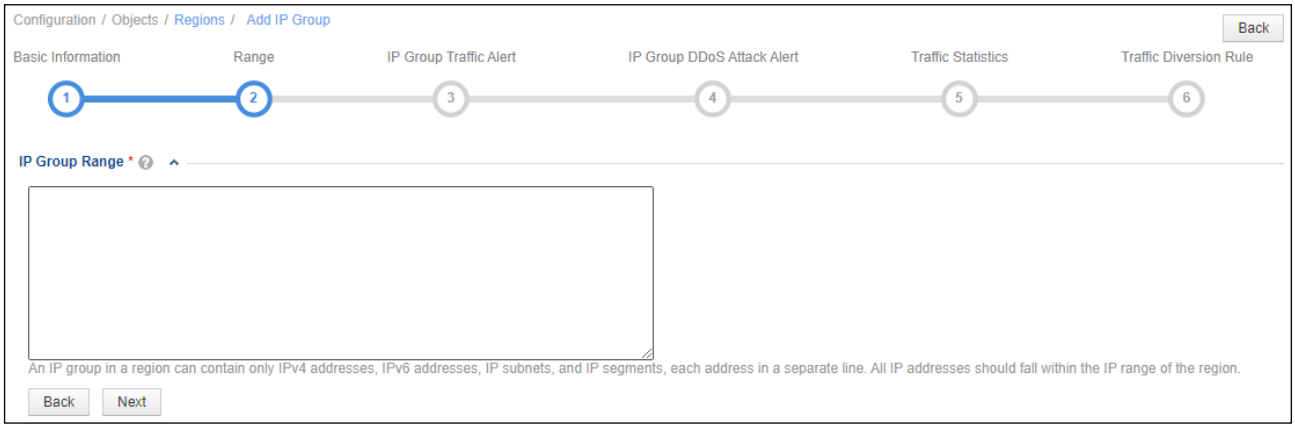
Table 5-13 Parameters for configuring basic information of an IP group

Parameter	Description
IP Group Name	Name of the IP group to be monitored. This parameter is mandatory.
Description	Necessary description of the IP group. A maximum of 500 characters are allowed.
IP Group Alert Template	Specifies an alert template for this IP group. The drop-down list displays existing alert templates. For the configuration of an IP group alert template, see section 5.2.3 IP Group Alert Template.
Send Diversion Notification	Controls whether to notify the related region's contact person of the diversion by email. If you select **Yes**, when an automatic diversion for an IP address in the IP group starts and ends, NTA will send a notification to the contact email address specified during creation of the region to which the IP group belongs.
Send Alert Notification	Controls whether to notify the contact person of the related region of generated alerts by email. If you select **Yes**, when an alert related to an IP address in the IP group is generated, NTA will send a notification to the contact email address specified during creation of the region to which the IP group belongs.
Send SNMP Trap	Controls whether to send alerts and diversion logs of this IP group to the SNMP server.

Parameter	Description
	If you select **Yes**, NTA will send alerts and diversion logs related to the IP group to the SNMP server.

b. Click **Next** and configure IP addresses to be included in the IP group on the page shown in Figure 5-36.

Figure 5-36 Range page for adding an IP group



IP address ranges in an IP group cannot be beyond the IP address ranges of the region. You can enter IPv4 and/or IPv6 addresses in the following formats:

- Range specified by a start IP address and an end IP address like 10.10.10.2-10.10.10.23 or 10.10.10.2-23
- IP/mask: IPv4 address with a netmask ranging from 15 to 32 or IPv6 address with a netmask ranging from 1 to 128.
- Specific IPv4 or IPv6 address.

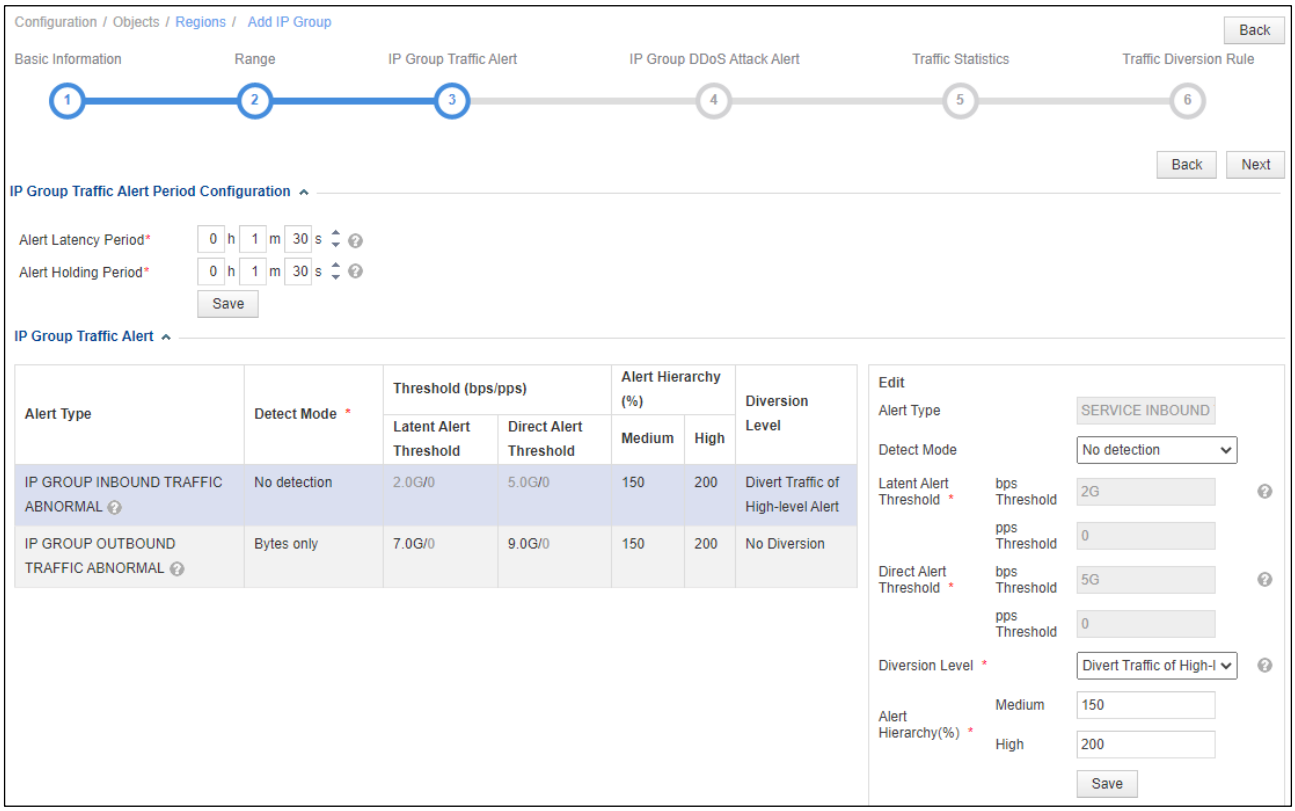
When the configured IP address conflicts with the existing IP group in a region, the system prompts a message indicating the IP group name and IP address or IP segment.

After completing the configuration, click **Next**.

c. Configure abnormal traffic alert policies on the page shown in Figure 5-37, including:

- Traffic alert thresholds
- Alert hierarchy
- Diversion levels

Figure 5-37 Traffic alert policies of the added IP group



For the description of parameters on this page, see Table 5-9. After completing the configuration, click **Save** to apply the parameter settings, and click **Next** to proceed.

d. Configure DDoS attack detection policies on the page shown in Figure 5-38, including:

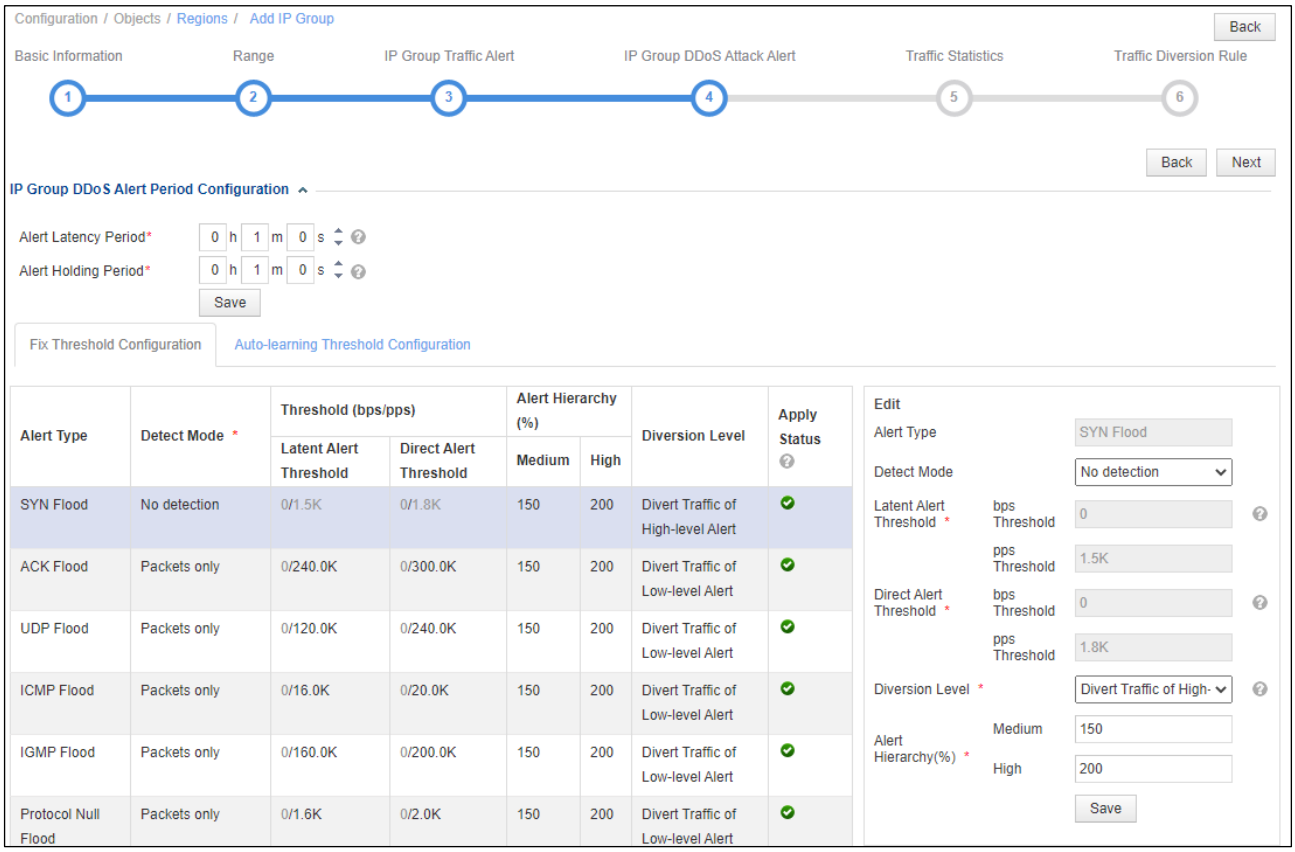
- Detection mode
- Alert thresholds
- Alert hierarchy
- Diversion levels

For DDoS attack detection for the entire IP group, you can set related thresholds using either of the following methods:

- Click the **Fix Threshold Configuration** tab to set fixed thresholds, as shown in Figure 5-38.

  For the description of parameters on this page, see Table 5-10.

Figure 5-38 IP Group DDoS Attack Alert configuration page



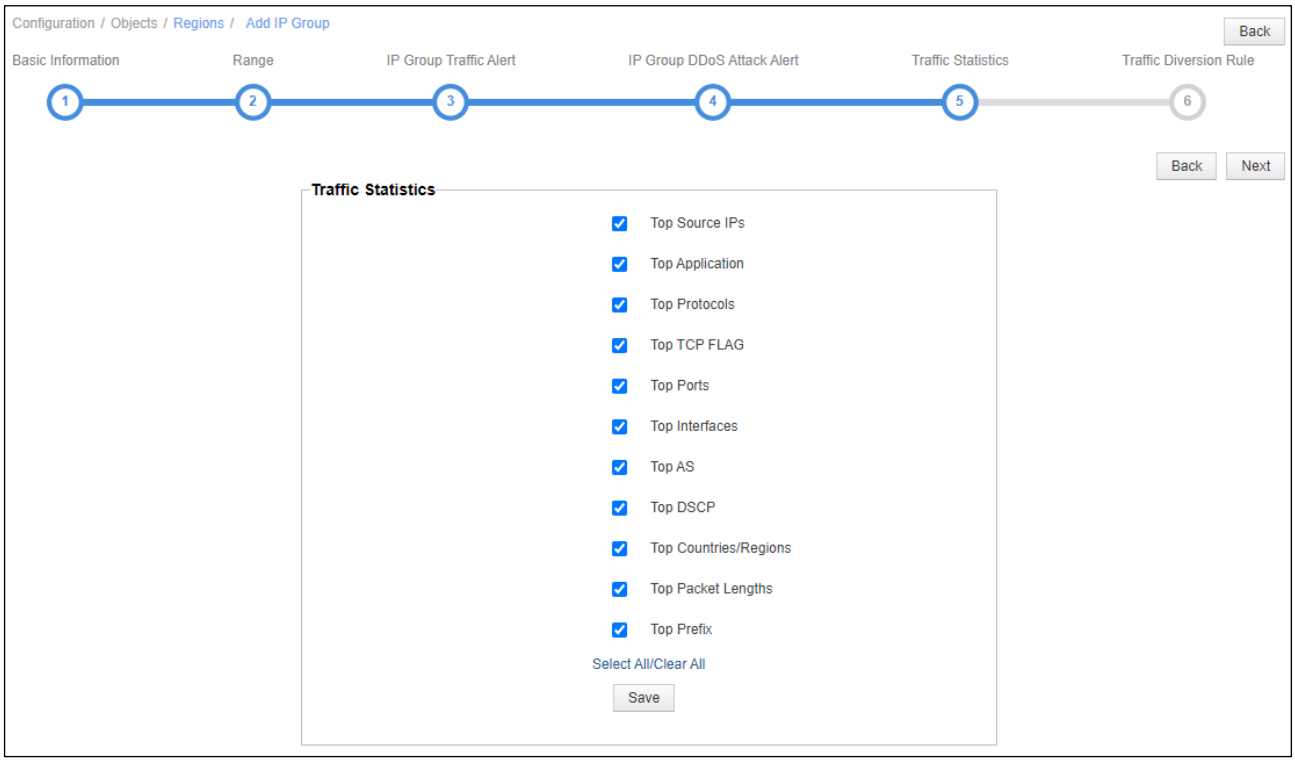
After completing the configuration, click **Save** to apply the parameter settings.

- Click the **Auto-learning Threshold Configuration** tab to configure NTA to dynamically adjust thresholds. For the description of related parameters, see Table 5-11.

  After completing the configuration, click **Save** to apply the parameter settings, and click **Next** to proceed.

e. Specify statistical items of traffic for the IP group on the page shown in Figure 5-39.

Figure 5-39 Traffic statistics configuration page

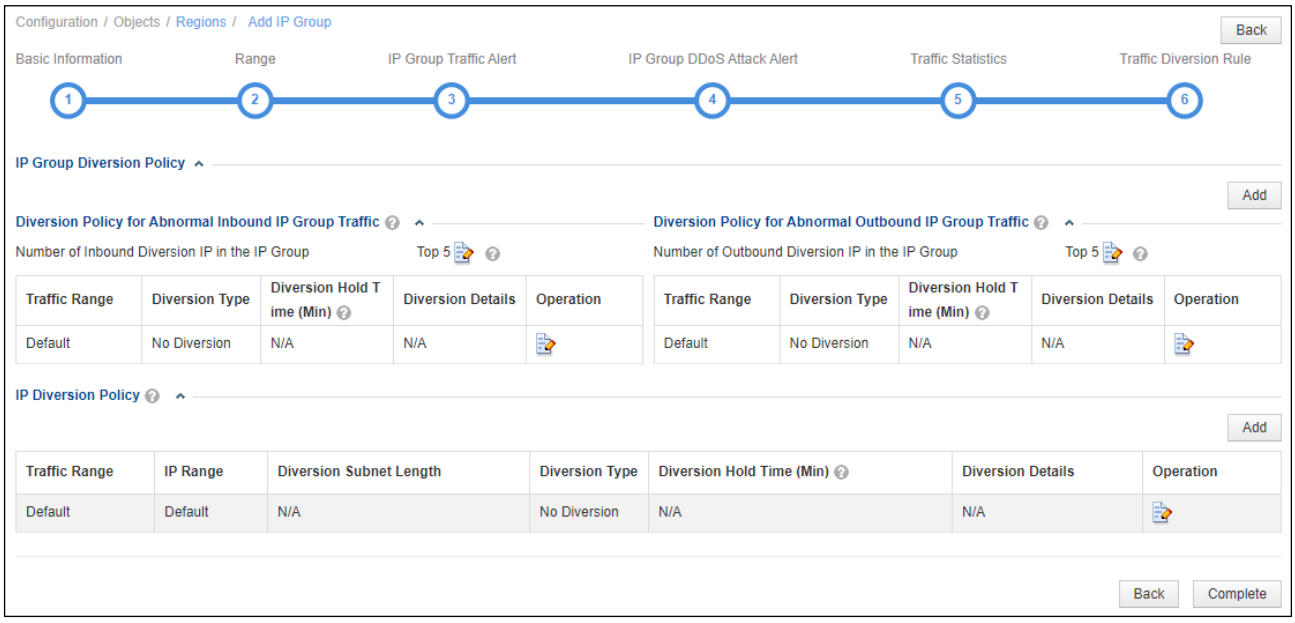


After completing the configuration, click **Save** to apply the parameter settings, and click **Next** to proceed.

f. Configure diversion policies on the page shown in Figure 5-40, including:

- Policies for diverting abnormal received or sent by the IP group
- Policies for diverting DDoS attack targeting a specific device

Figure 5-40 Traffic Diversion Rule configuration page

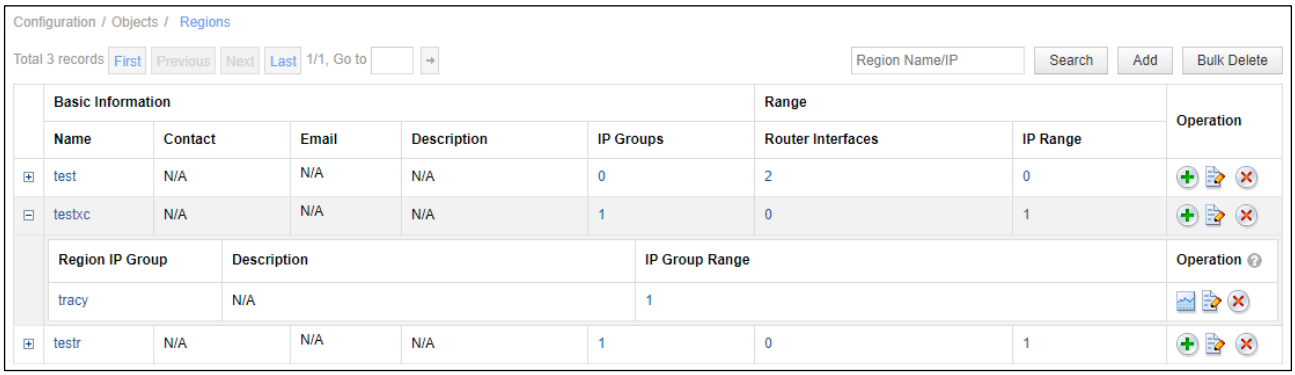


For the description of parameters on this page, see Table 5-11.

Step 3 View IP groups.

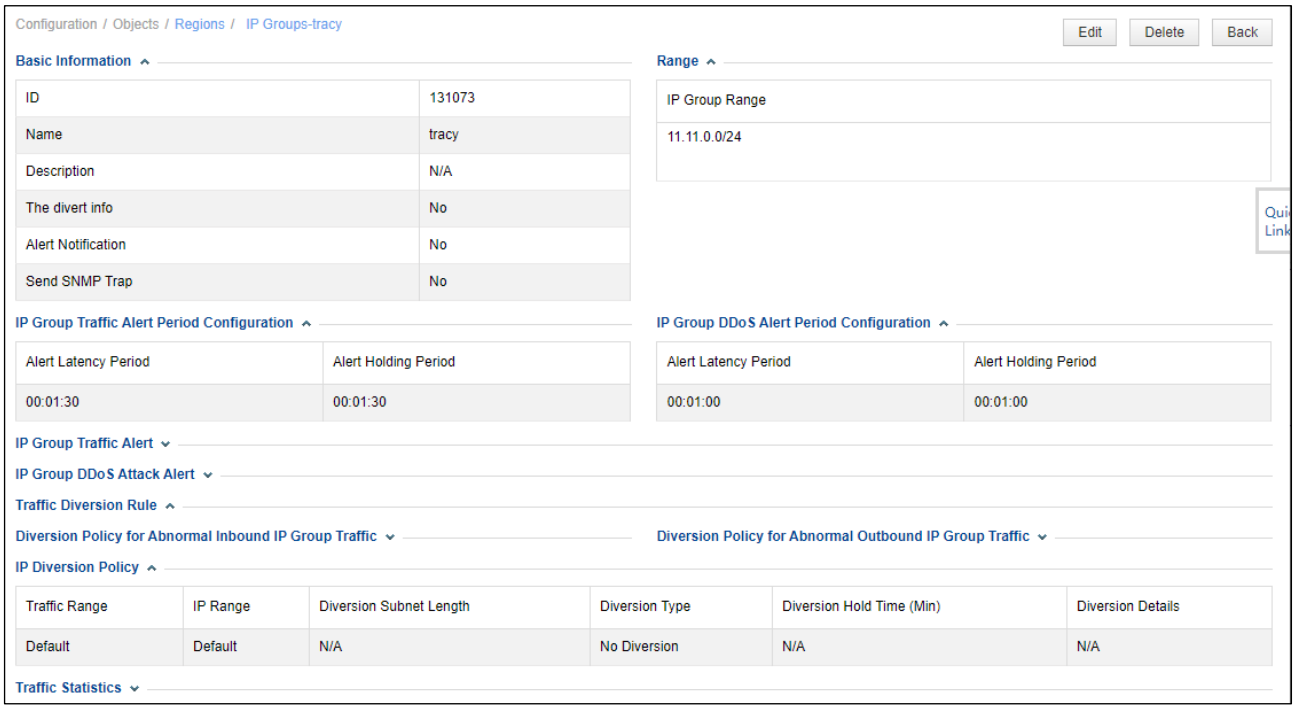
Click ⊞ on the left of a region name. All the existing IP groups in this region are then displayed, as shown in Figure 5-41.

Figure 5-41 IP groups included in a region



Click the name of an IP group. All settings of this IP group are then displayed, as shown in Figure 5-42.

Figure 5-42 Settings of an IP group



To modify the settings, click **Edit** in the upper-right corner. To delete this IP group, click **Delete**. To return to the **Regions** page, click **Back**.

----End

Configuring the Auto-Learning Baseline

DDoS attack alerting is implemented through alert thresholds. A too high threshold tends to cause false negatives. A too low threshold tends to cause a large number of false positives. Therefore, it is especially important to set proper thresholds. An IP group is a collection of IP addresses for similar businesses. Generally, the traffic of an IP group remains stable in the volume and characteristics. Therefore, NTA can automatically learn, record, and analyze network traffic of this IP group and then automatically generates proper thresholds for detecting various DDoS attacks. A baseline is the upper limit of traffic in normal conditions. NTA determines such an upper limit after learning traffic over some time and uses it as an attack alert threshold. This process is called traffic auto-learning.

If traffic auto-learning has been configured, NTA dynamically adjusts DDoS attack alert thresholds according to auto-learning results. NTA can calculate thresholds at an interval specified by **Time Granularity** (see section 5.3.4 Auto-learning Baseline Parameters) based on traffic learned in a day or seven days and then dynamically adjust these thresholds.

Traffic auto-learning is performed in three steps:

- After traffic auto-learning starts, NTA learns live traffic and, based on the actual traffic trend, generates latent alert thresholds using an appropriate algorithm.
- Based on global traffic auto-learning parameters, NTA generates direct alert thresholds and then raises the thresholds according to the auto-learning policy. For the configuration of global traffic auto-learning parameters, see section 5.3.4 Auto-learning Baseline Parameters.

- Thresholds can be applied to the IP group in either of the following ways:
  - Direct application
  - Manual application: Edit thresholds before manually applying them.

NTA can detect DDoS attacks according to dynamic thresholds only after these thresholds are applied.

Traffic auto-learning configuration includes starting learning, stopping learning, editing learning results, and applying baseline thresholds.

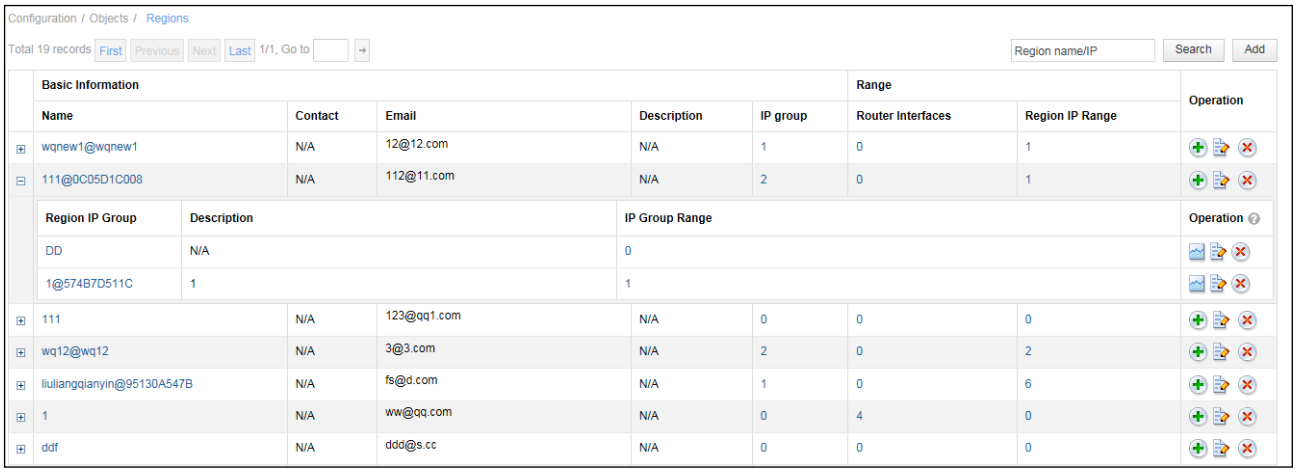
The procedure is as follows:

Step 1 Choose **Configuration > Objects > Regions**.

On the **Regions** page, you can see existing regions.

Click ⊞ on the left of a region name. All the existing IP groups in this region are then displayed, as shown in Figure 5-43.

Figure 5-43 IP groups included in a region



Step 2 Click 📈 in the **Operation** column to open the **Edit IP Group Auto-learning Baseline** page.

Figure 5-44 Edit IP Group Auto-learning Baseline page

By default, the page displays the traffic learning status for all DDoS attacks, which can be:

- **Not learned**: indicates that traffic learning has not started.
- **Learning**: indicates that the learning process is ongoing.
- **Learning failed**: indicates that traffic learning failed due to system exceptions.
- **Learning completed**: indicates that traffic learning has been completed.

For a new IP group, the traffic learning status for all attack types is **Not learned**.

For each attack type, you can start, stop, and restore learning.

Step 3 Start learning.

a. Click **Start Learning** in the area of a certain attack type. Alternatively, you can click **Bulk Learn** to start learning for all attack types that are in the **Not learned** state.

b. Configure basic settings in the dialog box shown in Figure 5-45.

Figure 5-45 Configuring traffic auto-learning

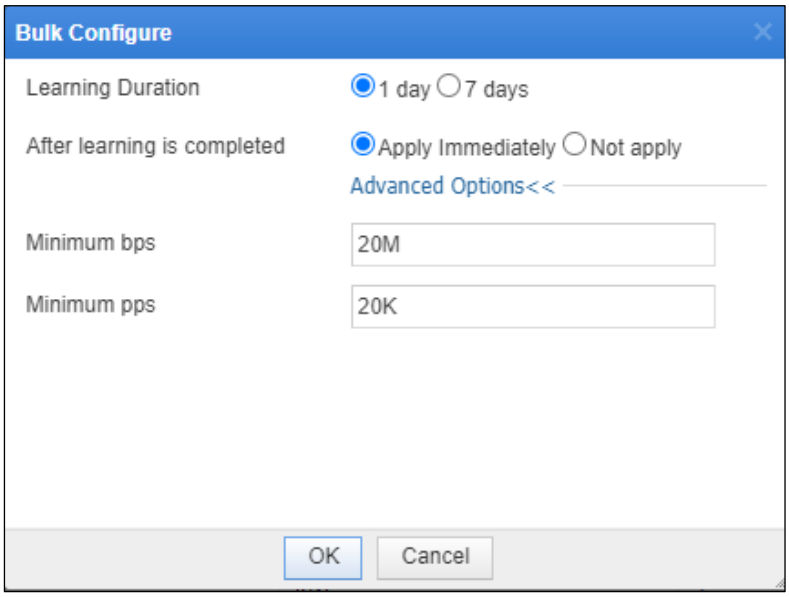


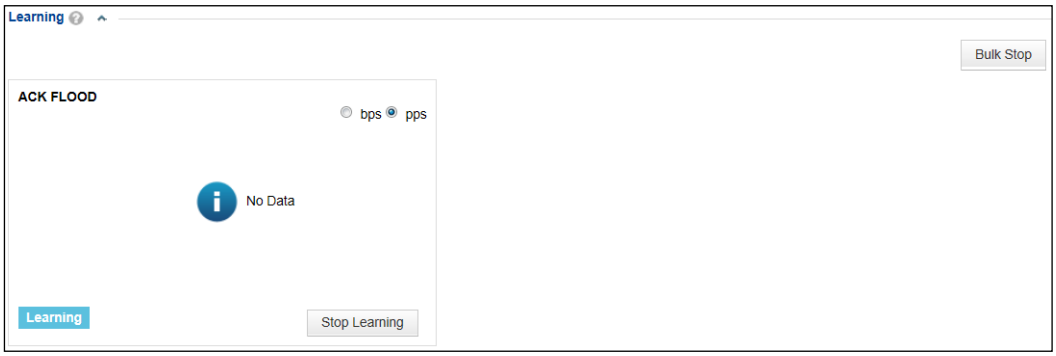
Table 5-14 describes parameters for configuring traffic auto-learning.

Table 5-14 Parameters for configuring traffic auto-learning

Parameter	Description
Learning Duration	Specifies the duration from when learning starts till it ends.
After learning is completed	Specifies when baseline thresholds are applied. • **Apply immediately**: indicates that baseline thresholds are applied for DDoS attack detection immediately after traffic auto-learning is completed. • **Not apply**: indicates that fixed thresholds are still used after traffic auto-learning is completed. In this case, you need to perform manual operations to make the baseline thresholds take effect. For details, see Step 6. Note In practice, thresholds are raised according to related global settings. For details, see section 5.3.4 Auto-learning Baseline Parameters.
Minimum bps	Specifies the lower limit for the traffic rate in bps. When the actual traffic rate is lower than the minimum bps specified here, NTA uses the latter for baseline threshold calculation.
Minimum pps	Specifies the lower limit for the traffic rate in pps. When the actual traffic rate is lower than the minimum pps specified here, NTA uses the latter for baseline threshold calculation.

c. Click **OK** to commit the settings. NTA starts learning and the status changes to **Learning**, as shown in Figure 5-46.

Figure 5-46 Auto-learning in progress



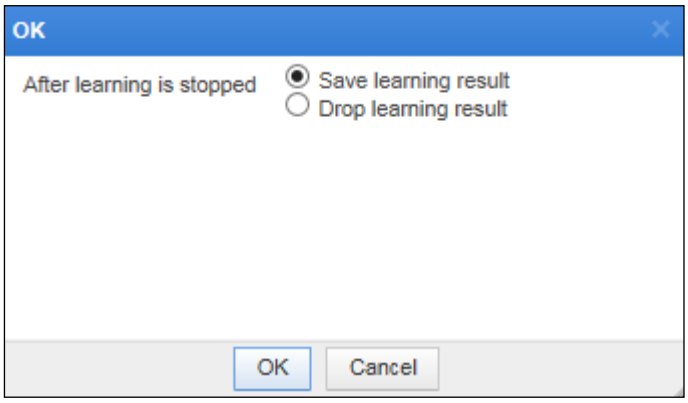
Step 4 Stop learning.

When the specified learning duration expires, NTA automatically stops learning.

You can also manually stop learning. To do so, click **Stop Learning** for a certain attack type. Alternatively, click **Bulk Stop** to stop learning for all attack types that are in the **Learning** state.

After you click **Stop Learning** or **Bulk Stop**, the system prompts you to save or drop learning results. Figure 5-47 shows the dialog box that appears after you click **Bulk Stop**.

Figure 5-47 Method of handling learning results



Learning results can be handled in either of the following ways:

- **Save learning result**: indicates that the learning result will be saved. In this case, when at least one value is determined based on the learning result, NTA takes the learning as successful.
- **Drop learning result**: indicates that the learning result will not be saved. In this case, NTA takes the learning as failed.

After selecting a method, click **OK**.

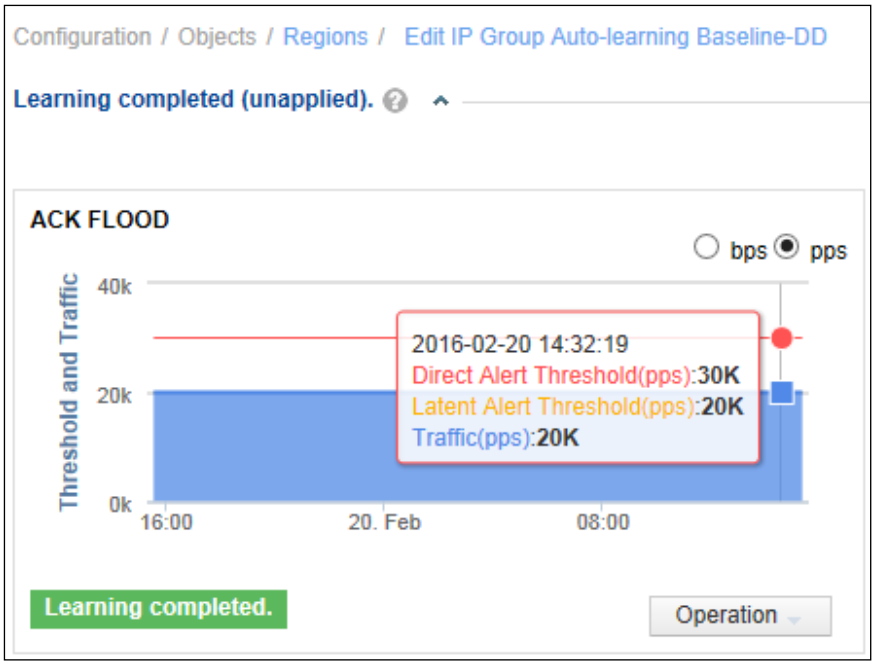
Step 5 Edit baseline data.

Learning results are displayed in the **Learning completed** area. From the curves, you can view the direct alert threshold, latent alert threshold, and traffic trend during the learning

period. Pointing to a specific position on a curve displays threshold and traffic values at that specific moment.

Figure 5-48 shows unapplied auto-learning data.

Figure 5-48 Baseline data obtained through auto-learning



Click **Operation** and then choose **Edit** from the drop-down menu, as shown in Figure 5-49. Then you can adjust the learning result.

Figure 5-49 Operations that can be performed on the learning result

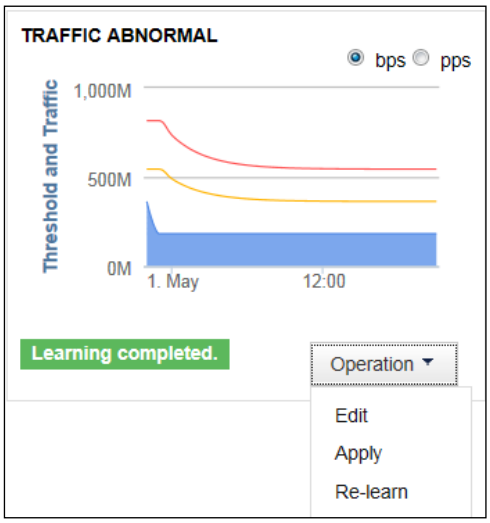
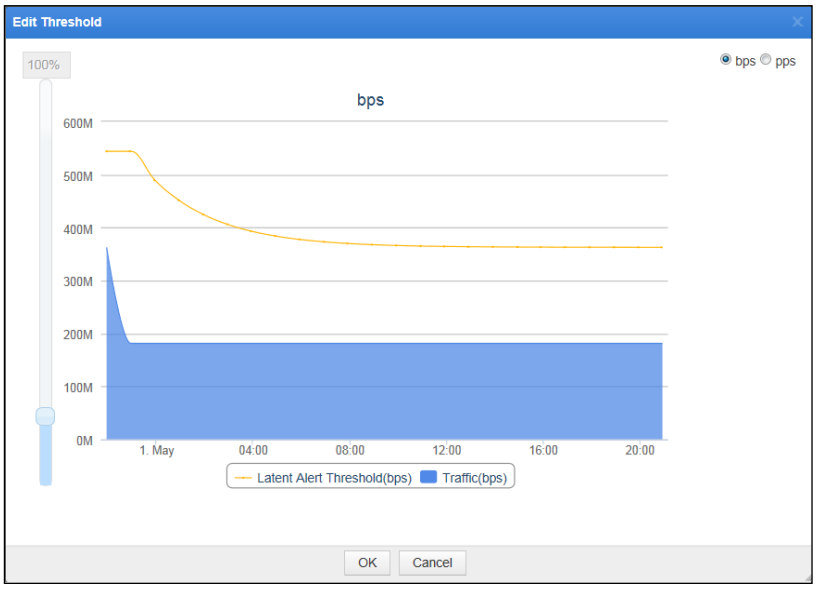


Figure 5-50 shows the **Edit Threshold** page. You can adjust only the latent alert threshold.

Figure 5-50 Edit Threshold page



A scroll bar is available on the left for you to increase or decrease the thresholds as a whole. You can also drag any point on the curve up or down to increase or decrease the value at that point of time. After the adjustment, click **OK**.

Step 6 Apply baseline thresholds.

If you select **Not apply** for the learning result, you can later manually apply the threshold to the IP group for the related attack type.

a. Click **Operation** on the page shown in Figure 5-49 and then choose **Apply** from the drop-down menu. Then the learning result is applied for attack detection.

b. Click **Bulk Operation** and then choose **Apply** from the drop-down menu. Then you can make unapplied baseline thresholds take effect immediately.

Step 7 Re-learn baseline thresholds.

Click **Operation** on the page shown in Figure 5-49 and then choose **Re-learn** from the drop-down menu. Then you can restart traffic learning.

----End

5.2 Alert Templates

The Alert Configuration Template module allows you to configure common alert templates as required. When configuring a policy, you can directly use a template to define alert parameters. NTA supports the following alert templates:

- Router Alert Template
- System Upgrade
- IP Group Alert Template

5.2.1 Router Alert Template

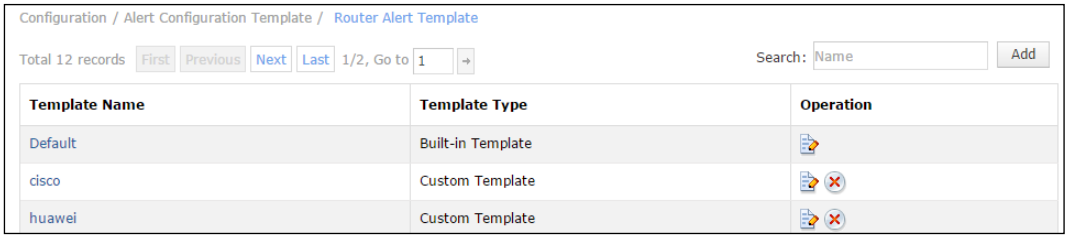
A router alert template is used to define bandwidth usage alert and performance alert parameters. After being configured, a router alert template can be referenced for adding a router, thereby simplifying parameter configuration.

To configure a router alert template, follow these steps:

Step 1 Choose **Configuration > Alert Configuration Template > Router Alert Template**.

The page shows all existing templates, as shown in Figure 5-51.

Figure 5-51 Router Alert Template page

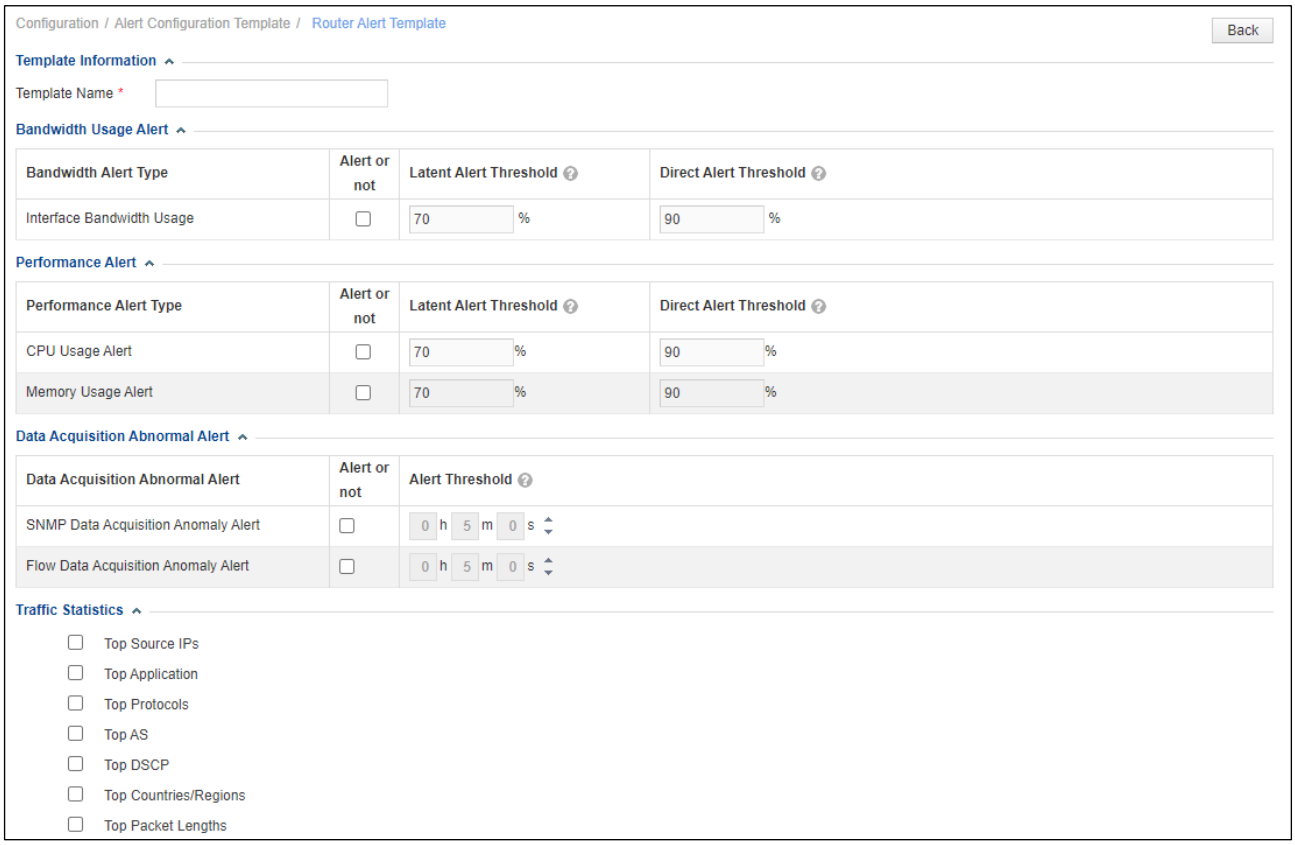


In the template list, the **Template Type** column shows the type of the template. **Default** indicates a built-in template. Other templates are custom ones. You can click in the **Operation** column to modify parameter settings. You can also click to delete a custom template.

Step 2 Add a template.

Click **Add**. The page for adding a template appears, as shown in Figure 5-52.

Figure 5-52 Adding a router alert template



You can define bandwidth usage alert, CPU usage alert, memory usage alert, and data acquisition abnormal alert (SNMP data acquisition anomaly and flow data acquisition anomaly) policies as well as traffic statistics in a template. Table 5-15 describes parameters for defining these policies.

Table 5-15 Parameters for configuring a router alert template

Parameter	Description
Template Name	Specifies the name of the template to be created.
Alert or not	Controls whether to enable alerting. An alerting policy can take effect only after this function is enabled.
Latent Alert Threshold	Specifies the bandwidth, CPU, or memory usage threshold that triggers NTA to generate an alert only after the usage stays at this level for some time.
Direct Alert Threshold	Specifies bandwidth, CPU, or memory usage threshold that triggers NTA to generate an immediate alert. Note The direct alert threshold must be greater than the latent alert threshold.
Alert Threshold	Specifies the threshold for the SNMP or flow data acquisition interruption duration, which triggers NTA to generate an immediate alert.
Traffic Statistics	Specifies statistical items of traffic.

Step 3 To modify template parameters, click in the **Operation** column.

Step 4 To delete a template, click in the **Operation** column.

----End

5.2.2 Region Alert Template

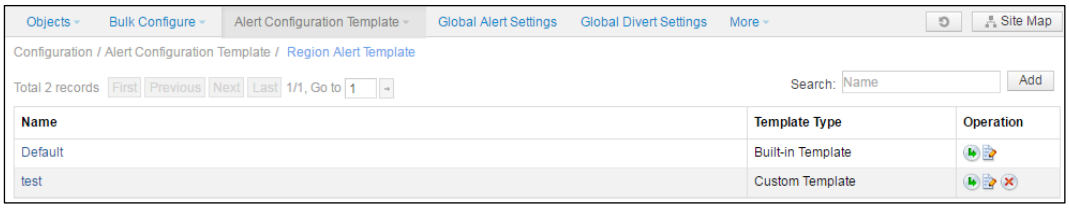
A region alert template is used to define traffic alert parameters, DDoS attack alert parameters, and traffic diversion rules. After being configured, a region alert template can be referenced for adding a region, thereby simplifying parameter configuration.

To configure a region alert template, follow these steps:

Step 1 Choose **Configuration > Alert Configuration Template > Region Alert Template**.

The page shows all existing templates, as shown in Figure 5-53.

Figure 5-53 Region Alert Template page

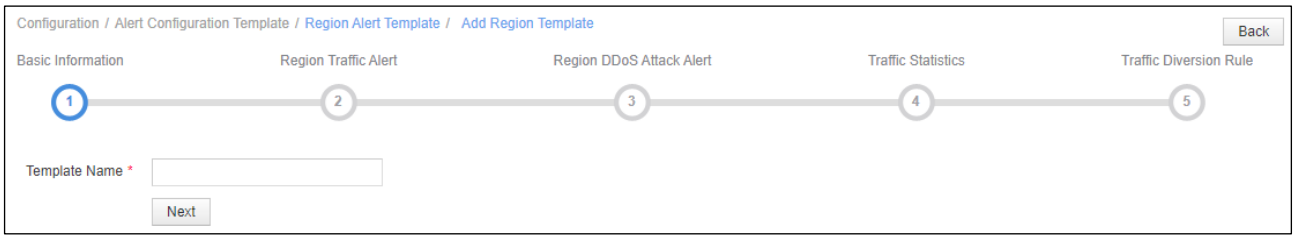


In the template list, the **Template Type** column shows the type of the template. **Default** indicates a built-in template. Other templates are custom ones. You can click in the **Operation** column to modify parameter settings. You can also click to delete a custom template.

Step 2 Add a template.

a. Click **Add**. The page for adding a template appears, as shown in Figure 5-54. You can define region traffic alert policies, region DDoS attack alert policies, traffic statistics, and traffic diversion rules in a template.

Figure 5-54 Basic information configuration page

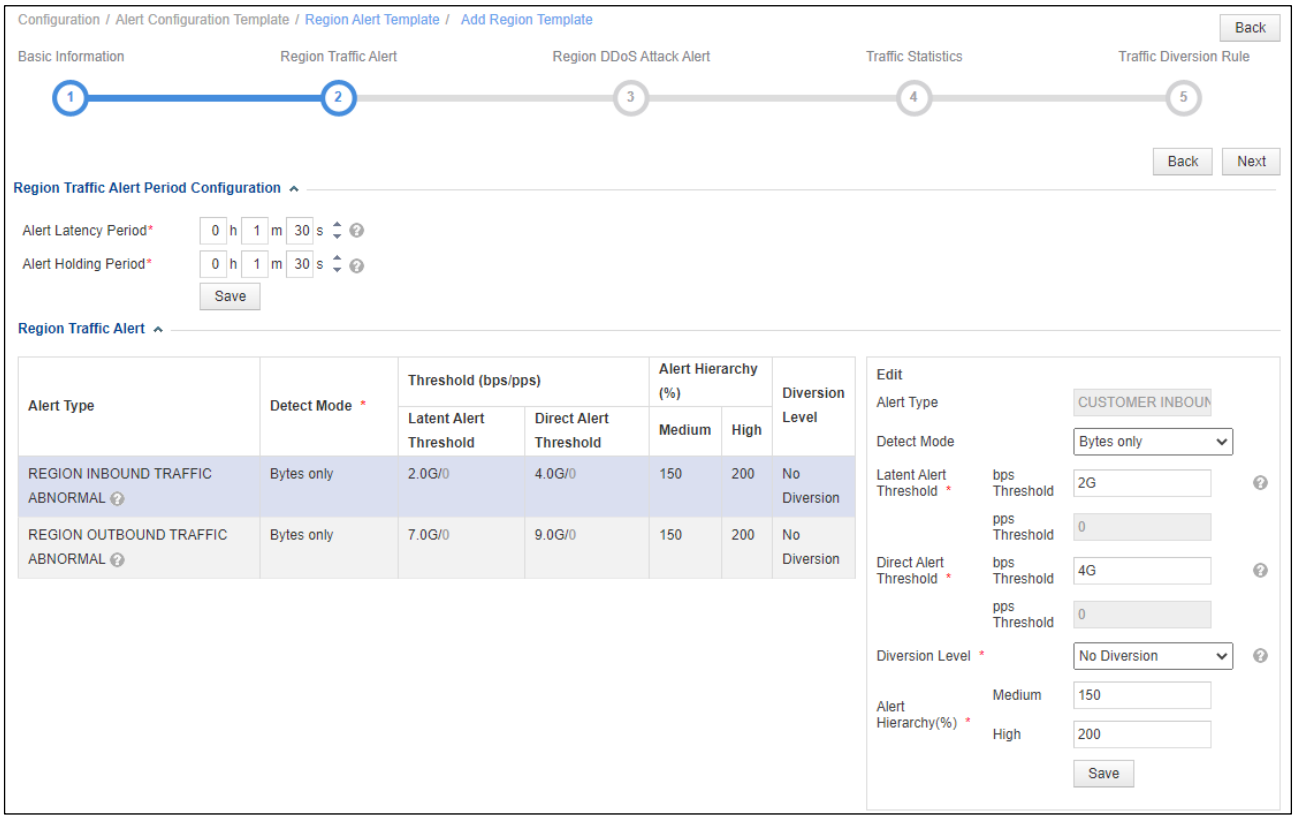


b. Enter a name and then click **Next**.

Step 3 Configure region traffic alert parameters.

For the description of parameters on this page, see Table 5-9.

Figure 5-55 Configuring region traffic alert policies

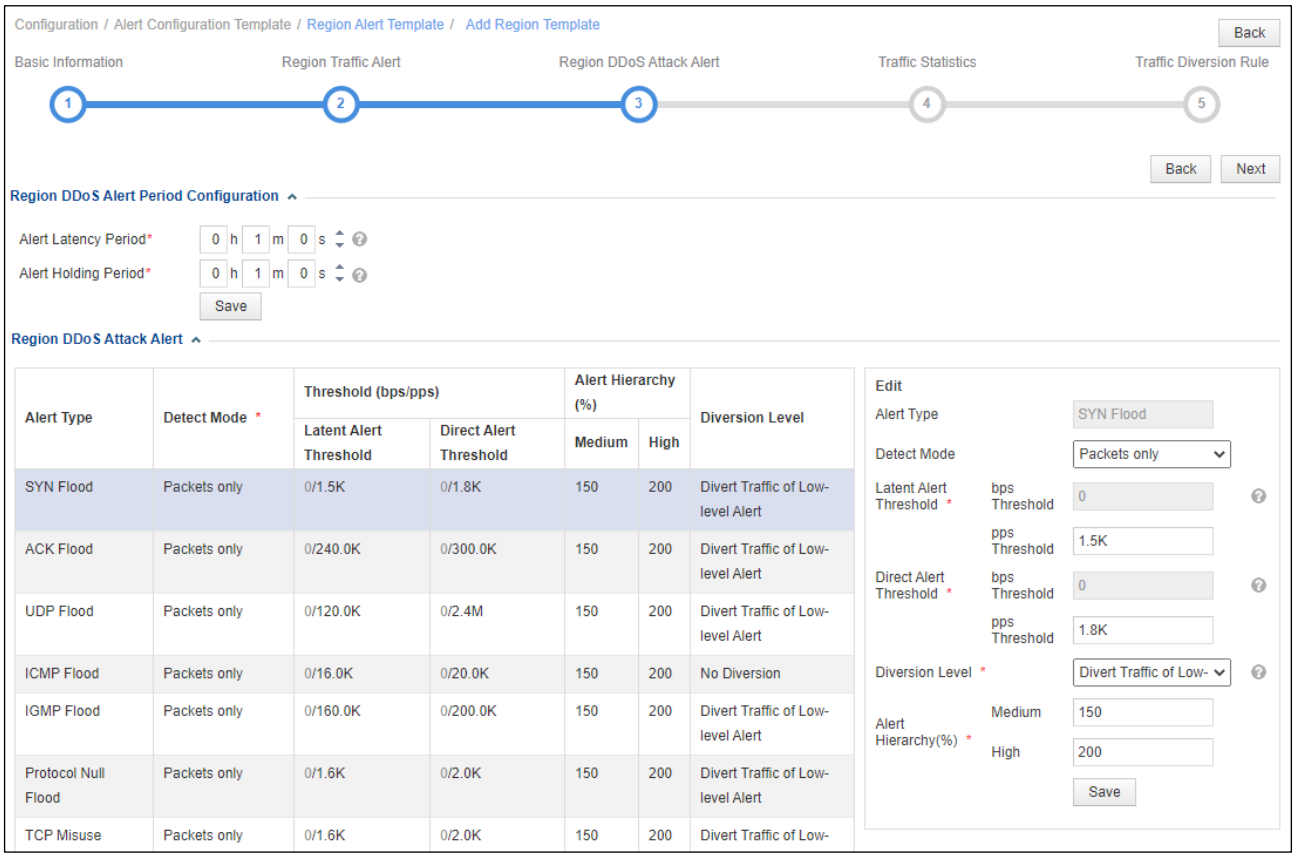


After completing the configuration, click **Save** to apply the parameter settings, and click **Next** to proceed.

Step 4 Configure region DDoS attack alert parameters.

For the description of parameters on this page, see Table 5-10.

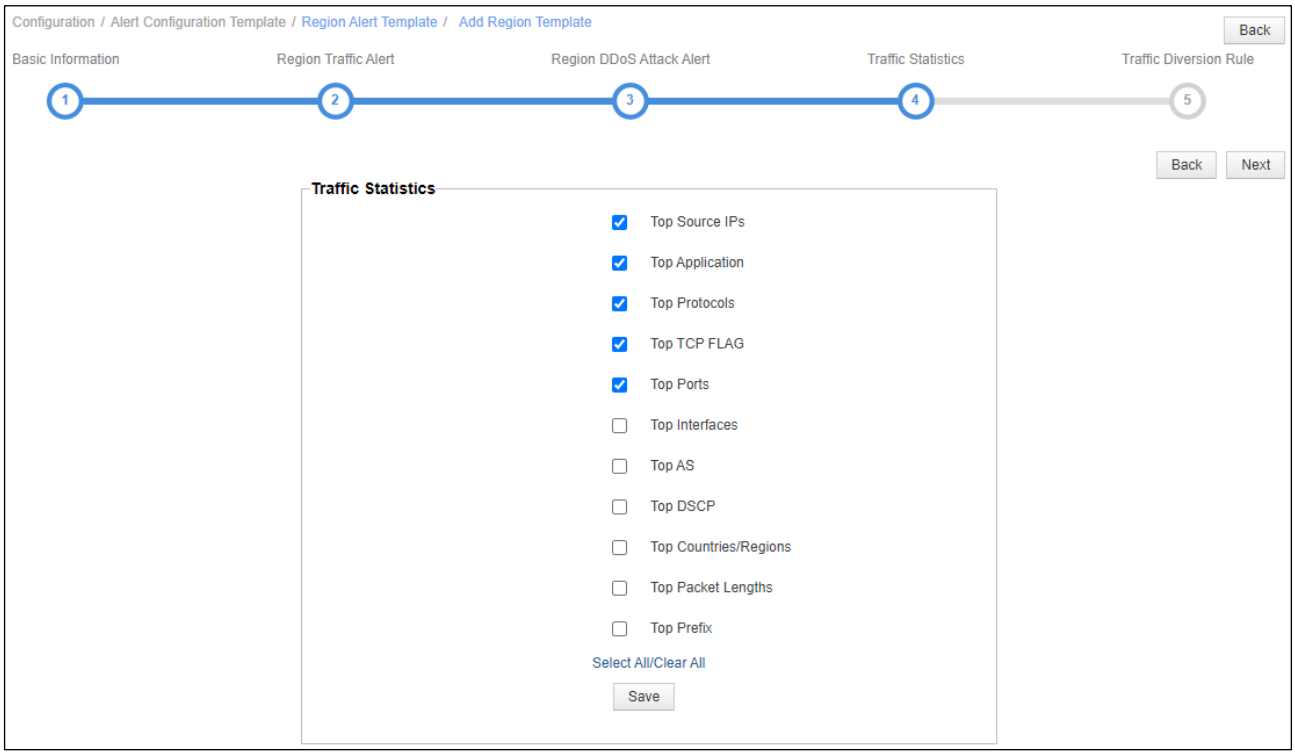
Figure 5-56 Configuring region DDoS attack alert parameters



After completing the configuration, click **Save** to apply the parameter settings, and click **Next** to proceed.

Step 5 Specify statistical items of traffic for the region on the page shown in Figure 5-57.

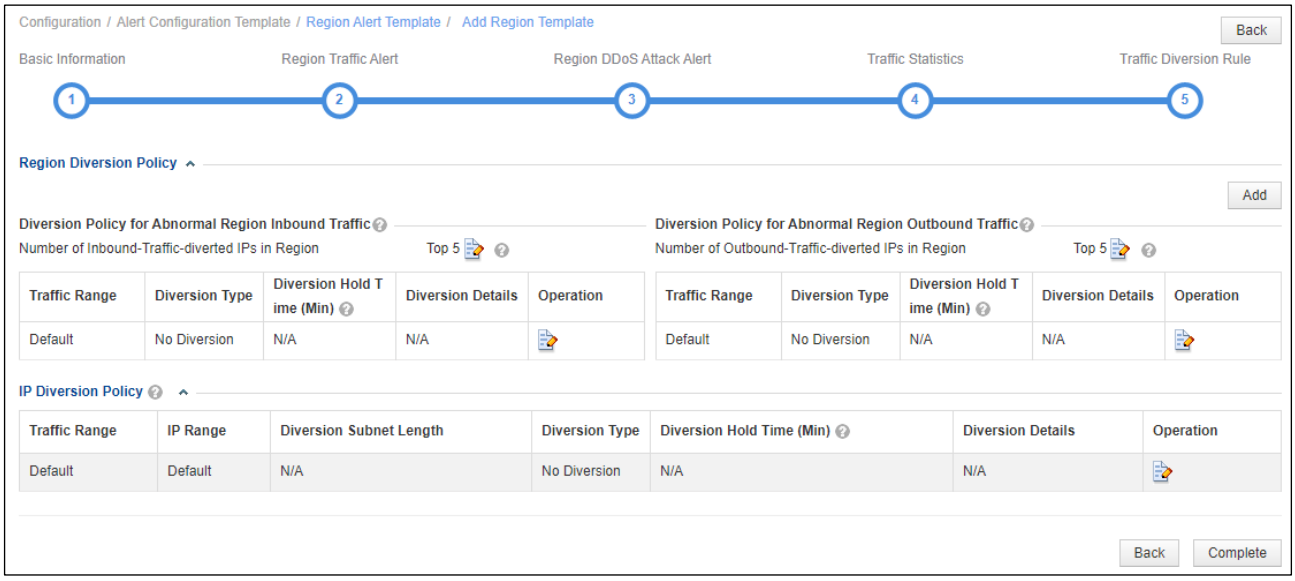
Figure 5-57 Configuring traffic statistics parameters for the region



Step 6 Configure traffic diversion rules.

For the description of parameters on this page, see Table 5-11.

Figure 5-58 Configuring region traffic diversion rules

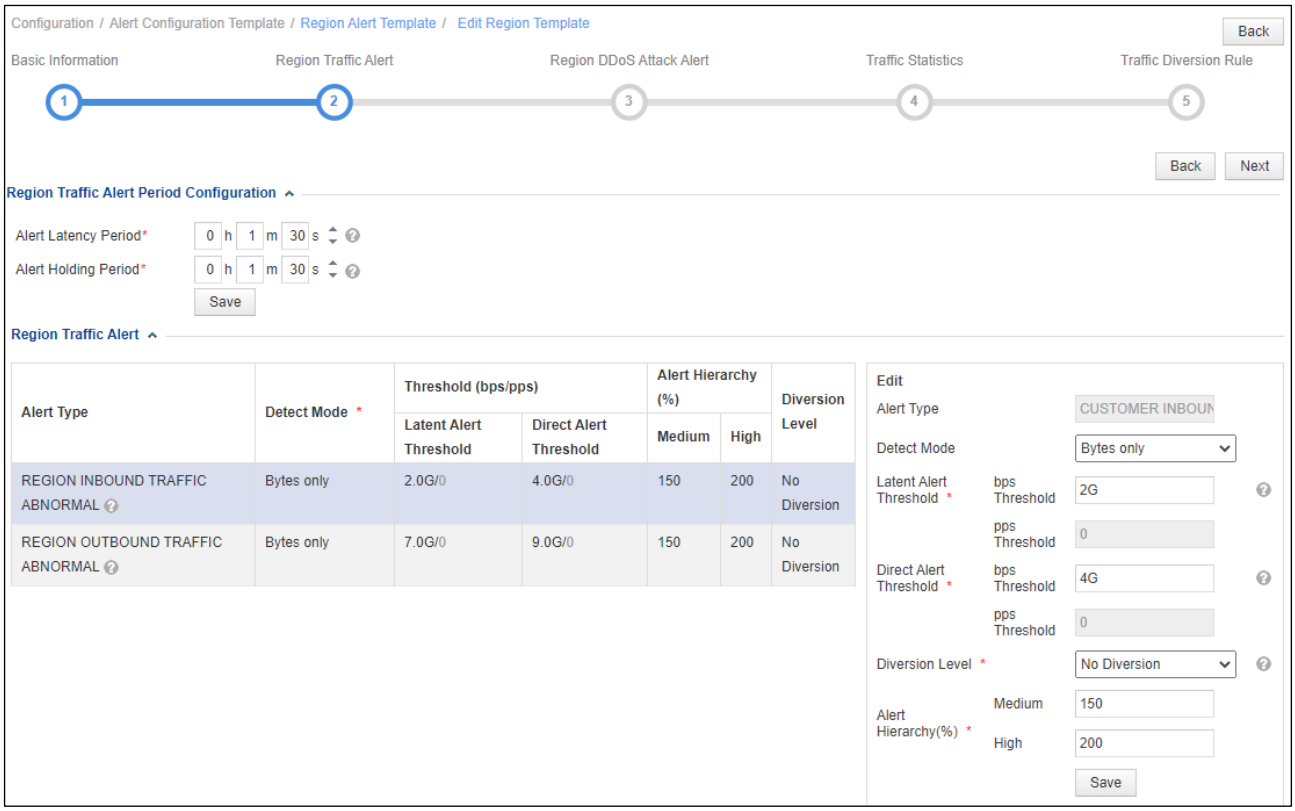


Step 7 Click **Complete** to commit the settings.

Step 8 View and edit a template.

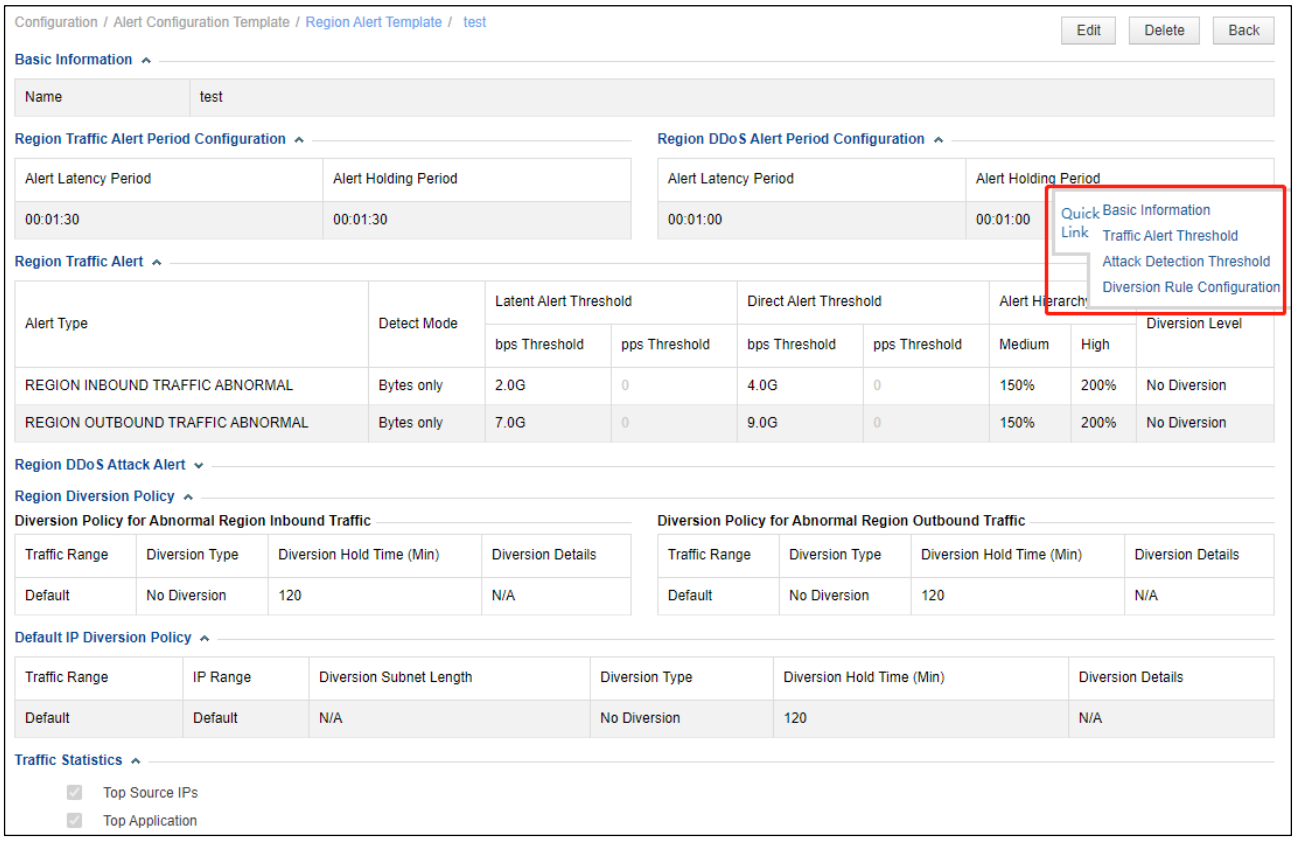
In the template list, click in the **Operation** column to view and edit region alert template parameters.

Figure 5-59 Edit Region Template page



You can also click a template name in the list to view all settings.

Figure 5-60 Region alert template settings displayed on one page



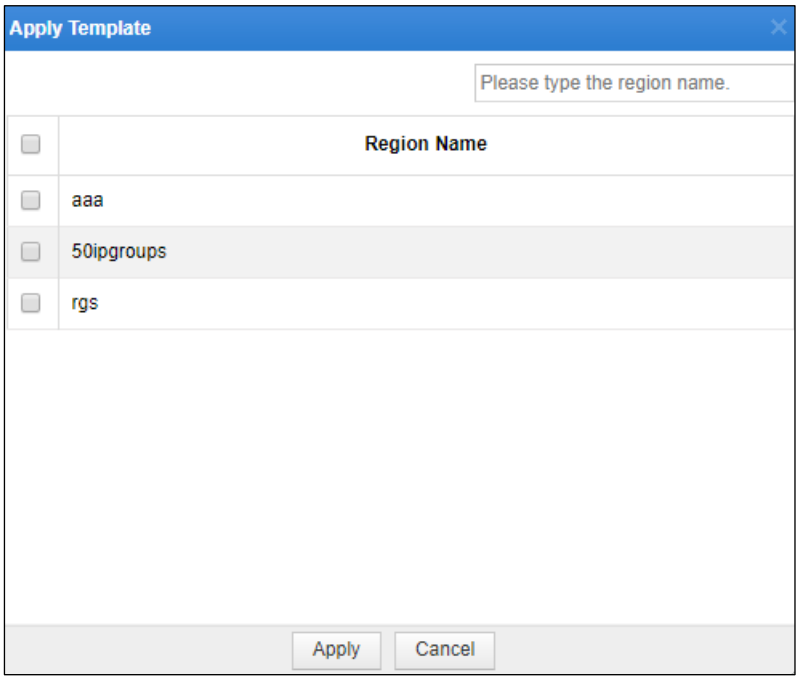
Click **Edit** in the upper-right corner to modify template settings. A shortcut link is available on this page, as shown in Figure 5-60, so that you can quickly navigate to the desired area.

Step 9 Apply the template.

An edited template can be used for previously applicable regions only after you perform an "apply" operation on it.

a. In the template list, click in the **Operation** column of the edited template.

Figure 5-61 Specifying regions to be covered by the edited template



b. Select one or more regions to which this template will apply.

Step 10 Delete a template.

In the template list, click in the **Operation** column to delete a template. You can also click the template name and click **Delete** on the page shown in Figure 5-60 to delete a template.

----End

5.2.3 IP Group Alert Template

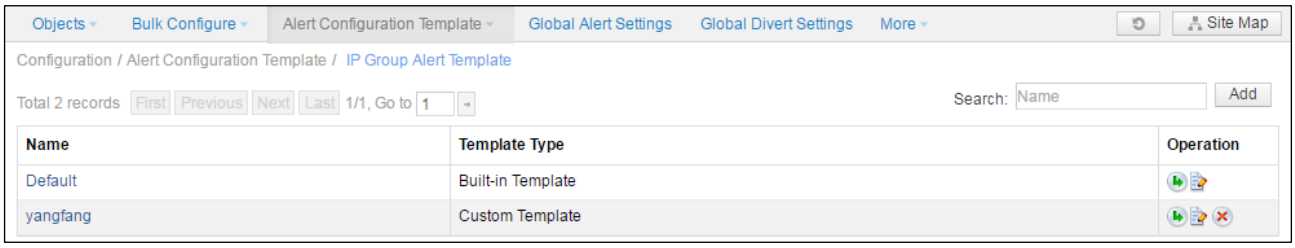
An IP group alert template is used to define traffic alert parameters, DDoS attack alert parameters, and traffic diversion rules. After being configured, an IP group alert template can be referenced for adding an IP group, thereby simplifying parameter configuration.

To configure an IP group alert template, follow these steps:

Step 1 Choose **Configuration > Alert Configuration Template > IP Group Alert Template**.

The page shows all existing templates, as shown in Figure 5-62.

Figure 5-62 IP Group Alert Template page

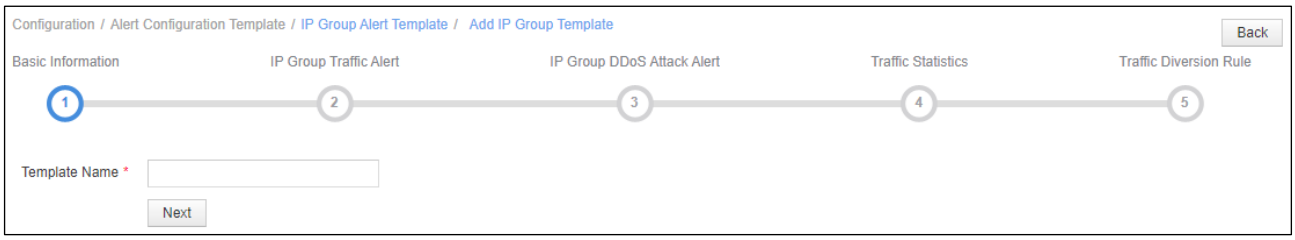


In the template list, the **Template Type** column shows the type of the template. **Default** indicates a built-in template. Other templates are custom ones. You can click in the **Operation** column to modify parameter settings. You can also click to delete a custom template. Add a template.

Step 2 Click **Add**.

The page for adding a template appears, as shown in Figure 5-63. You can define IP group traffic alert policies, DDoS attack alert policies, traffic statistics, and traffic diversion rules in a template.

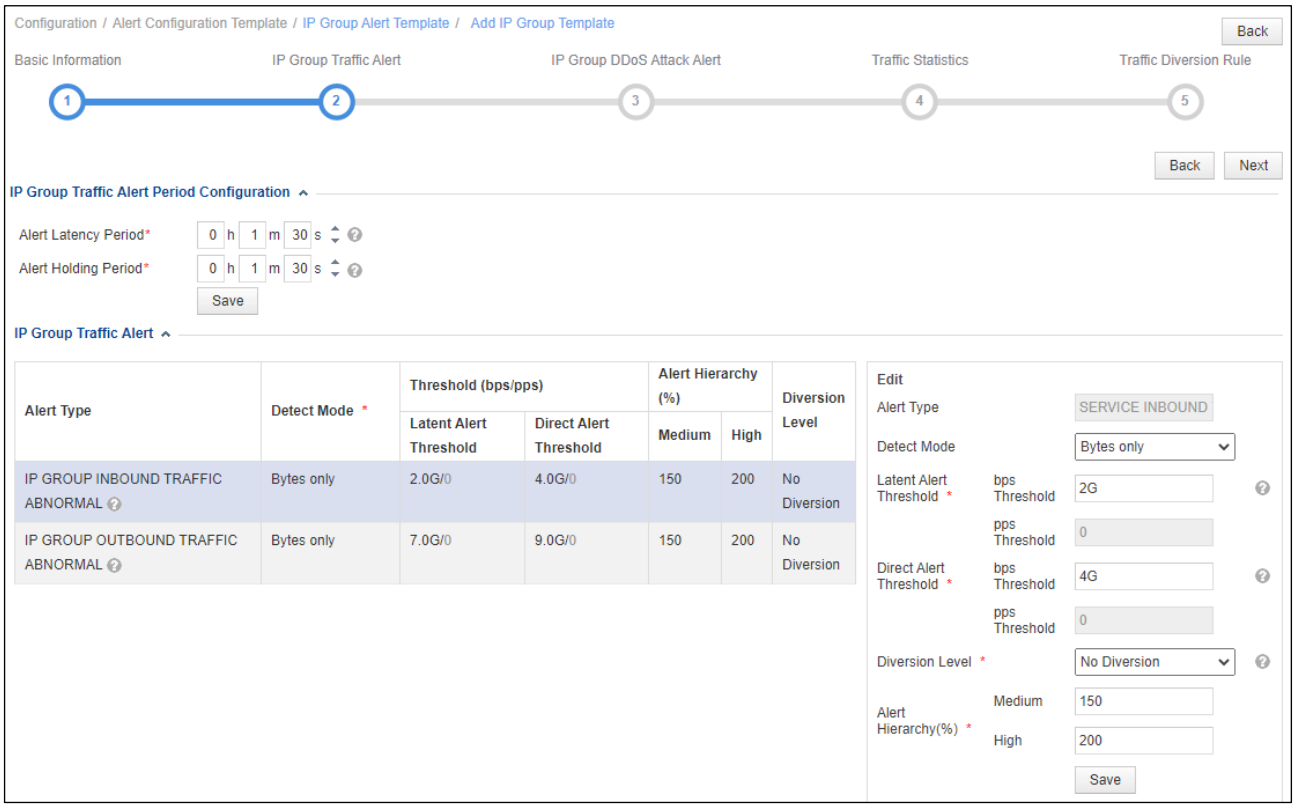
Figure 5-63 Configuring an alert template for an IP group



Enter a name and then click **Next**.

Step 3 Configure traffic alert parameters.

Figure 5-64 Configuring IP group traffic alert policies



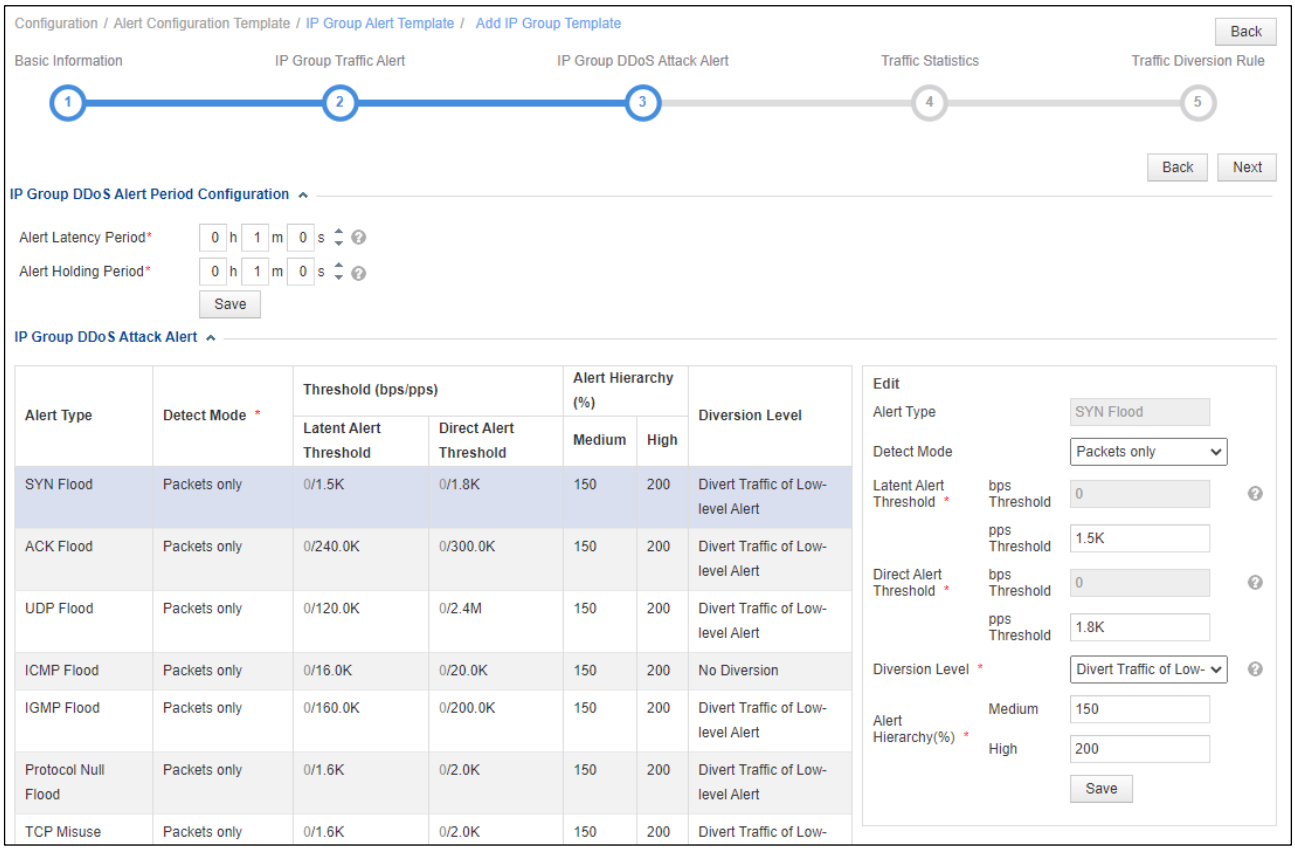
For the description of parameters on this page, see Table 5-9.

After completing the configuration, click **Save** to apply the parameter settings, and click **Next** to proceed.

Step 4 Configure DDoS attack alert policies.

NTA checks the total traffic of an IP group and adds up all types of traffic per second that match attack signatures. If the traffic rate exceeds a threshold, NTA deems that an attack occurs and generates an alert. NTA generates alerts at proper levels as specified by alert hierarchy policies. For alerts of a specified level, NTA will implement traffic diversion according to the diversion policy.

Figure 5-65 Configuring DDoS attack alerts for an IP group

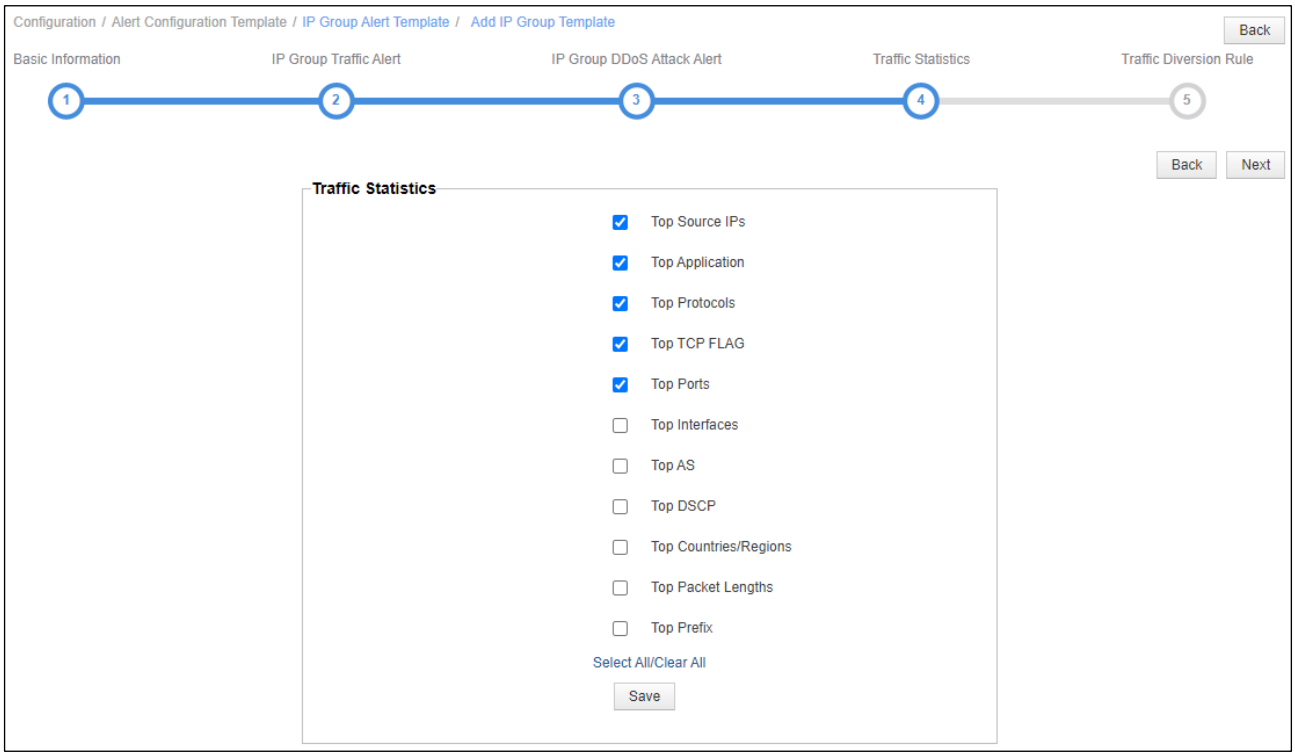


For the description of parameters on this page, see Table 5-10.

After completing the configuration, click **Save** to apply the parameter settings, and click **Next** to proceed.

Step 5 Specify statistical items of traffic for the IP group on the page shown in Figure 5-66.

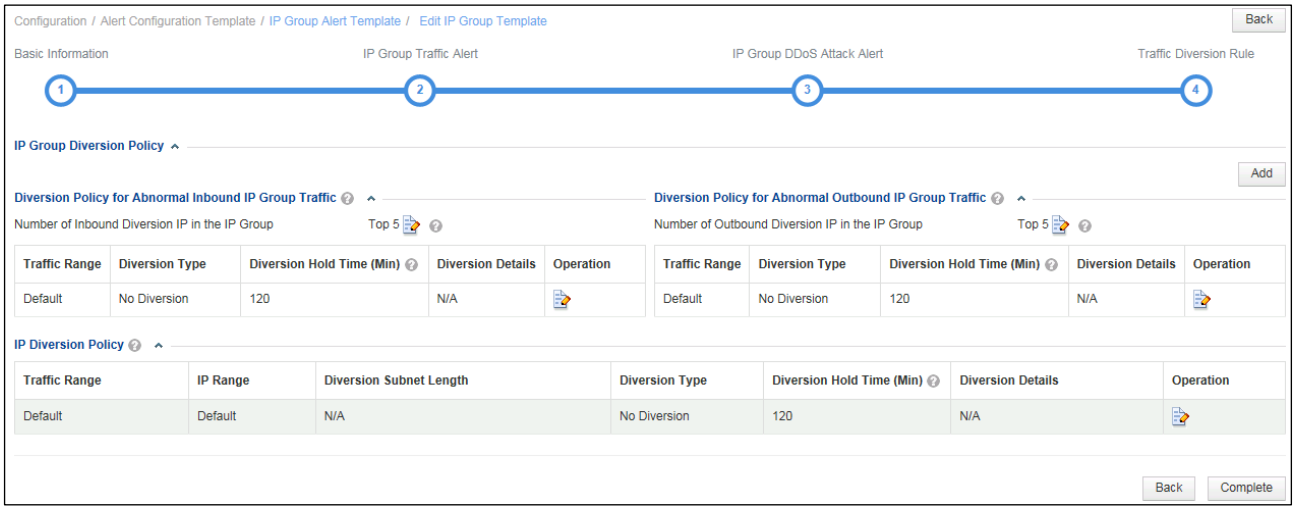
Figure 5-66 Configuring traffic statistics parameters for an IP group



Step 6 Configure traffic diversion rules.

For the description of parameters on this page, see Table 5-11.

Figure 5-67 Configuring traffic diversion rules for an IP group



Step 7 View and edit a template.

In the template list, click the template name to view all the settings of a template. Click **Edit** in the upper-right corner to modify template settings.

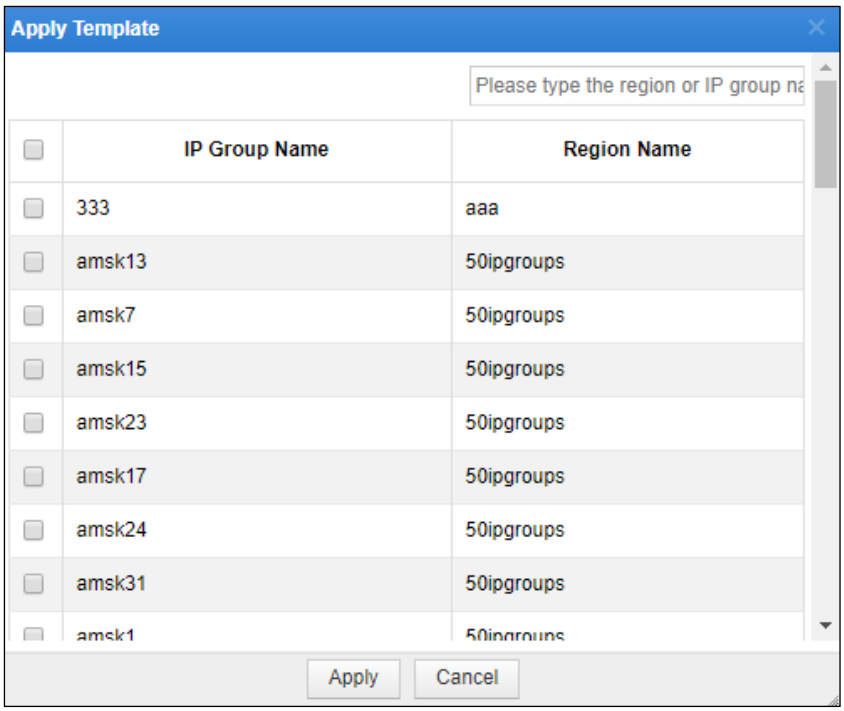
You can also click in the **Operation** column of the template list to edit parameter settings.

Step 8 Apply the template.

An edited template can be used for previously applicable IP groups only after you perform an "apply" operation on it.

a. In the template list, click in the **Operation** column of the edited template.

Figure 5-68 Specifying IP groups to be covered by the edited template



b. Select one or more IP groups to which this template will apply.

Step 9 Delete a template.

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

----End

5.3 Global Alert Settings

The Global Alert Settings module allows you to configure the following:

- Default DDoS Attack Detection Thresholds
- Alert Parameters
- Alert Plug-in Management
- Auto-learning Baseline Parameters
- Traffic Statistics

Note	The **Alert Parameters** and **Alert Plug-in Management** pages under **Global Alert Settings** of vNTA do not support configuration of the CPU temperature threshold and mainboard temperature threshold.

5.3.1 Default DDoS Attack Detection Thresholds

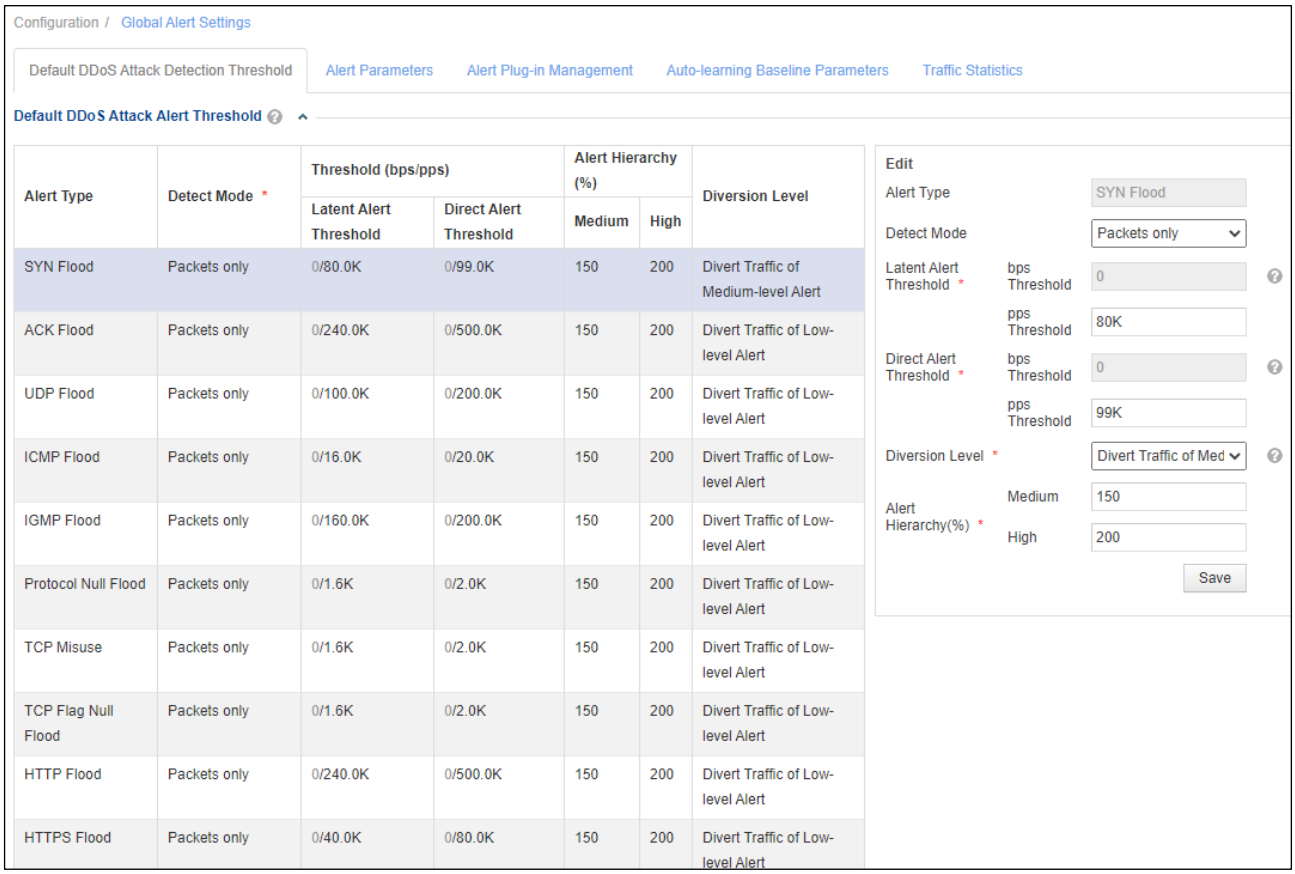
If a destination IP address does not belong to any IP group or region, NTA determines whether the IP address is the target of a DDoS attack based on default DDoS attack detection thresholds. You can view and modify these default settings on the **Default DDoS Attack Alert Threshold** page.

To view details about alerts, follow these steps:

Step 1 Choose **Configuration > Global Alert Settings > Default DDoS Attack Detection Threshold**.

The **Default DDoS Attack Alert Threshold** page displays default detection modes and parameters for all built-in DDoS attack types, as shown in Figure 5-69.

Figure 5-69 Default DDoS Attack Alert Threshold page



Step 2 Modify default values.

For each type of attack, modify the detection mode, latent alert threshold, direct alert threshold, diversion level, and alert hierarchy. For the description of parameters on this page, see Table 5-10.

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

----End

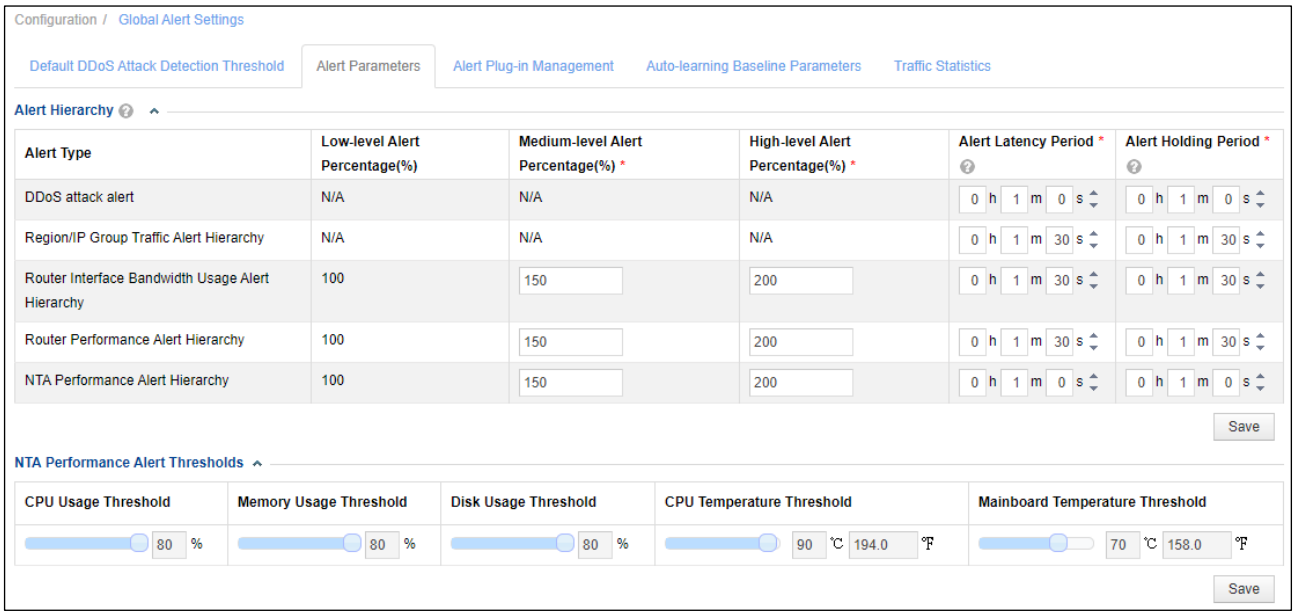
5.3.2 Alert Parameters

When detecting a DDoS attack, abnormal traffic, abnormal router interface usage and performance, or NTA system exception, NTA generates an alert. Alerts are classified into low, medium, and high levels based on the deviation from the threshold. On the **Alert Parameters** page, you can define the alert classification policy, alert latency period, and alert holding period.

The procedure is as follows:

Step 1 Choose **Configuration > Global Alert Settings > Alert Parameters**.

Figure 5-70 Alert Parameters page



Alert levels on this page are defined based on the traffic per second specified for the latent alert threshold. Alert levels are classified according to the ratio of actual traffic to the **Latent Alert Threshold** value. Table 5-16 describes parameters for defining alert levels.

Table 5-16 Global alert parameters

Parameter	Description
Low-level Alert Percentage(%)	Ratio of the actual traffic to a value specified by **Latent Alert Threshold**, at which a low-level alert is generated. Specifies the standard for defining a low-level alert. The default value is **100**, which cannot be edited. If the ratio of the actual traffic to the specified threshold is between the value specified by this parameter and that specified by **Medium-level Alert Percentage(%)**, the generated alert (direct or latent) is taken as a low-level one.

Parameter	Description
Medium-level Alert Percentage(%)	Ratio of the actual traffic to a value specified by **Latent Alert Threshold**, at which a medium-level alert is generated. The default threshold is **150**, and the maximum is **10000**. If the ratio of the actual traffic to the specified threshold is between the value specified by this parameter and that specified by **High-level Alert Percentage(%)**, the generated alert is taken as a medium-level one.
High-level Alert Percentage(%)	Ratio of the actual traffic to a value specified by **Latent Alert Threshold**, at which a high-level alert is generated. The default value is **200** and the maximum is **10000**.
Alert Latency Period	Specifies the time when NTA stays latent before generating an alert for traffic that remains at a specified level for some time. This period is the alert latency period. 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 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**).

Step 2 Configure NTA system performance alert, namely, the alert is triggered by abnormal CPU, memory, or disk usage, CPU temperature, board temperature, and fan status of NTA.

Step 3 After completing the configuration, click **Save**.

----End

5.3.3 Alert Plug-in Management

NTA has the following alert plug-ins:

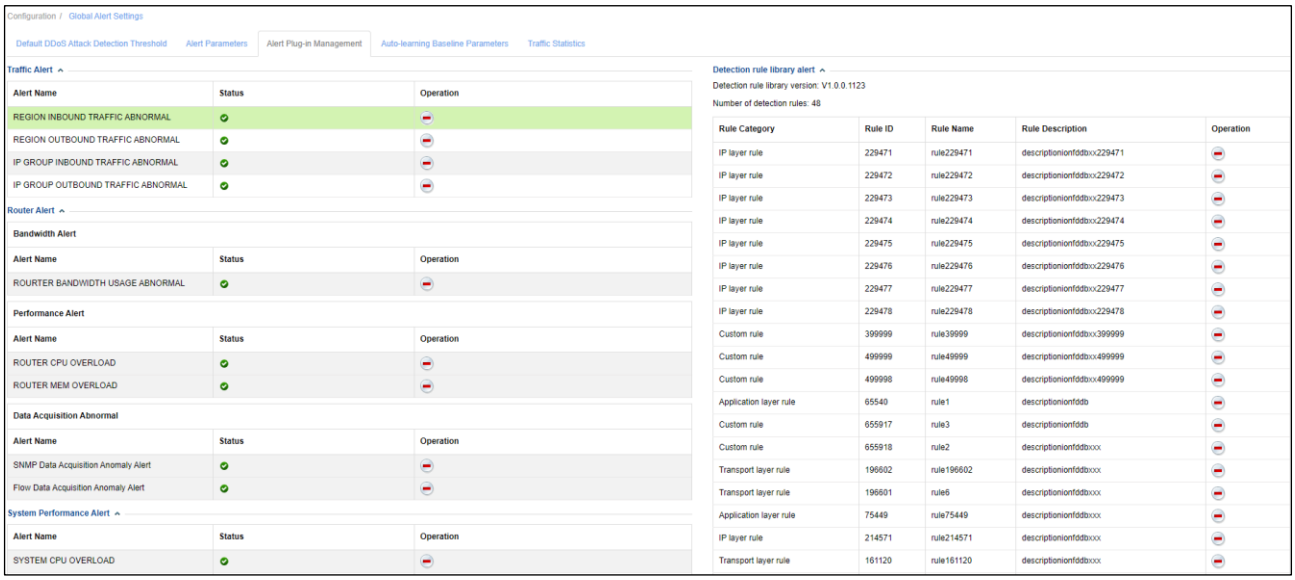
- Traffic alert plug-in: checks whether inbound and outbound traffic of a region or an IP group is abnormal.
- Router alert plug-in: checks whether the router interface usage and performance are abnormal.
- System performance alert plug-in: checks whether NTA performance is abnormal.
- Detection rule library alert plug-in: provides common detection rules.
- Attack alert plug-ins, classified into the following:
  - Custom attack alert plug-in: contains user-defined attack signatures.
  - Built-in attack alert plug-in: contains common attack signatures.

Each type of plug-in contains child plug-ins. You can enable or disable a child plug-in. After a child plug-in is disabled, the corresponding detection policy will not take effect.

To manage an alert plug-in, follow these steps:

Step 1 Choose **Configuration > Global Alert Settings > Alert Plug-in Management**.

Figure 5-71 Alert Plug-in Management page



Step 2 Enable or disable a child plug-in.

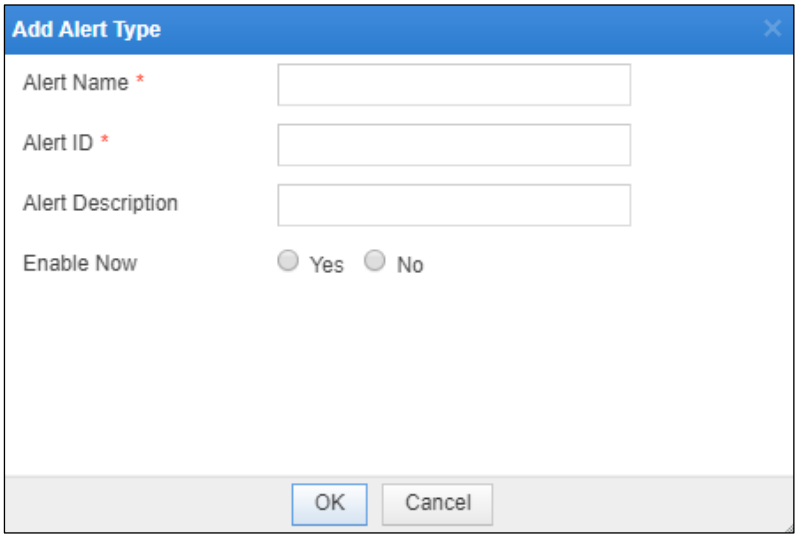
Click or in the **Operation** column to enable or disable the corresponding child plug-in. After a child plug-in is disabled, the corresponding detection policy will lose effect.

Step 3 Add a custom attack alert plug-in.

a. Add basic information.

Click **Add Custom Alert**.

Figure 5-72 Adding an alert type



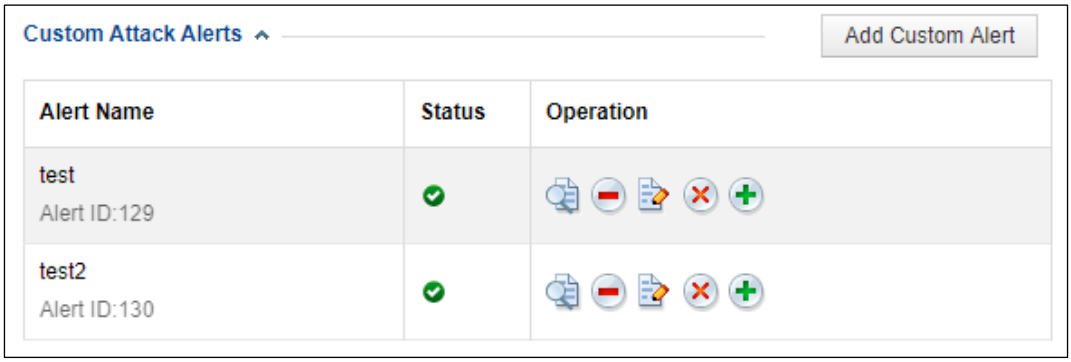
– Enter the alert name and alert ID, and, optionally, description, and choose whether to immediately enable the alert plug-in.

If you select **Enable Immediately**, the new plug-in will be in the Available state; otherwise, it will be in the Unavailable state.
After the plug-in is successfully created, you can click or in the **Operation** column to enable or disable the plug-in.

- Click **OK** to save the settings.

  The new alert plug-in is then displayed in the **Custom Attack Alerts** list, as shown in Figure 5-73.

Figure 5-73 Custom Attack Alerts list

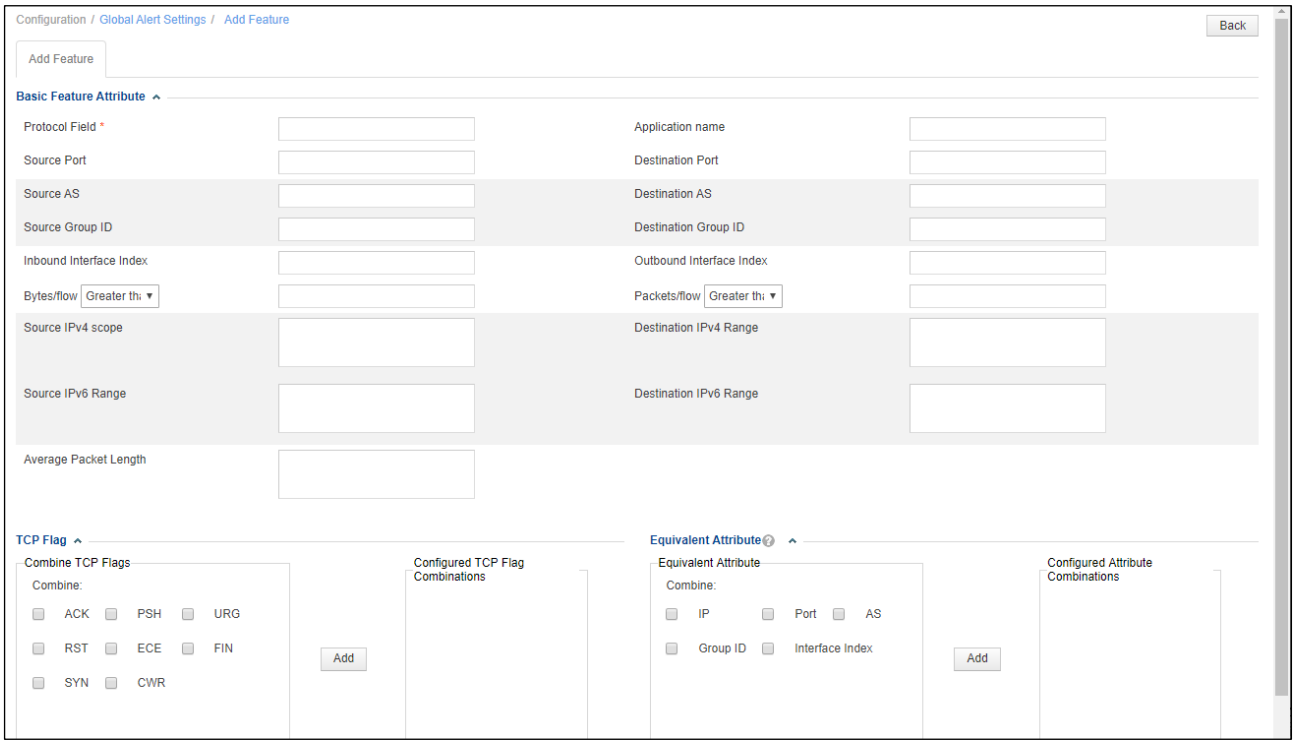


You can click in the **Operation** column to edit these custom alert plug-ins.

b. Add a signature.

Click in the **Operation** column to open the page shown in Figure 5-74.

Figure 5-74 Add Feature page



- Configure signature parameters according to your network conditions.
- After completing the configuration, click **Save**.

c. Delete a custom attack alert plug-in.

To delete a custom attack alert plug-in, click in the **Operation** column.

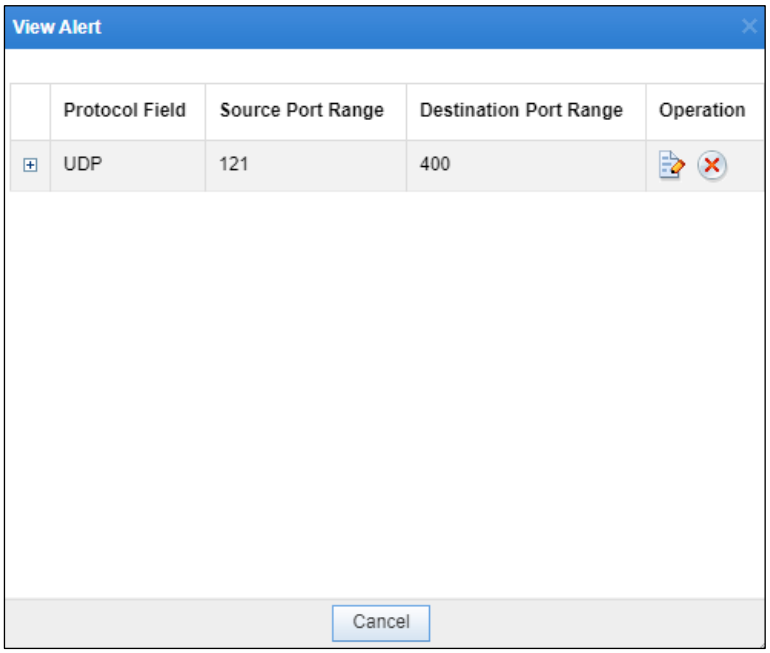
d. Edit a custom attack alert plug-in.

To edit a custom attack alert plug-in, click in the **Operation** column.

Step 4 View the referencing of a signature.

You can view fields of a built-in or custom attack alert plug-in by clicking in the **Operation** column.

Figure 5-75 Viewing fields of an attack alert plug-in

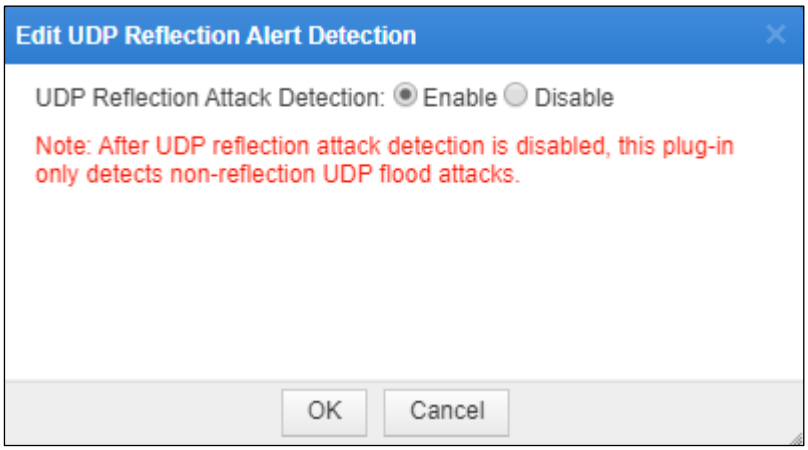


Step 5 Edit the UDP reflection alert detection setting.

You can click in the **Operation** column of UDP Flood to enable or disable the UDP reflection alert detection.

After **UDP Reflection Attack Detection** is set to **Enable**, when NTA detects UDP reflection attacks, only reflection attack alerts will be triggered. After **UDP Reflection Attack Detection** is set to **Disable**, NTA only detects non-reflection UDP flood attacks.

Figure 5-76 Configuring UDP reflection alert detection



----End

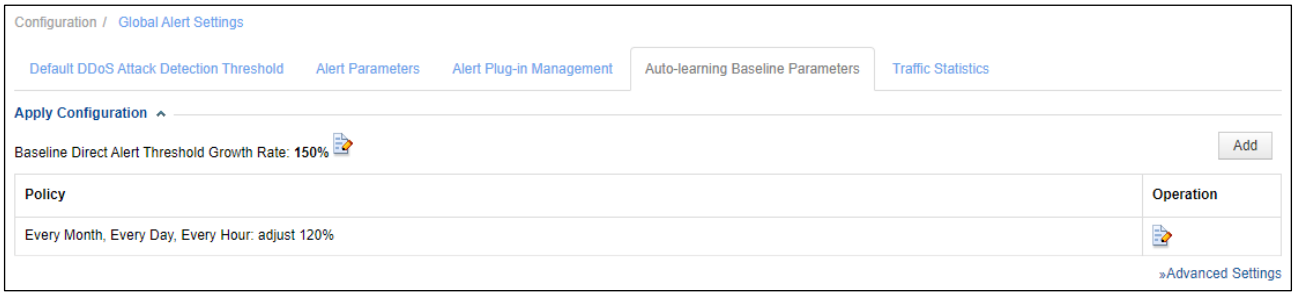
5.3.4 Auto-learning Baseline Parameters

Traffic auto-learning is a process whereby NTA automatically learns live traffic and determines proper thresholds, which can be adapted to different scenarios. Here is a description of how global parameters are configured for an IP group. For specific learning policies, see Configuring the Auto-Learning Baseline.

To configure global parameters for traffic auto-learning, follow these steps:

Step 1 Choose **Configuration > Global Alert Settings > Auto-learning Baseline Parameters**.

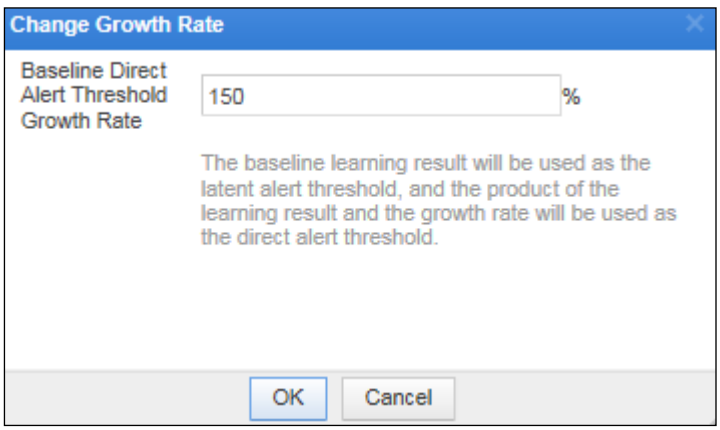
Figure 5-77 Auto-learning Baseline Parameters page



Step 2 Specify how much the baseline direct alert threshold should be raised.

The auto-learning result is the basis of determining the latent alert threshold. The direct alert threshold is the product of the latent alert threshold multiplied by the value specified here. The default value is **150%**. You can click to change the value in the dialog box shown in Figure 5-78.

Figure 5-78 Changing the direct alert threshold growth rate



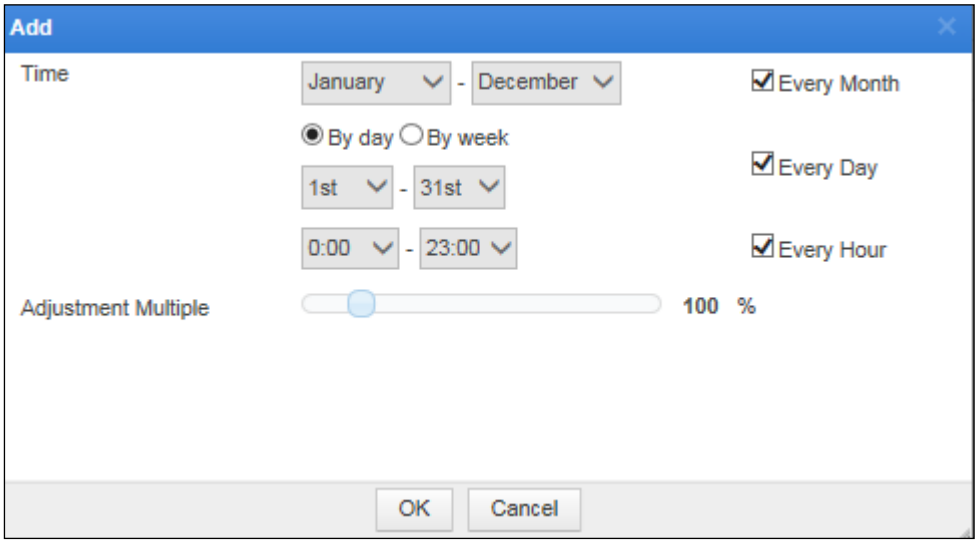
Change the value and click **OK**.

Step 3 Add a traffic auto-learning policy.

On particular days, traffic may rise sharply. You can have the latent alert threshold and direct alert threshold automatically raised for certain days to reduce false positives.

Click **Add**. The dialog box for adding a traffic auto-learning policy appears, as shown in Figure 5-79.

Figure 5-79 Adding a traffic auto-learning policy



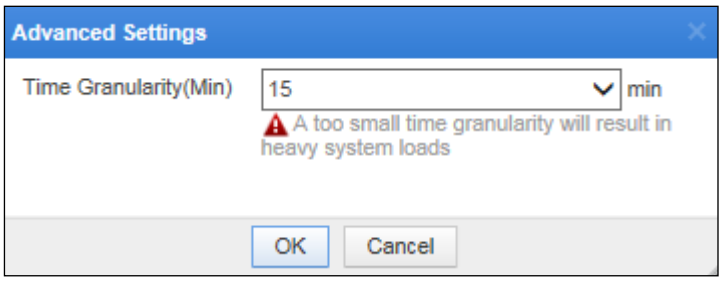
A traffic auto-learning policy specifies when and how much the growth rate needs to be adjusted. After a latent alert threshold is raised, the direct alert threshold is raised accordingly.

After changing the value, click **OK**.

Step 4 Change the time granularity.

The time granularity indicates the interval from when the threshold is calculated till it is applied for DDoS attack detection. It has a direct impact on the overall NTA performance and may cause unpredictable performance problems. Therefore, you are advised not to change the default value, which is **60** minutes. Click **Advanced Settings** in the lower-right corner of the **Apply Configuration** page. A dialog box appears, as shown in Figure 5-80.

Figure 5-80 Changing the time granularity



After changing the value, click **OK**.

Step 5 Move up or down a policy.

The default policy is always at the bottom. Other policies are presented in reverse chronological order. That is to say, the most recent policy comes first and has the highest priority. You can click or in the **Operation** column to move up or down a policy.

Step 6 To modify policy parameters, click in the **Operation** column.

Step 7 To delete a custom policy, click in the **Operation** column.

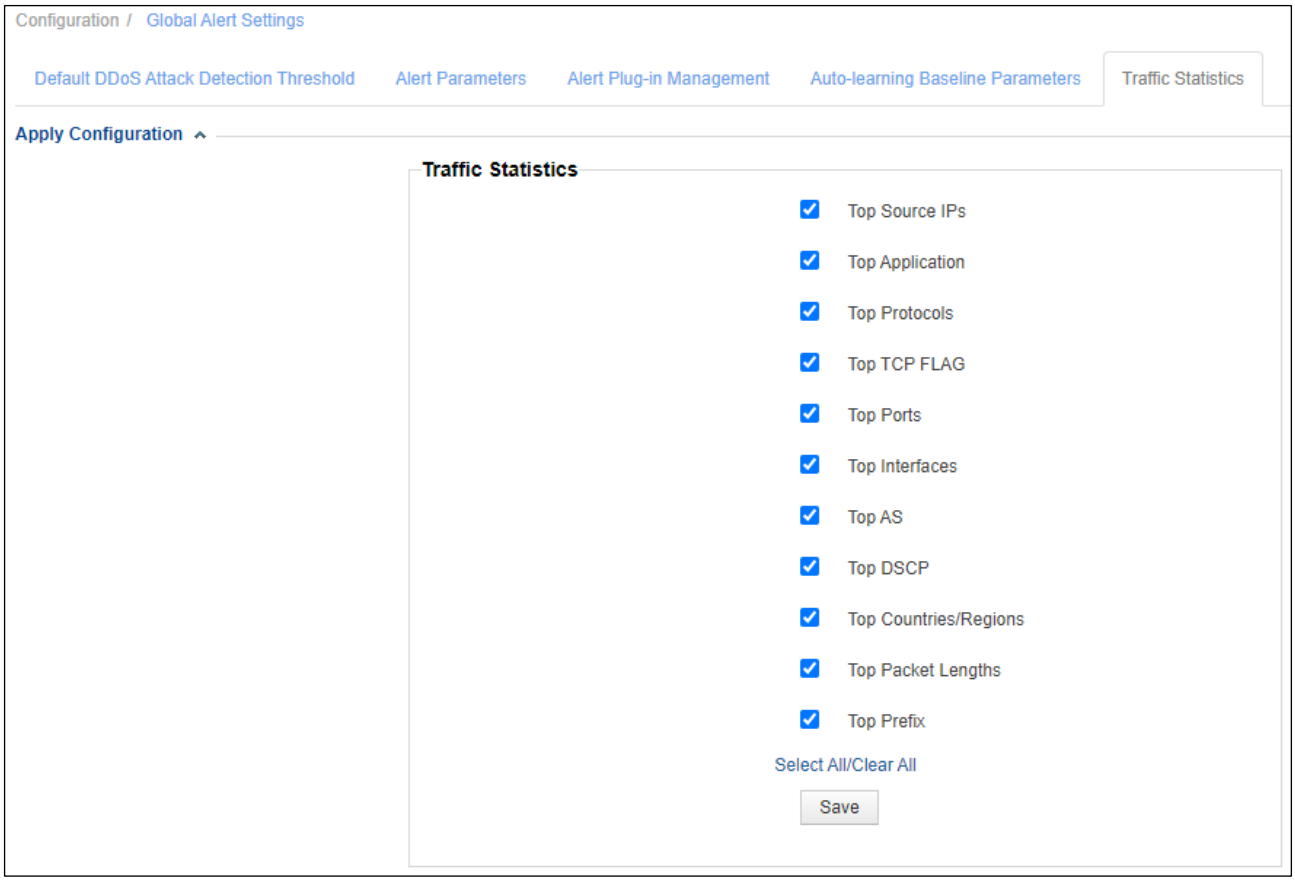
----End

5.3.5 Traffic Statistics

You can specify statistical items of traffic. The procedure is as follows:

Step 1 Choose **Configuration > Global Alert Settings > Traffic Statistics**.

Figure 5-81 Traffic Statistics page



Step 2 Select statistical items and click **Save**.

----End

5.4 Global Diversion Settings

The Global Divert Settings module allows you to configure the following:

- Default Diversion Configuration: configuration of a default policy for diverting attack traffic that does not match any policies
- BGP Configuration: configuration of BGP diversion and null route diversion parameters
- Protection Device Configuration: addition of ADS or a third-party protection device
- BGP FlowSpec Configuration: configuration of parameters for implementation of FlowSpec BGP.

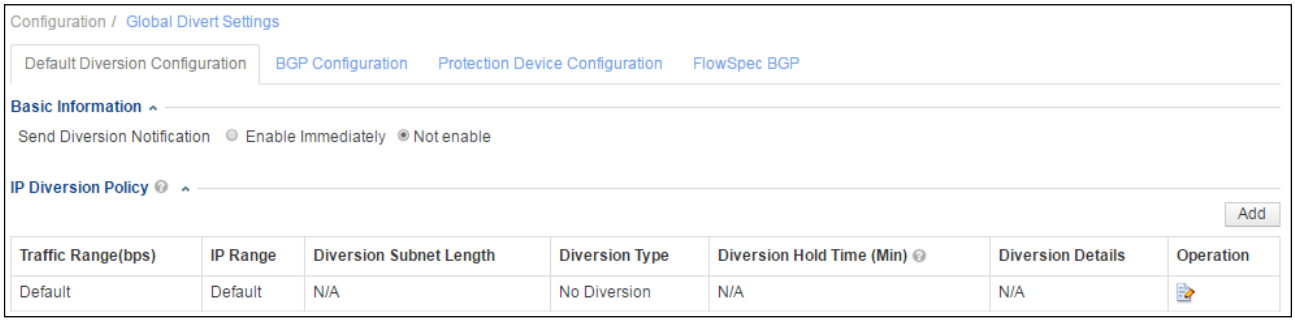
5.4.1 Default Diversion Configuration

You can configure a default diversion policy to divert DDoS attack traffic that does not match any policies.

The procedure is as follows:

Step 1 Choose **Configuration > Global Divert Settings > Default Diversion Configuration**.

Figure 5-82 Default Diversion Configuration page



Step 2 Configure the null route/BGP diversion holding time.

After sending a "Null Route/BGP Diversion" notification to a device, NTA will start a countdown to the revocation of the involved route. Once the diversion holding time expires, NTA revokes the route.

The default value of **Null Route/BGP Diversion Holding Time** is **120** minutes. You can change the value and then click **Save** to commit the change.

Step 3 Configure whether to divert traffic and whether to send a diversion notification when the diversion ends.

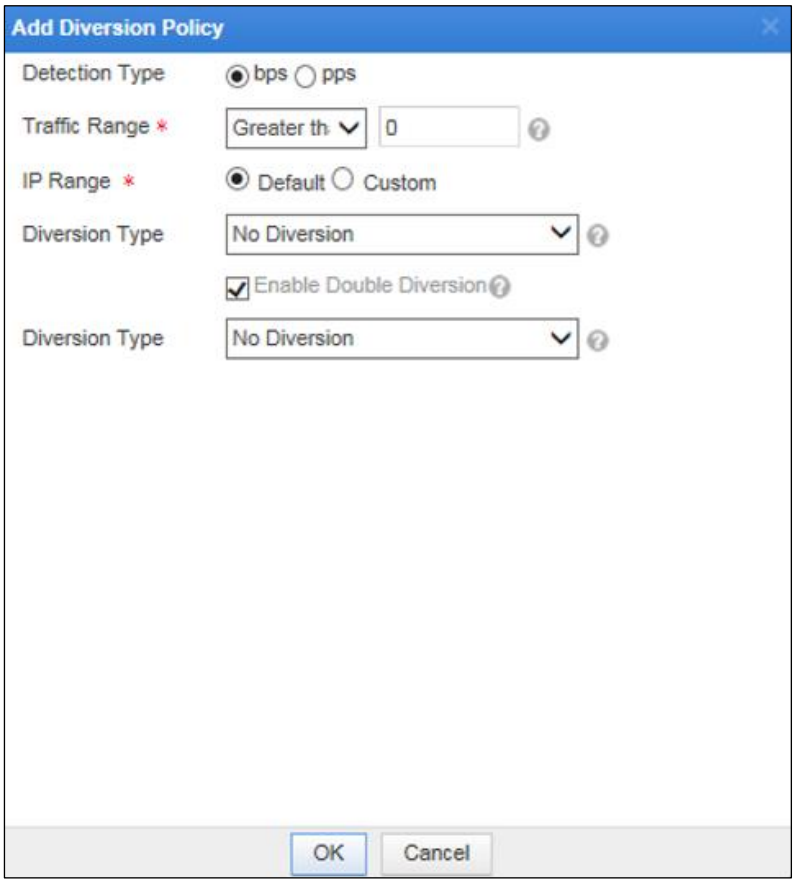
If you select **Enable Immediately**, NTA sends a diversion notification email to the designated address of the contact when the diversion targeting a region or IP groups within a region starts and ends. For how to configure the email address, see section 4.3.1.1 Configuring Mail Settings.

Step 4 Configure an IP address-specific diversion policy.

You can configure different diversion policies for DDoS attack traffic of different levels and IP address segments.

To add an IP address-specific diversion policy, click **Add** in the upper-right corner of the **IP Diversion Policy** area. A dialog box for adding such a policy appears, as shown in Figure 5-83.

Figure 5-83 Adding an IP address-specific diversion policy



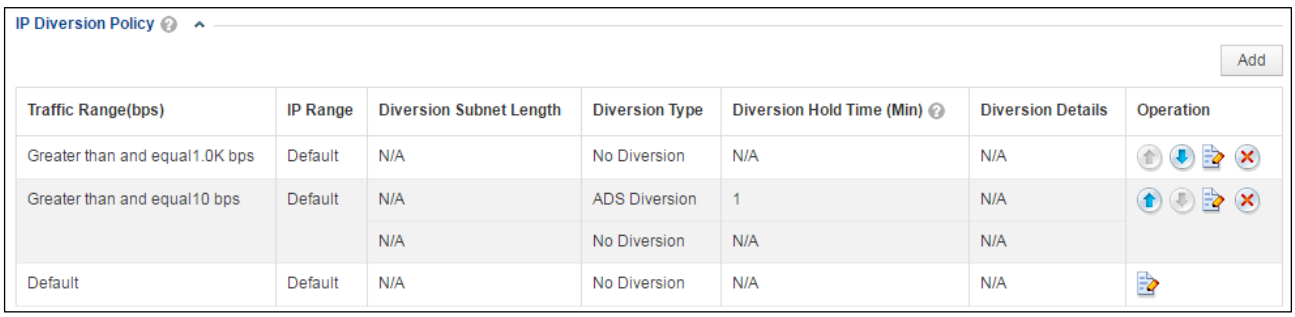
For the description of parameters, see Table 5-12.

After completing the configuration, click **OK**.

Step 5 Change the policy priority.

When multiple diversion policies are available, they are displayed in descending order of priority, as shown in Figure 5-84. The traffic is matched against diversion policies in the order of priority. Once a policy is hit, the traffic is diverted accordingly.

Figure 5-84 Traffic diversion policies sorted in descending order of priority



You can click in the **Operation** column to raise the priority or to lower the priority.

Step 6 Modify a policy.

To modify a policy, click in the **Operation** column.

Step 7 Delete a policy.

To delete a policy, click in the **Operation** column.

----End

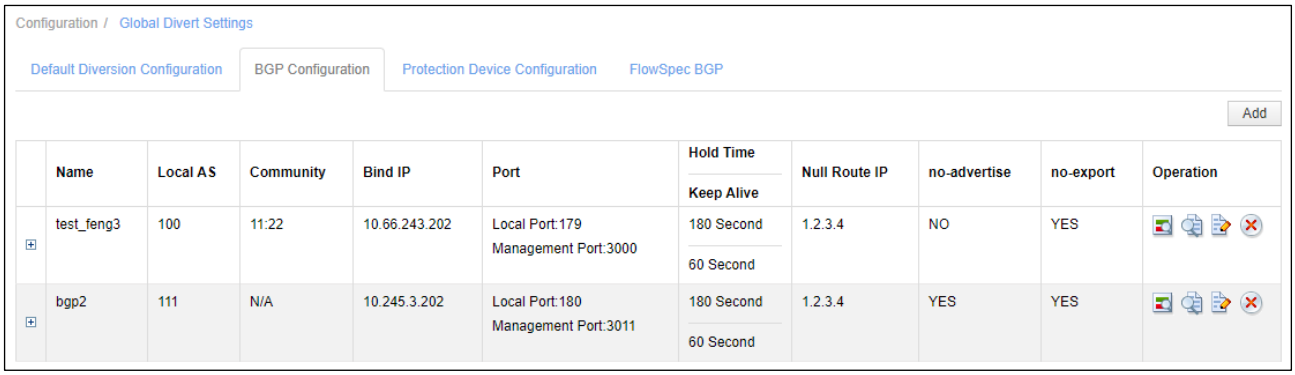
5.4.2 BGP Configuration

To implement null route or BGP diversion, NTA must establish iBGP neighborship with a router. Only in this way can NTA advertise route update notifications for diversion of attack traffic to a third-party device for cleaning. This module allows you to configure parameters for establishing a BGP session.

The procedure is as follows:

Step 1 Choose **Configuration > Global Divert Settings > BGP Configuration**.

Figure 5-85 BGP Configuration page



Step 2 Add a BGP entry.

Click **Add** in the upper-right corner of the **BGP Configuration** page. The page for adding a BGP entry appears, as shown in Figure 5-86.

Figure 5-86 Add BGP Session page

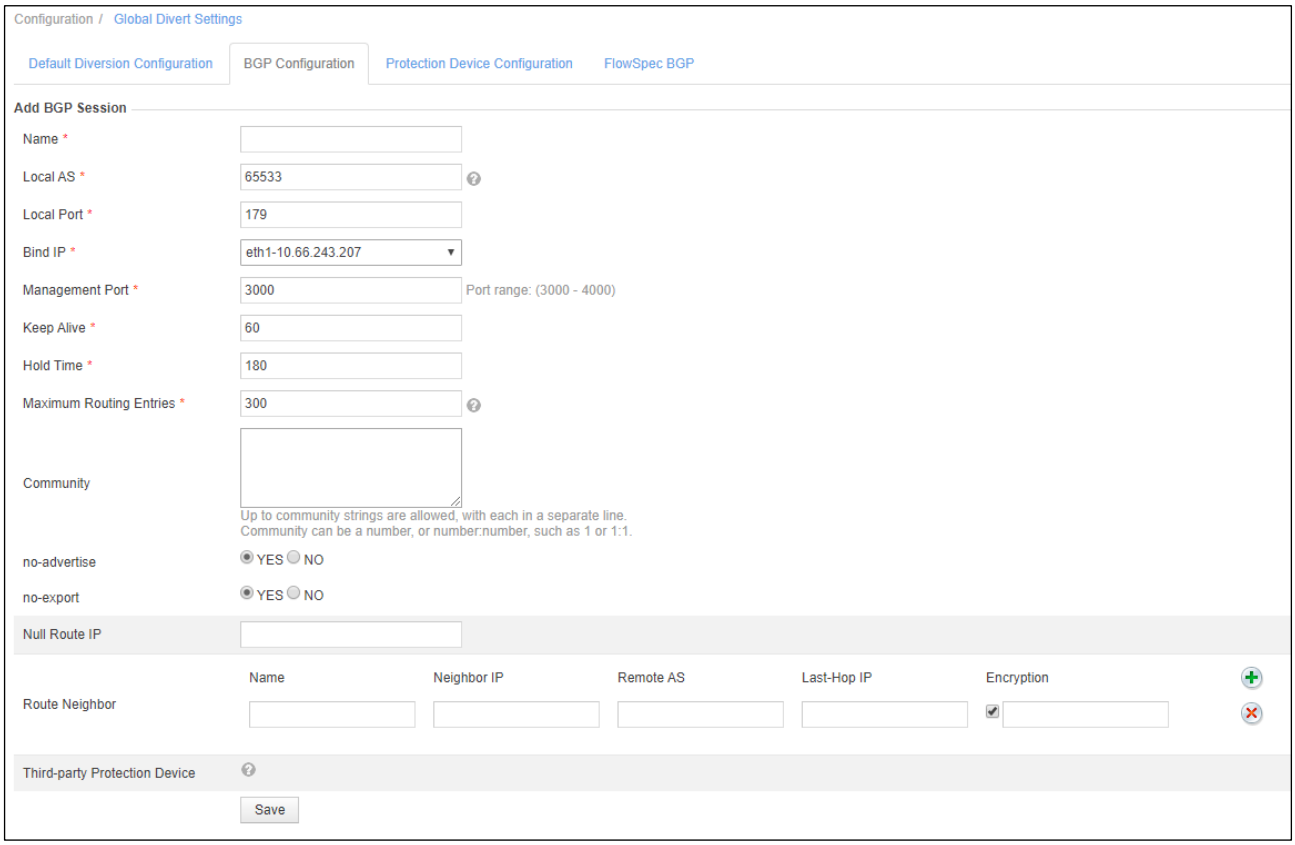


Table 5-17 describes parameters on this page.

Table 5-17 BGP configuration parameters

Parameter	Description
Name	Specifies a string that identifies the entry.
Local AS	Specifies the local AS number, which must be the same as that of the BGP neighbor; otherwise, neighborship cannot be established.
Local Port	Specifies the source port for data exchange with BGP neighbors. Generally, it is port 179.
Bind IP	Specifies the local IP address used by NTA to establish the BGP neighborship. When two NTA devices constitute a master/backup pair for HA and the local device is a master one, you must select a virtual IP address.
Management Port	Specifies the management port of the local route analysis module. The default value is recommended.
Keep Alive	Specifies the interval for sending keepalive messages to a BGP neighbor to ensure that the link with the neighbor is operating. The default value is **60** seconds.
Hold Time	Specifies the maximum time BGP waits between successive messages before closing the connection. Generally, it is 180 seconds.
Maximum Routing Entries	Specifies the maximum number of routing entries that NTA can send in a session based on this BGP entry. Specifying the maximum number can prevent router

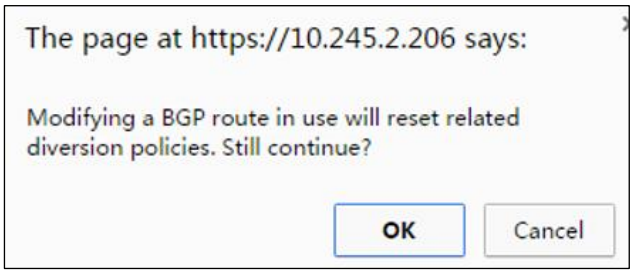
Parameter	Description
	performance from deteriorating because of NTA sending too many BGP messages.
Community	Specifies how the BGP-speaking router treats this route. A maximum of five communities are allowed, with each one in a separate line. In the text box to the right of **Community**, you can configure parameters other than **no-advertise and no-export**. The format is xxx:xxx. • **no-advertise**: If this parameter is set to **YES**, it indicates that this route is not advertised to any BGP peers. • **no-export**: If this parameter is set to **YES**, it indicates that this route is not advertised to other ASs.
Null Route IP	Specifies the destination IP address for null route diversion. Traffic reaching the null route IP address will be dropped. This parameter is required only when a BGP session is used in null-route diversion. Note • If traffic triggers null-route diversion, NTA uses the BGP protocol to set the next hop of the traffic to the null route IP address, sends a BGP Update message to the neighbor router, and diverts traffic to the BGP neighbor router. • Since a static route is configured on the router to direct all traffic destined for the null-route IP address to null, all traffic destined for the null route IP address will be dropped by the router.
Route Neighbor	Specifies a BGP neighbor, which can be added and deleted. To add a BGP neighbor, configure the following parameters: • **Name**: name of the router that establishes the BGP neighborship with NTA. • **Neighbor IP**: IP address of the router that establishes the BGP neighborship with NTA. • **Remote AS**: Specifies the remote autonomous system number of the router that establishes the BGP neighborship with NTA. • **Last-Hop IP**: IP address of the router that is the last hop of the route from the router to NTA. • **Encryption**: controls whether to encrypt BGP connections. Selecting this option indicates that communication between NTA and the BGP neighbor will be encrypted and requires you to enter a password in the adjacent text box.
Third-party Protection Device	Specifies a third-party device for traffic cleaning. For how to configure a third-party protection device, see section 5.4.3 Protection Device Configuration. This parameter is required only when a BGP session is used in BGP diversion. Note • If traffic triggers BGP diversion, NTA uses the BGP protocol to set the next hop of the traffic to a third-party protection device, sends a BGP Update message to the neighbor router, and diverts traffic to the BGP neighbor router. • Since a static route destined for the third-party device is configured on the router, traffic reaching the neighboring router will be diverted to the third-party device.

After completing the configuration, click **Save**.

Step 3 Modify a BGP entry.

Click in the **Operation** column.If the current BGP entry is being used in a session, modifying its parameters will cause the BGP service to restart and the diversion to end. At the same time, the system pops up a dialog box, as shown in Figure 5-87.

Figure 5-87 Message indicating that the BGP entry is in use



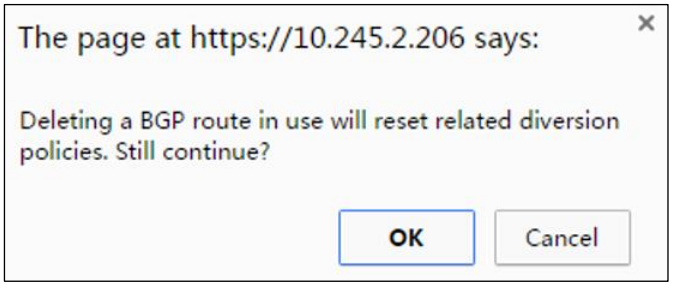
If you click **OK**, the related BGP session will be restarted. After that, you can modify the BGP entry.

Step 4 Delete a BGP entry.

Click in the **Operation** column.

Even if a BGP entry is being used in a session, you can successfully delete it as long as you click **OK** in the confirmation dialog box shown in Figure 5-88.

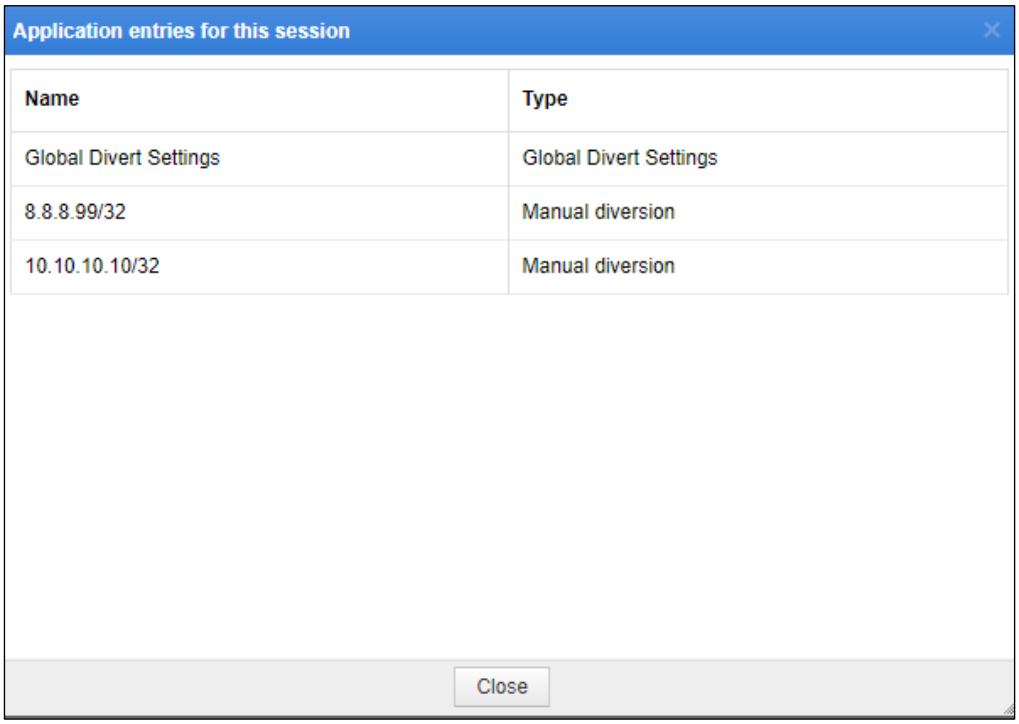
Figure 5-88 Confirmation dialog box for deleting a BGP entry



Step 5 View the referencing of an entry.

Clicking in the **Operation** column, you can view which regions or IP groups have referenced this session, as shown in Figure 5-89.

Figure 5-89 Referencing of a BGP session

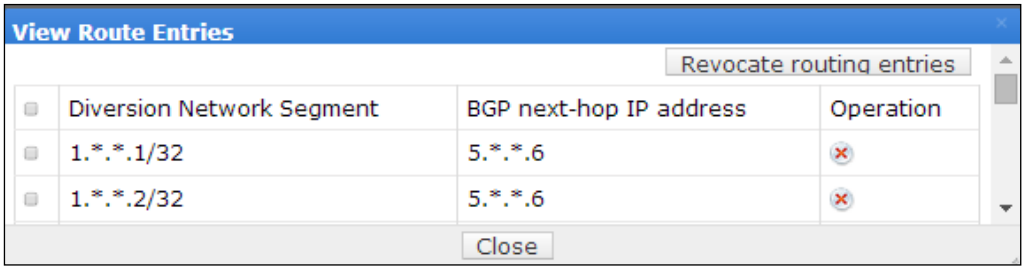


- **Name** indicates the name of the object that references this BGP session.
- **Type** indicates the type of the object that references this BGP session. It has the following values:
  - Region: indicates that the entry is referenced by a region.
  - IP group: indicates that the entry is referenced by an IP group.
  - Manual diversion: indicates that the related BGP session is triggered by manual diversion.
  - Global diversion: indicates that the object that references the session is not defined.

Step 6 View routing entries.

Clicking in the **Operation** column, you can view IP addresses whose traffic is diverted through this BGP entry, as shown in Figure 5-90.

Figure 5-90 Routing entries

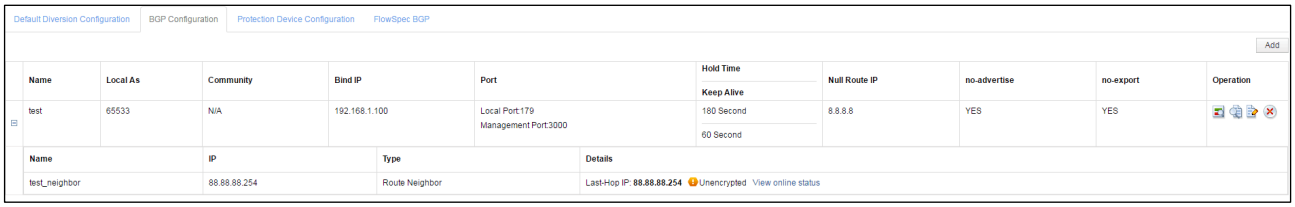


To cancel diversion of traffic destined for this IP address, click in the **Operation** column. To delete multiple routes in batches, select the desired ones and click **Revocate routing entries**.

Step 7 Query the BGP neighbor status.

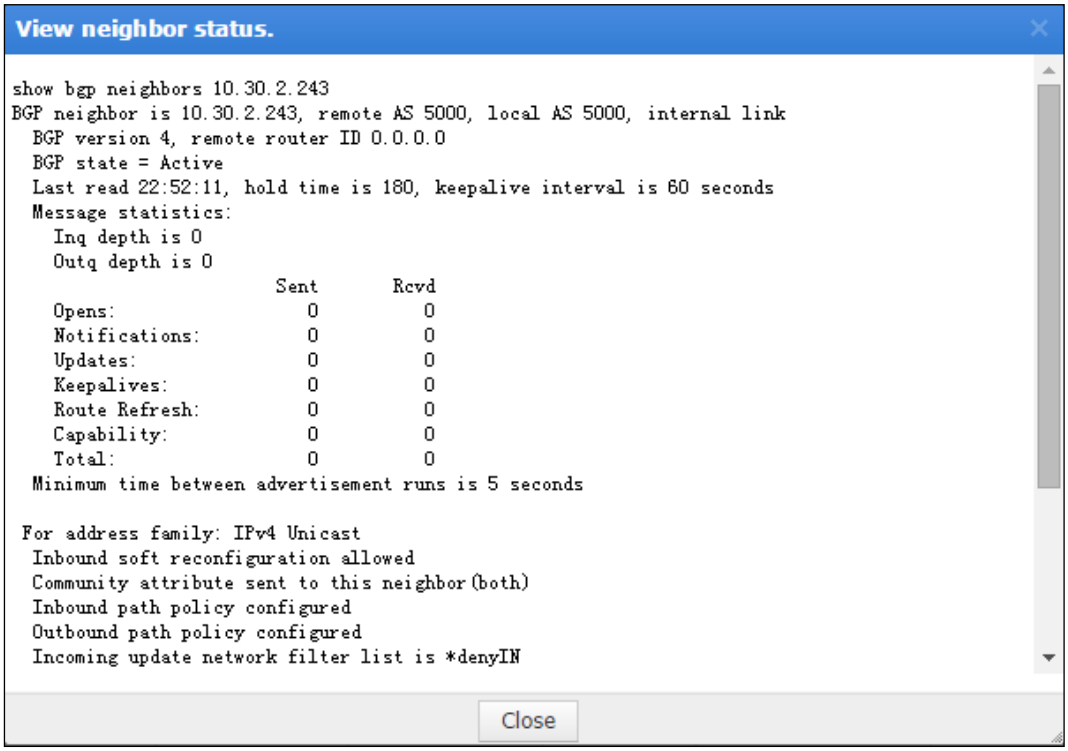
a. Click on the left of the BGP entry name to display the BGP neighbor, as shown in Figure 5-91.

Figure 5-91 Query of the BGP neighbor status



b. Click **View online status**. The BGP neighbor status is displayed, as shown in Figure 5-92.

Figure 5-92 BGP neighbor status query result



c. Click **Close** to complete the query.

----End

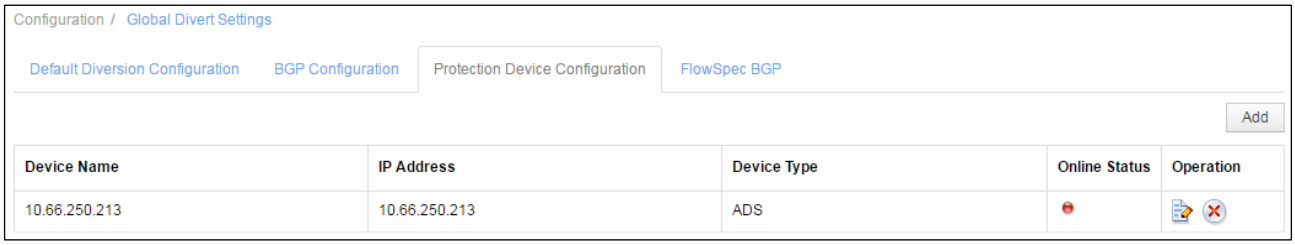
5.4.3 Protection Device Configuration

After detecting abnormal traffic, NTA can have such traffic diverted to ADS for cleaning. Alternatively, it can have the traffic diverted to a third-party protection device after sending a BGP routing notification to this device.

A protection device is either an ADS or a third-party protection device. To configure a protection device, follow these steps:

Step 1 Choose **Configuration > Global Divert Settings > Protection Device Configuration**.

Figure 5-93 List of protection devices



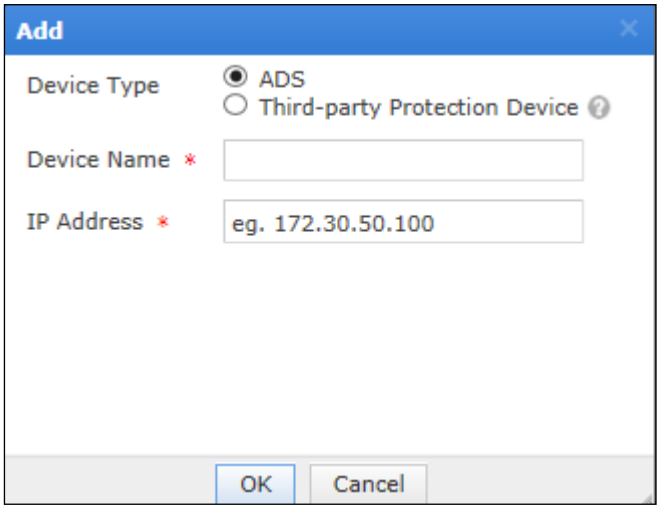
When **Device Type** is **ADS,** NTA checks whether the device is online. indicates that the device is online and indicates the opposite. For a third-party device, NTA does not check its status, which is always displayed as **N/A**.

Step 2 Add a protection device.

a. Click **Add** in the upper-right corner.

A dialog box appears, as shown in Figure 5-94.

Figure 5-94 Adding a protection device



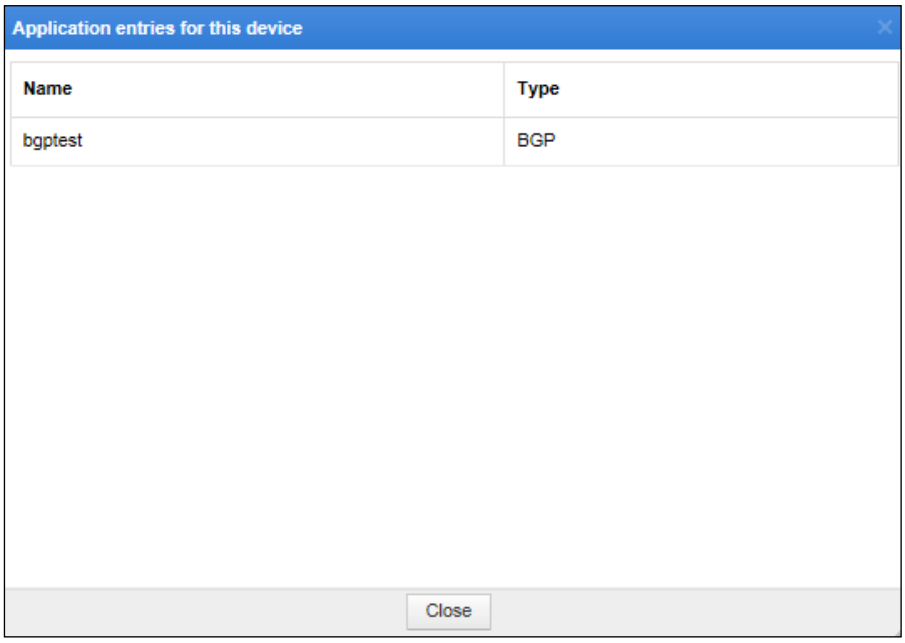
b. Select **ADS** or **Third-party Protection Device** for **Device Type**.

c. Enter the name and IP address of the device, and then click **OK**.

Step 3 View the use of a third-party device.

You can view the use of only a third-party device. Click in the **Operation** column. A dialog box appears, as shown in Figure 5-95.

Figure 5-95 Objects that have used the device



- **Name** indicates the name of an object that uses this device.
- **Type** indicates the type of the object that uses this device, which can only be **BGP**.

Step 4 Edit device information.

Click in the **Operation** column.

Step 5 Delete a device.

Click in the **Operation** column.

----End

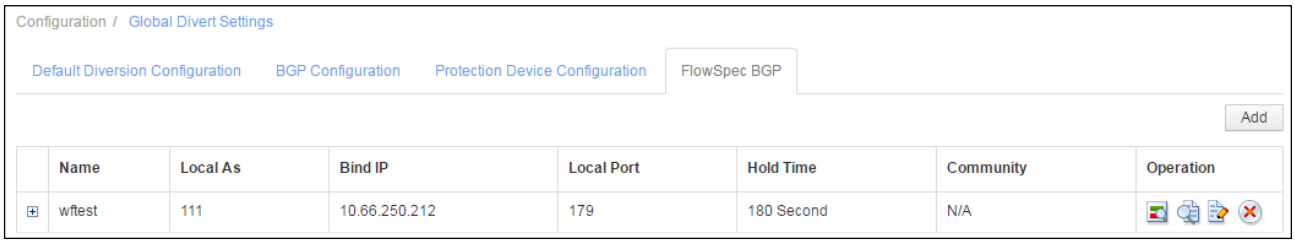
5.4.4 BGP FlowSpec Configuration

NTA supports the BGP flow specification (FlowSpec). To implement BGP FlowSpec, you must configure parameters for establishing a BGP FlowSpec session.

The procedure is as follows:

Step 1 Choose **Configuration** > **Global Divert Settings** > **FlowSpec BGP**.

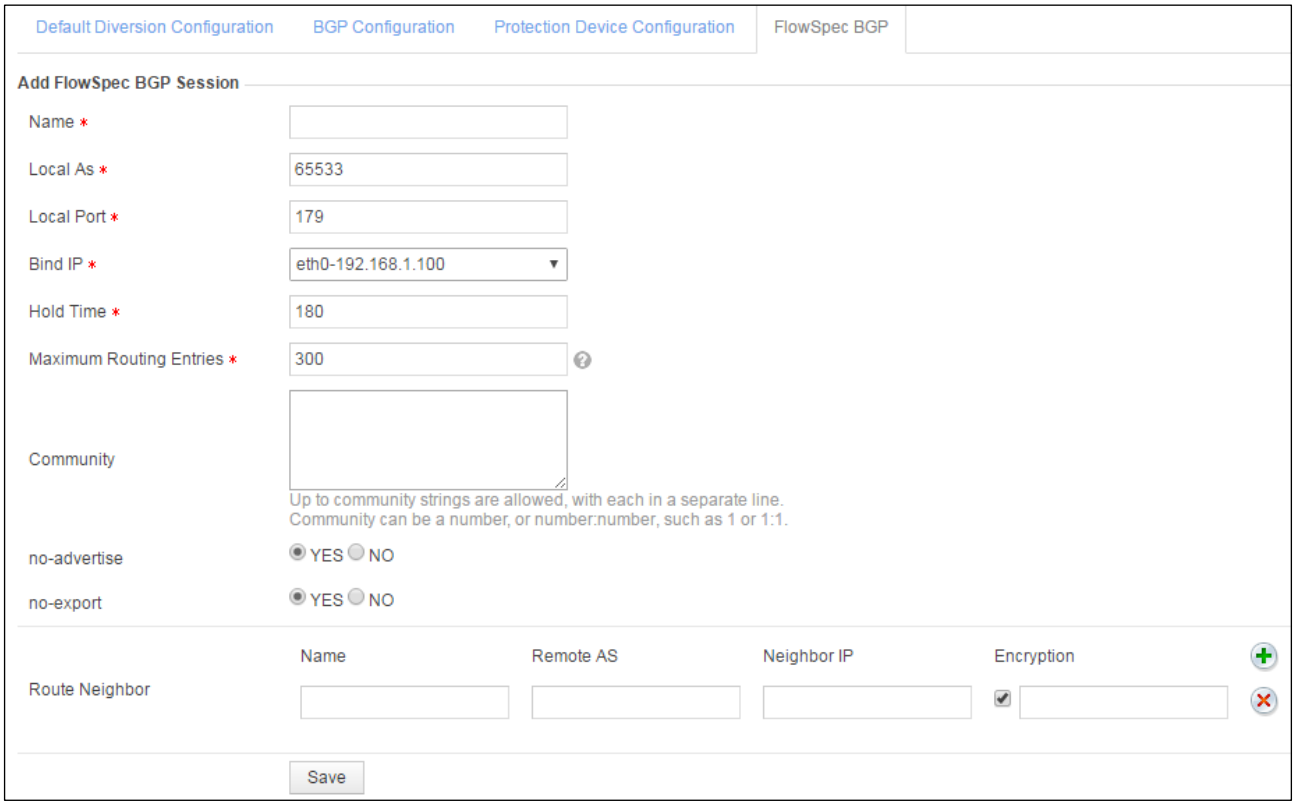
Figure 5-96 FlowSpec BGP page



Step 2 Add a BGP FlowSpec entry.

a. Click **Add** in the upper-right corner. The page for adding a BGP FlowSpec entry appears, as shown in Figure 5-97.

Figure 5-97 Adding a BGP FlowSpec entry



b. Configure parameters.

Table 5-18 BGP FlowSpec configuration parameters

Parameter	Description
Name	Specifies a string that identifies the entry.
Local AS	Specifies the local AS number, which must be the same as that of the BGP FlowSpec neighbor; otherwise, neighborship cannot be established.

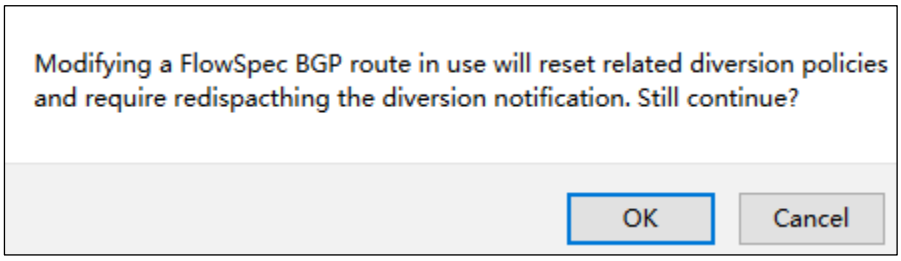
Parameter	Description
Local Port	Specifies the source port for data exchange with BGP FlowSpec neighbors. Generally, it is port 179.
Bind IP	Specifies the local IP address used by NTA to establish the BGP FlowSpec neighborship. When two NTA devices constitute a master/backup pair for HA and the local device is a master one, you need to select a virtual IP address.
Hold Time	Specifies the maximum time BGP FlowSpec waits between successive messages before closing the connection. Generally, it is 180 seconds.
Maximum Routing Entries	Specifies the maximum number of routing entries that NTA can send in a session based on this BGP FlowSpec entry. Specifying the maximum number can prevent router performance from deteriorating because of NTA sending too many BGP FlowSpec messages.
Community	Specifies how the BGP FlowSpec-speaking router treats this BGP FlowSpec routing message. A maximum of five community strings are allowed, with each one in a separate line. In the text box to the right of **Community**, you can type values other than **no-advertise** and **no-export** in the format of xxx:xxx. • **no-advertise**: The value of **YES** indicates that information about this route is not advertised to any BGP FlowSpec peers. • **no-export**: The value of **YES** indicates that information about this route is not advertised to other ASs.
Route Neighbor	Specifies a neighbor, which can be added and deleted. To add a BGP neighbor, configure the following parameters: • **Name**: name of the router that establishes the BGP FlowSpec neighborship with NTA. • **Remote AS**: number of the external AS. • **Neighbor IP**: IP address of the router that establishes the BGP FlowSpec neighborship with NTA. • **Encryption**: controls whether to encrypt BGP FlowSpec connections. Selecting this option indicates that communication between NTA and the BGP FlowSpec neighbor will be encrypted. In this case, you must set a password in the adjacent text box.

c. Click **Save** to commit the settings.

Step 3 Modify a BGP FlowSpec entry.

Click in the **Operation** column. If the current BGP FlowSpec entry is being used in a session, modifying its parameters will cause the BGP FlowSpec service to restart and the diversion to end. At the same time, the system pops up a dialog box, as shown in Figure 5-98.

Figure 5-98 Message indicating that the current BGP FlowSpec entry is in use

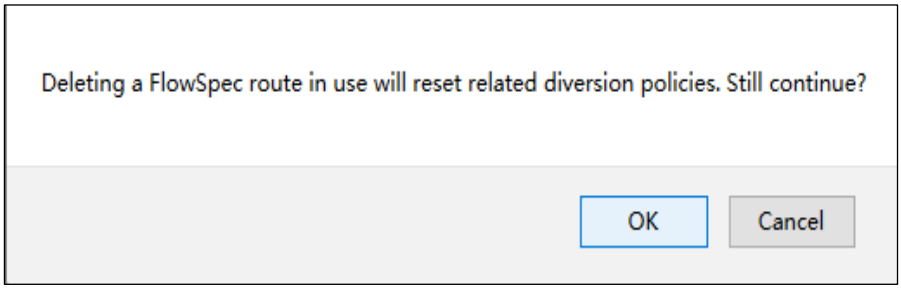


If you click **OK**, the related BGP FlowSpec session will be restarted. After that, you can modify the BGP FlowSpec entry.

Step 4 Delete a BGP FlowSpec entry.

Click in the **Operation** column. Even if a BGP FlowSpec entry is being used in a session, you can successfully delete it as long as you click **OK** in the confirmation dialog box shown in Figure 5-99.

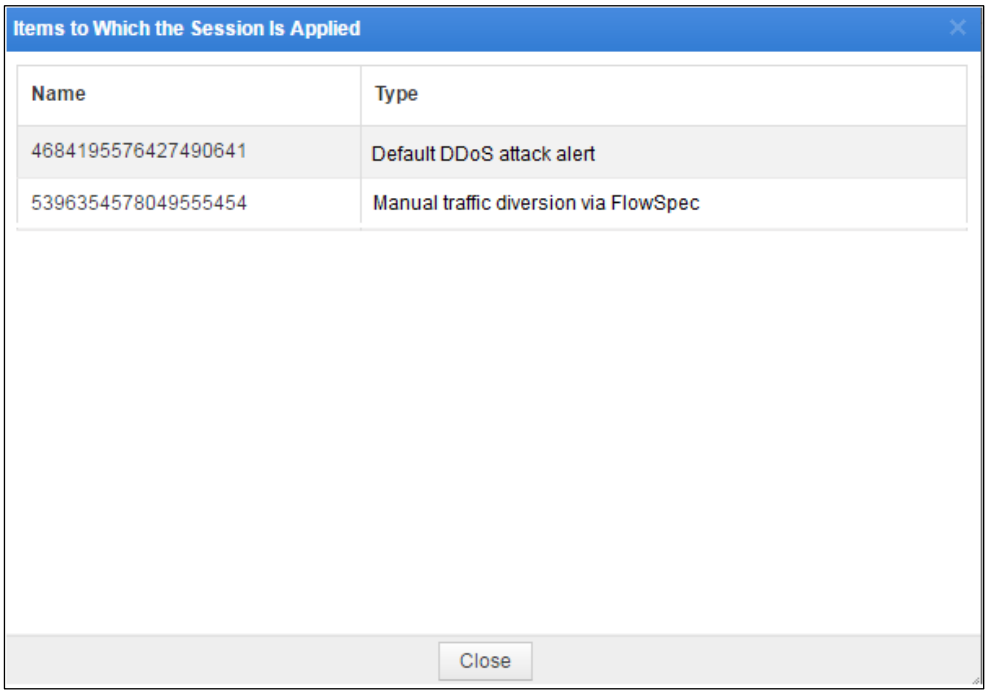
Figure 5-99 Confirmation dialog box for deleting a BGP FlowSpec entry



Step 5 View the referencing of an entry.

Clicking in the **Operation** column, you can view which regions or IP groups have referenced this entry, as shown in Figure 5-100.

Figure 5-100 Referencing of a BGP FlowSpec entry

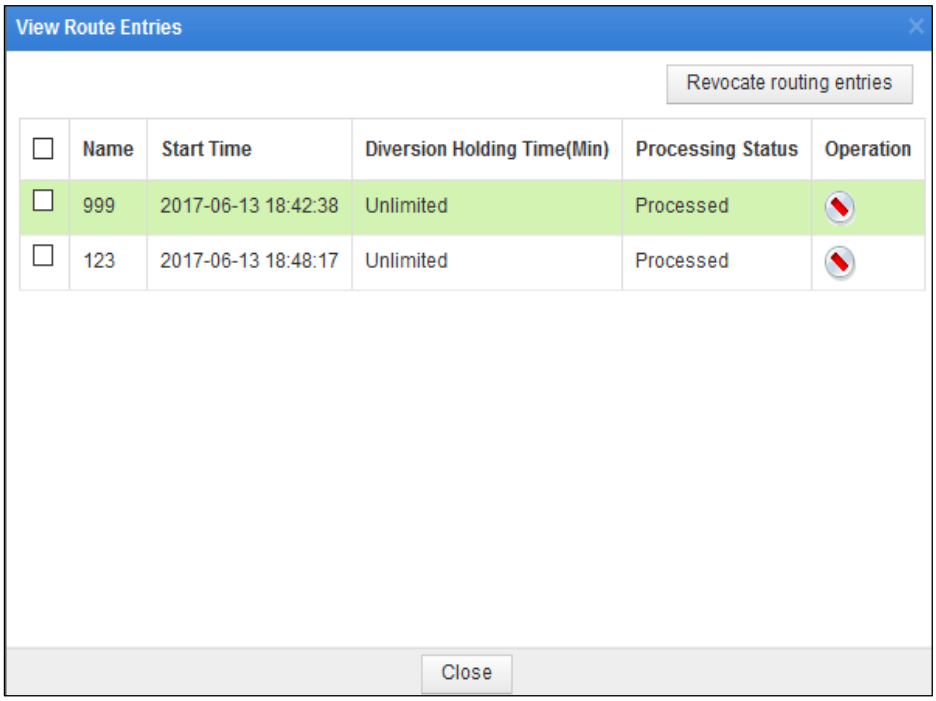


- **Name** indicates the name of the object (region or IP group) that references this BGP FlowSpec entry.
- **Type** indicates the type of the object that references this BGP FlowSpec entry. It has the following values:
  - Region: indicates that the entry is referenced by a region.
  - IP group: indicates that the entry is referenced by an IP group.
  - Manual diversion: indicates that the related session is triggered by manual diversion.
  - Global diversion: indicates that the object that references this entry is not defined.

Step 6 View routing entries.

Clicking in the **Operation** column, you can view IP addresses whose traffic is diverted through this BGP FlowSpec entry, as shown in Figure 5-101.

Figure 5-101 Viewing routing entries

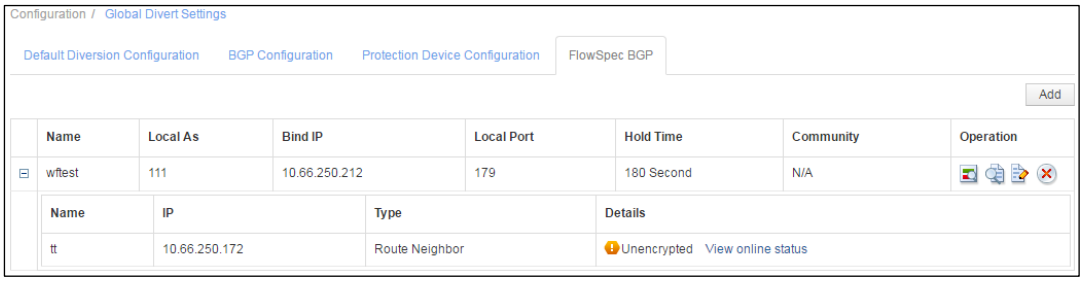


To cancel diversion of traffic destined for this IP address, click in the **Operation** column. To delete multiple routes in batches, select the desired ones and click **Revocate routing entries**.

Step 7 Query the neighbor status.

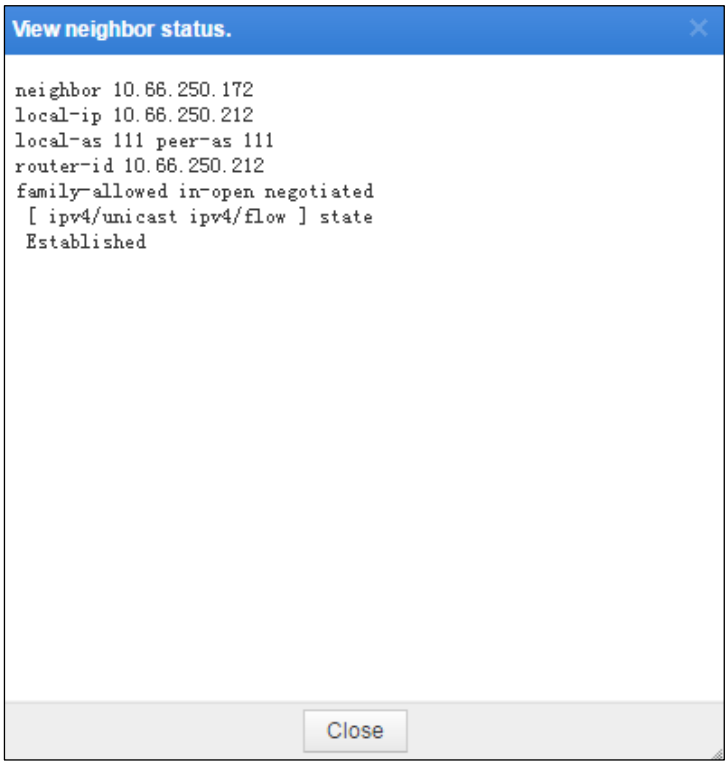
a. Click the add sign (+) on the left of the entry name to display the BGP FlowSpec neighbor, as shown in Figure 5-102.

Figure 5-102 BGP FlowSpec neighbor displayed



b. Click **View online status**. The neighbor status is displayed, as shown in Figure 5-103.

Figure 5-103 Neighbor status query result



c. Click **Close** to complete the query.

----End

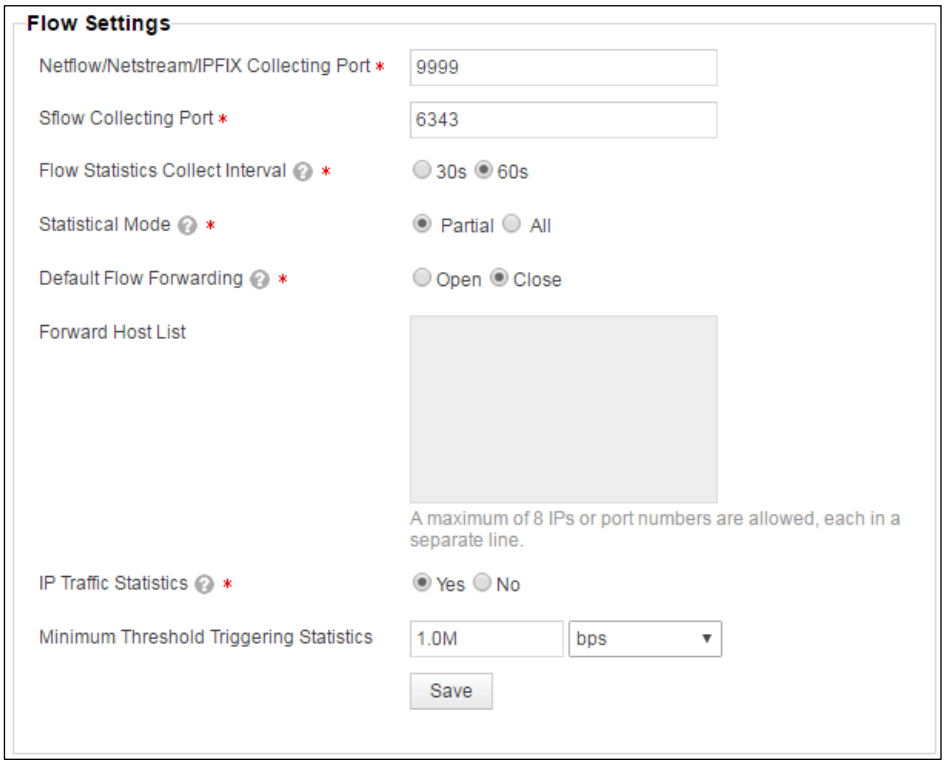
5.5 Flow Data Collection and Forwarding

NTA analyzes traffic and detects exceptions based on flow data sent by a device. The Flow Settings module allows you to configure default settings for Flow data collection and forwarding, including the port receiving Flow data and whether to forward Flow data as it is. During router configuration, you can specify Flow data collection and forwarding settings for each router or use default settings configured here. For details about the former method, see section 5.1.1.1 Configuring a Router.

To configure default settings for Flow data collection and forwarding, follow these steps:

Step 1 Choose **Configuration > Flow Settings**.

Figure 5-104 Flow Settings page



Step 2 Configure the parameters.

Table 5-19 Parameters of flow settings

Parameter	Description
Netflow/Netstream/IPFIX Collecting Port	The default port number is **9999**.
Sflow Collecting Port	The default port number is **6343**.
Flow Statistics Collect Interval	Specifies the interval at which Flow statistics are collected, which can be **30s** or **60s**.
Statistical Mode	Specifies a statistical mode. This parameter must be specified when **60s** is selected for **Flow Statistics Collect Interval**. • **Partial**: collects flow data within the 60-second statistical interval. • **All**: collects all flow data within the cache period. When the cache period of flows is shorter than or equal to 60 seconds, you are advised to select **All**; otherwise, select **Partial**.
Default Flow Forwarding	Controls whether NTA forwards the received Flow data. By default, the Flow data is not forwarded. When **this parameter** is set to **Open**, you must specify **Forward Host List**.
Forward Host List	Specifies the destination IP address and port number for Flow data forwarding. This parameter is required only when **Default Flow Forwarding** is set to **Open**.

Parameter	Description
IP Traffic Statistics	Controls whether NTA collects statistics on IP traffic. By default, statistics on IP traffic are not collected. When **this parameter** is set to **Open**, you must set **Minimum Threshold Triggering Statistics**.
Minimum Threshold Triggering Statistics	The statistical result is displayed only when the actual traffic in a cycle is greater than the specified threshold. For details, see section 9.6 IP Addresses.

Step 3 After completing the configuration, click **Save**.

----End

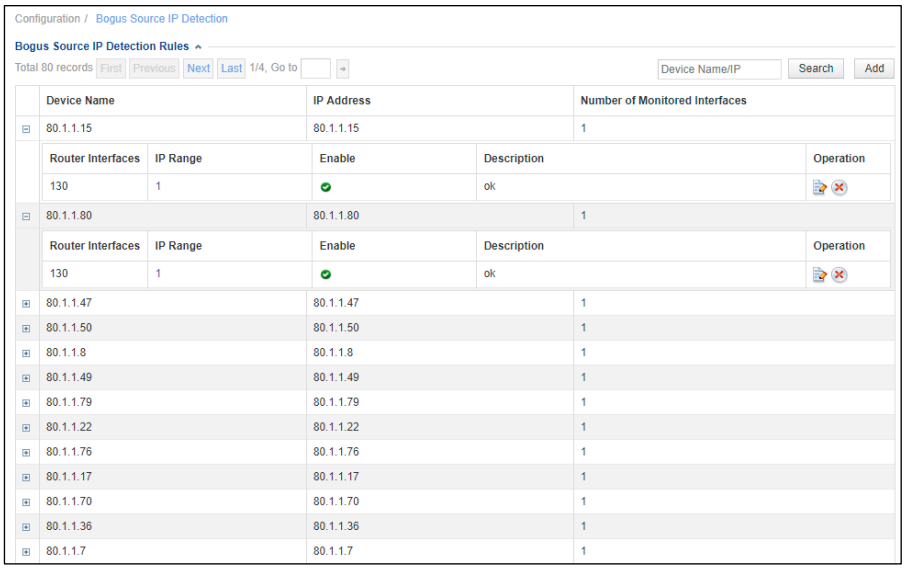
5.6 Detection of Bogus Source IP Addresses

If bogus source IP addresses are configured for router interfaces, NTA can discover and present these IP addresses and determine which interfaces they belong to.

To configure a bogus source IP address detection rule, follow these steps:

Step 1 Choose **Configuration > Bogus Source IP Detection**.

Figure 5-105 Bogus source IP address detection rules

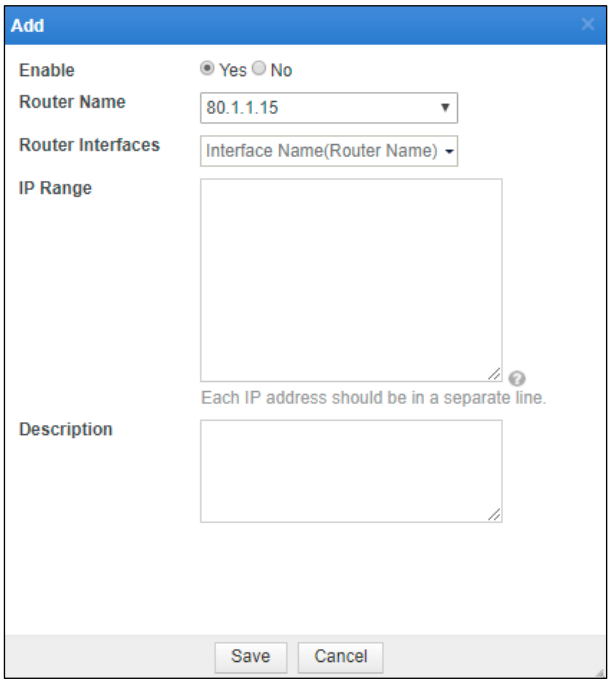


You can click to delete a rule or to edit a rule.

Step 2 Create a bogus source IP address detection rule.

Click **Add** in the upper-right corner of the page to create a bogus source IP address detection rule.

Figure 5-106 Creating a bogus source IP address detection rule



Step 3 Configure parameters.

Table 5-20 Parameters for configuring a bogus source IP address detection rule

Parameter	Description
Enable	Controls whether to enable the new rule. This rule can take effect only after it is enabled.
Router Name	Router name to be checked against this rule.
Router Interfaces	Router interface name to be checked against this rule.
IP Range	Router interfaces' IP address range to be checked against this rule.
Description	Brief information of this rule.

Step 4 After completing the configuration, click **Save** to save the settings.

----End

5.7 NTI

NTA can collaborate with NSFOCUS Threat Intelligence center (NTI). When an alert is generated, users can search for associated information available on NTI to learn details about the attack source, such as the geographical information, port information, associated domain names, ASN, and security information.

Note	To use the NTI collaboration function, you must select the NTI module when creating an NTA license. After the license (whether trial or paid) expires, the NTI query function becomes unavailable. You can search for IP addresses via NTI for a maximum of 1000 times every day.

To configure the collaboration with NTI, follow these steps:

Step 1 Choose **Configuration > Threat Intelligence**.

Figure 5-107 Threat Intelligence page

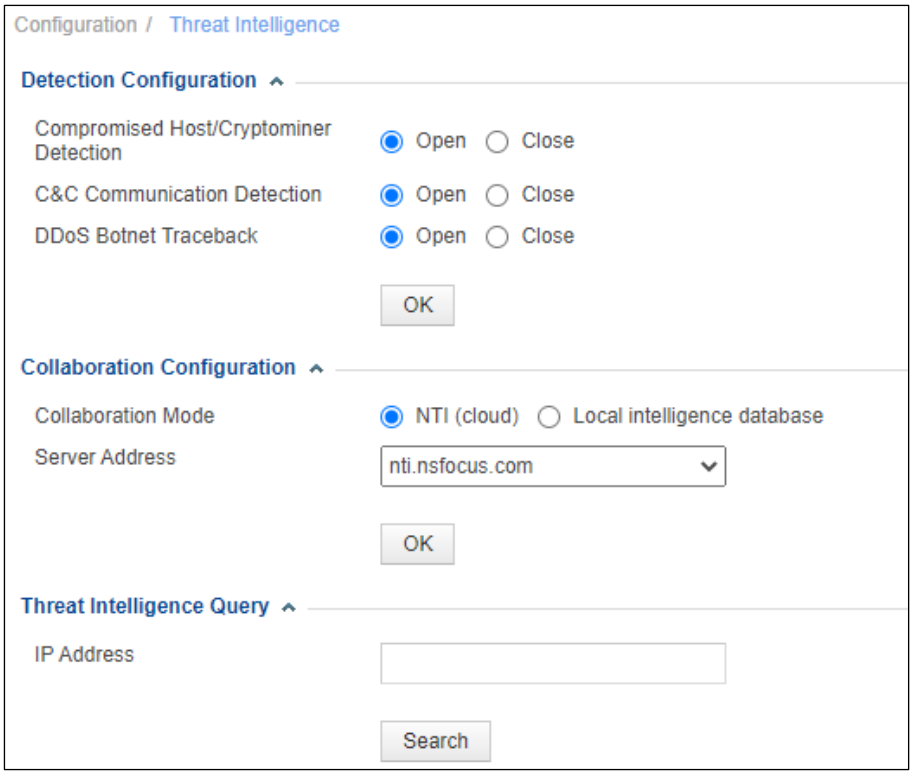


Table 5-21 describes parameters for configuring NTA to collaborate with NTI.

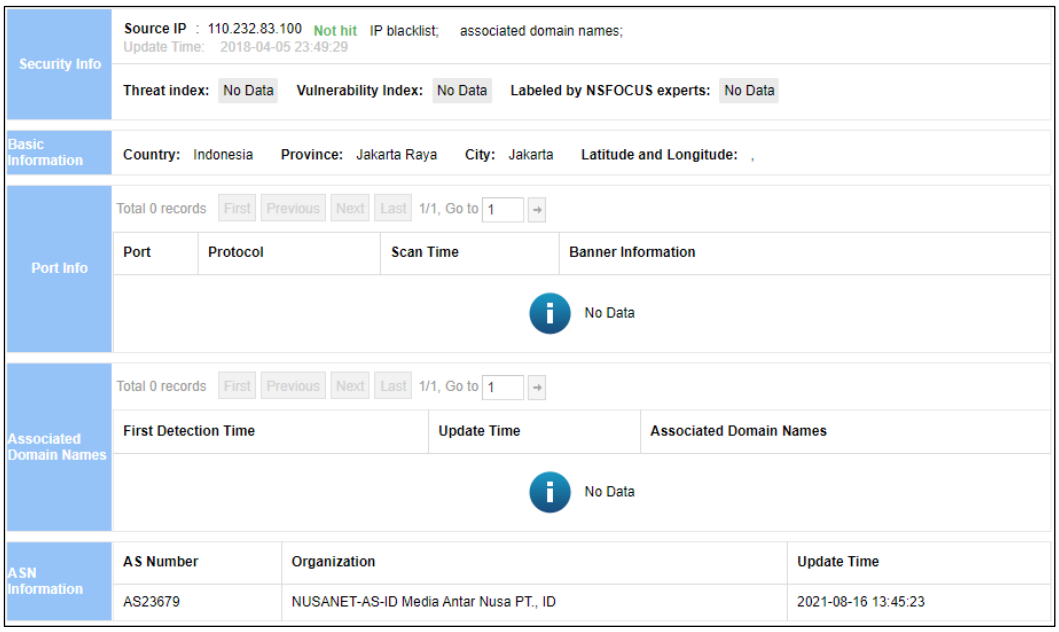
Table 5-21 Parameters for configuring NTA to collaborate with NTI

Parameter	Description
Compromised Host/Cryptominer Detection	Controls whether to enable compromised host/cryptominer detection.
C&C Communication Detection	Controls whether to enable C&C communication detection.
DDoS Botnet Traceback	Controls whether to enable DDoS botnet traceback.

Parameter	Description
Collaboration Mode	Specifies an intelligence database that NTA will collaborate with, which can be either of the following: • **NTI (cloud)**: This option requires you to further configure the server address. • **Local intelligence database**: This requires no further configuration.
Server Address	Specifies the address of the NTI server, which can be chosen from the drop-down list.
IP Address	Specifies the attack source IP address to be queried. Only IPv4 addresses are supported.

Step 2 Type the IP address to be queried and click **Search**.

Figure 5-108 Threat intelligence query result



----End

5.8 Data Dictionary

The Data Dictionary module allows you to define common applications and Autonomous Systems (ASs), whose information will be intuitively displayed on the web-based manager. A data dictionary consists of either of the following:

- Application Ports
- Autonomous Systems

5.8.1 Application Ports

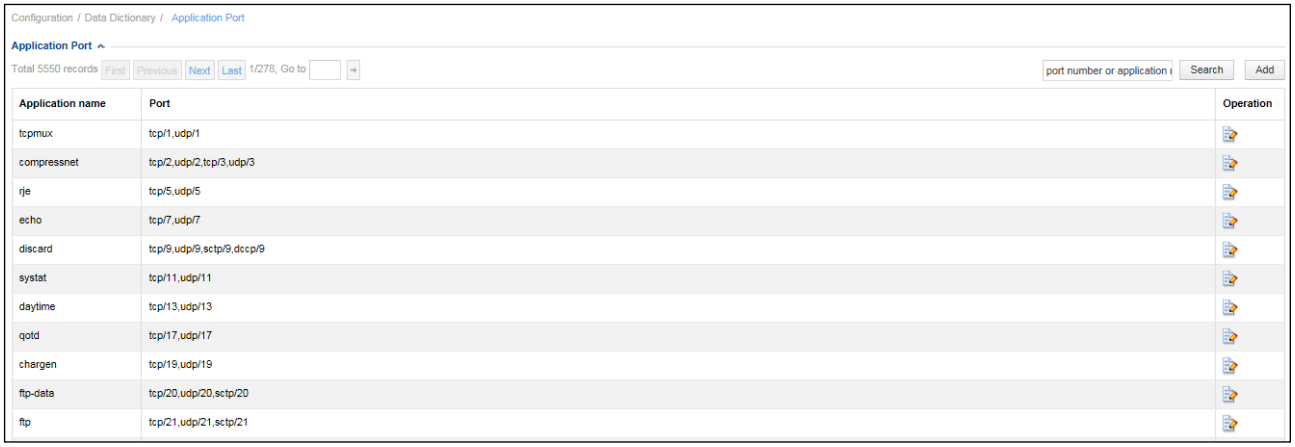
After an application is defined with both the protocol name and port number, the application name will be displayed in the **Top5 Applications Traffic** chart of a router or region under **Monitor > Routers** or **Monitor > Regions**. An application can be either of the following:

- Built-in application: can be edited, but cannot be deleted.
- Custom application: can be added, modified, and deleted.

To configure an application port, follow these steps:

Step 1 Choose **Configuration > Data Dictionary > Application Port**.

Figure 5-109 Application Port page

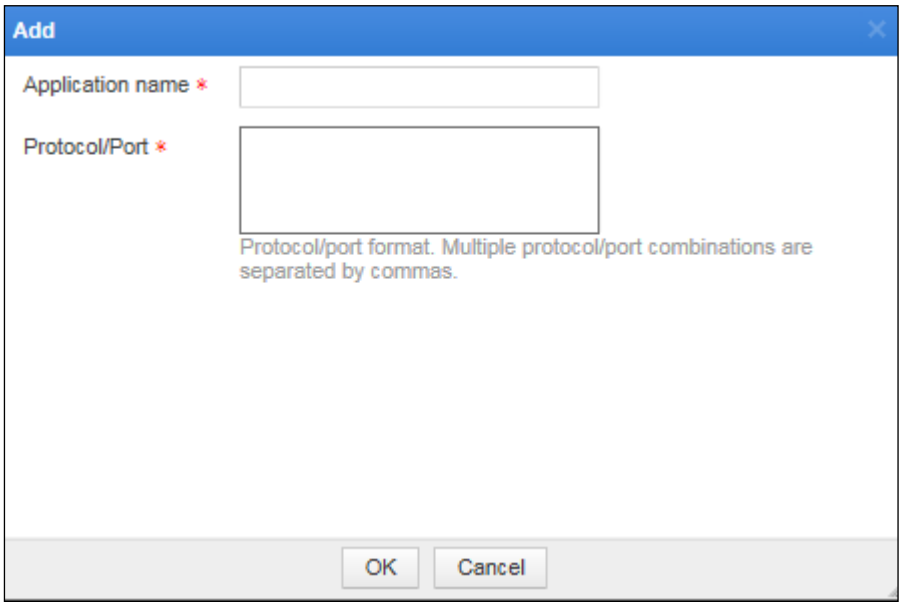


All applications are listed. For a custom application, you can click in the **Operation** column to modify its settings or click to delete this application. For a built-in application, only the icon is displayed in the **Operation** column, indicating that you can only modify its settings, but cannot delete it.

Step 2 Add an application.

Click **Add**. The dialog box for adding an application appears, as shown in Figure 5-110.

Figure 5-110 Adding an application



Enter the application name. Specify **Protocol/Port** in the format of "protocol name/port number", such as tcp/455. Multiple protocol/port pairs are separated with a comma (,), such as "tcp/455,udp/456".

After completing the configuration, click **OK**.

Step 3 Query application ports.

Click **Last** or **Next** or specify a page number to query application ports on that page. Alternatively, enter the port name and click **Search**.

----End

5.8.2 Autonomous Systems

An autonomous system (AS) is a network consisting of mutually connected routing devices that use the same routing protocol. After a common AS is defined as an organization, the organization name will be displayed in the **Top5 AS Traffic** chart of a region or router under **Monitor > Regions** or **Monitor > Routers** on the web-based manager of NTA.

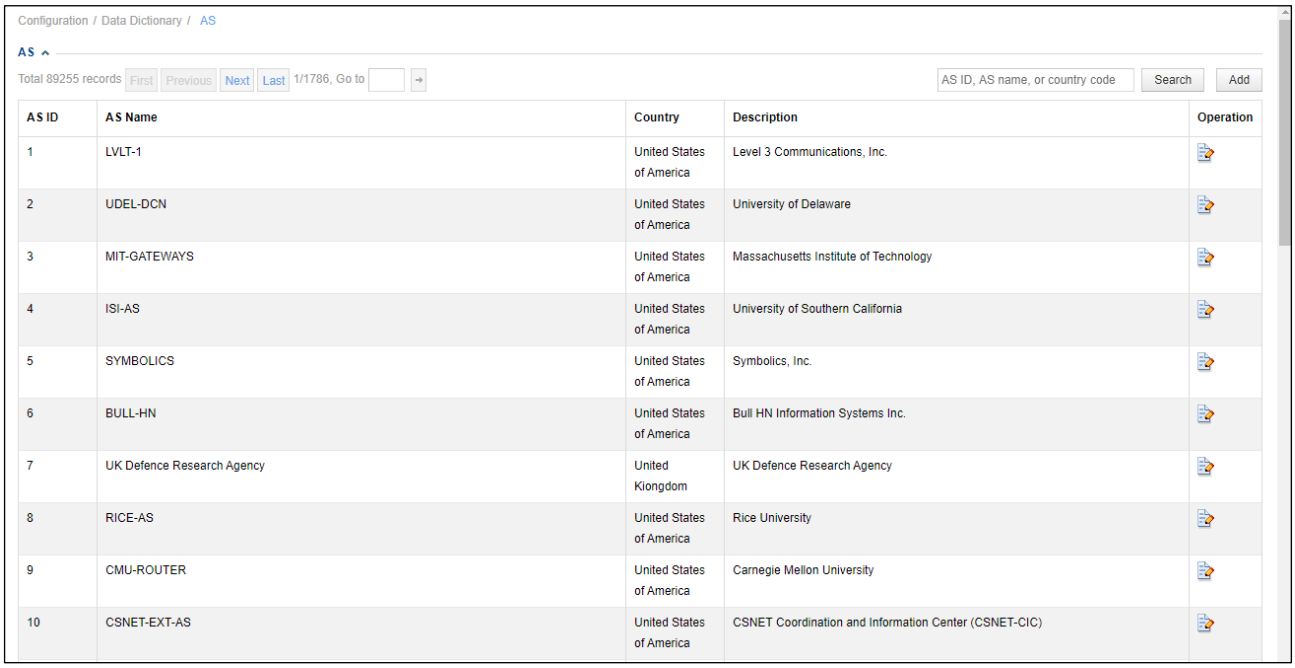
An AS can be either of the following:

- Built-in AS: can be edited, but cannot be deleted.
- Custom AS: can be added, modified, and deleted.

To configure an AS, follow these steps:

Step 1 Choose **Configuration > Data Dictionary > AS**.

Figure 5-111 AS page



AS ID	AS Name	Country	Description	Operation
1	LVLT-1	United States of America	Level 3 Communications, Inc.	
2	UDEL-DCN	United States of America	University of Delaware	
3	MIT-GATEWAYS	United States of America	Massachusetts Institute of Technology	
4	ISI-AS	United States of America	University of Southern California	
5	SYMBOLICS	United States of America	Symbolics, Inc.	
6	BULL-HN	United States of America	Bull HN Information Systems Inc.	
7	UK Defence Research Agency	United Kiongdom	UK Defence Research Agency	
8	RICE-AS	United States of America	Rice University	
9	CMU-ROUTER	United States of America	Carnegie Mellon University	
10	CSNET-EXT-AS	United States of America	CSNET Coordination and Information Center (CSNET-CIC)	

Step 2 Add an AS.

Click **Add** in the upper-right corner of the **AS** page. The dialog box for adding an AS appears, as shown in Figure 5-112.

Figure 5-112 Adding an AS

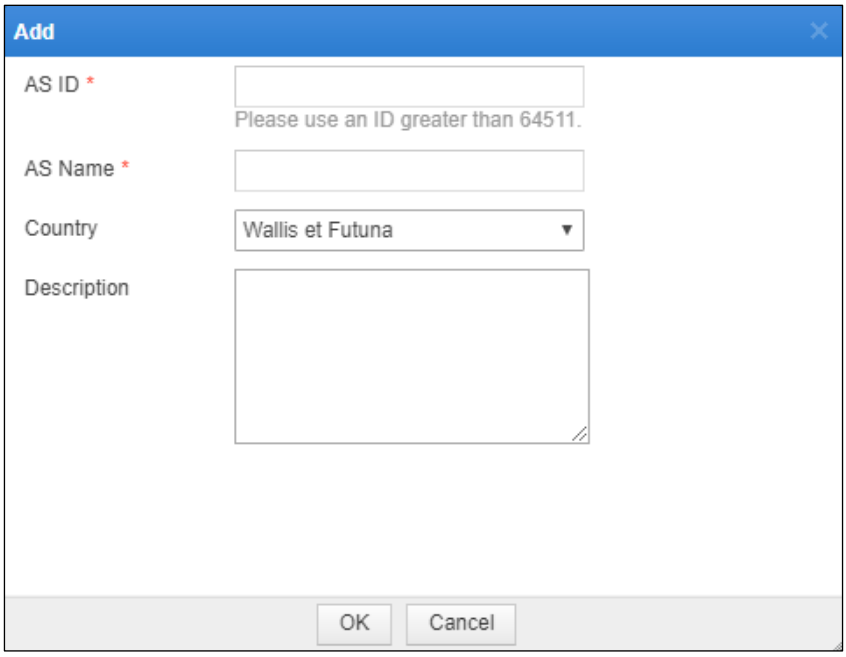


Table 5-22 describes parameters for adding an AS.

Table 5-22 Parameters for adding an AS

Parameter	Description
AS ID	Specifies the ID of the AS, which must be an integer greater than 64511. This parameter is mandatory.
AS Name	Specifies the AS name to be displayed in the **Top5 AS Traffic** chart of a region or router under **Monitor > Regions** or **Monitor > Routers**. This parameter is mandatory.
Country	Specifies the country/region where the AS is located.
Description	Briefly describes the AS such as the usage of the AS.

After completing the configuration, click **OK**.

Step 3 Modify AS settings.

Click in the **Operation** column. In the dialog box that appears, you can modify parameters except the AS ID.

Step 4 Delete an AS.

Only a custom AS can be deleted.

From the AS list, select an AS and click in the **Operation** column. The selected AS will be deleted after you click **OK** to confirm your operation.

Step 5 Query ASs.

Click **Last** or **Next** or specify a page number to query ASs on that page. Alternatively, enter the AS name and click **Search**.

----End

5.9 Bulk Configuration

This section describes how to configure regions, IP groups, and auto-learning settings in batches.

5.9.1 Bulk Configuring Regions

To configure regions in batches, follow these steps:

Step 1 Choose **Configuration > Bulk Configure > Regions**.

Figure 5-113 Page for bulk configuring regions

Step 2 Click **Add**.

A new box is displayed for you to add a region, as shown in Figure 5-114.

You can click **Add** repeatedly to add more regions.

Figure 5-114 Bulk configuring regions

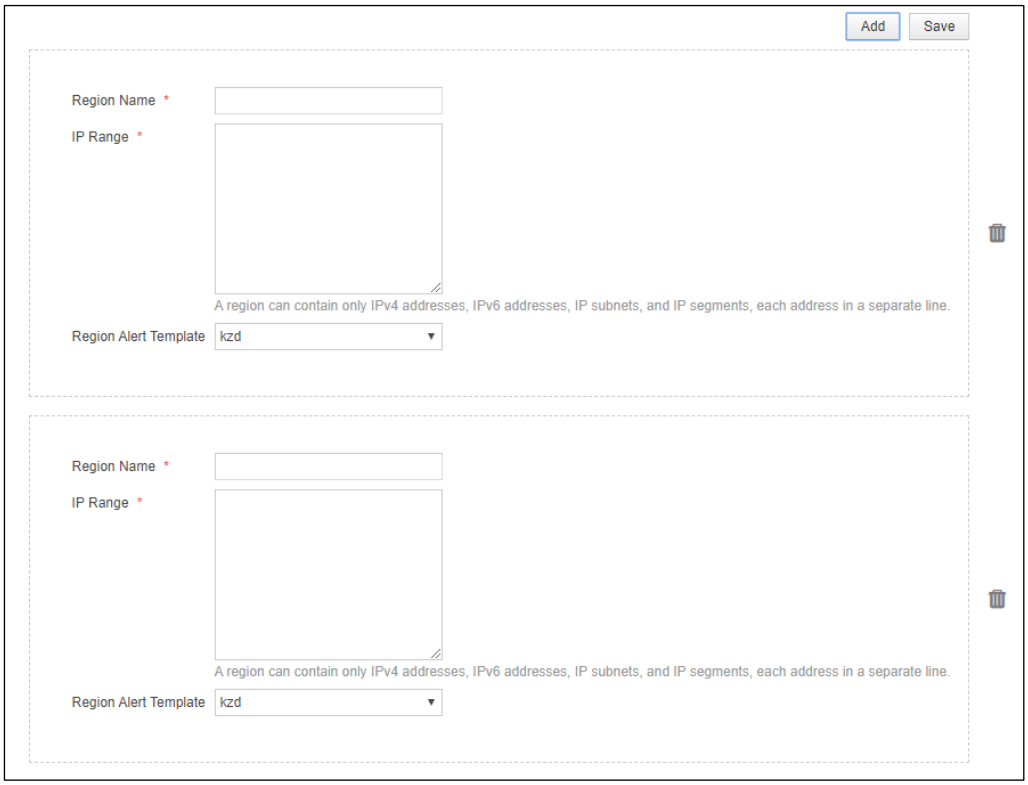


Table 5-23 describes parameters for configuring a region.

Table 5-23 Region configuration parameters

Parameter	Description
Region Name	Name of the new region. This parameter is mandatory.
IP Range	IP addresses and IP segments covered by the region. This parameter is mandatory.
Region Alert Template	Alert template for the region.

Step 3 Configure parameters for these regions one by one and then click **Save** to commit the settings.

----End

5.9.2 Bulk Configuring IP Groups

To configure IP groups in batches, follow these steps:

Step 1 Choose **Configuration > Bulk Configure > IP Groups**.

Figure 5-115 Page for bulk configuring IP groups

Step 2 Click **Add**.

A new box is displayed for you to add an IP group, as shown in Figure 5-116.

You can click **Add** repeatedly to add more IP groups.

Figure 5-116 Bulk configuring IP groups

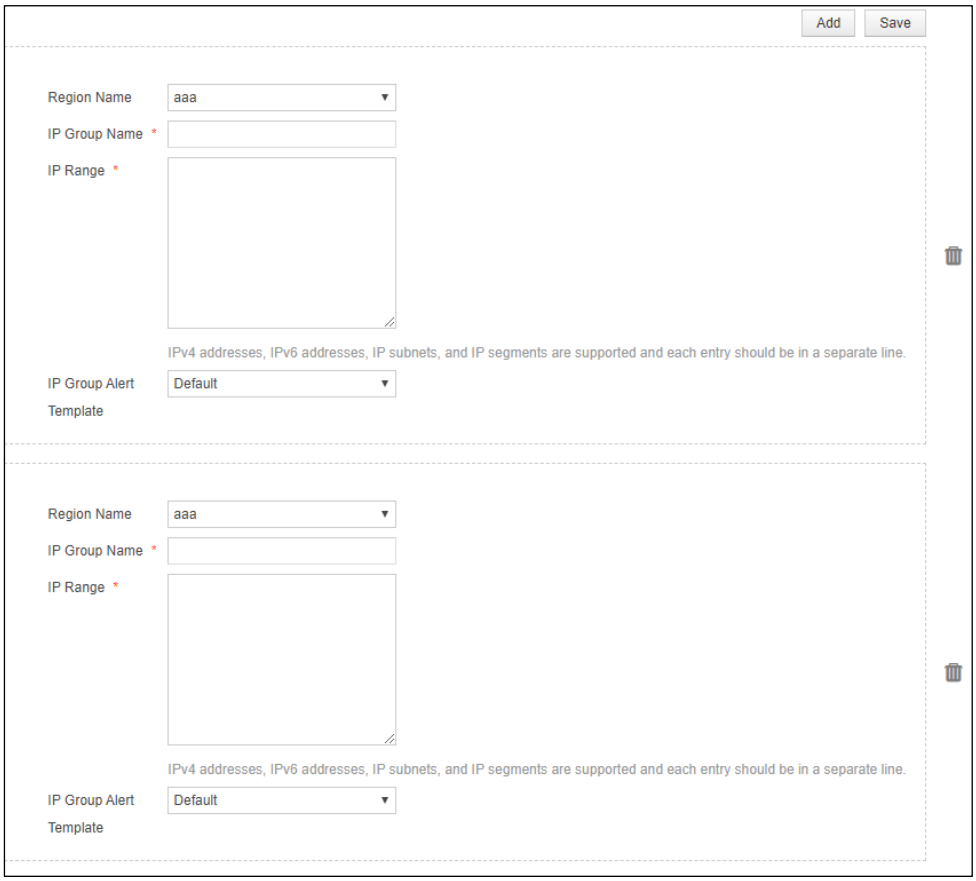


Table 5-24 describes parameters for configuring an IP group.

Table 5-24 IP group configuration parameters

Parameter	Description
Region Name	Region to which the IP group belongs.
IP Group Name	Name of the new IP group. This parameter is mandatory.
IP Range	IP addresses and IP segments covered by the IP group. This parameter is mandatory.
IP Group Name	Alert template for the IP group.

Step 3 Configure parameters for these IP groups one by one and then click **Save** to commit the settings.

----End

5.9.3 Bulk Configuring Auto-Learning

To configure auto-learning in batches for multiple regions, follow these steps:

Step 1 Choose **Configuration > Objects > Regions**.

Step 2 Click **Bulk Auto-learning** in the upper-right corner of the page.

Check boxes appear in the leftmost column.

Step 3 Select one or more regions and click **Bulk Auto-learning** again.

A dialog box appears, as shown in Figure 5-45.

Step 4 Configure parameters.

For the description of parameters, see Table 5-14.

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

Then NTA begins to automatically learn traffic of these regions.

----End

6 Log Management

This chapter describes how to view and manage logs generated by NTA, containing the following sections:

Section	Description
Log Query	Describes how to set query conditions to find desired logs.
Log Parameters	Describes detailed information about log parameters.

6.1 Log Query

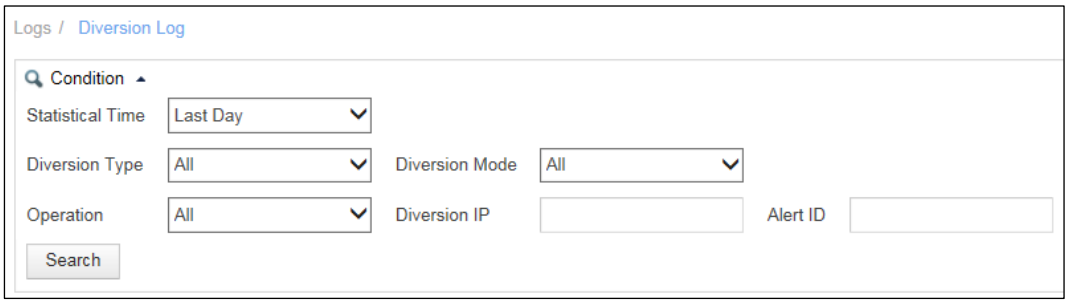
By viewing various logs, you can analyze events that triggered policy-based protection and then take immediate measures to ensure network security.

The query procedure is the same for all types of logs. To search for logs (for example, diversion logs), follow these steps:

Step 1 Open the log query page.

For example, Choose **Logs** > **Diversion Log**. The **Diversion Log** page appears, as shown in Figure 6-1.

Figure 6-1 Diversion Log page



Step 2 Set query parameters.

You can set one or multiple query parameters, which vary with log types. For details about query parameters for diversion logs, see Table 6-1. For details about query parameters for audit logs, see Table 6-2. For details about query parameters for running logs, see Table 6-3.

The **Statistical Time** parameter is available for all logs, which indicates the period during which logs are generated. It has the following values:

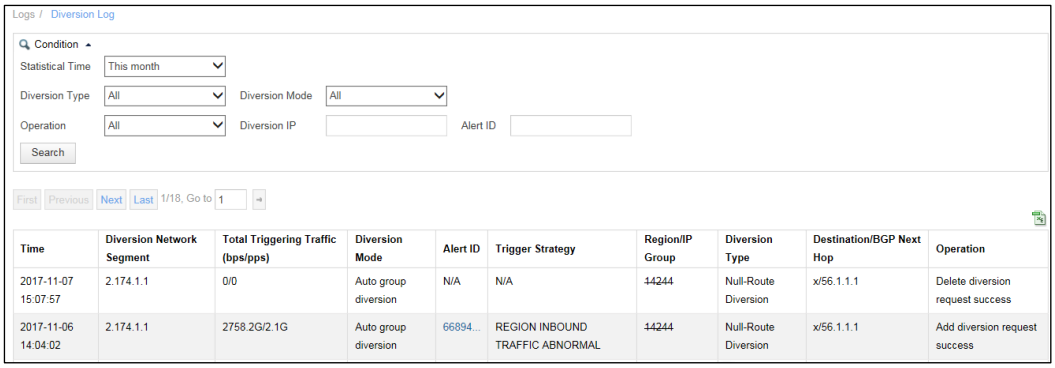
- **Last Day**: indicates the duration from current time of the previous day to the current time. This is the default value.
- **Yesterday**: indicates the duration from 00:00:00 to 23:59 yesterday.
- **This week**: indicates the duration from 00:01 on Monday to the current time.
- **This month**: indicates the time period from 00:01 on the first day of the month to current time.
- **Custom**: indicates a duration that you customize.

For other parameters, if you do not specified them, they are left at default settings, which can be **All** or empty.

Step 3 Click **Search**.

The information about logs meeting the conditions is displayed, as shown in Figure 6-2.

Figure 6-2 Search result



Step 4 Click in the upper-right corner to export all listed logs to a local disk drive.

In the dialog box that appears, you can choose to open the file or save it to a local disk drive, and then click **OK**.

Note	If there are more than 10000 logs, log export will fail, and the system displays an error message.

----End

6.2 Log Parameters

This section describes details about log parameters. Logs fall into four categories:

- Diversion Log

- Audit Log
- Running Log
- FlowSpec Diversion Log

6.2.1 Diversion Log

The diversion log provides information about all events of traffic diversion by NSFOCUS ADS or a third-party protection device at the request of NTA.

Table 6-1 describes parameters of the diversion log.

Table 6-1 Parameters of the diversion log

Parameter	Description
Time	Indicates the period during which logs are generated.
Diversion Network Segment	Indicates the network segment from which traffic is diverted.
Total Triggering Traffic (bbs/pps)	Indicates the traffic triggering the diversion.
Diversion Mode	Indicates the diversion mode, which can be one of the following: • **Auto IP Diversion**: indicates that traffic to a specific IP address is diverted when DDoS attack traffic is detected. • **Auto Group Diversion**: indicates that traffic to an IP group is diverted due to traffic anomaly. • **Manual IP diversion**: indicates that traffic to an IP address or IP segment is diverted when hitting a manual traffic diversion rule or when you revoke an auto IP diversion route. • **Manual Group Diversion**: indicates that traffic to an IP group is diverted when traffic anomaly occurs or when you revoke diversion. • **Manual FlowSpec Diversion**: indicates that FlowSpec traffic is diverted because of its anomaly, or such diversion is manually revoked.
Alert ID	Indicates the ID of the alert triggering the diversion event. Clicking this alert ID, you can view alert details.
Trigger Strategy	Indicates the name of policy which triggers diversion.
Region/IP Group	Indicates the region or IP group that the diverted network segment belongs to.
Diversion Type	Indicates the diversion type, which can be one of the following: • **ADS Diversion**: indicates that traffic is diverted to ADS devices. • **Null-Router Diversion**: indicates that traffic is diverted to a null route IP address using the Border Gateway Protocol (BGP). In this case, BGP next-hop IP address is the null route IP address. • **BGP Diversion**: indicates that traffic is diverted to a protection device using BGP. In this case, the IP address of the protection device is the BGP next-hop IP address.
Destination/BGP Next-Hop	Indicates the destination of traffic diversion, which can be the ADS device or BGP next-hop IP address

Parameter	Description
Operation	Indicates the operation, which can be one of the following: • **Add diversion request success**: indicates that NTA's diversion request is successfully added on a router or ADS. • **Delete diversion request success**: indicates that NTA's diversion request is successfully deleted from a router or ADS. • **Add diversion request failed**: indicates that NTA's diversion request fails to be added on a router or ADS. • **Delete diversion request failed**: indicates that NTA's diversion request fails to be deleted from a router or ADS.

6.2.2 Audit Log

The audit log provides information about all configurations on NTA.

Table 6-2 describes parameters of the audit log.

Table 6-2 Parameters of the audit log

Parameter	Description
Time	Indicates when the system is configured.
Username	Indicates the user name you use for configuring NTA.
Client IP	Indicates the IP address of your computer on which you configure NTA.
Module	Indicates the modules you have configured.
Description	Indicates brief description about the event.
Operation Result	Indicates whether configuration is successful.

6.2.3 Running Log

The running log provides information about the running of NTA and BGP neighborship status changes.

Table 6-3 describes parameters of the running log.

Table 6-3 Parameters of the running log

Parameter	Description
Statistical Time	Specifies the period when running logs are generated.
Source	Indicates the module which generates running logs, which can be:

Parameter	Description
	• **All**: no limitation on the source of logs • **System Engine**: generates logs about the running of NTA. • **BGP Service**: generates logs about BGP status changes. • **FlowSpec BGP**: generates logs about the status changes of NTA's BGP neighbor during FlowSpec diversion. • **NTPD Log**: generates logs about the status changes of the NTPD service. Such logs are generated when NTA and the NTP clock source have a time difference of 1000 seconds. • **Interface Link Status**: generates interface link status logs. Such logs are generated when the status of an interface changes from up to down or from down to up.
Description	Indicates brief description about the event.

6.2.4 FlowSpec Diversion Log

The FlowSpec diversion log provides information about all events of traffic diversion via FlowSpec.

Table 6-4 describes parameters of the FlowSpec diversion log.

Table 6-4 Parameters of the FlowSpec diversion log

Parameter	Description
Name	Number of the FlowSpec diversion event.
Alert ID	ID of the alert corresponding to this event.
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If this IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Protocol	Protocol used for exchanging routing information during diversion of traffic via FlowSpec.
Source Network Segment	Source IP address of traffic diverted via FlowSpec.
Source Port	Source port of traffic diverted via FlowSpec.
Destination Network Segment	Destination IP address of traffic diverted via FlowSpec.
Destination Port	Destination port of traffic diverted via FlowSpec.
Start Time	Time when traffic diversion starts.
Packet Length	Length of diverted packets.
Action	Action taken on the diverted traffic.
FLowSpec BGP	Name of the BGP FlowSpec entry.
Diversion Mode	Mode of diversion, which can be automatic FlowSpec diversion or manual FlowSpec diversion.
Operation Type	Indicates the operation, which can be one of the following:

Parameter	Description
	• **Add diversion success**: indicates that NTA's diversion request is successfully added on a router. • **Delete diversion success**: indicates that NTA's diversion request is successfully deleted from a router. • **Add diversion failure**: indicates that NTA's diversion request fails to be added on a router. • **Delete diversion failure**: indicates that NTA's diversion request fails to be deleted from a router.
Details	Brief description of the message.

7 Report Management

This chapter describes how to generate, view, and manage immediate reports, containing the following sections:

Section	Description
Overview	Describes the NTA report system.
Traffic Report	Describes how to query traffic reports based on specific conditions.
DDoS Attack Report	Describes how to query attack reports based on specific conditions.
Bogus Source IP Report	Describes how to query bogus source IP reports based on specific conditions.
Traffic Comparison Report	Describes how to query traffic comparison reports based on specific conditions.
Email Sending Configuration	Describes how to configure scheduled sending of reports via email.

7.1 Overview

NTA has a flexible report system, which can generate various reports based on the combination of different conditions. The system provides real-time and historical reports, supporting viewing of reports for the last 1/7/30 days, by day/week/month, or for a custom period. In other words, NTA provides not only real-time monitoring reports but also historical reports for future reference and forensics. This chapter describes how to generate, view, and manage reports in real time.

The reports fall into four categories: attack reports and DDoS attack reports.

- Traffic report: indicates traffic reports that are generated as required in real time.
- DDoS attack report: indicates attack reports that are generated as required in real time.
- Bogus source IP report: indicates reports that are generated as required for a specific bogus source IP address in real time.
- Traffic comparison report: indicates reports that are generated as required for traffic comparison in real time.

7.2 Traffic Report

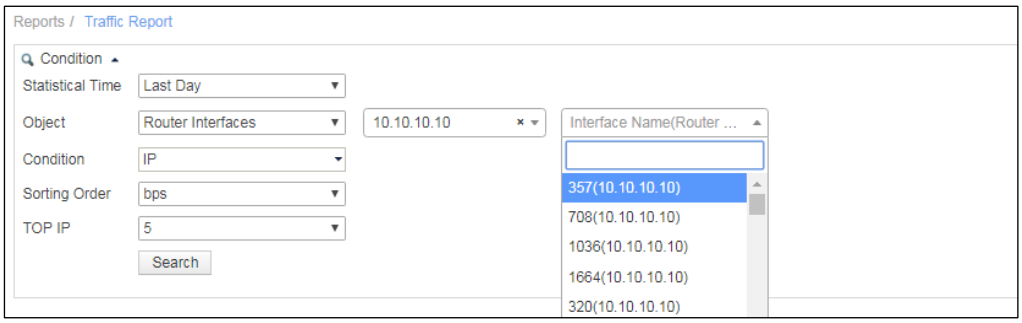
Traffic reports on various objects in different time periods can be generated as required.

To query traffic reports, follow these steps:

Step 1 Choose **Reports > Traffic Report**.

The custom report query page appears, as shown in Figure 7-1.

Figure 7-1 Traffic Report page



Step 2 Set search conditions.

Table 7-1 describes conditions for querying traffic reports.

Table 7-1 Conditions for querying traffic reports

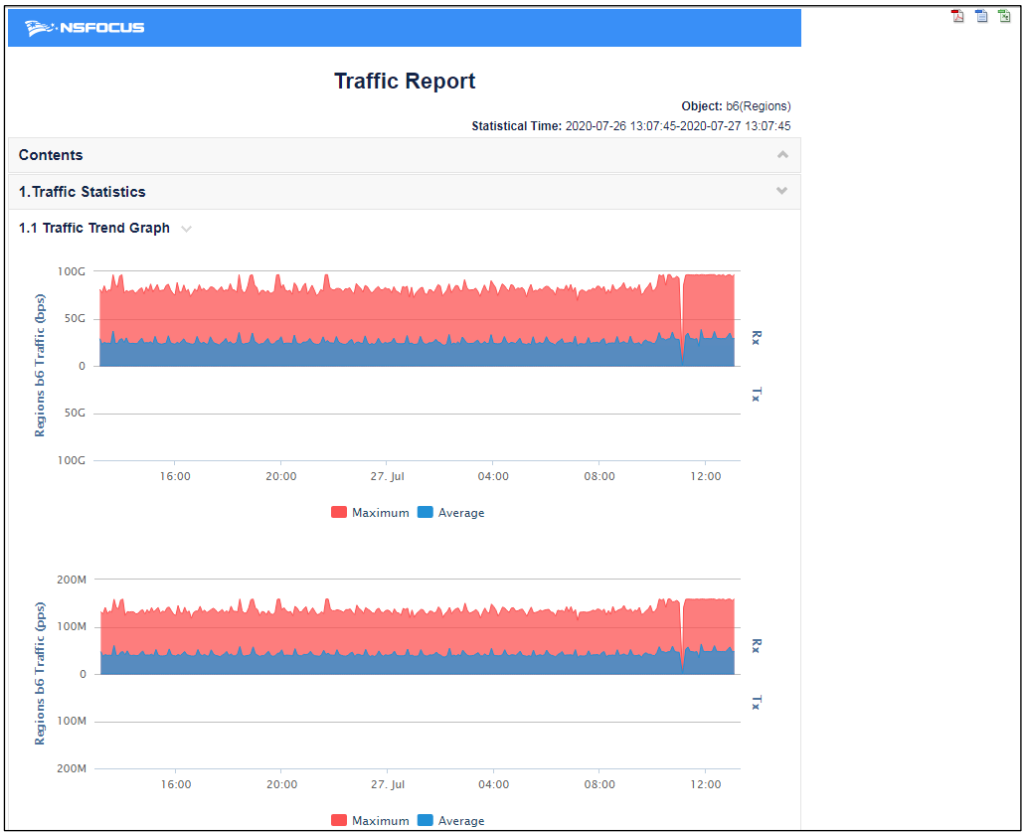
Parameter	Description
Statistical Time	Indicates the statistical period. It has the following values: • **Last Day**: indicates that the period from the current time yesterday to now. • **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: Selecting a specific date displays all traffic data on this day. If the date is the current day, the statistical period starts from 00:00 of the current day till the current time. • **By week**: Selecting a specific date displays all traffic data in the week of the specified date. If the date is a day in the current week, the statistical period starts from 00:00 on Monday of the current week to the current time. • **By month**: Selecting a specific month displays all traffic data in the month. If the current month is selected, the statistical period starts from 00:00 on the first day of the current month till the current time. • **Custom**: indicates a custom period specified by the start time and end time that you define.
Object	Indicates the statistical object. It has the following values: • **Regions**: indicates that the report covers statistics among traffic in a specified region. To select a region, click **Select**, select the desired region in the displayed dialog box, and click **OK**. Then the **Select** text box displays the name of the selected region.

Parameter	Description
	• **IP Groups**: indicates that the report covers statistics among traffic in a specified IP group. To select an IP group, click **Select**, select the desired IP group in the displayed dialog box, and click **OK**. Then the **Select** text box displays the name of the selected IP group. • **Router Interfaces**: indicates that the report covers statistics among traffic on a specified router interface. To select a router interface, click **Select**, select the desired router interface in the displayed dialog box, and click **OK**. Then the **Select** text box displays the name of the selected router interface**.** • **Router Interface Groups**: indicates that the report covers statistics among traffic in a specified router interface group. To select a router interface group, click **Select**, select the desired router interface group in the displayed dialog box, and click **OK**. Then the **Select** text box displays the name of the selected router interface group.
Condition	Indicates the dimension in which statistics are collected. It has the following values: • IP • AS • Application name • Protocol • Packet length • DSCP • Prefix • Country/Region For example, if you select **IP**, the report covers statistics about top IP addresses by traffic in the specified statistical range.
Sorting Order	Indicates the unit of the traffic rate for sorting top traffic volumes, which can be bps or pps. Note A single traffic report can display traffic data expressed in both pps and bps.
TOP	Indicates that reports on top 5, top 10, top 20, top 50, or top 100 traffic will be generated.

Step 3 Click **Search**.

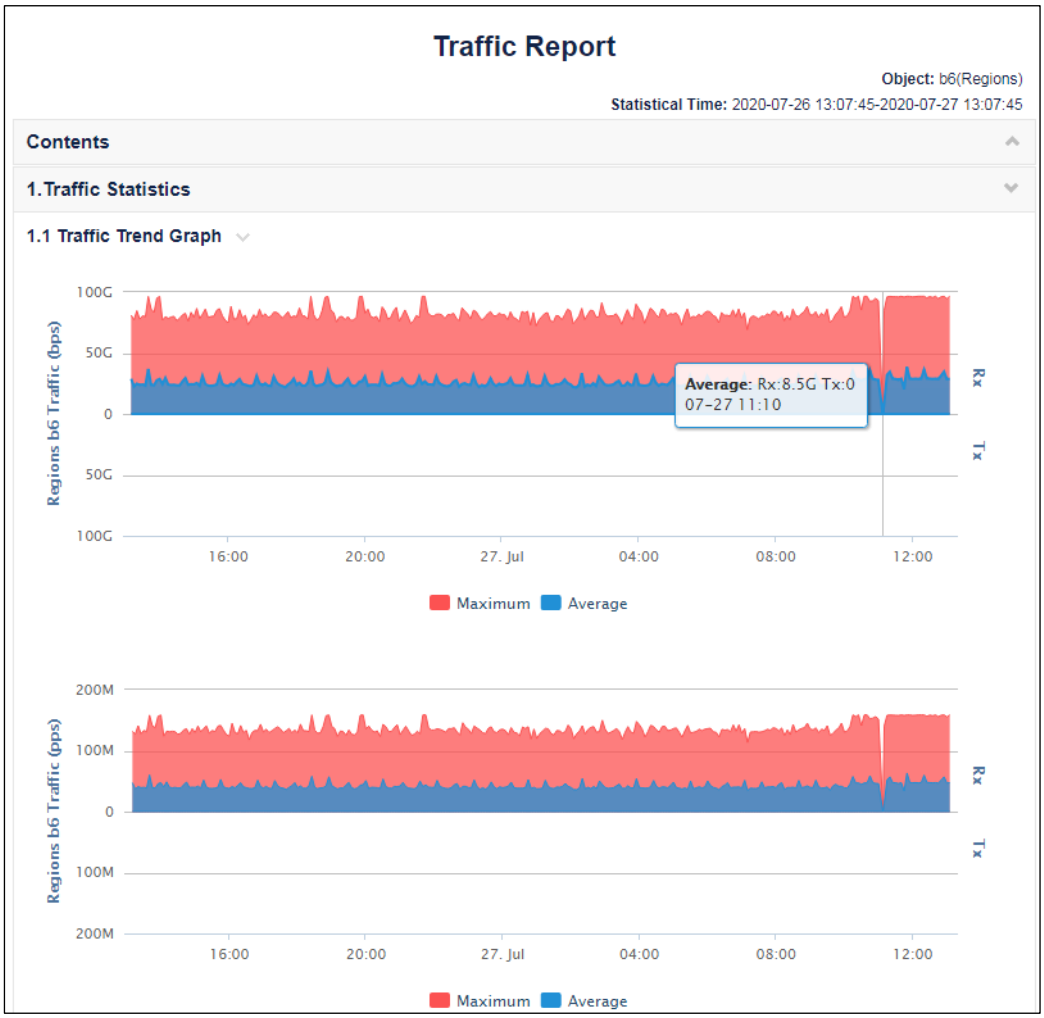
A report covering statistics meeting query conditions is displayed on a new page, as shown in Figure 7-2.

Figure 7-2 Traffic report



You can view traffic reports online. Pointing to an image on the report displays detailed statistical data, as shown in Figure 7-3.

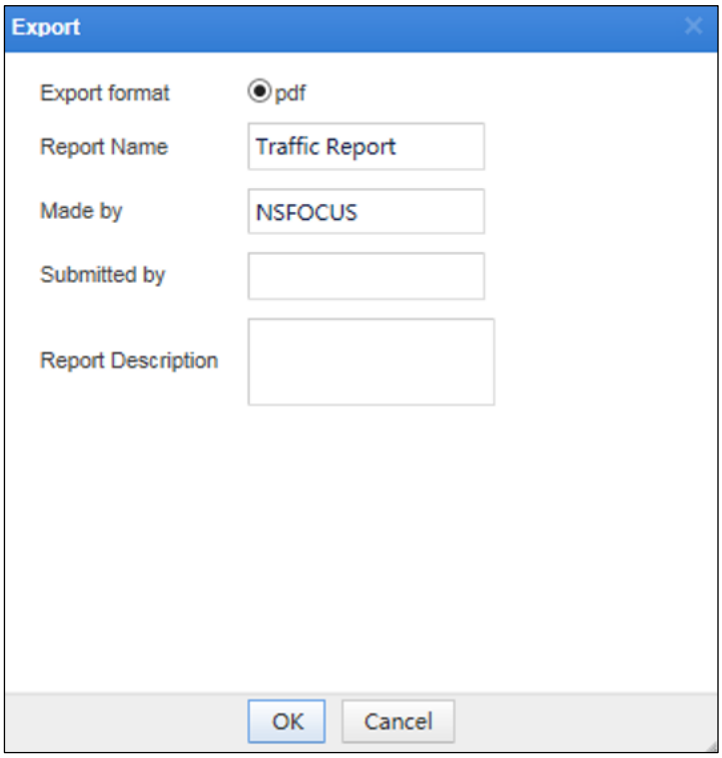
Figure 7-3 Detailed statistical data in a traffic report



Step 4 Export a report.

To export a report as an .xml or .csv file, click , , or in the upper-right corner of the page. Figure 7-4 shows the export dialog box if a user clicks .

Figure 7-4 Exporting a report



Step 5 Set export conditions.

Table 7-2 describes parameters for exporting traffic reports.

Table 7-2 Parameters for exporting traffic reports

Parameter	Description
Format	Indicates the report format, which can be.pdf, .xml, or .csv.
Report Name	Indicates the name of the report after export.
Made by	Indicates the name of the report creator, which is displayed in the report after export.
Submitted by	Indicates the name of the person who submits the report. It is displayed in the report after export.
Report Description	Indicates description of the report.

Step 6 Click **OK**.

The report is exported to a local disk drive.

----End

7.3 DDoS Attack Report

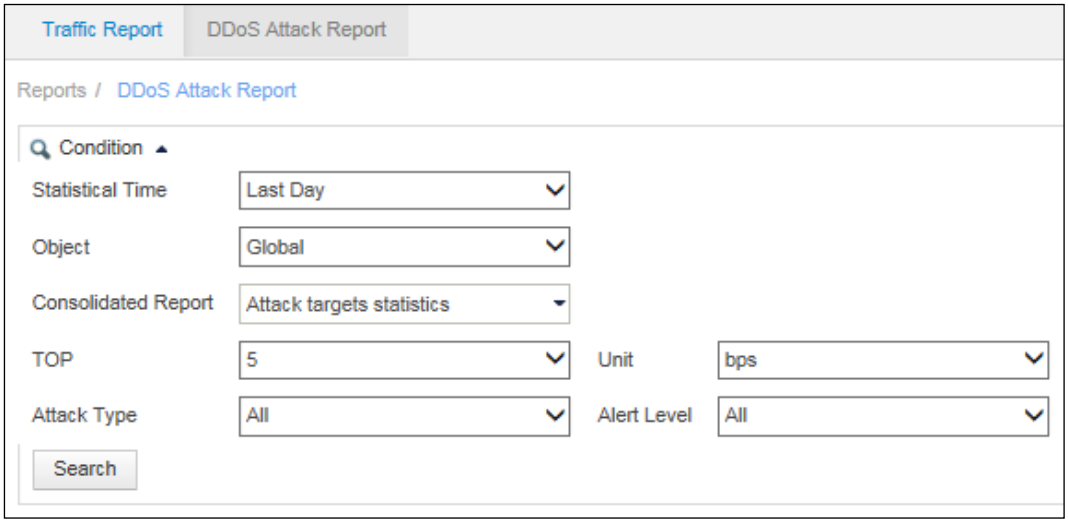
Reports about attacks against various targets in various periods can be generated based on user-defined conditions.

To query an attack report, follow these steps:

Step 1 Choose **Reports > DDoS Attack Report**.

The **DDoS Attack Report** page appears, as shown in Figure 7-5.

Figure 7-5 DDoS Attack Report page



Step 2 Set query conditions.

Table 7-3 Conditions for querying DDoS attack reports

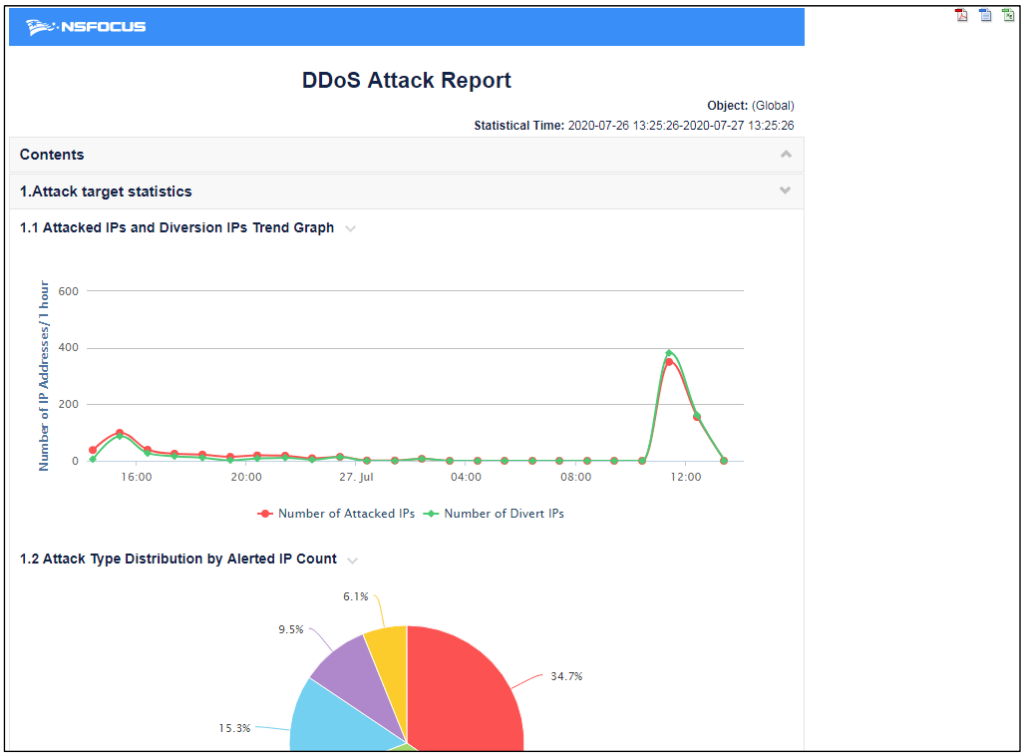
Parameter	Description
Statistical Time	Indicates the statistical period. It has the following values: • **Last Day**: indicates that the period from the current time yesterday to now. • **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: Selecting a specific date displays all traffic data on this day. If the date is the current day, the statistical period starts from 00:00 of the current day till the current time. • **By week**: Selecting a specific date displays all traffic data in the week of the specified date. If the date is a day in the current week, the statistical period starts from 00:00 on Monday of the current week to the current time. • **By month**: Selecting a specific month displays all attacks data in the month. If the month of current date is selected, the statistical period is from the first day of the month to the current time. • **Custom**: indicates a custom period specified by the start time and end time that you define.
Object	Indicates the statistical object. It has the following values:

Parameter	Description
	• **Global**: indicates that the report covers statistics on DDoS attacks against IP addresses that do not belong to any regions or IP groups. • **Regions**: indicates that the report covers statistics on DDoS attacks against IP addresses in selected regions. To select regions, click **Select**, select desired regions in the displayed dialog box, and click **OK**. The number of selected regions will be displayed in the text box. • **IP group**: indicates that the report covers statistics on DDoS attacks against IP addresses in selected IP groups. To select IP groups, click **Select**, select desired IP groups in the displayed dialog box, and click **OK**. The number of selected IP groups will be displayed in the text box. • **IP Address/IP Segment**: indicates that the report covers statistics on DDoS attacks against a specified IPv4 address or segment. You can type the desired IPv4 addresses or segments in the text box.
Consolidated Report	Indicates the types of statistical content contained in the report, including attack target statistics, attack alert statistics, attack traffic statistics, or attack source statistics.
TOP	Indicates how many top DDoS attack traffic rates will be covered by the report, which can be top 5, 10, 20, 50, or 100.
Unit	Indicates the unit in which the top DDoS attack traffic rates are expressed, which can be **bps** or **pps**.
Attack Type	Indicates the type of DDoS attacks whose statistics will be covered by the report.
Alert Level	Indicates the alert level of DDoS attacks whose statistics will be covered by the report.

Step 3 Click **Search**.

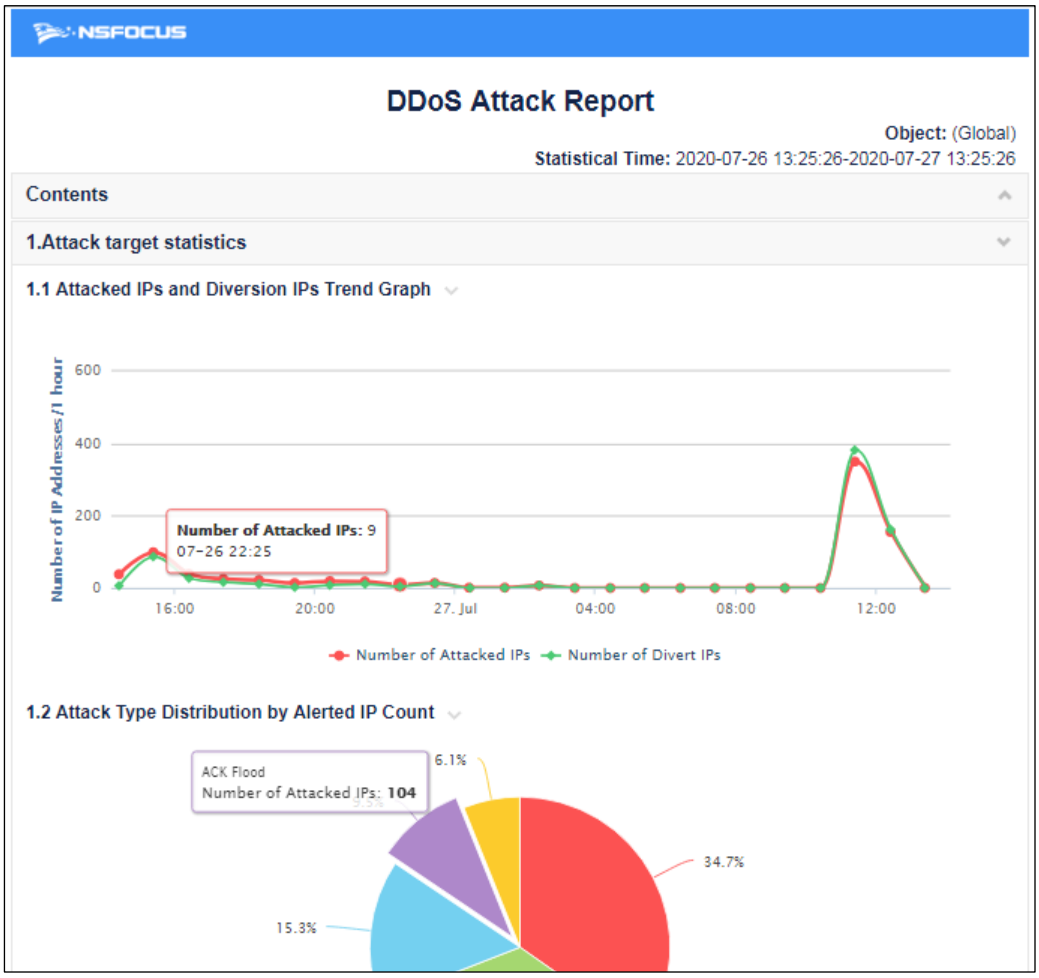
A report covering statistics meeting query conditions is displayed on a new page, as shown in Figure 7-6.

Figure 7-6 DDoS attack report



You can view traffic reports online. Pointing to an image on the report displays detailed statistical data, as shown in Figure 7-7.

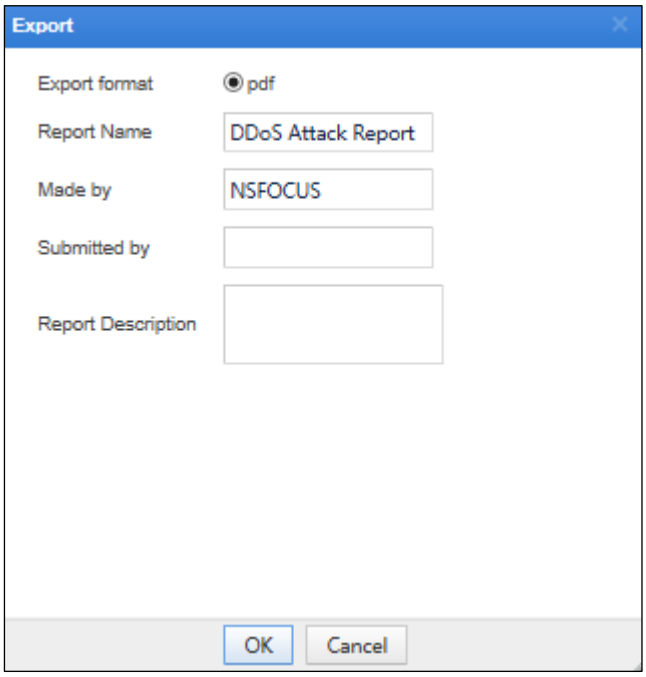
Figure 7-7 Detailed statistical data in a DDoS report



Step 4 Export a report.

To export a report as an .xml, .csv, or .pdf file, click , , or in the upper-right corner of the page. Figure 7-8 shows the report export dialog box if a user clicks .

Figure 7-8 Exporting a report



Step 5 Set export conditions.

For parameters for exporting DDoS attack reports, see Table 7-2.

Step 6 Click **OK**.

The report is exported to a local disk drive.

----End

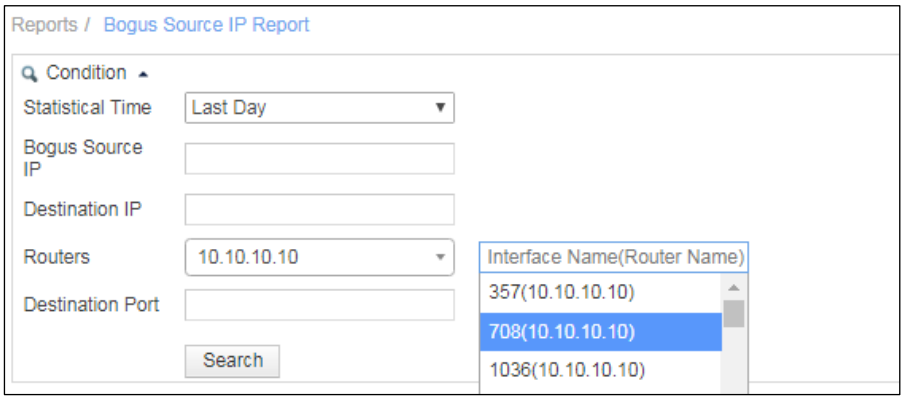
7.4 Bogus Source IP Report

Reports on bogus source IP addresses detected in a specific period can be generated based on user-defined conditions for a specified object.
To query a bogus source IP report, follow these steps:

Step 1 Choose **Reports** > **Bogus Source IP Report**.

The report query page appears, as shown in Figure 7-9.

Figure 7-9 Search area of bogus source IP reports



Step 2 Set query conditions.

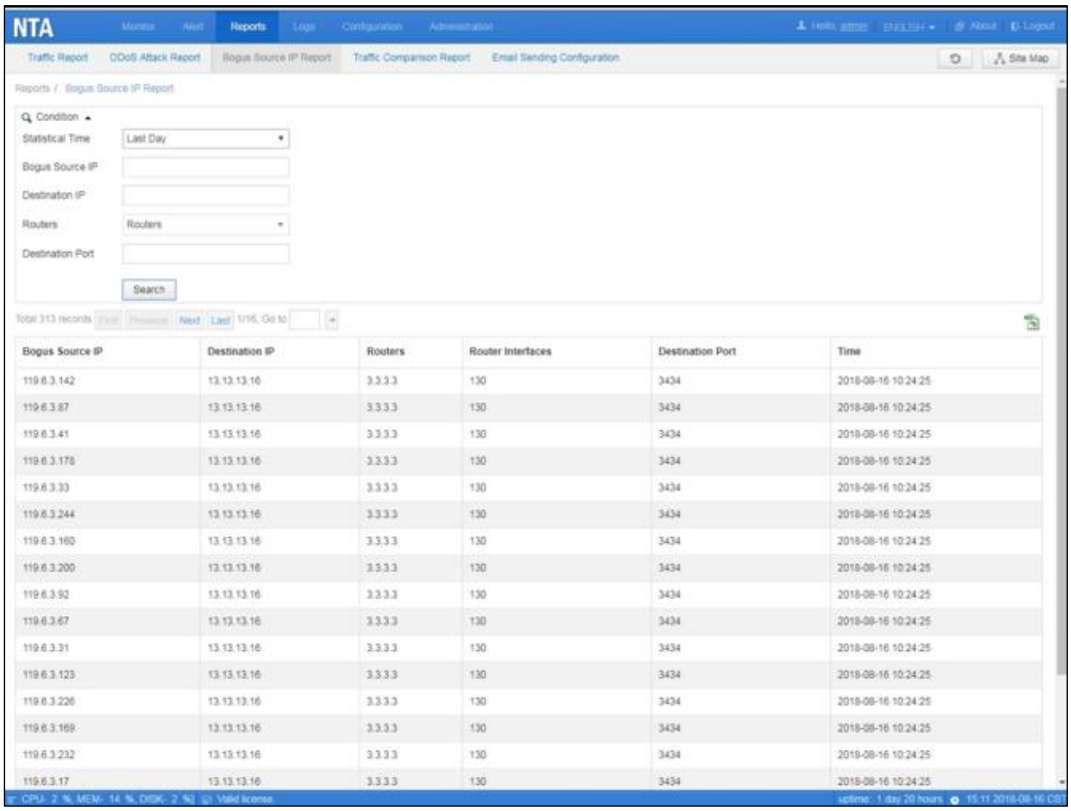
Table 7-4 Parameters for querying a bogus source IP report

Parameter	Description
Statistical Time	Indicates the statistical period. It has the following values: • **Last Day**: indicates the period from the current time yesterday to now. • **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: Selecting a date displays all traffic data of the specified bogus source IP address on this day. If you select the current date, the statistical period starts from 00:00 of the current day till the current time. • **By week**: Selecting a specific date displays all traffic data of the specified bogus source IP address in the week of the selected date. If you select the current date, the statistical period starts from 00:00 on Monday of the current week to the current time. • **By month**: Selecting a specific month displays all traffic data of the specified bogus source IP address in the month. If you select the current month, the statistical period is from the first day of the month to the current time. • **Custom**: indicates a custom period specified by the start time and end time that you define.
Bogus Source IP	Bogus source IP address to be queried.
Destination IP	Destination IP address to be queried.
Routers	Router to be queried.
Destination Port	Destination port to be queried.

Step 3 Click **Search**.

A report covering statistics meeting the specified query conditions is displayed as shown in Figure 7-10.

Figure 7-10 Bogus source IP report



Step 4 Export the report.

Click to export the report as a .csv file.

a. Set export conditions.

For parameters for exporting reports, see Table 7-2.

b. Click **OK**.

The report is exported to the specified local path.

----End

7.5 Traffic Comparison Report

Traffic comparison reports can contain either of the following types of contents:

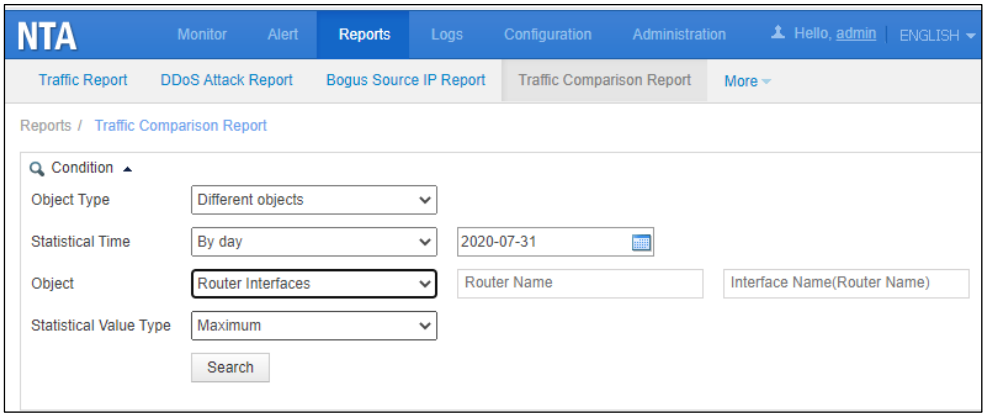
- A comparative analysis is made around traffic of the same statistical object (routers, router interfaces, router interface groups, regions, or IP groups) in different periods to discover abnormal traffic in time.
- A comparative analysis is made around traffic of different statistical objects (routers, router interfaces, router interface groups, regions, or IP groups) in the same period to discover abnormal traffic in time.

To query a traffic comparison report, follow these steps:

Step 1 Choose **Reports > Traffic Comparison Report**.

The custom report query page appears, as shown in Figure 7-11.

Figure 7-11 Search area of traffic comparison reports



Step 2 Set query conditions.

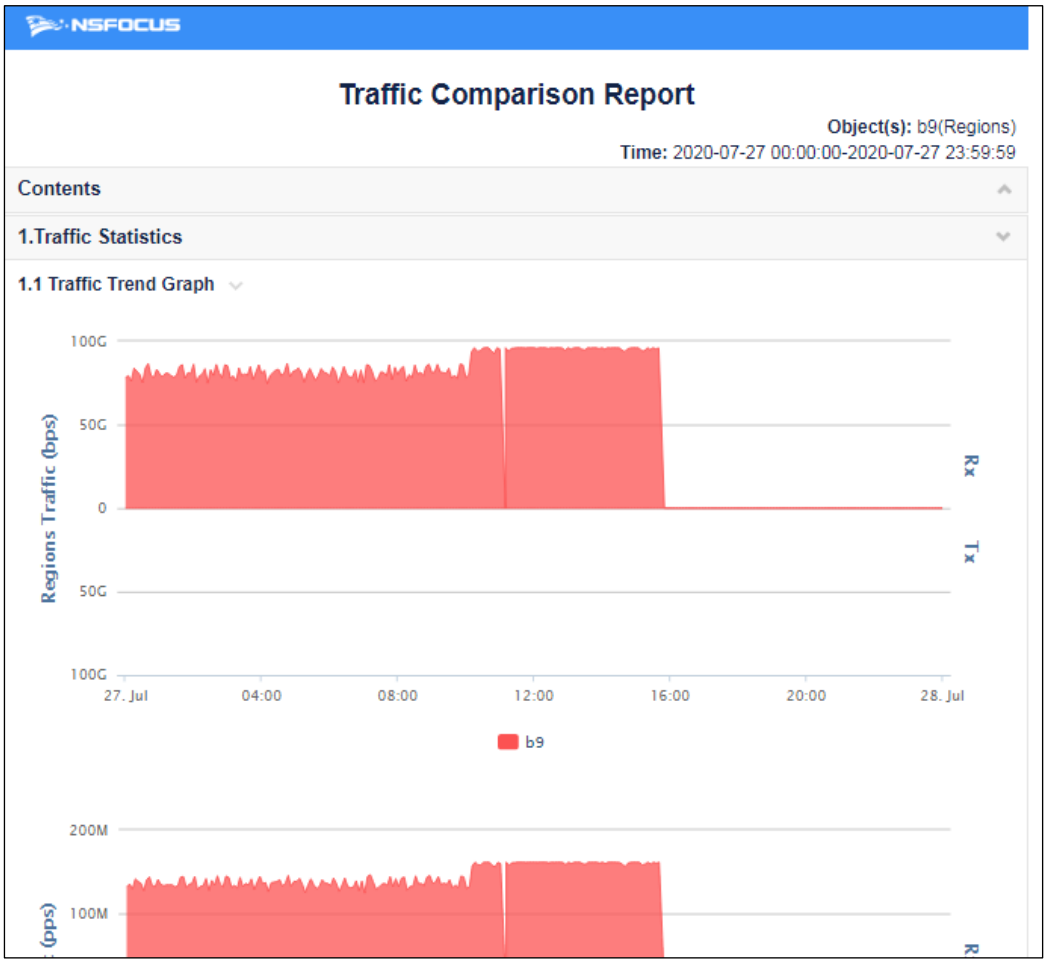
Table 7-5 Parameters for querying a traffic comparison report

Parameter	Description
Object Type	Specifies whose traffic will be compared, the same object or different objects.
Statistical Time	Indicates the statistical period. It has the following values: • **Last Day**: indicates the period from the current time yesterday to now. • **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: Selecting a specific date displays all traffic data of the statistical object on this day. If the date is the current day, the statistical period starts from 00:00 of the current day till the current time. • **By week**: Selecting a specific date displays all traffic data of the statistical object in the week of the specified date. If the date is a day in the current week, the statistical period starts from 00:00 on Monday of the current week to the current time. · **By month**: Selecting a specific month displays all traffic data of the statistical object in the month. If the month of current date is selected, the statistical period is from the first day of the month to the current time. • **Custom**: indicates a custom period specified by the start time and end time that you define.
Statistical object	Statistical object.
Statistics Value Type	Maximum value or average value for statistics.

Step 3 Click **Search**.

A report covering statistics meeting the specified query conditions is displayed on a new page. For example, a report for comparing traffic data of the same router is displayed in Figure 7-12.

Figure 7-12 Report for comparing traffic data of the same router



Step 4 Export the report.

To export a report as an .xml, .csv, or .pdf file, click , , or in the upper-right corner of the page.

a. Set export conditions.

For parameters for exporting reports, see Table 7-2.

b. Click **OK**.

The report is exported to the specified local path.

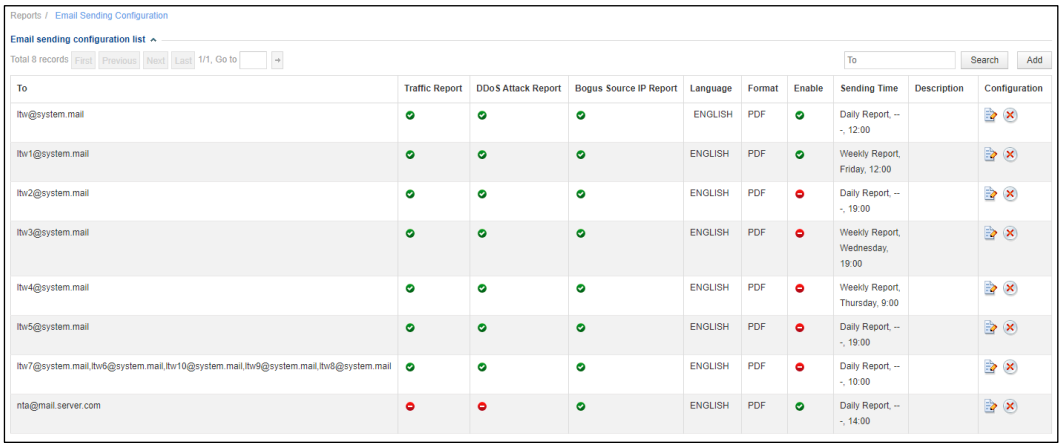
----End

7.6 Email Sending Configuration

You can configure email sending settings to send reports to a designated email address. To configure email sending settings, follow these steps:

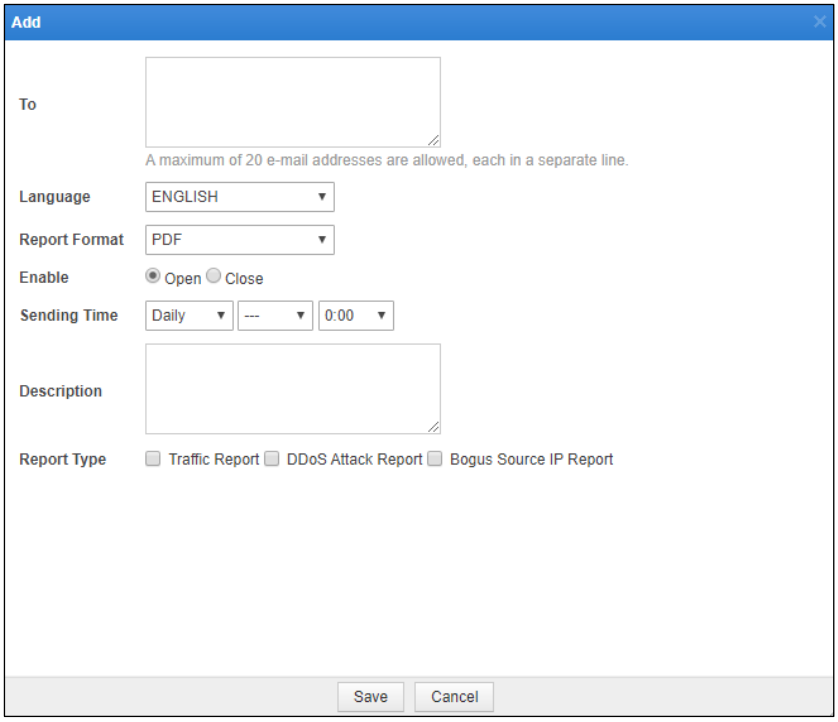
Step 1 Choose **Reports > Email Sending Configuration**.

Figure 7-13 Email sending configuration



Step 2 Click **Add** to the upper right of the list to create an email sending rule.

Figure 7-14 Creating an email sending rule



Step 3 Specify one or more email addresses that receive reports and set report sending and filtering conditions.

Step 4 After completing the configuration, click **Save** to save the settings.

----End

8 Alert Management

This chapter describes how to view and manage alert information, containing the following sections:

Section	Description
Overview	Describes how to view overall alert statistics, basic information about a specific type of alerts, and alert details.
Alert Query	Describes how to set conditions to query desired alerts.

8.1 Overview

This section describes how to view overall alert statistics, basic information about a specific type of alerts, and alert details. It involves the following:

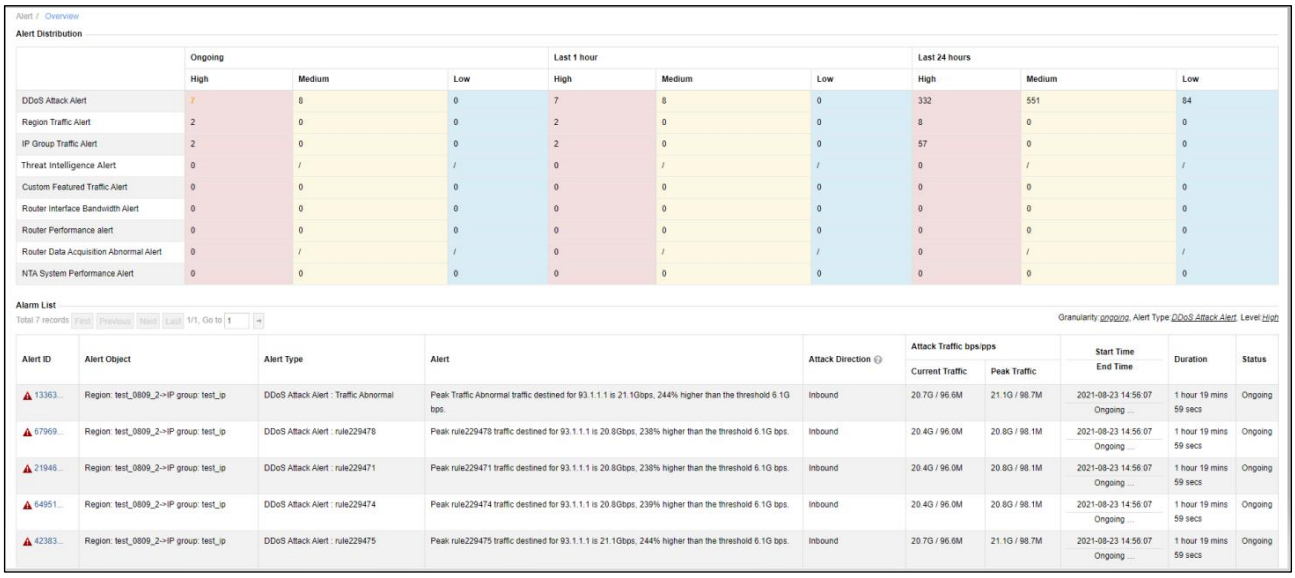
- Viewing Overall Alert Statistics: provides information about all alerts.
- Viewing Information About Specified Alerts:
  - Information about the alerted traffic
  - Top 5 information, covering source IP addresses, ports, interfaces, protocols, source ASs, source subnets, and TCP flags.

8.1.1 Viewing Overall Alert Statistics

On the **Overview** page, you can view information about all alerts detected by NTA, including ongoing alerts, alerts ending in the past hour, and alerts ending in the past 24 hours.
To view alert information, follow these steps:

Step 1 Choose **Alert > Overview**.

Figure 8-1 Overview of alerts



Alert Distribution displays statistical information about alerts of all types, including ongoing alerts, alerts ending in the past hour, and alerts ending in the past 24 hours.

Step 2 View detailed alert information.

Alarm List displays detailed information about a specific type of alerts. By default, ongoing DDoS attack alerts with a high level are displayed here, as shown in Figure 8-1.

To view brief information about alerts with a specified level, click a number in the alert distribution list. After you click it, the number turns orange. For example, high-level region traffic alerts in the last hour are displayed in **Alarm List**, as shown in Figure 8-2.

Figure 8-2 Viewing detailed alert information

Table 8-1 describes parameters in the alert list.

Table 8-1 Parameters in the alert list

Parameter	Description
Alert ID	Indicates the unique identifier of the alert.
Level	Indicates the alert level according to alert parameters configured in Global Alert Settings (see section 5.3.2 Alert Parameters). It is displayed as an icon. Pointing to the icon displays the alert level. • : indicates the low level. • : indicates the medium level. • : indicates the high level.
Alert Object	Indicates the object that triggers the alert, which can be a router, region, or IP group. If the corresponding object cannot be found, **Trigger the global default policy to generate an alert** is displayed here.
Alert Type	Indicates the type of the alert. It has the following values: • **DDoS Attack Alert**: indicates alerts triggered by DDoS attacks. The type of DDoS attacks is also displayed, like **DDoS Attack Alert: SYN FLOOD**. • **Region Traffic Alert:** indicates alerts triggered by abnormal inbound or outbound region traffic. • **IP Group Traffic Alert**: indicates alerts triggered by abnormal traffic received or sent by an IP group. • **Threat Intelligence Alert**: indicates alerts triggered by IP group assets matching the threat intelligence database. • **Router Interface Bandwidth Alert**: indicates alerts triggered by abnormal interface bandwidth usage of a router. • **Router Performance Alert**: indicates alerts triggered by abnormal CPU or memory usage of a router. • **Router Data Acquisition Abnormal Alert**: indicates alerts triggered by a router failing to collect data (i.e., failing to report flow and SNMP data to NTA). • **Custom Featured Traffic Alert**: indicates alerts triggered by traffic that contains custom attack signatures. • **NTA System Performance Alert**: indicates alerts triggered by abnormal CPU or memory usage of NTA.
Alert	Indicates details about the alert.
Attack Direction	Indicates the attack direction, which can be outbound or inbound. If the destination IP address belongs to a region or IP group, the attack direction is inbound. If the destination IP address is a global one, the attack direction is outbound. To use this function, you need to configure the IP address of the asset to be protected to belong to a region or IP group.
Current Traffic	Indicates the value of current traffic in bps or in pps. For an ended alert, it is displayed as "-/-".
Peak Traffic	Indicates the maximum traffic rate in bps or pps during the alert.
Start Time	Indicates the start time of the alert.
End Time	Indicates the end time of the alert. If the alert persists, **Ongoing** is displayed.
Duration	Indicates the duration of the alert from the start time to current time.

Parameter	Description
Status	Indicates the status of the alert, which can be **Ongoing** or **Ended**.

To view details about an alert report and download it, click an alert ID in **Alarm List**. For details, see section 8.1.2 Viewing Information About Specified Alerts.

8.1.2 Viewing Information About Specified Alerts

Choose **Alert > Overview**. In **Alarm List**, click an alert ID to view details about this alert, including:

- Basic information: includes basic alert information and traffic details.
- Top 5 information: top 5 information varies with alert types. It usually covers IP addresses, ports, interfaces, protocols, ASs, prefixes, TCP flags, packet lengths, DSCPs (Differentiated Services Code Point), and countries/regions.

8.1.2.1 Basic Information

On the **Overview** page, you can view only basic information about alerts. The **Alarm List** area presents alert information for the last 12 months and traffic trend data for the last six months.You can click an alert ID to view details about this alert.

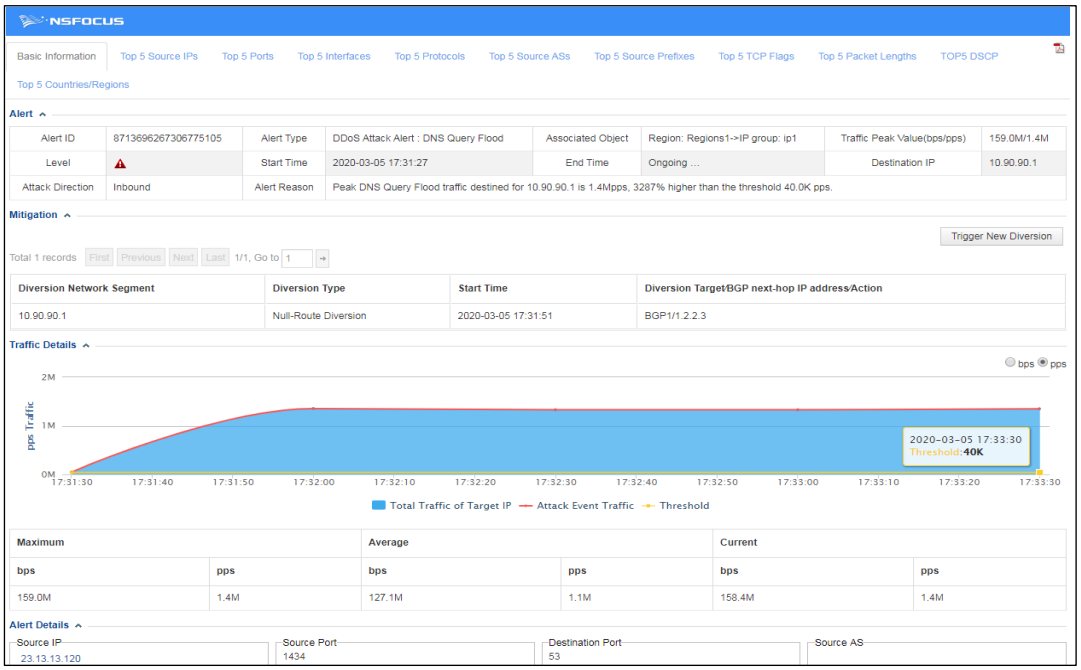
Note	You can view details only about the following types of alert by clicking their alert IDs in **Alarm List**: **DDoS Attack Alert**, **Region Traffic Alert**, **IP Group Traffic Alert**, and **Custom Featured Traffic Alert**.

To view details about alerts, follow these steps:

Step 1 Choose **Alert > Overview**, and click a specific alert ID in **Alarm List**.

A page displaying details about the alert appears, as shown in Figure 8-3.

Figure 8-3 Page displaying details about an alert



Step 2 View basic information about the alert.

Table 8-2 describes basic alert parameters.

Table 8-2 Basic alert parameters

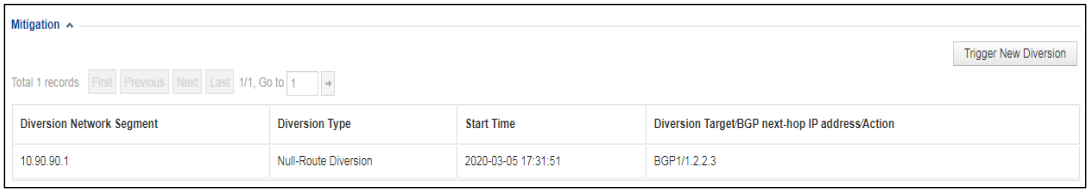
Parameter	Description
Alert ID	Indicates the unique identifier of the alert.
Alert Type	Indicates the type of the alert. If the alert is a DDoS attack alert, the specific DDoS attack type is also displayed, like **DDoS Attack Alert: SYN FLOOD**.
Associated Object	Indicates the object that triggers the alert, which can be a router, region, or IP group. If the corresponding object cannot be found, **Trigger the global default policy to generate an alert** is displayed here.
Traffic Peak Value(bps/pps)	Indicates the maximum traffic rate in bps or pps during the alert.
Level	Indicates the alert level according to alert parameters configured in Global Alert Settings (see 5.3.2 Alert Parameters). It is displayed as an icon. Pointing to the icon displays the alert level. • : indicates the low level. • : indicates the medium level. • : indicates the high level.
Start Time	Indicates the start time of the alert.
End Time	Indicates the end time of the alert. If the alert persists, **Ongoing** is displayed.
Destination IP	For a DDoS attack alert, the attacked IP address is displayed, namely, the target IP address. For a traffic anomaly alert, "-"is displayed.

Parameter	Description
Attack Direction	Indicates the attack direction, which can be outbound or inbound.
Alert Reason	Indicates detailed description about the cause of the alert.

Step 3 View the mitigation solution.

In the **Mitigation** area, you can view information about the diversion triggered by the alert, as shown in Figure 8-4.

Figure 8-4 Information about the diversion triggered by the alert

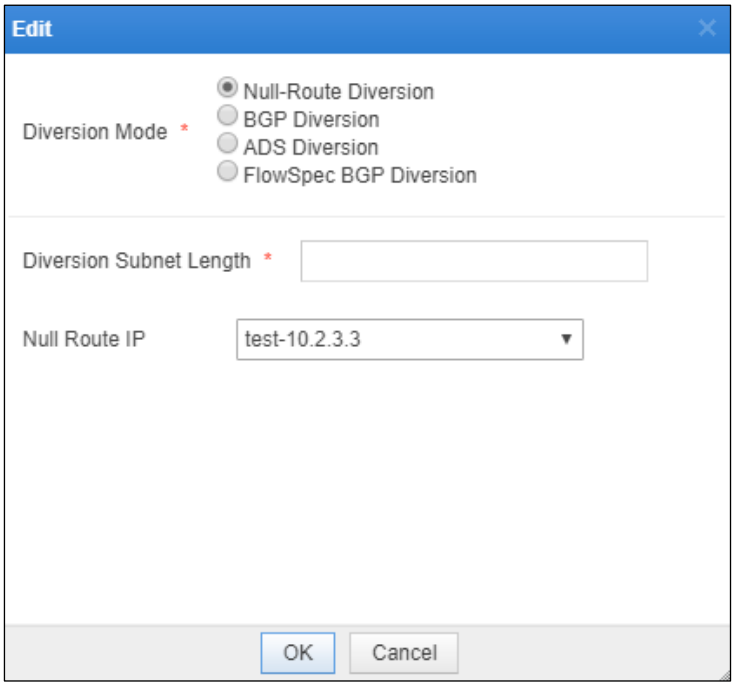


Trigger New Diversion is available only when the alert status is "Ongoing".

- If no diversion information appears, it indicates that the alert has not triggered diversion. You can click **Trigger New Diversion** to manually start diversion for the alert.

Figure 8-5 shows the dialog box for configuring manual diversion.

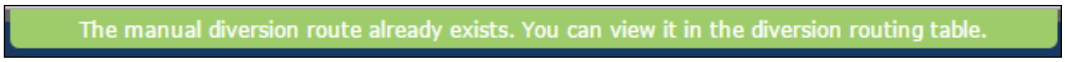
Figure 8-5 Configuring manual diversion



For the description of manual diversion, see Table 9-13. After completing the configuration, click **OK**.

- If diversion information already appears, as shown in Figure 8-4, after you click **Trigger New Diversion** and **OK**, the system displays a message shown in Figure 8-6.

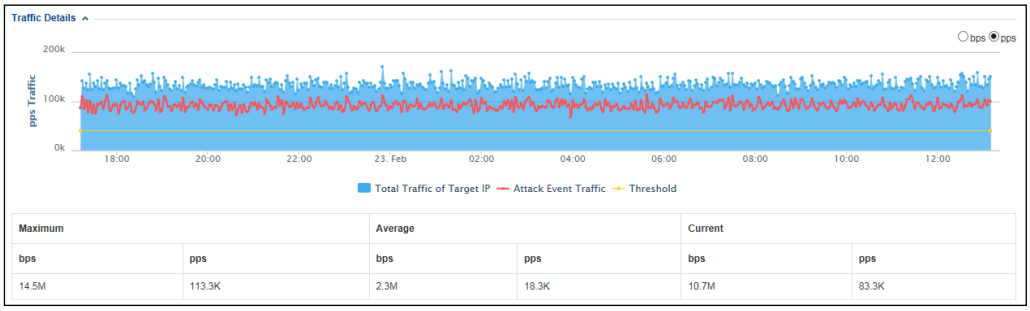
Figure 8-6 Prompt message



Step 4 View traffic details.

Information about overall traffic of the alert source (for a DDoS attack, it is the target IP address) is displayed, as shown in Figure 8-7. The duration is from the start time to end time (if the alert persists, it is from the start time to the current time).

Figure 8-7 Viewing traffic details



For DDoS attack alerts, three curves are displayed. You can view traffic in pps or bps.

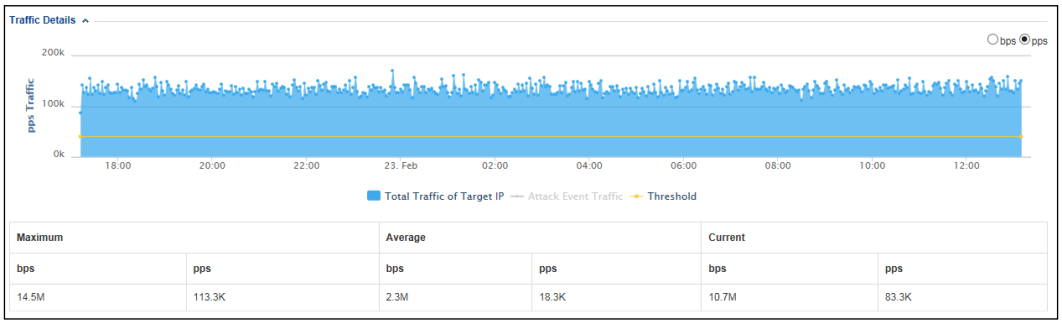
- **Total Traffic of Target IP**: indicates the trend curve of total traffic to the target IP address during the attack event which triggers the alert.
- **Attack Event Traffic**: indicates the trend curve of attack traffic to the target IP address during the attack event which triggers the alert.
- **Threshold**: indicates the trend of attack detection thresholds (in bps or pps). If a fixed detection threshold is used, the trend is displayed as a straight horizontal line; if thresholds obtained from baseline auto-learning are used, the trend curve changes over time.

You can click a curve name to remove the corresponding curve, and re-click the curve name to resume its display. As shown in Figure 8-8, only the curve for total traffic of the target IP address is displayed.

The table under the curve shows the maximum, average, and current traffic rates of the attack during the alert.

Note	Only two curves are available for traffic alert: **Attack Event Traffic** and **Threshold**.

Figure 8-8 Traffic details

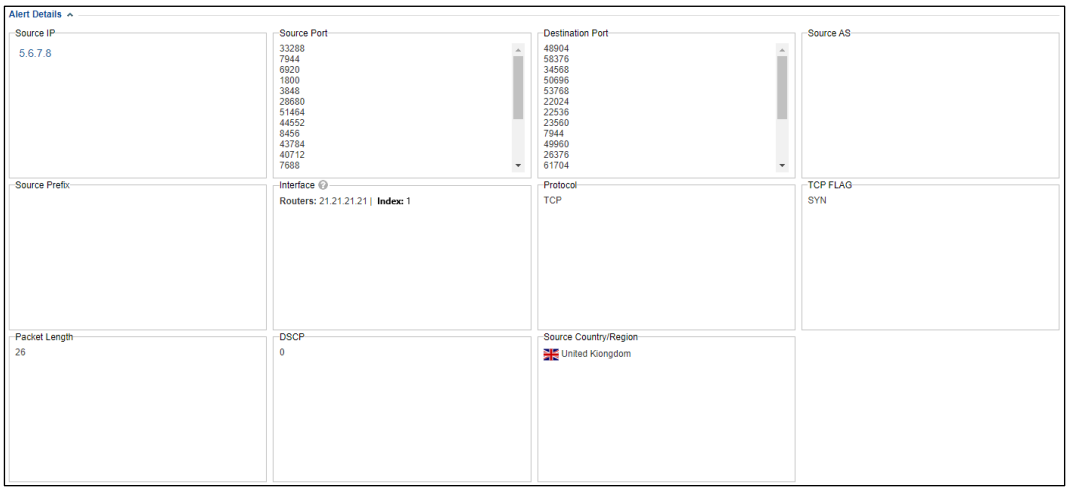


Step 5 View alert details.

Details of a DDoS attack alert event are slightly different from those of a traffic alert event.

Note	If you configure application ports or ASs in **Data Dictionary**, the corresponding object name will be displayed here, making the display more intuitive. For how to configure the data dictionary, see section 5.8 Controls whether to enable compromised host/cryptominer detection..

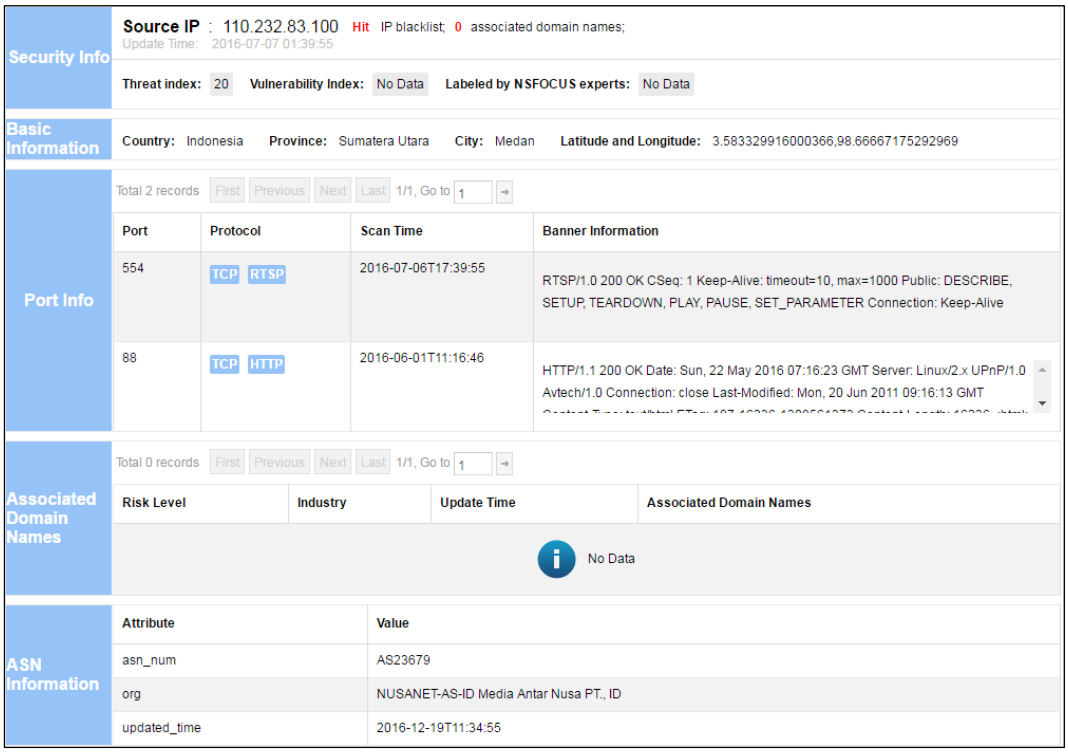
Figure 8-9 Viewing alert details



Step 6 Click an IP address in the **Source IP** text box to view its details.

Note	To view details about an IP address, you need to configure NTI collaboration in advance. For details, see section 5.7 NTI.

Figure 8-10 Viewing details about a source IP address



Step 7 In Figure 8-3, click in the upper-right corner and configure parameters in the **Export** dialog box to export an attack event report.

Figure 8-11 Exporting a report

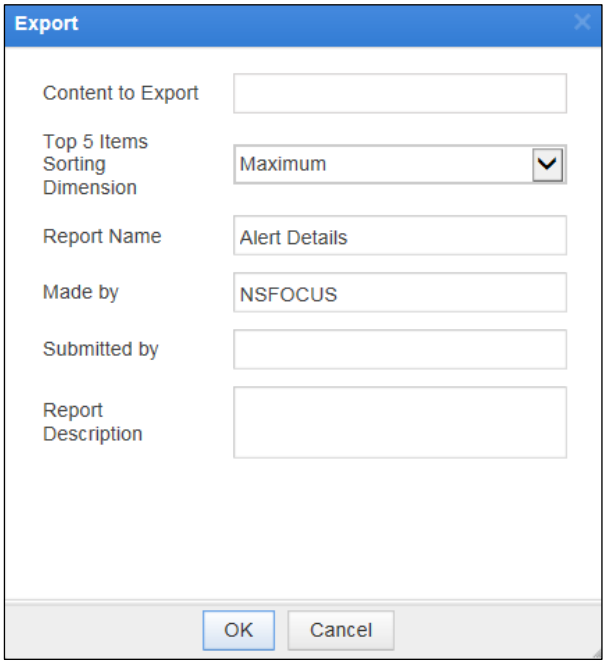


Table 8-3 Parameters for exporting a report

Parameter	Description
Content to Export	Specifies the content to export, including basic information, top 5 source IP addresses, top 5 ports, top 5 interfaces, top 5 protocols, top 5 source ASs, top 5 source subnets, and top 5 TCP flags.
Top 5 Items Sorting Dimension	Specifies how top 5 items are sorted, which can be **Maximum**, **Current**, or **Average**.
Report Name	Specifies the report name, which is **Alarm Details** by default.
Made by	Specifies the person who makes this report, which is **NSFOCUS** by default.
Submitted by	Specifies to whom this report is sent.
Report Description	Brief description of this report.

----End

8.1.2.2 Top 5 Information

Top 5 information varies with alert types. It usually covers source IP addresses, ports, interfaces, protocols, source ASs, source subnets, and TCP flags.

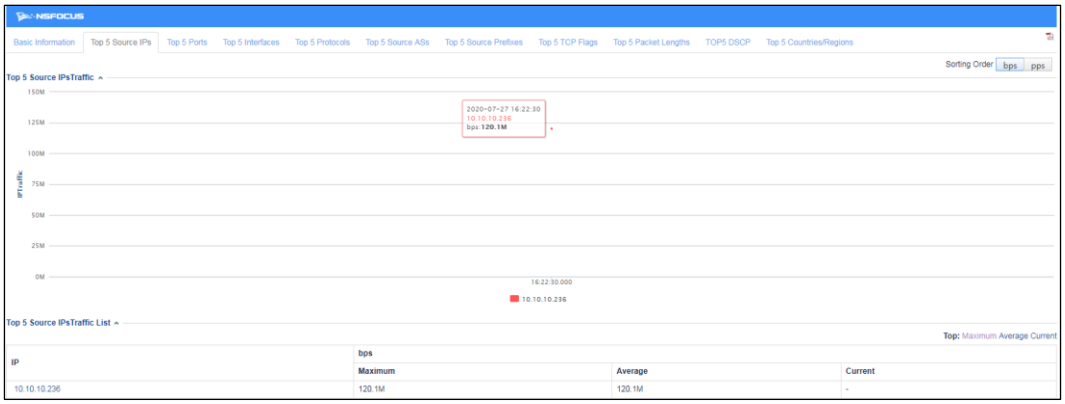
This section takes top 5 source IP addresses of DDoS attack alert as an example to introduce top 5 information.

Step 1 Choose **Alert > Overview**. In **Alarm List**, click a specific alert ID to view detailed information in a new page.

Step 2 Click the **Top 5 Source IPs** tab.

Alerts' top 5 source IP addresses are displayed. By default, top 5 source IP addresses ranked by maximum traffic rates in bps are displayed, as shown in Figure 8-12.

Figure 8-12 Top 5 source IP addresses of DDoS attack alerts



The curves show the traffic trends of the top 5 source IP addresses.

Step 3 View alerts' top 5 source IP addresses ranked by bps or pps.

By default, source IP addresses are ranked by traffic rate in bps. You can click **pps** in the upper-right corner to rank them by traffic rate in pps.

Step 4 Display all or partial curves.

By default, traffic curves of the top 5 source IP addresses are all displayed. You can click an IP address to remove its corresponding curve and re-click it to resume its display.

Step 5 (Optional) View maximum, average, and current traffic of the top 5 source IP addresses.

The table under curves lists top 5 source IP addresses with maximum, average, and current traffic rates. By default, top 5 source IP addresses ranked by maximum traffic rate are displayed. You can click **Average** or **Current** to rank the source IP addresses by average or current traffic rate in descending order.

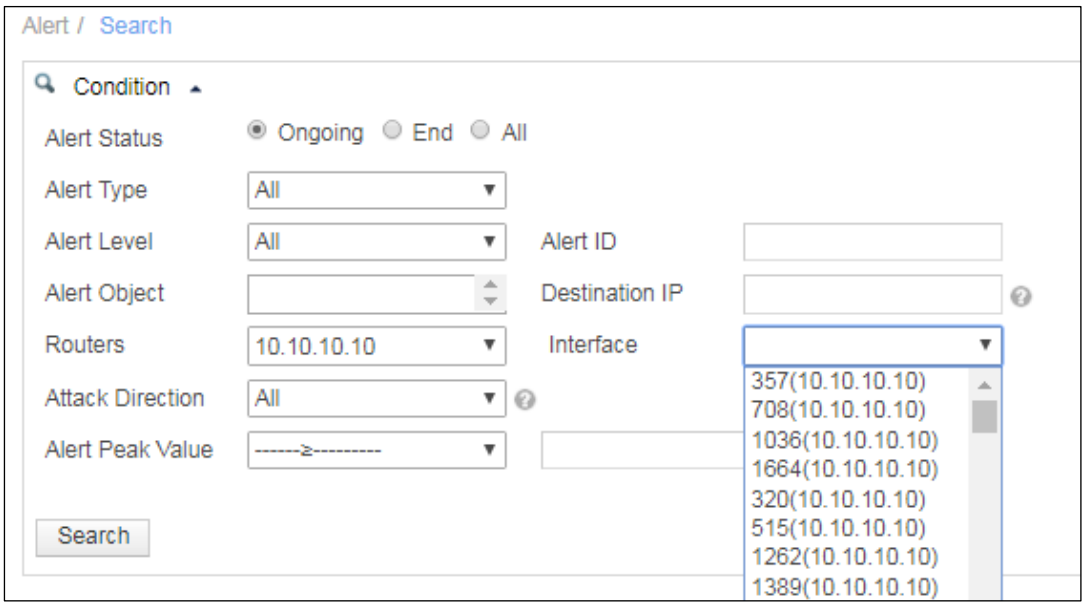
----End

8.2 Alert Query

You can set conditions to query desired alerts. To query alerts, follow these steps:

Step 1 Choose **Alert > Search**.

Figure 8-13 Searching for alerts



Step 2 Set query conditions.

Table 8-4 Parameters for querying alerts

Parameter	Description
Alert Status	Status of alerts to be queried, which can be one of the following: • **Ongoing**: indicates ongoing alerts.

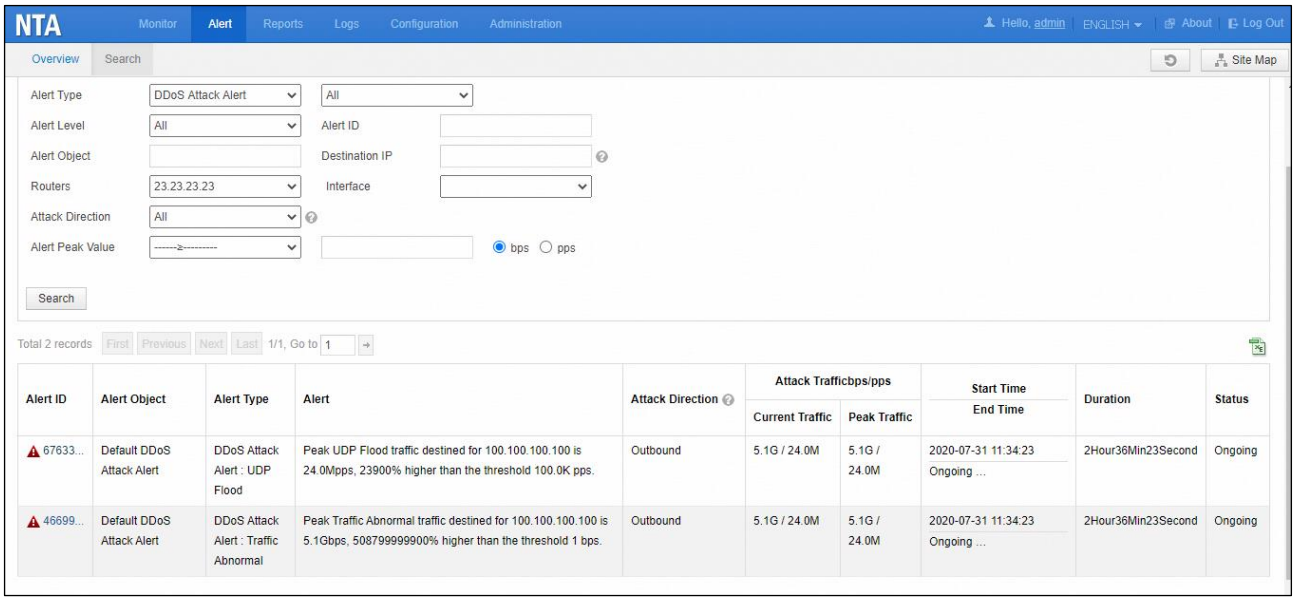
Parameter	Description
	• **End**: indicates ended alerts. • **All**: indicates all alerts
Statistical Time	This parameter is available only when **Alert Status** is set to **End** or **All**. It specifies a period, and alerts generated in this period will be queried. The value can be one of the following: • **Last Day**: indicates the duration from current time of the previous day to the current time. This is the default value. • **Last 7 days**: indicates the duration from current time 7 days before to the current time. • **Last 30 days**: indicates the duration from current time 30 days before to the current time. • **By day**: indicates a specific date (from 00:00 to 23:59 of that day). • **By week**: indicates the week to which the specified date belongs. • **By month**: indicates the month to which the specified date belongs. The duration starts from 00:00 on the first day to 23:59 on the last day of the month. • **Custom**: indicates a duration that you customize.
Alert Type	Selecting specific types from the drop-down list indicates that only alerts of the selected types are queried. Selecting **All** indicates that alerts of all types are queried. • **DDoS Attack Alert**: indicates alerts triggered by DDoS attacks. • **Region Traffic Alert:** indicates alerts triggered by abnormal inbound or outbound region traffic. • **IP Group Traffic Alert**: indicates alerts triggered by abnormal traffic received or sent by an IP group. • **Threat Intelligence Alert**: indicates alerts triggered by IP group assets matching the threat intelligence database. • **Router Alert**: indicates alerts triggered by abnormal CPU or memory usage of a router. • **Router Interface Bandwidth Alert**: indicates alerts triggered by abnormal interface bandwidth usage of a router. • **Router Data Acquisition Abnormal Alert**: indicates alerts triggered by a router failing to collect data (i.e., failing to report flow and SNMP data to NTA). • **Custom Featured Traffic Alert**: indicates alerts triggered by traffic that contains custom attack signatures. • **NTA System Performance Alert**: indicates alerts triggered by abnormal CPU or memory usage of NTA.
Alert Peak Value	Indicates the peak traffic when the alert was being generated. The peak value can be in a specified range, greater than or equal to a numerical value, or smaller than or equal to a numerical value. Also, the peak value can be expressed in bps or pps.
Alert Level	Falls into three levels: **High**, **Medium**, and **Low**. If you select **All**, alerts of all levels will be retrieved.
Routers	Selecting router interfaces from the drop-down list indicates only alerts of the selected router interfaces. Note This parameter is required only when alerts concerning router performance and

Parameter	Description
	interface bandwidth are queried.
Interface	Indicates the interface of a router.
Alert ID	Entering a specific alert ID indicates only the corresponding alert. Entering no specific alert ID indicates any alerts.
Destination IP	You can enter a specific IP address or IP segment for alert query alert.
Alert Object	Indicates objects whose alerts will be queried. Clicking in the text box will display all available alert objects, including: • **Region and IP group**: Fuzzy query is supported, that is, after you type part of an object name, the system will show the full names containing your input. • **Default**: The system will query alerts of objects that belong to neither a region nor an IP group. Multiple objects can be selected and these selected objects form an OR relationship. That is to say, alerts of one selected object, once retrieved, will be displayed. If this text box is left empty, there is no restriction on alert objects and alerts that meet other conditions are displayed.
Attack Direction	Indicates the attack direction, which can be outbound or inbound.

Step 3 Click **Search**.

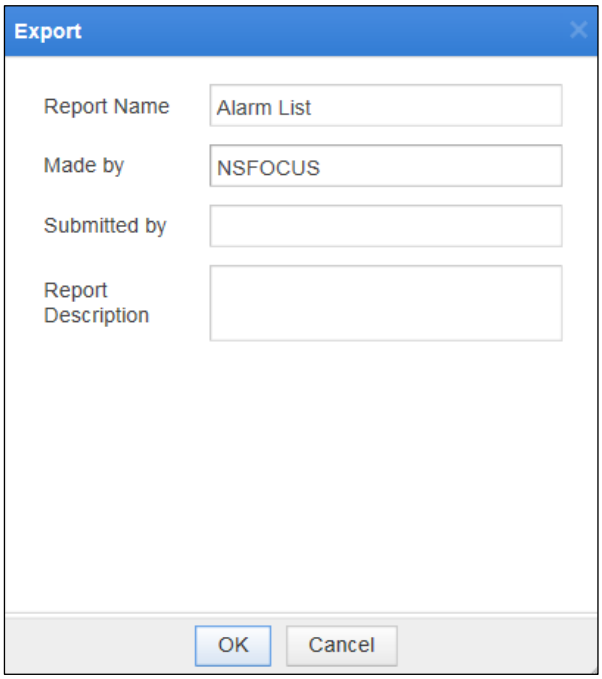
Alerts meeting the conditions will be displayed, as shown in Figure 8-14.

Figure 8-14 Alert search result



Step 4 Click to export the current alert list.

Figure 8-15 Exporting the alert list



Step 5 Configure parameters in the **Export** dialog box.

Table 8-5 Parameters for exporting the alert list

Parameter	Description
Report Name	Specifies the report name, which is **Alarm List** by default.
Made by	Specifies the person who makes this report, which is **NSFOCUS** by default.
Submitted by	Specifies to whom this report is sent.
Report Description	Brief description of this report.

To view details about an alert, click its alert ID. For details, see section 8.1.2 Viewing Information About Specified Alerts.

----End

9 Monitoring

This chapter describes how to view and manage all monitoring information, containing the following sections:

Section	Description
View Management	Describes how to manage views on monitoring pages.
Overall Monitoring Statistics	Describes how to view statistics about traffic of and attacks against routers, regions, and IP groups monitored by NTA.
Regions	Describes how to view alert and traffic statistics of all regions, detailed monitoring information of each region, and detailed monitoring information of specific IP addresses.
Routers	Describes how to view performance and traffic statistics of routers monitored by NTA and monitoring information of each router.
Router Interface Groups	Describes how to view traffic statistics of router interface groups monitored by NTA and detailed monitoring information of each router interface group.
IP Addresses	Describes how to view traffic statistics of specific IP addresses.
Diversion Routing Table	Describes how to view dynamically added routing tables for IP address- and group-specific diversion, and how to configure routes for manual traffic diversion.
Traffic Auto-learning	Describes how to check the traffic auto-learning results of IP groups.
Local Status	Describes how to view NTA's system status, basic information, system services, and local interface status.

9.1 View Management

NTA provides monitoring views, each consisting of several panes, to present monitoring statistics to users. These views are displayed on monitoring pages under **Monitor**.

Uses can customize monitoring views as required by doing the following:

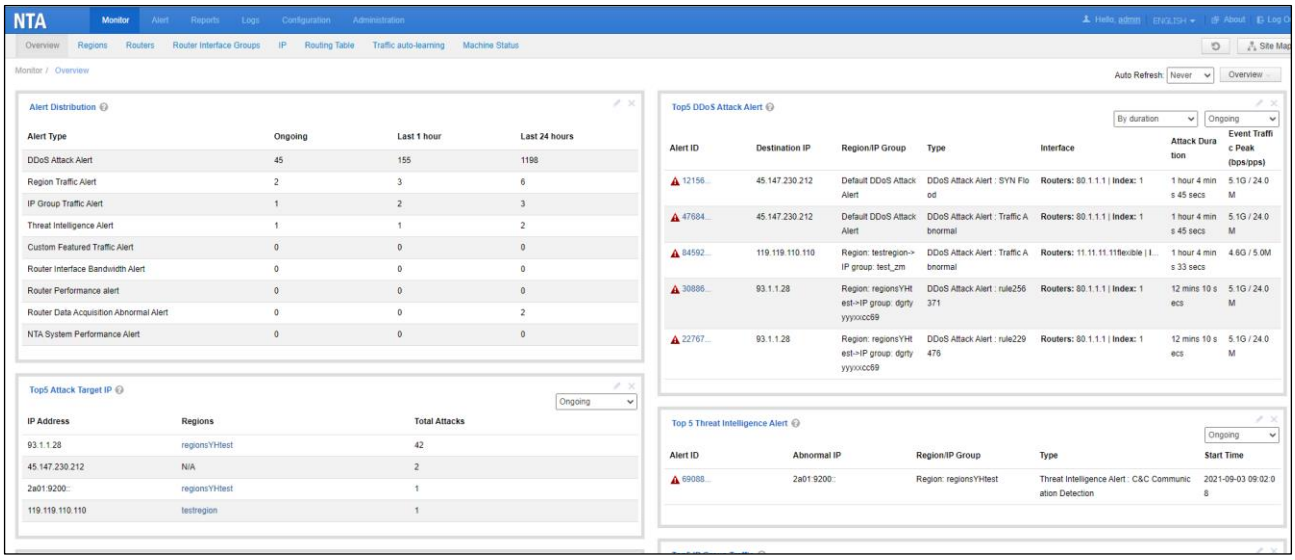
- Adding a View
- Editing a View
- Switching to a Desired View
- Setting a View as Default

Using the **Overview** page under **Monitor** as an example, this section describes how to manage and configure views.

9.1.1 Adding a View

Step 1 Choose **Monitor** > **Overview**.

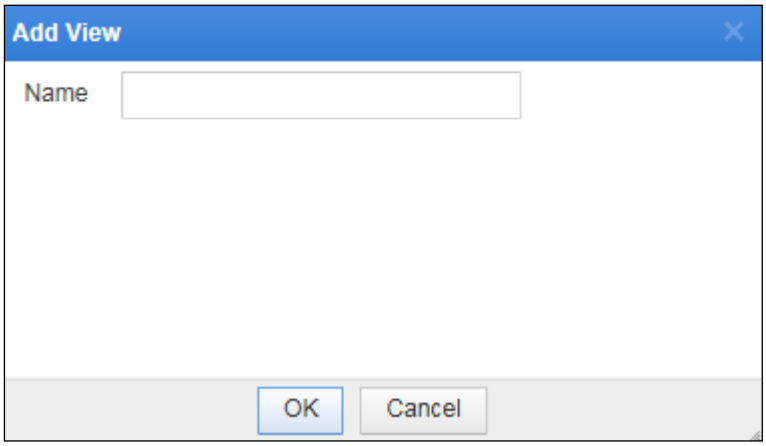
Figure 9-1 Monitoring overview



When the **Overview** page is opened, it automatically displays the default monitoring view. Initially, the default monitoring view is **Overview**.

Step 2 In the upper-right corner of the **Overview** page, click the button showing the view name (**Overview** in this example), and click **Add View** on the dropped-down list.

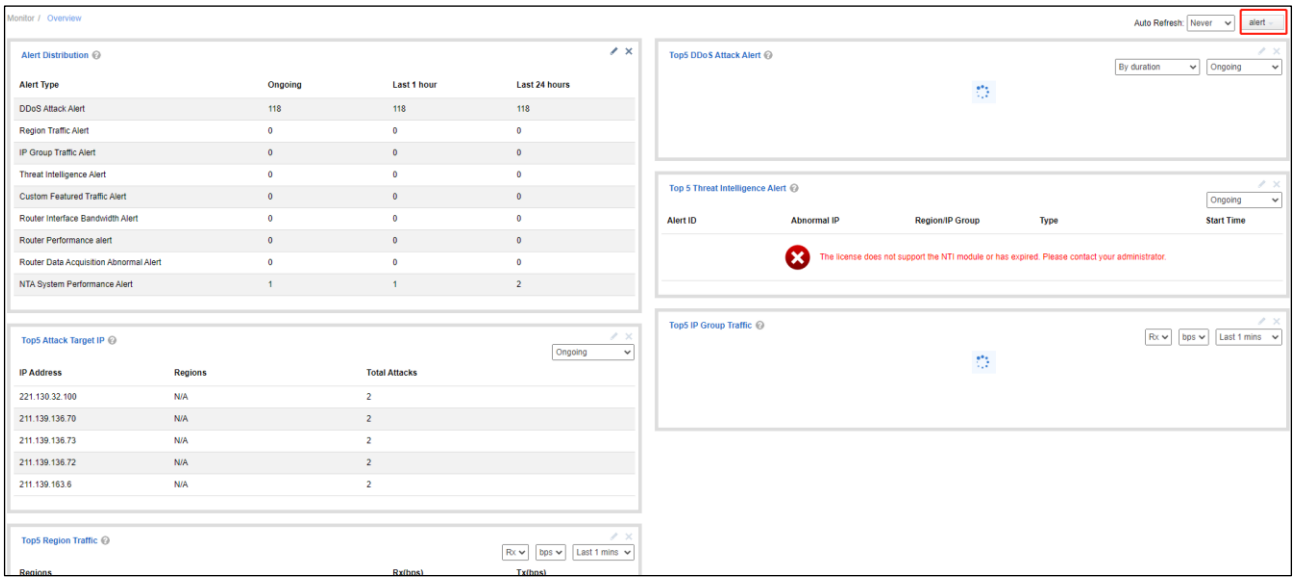
Figure 9-2 Adding a view



Step 3 Enter a view name (**alert** for example) and click **OK**.

The view is added successfully and displayed on the **Overview** page. To delete the current view, you can click **Overview** in the upper-right corner and then click **Delete View** on the drop-down list.

Figure 9-3 New view named alert



----End

Initially, a new view contains all panes. You can delete an unnecessary pane by clicking ✕ in the upper-right corner of the pane and then **OK** in the confirmation dialog box that pops up.

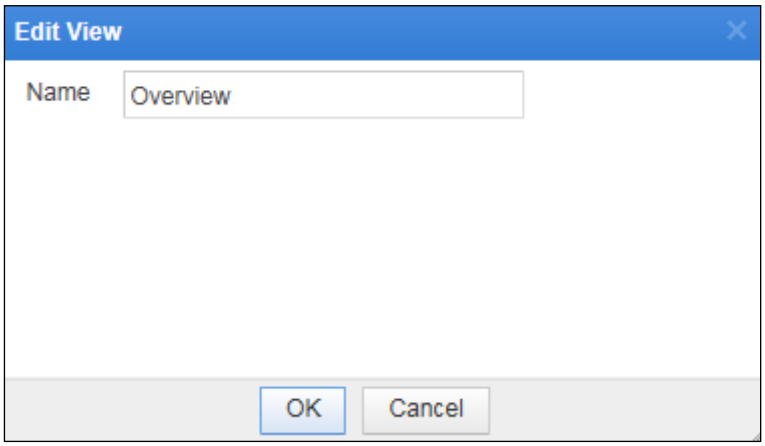
9.1.2 Editing a View

You can change the view name, delete a pane, add a pane, or move a pane.

9.1.2.1 Changing the View Name

Step 1 In the upper-right corner of the **Overview** page, click the button showing the view name (**Overview** in this example), and click **Edit View** on the dropped-down list.

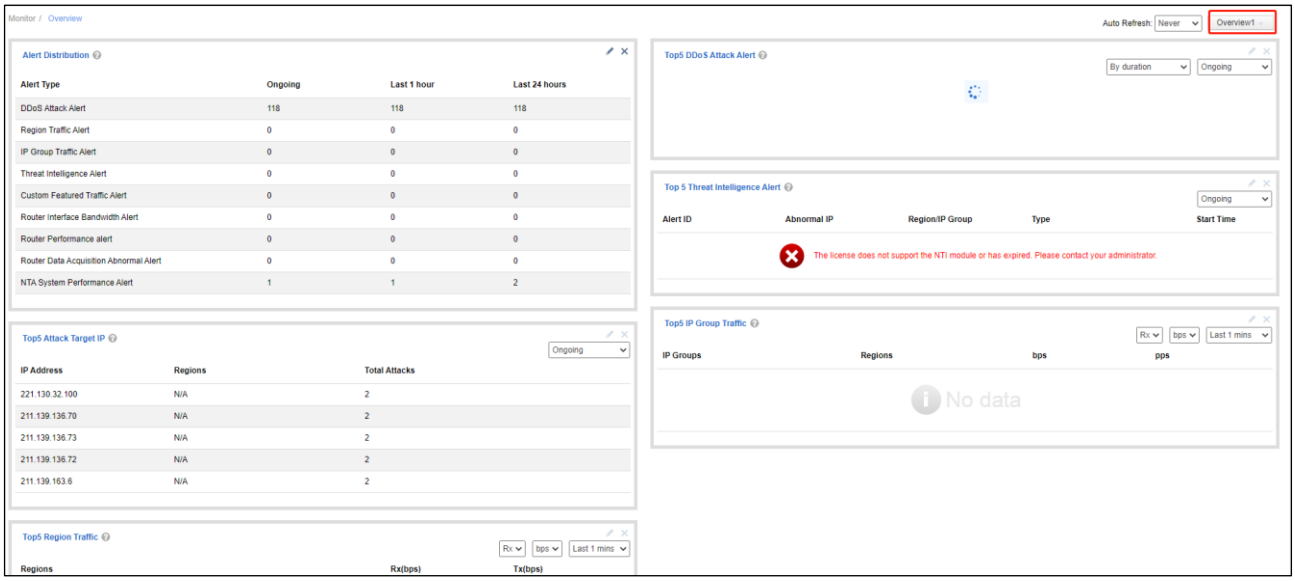
Figure 9-4 Editing the view name



Step 2 Change the view name from **Overview** to a desired one (**Overview1** for example) and click **OK**.

The new view name is displayed in the upper-right corner of the page.

Figure 9-5 View with the new name

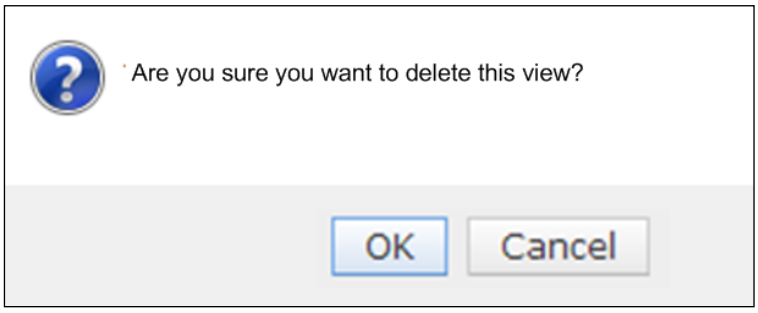


----End

9.1.2.2 Deleting a Pane

To delete a pane from a view, click ✕ in the upper-right corner of the pane and then **OK** in the confirmation dialog box that pops up, as shown in Figure 9-6.

Figure 9-6 Confirmation dialog box for deleting a pane

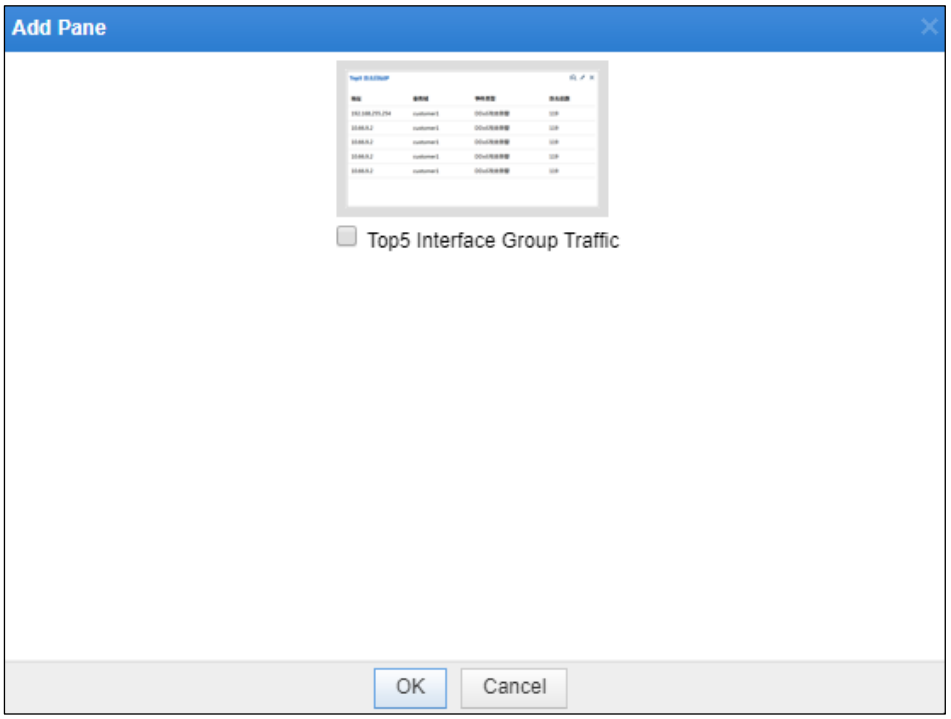


Then the pane disappears from the view.

9.1.2.3 Adding a Pane

Step 1 In the upper-right corner of the **Overview** page, click **Overview** and select **Add Pane** in the dropped-down list.

Figure 9-7 Adding a pane



Step 2 Select a desired pane to add to the view and click **OK**.

----End

9.1.2.4 Moving a Pane

To move a pane, hold the mouse on the pane name and drag it to the desired position.

9.1.2.5 Editing Pane Properties

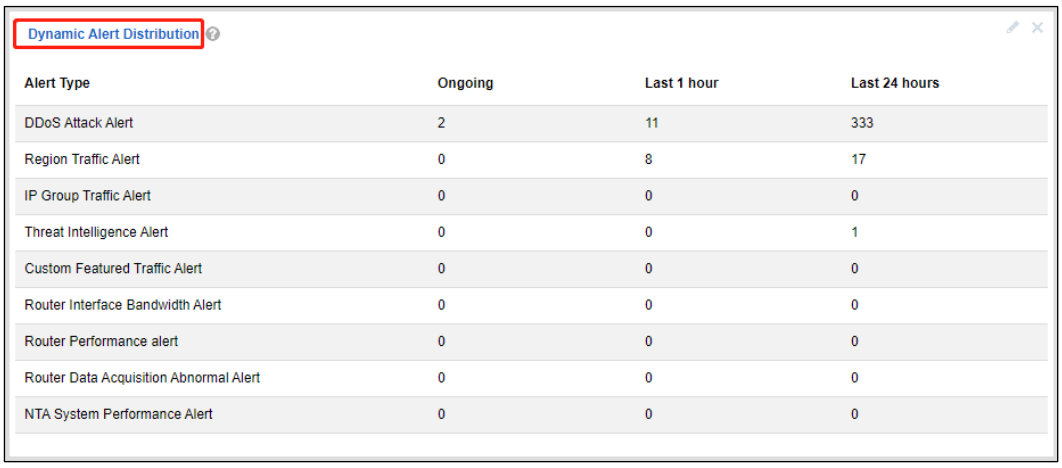
Step 1 Click in the upper-right corner of the pane.

Figure 9-8 Editing pane properties

Step 2 Change the pane's title and frame color and click **OK**.

For example, change the pane title from **Alert Distribution** to **Dynamic Alert Distribution** and its frame color from grey to yellow. Figure 9-9 shows the modified pane.

Figure 9-9 Modified pane



Alert Type	Ongoing	Last 1 hour	Last 24 hours
DDoS Attack Alert	2	11	333
Region Traffic Alert	0	8	17
IP Group Traffic Alert	0	0	0
Threat Intelligence Alert	0	0	1
Custom Featured Traffic Alert	0	0	0
Router Interface Bandwidth Alert	0	0	0
Router Performance alert	0	0	0
Router Data Acquisition Abnormal Alert	0	0	0
NTA System Performance Alert	0	0	0

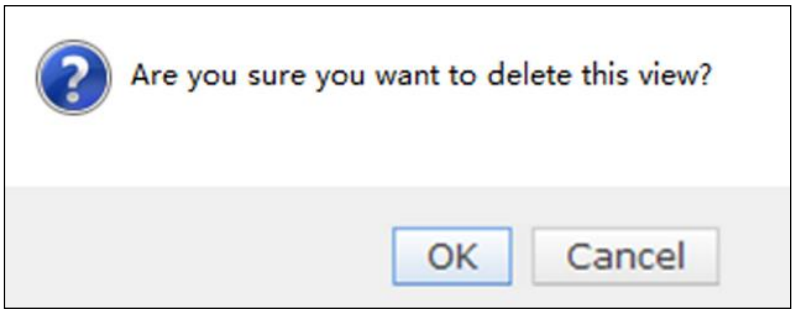
----End

9.1.2.6 Deleting a View

Step 1 Click the view name button (**Overview** by default) and select the desired view.

Step 2 Select **Delete View** from the drop-down list, and click **OK** in the confirmation dialog box that pops up, as shown in Figure 9-10.

Figure 9-10 Confirmation dialog box for deleting a view



----End

9.1.3 Switching to a Desired View

When the **Overview** page is opened, it automatically displays the default view. To switch to a desired view, click the view name button in the upper-right corner of the page, and click the desired view. Then the **Overview** page displays the desired view.

9.1.4 Setting a View as Default

When the **Overview** page is opened, it automatically displays the default view, which can be changed.

To set a view as default, switch to the view, click the view name in the upper-right corner of the page, and click **As Default View**. The next time the **Overview** page is opened, it automatically displays the new default view.

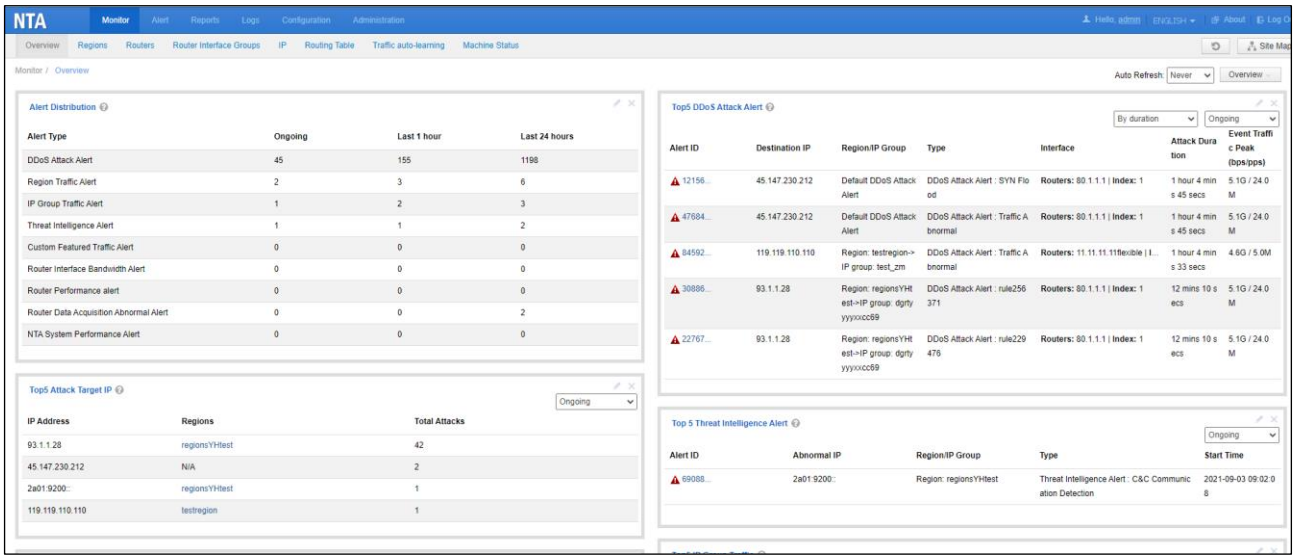
9.2 Overall Monitoring Statistics

NTA monitors routers, regions, interfaces, and IP groups. On the **Overview** page under **Monitor**, you can view overall monitoring statistics about traffic of and attacks against routers, regions, interfaces, and IP groups monitored by NTA.

To view overall monitoring statistics, follow these steps:

Step 1 Choose **Monitor** > **Overview**.

Figure 9-11 Overall monitoring statistics



Step 2 Manage the monitoring view and its panes.

When the **Overview** page is opened, it automatically displays the default monitoring view, which is initially **Overview**. You can switch to a desired view by clicking the view name button in the upper-right corner of the page and clicking the desired view.

NTA allows a maximum of eight panes in a single monitoring view to present monitoring information to users. Table 9-1 describes the panes in details.

Table 9-1 Monitoring pane description

Pane	Description
Top 5 Attack Target IP	Displays top 5 IP addresses encountering most attacks. By default, the pane displays top 5 attacked IP addresses under ongoing attacks (**Ongoing**). Alternatively, you can configure the pane to display top 5 IP addresses under attacks ending in the past hour (**End(Last 1 hour)**) or past 24 hours (**End(Last 24 hour)**). You can click a region name to view more specific monitoring information. For details, see section 9.3 Regions.
Alert Distribution	Statistical information about alerts of all types, including ongoing alerts, alerts ending in the past hour, and those ending in the past 24 hours. For details, see section 8.1 Overview.
Top 5 DDoS Attack Alert	Displays top 5 DDoS attack alerts. By default, alerts are sorted by attack duration. Alternatively, you can configure the pane to sort them by peak traffic in bps or pps in DDoS attacks. By default, the pane displays top 5 alerts for ongoing DDoS attacks (**Ongoing**). Alternatively, you can configure the pane to display top 5 alerts for DDoS attacks ending in the past hour (**End(Last 1 hour)**) or past 24 hours **(End(Last 24 hours)**). You can also click the ID of a listed alert to view its details. For details, see section 8.1.2 Viewing Information About Specified Alerts.
Top 5 Threat Intelligence	Displays top 5 alerts triggered by IP group assets matching the threat

Pane	Description
Alerts	intelligence database. These alerts are ranked by attack duration by default. By default, ongoing alerts are displayed. You can also choose to view top 5 alerts that have ended in the last hour or those in the last 24 hours. You can also click an alert ID to view details of the alert. For details, see section 8.1.2 Viewing Information About Specified Alerts.
Top 5 Region Traffic	Displays top 5 regions by traffic received or transmitted within a specified interval. By default, interface groups are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the pane to sort interface groups by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (**Last 1 mins**), hour (**Last 1 hour**), or 24 hours (**Last 24 hours**). You can click a region's name to view its specific monitoring information. For details, see section 9.3 Regions.
Top 5 IP Group Traffic	Displays top 5 IP groups by traffic received or transmitted within a specified interval. By default, IP groups are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the pane to sort items by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (**Last 1 mins**), hour (**Last 1 hour**), or 24 hours (**Last 24 hours**). You can click a region name to view more specific monitoring information. For details, see section 9.3 Regions.
Top 5 Interface Traffic	Displays top 5 interfaces by traffic received or transmitted within a specified interval. By default, interfaces are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the pane to sort interfaces by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (**Last 1 mins**), hour (**Last 1 hour**), or 24 hours (**Last 24 hours**). You can click an interface's name to view its specific monitoring information. For details, see section 9.4 Routers.
Top 5 Interface Group Traffic	Displays top 5 interface groups by traffic received or transmitted within a specified interval. By default, interface groups are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the pane to sort interfaces by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (**Last 1 mins**), hour (**Last 1 hour**), or 24 hours (**Last 24 hours**). You can click an interface group's name to view its specific monitoring information. For details, see section 9.5 Router Interface Groups.

Initially, NTA provides only one view (**Overview**) on the **Overview** page under **Monitor**. To meet monitoring needs, you can add views, delete views, set a view as default, and add, delete, and edit panes in views. For details, see section 9.1 View Management.

Step 3 Refresh the page to obtain the latest monitoring information.

The default setting for **Auto Refresh** is **Never**, indicating that the system does not automatically refresh the page to obtain the latest monitoring information. Alternatively, you can set **Auto Refresh** to **30 sec**, **1 min**, or **5 mins**.

Note that the **Auto Refresh** setting is automatically restored to **Never** after the user exits or manually refreshes the page.

----End

9.3 Regions

NTA monitors regions and provides related monitoring information. On the **Regions** page under **Monitor**, you can perform the following:

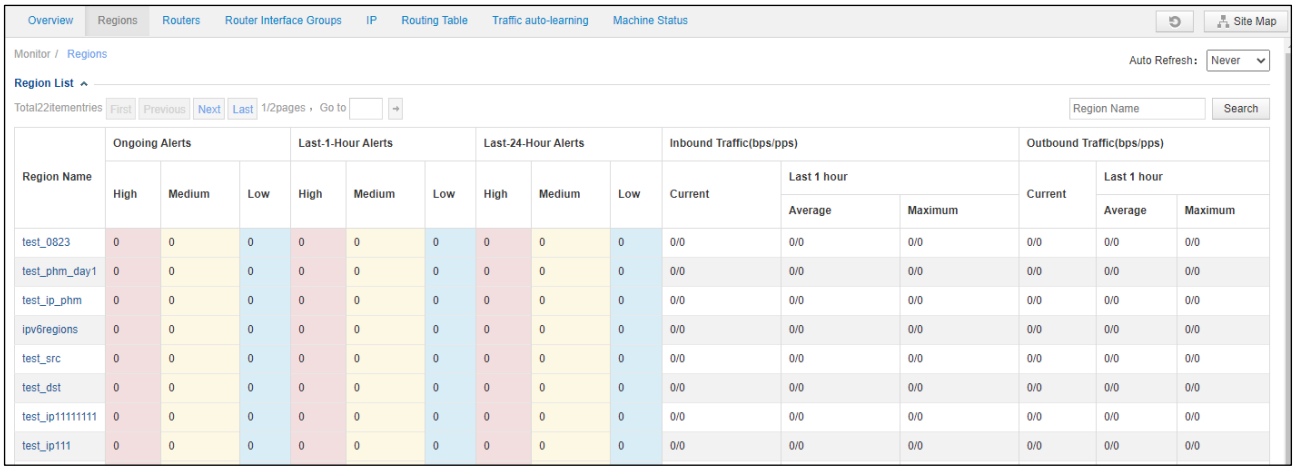
- Viewing Alert and Traffic Statistics of All Regions
- Viewing Monitoring Information of a Specific Region

9.3.1 Viewing Alert and Traffic Statistics of All Regions

To view alert and traffic statistics of all regions, choose **Monitor > Regions.**

The **Regions** page appears, listing regions and their alert and traffic statistics.

Figure 9-12 Alert and traffic statistics of regions

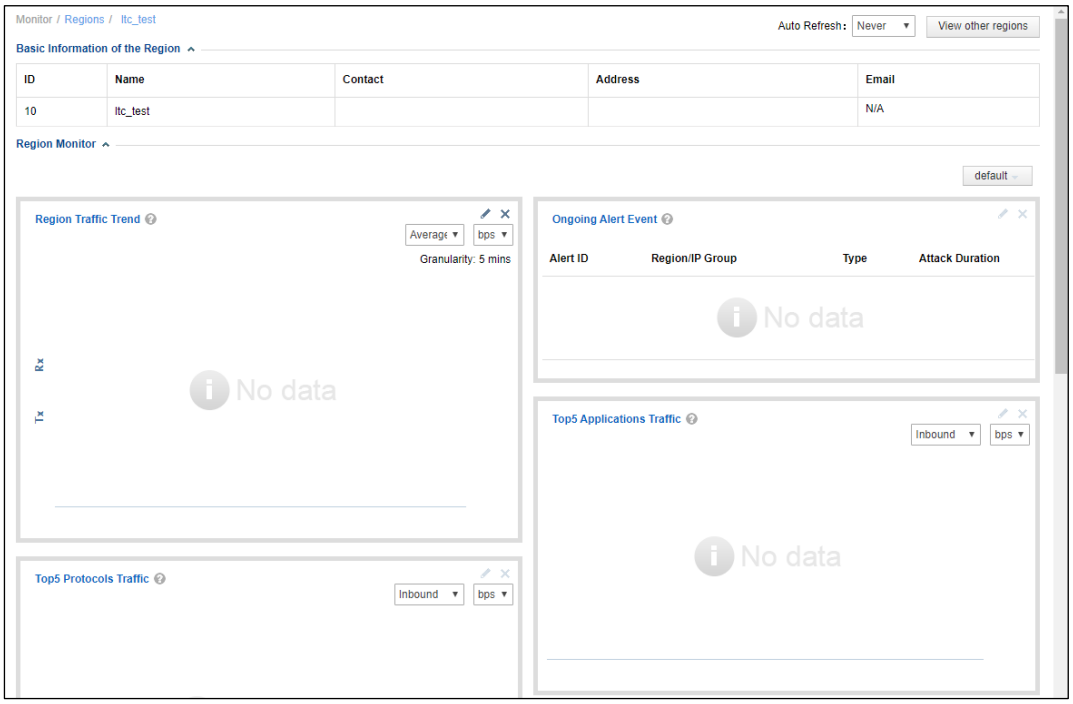


The page displays alert and traffic statistics of all regions. Alert statistics cover all high-, medium-, and low-level alerts that are ongoing, ending in the past hour, and ending in the past 24 hours. Traffic statistics cover the maximum and average traffic that each region receives and transmits currently and in the past hour.

9.3.2 Viewing Monitoring Information of a Specific Region

Click the name of a desired region in the **Region Name** column on the **Regions** page.

Figure 9-13 Detailed monitoring information of a region



You can click **View other regions** in the upper-right corner of the current page to return to the previous page.

The page consists of two areas: **Basic Information of the Region** and **Region Monitor**, which show basic region information and detailed monitoring data respectively.

When the page is opened, it automatically displays the default monitoring view, which is initially the **Default** view. You can switch to a desired view by clicking the view name button in the upper-right corner of the **Region Monitor** area and clicking the desired view.

Pointing to the region traffic trend graph displays the traffic data of the current node.

NTA allows a maximum of seven panes in a single region monitoring view to present monitoring information to users. Table 9-2 describes the panes in details.

Table 9-2 Monitoring pane description

Pane	Description
Ongoing Alert Event	Displays the statistics about ongoing alerts, including alert IDs, levels, regions/IP groups to which alerts belong, alert types, and alert durations. You can click the ID of an alert to view more specific monitoring information about the alert. For details, see section 8.1.2 Viewing Information About Specified Alerts.
Region Traffic Trend	Displays the trend of average or maximum traffic of a region within a specified interval. Traffic statistics of the region are collected every 5 minutes to obtain the trend. The default interval is 3 hours. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about the region's average traffic expressed in bps.
Top 5 IP Traffic	Displays top 5 IP addresses in the region by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the

Pane	Description
	upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 IP Group Traffic	Displays top 5 IP groups in the region by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Protocols Traffic	Displays top 5 protocols in the region by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Applications Traffic	Displays top 5 applications in the region by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 AS Traffic	Displays top 5 autonomous systems (ASs) in the region by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps. If the organization name of the AS is defined in the data dictionary, the name is displayed here. For how to configure ASs, see section 5.8.2 Autonomous Systems.
Top 5 Packet Length Traffic	Displays top 5 packet lengths of all packets received and transmitted by a region within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Prefix Traffic	Displays top 5 prefixes in the region by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 DSCP Traffic	Displays top 5 DSCPs in the region by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Country/Region Traffic	Displays top 5 countries/regions in the region by traffic received or transmitted within a specified interval.The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.

Initially, NTA provides only one view (**Default**) in the monitoring page of a region. To meet monitoring needs, you can add views, delete views, set a view as default, and add, delete, and edit panes in views. For details, see section 9.1 View Management.

You can refresh the page to obtain the latest monitoring information. The default setting for **Auto Refresh** is **Never**, indicating that the system does not automatically refresh the page to obtain the latest monitoring information. Alternatively, you can set **Auto Refresh** to **30 sec**, **1 min**, or **5 mins** on the **Regions** page or the page displaying information about a specific region.

Note that the **Auto Refresh** setting is automatically restored to **Never** after the user exits or manually refreshes the page.

9.4 Routers

NTA monitors routers and provides related monitoring information. On the **Routers** page under **Monitor**, you can perform the following:

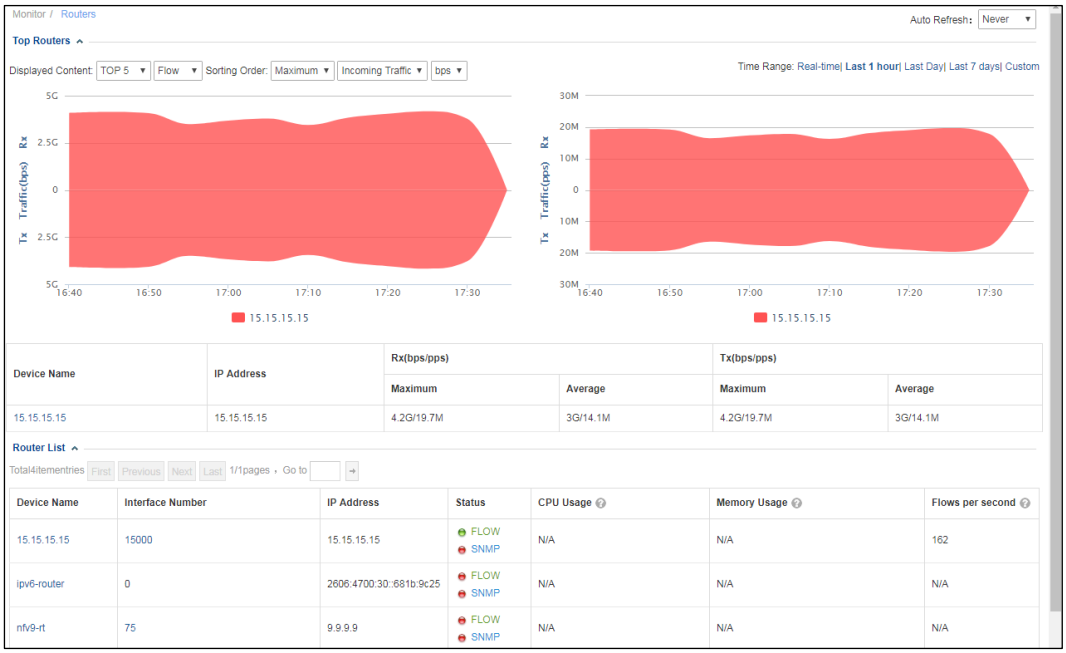
- Viewing Overall Statistics of Routers
- Viewing Monitoring Information of Interfaces on a Specific Router

9.4.1 Viewing Overall Statistics of Routers

Step 1 Choose **Monitor > Routers**.

The **Routers** page appears, showing performance and traffic statistics of all NTA-monitored routers.

Figure 9-14 Router monitoring



Step 2 View top routers with the heaviest traffic.

The **Top Routers** area shows curves indicating traffic statistics of the top routers with the heaviest traffic, as shown in Figure 9-15.

Figure 9-15 Top routers with the heaviest traffic

You can set the following display parameters to view desired statistics:

- **Displayed Content**: specifies the content to be displayed. By default, traffic curves of the top 5 routers with the heaviest flow traffic are displayed. You can set parameters to view the curves of top 5, top 10, or top 20 routers with the heaviest flow or SNMP traffic.
- **Sorting Order**: specifies how traffic is sorted, by maximum or average traffic, by incoming or outgoing traffic, and by pps or bps.
- **Time Range**: specifies the period in which traffic statistics are collected. The value can be **Real-time**, **Last 1 hour**, **Last Day**, **Last 7 days**, or **Custom**.

The table shows statistics about traffic received and sent by top routers. Clicking the name of a router can view more specific monitoring information, as shown in Figure 9-18.

Step 3 View statistics of all routers under monitoring.

The **Router List** area lists statistics of all routers. After you enable PPPoE interfaces in the console, you can view their number on the web-based manager. For how to enable PPPoE interfaces, see section 10.9 Enable/Disable PPPoE Interfaces

Figure 9-16 Statistics of all routers under monitoring

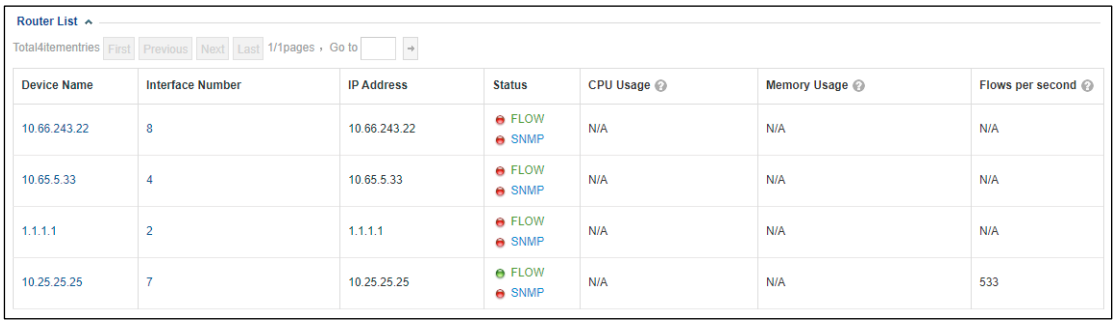


Table 9-3 describes parameters of performance and traffic statistics of NTA-monitored routers.

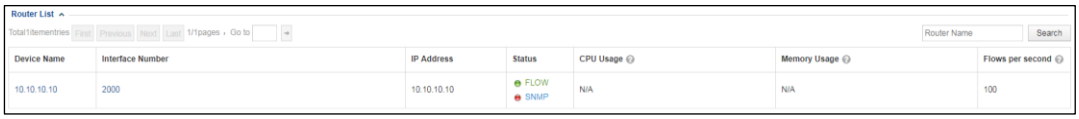
Table 9-3 Parameters of performance and traffic statistics

Parameter	Description
Device Name	Name of the router.
Interface Number	Number of router interfaces obtained via SNMP or flow data. Clicking a number in the **Interface Number** column displays information about all monitored interfaces of the router, including basic settings, interface bandwidth usage, and inbound and outbound traffic.
IP Address	IP address that identifies the router.
Status	Indicates whether the device is receiving flow and SNMP data. A red indicator means that the device is receiving data, while a green indicator means otherwise.
CPU Usage	CPU usage of the router. To obtain the CPU usage of a monitoring object, when configuring a monitoring object under **Configuration > Objects**, a user needs to enable **SNMP Collection** and set related parameters during the **SNMP Configuration** phase, and enable **CPU Usage Alert** during the **Router Alert Configuration** phase. Otherwise, data related to the CPU usage of the monitoring object cannot be obtained, and the CPU usage is displayed as **N/A**.
Memory Usage	Memory usage of the router. To obtain memory usage of a monitoring object, when configuring a monitoring object under **Configuration > Objects**, a user needs to enable **SNMP Collection** and set related parameters during the **SNMP Configuration** phase, and enable **Memory Usage Alert** during the **Router Alert Configuration** phase. Otherwise, data related to the memory usage of the monitoring object cannot be obtained, and the memory usage is displayed as **N/A**.
Flows per second	Number of flows received by a router per second. **N/A** indicates that no flows are received or the flow receiving configuration is incorrect.

Step 4 Search for a specific router

Type the name of a desired router in the search box. NTA supports fuzzy search.

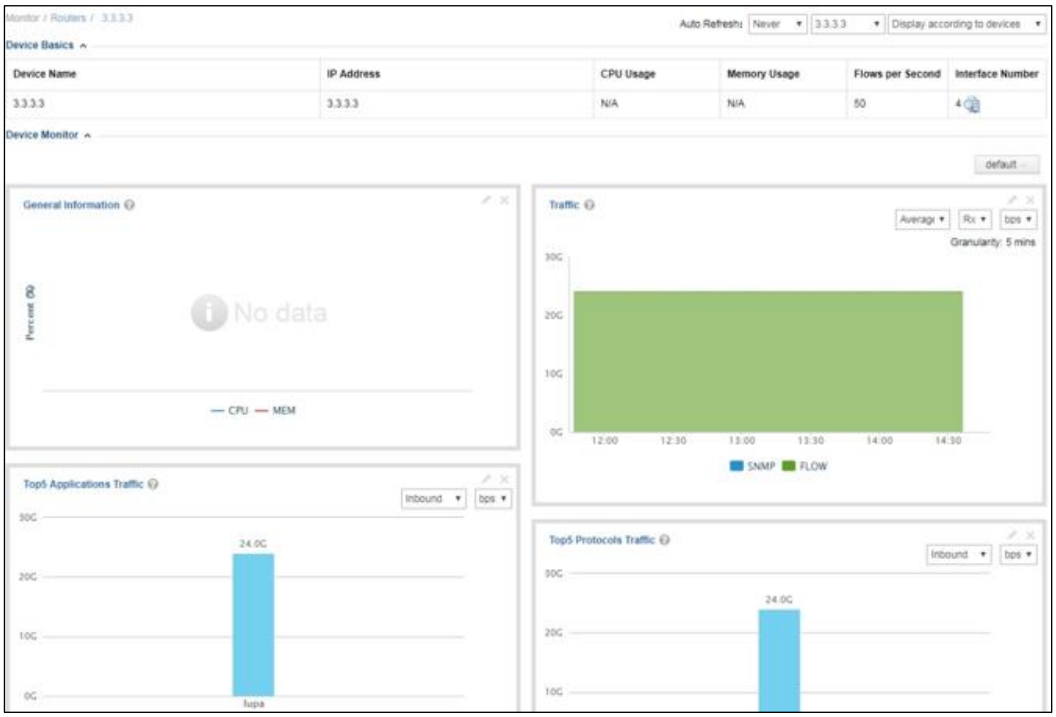
Figure 9-17 Searching for a specific router



Step 5 View the monitoring information of a specific router.

Click the name of a desired router in the **Device Name** column. A page appears, showing the detailed monitoring information about the router.

Figure 9-18 Detailed monitoring information of a router



The page consists of two areas: **Device Basics** and **Device Monitor**, which show basic device information and detailed monitoring information respectively. When the page is opened, it automatically displays the default monitoring view, which is initially **Default**. You can switch to a desired view by clicking the view name button in the upper-right corner of the **Device Monitor** area and clicking the desired view.

Pointing to the router traffic trend graph displays the traffic data of the current node. NTA allows a maximum of six panes in a single router monitoring view to present monitoring information to users. Table 9-4 describes the panes in details.

Table 9-4 Monitoring pane description

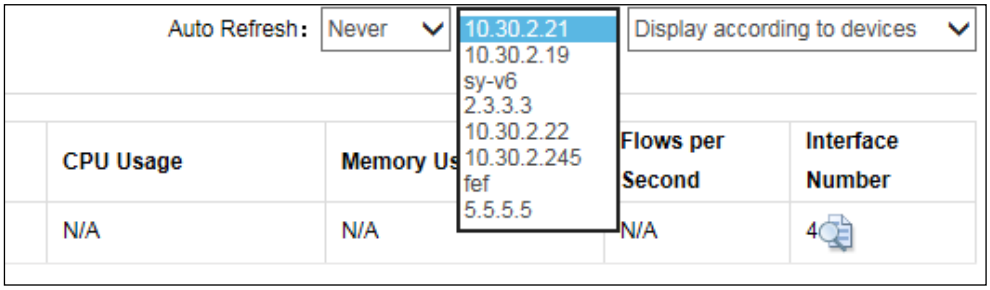
Pane	Description
General Information	Displays the CPU and memory usage. The CPU and memory usage is obtained via SNMP. Therefore, to obtain CPU and memory usage of a router, you needs to enable **SNMP Collection** when configuring a router as a monitoring object under **Configuration** > **Objects**.
Ongoing Alert Event	Displays information about ongoing CPU and memory usage alerts on the router, including the ID, level, type, and duration of alerts. You can click the ID of an alert to view more specific monitoring information about the alert. For details, see section 8.1.2 Viewing Information About Specified Alerts.
Top 5 Protocols Traffic	Displays top 5 protocols on the router by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Interface Traffic	Displays top 5 interfaces on the router by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the

Pane	Description
	upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic. Interface names are obtained via SNMP. If SNMP is not configured, interface indexes obtained via flows are used as interface names.
Top 5 Applications Traffic	Displays top 5 applications on the router by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 AS Traffic	Displays top 5 ASs on the router by traffic received or transmitted within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic. If the organization name of the AS is defined in the data dictionary, the name is displayed here. For how to configure ASs, see section 5.8.2 Autonomous Systems.
Traffic	Displays the traffic trend of the router within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, statistics on average received traffic in bps are displayed. Note If the granularity is set to 5 minutes, NTA obtains the traffic rate every 30 seconds, calculates the average or maximum traffic value of every five minutes, and uses the value as a dot in the trend curve.
Top 5 Packet Length Traffic	Displays top 5 packet lengths of all packets received and transmitted by a router within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Prefix Traffic	Displays top 5 prefixes on the router by traffic received or transmitted during a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 DSCP Traffic	Displays top 5 DSCPs on the router by traffic received or transmitted during a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Country/Region Traffic	Displays top 5 countries/regions on the router by traffic received or transmitted during a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.

Initially, NTA provides only one view (**Default**) on the monitoring page of a router. To meet monitoring needs, you can add views, delete views, set a view as default, and add, delete, and edit panes in views. For details, see section 9.1 View Management.

Step 6 To switch to the monitoring page of another router, expand the drop-down box next to the **Auto Refresh** drop-down box and click the name of the desired router.

Figure 9-19 Switching to the monitoring page of another router



To view statistics of interfaces on the current router, expand the rightmost drop-down list in the upper-right corner of the page, and click **Display according to interfaces**. Then, a page appears, showing statistics about the interfaces on the router. For details, see section 9.4.2 Viewing Monitoring Information of Interfaces on a Specific Router.

Step 7 Refresh the page to obtain the latest monitoring information.

The default setting for **Auto Refresh** is **Never**, indicating that the system does not automatically refresh the page to obtain the latest monitoring information. Alternatively, a user can set **Auto Refresh** on the **Routers** page or the page displaying information about a specific router to **30 sec**, **1 min**, or **5 mins**.

Note that the **Auto Refresh** setting is automatically restored to **Never** after the user exits or manually refreshes the page.

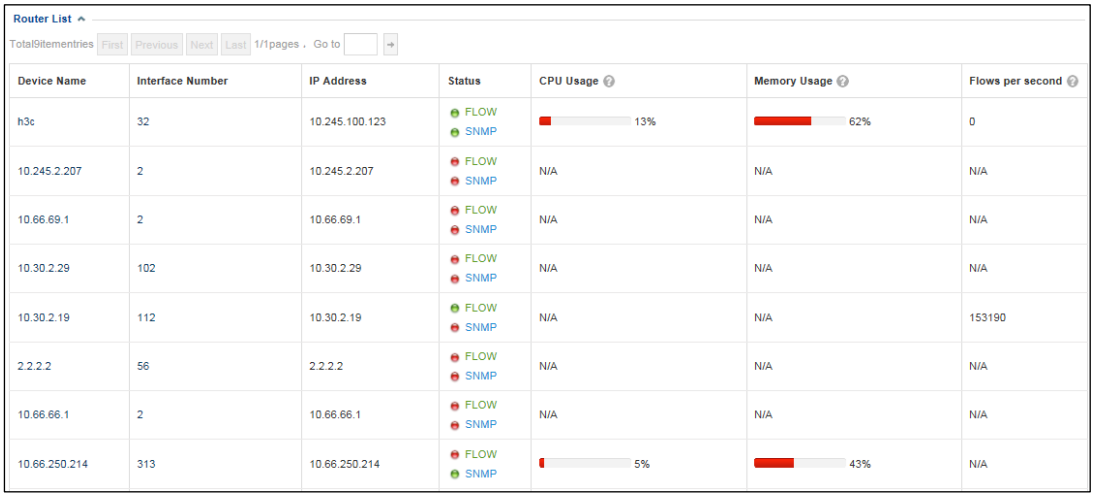
----End

9.4.2 Viewing Monitoring Information of Interfaces on a Specific Router

Step 1 Choose **Monitor > Routers**.

The **Routers List** area appears, listing routers and their statistics.

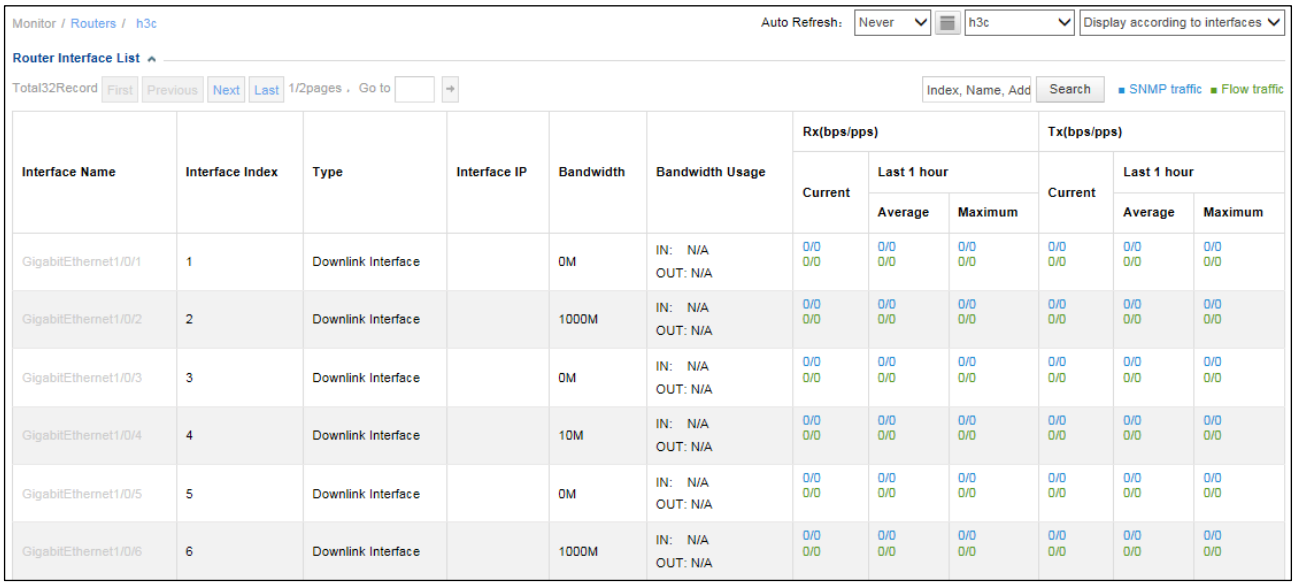
Figure 9-20 Monitoring statistics of routers



Step 2 View statistics about all interfaces on a specific router.

Click the number in the **Interface Number** column to view information of all monitored interfaces of the router, including basic settings, interface bandwidth usage, and inbound and outbound traffic.

Figure 9-21 Page showing interface monitoring information



On this page, you can type the index, name, or IP address of an interface to check desired monitoring information.

Table 9-5 describes parameters in the router interface list.

Table 9-5 Parameters in the router interface list

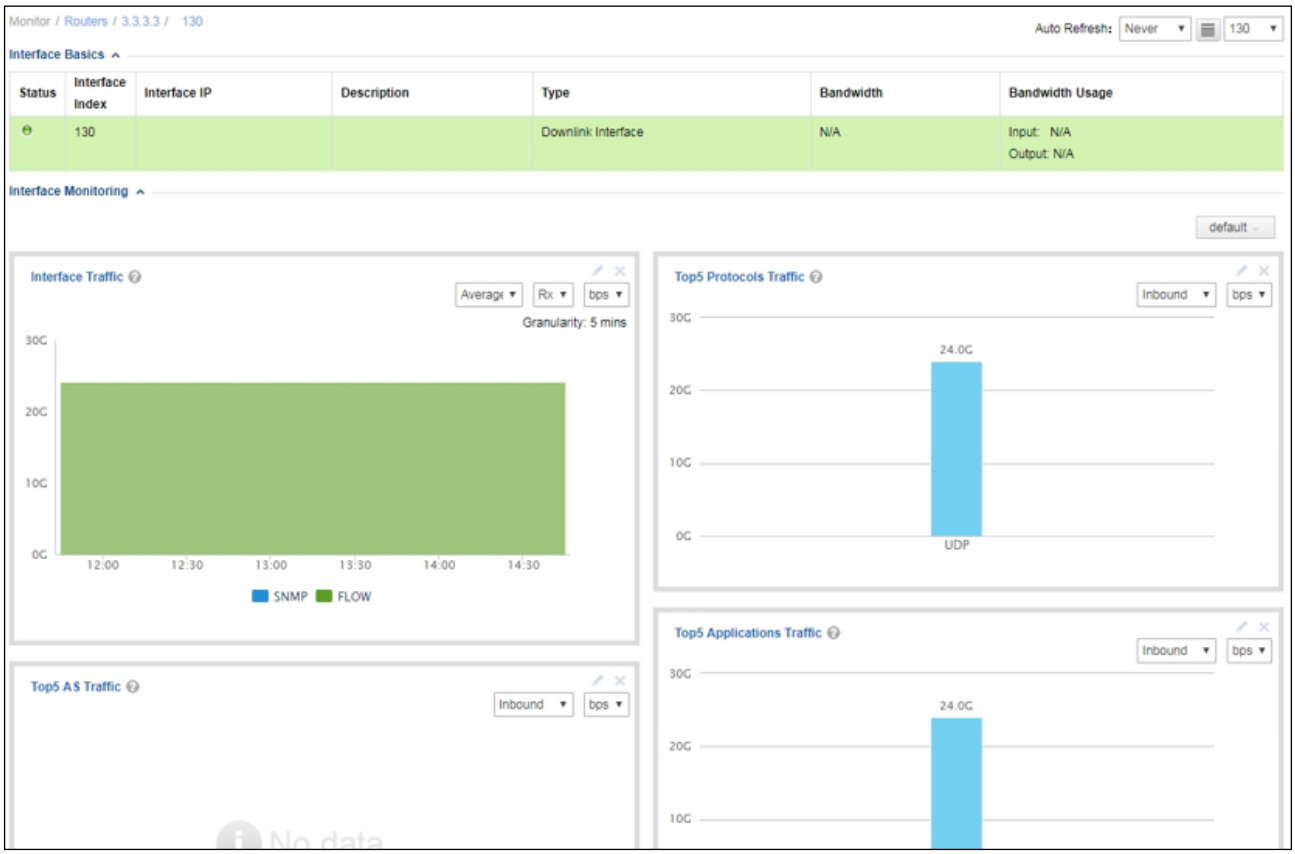
Parameter	Description
Interface Name	Interface name that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router or exceptions occur during SNMP data transmission, the interface index will be displayed as the interface name. The interface name will turn blue from gray only when SNMP monitoring is enabled on the interface of the router. For how to enable SNMP monitoring, see section 5.1.1.2 Configuring Router Interfaces.
Interface Index	Interface index that NTA obtains from the router via flow data.
Type	Type of the interface, which may be an uplink or downlink interface.
Interface IP	Interface IP address that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router or SNMP collection is enabled but no IP address is configured for the interface, nothing is displayed here.
Bandwidth	Interface bandwidth that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router or exceptions occur during SNMP data transmission, **N/A** will be displayed.
Bandwidth Usage	Interface bandwidth usage that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router, exceptions occur during SNMP data

Parameter	Description
	transmission, or if SNMP collection is enabled but monitoring is disabled for the interface, **N/A** is displayed.
Rx (bps/pps)	Information about traffic received over the interface, including current traffic and average and maximum traffic in the past hour. Characters in blue indicate SNMP traffic, and those in green indicate flow traffic.
Tx (bps/pps)	Information about traffic transmitted over the interface, including current traffic and average and maximum traffic in the past hour. Characters in blue indicate SNMP traffic, and those in green indicate flow traffic.

Step 3 View monitoring information of a specific interface.

Click the name of the desired interface. A page appears, showing monitoring information of the interface.

Figure 9-22 Monitoring information of a specific interface



Initially, NTA provides only one view (**Default**) on the monitoring page of an interface. To meet monitoring needs, you can add views, delete views, set a view as default, and add, delete, and edit panes in views. For details, see section 9.1 View Management.

NTA allows a maximum of five panes in a single router monitoring view to present monitoring information to users. Table 9-6 describes the panes in details.

Table 9-6 Monitoring pane description

Pane	Description
Interface Traffic	Displays the trend of average or maximum traffic of an interface within a specified interval. Traffic statistics of the interface are calculated every 5 minutes to obtain the trend. The default interval is 3 hours. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about average received traffic.
Top 5 IP Traffic	Displays top 5 IP addresses by traffic received or transmitted over the interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Protocols Traffic	Displays top 5 protocols by traffic received or transmitted over the interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Applications Traffic	Displays top 5 applications by traffic received or transmitted over the interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 AS Traffic	Displays top 5 ASs by traffic received or transmitted over the interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Packet Length Traffic	Displays top 5 packet lengths of all packets received and transmitted by an interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Prefix Traffic	Displays top 5 prefixes by traffic received or transmitted over the interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 DSCP Traffic	Displays top 5 DSCPs by traffic received or transmitted over the interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.
Top 5 Country/Region Traffic	Displays top 5 countries/regions by traffic received or transmitted over the interface within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic.

Step 4 View monitoring information of another interface on the router.

In the upper-right corner of the page, expand the rightmost drop-down list, and click the name of a desired interface. Then, the monitoring page of the desired interface appears.

Step 5 Refresh the page to obtain the latest monitoring information.

The default setting for **Auto Refresh** is **Never**, indicating that the system does not automatically refresh the page to obtain the latest monitoring information. Alternatively, you can set **Auto Refresh** to **30 sec**, **1 min**, or **5 mins**.

Note that the **Auto Refresh** setting is automatically restored to **Never** after the user exits or manually refreshes the page.

----End

9.5 Router Interface Groups

The **Router Interface Groups** page under **Monitor** shows traffic statistics of all NTA-monitored router interface groups and detailed monitoring information of each router interface group.

To view monitoring information of router interface groups, follow these steps:

Step 1 Choose **Monitor > Router Interface Groups**.

The **Router Interface Groups** page appears, showing traffic statistics of all NTA-monitored router interface groups.

Figure 9-23 Monitoring information of router interface groups

Table 9-7 describes the parameters of traffic statistics about NTA-monitored router interface groups.

Table 9-7 Parameters in the router interface group list

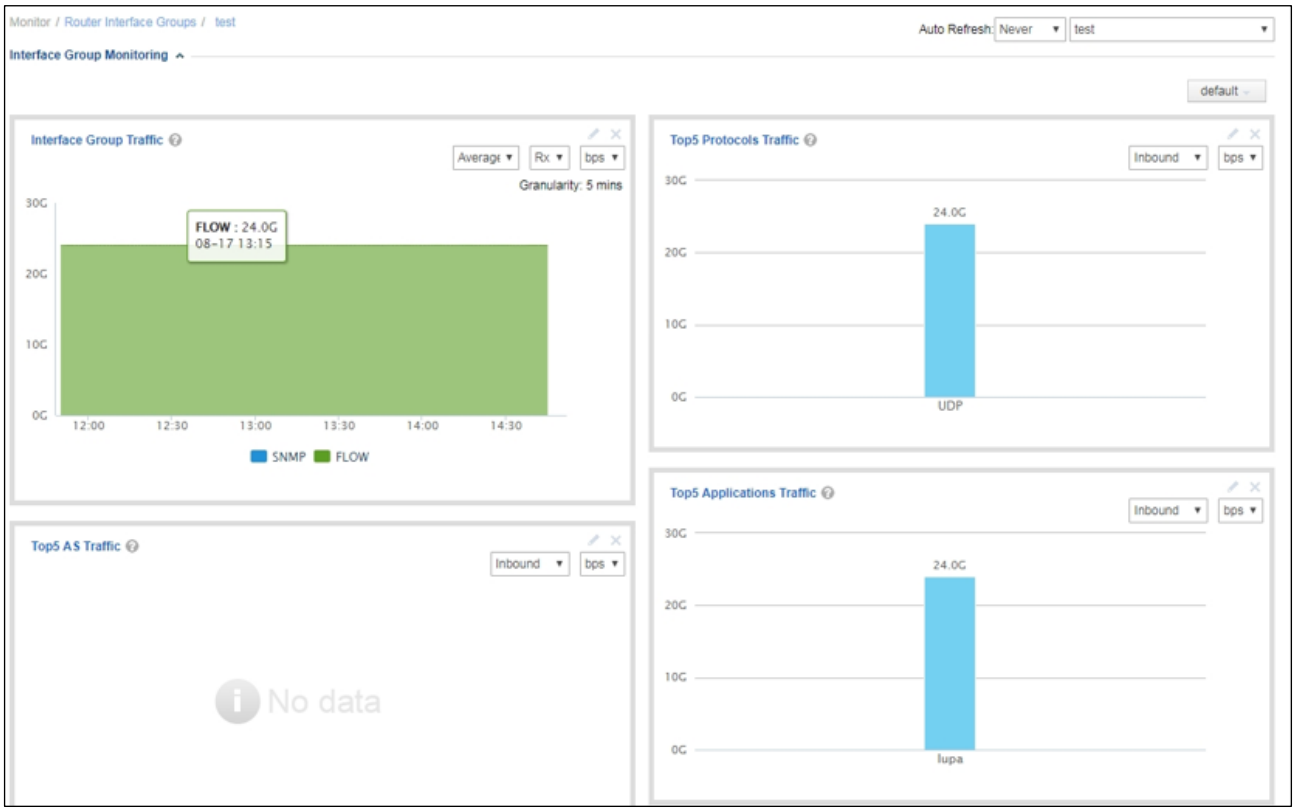
Parameter	Description
Interface Index	Index value that uniquely identifies the interface.
Name	Router interface group name.
Rx (bps/pps)	Information about traffic received by the router interface group, including current traffic and average and maximum traffic in the past hour.
Tx (bps/pps)	Information about traffic transmitted by the router interface group, including current traffic and average and maximum traffic in the past hour.

Step 2 View detailed monitoring information of a specific router interface group.

Click the name of a desired router interface group in the **Name** column. A page appears, showing the detailed monitoring information of the interface group.

Pointing to the interface traffic trend graph displays the traffic data of the current node.

Figure 9-24 Detailed monitoring information of a specific router interface group



NTA allows a maximum of four panes in a single router interface group monitoring view to present monitoring information to users. Table 9-8 describes the panes in details.

Table 9-8 Monitoring pane description

Pane	Description
Interface Group Traffic	Displays the trend of average or maximum traffic of the router interface group within a specified interval. Traffic statistics of the interface group are calculated every 5 minutes to obtain the trend. The default interval is 3 hours. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about the interface group's average received traffic expressed in bps.
Top 5 Protocols Traffic	Displays top 5 protocols by traffic received or transmitted by the interface group within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Applications Traffic	Displays top 5 applications by traffic received or transmitted by the interface group within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 AS Traffic	Displays top 5 protocols by traffic received or transmitted by the interface group within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Packet Length	Displays top 5 packet lengths of all packets received and transmitted by an

Pane	Description
Traffic	interface group within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Prefix Traffic	Displays top 5 prefixes by traffic received or transmitted by the interface group within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 DSCP Traffic	Displays top 5 DSCPs by traffic received or transmitted by the interface group within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.
Top 5 Country/Region Traffic	Displays top 5 countries/regions by traffic received or transmitted by the interface group within a specified interval. The default interval is 5 minutes. You can click in the upper-right corner of the pane to change the interval. By default, the system displays statistics about received traffic expressed in bps.

Initially, NTA provides only one view (**Default**) on the monitoring page of a router. To meet monitoring needs, you can add views, delete views, set a view as default, and add, delete, and edit panes in views. For details, see section 9.1 View Management.

To switch to the monitoring page of another router interface group, expand the drop-down box next to the **Auto Refresh** drop-down box and click the name of the desired interface group. See Figure 9-25.

Figure 9-25 Switching to the monitoring page of another router interface group

Step 3 Refresh the page to obtain the latest monitoring information.

The default setting for **Auto Refresh** is **Never**, indicating that the system does not automatically refresh the page to obtain the latest monitoring information. Alternatively, you can set **Auto Refresh** to **30 sec**, **1 min**, or **5 mins** on the **Router Interface Groups** page or the page displaying information about a specific router interface group.

Note that the **Auto Refresh** setting is automatically restored to **Never** after the user exits or manually refreshes the page.

----End

9.6 IP Addresses

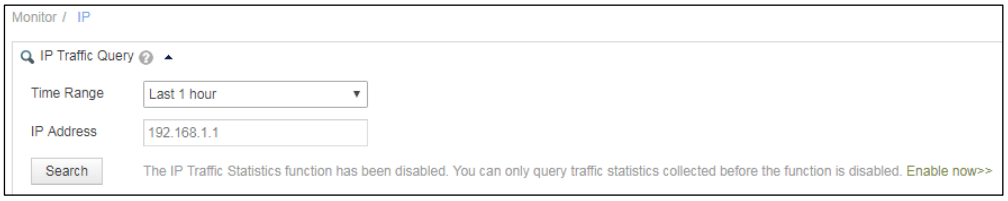
You can view traffic statistics of a specified IP address on the **IP** page. Note that traffic statistics collected during the period when IP traffic statistics are disabled cannot be retrieved.

For how to enable IP traffic statistics collection, see section 5.5 Flow Data Collection and Forwarding.

To view traffic statistics of an IP address, follow these steps:

Step 1 Choose **Monitor > IP**.

Figure 9-26 IP traffic query



Step 2 Set query conditions.

Table 9-9 Parameters for querying traffic statistics of an IP address

Parameter	Description
Time Range	Specifies the time range, which can be **Last 1 hour**, **Last Day**, **Last 7 days**, **Last 30 days**, or **Custom**. The default value is **Last 1 hour**. If **Time Range** is set to **Custom**, you need to set **Start Time** and **End Time**.
IP Address	Specifies the IP address whose traffic statistics are to be queried. This parameter is mandatory.

Step 3 Click **Search**.

Monitoring information of the specified IP address is displayed.

Figure 9-27 Monitoring information of the specified IP address

Two curves show the trends of the received (Rx) and transmitted (Tx) traffic of the specified IP address, respectively. The statistical granularity varies with the time range.

Step 4 Refresh the page to obtain the latest monitoring information.

The default setting for **Auto Refresh** is **Never**, indicating that the system does not automatically refresh the page to obtain the latest monitoring information. Alternatively, you can set **Auto Refresh** to **30 sec**, **1 min**, or **5 mins**.

Note that the **Auto Refresh** setting is automatically restored to **Never** after the user exits or manually refreshes the page.

----End

9.7 Diversion Routing Table

Diversion routes on NTA are classified into the following types:

- IP Diversion — routes for diverting DDoS attack traffic destined for individual IP addresses, which are displayed dynamically.
- FlowSpec Diversion — routes for diverting DDoS attack traffic via FlowSpec, which are displayed dynamically.
- Group Diversion — routes for diverting abnormal inbound or outbound group traffic, which are displayed dynamically.
- Manual Traffic Diversion — static route that is manually added by users for forced diversion.
- FlowSpec Manual Traffic Diversion — static route that is manually added by users for forced diversion via FlowSpec.

9.7.1 IP Diversion

When a single IP address is under DDoS attacks, NTA diverts the attack traffic according to configured policies. During the diversion, the route for the diversion is displayed on the **IP Diversion** page under **Monitor > Routing Table**. After the diversion is complete, the route will be automatically removed from the page. You can also manually delete an IP diversion route.

To view IP diversion routes, follow these steps:

Step 1 Choose **Monitor > Routing Table > IP Diversion**.

The **IP Diversion** page appears, listing IP diversion routes.

Figure 9-28 IP diversion routes

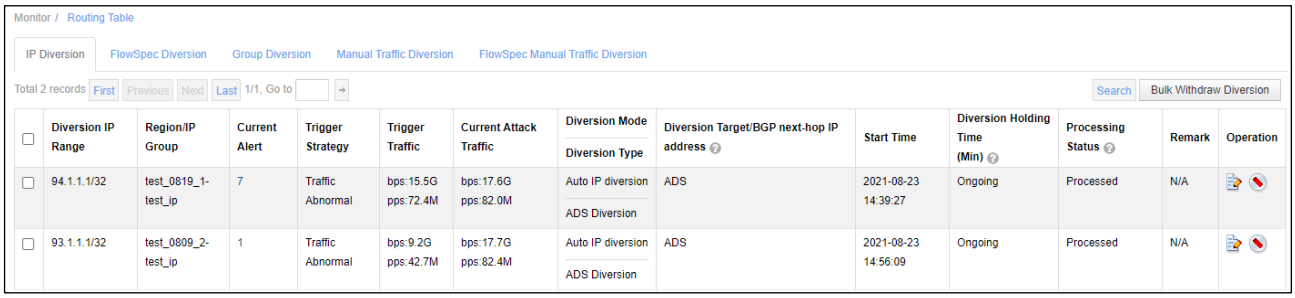


Table 9-10 describes parameters in the IP diversion route list.

Table 9-10 Parameters of IP diversion routes

Parameter	Description
Diversion IP Range	IP address and its subnet mask whose traffic is diverted.
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If such an IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Current Alert	Number of ongoing alerts. Holding the mouse over the number displays alert causes.
Trigger Strategy	Type of the alert that triggers the diversion.
Trigger Traffic	Traffic that triggers the diversion in bps and pps.
Current Attack Traffic	Current attack traffic in bps and pps.
Diversion Mode	Mode of the IP diversion, which can be either of the following: • **Auto IP Diversion**: indicates that traffic to a specific IP address is diverted when DDoS attack traffic is detected. • **Manual IP diversion**: indicates that traffic of an IP address or IP segment is diverted when hitting a manual traffic diversion rule or when you revoke an auto IP diversion route.
Diversion Type	Type of the IP diversion, which can be one of the following: • **ADS Diversion**: indicates that traffic is diverted to ADS devices. • **Null-Route Diversion**: indicates that traffic is diverted to a null-route IP address using the Border Gateway Protocol (BGP). In this case, BGP next-hop IP address is the null-route IP address. • **BGP Diversion**: indicates that traffic is diverted to a protection device using BGP. In this case, the IP address of the protection device is the BGP next-hop IP address.
Diversion Target/BGP next-hop IP address	• **Diversion Destination**: indicates the destination to which traffic is diverted. It displays information about the ADS device or BGP session. • **BGP Next-Hop IP Address**: information displayed only when **Diversion Type** is **BGP Diversion** or **Null-Route Diversion**. • When **Diversion Type** is **BGP Diversion**, **BGP Next-Hop IP Address** information shows the IP address of the target protection device of the diversion.

Parameter	Description
	• When **Diversion Type** is **Null-Route Diversion**, **BGP Next-Hop IP Address** information shows the null-route IP address of the diversion.
Start Time	Time when traffic diversion starts.
Diversion Holding Time (Min)	Time during which diversion is conducted. This parameter takes effect only when **Diversion Type** is **Null-Route Diversion** or **BGP Diversion**. NTA starts a countdown immediately after sending a null-route/BGP diversion route, and automatically revokes the diversion after the diversion duration expires.
Processing Status	Indicates whether NTA successfully processes a diversion request. Note that "Processed" does not mean that the router or ADS successfully sends a diversion route. In fact, "Processed" only means that NTA successfully sends a diversion request.
Remark	Necessary supplementary information about the route. If there are remarks, is displayed, and you can view the remarks by moving the mouse over . If there are no remarks, **N/A** is displayed. You can click in the **Operation** column to add and edit remarks.
Operation	• Click to add and edit remarks. • Click to manually revoke the diversion route.

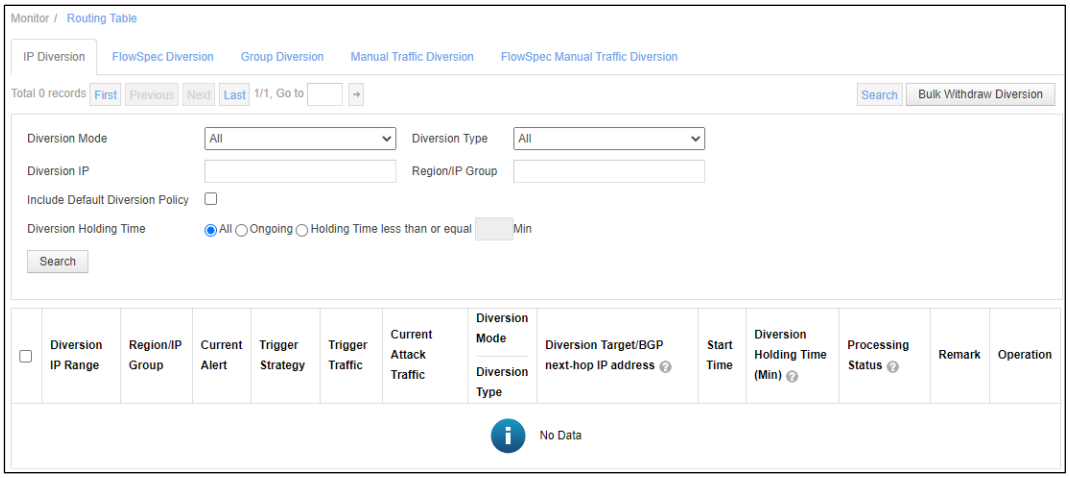
Step 2 Search for desired diversion routes.

If there are many routes, you can locate specific routes by using the searching function, including the diversion routes of regions and IP groups as well as the default diversion route.

a. Click **Search** in the upper-right corner of the page.

An area appears, showing search conditions.

Figure 9-29 Conditions for searching for IP diversion routes



b. Specify search conditions and click **Search** at the bottom of the area.

Then, only the desired routes satisfying the search conditions are displayed in the table.

Step 3 Manually revoke group diversion routes.

- Revoke a single diversion route.

  Click in the **Operation** column to manually revoke an IP diversion route.

  After the revocation, the **Diversion Mode** of the route will change to **Manual IP Diversion**, and the route will be automatically removed. You can view the log about the related diversion among the logs whose **Diversion Mode** is **Manual IP Diversion** on the **Diversion Log** page under **Logs**.

- Revoke diversion routes in batches.

  Select the check boxes of multiple routes and click **Bulk Withdraw Diversion** to delete these routes in one go.

----End

9.7.2 FlowSpec Diversion

On this tab page, you can query active diversion routes for traffic diversion via FlowSpec. Such a route will be automatically deleted after the diversion is complete. You can also manually delete a FlowSpec diversion route.

To view active FlowSpec diversion routes, follow these steps:

Step 1 Choose **Monitor > Routing Table > FlowSpec Diversion**.

Figure 9-30 FlowSpec Diversion page

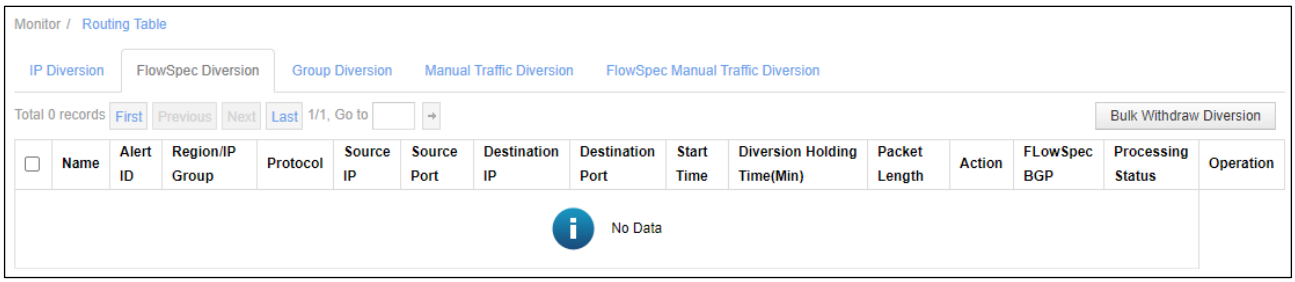


Table 9-11 describes parameters of FlowSpec diversion routes.

Table 9-11 FlowSpec diversion route parameters

Parameter	Description
Name	Number of the FlowSpec diversion route.
Alert ID	ID of the alert corresponding to this diversion event.
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If this IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Protocol	Protocol used for exchanging routing information during diversion of traffic via FlowSpec.
Source IP	Source IP address of traffic diverted via FlowSpec.
Source Port	Source port of traffic diverted via FlowSpec.
Destination IP	Destination IP address of traffic diverted via FlowSpec.

Parameter	Description
Destination Port	Destination port of traffic diverted via FlowSpec.
Start Time	Time when traffic diversion starts.
Diversion Holding Time (Min)	Time during which diversion is conducted. This parameter takes effect only when **Diversion Type** is **FlowSpec BGP Diversion**. NTA starts a countdown immediately after sending a null-route/BGP FlowSpec diversion route, and automatically revokes the diversion after the diversion duration expires.
Packet Length	Length of diverted packets.
Action	Action taken on the diverted traffic.
FLowSpec BGP	Name of the BGP FlowSpec session.
Processing Status	Indicates whether NTA successfully processes a diversion request. Note that "Processed" does not mean that the router or ADS successfully sends a diversion route. In fact, "Processed" only means that NTA successfully sends a diversion request.
Operation	• You can click to add and edit remarks. • You can click to manually revoke the diversion route.

Step 2 Manually revoke BGP FlowSpec diversion routes.

- Revoke a single diversion route.

  Click in the **Operation** column to manually revoke a BGP FlowSpec diversion route.

  After the revocation, the **Diversion Mode** of the route will change to **Manual IP Diversion**, and the route will be automatically removed. A user can view the message about the related diversion among all messages whose **Diversion Mode** is **Manual IP Diversion** on the **FlowSpec Diversion Logs** page under **Logs**.

- Revoke diversion routes in batches.

  Select the check boxes of multiple routes and click **Bulk Withdraw Diversion** to delete these routes in one go.

----End

9.7.3 Group Diversion

Group diversion routes are used for diversion of abnormal traffic received or transmitted by regions and IP groups. Group diversion routes are displayed dynamically. That is, a group diversion route is displayed when abnormal traffic received or transmitted by a region or IP group is diverted according to configured policies, and removed automatically when the diversion is completed.

You can view and manually revoke group diversion routes.

Step 1 Choose **Monitor > Routing Table > Group Diversion**.

A page appears, showing group diversion routes.

Figure 9-31 Group diversion routes

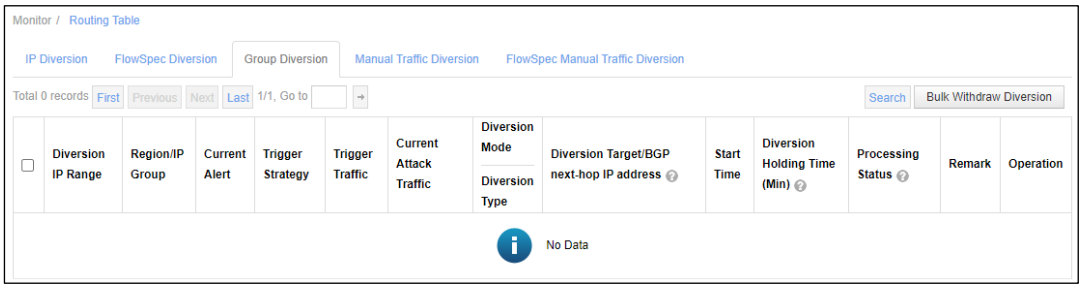


Table 9-12 describes parameters of group diversion routes.

Table 9-12 Parameters of group diversion routes

Parameter	Description
Diversion IP Range	IP address and its subnet mask whose traffic is diverted.
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If such an IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Current Alert	Number of ongoing alerts. Holding the mouse over the number displays alert causes.
Trigger Strategy	Type of the alert that triggers the diversion.
Trigger Traffic	Rate and unit of the traffic that triggers the diversion.
Current Attack Traffic	Current attack traffic.
Diversion Mode/Diversion Type	• **Diversion Mode**: Mode of group diversion, which can only be **Auto Diversion**. • **Diversion Type**: type of group diversion, which can be one of the following: • **ADS Diversion**: indicates that traffic is diverted to ADS devices. • **Null-Route Diversion**: indicates that traffic is diverted to a null-route IP address using BGP. In this case, BGP next-hop IP address is the null-route IP address. • **BGP Diversion**: indicates that traffic is diverted to a protection device using BGP. In this case, the IP address of the protection device is the BGP next-hop IP address.
Diversion Target/BGP next-hop IP address	• When **Diversion Type** is **BGP Diversion**, **BGP Next-Hop IP Address** information shows the IP address of the target protection device of the diversion. • When **Diversion Type** is **Null-Route Diversion**, **BGP Next-Hop IP Address** information shows the null-route IP address of the diversion.
Start Time	Time when traffic diversion starts.
Diversion Holding Time (Min)	Time during which diversion is conducted. This parameter takes effect only when **Diversion Type** is **Null-Route Diversion** or **BGP Diversion**. NTA starts a countdown immediately after sending a null-route/BGP diversion route, and automatically revokes the diversion after the diversion duration expires.
Processing Status	Indicates whether NTA successfully processes a diversion request.

Parameter	Description
	Note that "Processed" does not mean that the router or ADS successfully sends a diversion route. In fact, "Processed" only means that NTA successfully sends a diversion request.
Remark	Necessary supplementary information about the route. If there are remarks, is displayed, and you can view the remarks by moving the mouse over . If there are no remarks, **N/A** is displayed. You can click in the **Operation** column to add and edit remarks.
Operation	• Click to add and edit remarks. • Click to manually revoke the diversion route.

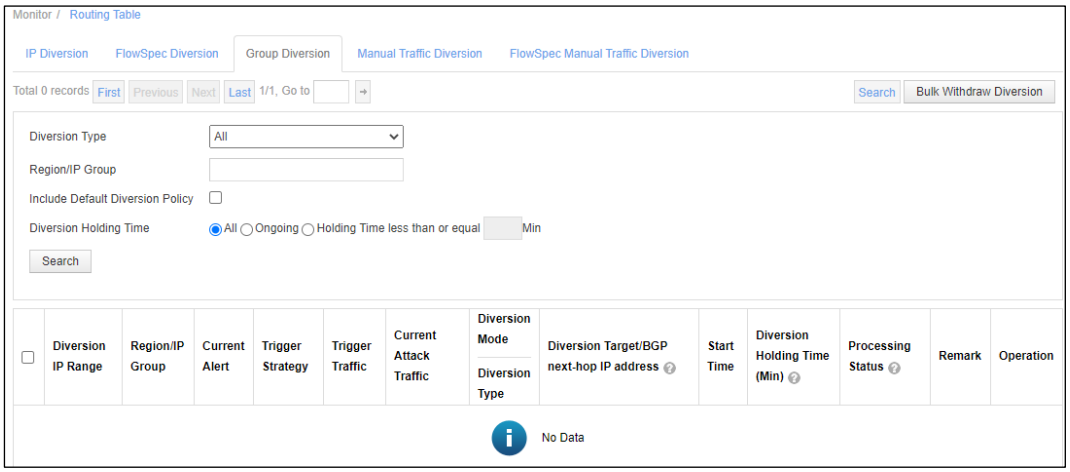
Step 2 Search for desired diversion routes.

If there are many routes, a user can locate specific routes by using the searching function.

a. Click **Search** at the upper-right corner of the page.

An area appears, showing search conditions.

Figure 9-32 Query result of group diversion routes



b. Specify search conditions and click **Search** at the bottom of the area.

Then, only the desired routes satisfying the search conditions are displayed in the table, as shown in Figure 9-32.

Step 3 Manually revoke group diversion routes.

- Revoke a single diversion route.

  Click to manually revoke the diversion route.

  After the revocation, the **Diversion Mode** of the route will change to **Manual Group Diversion**, and the route will be automatically removed. A user can view the log about the related diversion among the logs whose **Diversion Mode** is **Manual Group Diversion** on the **Diversion Logs** page under **Logs**.
- Revoke diversion routes in batches.

Select the check boxes of multiple routes and click **Bulk Withdraw Diversion** to delete these routes in one go.

----End

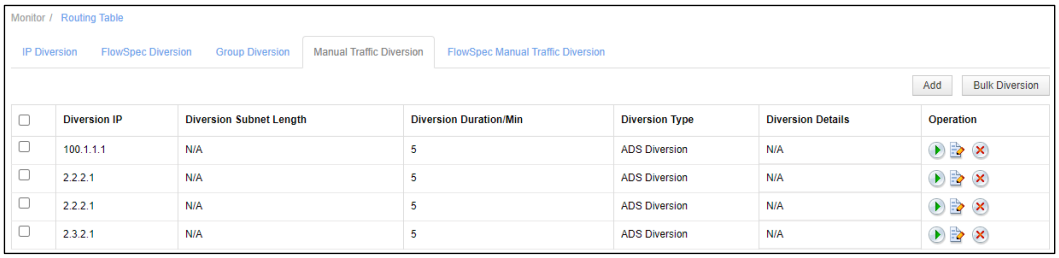
9.7.4 Manual Traffic Diversion

Manual diversion routes refer to static routes that are manually added by users for forced diversion.

Step 1 Choose **Monitor > Routing Table > Manual Traffic Diversion**.

A page appears, showing manual diversion routes.

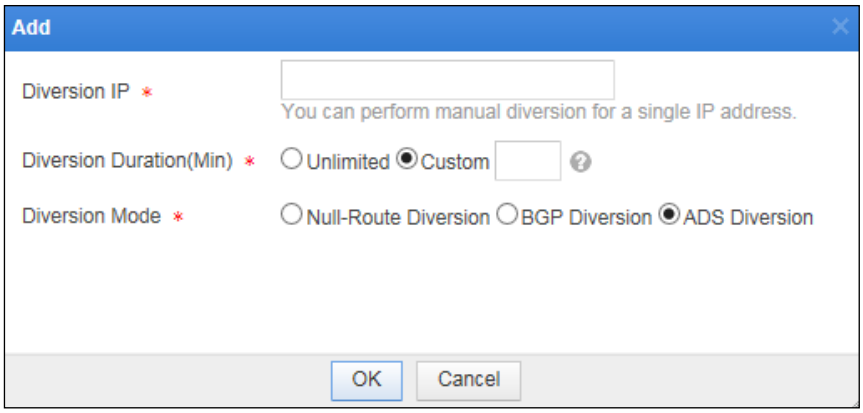
Figure 9-33 Manual diversion routes



Step 2 Add a manual diversion route.

a. Click **Add** in the upper-right corner of the page.

Figure 9-34 Adding a manual diversion route



b. Configure parameters in the **Add** dialog box that appears.

Table 9-13 Parameters for adding a manual diversion route

Parameter	Description
Diversion IP	IP address whose traffic is to be diverted.
Diversion Subnet	Subnet length of the IP address or IP segment whose traffic is to be diverted.

Parameter	Description
Length	This parameter appears and needs to be specified when **Diversion Type** is set to **Null-Route Diversion** or **BGP Diversion**.
Diversion Duration(Min)	Specifies manual diversion duration. It has the following values: • **Unlimited**: specifies that the diversion will last till the administrator manually revokes it. For how to revoke diversion, see section 9.7.1 IP Diversion or 9.7.2 FlowSpec Diversion. • **Custom**: specifies a duration. When the dura tion expires, NTA automatically revokes the diversion. Note For ADS diversion, after receiving a diversion revocation request from NTA, ADS does not immediately revoke diversion. In fact, ADS revoking diversion has nothing to do with whether NTA sends a diversion revocation request. ADS checks for DDoS attacks on its own. If there are DDoS attacks, ADS continues to divert traffic. If there is no DDoS attack, ADS revokes diversion after a 5-minute countdown.
Diversion Mode	Type of diversion, which can be one of the following: • **ADS Diversion**: indicates that NTA diverts attack traffic to ADS. For how to specify such an ADS for this purpose, see section 5.4.3 Protection Device Configuration. • **BGP Diversion**: indicates that NTA sends a BGP routing notification to the router for traffic diversion. For this purpose, you need to select a configured third-party router. For details, see section 5.4.3 Protection Device Configuration. For details about how to configure BGP parameters for sending routing notifications, see section 5.4.2 BGP Configuration. • **Null-Route Diversion**: indicates that NTA will drop attack traffic by diverting it to a null route. When **Null-Route Diversion** is selected, **Null Route IP** appears. You need to select a null-route IP address for the parameter. For details, see section 5.4.2 BGP Configuration.

c. Click **OK** to commit the settings.

Step 3 Dispatch diversion routes.

- Dispatch a single diversion route.

  In the manual diversion route table, click in the **Operation** column of a diversion route. Then the route is dispatched to implement traffic diversion.

  You can click to stop diversion.

- Dispatch diversion routes in batches.

  Select the check boxes of multiple routes and click **Bulk Diversion** to dispatch these routes in one go.

Step 4 Edit a manual diversion route.

In the manual diversion route table, click in the **Operation** column of a diversion route. Then an **Edit** dialog box appears, where you can edit parameters of the route.

Step 5 Delete a manual diversion route.

In the manual diversion route table, click in the **Operation** column of a diversion route and click **OK** in the confirmation dialog box. Then the route disappears from the table.

Step 6 Cancel a manual diversion route.

After a diversion route is dispatched, you can click in the **Operation** column to cancel this route. After this operation, the route will be automatically removed. You can view the log about the related diversion among the logs whose **Diversion Mode** is **Manual Group Diversion** on the **Deiversion Log** page under **Logs**.

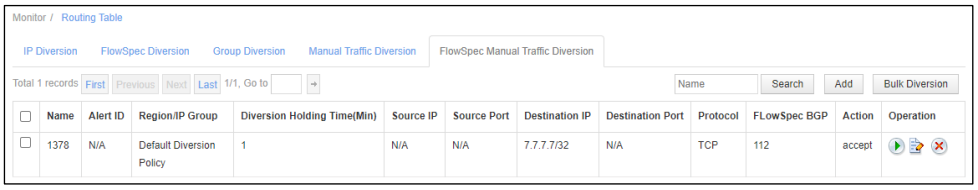
----End

9.7.5 FlowSpec Manual Traffic Diversion

FlowSpec manual diversion routes refer to static routes that are manually added by users for forced diversion via FlowSpec.

Step 1 Choose **Monitor > Routing Table > FlowSpec Manual Traffic Diversion**.

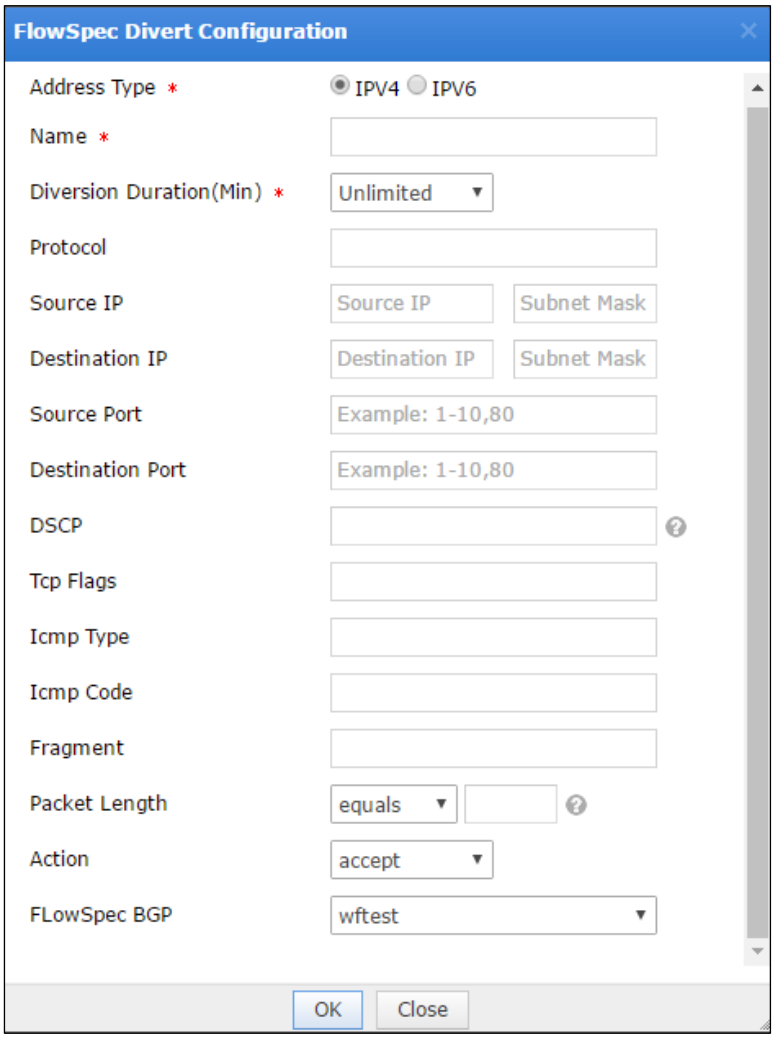
Figure 9-35 FlowSpec Manual Traffic Diversion page



Step 2 Add a FlowSpec manual diversion route.

a. Click **Add** in the upper-right corner.

Figure 9-36 Adding a FlowSpec manual diversion route



b. Configure parameters.

Table 9-14 Parameters for configuring a FlowSpec manual diversion route

Parameter	Description
Address Type	IP address types supported by FlowSpec manual diversion routes.
Name	Number of the FlowSpec manual diversion route.
Diversion Duration(Min)	Specifies the diversion duration, which can be either of the following: • **Unlimited**: indicates no limitation on the diversion duration. • **Custom time**: allows you to set a diversion duration. After a value is specified, NTA will start a countdown when the diversion begins. When the specified duration expires, the diversion automatically stops.
Protocol	Protocol of traffic to be filtered. If one or more protocols are specified here, NTA checks only traffic of the specified protocols. This field is available only when you select **IPV4** for **Address Type**.

Parameter	Description
Source IP	Specifies the source IP address and subnet mask of traffic to be diverted via FlowSpec. Only one source IP address can be configured. After the configuration, NTA checks only traffic from the specified IP address.
Source Port	Source port of traffic to be diverted via FlowSpec. After the configuration, NTA checks only traffic from the specified port.
Destination IP	Specifies the destination IP address and subnet mask of traffic to be diverted via FlowSpec. Only one destination IP address can be configured. After the configuration, NTA checks only traffic to the specified IP address.
Destination Port	Destination port of traffic to be diverted via FlowSpec. After the configuration, NTA checks only traffic to the specified port.
DSCP	Specifies the DSCP value. This field is available only when you select **IPV4** for **Address Type**.
Flow Label	This field is available only when you select **IPV6** for **Address Type**. Specifies a flow label.
Next Header	Specifies the protocol of the next packet header. This field is available only when you select **IPV6** for **Address Type**.
Tcp Flags	Specifies a TCP flag bit.
Icmp Type	Specifies an ICMP type.
Icmp Code	Specifies an ICMP code.
Fragment	Specifies a fragment type. This field is available only when you select **IPV4** for **Address Type**.
Packet Length	Specifies the length of packets to be diverted to be equal to, greater than, or smaller than a value or within a range.
Action	Specifies an action to be taken by NTA on packets that match the preceding settings.
FLowSpec BGP	Specifies a BGP FlowSpec entry from the existing ones.

c. Click **OK** to commit the settings.

Step 3 Dispatch FlowSpec manual diversion routes.

- Dispatch a single diversion route.

  In the route table, click in the **Operation** column of a diversion route. Then the route is dispatched to implement traffic diversion.

- Dispatch diversion routes in batches.

  Select the check boxes of multiple routes and click **Bulk Diversion** to dispatch these routes in one go.

Step 4 Edit a FlowSpec manual diversion route.

In the route list, click in the **Operation** column of a diversion route. Then an **Edit** dialog box appears, where you can edit parameters of the route.

Step 5 Delete a FlowSpec manual diversion route.

In the route table, click in the **Operation** column of a diversion route and click **OK** in the confirmation dialog box. Then the route disappears from the table.

Step 6 Cancel a FlowSpec manual diversion route.

After a diversion route is dispatched, you can click in the **Operation** column to cancel this route. After this operation, the route will be automatically removed. You can view the log about the related diversion among the logs whose **Diversion Mode** is **Manual Group Diversion** on the **Deiversion Log** page under **Logs**.

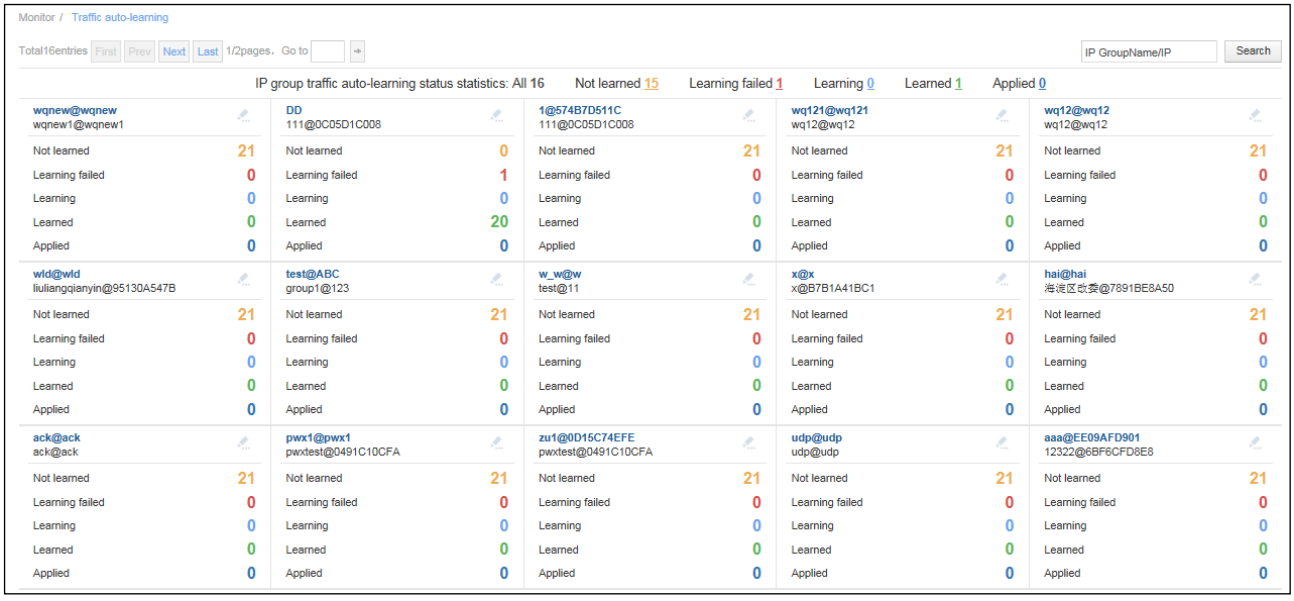
----End

9.8 Traffic Auto-learning

For an IP group with baseline auto-learning enabled, its traffic auto-learning status (such as **Learning**, **Learning failed**, or **Learned**) and learning results**,** are presented on the **Traffic auto-learning** page.

Step 1 Choose **Monitor > Traffic auto-learning**.

Figure 9-37 Monitoring of traffic auto-learning results

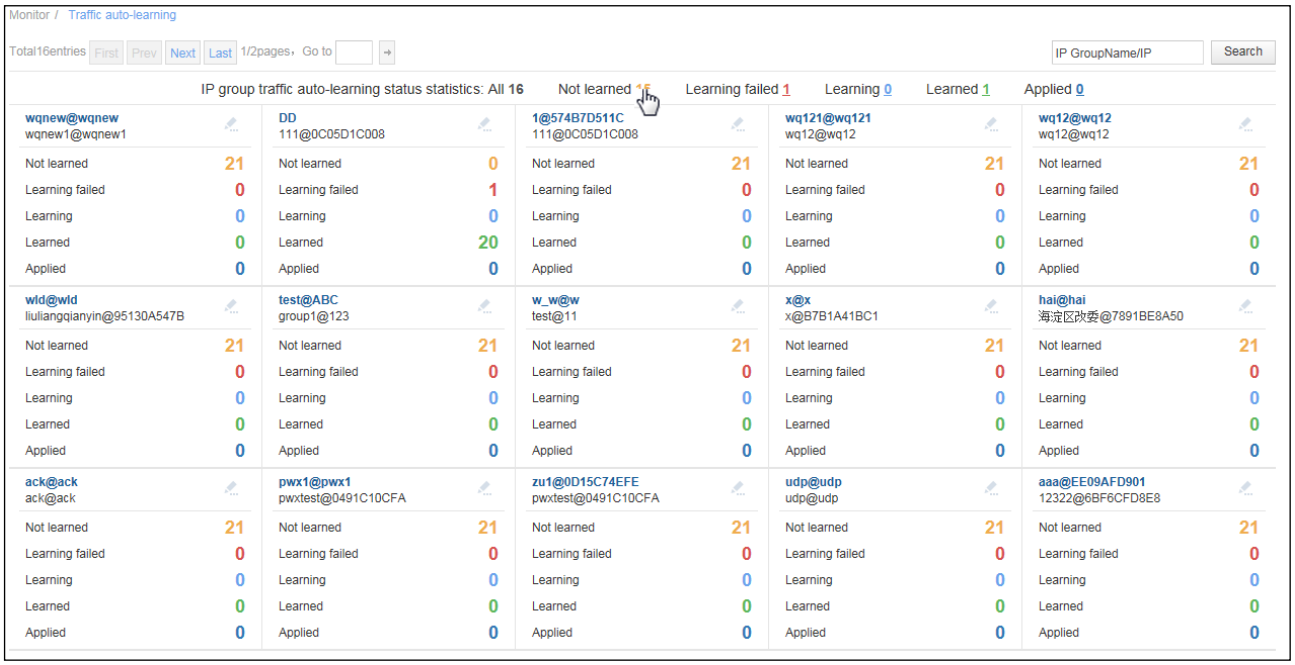


This page presents the traffic auto-learning information of IP groups with baseline auto-learning enabled.

Step 2 View traffic auto-learning information of IP groups by learning status.

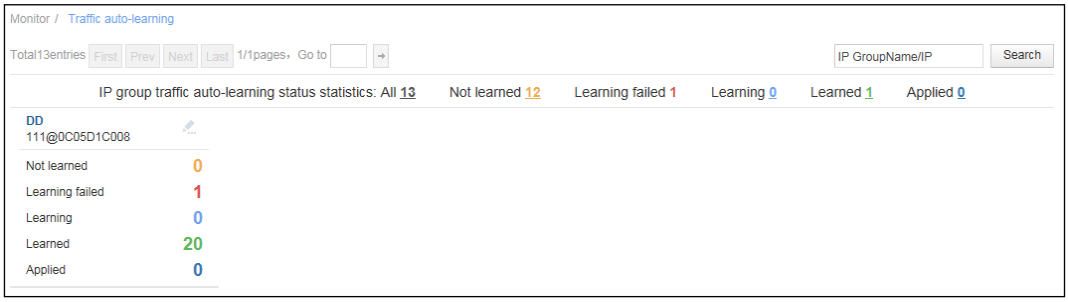
IP group statistics by auto-learning status are listed at the top of the page. Pointing to a number following the status, the mouse pointer will turn to the hand shape from the angled arrow, as shown in Figure 9-38.

Figure 9-38 Viewing auto-learning results of all IP groups



Clicking the number after the learning status shows statistics of IP groups in this specific learning state. For example, clicking the number next to **Learning** displays traffic auto-learning information of all IP groups in the Learning state, as shown in Figure 9-39.

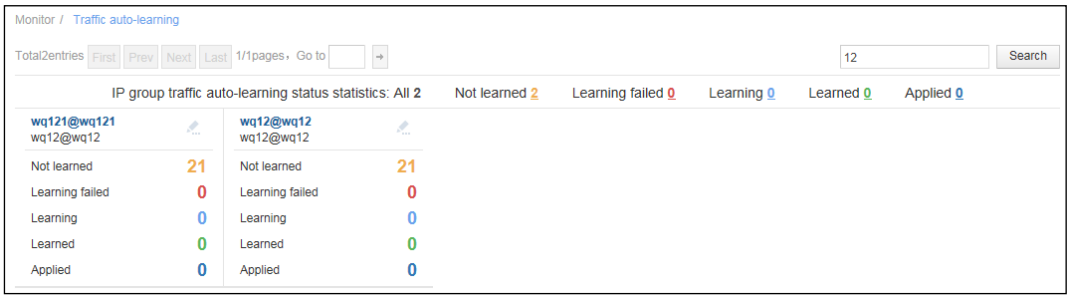
Figure 9-39 Viewing auto-learning results of IP groups in a specific learning state



Step 3 Search for IP groups.

Fuzzy search is supported. That is to say, after you type part of an IP group name and click **Search**, the system presents traffic auto-learning statistics of IP groups with names including your input. See Figure 9-40.

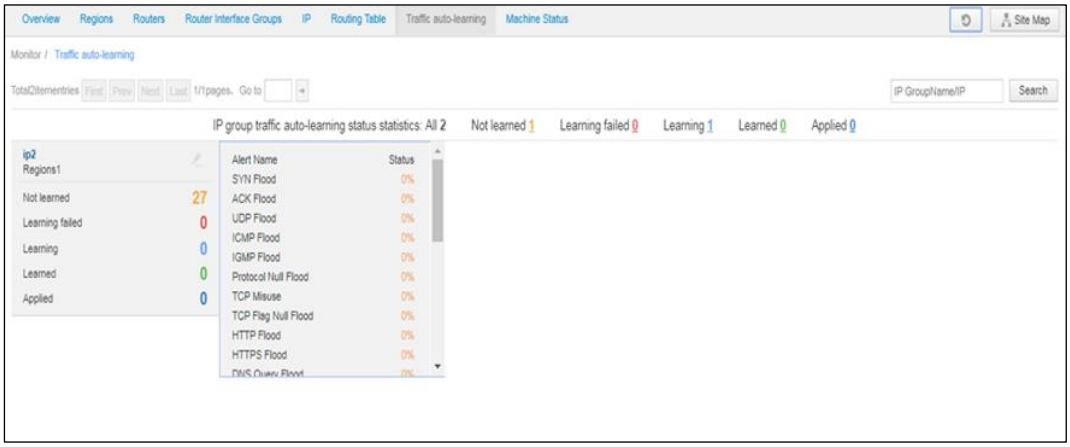
Figure 9-40 Checking search results



Step 4 View DDoS attack alerts of an IP group.

Pointing to an IP group, you can check DDoS attack alerts of this IP group.

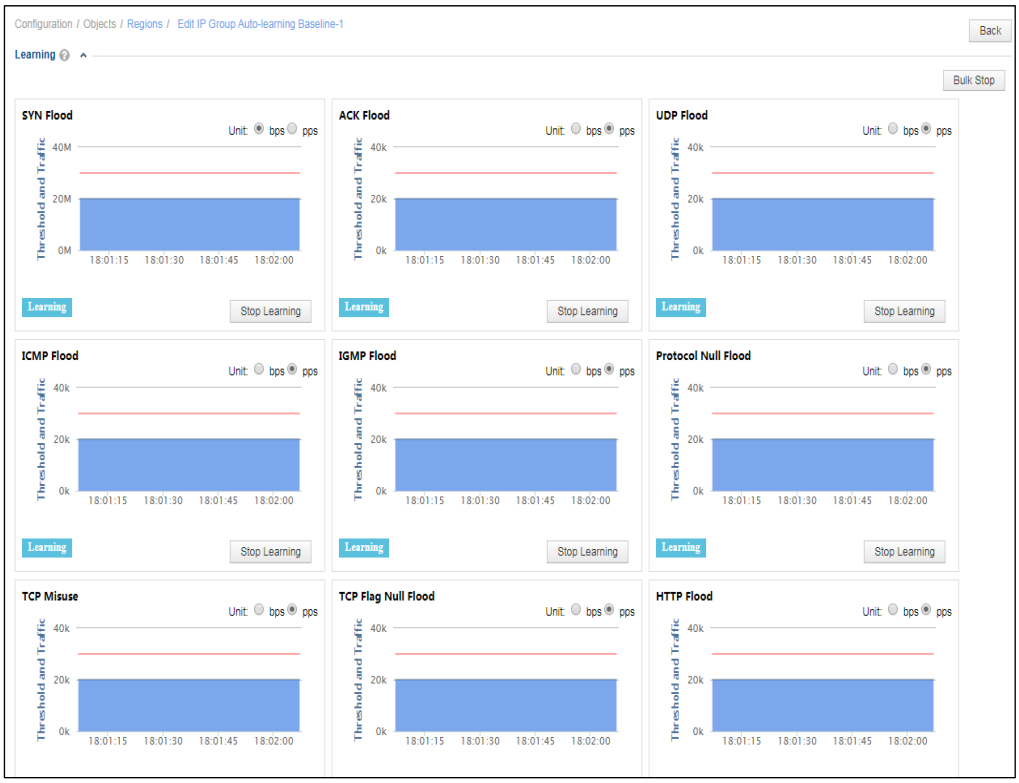
Figure 9-41 Viewing DDoS attack alerts of an IP group



Step 5 View the auto-learning baseline configuration of an IP group.

You can click to view learning baseline configuration of an IP group, as shown in Figure 9-42. For details, see "Configuring the Auto-Learning Baseline" in section 5.1.3.7 Configuring an IP Group and Related Policies.

Figure 9-42 Editing auto-learning baseline settings of an IP group



----End

9.9 Local Status

The Machine Status module presents the system status, basic information, system service, and interface status of the local NTA.

To view the status of the local machine, follow these steps:

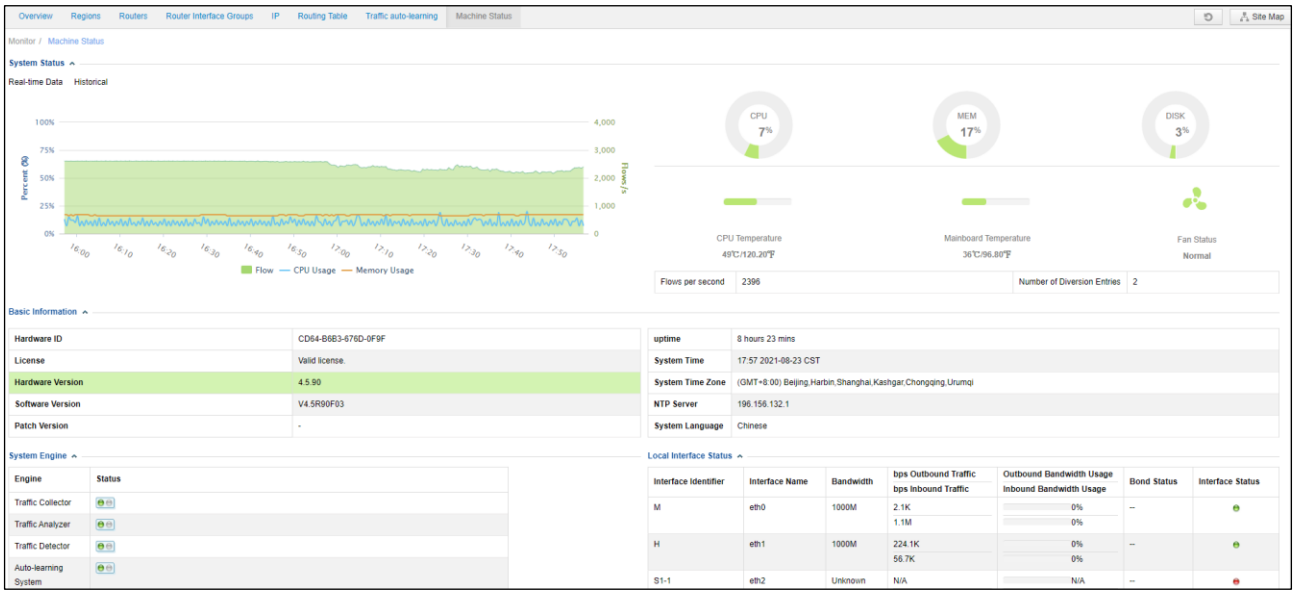
Step 1 Choose **Monitor > Machine Status**.

The **Machine Status** page appears, consisting of five parts:

- System Status
- Basic Information
- System Engine
- Local Interface Status
- Real-Time System Information

Note	The **Machine Status** page of vNTA does not show the CPU temperature, mainboard temperature, and fan status.

Figure 9-43 Machine Status page



System Status

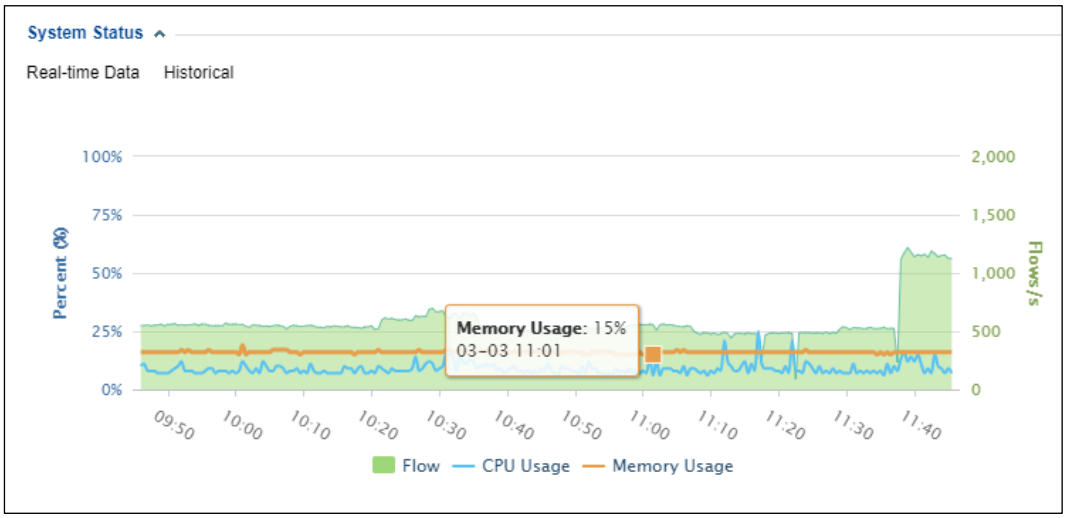
This area displays real-time data in last two hours by default. You can click **Historical** and specify a period to view desired data.

The left chart, as shown in Figure 9-43, displays trends of flow rates and resource usage:

- **Flow**: trend of the average rate at which flow packets are received every 30 seconds
- **CPU Usage**: CPU usage trend
- **Memory Usage**: memory usage trend

Pointing to a specific position on a curve displays the specific CPU usage, memory usage, or the number of flows at that specific moment, as shown in Figure 9-44. There are three items at the bottom of the chart. You can click any of the three items to remove the related curve from the chart, and re-click the item to add the related curve back to the chart. For example, if you click **Memory Usage**, the memory usage curve disappears from the chart and **Memory Usage** turns to gray, as shown in Figure 9-44.

Figure 9-44 Left chart in the System Status area



The right chart, as shown in Figure 9-43, displays the current system status, including the system CPU, memory, and disk usage, CPU temperature, motherboard temperature, and fan status.

- **Flows per second**: average rate at which flow packets are received in the past 30 seconds.
- **Number of Diversion Entries**: number of IP addresses whose traffic is being diverted.

Basic Information

This area displays basic NTA information, as described in Table 9-15.

Table 9-15 Basic NTA information.

Parameter	Description
Hardware ID	Unique hardware ID of NTA.
License	Indicates whether a correct license has been imported. If yes, **Valid license** is displayed. For how to import a license, see section 4.8 License.
Hardware Version	Current firmware version of NTA.
Software Version	Current software version of NTA.
Patch Version	Version of the patch that was last installed on NTA, if NTA has been upgraded by installing patch files.
Uptime	Duration since the system's last startup till now.
System Time	Time of the system's internal clock. You can change the system time to your local time zone. For details, see section 4.1.1.1 Configuring Basic Information.
System Time Zone	Time zone of the system's internal clock. You can change the system time zone to your local time zone. For details, see section 4.1.1.1 Configuring Basic Information.
NTP Server	NTP server used for system time synchronization. You can change the NTP server based on your network environment. For details, see section 4.1.1.1 Configuring Basic Information.

Parameter	Description
System Language	Default language of the system's GUI. You can change the default system language. For details, see section 4.1.1.1 Configuring Basic Information.

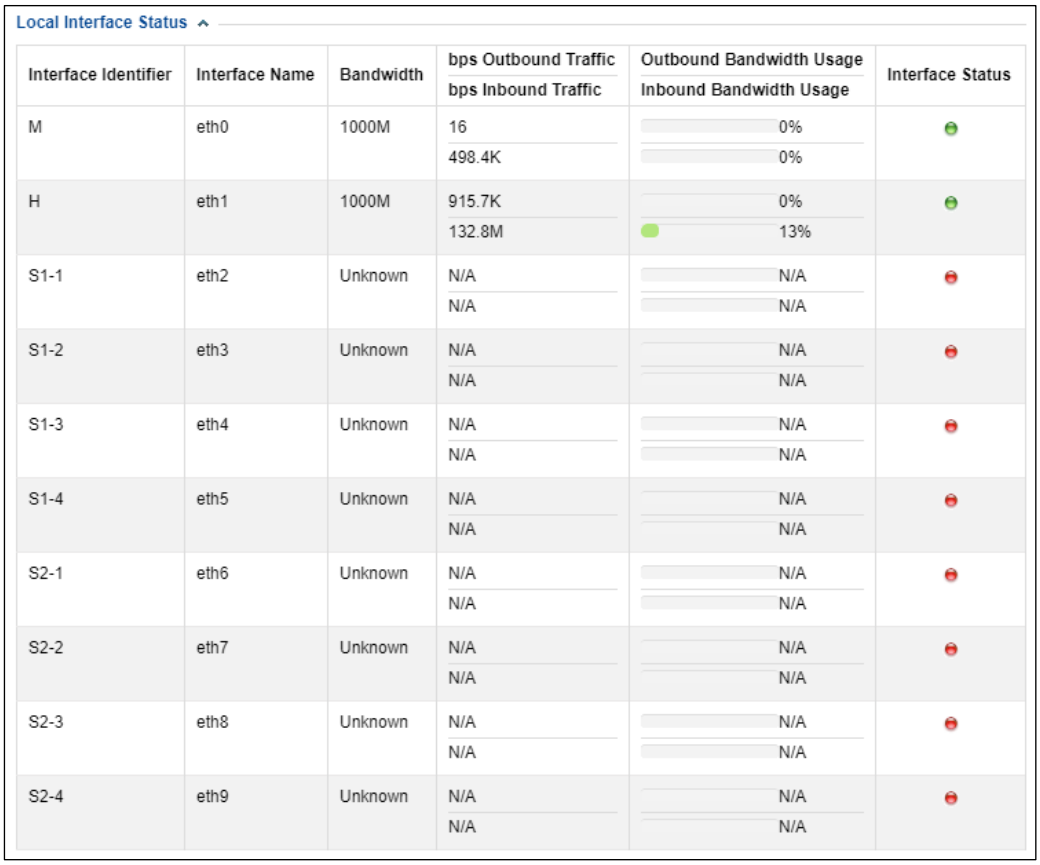
System Engine

This area shows service status, that is, whether a service is enabled or disabled. For how to enable or disable a service, see section 4.1.1.3 Configuring System Engines.

Local Interface Status

This area shows information about physical interfaces on NTA.

Figure 9-45 Local interface status



For descriptions of the parameters of local interface status, see Table 4-2.

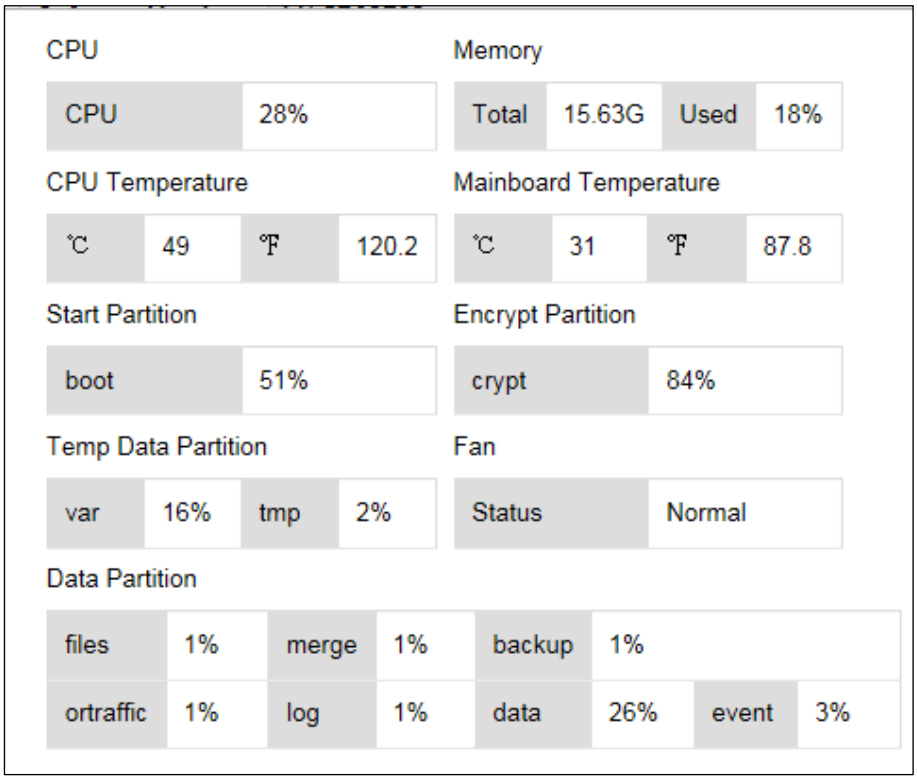
Real-Time System Information

The status bar at the bottom of the page dynamically shows real-time system information, including CPU usage, memory usage, disk usage, system uptime, system time, and license validity.

- Clicking the left part of the status bar displays more information, including CPU usage, memory usage, CPU temperature, motherboard temperature, fan status, and usage of each partition, as shown in Figure 9-46.

Note	The **System Engine Status** page of vNTA does not show the CPU temperature, mainboard temperature, and fan status.

Figure 9-46 More system information



- Clicking **Valid license** displays the **License** page on which you can view license information. For details, see section 4.8 License.

Step 2 To obtain the latest local status information, click in the upper-right corner of the page.

----End

10 Console-based Management

Via the console port, the console administrator (**admin**) can access the console user interface of NTA and perform basic operations, such as initial system configurations, status detection, and restoration of initial configurations. When failing to log in to the web-based manager or perform certain management via the web-based manager, you can manage NTA via the console user interface.

For details about how to log in to the console user interface, see section 3.2.2 Login.

Note	You can run a command in the format of "upper-level command+space+?", for example, **net ?**, to view all available lower-level commands under the upper-level command.

This chapter describes common configurations for console-based NTA management, containing the following sections:

Section	Description
Configuring the Network	Describes how to configure the network via commands.
Viewing or Configuring System Time	Describes how to configure system time via a command.
Controlling System Engines	Describes how to control system engines via a command.
Configuring the ACL	Describes how to configure the ACL via a command.
Resetting the Console Password	Describes how to reset the password for login to the console user interface via a command.
Viewing System Configurations	Describes how to view system configurations via a command.
Controlling the Web Service	Describes how to control the web service via a command.
Performing System Management	Describes how to perform system management via a command.
Enabling/Disabling PPPoE Interfaces	Describes how to enable/disable PPPoE interfaces.

Section	Description
Restarting the Device	Describes how to restart the device via a command.
Powering Off the Device	Describes how to power off the device via a command.
Exiting the Privileged Mode	Describes how to exit the privileged mode via a command.
Exiting the Console	Describes how to exit and close the console user interface via a command.
Viewing the Help Information of the Console	Describes how to view the help information of the console user interface via a command.
Enabling/Disabling Cloud-based Authentication	Describes how to enable or disable cloud-based authentication.
Viewing System Logs	Describes how to view system logs via a command.
Viewing Resources Consumed by Processes	Describes how to view NTA resources consumed by processes via a command.

10.1 Configuring the Network

Step 1 After entering the privileged mode, type **net ?** and press **Enter**.

The network configuration menu appears, as shown in Figure 10-1.

Figure 10-1 Network configuration 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
```

Type one of the following digits to use the corresponding function:

- **1**: View the existing network settings.
- **2**: Add an interface IP address.
- **3**: Delete an interface IP address.
- **4**: Enter a default gateway.
- **5**: Add a route.
- **6**: Delete a route.
- **7**: Add a DNS server.
- **8**: Restore the default network configuration.

- **0**: Exit the network configuration.

10.1.1 Viewing Network Settings

Type **1** and press **Enter** to view the existing network settings, as shown in Figure 10-2.

Figure 10-2 Existing network settings

```
> 1
inet family
+-------------------------------------------------------------+
|   adapter|                                IP|           netmask|
+-------------------------------------------------------------+
Default gateway: None

inet6 family
+-------------------------------------------------------------+
|   adapter|                                IP|         prefixlen|
+-------------------------------------------------------------+
|      eth0|      fe80::210:f3ff:fe2d:2c8c|                64|
+-------------------------------------------------------------+
Default gateway: None

Domain name servers: 8.8.8.8

IPv4 route
+-------------------------------------------------------------------------+
|No      Destination          Gateway          Genmask  Flags Iface|
+-------------------------------------------------------------------------+

IPv6 route
+-------------------------------------------------------------------------------------+
|No                     Destination                          Gateway  Flags Iface|
+-------------------------------------------------------------------------------------+
```

10.1.2 Adding an Interface IP Address

Step 1 After entering the network configuration menu in privileged mode, type **net ?** and press **Enter**.

Step 2 Add an interface IP address.

Type **2** to add an interface IP address, which can be either an IPv4 or IPv6 address.

a. Determine the format of the IP address.

Type **1** for the IPv4 format or **2** for the IPv6 format.

b. Select the interface number.

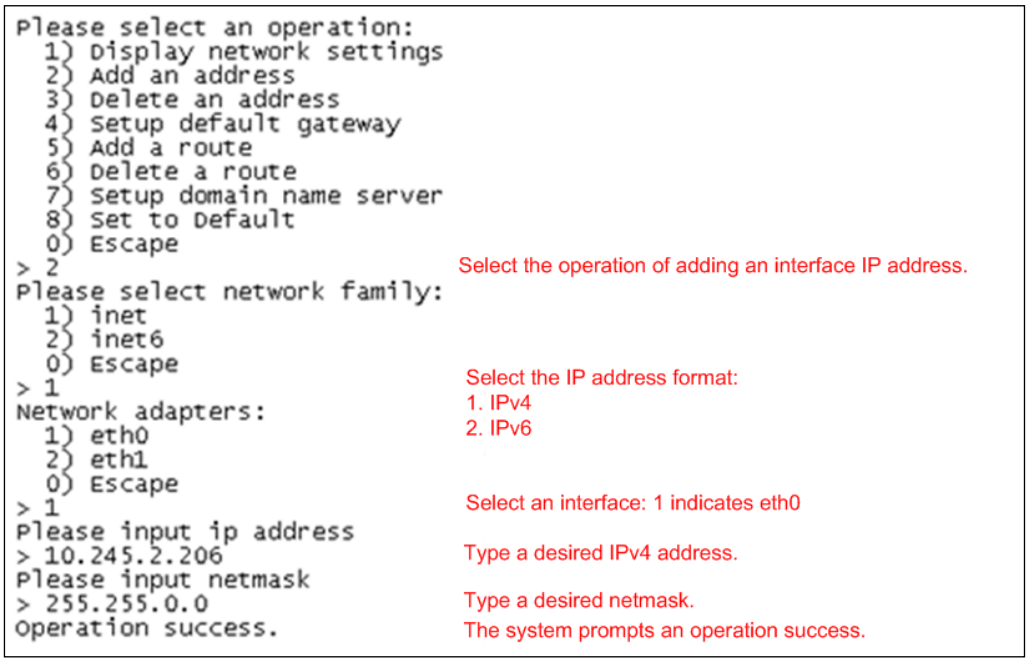
The value **1** indicates eth0, **2** indicates eth1, and **0** indicates the exit of the configuration.

c. Configure an IP address.

Type an IP address as prompted and press **Enter**. For an IPv4 address, you need to type the subnet mask. For an IPv6 address, you need to type the prefix length.

d. Configure the gateway address.

Figure 10-3 Configuring an IPv4 address of an interface



Step 3 Delete an interface IP address.

Type **3** to delete an interface IP address, which can be either an IPv4 or IPv6 address. See Figure 10-4.

Figure 10-4 Deleting an interface IP address

```
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
> 3
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Network adapters:
  1) eth0
  2) eth1
  0) Escape
> 1
Please select an ip address
  1) 192.168.1.100/255.255.255.0
  2) 10.245.2.206/255.255.0.0
  0) Escape
> 2
Are you sure to delete 10.245.2.206/255.255.0.0 from eth0?[y/n]
> y
Operation success.
```

----End

10.1.3 Configuring a Route

Default routes and non-default routes are configured using different commands.

- Figure 10-5 shows how to configure a default IPv4 route.

Figure 10-5 Configuring a default IPv4 route in privileged mode

```
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
> 4                                  Select the operation of adding a default route.
Please select network family:        Select the protocol stack:
  1) inet                            1. IPv4
  2) inet6                           2. IPv6
  0) Escape
> 1
Please input default gateway address
> 10.245.255.254                    Type the IP address of the gateway.
Operation success.
```

- Figure 10-6 shows how to configure a default IPv6 route.

Figure 10-6 Configuring a default IPv6 route in privileged mode

```
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
> 5
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Please input destination(IP or network)
> 10.30.2.10
Please input gateway
> 10.245.1.1
Network adapters:
  1) auto
  2) eth0
  3) eth1
  0) Escape
> 2
Operation success.
```

10.1.4 Configuring DNS Servers

Figure 10-7 shows how to configure DNS servers on the console-based manger.

Figure 10-7 Configuring DNS servers in privileged mode

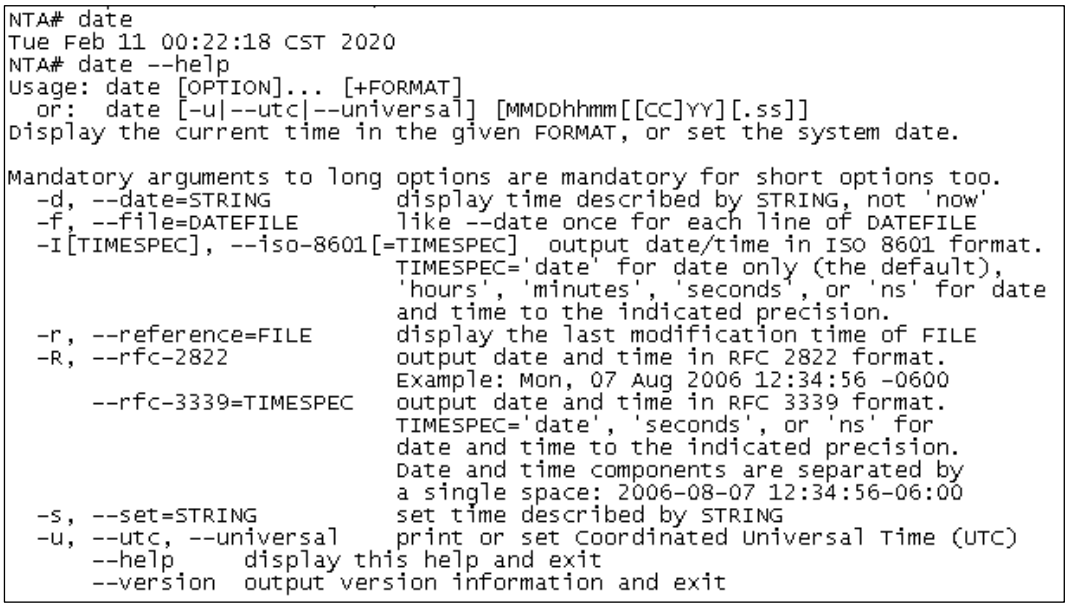
```
NTA# net

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
> 7                                          Select the operation of adding DNS servers.
Please input 1-2 domain server ip address:
> 8.8.8.8                                    Type the IP address of one or two DNS servers.
```

10.2 Viewing or Configuring System Time

You can run the **date** command to view or configure the system time.

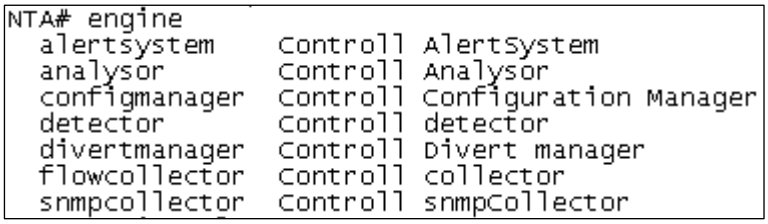
Figure 10-8 Configuring system time



10.3 Controlling System Engines

You can run the **engine** command to control NTA engines.

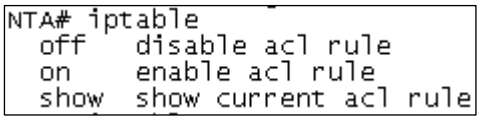
Figure 10-9 Controlling system engines



10.4 Configuring the ACL

You can run the **iptable** command for ACL management.

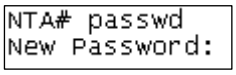
Figure 10-10 Configuring the ACL



10.5 Resetting the Console Password

You can run the **passwd** command to reset the password for login to the console user interface.

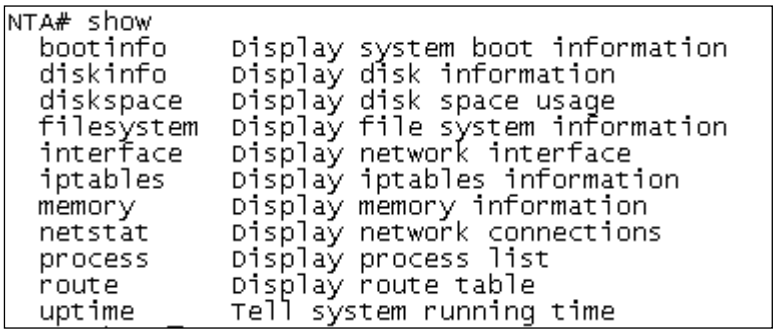
Figure 10-11 Resetting the login password of the console user interface



10.6 Viewing System Configurations

You can run the **show** command to view basic system information, as shown in Figure 10-12.

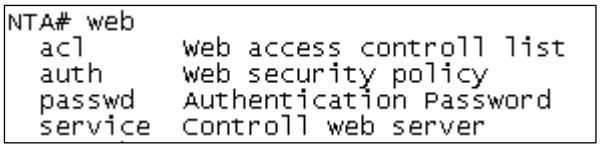
Figure 10-12 Viewing system configuration



10.7 Controlling the Web Service

You can run the **web** command for web service control.

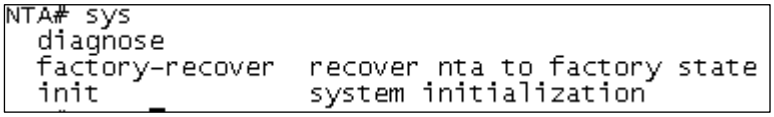
Figure 10-13 Controlling the web service



10.8 Performing System Management

You can run the **sys** command for system management.

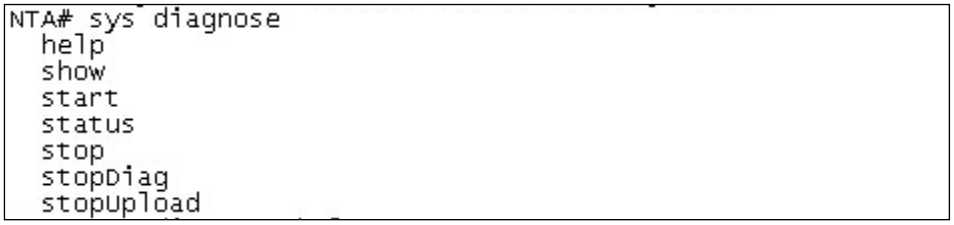
Figure 10-14 Performing system management



10.8.1 Configuring One-Click Fault Collection

You can run the **sys diagnose** command to configure fault collection, as shown in Figure 10-15.

Figure 10-15 Configuring one-click fault collection



You can perform the following operations:

- Collect fault information.

  The command is as follows:

```
#sys diagnose start-s [source] -x [proto] -u [username] -p [password] -P [port]
-h [host] -o [destination]
```

Table 10-1 describes parameters in this command.

Table 10-1 Parameters in the sys diagnose start command

Parameter	Description
-s [source]	This parameter is optional. The function of this command depends on whether this parameter is set: • If this parameter is not set, this command collects fault information and uploads the collected fault logs. • If this parameter is set, this command uploads the specified fault information. In this case, **source** specifies the target fault information file.
-x [proto]	Specifies the protocol through which fault information is uploaded. The value can be **ftp**, **scp**, or **sftp**. This parameter is optional.
–u [username] -p [password]	Specifies the user name and password for uploading fault information. This parameter is optional.
-P [port]	Specifies the destination port number to which fault information is uploaded. This parameter is optional.
-h [host]	Specifies the destination IP address to which fault information is uploaded. This parameter is optional.
-o [destination]	Specifies the destination path to which fault information is uploaded. This parameter is optional.

b. Collect but not upload fault information.

```
#sys diagnose start
```

c. Upload but not collect fault information.

Note	The ongoing fault collection will be stopped during upload.

You can use the FTP protocol to upload the fault information file, **failure_info_20140620173330.bin**, to the tmp directory of the host 10.66.13.41:

```
#sys diagnosestart -s failure_info_20140620173330.bin -x ftp -u admin -p nsfocus123
-P 2 -h 10.66.13.41 -o /tmp/
```

d. Collect fault information and use the FTP protocol to upload fault information to the **tmp** directory of the host 10.66.13.41:

```
#sys diagnose start -x ftp -u admin -p nsfocus123 -P 21 -h 10.66.13.41 -o /tmp/
```

- Check whether fault information is being collected or uploaded.

```
#sys diagnose status
```

- Stop both fault collection and upload:

```
#sys diagnose stop
```

- Stop fault collection:

```
#sys diagnose stopdiag
```

- Stop fault information upload:

```
#sys diagnose stopupload
```

- Display the encrypted fault information file:

```
#sys diagnose show
```

10.8.2 Restoring Factory Settings

You can run the **sys factory-recover** command to restore NTA to factory settings, as shown in Figure 10-16.

Figure 10-16 Restoring factory settings

```
NTA# sys factory-recover
  <cr>
```

10.9 Enabling/Disabling PPPoE Interfaces

You can run the **set pppoe on / off** command to enable/disable PPPoE interfaces, as shown in Figure 10-17. After enabling PPPoE interfaces, you can view the number of the PPPoE interfaces by choosing **Configuration > Objects > Routers** or **Monitor > Routers**.

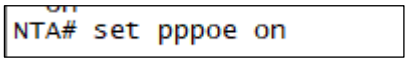
To enable/disable PPPoE interfaces, perform the following steps:

Step 1 Delete all rounters on the web-based manager. For details, see 5.1.1 Router.

Step 2 Run the **set pppoe on / off** command to enable/disable PPPoE interfaces in the console.

Step 3 Add the desired router on the web-based manager. For details, see 5.1.1 Router.

Figure 10-17 set pppoe on

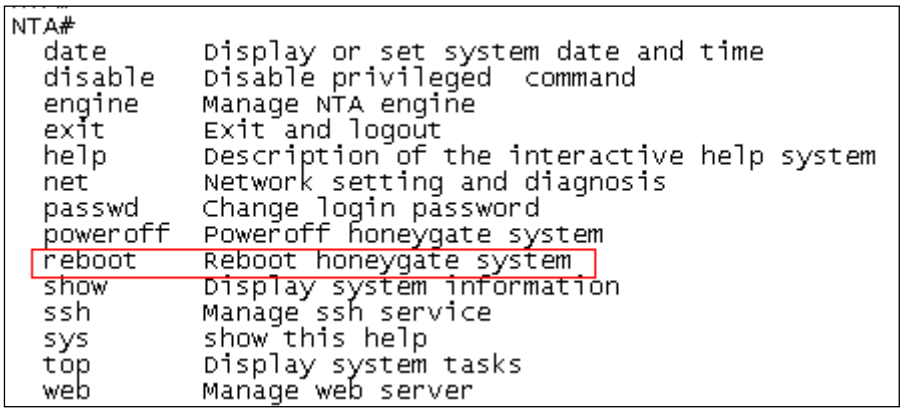


----End

10.10 Restarting the Device

You can run the **reboot** command to restart the system, as shown in Figure 10-18.

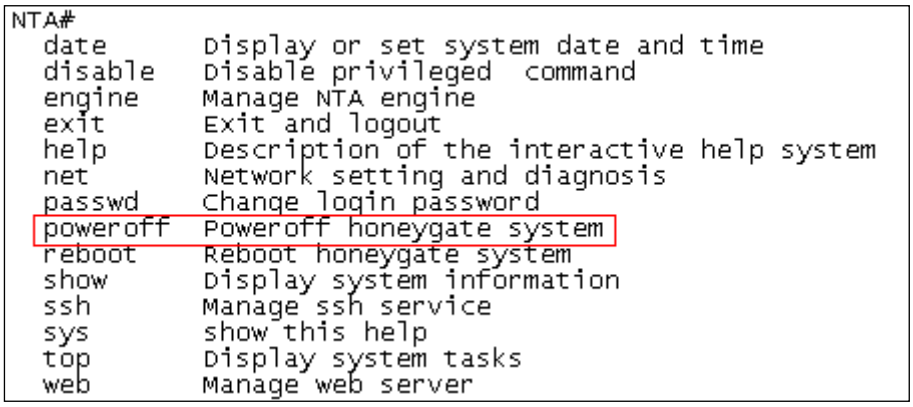
Figure 10-18 Restarting the system.



10.11 Powering Off the Device

You can run the **poweroff** command to power off the device, as shown in Figure 10-19.

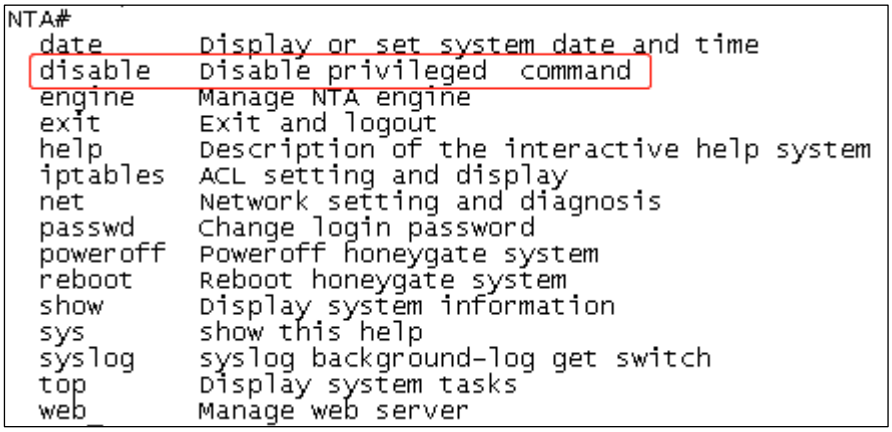
Figure 10-19 Powering off the device



10.12 Exiting the Privileged Mode

You can run the **disable** command to exit the privileged mode.

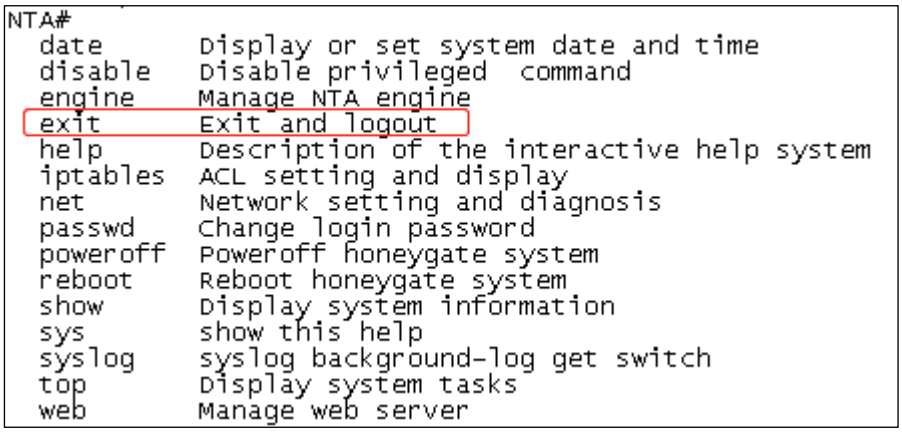
Figure 10-20 Exiting the privileged mode



10.13 Exiting the Console

You can run the **exit** command to exit the console user interface.

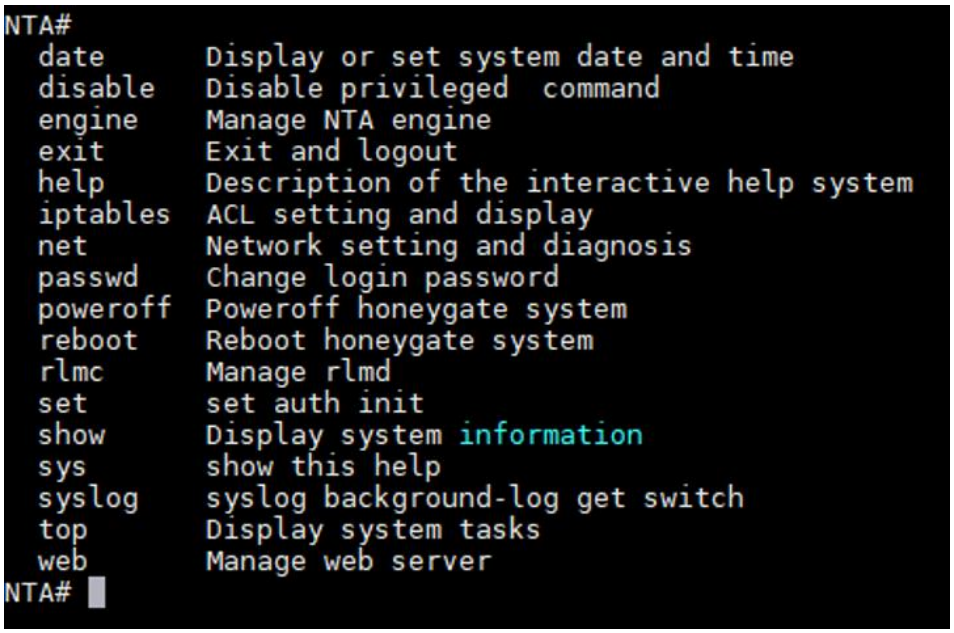
Figure 10-21 Exiting the console user interface



10.14 Viewing the Help Information of the Console

You can run the **help** command to view the help information of the console.

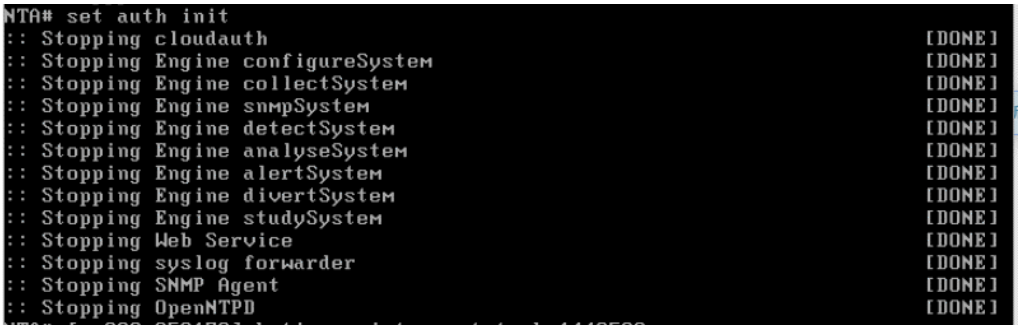
Figure 10-22 Viewing the help information of the console



10.15 Enabling/Disabling Cloud-based Authentication

You can run the **set auth init** command to enable or disable cloud-based authentication.

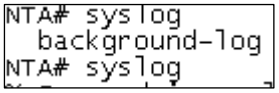
Figure 10-23 Enabling/disabling cloud-based authentication



10.16 Viewing System Logs

You can run the **syslog** command to view system logs.

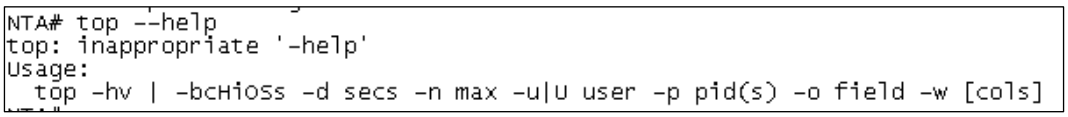
Figure 10-24 Viewing system logs



10.17 Viewing Resources Consumed by Processes

You can run the **top** command to view NTA resources consumed by processes.

Figure 10-25 Viewing NTA resources consumed by processes



A Abbreviations

Abbreviation	Full Spelling
AS	autonomous system
ADS	Anti-DDoS System
ADS M	NSFOCUS Anti-DDoS System Management
BGP	Border Gateway Protocol
bps	bits per second
pps	packets per second
DDoS	distributed denial of service
DNS	Domain Name System
HTTP	Hyper Text Transfer Protocol
IDC	Internet data venter
IP	Internet Protocol
SSH	Secure Shell
NTP	Network Time Protocol
NTA	Network Traffic Analyzer
ESPC	Enterprise Security Planning Customer
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
Spap	Shiva Password Authentication Protocol
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol

B Default Parameters

B.1 Default Network Settings

B.1.1 Default Settings of Local Interfaces

eth0 (M interface)	192.168.1.100/255.255.255.0
Other Interfaces	No IP address configured

B.1.2 Default Route Settings

IPv4 Default Gateway	192.168.1.1
IPv6 Default Gateway	None

B.2 Default Administrator Accounts

B.2.1 Web Operator

User Name	admin
Password	

B.2.2 Web Auditor

User Name	auditor
Password	

B.2.3 Console Administrator

User Name	admin
Password	

B.2.4 SSH Administrator

User Name	conadmin
Password	k@eT!23i
SSH Service Port	50022

B.3 Communication Parameters of the Console Port

Baud Rate	115200
Data Bits	8

B.4 Flow Collecting and Forwarding

NetFlow/NetStream/IPFIX Collecting Port	9999
sFlow Collecting Port	6343

C IPv4/IPv6 Support

The following table lists NTA's support for IPv4 and IPv6.

Function		IPv4	IPv6
Web login	Web login	√	√
Third-party interface	email	√	√
	snmp	√	√
	syslog	√	√
	Cloud platform	√	×
	Third-party cloud platform	√	√
	bsa	√	×
	Cloud cleaning	√	×
	Management mode	√	√
	ATM	√	×
	NTI	√	×
Network interface configuration	Interface configuration IPv6	√	√
	Route	√	√
	DNS server	√	√
System configuration	NTP server	√	√
Diagnosis tools	ping	√	√
	traceroute	√	√
	telnet	√	√
User management	acl	√	√
	Web API whitelist	√	√
	Radius authentication	√	×
Hot standby	HA	√	√

Function		IPv4	IPv6
Core business	Detection alerts	√	√
	Alert whitelist	√	√
	Diversion	√	√
	Flow settings	√	√
	Routers	√	√
	Regions	√	√
	IP groups	√	√
	Protection device configuration	√	√
	BGP configuration	√	√
Reports	Reports	√	√