

Hillstone Networks, Inc.

StoneOS WebUI Guide

Version 5.5R5



Copyright 2017 Hillstone Networks, Inc.. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks, Inc..

Hillstone Networks, Inc.

Contact Information:

US Headquarters:

Hillstone Networks

5201 Great America Pkwy, #420

Santa Clara, CA 95054

Phone: 1-408-508-6750

<http://www.hillstonenet.com/about-us/contact/>

About this Guide:

This guide gives you comprehensive configuration instructions of Hillstone Networks, Inc. StoneOS .

For more information, refer to the documentation site: <http://docs.hillstonenet.com>.

To provide feedback on the documentation, please write to us at:

hs-doc@hillstonenet.com

Hillstone Networks, Inc.

TWNO: TW-WUG-UNI-A-5.5R5-EN-V1.0-2017/12/15

Contents

Contents	1
Welcome	1
Chapter 1 Getting Started Guide	2
Initial Visit to Web Interface	3
Preparing the StoneOS System	4
Installing Licenses	4
Creating a System Administrator	4
Adding Trust Hosts	5
Upgrading StoneOS Firmware	6
Updating Signature Database	6
Connecting to Internet Under Routing Mode	7
Restoring Factory Settings	11
Restoring using a pin	11
Restoring via WebUI	11
Chapter 2 Deploying Your Device	12
How a Firewall Works	13
StoneOS System Architecture	13
General Rules of Security Policy	14
Packet Processing Rule	14
Forwarding Rule in Layer 2	14
Forwarding Rule in Layer 3	16
Deploying Transparent Mode	18
Deploying Routing Mode	22
Deploying Mix Mode	26
Deploying Tap Mode	27
Chapter 3 Dashboard	29
Network Risk Status	29
Threatscape	29
Threat Map of External Attacker	30
Threats	30
Critical Assets	30
My Threats	31
Application	31
Total Traffic/Concurrent Sessions/New Sessions	31
System Alarm	31
Physical Interface	32

System Information	32
Specified Period	33
Chapter 4 iCenter	34
Critical Assets	34
Risky Hosts	36
Threat	37
Mitigation	42
Chapter 5 Network	43
Security Zone	44
Configuring a Security Zone	44
Interface	46
Configuring an Interface	47
Creating a PPPoE Interface	47
Creating a Tunnel Interface	50
Creating a Virtual Forward Interface	54
Creating a Loopback Interface	57
Creating an Aggregate Interface	59
Creating a Redundant Interface	63
Creating an Ethernet Sub-interface/an Aggregate Sub-interface/a Redundant Sub-interface	63
Creating a VSwitch Interface/a VLAN Interface	65
Editing an Interface	66
MGT Interface	71
Configuring a MGT Interface	71
VLAN	72
Configuring a VLAN	72
DNS	73
Configuring a DNS Server	73
Configuring a DNS Proxy	73
Configuring an Analysis	74
Configuring a DNS Cache	74
NBT Cache	75
DHCP	77
Configuring a DHCP Server	77
Configuring a DHCP Relay Proxy	80
DDNS	81
Configuring a DDNS	81
PPPoE	83
Configuring PPPoE	83
Virtual Wire	85

Configuring a Virtual-Wire	85
Configuring the Virtual Wire Mode	85
Virtual Router	87
Creating a Virtual Router	87
Global Configuration	87
Virtual Switch	89
Creating a VSwitch	89
Port Mirroring	90
Outbound Link Load Balancing	91
Configuring LLB Profile	91
Configuring LLB Rule	92
Configuring DNS Balance	93
Inbound Link Load Balancing	94
Creating a SmartDNS Rule Table	94
Application Layer Gateway (ALG)	96
Enabling ALG	96
Global Network Parameters	97
Configuring Global Network Parameters	97
Configuring Protection Mode	98
Chapter 6 Advanced Routing	100
Destination Route	101
Creating a Destination Route	101
Destination-Interface Route	102
Creating a Destination-Interface Route	102
Source Route	104
Creating a Source Route	104
Source-Interface Route	106
Creating a Source-Interface Route	106
ISP Profile	108
Creating an ISP Profile	108
Uploading an ISP Profile	108
Saving an ISP Profile	109
ISP Route	110
Creating an ISP Route	110
Policy-based Route	112
Creating a Policy-based Route	112
Creating a Policy-based Route Rule	112
Adjusting Priority of a PBR Rule	115
Applying a Policy-based Route	116

DNS Redirect	117
Configuring the Global Match Order	117
WAP Traffic Distribution	117
Enabling WAP Traffic Distribution	118
Configuring a DNS Server	118
Creating Host Book	118
Creating a Policy-based Route Rule	118
Video Streaming Redirection	118
RIP	120
Creating RIP	120
Chapter 7 Authentication	123
Authentication Process	123
Web Authentication	124
Using WebAuth Wizard	124
Configuring Global Parameters for WebAuth	125
NTLM Authentication	127
Modifying WebAuth Page	129
Single Sign-On	131
Enabling SSO Radius for SSO	131
Using AD Scripting for SSO	132
Step 1: Configuring the Script for AD Server	132
Step 2: Configuring AD Scripting for StoneOS	135
Using AD Polling for SSO	135
Using SSO Monitor for SSO	138
Using AD Agent Software for SSO	139
Step 1: Installing and Running AD Security Agent on a PC or Server	140
Step 2: Configuring AD server for StoneOS	142
802.1x	144
Configuring 802.1x	144
Creating 802.1x Profile	144
802.1x Global Configuration	145
Viewing Online Users	146
PKI	147
Creating a PKI Key	147
Creating a Trust Domain	148
Importing/Exporting Trust Domain	149
Importing Trust Certification	150
Online Users	151
Chapter 8 VPN	152

IPSec VPN	153
Basic Concepts	153
Security Association (SA)	153
Encapsulation Modes	153
Establishing SA	153
Using IPSec VPN	153
Configuring an IKE VPN	155
Configuring a Phase 1 Proposal	155
Configuring a Phase 2 Proposal	156
Configuring a VPN Peer	158
Configuring an IKE VPN	160
Configuring a Manual Key VPN	163
Viewing IPSec VPN Monitoring Information	166
Configuring PnPVPN	168
PnPVPN Workflow	168
PnPVPN Link Redundancy	168
Configuring a PnPVPN Client	168
Configuring IPSec-XAUTH Address Pool	170
SSL VPN	172
Configuring an SSL VPN	172
Configuring Resource List	178
Configuring an SSL VPN Address Pool	180
Configuring SSL VPN Login Page	182
Host Binding	183
Configuring Host Binding	183
Configuring Host Binding and Unbinding	183
Configuring a Super User	183
Configuring a Shared Host	184
Importing/Exporting Host Binding List	185
Host Checking	186
Role Based Access Control and Host Checking Procedure	186
Configuring a Host Checking Profile	187
SSL VPN Client for Windows	190
Downloading and Installing Secure Connect	190
Using Username/Password Authentication	190
Using Username/Password + Digital Certificate Authentication	192
Using Digital Certificate Only	192
Starting Secure Connect	193
Starting via Web	193

Using Username/Password Authentication	193
Using Username/Password + USB Key Certificate Authentication	194
Using Username/Password + File Certificate Authentication	195
Using USB Key Certificate Only Authentication	196
Using File Certificate Only Authentication	196
Starting Directly	197
Using Username/Password Authentication	197
Using Username/Password + USB Key Certificate Authentication	199
Using Username/Password + File Certificate Authentication	200
Using USB Key Certificate Only	202
Using File Certificate Only	203
Viewing Secure Connect GUI	204
General	204
Interface	205
Route	205
Viewing Secure Connect Menu	205
Configuring Secure Connect	206
Configuring General Options	206
Configuring a Login Entry	206
SSL VPN Client for Android	208
Downloading and Installing the Client	208
Starting and Logging into the Client	208
GUI	209
Connection Status	209
Configuration Management	209
Adding a Login Entry	209
Editing a Login Entry	210
Deleting a Login Entry	210
Modifying the Login Password	210
Disconnecting the Connection or Logging into the Client	210
Connection Log	210
System Configuration	210
About Us	211
SSL VPN Client for iOS	212
Deploying VPN Configurations	212
Connecting to VPN	216
Introduction to GUI	216
Connection Status	217
Connection Log	217

About US	217
SSL VPN Client for Mac OS	217
Downloading and Installing Client	217
Starting Client and Establishing Connection	218
GUI	218
Toolbar	218
Connection List	219
Connection Information	219
Status Bar	219
Menu	219
SSL VPN Client for Linux	220
Downloading and Installing Client	220
Starting Client and Establishing Connection	222
Upgrading and Uninstalling Client	224
GUI	226
Toolbar	226
Connection List	226
Connection Information	226
Status Bar	227
Menu	227
L2TP VPN	228
Configuring an L2TP VPN	228
Configuring an L2TP VPN Address Pool	230
Viewing L2TP VPN Online Users	232
Chapter 9 Object	233
Address	234
Creating an Address Book	234
Viewing Details	235
Host Book	236
Creating a Host Book	236
Service Book	237
Predefined Service/Service Group	237
User-defined Service	237
User-defined Service Group	237
Configuring a Service Book	237
Configuring a User-defined Service	238
Configuring a User-defined Service Group	239
Viewing Details	240
Application Book	241

Editing a Predefined Application	241
Creating a User-defined Application	241
Creating a User-defined Application Group	242
Creating an Application Filter Group	242
Creating a Signature Rule	242
Viewing Details	244
SLB Server Pool	245
Configuring SLB Server Pool and Track Rule	245
Viewing Details of SLB Pool Entries	246
Schedule	247
Periodic Schedule	247
Absolute Schedule	247
Creating a Schedule	247
AAA Server	249
Configuring a Local AAA Server	249
Configuring Radius Server	250
Configuring Active Directory Server	252
Configuring LDAP Server	255
Configuring TACACS+ Server	257
Connectivity Test	258
User	259
Configuring a Local User	259
Creating a Local User	259
Creating a User Group	261
Import User Password List	261
Export User Password List	261
Configuring a LDAP User	262
Synchronizing Users	262
Configuring an Active Directory User	262
Synchronizing Users	262
Configuring a IP-User Binding	262
Adding User Binding	262
Import Binding	263
Export Binding	263
Role	264
Creating a Role	264
Creating a Role Mapping Rule	264
Creating a Role Combination	265
Track Object	267

Creating a Track Object	267
Send Object	269
Creating a Send Object	269
Viewing Relevant Alarm Rules	269
URL Filter	270
Configuring URL Filter	270
Viewing URL Hit Statistics	273
Viewing Web Surfing Records	274
Configuring URL Filter Objects	274
Predefined URL DB	274
Configuring Predefined URL Database Update Parameters	274
Upgrading Predefined URL Database Online	275
Upgrading Predefined URL Database from Local	275
User-defined URL DB	275
Configuring User-defined URL DB	275
Importing User-defined URL	276
Clearing User-defined URL	276
URL Lookup	277
Inquiring URL Information	277
Configuring URL Lookup Servers	277
Keyword Category	278
Configuring a Keyword Category	278
Warning Page	279
Configuring Block Warning	279
Configuring Audit Warning	280
Data Security	281
Configuring Data Security Objects	282
Predefined URL DB	282
Configuring Predefined URL Database Update Parameters	282
Upgrading Predefined URL Database Online	283
Upgrading Predefined URL Database from Local	283
User-defined URL DB	283
Configuring User-defined URL DB	283
Importing User-defined URL	284
Clearing User-defined URL	284
URL Lookup	285
Inquiring URL Information	285
Configuring URL Lookup Servers	285
Keyword Category	286

Configuring a Keyword Category	286
Warning Page	287
Configuring Block Warning	287
Configuring Audit Warning	288
Bypass Domain	288
User Exception	289
File Filter	290
Creating File Filter Rule	290
Network Behavior Record	292
Configuring Network Behavior Recording	292
Viewing Logs of Network Behavior Recording	294
Chapter 10 Policy	295
Security Policy	296
Configuring a Security Policy Rule	296
Viewing and Searching Security Policy Rules	300
Managing Security Policy Rules	301
Enabling/Disabling a Policy Rule	302
Cloning a Policy Rule	302
Adjusting Security Policy Rule Position	302
Configuring Default Action	302
Viewing and Clearing Policy Hit Count	303
Hit Count Check	303
Rule Redundancy Check	303
Schedule Validity Check	304
Showing Disabled Policies	304
User Online Notification	305
Configuring User Online Notification	305
Configuring the Parameters of User Online Notification	305
Viewing Online Users	306
iQoS	307
Implement Mechanism	307
Pipes and Traffic Control Levels	307
Pipes	307
Traffic Control Levels	309
Enabling iQoS	309
Pipes	311
Basic Operations	311
Configuring a Pipe	311
Viewing Statistics of Pipe Monitor	317

NAT	318
Basic Translation Process of NAT	318
Implementing NAT	318
Configuring SNAT	319
Enabling/Disabling a SNAT Rule	321
Adjusting Priority	321
Copying/Pasting a SNAT Rule	322
Exporting NAT444 Static Mapping Entries	322
Hit Count	322
Clearing NAT Hit Count	322
Hit Count Check	322
Configuring DNAT	324
Configuring an IP Mapping Rule	324
Configuring a Port Mapping Rule	324
Configuring an Advanced NAT Rule	325
Enabling/Disabling a DNAT Rule	327
Copying/Pasting a DNAT Rule	328
Adjusting Priority	328
Hit Count	328
Clearing NAT Hit Count	328
Hit Count Check	329
SLB Server	330
Viewing SLB Server Status	330
Viewing SLB Server Pool Status	330
Session Limit	331
Configuring a Session Limit Rule	331
Clearing Statistic Information	332
ARP Defense	333
Configuring ARP Defense	334
Configuring Binding Settings	334
Adding a Static IP-MAC-Port Binding	334
Obtaining a Dynamic IP-MAC-Port Bindings	334
Bind the IP-MAC-Port Binding Item	335
Importing/Exporting Binding Information	336
Configuring Authenticated ARP	336
Configuring ARP Inspection	337
Configuring DHCP Snooping	338
Viewing DHCP Snooping List	339
Configuring Host Defense	339

SSL Proxy	341
Work Mode	341
Working as Gateway of Web Clients	342
Configuring SSL Proxy Parameters	342
Specifying the PKI Trust Domain of Device Certificate	342
Obtaining the CN Value	342
Configuring a Trusted SSL Certificate List	343
Importing Device Certificate to Client Browser	343
Configuring a SSL Proxy Profile	343
Working as Gateway of Web Servers	345
Configuring a SSL Proxy Profile	345
Binding a SSL Proxy Profile to a Policy Rule	346
Global Blacklist	347
Configuring IP Block Settings	347
Configuring Service Block Settings	347
Chapter 11 Threat Prevention	349
Threat Protection Signature Database	349
Anti Virus	351
Configuring Anti-Virus	352
Preparing	352
Configuring Anti-Virus Function	352
Configuring an Anti-Virus Rule	353
Configuring Anti-Virus Global Parameters	355
Intrusion Prevention System	356
Signatures	356
Configuring IPS	357
Preparation	357
Configuring IPS Function	357
Configuring an IPS Rule	358
IPS Global Configuration	372
Signature List	373
Searching Signatures	374
Managing Signatures	374
Configuring IPS White list	375
Sandbox	376
Configuring Sandbox	377
Preparation	377
Configuring Sandbox	377
Configuring a Sandbox Rule	377

Threat List	379
Trust List	380
Sandbox Global Configurations	380
Critical Assets	380
Configuring Critical Asset Object	380
Attack-Defense	382
ICMP Flood and UDP Flood	382
ARP Spoofing	382
SYN Flood	382
WinNuke Attack	382
IP Address Spoofing	382
IP Address Sweep and Port Scan	382
Ping of Death Attack	382
Teardrop Attack	383
Smurf Attack	383
Fraggle Attack	383
Land Attack	383
IP Fragment Attack	383
IP Option Attack	383
Huge ICMP Packet Attack	383
TCP Flag Attack	383
DNS Query Flood Attack	383
TCP Split Handshake Attack	383
Configuring Attack Defense	384
Perimeter Traffic Filtering	391
Enabling Perimeter Traffic Filtering	391
Configuring User-defined Black/White List	391
Configuring Third-party Black List	392
Searching Black/White List	392
Abnormal Behavior Detection	394
Host Defender	394
DNS Defender	395
Viewing the Abnormal Behavior Detection Information	395
Mitigation	397
Mitigation Rule	397
Configuring a User-defined Mitigation Rule	397
Enabling Mitigation	399
Viewing Mitigation Action	399
Advanced Threat Detection	400

Configuring Advanced Threat Detection	400
Viewing Advanced Threat Detection Information	400
Anti-Spam	402
Configuring Anti-Spam	403
Preparing	403
Configuring Anti-Spam Function	403
Configuring an Anti-Spam Rule	403
Anti-Spam Global Configuration	406
Chapter 12 Monitor	407
Monitor	408
Host Monitor	409
Host Details	409
Share Access Detect	410
IQoS Monitor	411
IQoS Summary	411
IQoS Details	412
Service/Network Node Monitor	414
Viewing Service/Network Node Monitor Information	416
Device Monitor	417
Summary	417
Statistical Period	418
URL Hit	419
Summary	419
User/IP	419
URL	420
URL Category	420
Statistical Period	421
Link State Monitor	422
Link State	422
Link Configuration	422
Statistical Period	423
Authentication User	425
Alarm	426
Alarm as a Monitor	426
Alarms by Time	426
Alarm by Severity	427
Alarm Details	427
Alarm Rule	429
Configuring Interface Bandwidth	429

Creating an Alarm Rule	430
Reporting	432
Report File	433
User-defined Task	434
Creating a User-defined Task	434
Enabling/Disabling the User-defined Task	436
Viewing Report Files	436
Predefined Task	437
Generating Report Tasks	437
Viewing Report Files	438
Logging	439
Log Severity	439
Destination of Exported Logs	439
Log Format	440
My Logs	441
Event Logs	442
Network Logs	443
Configuration Logs	444
Threat Logs	445
Session Logs	446
PBR Logs	446
NAT Logs	447
URL Logs	448
File Filter Logs	449
Network Behavior Record Logs	450
CloudSandBox Logs	450
Log Configuration	451
Creating a Log Server	451
Configuring Log Encoding	451
Adding Email Address to Receive Logs	451
Specifying a Unix Server	452
Specifying a Mobile Phone	452
Managing Logs	453
Configuring Logs	453
Option Descriptions of Various Log Types	453
Chapter 13 Diagnostic Tool	459
Global Fault Detection	460
Configuring Search Conditions	460
Viewing Search Results	461

Packet Path Detection	462
Configuring Packet Path Detection	462
Emulation Detection	462
Online Detection	463
Imported Detection	465
Detected Sources	466
Packet Capture Tool	467
Configuring Packet Capture Tools	467
Test Tools	469
DNS Query	469
Ping	469
Traceroute	469
Chapter 14 High Availability	470
Basic Concepts	470
HA Cluster	470
HA Group	470
HA Node	470
Virtual Forward Interface and MAC	471
HA Selection	471
HA Synchronization	471
Configuring HA	472
Chapter 15 System Management	474
System Information	475
Viewing System Information	475
Device Management	477
Administrators	477
VSYN Administrator	477
Creating an Administrator Account	478
Admin Roles	479
Trust Host	480
Creating a Trust Host	480
Management Interface	481
System Time	482
Configuring the System Time Manually	482
Configuring NTP	483
NTP Key	483
Creating a NTP Key	484
Option	484
Rebooting the System	486

System Debug	486
Failure Feedback	486
System Debug Information	486
Configuration File Management	487
Managing Configuration File	487
Viewing the Current Configuration	488
SNMP	489
SNMP Agent	489
SNMP Host	490
Trap Host	491
V3 User Group	491
V3 User	492
Upgrading System	494
Upgrading Firmware	494
Updating Signature Database	494
License	496
Viewing License List	497
Applying for a License	498
Installing a License	498
Mail Server	500
Creating a Mail Server	500
SMS Parameters	501
SMS Modem Devices	501
Configuring SMS Parameters	501
Testing SMS	501
Connecting to HSM	502
HSM Deployment Scenarios	502
Connecting to HSM	502
Connecting to Hillstone CloudView	503
CloudView Deployment Scenarios	503
Connecting to Hillstone CloudView	504
VSYS (Virtual System)	505
VSYS Objects	505
Root VSYS and Non-root VSYS	505
VRouter, VSwitch, Zone and Interface	506
Shared VRouter	506
Shared VSwitch	506
Shared Zone	506
Shared Interface	506

Interface Configuration	506
Creating Non-root VSYS	507
Configuring Dedicated and Shared Objects for Non-root VSYS	507
Configuring VSYS Quota	508
Entering the VSYS	511

Welcome

Thanks for choosing Hillstone products!

This part introduces how you get user guides of Hillstone products.

Getting Started Guide:

- Getting Started Guide ([Download PDF](#))

Cookbook (recipes):

- StoneOS 5.5 Cookbook ([Download PDF](#))

OS Operation Guides:

- StoneOS Command Line Interface User Guide ([Download PDF](#))
- StoneOS WebUI User Guide ([Download PDF](#))
- StoneOS Log Messages Reference Guide ([Download PDF](#))
- StoneOS SNMP Private MIB Reference Guide ([Download PDF](#))
- StoneOS Addendum Book for P Releases ([Download PDF](#))

Hardware Installation Guides:

- Hardware Reference Guide of all series platforms ([Download PDF](#))
- Expansion Modules Reference Guide of all modules ([Download PDF](#))

Other Support Links:

- Webiste: www.hillstonenet.com
- Download Documentations: <http://docs.hillstonenet.com>
- Technical Support: 1-800-889-9860

Chapter 1 Getting Started Guide

This guide helps you go through the initial configuration and the basic set-up of your Hillstone device. The intended reader is your company's network administrator.

This guide is used when you have finished mounting your device. After following the steps in this guide, your private network will be able to access the Internet. To set up security functions, you will need to read the User Guide (WebUI User Guide or CLI User Guide).

You may configure your firewall in the following sequence:

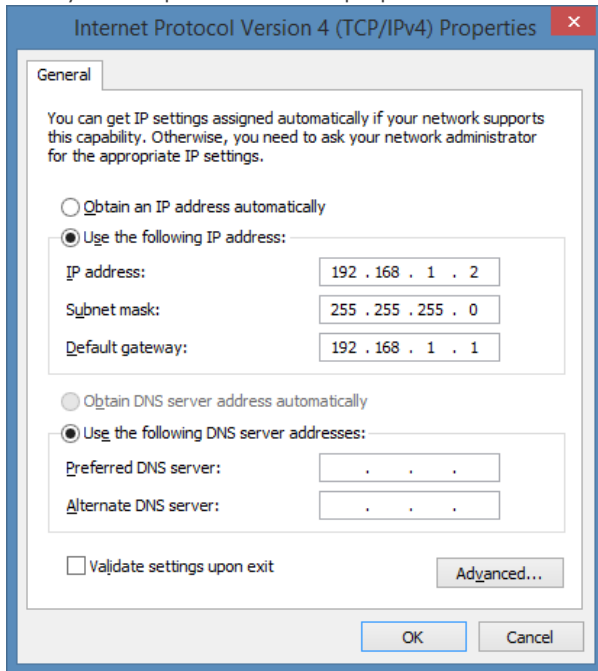
1. ["Initial Visit to Web Interface" on Page 3](#)
2. ["Preparing the StoneOS System" on Page 4](#), including:
 - ["Installing Licenses" on Page 4](#)
 - ["Creating a System Administrator" on Page 4](#)
 - ["Adding Trust Hosts" on Page 5](#)
 - ["Upgrading StoneOS Firmware" on Page 6](#)
 - ["Updating Signature Database" on Page 6](#)
3. ["Connecting to Internet Under Routing Mode" on Page 7](#)
4. ["Restoring Factory Settings" on Page 11](#)

Initial Visit to Web Interface

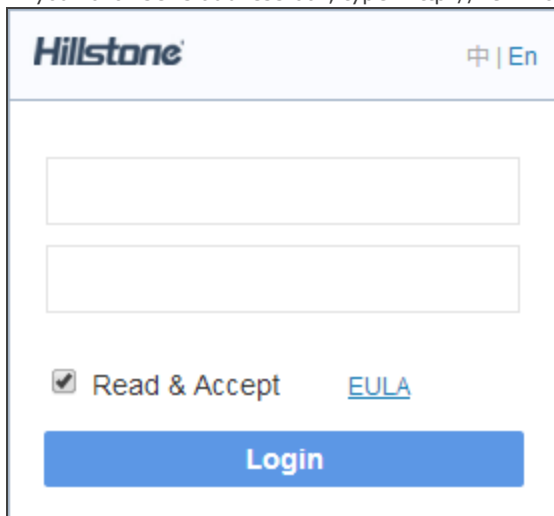
Interface eth0/0 is configured with IP address 192.168.1.1/24 by default and it is open to SSH、PING、SNMP、HTTP connection types(except for some custom versions). For the initial visit, use this interface.

To visit the web interface for the first time, take the following steps:

1. Go to your computer's Ethernet properties and set the IPv4 protocol as below.



2. Connect an RJ-45 Ethernet cable from your computer to the eth0/0 of the device.
3. In your browser's address bar, type "http://192.168.1.1" and press **Enter**.



4. In the login interface, type the default username and password: hillstone/hillstone.
5. At the first sign of address, the user needs to read and accept the EULA (end-user license agreements), click **EULA** to view the details of EULA.
6. Click **Login**, and the device's system will initiate.

Preparing the StoneOS System

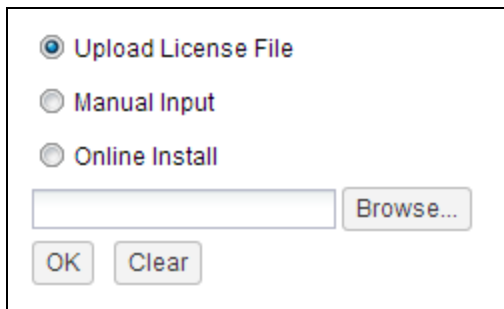
Installing Licenses

Licenses control features and performance.

Before installing any license, you must purchase a license code.

To install a license, take the following steps:

1. Go to **System > License**.
2. **Choose one of the three ways to import a license:**



- **Upload License File:** Select the radio button, click **Browse**, and select the license file (a .txt file).
 - **Manual Input:** Select the radio button, and paste the license code into the text box.
 - **Online Install:** Select the **Online Install** radio button and click the **Online Install** button, your purchased licenses will be automatically installed. It should be noted that the licenses must be in an activated status in the Hillstone Online Registration Platform (<http://onlinelic.hillstonenet.com/reqlicense>). (To activate the license, you need to log into the platform using your username and password. The username is the same as your email which was provided when placing the order. Hillstone will send the password by email. Then, activate the licenses that need to be installed. If you purchased the device from a Hillstone agent, please contact the agent to activate the licenses.)
3. Click **OK**.
 4. To make the license take effect, reboot the system. Go to **System > Device Management > Options**, and click **Reboot**.

Creating a System Administrator

System administrator has the authority to read, write and execute all the features in system.

To create a system administrator, take the following steps:

1. Go to **System > Device Management > Administrator**.
2. Click **New**.

Configuration

Name: Admin (4-31) characters

Role: Administrator

Password: (4-31) characters

Confirm Password:

Login Type: ☒ Console ☒ Telnet
☒ SSH ☒ HTTP
☒ HTTPS
☒ Select All

Description: (0-127) characters

OK Cancel

In the Admin Configuration dialog box, enter values

Option	Value
Name	Admin
Role	Administrator
Password	123456
Confirm Password	123456
Login Type	Select Telnet , SSH , HTTP and HTTPS .

- Click **OK**.



Note: The system has a default administrator "hillstone", which cannot be deleted or renamed.

Adding Trust Hosts

The trust host is administrator's host. Only computers included in the trust hosts can manage system.

To add a trust host, take the following steps:

- Go to **System > Device Management**.
- Select **Trust Host** tab, and click **New**.

Trust Host Configuration

Type: ☒ IP/Netmask ☐ IP Range

IP: 192.168.1.2 / 24

Login Type: ☒ Telnet ☒ SSH ☒ HTTP ☒ HTTPS

OK Cancel

In the Trust Host Configuration dialog box, enter value

Option	Value
Type	Select IP/Netmask
IP	192.168.1.2/24
Login Type	Select all: Telnet, SSH, HTTP and HTTPS

3. Click **OK**.

Upgrading StoneOS Firmware



Note: Back up your configuration files before upgrading your system.

To upgrade your system firmware, take the following steps:

1. Go to **System > Upgrade Management**.
2. Select **Browse** and choose the new image from your local computer.
3. Click **Reboot to make new firmware take effect**, then click **Apply**.
4. System will automatically reboot when it finishes installing the new firmware.

Updating Signature Database

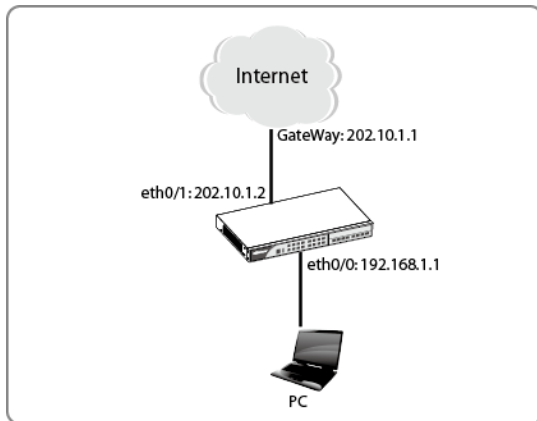
Features that require constant updates of signature are license controlled. You must purchase the license in order to be able to update the signature libraries. By default, the system will automatically update the databases daily.

To update a database, take the following steps:

1. Go to **System > Upgrade Management**, and click the <Signature Database Update> tab.
2. **Find your intended database, and choose one of the following two ways to upgrade.**
 - **Remote Update:** Click **Update**, and system will automatically update the database.
 - **Local Update:** Select **Browse** to open the file explorer, and select your local signature file to import it into system.

Connecting to Internet Under Routing Mode

In routing mode, the device is working as a gateway and router between two networks. This section shows how to connect and configure a new Hillstone device in routing mode to securely connect the private network to the Internet.



To get your private network access to Internet through a Hillstone device, take the following steps:

Step 1: Connecting to the device

1. Connect one port (e.g. eth0/1) of Hillstone device to your ISP network. In this way, "eth0/1" is in the untrust zone.
2. Connect your internal network to another Ethernet interfaces (e.g. eth0/0) of the device. This means "eth0/0" is connected to the trust zone.
3. Power on the Hillstone device and your PCs.
4. If one of the internal interfaces already has been configured with an IP address, use a browser to visit that address from one of your internal PCs.
If it is a new device, use the methods in ["Initial Visit to Web Interface"](#) on Page 3 to visit.
5. Enter "hillstone" for both the username and the password.

Step 2: Configuring interfaces

1. Go to **Network > Interface**.

2. Double click **eth0/1**.

Ethernet Interface

Basic

Interface Name: ethernet0/1

Description: (0-63) chars

Binding Zone: ☐ Layer 2 Zone ☒ Layer 3 Zone ☐ TAP ☐ No Binding

Zone: untrust

IP Configuration

Type: ☒ Static IP ☐ DHCP ☐ PPPoE

IP Address: 202.10.1.2

Net mask: 255.255.255.0

☐ Set as Local IP

☐ Enable DNS Proxy ☒ Proxy ☐ Proxy-Trans

☐ Enable DNS Bypass

Advanced DHCP... DDNS

Management

☒ Telnet ☒ SSH ☒ Ping ☒ HTTP ☒ HTTPS ☐ SNMP

Routing

Reverse Route: ☐ Enable ☐ Close ☒ Auto

WAP traffic distribution: ☐ Enable

OK Cancel

In the Ethernet Interface dialog box, enter values

Option	Value
Binding Zone	L3-zone
Zone	untrust
Type	Static IP
IP Address	202.10.1.2 (public IP address provided by your ISP)
Netmask	255.255.255.0
Management	Select protocols that you want to use to access the device.

3. Click **OK**.

Step 3: Creating a NAT rule to translate internal IP to public IP

1. Go to **Policy > NAT > SNAT**.
2. Select **New**

NAT Configuration

Basic

Virtual Router: Virt1

Source Address: Address Entry

Destination Address: Any

Egress Interface: ethernet0/1

Service: Any

Translated to: ☒ Egress IP ☐ Specified IP ☐ No NAT

NAT mode: ☒ Source NAT ☐ Destination NAT

NAT type: ☒ Static ☐ Dynamic

If "Static" is selected, all sessions of the source IP will be mapped to a fixed IP

HA group: ☒ 0 ☐ 1

Description: (0-63) characters

OK Cancel

In the SNAT Configuration dialog box, enter values

Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Egress	Egress interface, ethernet 0/1
Translated	Egress IP
Sticky	Enable

3. Click **OK**.

Step 4: Creating a security policy to allow internal users access Internet.

1. Go to **Policy > Security Policy**.
2. Click **New**.

The screenshot shows the 'Policy Configuration' dialog box with the 'Basic' tab active. The 'Source' section has 'Zone' set to 'trust' and 'Address' set to 'any'. The 'Destination' section has 'Zone' set to 'untrust', 'Address' set to 'any', and 'Service' set to 'any'. The 'Action' section has 'Permit' selected. There are 'OK' and 'Cancel' buttons at the bottom right.

In the Policy Configuration dialog box, enter values.

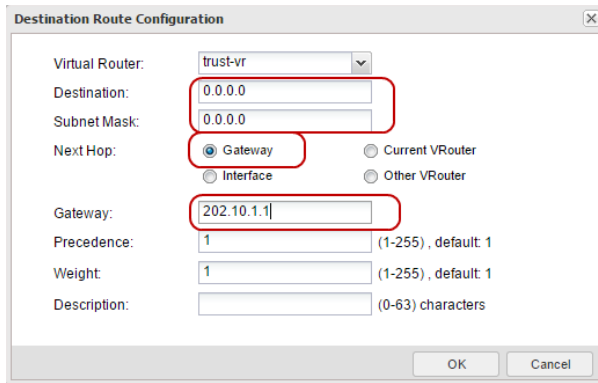
Source Information	
Zone	trust
Address	Any
Destination Information	
Zone	untrust
Address	Any
Other Information	
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

3. Click **OK**.

Step 5: Configuring a default route

1. Go to **Network > Routing > Destination Route**.

2. Click **New**.



The image shows a 'Destination Route Configuration' dialog box. It contains the following fields and options:

- Virtual Router:** A dropdown menu with 'trust-vr' selected.
- Destination:** A text input field containing '0.0.0.0'.
- Subnet Mask:** A text input field containing '0.0.0.0'.
- Next Hop:** A group of four radio buttons: 'Gateway' (selected), 'Current VRouter', 'Interface', and 'Other VRouter'.
- Gateway:** A text input field containing '202.10.1.1'.
- Precedence:** A text input field containing '1', with '(1-255), default: 1' to its right.
- Weight:** A text input field containing '1', with '(1-255), default: 1' to its right.
- Description:** A text input field, with '(0-63) characters' to its right.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

In the **Destination Route Configuration** dialog box, enter values.

Option	Value
Destination	0.0.0.0 (means all network)
Subnet Mask	0.0.0.0 (means all subnets)
Gateway	202.10.1.1 (gateway provided by your ISP)

3. Click **OK**.

Restoring Factory Settings



Note: Resetting your device will erase all configurations, including the settings that have been saved. Please be cautious!

To restore factory's default settings, you may use one of the following two ways:

- "Restoring using a pin" on Page 11
- "Restoring via WebUI" on Page 11

Restoring using a pin

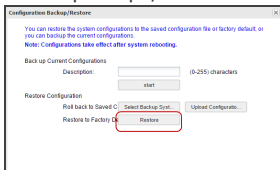
To restore factory default settings using a Web interface, take the following steps:

1. Power off the device.
2. Use a pin to press the CLR pinhole on the front panel; keep pressing and power on the devcie.
3. Keep pressing until the STA and ALM indicators on the front panel turn a constant red; release the pin. System will start to reset itself.
4. When restoring is complete, system will reboot automatically.

Restoring via WebUI

To restore factory default settings using a Web interface, take the following steps:

1. Go to **System > Configuration File Management**.
2. Click **Backup Restore**.
3. In the prompt, click **Restore**.



4. Click **OK** to confirm.
5. The device will automatically reboot and be back to factory settings.

Chapter 2 Deploying Your Device

This chapter introduces how a firewall works and its most commonly used scenarios. Understanding the system structure, basic elements and flow chart will help you in better organizing your network and making the most of the firewall product.

- ["How a Firewall Works" on Page 13](#)

A firewall has more than one deployment scenario. Each scenario applies to one environment requirement. The usual deployment modes are:

- ["Deploying Transparent Mode" on Page 18](#)
Transparent mode is a situation when the IT administrator does not wish to change his/her existing network settings. In transparent mode, the firewall is invisible to the network. Because no IP address configuration is needed, the firewall only provides security features.
- ["Deploying Routing Mode" on Page 22](#)
Routing mode applies when the firewall offers both routing and NAT functions. In routing mode, the firewall connects two networks typically, an internal network and the Internet, and the firewall interfaces are configured with IP addresses.
- ["Deploying Mix Mode" on Page 26](#)
If a firewall has Layer-2 interfaces and Layer-3 interfaces, it is in mix mode.
- ["Deploying Tap Mode" on Page 27](#)
When an IT administrator only wants the monitor, IPS or statistic function of a firewall, while not a gateway device, using tap mode is the right choice. In tap mode, the firewall is not directly connected within the network.

How a Firewall Works

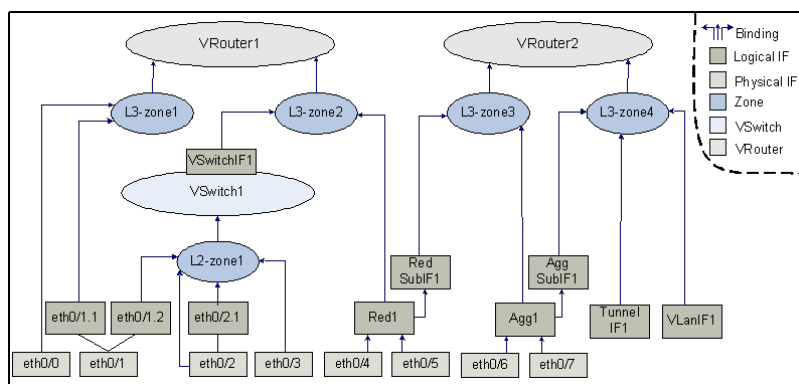
A firewall is a network security device. It protects a network by controlling the traffic that comes in and out of that network. The basic mechanism of how a firewall works is that allowing or denying the data packet by identifying whether it matches the policy rules or not. Besides security functions, a firewall can also work as a bridging device to connect a trust zone (internal network) and untrust zone (external network).

StoneOS System Architecture

The elements that constitute StoneOS system architecture are:

- **Zone:** Zones divide network into multiple segments, for example, trust (usually refers to the trusted segments such as the Intranet), untrust (usually refers to the untrusted segments where security threats exist).
- **Interface:** Interface is the inlet and outlet for traffic going through security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface and the corresponding policy rules should also be configured to allow traffic transmission between different security zones. Multiple interfaces can be bound to one security zone, but one interface cannot be bound to multiple security zones.
- **VSwitch:** VSwitch is short for Virtual Switch. A VSwitch functions as a switch in Layer 2. After binding a Layer 2 zone to a VSwitch, all the interfaces in the zone are also bound to the VSwitch. There is a default VSwitch named VSwitch1. By default, all Layer 2 zones will be bound to VSwitch1. You can create new VSwitches and bind Layer 2 zones to VSwitches. Each VSwitch is a Layer 2 forwarding zone with its own MAC address table which supports the Layer 2 traffic transmission for the device. Furthermore, the VSwitchIF helps the traffic to flow between Layer 2 and Layer 3.
- **VRouter:** VRouter is Virtual Router and also abbreviated as VR. A VRouter functions as a router with its own routing table. There is a default VR named trust-vr. By default, all the Layer 3 zones will be bound to trust-vr automatically. The system supports the multi-VR function and the max VR number varies from different platforms. Multiple VRs make the device work as multiple virtual routers, and each virtual router uses and maintains its own routing table. The multi-VR function allows a device to achieve the effects of the address isolating in different route zones and the address overlapping in different VRs, as well as avoiding leakage of route to some extent and enhancing route security of network.
- **Policy:** Policy is used to control the traffic flow in security zones/segments. By default Hillstone devices will deny all traffic in security zones/segments, while the policy can identify which flow in security zones or segments will be permitted, and which will be denied, which is specifically based on policy rules.

For the relationships among interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationships among them are:

- Interfaces are bound to security zones. Interfaces bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One interface can be only bound to one security zone; interface and its sub interface can belong to different security zones.

- Security zones are bound to a VSwitch or VRouter. Layer 2 security zones are bound to a VSwitch (by default the predefined Layer 2 security zone is bound to the default VSwitch1), and Layer 3 security zones are bound to a VRouter (by default the predefined Layer 3 security zone is bound to the default trust-vr), thus realizing the binding between the interfaces and VSwitch or VR. One security zone can be only bound to one VSwitch or VR.

General Rules of Security Policy

By default, all interfaces, even in the same zone, cannot communicate. Traffic in different zones are not allowed to be transferred either. In order to change the rule, you need to set up new policy rules to allow traffic forwarding.



Note: To allow bidirectional traffic, you need to set up two policies: one is from source to destination, the other is from destination to source. If there is only one-direction initiative access, the responsive direction only need to respond to that visit, you will need to create only one-way policy (from source to destination).

This part explains what policy is needed to allow interfaces in different zones, VSwitches, or VRouters to communicate. The rules are:

- **Interfaces in the same zone**

To allow interfaces in the same zone to communicate, you need to create a policy whose source and destination are both the zone which the interfaces belong to.

For example, to allow eth0/0 and eth0/1 to communicate, you need to create an "allowing" policy with source L3-zone and destination L3-zone.

- **Zones of two interfaces are under the same VSwitch**

To allow communication of interfaces in different zones under the same VSwitch, you need to create two policies: one policy is to allow traffic from a zone to another; the other policy is to allow traffic in the opposite direction.

For example, to allow eth0/2 and eth0/3 to communicate, you should create a policy whose source is L2-zone1 and destination is L2-zone2, then create another policy to allow traffic from L2-zone2 to L2-zone1.

- **Zones of two interfaces are under different VSwitches**

Each VSwitch has its VSwitch interface (VSwitchIF) which is bound to a Layer-3 zone. To allow interfaces in different zones under different VSwitches to communicate, you need to create an "allowing" policy where the source is the zone of one VSwitchIF and the destination is the zone of the other VSwitchIF. After that, create another policy of the opposite direction.

- **Zones of two L3 interfaces are under the same VRouter**

To allow two L3 interfaces to communicate, you need to create a policy allowing one zone to the other zone.

For example, to allow communication between eth0/0 and eth0/5, you should create a policy from L3-zone1 to L3-zone2, and then create an opposite direction policy.

- **Zones of two L3 interfaces are under different VRouters**

To allow two L3 interfaces in two different zones of different VRouters, you need to create a policy with the source being one VRouter and the destination being the other VRouter. Then you create a policy of the opposite direction.

- **An L2 interface and an L3 interface under the same VRouter**

To allow communication between an L2 interface and an L3 interface under the same VRouter, you will need to create a policy whose source is the zone which binds the VSwitchIF of L2 interface and the destination is the zone of L3 interface. After that, create a policy of the opposite direction.

For example, to allow eth0/0 and eth0/2 to communicate, create a policy from L3-zone1 to L2-zone1, and its opposite direction policy.

Packet Processing Rule

Forwarding Rule in Layer 2

Forwarding within Layer 2 means it is in one VSwitch. StoneOS system creates a MAC address table for a VSwitch by source address learning. Each VSwitch has its own MAC address table. The packets are forwarded according to the

types of the packets, including IP packets, ARP packets, and non-IP-non-ARP packets.

The forwarding rules for IP packets are:

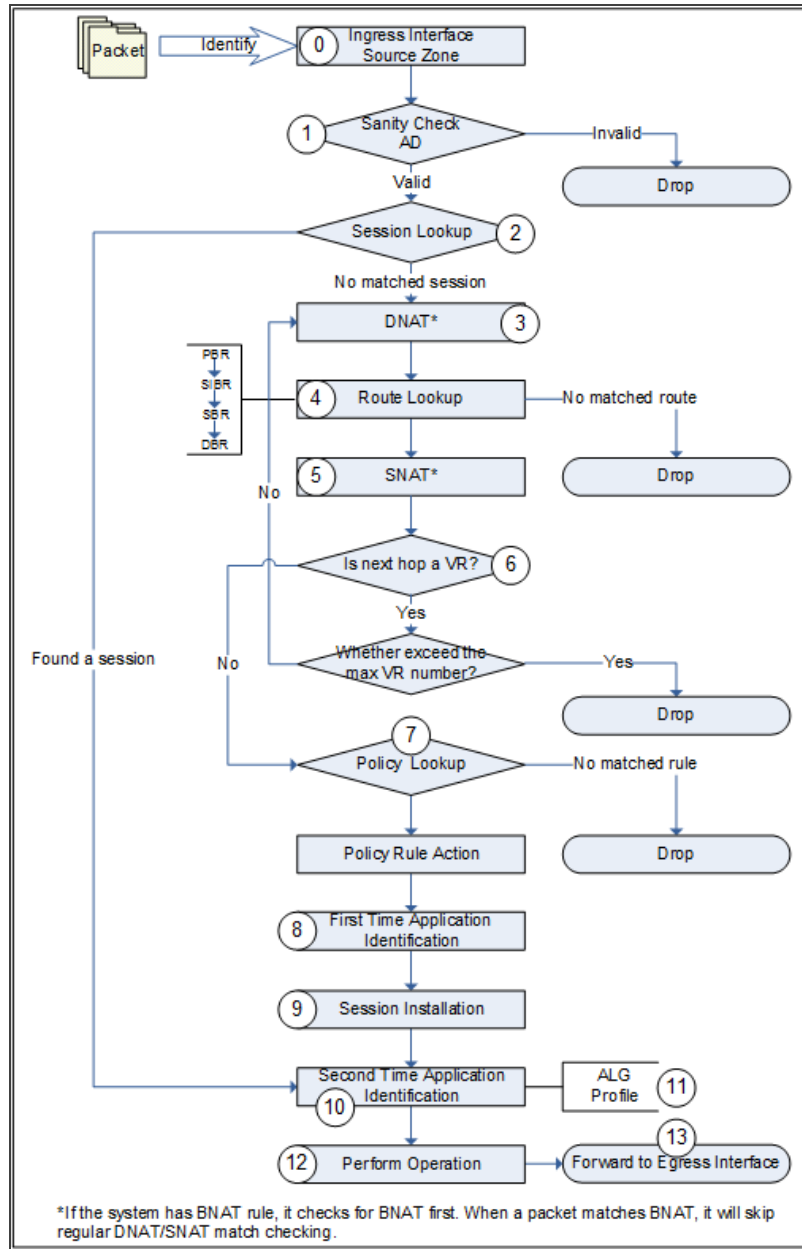
1. Receive a packet.
2. Learn the source address and update the MAC address table.
3. If the destination MAC address is a unicast address, the system will look up the egress interface according to the destination MAC address. And in this case, two situations may occur:
 - If the destination MAC address is the MAC address of the VSwitchIF with an IP configured, system will forward the packet according to the related routes; if the destination MAC address is the MAC address of the VSwitchIF with no IP configured, system will drop the packet.
 - Figure out the egress interface according to the destination MAC address. If the egress interface is the source interface of the packet, system will drop the packet. Otherwise, system will forward the packet from the egress interface.

If no egress interfaces (unknown unicast) is found in the MAC address table, jump to Step 6 directly.

4. Figure out the source zone and destination zone according to the ingress and egress interfaces.
5. Look up the policy rules and forward or drop the packet according to the matched policy rules.
6. If no egress interface (unknown unicast) is found in the MAC address table, system will send the packet to all the other L2 interfaces. The sending procedure is: take each L2 interface as the egress interface and each L2 zone as the destination zone to look up the policy rules, and then forward or drop the packet according to the matched policy rule. In a word, forwarding of unknown unicast is the policy-controlled broadcasting. Process of broadcasting packets and multicasting packets is similar to the unknown unicast packets, and the only difference is the broadcast packets and multicast packets will be copied and handled in Layer 3 at the same time.

For the ARP packets, the broadcast packet and unknown unicast packet are forwarded to all the other interfaces in the VSwitch, and at the same time, system sends a copy of the broadcast packet and unknown unicast packet to the ARP module to handle.

Forwarding Rule in Layer 3



0. Identify the logical ingress interface of the packet to determine the source zone of the packet. The logical ingress interface may be a common interface or a sub-interface.
1. System performs sanity check to the packet. If the attack defense function is enabled on the source zone, system will perform AD check simultaneously.
2. Session lookup. If the packet belongs to an existing session, system will perform Step 11 directly.
3. DNAT operation. If a DNAT rule is matched, system will mark the packet. The DNAT translated address is needed in the step of route lookup.
4. Route lookup. The route lookup order from high to low is: PBR > SIBR > SBR > DBR > ISP route. Until now, the system has known the logical egress and destination zone of the packet.

5. SNAT operation. If a SNAT rule is matched, system will mark the packet.
6. VR next hop check. If the next hop is a VR, system will check whether it is beyond the maximum VR number (current version allows the packet traverse up to three VRs). If it is beyond the maximum number, system will drop the packet; if it is within the maximum number range, return to Step 4. If the next hop is not a VR, go on with policy lookup.
7. Policy lookup. System looks up the policy rules according to the packet's source/destination zones, source/destination IP and port, and protocol. If no policy rule is matched, system will drop the packet; if any policy rule is matched, the system will deal with the packet as the rule specified. And the actions can be one of the followings:
 - Permit: Forward the packet.
 - Deny: Drop the packet.
 - Tunnel: Forward the packet to the specified tunnel.
 - Fromtunnel: Check whether the packet originates from the specified tunnel. System will forward the packet from the specified tunnel and drop other packets.
 - WebAuth: Perform WebAuth on the specified user.
8. First time application identification. System tries to identify the type of the application according to the port number and service specified in the policy rule.
9. Establish the session.
10. If necessary, system will perform the second time application identification. It is a precise identification based on the packet contents and traffic action.
11. Application behavior control. After knowing the type of the application, system will deal with the packet according to the configured profiles and ALG.
12. Perform operations according to the records in the session, for example, the NAT mark.
13. Forward the packet to the egress interface.

Deploying Transparent Mode

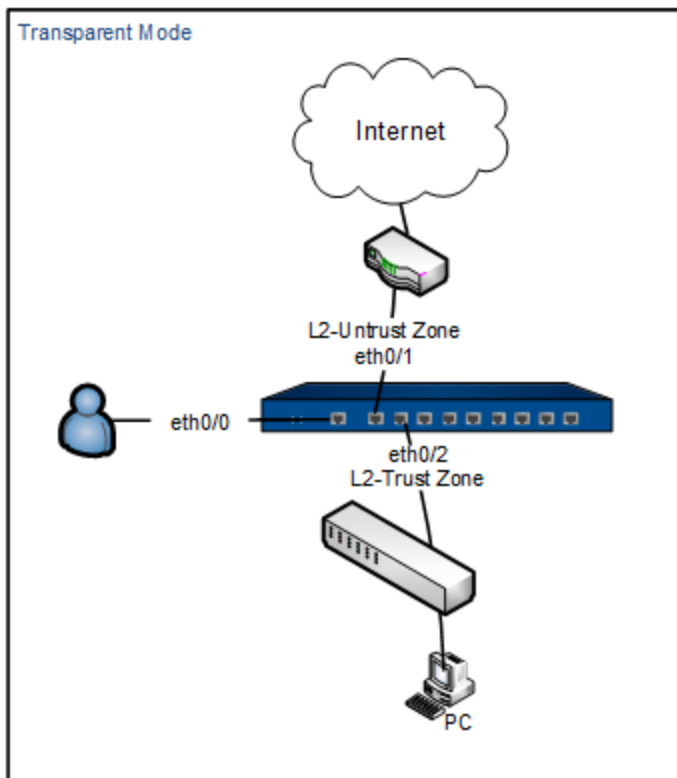
Transparent mode is also known as bridge mode or transparent bridging mode. Transparent mode is used when the IT administrator does not wish to change the existing network layout. Normally, the existing network has already set up routers and switches. The firewall will be used as a security device.

Transparent mode has the following advantages:

- No need to change IP addresses
- No need to set up NAT rule

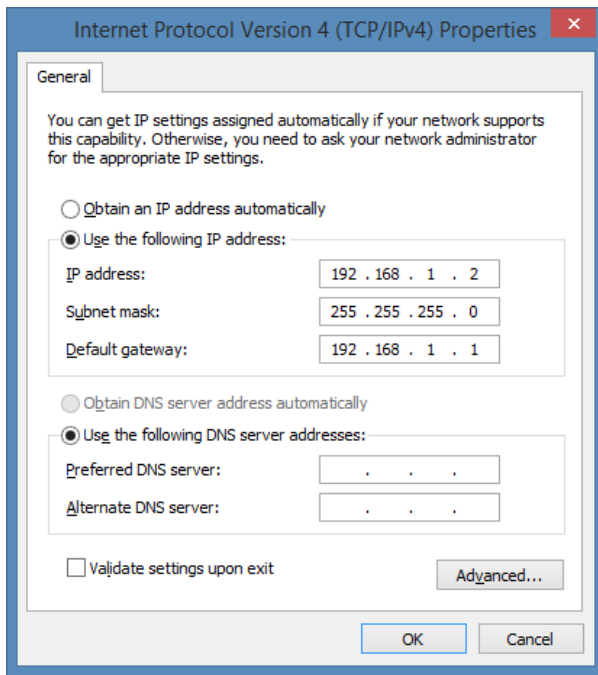
Under normal circumstances, the firewall in transparent mode is deployed between the router and the switch of the protected network, or it is installed between the Internet and a company's router. The internal network uses its old router to access the Internet, and the firewall only provides security control features.

This section introduces a configuration example of a firewall deployed between a router and a switch. In this example, the administrator uses eth0/0 to manage the firewall. The firewall's eth0/1 is connected to a router (which is connecting to the Internet) and eth0/2 is connected to a switch (which is connecting to internal network).



Step 1: Initial log in the firewall

1. In the administrator's Ethernet properties, set the IPv4 protocol as below.



2. Connect an RJ-45 Ethernet cable from the computer to the eth0/0 of the device.
3. In the browser's address bar, type "http://192.168.1.1" and press **Enter**.
4. In the login interface, type the default username and password: hillstone/hillstone.
5. Click **Login**, and the device's system will initiate.

Step 2: Configure interface and zone

- Configure eth0/1 as an Internet connected interface.
 1. Select **Network > Interface**.
 2. Double click ethernet0/1, and configure in the prompt.

Basic

Interface Name: ethernet0/1

Description: (0-63) characters

Binding Zone: ☒ Layer 2 Zone ☐ Layer 3 Zone ☐ TAP

Zone: I2-untrust

3. Click **OK**.

- Configure eth0/2 as a private network connected interface.

1. Select **Network > Interface**.
2. Double click ethernet0/2, and configure in the prompt.

Basic

Interface Name: ethernet0/2

Description: (0-63) characters

Binding Zone: ☒ Layer 2 Zone ☐ Layer 3 Zone ☐ TAP

Zone: l2-trust

3. Click **OK**.

Step 3: Configuring policies

- Create a policy to allow visiting the Internet.

1. Select **Policy > Security Policy**.
2. Click **New**.

Policy Configuration

Basic Protection Options

Source

Zone: l2-trust

Address: any

User:

Destination

Zone: l2-untrust

Address: any

Service: any

Application:

Action: ☒ Permit ☐ Deny ☐ Secured connection

☐ Enable Web Redirect ⓘ

OK Cancel

3. Click **OK**.

- Create a policy to allow the Internet to visit a private network.

1. Select **Policy > Security Policy**.
2. Click **New**.

Policy Configuration

Basic Protection Options

Source

Zone: l2-trust

Address: any

User:

Destination

Zone: l2-untrust

Address: any

Service: any

Application:

Action: ☒ Permit ☐ Deny ☐ Secured connection

☐ Enable Web Redirect ⓘ

OK Cancel

3. Click **OK**.

- The two policies above ensure communication between a private network and the Internet. If you want to set up more details, e.g. to limit P2P download, you can add more policies and overlap the new policies with the old ones. The match sequence of policies is determined by their position in the policy list, not their ID numbers.

(Optional) Step 4: Configuring VSwitch Interface for managing the firewall.

If you want any PC in the private network to visit and configure the firewall, you can configure a VSwitch interface as a management interface.

1. Select **Network > Interface**.
2. Double click vswitchif1.

Basic

Interface Name: vswitchif1

Description: (0-63) characters

Binding Zone: ☐ Layer 2 Zone ☒ Layer 3 Zone ☐ TAP ☐ No Binding

Zone: trust

IP Configuration

Type: ☒ Static IP ☐ DHCP ☐ PPPoE

IP Address: 192.168.1.100

Netmask: 24

☐ Enable DNS Proxy ☒ Proxy ☐ Proxy-Trans

☐ Enable DNS Bypass

Advanced DHCP... DDNS

Management

☒ Telnet ☒ SSH ☒ Ping ☒ HTTP ☒ HTTPS ☒ SNMP

Routing

Reverse Route: ☒ Enable ☐ Close ☐ Auto

WAP traffic distribution: ☐ Enable

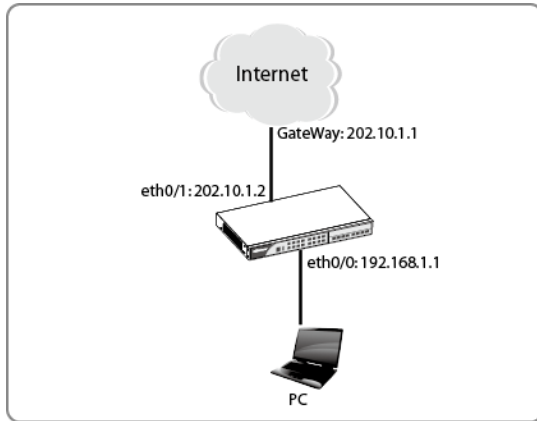
3. Click **OK**.
4. With any PC in the private network, enter the IP address of vswitchif1, and you will visit the firewall web user interface.

Deploying Routing Mode

Routing mode deployment often uses the NAT function, so it is also called NAT mode. In routing mode, each interface has its IP address which means interfaces are in the layer 3 zone. A firewall in routing mode can work as a router and a security device.

Routing mode is mostly used when the firewall is installed between an internal network and the Internet.

The example which is based on the below topology shows you how to connect and configure a new Hillstone device in routing mode. The device connects a private network to the Internet.



Step 1: Connecting to the device

1. Connect one port (e.g. eth0/1) of the Hillstone device to your ISP network. In this way, "eth0/1" is in the untrust zone.
2. Connect your internal network to another Ethernet interface (e.g. eth0/0) of the device. This means "eth0/0" is connected to the trust zone.
3. Power on the Hillstone device and your PCs.
4. If one of the internal interfaces already has been configured with an IP address, use a browser to visit that address from one of your internal PCs.
If it is a new device, use the methods in "[Initial Visit to Web Interface](#)" on Page 3 to visit.
5. Enter "hillstone" for both the username and the password.

Step 2: Configuring interfaces

1. Go to **Network > Interface**.
2. Double click **eth0/1**.

In the Ethernet Interface dialog box, enter values

Option	Value
Binding Zone	L3-zone
Zone	untrust
Type	Static IP
IP Address	202.10.1.1 (public IP address provided by your ISP)
Netmask	255.255.255.0
Management	Select the protocols that you want to use to access the device.

- Click **OK**.

Step 3: Creating a NAT rule to translate internal IP to public IP

- Go to **Policy > NAT > SNAT**.
- Select **New**

In the SNAT Configuration dialog box, enter values

Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Egress	Egress interface, ethernet 0/1
Translated	Egress IP
Sticky	Enable

- Click **OK**.

Step 4: Creating a security policy to allow internal users to access the Internet.

1. Go to **Policy > Security Policy**.
2. Click **New**.

The screenshot shows the 'Policy Configuration' dialog box with the 'Basic' tab active. The following fields are highlighted with red boxes: Source Zone (trust), Source Address (any), Destination Zone (untrust), Destination Address (any), Service (any), and the Action radio button (Permit). The 'Options' tab is also visible, showing 'Enable Web Redirect' and 'Secured connection' options.

In the Policy Configuration dialog box, enter values.

Source Information	
Zone	trust
Address	Any
Destination Information	
Zone	untrust
Address	Any
Other Information	
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

3. Click OK.

Step 5: Configuring a default route

1. Go to **Network > Routing > Destination Route**.
2. Click **New**.

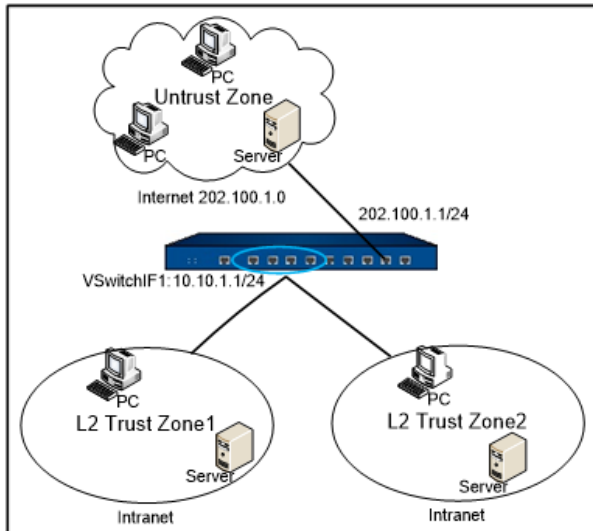
The screenshot shows the 'Destination Route Configuration' dialog box. The following fields are highlighted with red boxes: Virtual Router (trust-vr), Destination (0.0.0.0), Subnet Mask (0.0.0.0), Next Hop (Gateway), Gateway (202.10.1.1), Precedence (1), and Weight (1). The 'Current VRouter' and 'Other VRouter' radio buttons are also visible.

In the Destination Route Configuration dialog box, enter values.

Option	Value
Destination	0.0.0.0 (means all network)
Subnet Mask	0.0.0.0 (means all subnets)
Gateway	202.10.1.1 (gateway provided by your ISP)

Deploying Mix Mode

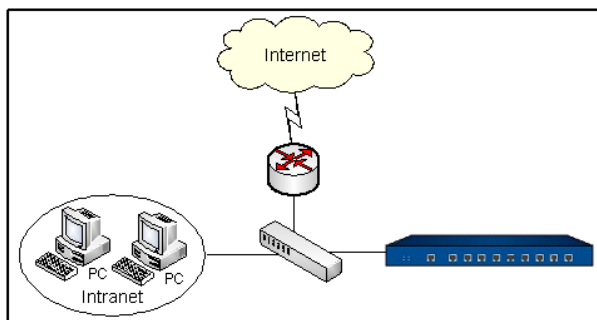
If the firewall has both L2 interfaces (transparent mode) and L3 interfaces (routing mode), the firewall is in mix mode.



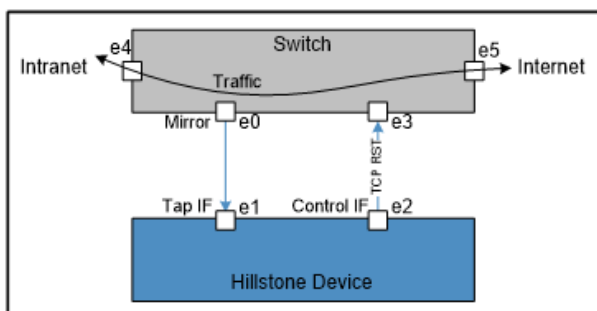
To configure a mix mode, you need to combine the routing mode of the deployment methods with the transparent mode. Please refer to these two modes.

Deploying Tap Mode

In most cases, the security device is deployed within the network as a serial node. However, in some other scenarios, an IT administrator would just want the auditing and statistical functions like IPS, antivirus, and Internet behavior control. For these features, you just need to connect the device to a mirrored interface of a core network. The traffic is mirrored to the security device for auditing and monitoring.



The bypass mode is created by binding a physical interface to a tap zone. Then, the interface becomes a bypass interface.



Use an Ethernet cable to connect e0 of the Switch with e1 of the Hillstone device. The interface e1 is the bypass interface and e2 is the bypass control interface. The interface e0 is the mirror interface of the switch. The switch mirrors the traffic to e1 and the Hillstone device will monitor, scan, and log the traffic received from e1. After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, viruses, or illegal network behaviors, it will send a TCP RST packet from e2 to the switch to tell it to reset the connections.



Note: Before configuring tap mode in the device, you need to set up an interface mirroring your primary switch. Mirror the traffic of the switch from e0 to e1, and the device can scan, monitor and count the mirrored traffic.

Here provides an example of monitoring IPS in tap mode.

Step 1: Creating tap mode by binding an interface

1. Select **Network > Zone**, and click **New**.

Basic

Zone: (1-31) characters

Description: (0-63) characters

Type: ☐ Layer 2 Zone ☐ Layer 3 Zone ☒ TAP

Virtual Router:

Binding Interface:

Removing an interface from a zone will clear the IP configuration of the interface.

Option	Value
Zone	enter a name, e.g. "tap-zone" .
Type	TAP
Binding Interface	Select the bypass interface (only a physical interface, aggregate interface or redundant interface can apply, sub-interface is not allowed).

2. Click **OK**.

Step 2: Creating an IPS rule

1. Select **Object > Intrusion Prevention System**.
2. Click **New**.
3. Enter the rule name.
4. Configure the signatures settings.
5. Configure the protocol settings.
6. Click **OK** to complete IPS rule configuration.

Step 3: Add IPS rule into Tap zone

1. Select Network > Zone, and double-click the tap zone created in step 1.
2. In the Treat Prevention tab, enable IPS and select the IPS rule created.

Intrusion Prevention System: ☒ Enable profile:

defense direc:

3. Click **OK**.

(Optional) Block traffic in switch

A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, viruses, or illegal network behaviors, it will send a TCP RST packet from e2 to the switch to tell it to reset the connections.

By default, the bypass interface itself is the control interface. However, you may also change the control interface.

To change a bypass control interface, you can only use the command line interface:

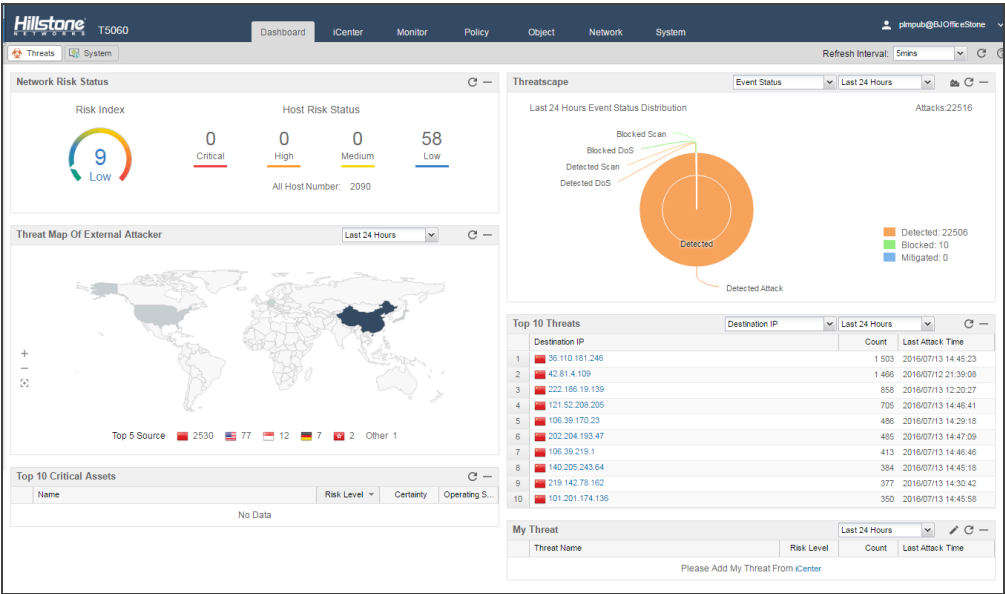
tap control-interface *interface-name*

- *interface-name* - Specifies which interface is used as the bypass control interface.

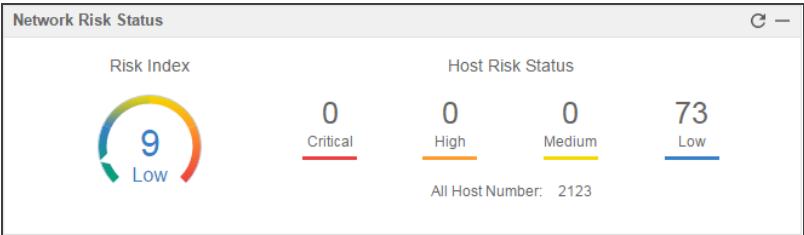
Chapter 3 Dashboard

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

The dashboard shows the system and threat information. The layout of the dashboard is shown below:



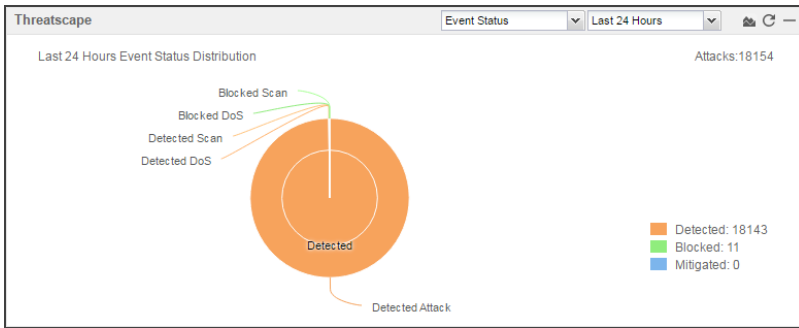
Network Risk Status



- Threat Index: Display the threat index of the system, The threat index is calculated by system based on the pro-active detection data. The score is divided into five levels. Low [0-25), Medium [25-50), High [50-75), Critical [75-100).
- Host Threat Status: Display the number of hosts for the four severity levels and the total number of hosts.

Threatscape

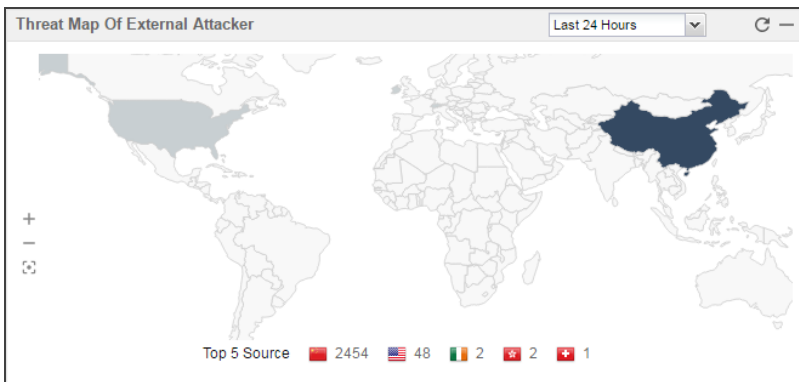
The threat information statistic chart are displayed within the [specified period](#).



- Click **Event Status** to specify the display type of chart.
- Hover your mouse over the chart to see the number of attacks.
- Click **Details** to jump to the iCenter page, and the list will display with the corresponding threat status, threat type or threat level.
- Click the to switch between the pie chart and the trend chart.

Threat Map of External Attacker

Display all the external attackers' geographic distribution in the map.



- Hover your mouse over the marked region to see the number of generated threats.

Threats

Display the top 10 threats information within the [specified period](#).

Top 10 Threats			
	Destination IP	Count	Last Attack Time
1	106.39.18.68	3	2016/07/21 09:02:17
2	10.188.15.38	1	2016/07/20 16:55:44
3	114.247.228.20	1	2016/07/21 13:14:49

- Click **Destination IP** to specify the type of display: Destination IP, Source IP or Threat Name.

Critical Assets

Display the risk level, certainty, and operating system of the top 10 critical assets.

Top 10 Critical Assets				
	Name	Risk Level	Certainty	Operating S...
1	20	High	95%	
2	10	Low	0%	
3	20 7	Low	0%	
4	20 8	Low	52%	
5	20	Low	0%	
6	20 5	Low	80%	
7	20 0	Low	54%	
8	20 9	Low	47%	

- Click the name of the critical asset to view the corresponding information in the Critical Assets page in iCenter.

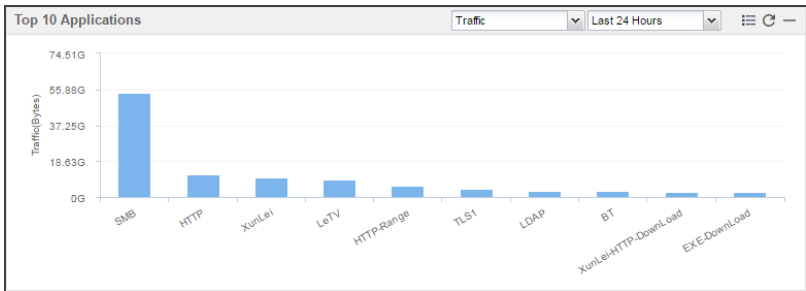
My Threats

Display the concerned threat information.

My Threat				
Threat Name		Risk Level	Count	Last Attack Time
Please Add My Threat From iCenter				

Application

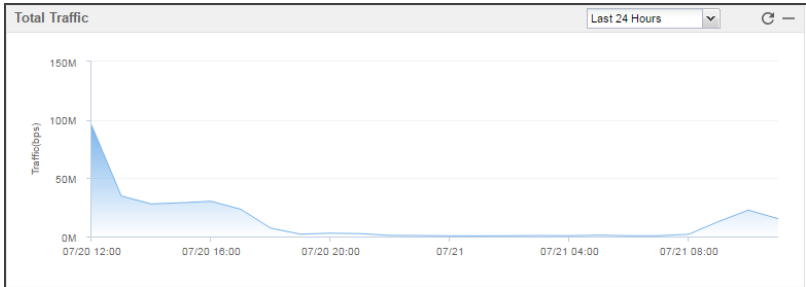
Display the top 10 application traffic information within the [specified period](#).



- Specify the type of display: by Traffic or by New Sessions from the drop-down menu.
- Click and , switch between the table and the bar chart.
- Hover your mouse over a bar, to view users' total traffic or new sessions.

Total Traffic/Concurrent Sessions/New Sessions

Show the Total Traffic/Concurrent Sessions/New Sessions within the [specified period](#).
















System Alarm

Display the detail information of untreated statistical alarm events within the [specified period](#) in tables.

System Alarm		
		Last 24 Hours
Severity	Message	Last Time
No Data		

Physical Interface

Display the statistical information of interfaces, including the interface name, IP address, upstream speed, downstream speed, and total speed.

Physical Interface					
	Name	IP Address	Speed Out	Speed In	Total Speed
1	 ethernet0/0	114.247.228.18/28	1.62 Mbps	2.51 Mbps	4.13 Mbps
2	 ethernet0/1	106.39.18.66/28	1.09 Mbps	1.42 Mbps	2.52 Mbps
3	 ethernet0/2	0.0.0.0/0	0 bps	0 bps	0 bps
4	 ethernet0/3	0.0.0.0/0	0 bps	0 bps	0 bps
5	 ethernet0/4	0.0.0.0/0	0 bps	0 bps	0 bps
6	 ethernet0/5	0.0.0.0/0	0 bps	0 bps	0 bps
7	 ethernet1/0	10.89.5.1/24	59.02 Kbps	601.4 Kbps	660.42 Kbps
8	 ethernet1/1	10.188.3.1/24	484.36 Kbps	33.61 Kbps	517.97 Kbps
9	 ethernet1/2	10.89.9.1/24	31.73 Kbps	42.46 Kbps	74.19 Kbps
10	 ethernet1/3	10.89.10.1/23	338.18 Kbps	366.03 Kbps	704.21 Kbps
11	 ethernet1/4	192.168.60.1/24	48.74 Kbps	4.58 Kbps	53.33 Kbps
12	 ethernet1/5	10.89.15.1/24	265.24 Kbps	275.6 Kbps	540.84 Kbps
13	 ethernet1/6	10.89.19.1/22	2.91 Mbps	2.07 Mbps	4.98 Mbps


System Information

System information include.

- Serial number: The serial number of the device.
- Host name: The host name of the device.
- Platform: The platform type of the device.
- System Time: The time of system.
- System Uptime: The running time of system.
- HA State: The HA State of device:
 - Standalone: Non-HA mode which represents HA is disabled.
 - Init: Initial state.
 - Hello: Negotiation state which represents the device is negotiating the relationship between master and backup.
 - Master: Master state which represents current device is master.
 - Backup: Backup state which represents current device is backup.
 - Failed: Fault state which represents the device is failed.
- Firmware: The version number and version time of the firmware running on the device.
- Boot File: The boot file name.
- Anti Virus Signature: The version number and time of the anti virus signature database.
- IPS Signature: The version number and time of the IPS signature database.
- URL Category Database: The version number and time of the URL category database.
- Application Signature: The version number and time of the application signature database.
- IP Reputation Database: The version number and time of the IP reputation database.

- Mitigation Rule Database: The version number and time of the mitigation rule database.
- Abnormal Behavior Model Database: The version number and time of the abnormal behavior model database.
- Malware Behavior Model Database: The version number and time of the malware behavior model database.

Specified Period

System supports the predefined time cycle and the custom time cycle. Click () on the top right corner of each tab to set the time cycle.

- Realtime: Display the statistical information within 5 minutes of the current time.
- Last Hour: Display the statistical information within the latest 1 hour.
- Last Day: Display the statistical information within the latest 1 day.
- Last Week: Display the statistical information within the latest 1 week.
- Last Month: Display the statistical information within the latest 1 month.
- Custom: Customize the time cycle. Select **Custom** and the **Custom Date and Time** dialog. Select the start time and the end time as needed.

In the top-right corner, you can set the refresh interface of the displayed data.

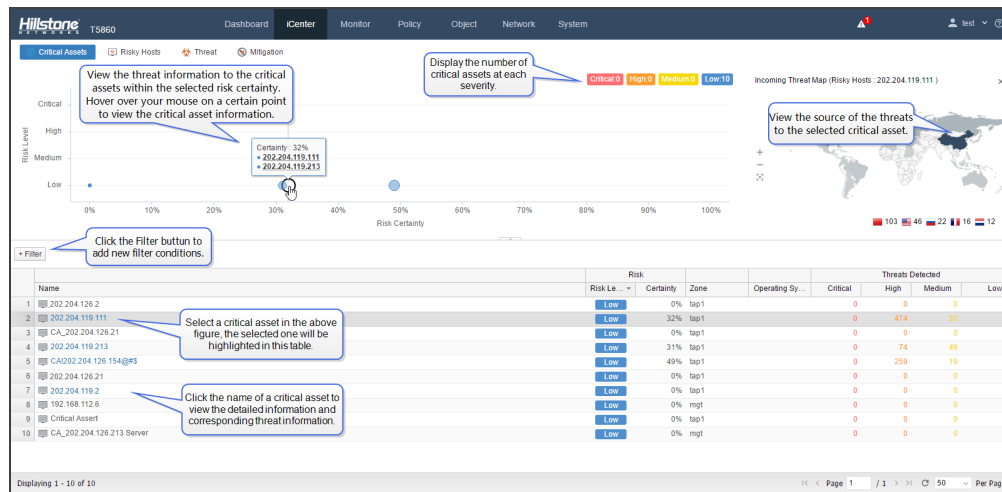
Chapter 4 iCenter

This feature may not be available on all platforms. Please check actual page in system to see whether your device delivers this feature.

The multi-dimensional features show all the critical assets, risky hosts, and threats to the whole network in depth. threats of the whole network.

Critical Assets

The Critical Assets page displays the detailed information of the critical assets and the related threat information. Click iCenter and the Critical Assets page will display then.

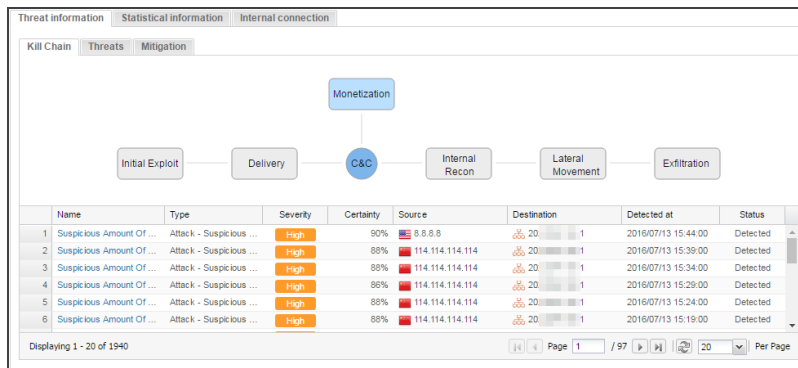


Click the link of the critical name in the list to view the following information of this critical asset:

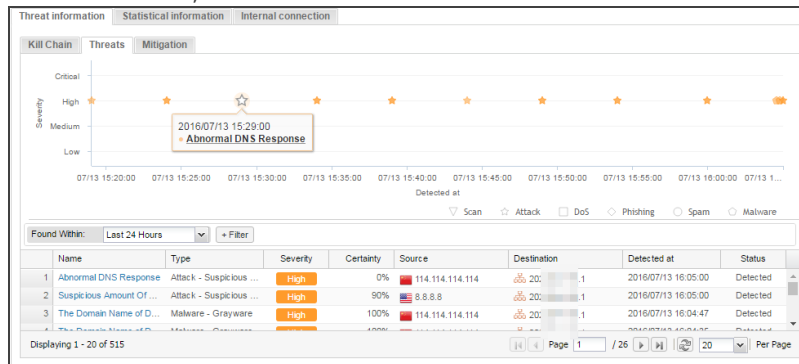
- Detailed information: Display the name of the critical asset, the hostname/IP (If the hostname cannot be identified, IP will be displayed), operating system, status, zone, risk level (the white line points to the risk level of this critical assets), and certainty.



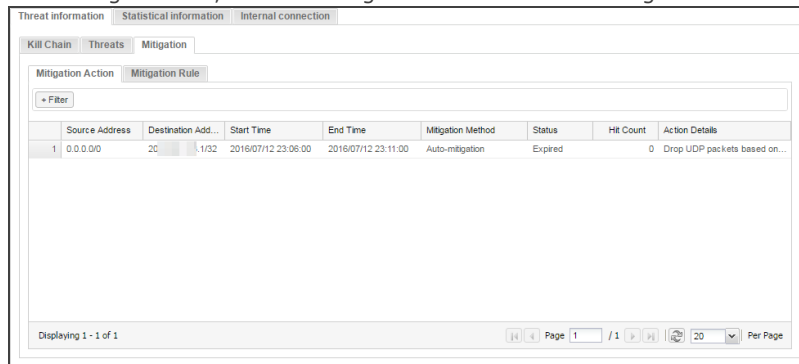
- Threat information: Displays the kill chain, threats, and mitigation.
 - In the Kill Chain tab, view the attacks and threats to this critical asset that exist in each stage of the kill chain. A highlighted stage means there are attacks and threats in this stage. Click this stage to display all threat information in this stage. Click the threat name in the list to view the threat information.



- In the Threats tab, view all attacks and threats from or to the critical asset.



- In the Mitigation tab, view the mitigation actions and the mitigation rules.



- Statistical information: The statistics about the applications, traffic, and connections related to the critical asset, including the statistic that the critical asset is the source IP of the sessions, the statistic that the critical asset is the destination IP of the sessions, and the statistic that the critical asset is source IP or destination IP.

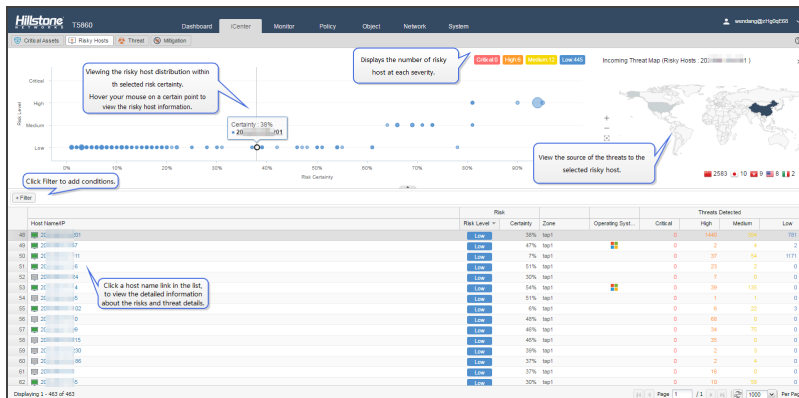
Threat information			
Statistical information			
Internal connection			
Application			
Traffic			
Connection			
Last 60 Minutes			
Destination IP			
Source IP			
All			
Application	Risk	Traffic	New Sessions
DNS	3	21.93 MB(0.94%)	197.85(0.90%)
eMule	5	4.07 KB(0.02%)	18(0.01%)
Youku-DNS	3	3.4 KB(0.02%)	24(0.01%)
Cyclone	5	3.37 KB(0.01%)	16(0.01%)
QIYI-DNS	3	1.39 KB(0.01%)	10(0.01%)
Xbox	3	220 B(0.00%)	2(0.00%)

- Internal connection: The Host tab displays the host information that interacts with the critical asset, the Address tab displays traffic and new sessions of IPs that interact with the critical asset, the Application tab displays traffic and new sessions of applications that interact with the critical asset.

Threat information			
Statistical information			
Internal connection			
Host			
Address			
Application			
Last 60 Minutes			
Destination IP			
Source IP			
All			
Source IP	Traffic	New Sessions	
12.101	516.42 KB(2.30%)	3.656(1.85%)	
20.1	220.35 KB(0.96%)	360(0.18%)	
17.43	163.45 KB(0.73%)	1.103(0.56%)	
17.335	160.31 KB(0.71%)	1.088(0.55%)	
17.42	157.49 KB(0.70%)	1.067(0.54%)	
17.41	153.81 KB(0.68%)	1.047(0.53%)	
12.5	133.76 KB(0.60%)	953(0.48%)	
Application	Risk	Traffic	New Sessions
DNS	3	516.36 KB(99.99%)	3.655(99.97%)
Xbox	3	68 B(0.01%)	1(0.03%)

Risky Hosts

Host risk refers to the attacker host and the victim host. Based on the threat level, the **Risky Hosts** tab displays the statistics of all risky hosts and threat information of the whole network. Select **iCenter > Risky Hosts**.

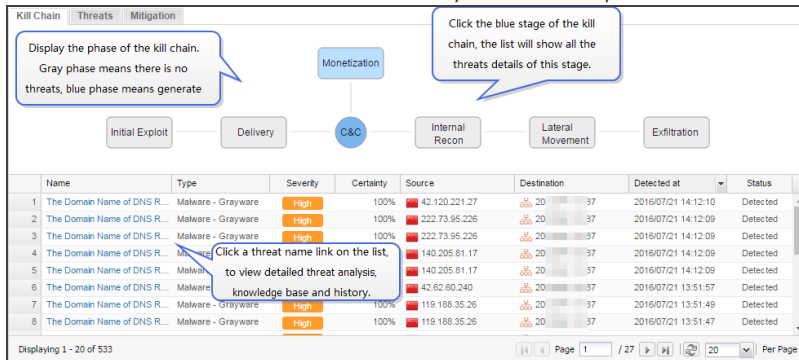


Click a host name link on the list to view detailed information about the risks, kill chain, and threat details.

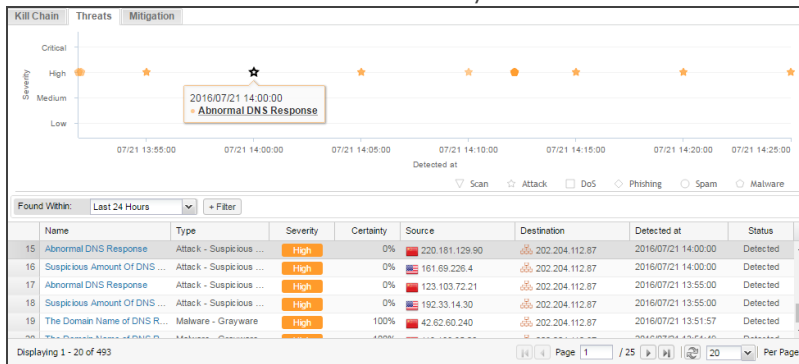
- Detailed information:** Displays the hostname/IP (if the hostname cannot be identified, the IP will be displayed), operating system, status, zone, risk level (the white line points to the risk level of this critical assets), and certainty.



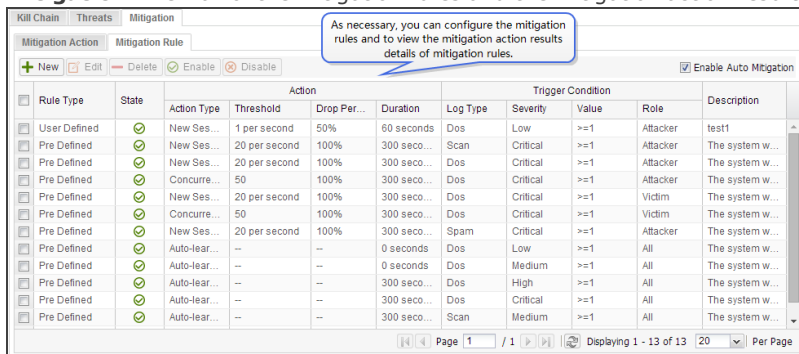
- **Kill Chain:** View the threat about the risky host in each phase of the kill chain.



- **Threats:** View all the threats about the risky host.



- **Mitigation:** View all of the mitigation rules and the mitigation action results details of mitigation rules.

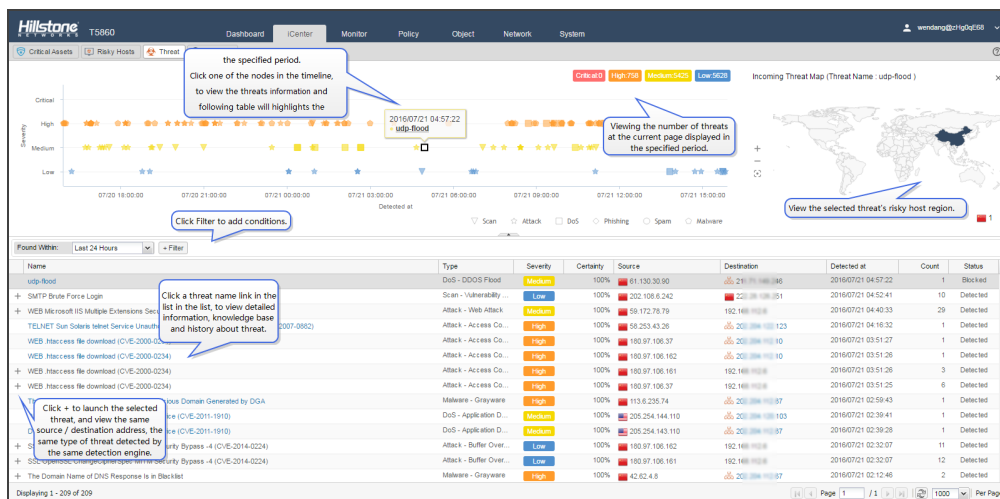


For a Mitigation function introduction, see "Mitigation" on Page 397.

Click a threat name link in the list to view the detailed information, source/destination, knowledge base and history about threat. For a detailed description, see the next section [Threat](#).

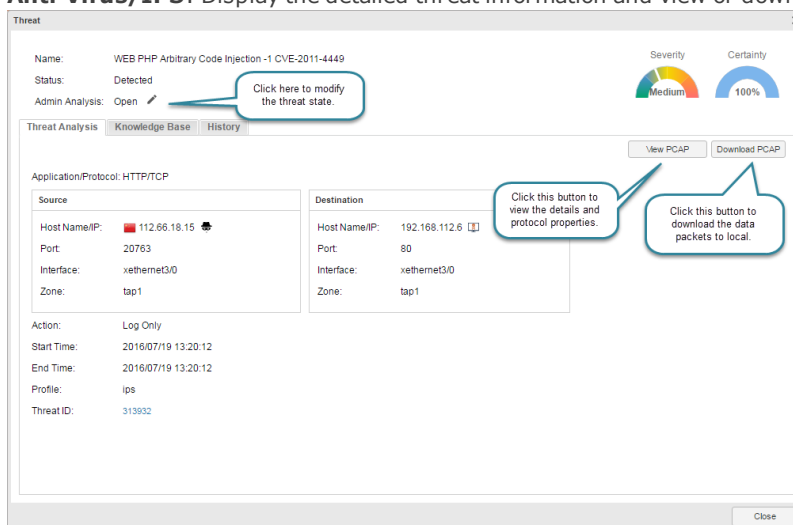
Threat

Threats tab statistics and displays the all threats information of the whole network within the "Specified Period" on Page 33. Click **iCenter**, and click **Threat** tab.



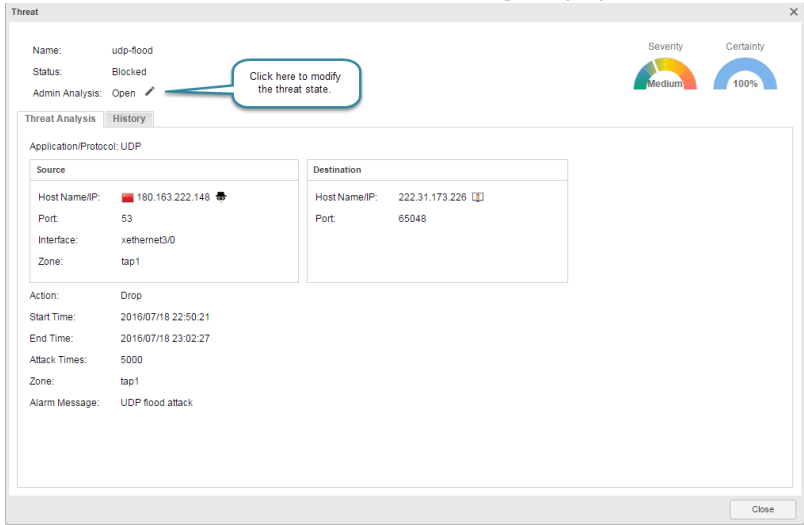
Click a threat name link in the list to view the detailed information , source/destination, knowledge base and history about the threat.

- Threat Analysis: Depending on the threats of the different detection engine , the content of Threat Analysis tab is also different.
- Anti Virus/IPS:** Display the detailed threat information and view or download the evidence packets.



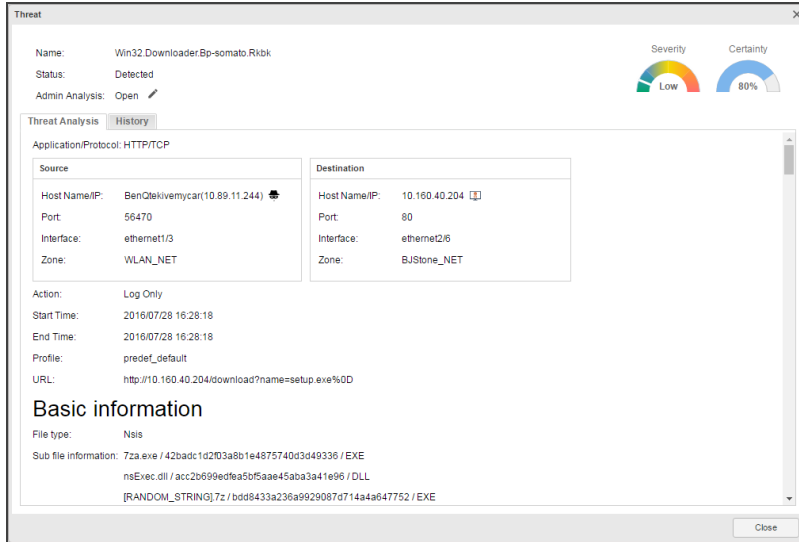
For the Anti Virus/IPS function introduction, see "Anti Virus" on Page 351/" Intrusion Prevention System" on Page 356.

- **Attack Defense/Perimeter Traffic Filtering:** Display the threat detailed information.



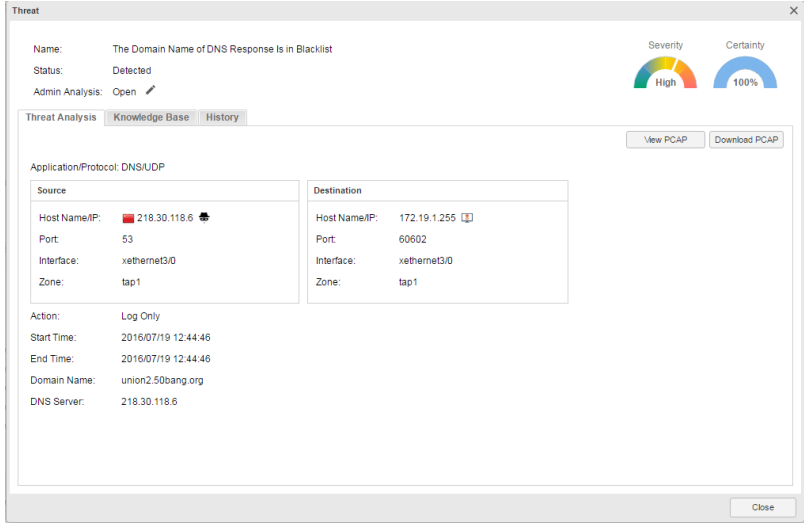
For the Attack Defense/Perimeter Traffic Filtering function introduction, see "Attack-Defense" on Page 382/"Perimeter Traffic Filtering" on Page 391.

- **Sandbox Threat Detection:** Display the detailed threat information of the suspicious file.



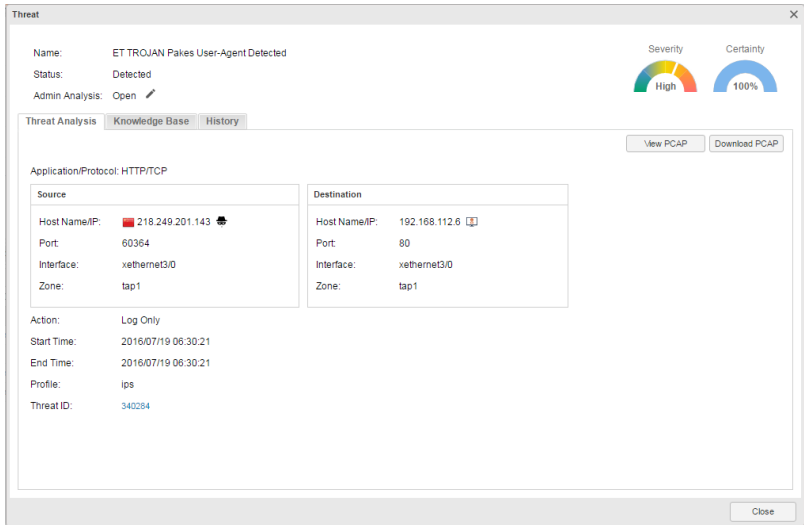
For the Sandbox function, see "Sandbox" on Page 376.

- **Abnormal Behavior Detection:** Display the abnormal behavior detection information.



For the Abnormal Behavior Detection function introduction, see "Abnormal Behavior Detection" on Page 394.

- **Advanced Threat Detection:** Display the advanced threat detection information, malware reliability information etc.



For the Advanced Threat Detection function introduction, see "Advanced Threat Detection" on Page 400.

- **Anti-Spam:** Display the spam filter information, such as sender and subject of spam.

Threat

Name:Valid Bulk

Status:Detected

Admin Analysis:Open

Severity

Certainty

Threat Analysis

History

Application/Protocol:POP3/TCP

Source

Host Name/IP:220.181.12.110

Port:110

Interface:ethernet0/2

Zone:trust

Destination

Host Name/IP:192.168.1.2

Port:46361

Interface:ethernet0/3

Zone:trust

Action:Log Only

Start Time:2017/11/17 17:50:22


End Time:2017/11/17 17:50:22

Sender:ccsvc@message.cmbchina.com

Subject:招商银行信用卡电子账单2017年11月

Profile:test

For the Anti-Spam information, see "Anti-Spam" on Page 402.

- Knowledge Base: Display the specified threat description, solution, etc. of the threats detected by IPS , Abnormal Behavior Detection and Advanced Threat Detection.
- Threat History: Display the selected threat historical information of the whole network .
- Admin Analysis: Click  to modify the threat state(Ignore, Confirmed, False Positive, Fixed)

Admin Analysis [X]

Marking: False Positive [v] [View history]

Marking Scope: ☒ Only one ☐ All
 [v] More Options

Signature Processing: ☒ Disable Signature ☒ Add Whitelist
☐ Source Address ☐ Destination Address

Comment: [Text Area]

[OK] [Cancel]

In the Admin Analysis dialog box, enter the configurations.

Option	Description
Marking	Select the state of threat, includes Ignore, Confirmed, False Positive and Fixed.
View history	View the analysis history of selected threat.
Marking Scope	Select the marking scope of the threat entry . The system supports batch tagging of the threat entries of same source address or the same destination address, aggregated threat entries, or all threat entries.

Option	Description
Signature Processing	<p>When the selected IPS threat entry is marked as False Positives, the corresponding signature ID can be disabled or added to the white list.</p> <ul style="list-style-type: none"> • Disable Signature : Select Disable Signature checkbox to disable the signature ID of selected threat entry. • Add Whitelist: Select Add Whitelist checkbox to add the corresponding signature ID to the IPS white list, the system no longer reports alarms or blocks to the white list, thus reducing the false alarm rate of threats. <ul style="list-style-type: none"> • Source Address: Select Source Address checkbox to add the corresponding signature ID and the corresponding source address to the white list. • Destination Address: Select Destination Address checkbox to add the corresponding signature ID and the corresponding destination address to the white list. <p>Note: About the IPS White list, see "Configuring IPS White list" on Page 375</p> <p>When the selected Attack Defense threat entry is marked as False Positives, the corresponding source address can be added to the white list.</p> <ul style="list-style-type: none"> • Add Whitelist: Select Add Whitelist checkbox to add the corresponding source address to the whitelist , and the IP address is exempt from attack defense check. <p>Note: About whitelist, see the Whitelist configuration of "Configuring Attack Defense" on Page 384.</p>

Mitigation

For the Mitigation function introduction, see ["Mitigation" on Page 397](#).

Chapter 5 Network

This chapter describes factors and configurations related to network connection, including:

- **Security Zone:** The security zone divides the network into different section, such as the trust zone and the untrust zone. The device can control the traffic flow from and to security zones once the configured policy rules have been applied.
- **Interface:** The interface allows inbound and outbound traffic flow to security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone.
- **MGT Interface:** To facilitate the management of the device and meet the requirement of separating the management traffic from the data traffic, system has an independent management interface(MGT Interface).
- **VLAN:** Virtual LAN.
- **DNS:** Domain Name System.
- **DHCP:** Dynamic Host Configuration Protocol.
- **DDNS:** Dynamic Domain Name Server.
- **PPPoE:** Point-to-Point Protocol over Ethernet.
- **Virtual-Wire:** The virtual wire allows direct Layer 2 communications between sub networks.
- **Virtual Router:** Virtual Router (Virtual Router for short) acts as a router. Different Virtual Routers have their own independent routing tables.
- **Virtual Switch:** Running on Layer 2, VSwitch acts as a switch. Once a Layer 2 security zone is bound to a VSwitch, all the interfaces bound to that zone will also be bound to the VSwitch.
- **Port Mirroring:** Allow users to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.
- **Link Load Balancing:** It takes advantage of dynamic link detection technique to assign traffic to different links appropriately, thus making full use of all available link resources.
- **Application Layer Gate:** ALG can assure the data transmission for the applications that use multiple channels and assure the proper operation of VoIP applications in the strictest NAT mode.
- **Global Network Parameters:** These parameters mainly include the IP packet's processing options, like IP fragmentation, TCP MSS value, etc.

Security Zone

Security zone is a logical entity. One or more interfaces can be bound to one zone. A zone applied with a policy is known as a security zone, while a zone created for a specific function is known as a functional zone. Zones have the following features:

- An interface should be bound to a zone. A Layer 2 zone will be bound to a VSwitch, while a Layer 3 zone will be bound to a VRouter. Therefore, the VSwitch to which a Layer 2 zone is bound decides which VSwitch the interfaces belong to in that Layer 2 zone, and the VRouter to which a Layer 3 zone is bound decides which VRouter the interfaces belong to in that Layer 3 zone.
- Interfaces in Layer 2 and Layer 3 are working in Layer 2 mode and Layer 3 mode respectively.
- System supports internal zone policies, like trust-to-trust policy rule.

There are 8 pre-defined security zones in StoneOS, which are trust, untrust, dmz, L2-trust, L2-untrust, L2-dmz, vpn-hub (VPN functional zone) and ha (HA functional zone). You can also customize security zones. Pre-defined security zones and user-defined security zones have no difference in functions, so you can make your choice freely.

Configuring a Security Zone

To create a security zone, take the following steps:

1. Select **Network > Zone**.
2. Click **New**.

Zone Configuration

Basic Threat Protection Data Security

Basic

Zone: (1-31) chars

Description: (0-63) chars

Type: ☐ Layer 2 Zone ☒ Layer 3 Zone ☐ TAP

Virtual Router:

Binding Interface:

Removing an interface from a zone will clear the IP configuration of the interface.

Advanced

Application Identification: ☐ Enable

WAN Zone: ☐ Enable

NetBIOS over TCP/IP (NBT) Cache: ☐ Enable

Share Access Detect: ☐ Enable

OK Cancel

3. In the Zone Configuration text box, type the name of the zone into the Zone box.
4. Type the descriptions of the zone in the Description text box.
5. Specify a type for the security zone. For a Layer 2 zone, select a VSwitch for the zone from the VSwitch drop-down list below; for a Layer-3 zone, select a VRouter from the Virtual Router drop-down list. If TAP is selected, the zone created is a tap zone, which is used in Bypass mode.
6. Bind interfaces to the zone. Select an interface from the Binding Interface drop-down list.
7. If needed, select the **Enable** check box to enable APP identification for the zone.

8. If needed, select the **Enable** check box to set the zone to a WAN zone, assuring the accuracy of the statistic analysis sets that are based on IP data.
9. If needed, select the **Enable** check box to enable NetBIOS host query for the zone. For detailed instructions, see ["DNS" on Page 73](#).
10. If needed, select the **Enable** check box to enable share access detect for the zone. It is a share access detect method based on the application characteristic, which is used to detect the users' private behavior of shared access to Internet. For detailed instructions, see ["Share Access Detect" on Page 410](#).
11. If needed, select Threat Protection tab and configure the parameters for Threat Protection function. For detailed instructions, see ["Chapter 11 Threat Prevention" on Page 349](#).
12. If needed, select Data Security tab and configure the parameters for Data Security function. For detailed instructions, see ["Data Security" on Page 281](#).
13. Click **OK**.



Note:

- Pre-defined zones cannot be deleted.
- When changing the VSwitch to which a zone belong, make sure there is no binding interface in the zone.

Interface

Interfaces allow inbound and outbound traffic to flow to security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface, and the corresponding policy rules should also be configured to allow traffic transmission between different security zones. Multiple interfaces can be bound to one security zone, but one interface cannot be bound to multiple security zones.

The security devices support various types of interfaces which are basically divided into physical and logical interfaces based on the nature.

- **Physical Interface:** Each Ethernet interface on devices represents a physical interface. The name of a physical interface, consisting of media type, slot number and location parameter, is pre-defined, like ethernet2/1 or ethernet0/2.
- **Logical Interface:** Include sub-interface, VSwitch interface, VLAN interface, loopback interface, tunnel interface, aggregate interface, redundant interface, PPPoE interface and Virtual Forward interface.

Interfaces can also be divided into Layer 2 interface and Layer 3 interface based on their security zones.

- **Layer 2 Interface:** Any interface in Layer 2 zone or VLAN.
- **Layer 3 Interface:** Any interface in Layer 3 zone. Only Layer 3 interfaces can operate in NAT/routing mode.

Different types of interfaces provide different functions, as described in the table below.

Type	Description
Sub-interface	The name of an sub-interface is an extension to the name of its original interface, like ethernet0/2.1. System supports the following types of sub-interfaces: Ethernet sub-interface, aggregate sub-interface and redundant sub-interface. An interface and its sub-interfaces can be bound to one single security zone, or to different zones.
VSwitch interface	A Layer 3 interface that represents the collection of all the interfaces of a VSwitch. The VSwitch interface is virtually the upstream interface of a switch that implements packet forwarding between Layer 2 and Layer 3.
VLAN interface	A Layer 3 interface that represents the collection of all the Ethernet interfaces within a VLAN. If only one Ethernet interface is in UP state, the VLAN interface will be UP as well. The VLAN interface is the outbound communication interface for all the devices within a VLAN. Typically its IP address is the gateway's address of the network device within the VLAN.
Loopback interface	A logical interface. If only the security device with loopback interface configured is in the working state, the interface will be in the working state as well. Therefore, the loopback interface is featured with stability.
Tunnel interface	Only a Layer 3 interface, the tunnel interface acts as an ingress for VPN communications. Traffic flows into VPN tunnel through this interface.
Aggregate interface	Collection of physical interfaces that include 1 to 16 physical interfaces. These interfaces averagely share the traffic load to the IP address of the aggregate interface, in an attempt to increase the available bandwidth for a single IP address. If one of the physical interfaces within an aggregate interface fails, other physical interfaces can still process the traffic normally. The only effect is the available bandwidth will decrease.
Redundant interface	The redundant interface allows backup between two physical interfaces. One physical interface, acting as the primary interface, processes the inbound traffic, and another interface, acting as the alternative interface, will take over the processing if the primary interface fails.
PPPoE interface	A logical interface based on Ethernet interface that allows connection to PPPoE servers over PPPoE protocol.
Virtual Forward interface	In HA environment, the Virtual Forward interface is HA group's interface designed for traffic transmission.

Configuring an Interface

The configuration options for different types of interfaces may vary. For more information, see the following instructions.

Both IPv4 and IPv6 address can be configured for the interface, but IPv6 address is not supported for the PPPoE interface.

Creating a PPPoE Interface

To create a PPPoE interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > PPPoE Interface**.



In the **Basic** tab, configure the following.

Option	Description
Interface Name	Specifies a name for the PPPoE interface.
Description	Enter descriptions for the PPPoE interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 zone. If TAP is selected, the interface will bind to a tap zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Select this check box to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not selecting this check box disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
User	Specifies a username for PPPoE.
Password	Specifies PPPoE user's password.
Confirm password	Enter the password again to confirm.
Idle interval	If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connections; if the interface requires Internet access, the system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.
Re-connect interval	Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.
Set gateway information from PPPoE server as the default gateway route	With this selected checkbox, system will set the gateway information provided by PPPoE server as the default gateway route.
Advanced	In the Advanced dialog, configure advanced options for PPPoE, includ-

Option	Description
	<p>ing:</p> <ul style="list-style-type: none"> • Access concentrator - Specifies a name for the concentrator. • Authentication - The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). • Netmask - Specifies a netmask for the IP address obtained via PPPoE. • Static IP - You can specify a static IP address and negotiate about using this address to avoid IP change. To specify a static IP address, type it into the box. • Distance - Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight - Specifies a route weight. The value range is 1 to 255. The default value is 1. • Service - Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically.
DDNS	In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	<p>Enable or Disable reverse route as needed:</p> <ul style="list-style-type: none"> • Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is to say, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
WAP Traffic Distribution	<p>Select the Enable check box and configure as follows:</p> <ul style="list-style-type: none"> • Destination IP Replacement: Select the Enable check box, and specify the logs you need to record. If All is selected in WAP Log Record section, system will record all the traffic logs; while if Destination IP Replacement radio button is selected, system will record logs for the translated traffic. • Destination Service Port 1/Destination Service Port 2: Specifies the HTTP port number for the WAP gateway.
Proactive	Select the Enable check box to enable proactive webauth function and

Option	Description
WebAuth	<p>Specify the AAA server.</p> <p>After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.</p>

In the Properties tab, configure properties for the interface.

Option	Description
MTU	Specifies a MTU for the interface. The value range is 1280 to 1500/1800 bytes. The default value is 1500. The max MTU may vary on different Hillstone platforms.
ARP Learning	Select the Enable checkbox to enable ARP learning.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.
MAC clone	Select the MAC clone check box to enable the MAC clone function. System clones a MAC address in the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will restore the default MAC address.
Mirror	Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.

In the Advanced tab, configure advanced options for the interface.

Option	Description
Shutdown	<p>System supports interface shutdown. You can not only force a specific interface to shut down, but also control the time it shuts down by schedule or according to the link status of tracked objects. Configure the options as below:</p> <ol style="list-style-type: none"> 1. Select the Shut down check box to enable interface shutdown. 2. To control the shutdown by schedule or tracked objects, select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list.
Monitor and Backup	<p>Configure the options as below:</p> <ol style="list-style-type: none"> 1. Select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list. 2. Select an action: <ul style="list-style-type: none"> • Shut down the interface: During the time specified in the schedule, or when the tracked object fails, the interface will be shut down and its related route will fail;

Option	Description
	<ul style="list-style-type: none"> Migrate traffic to backup interface: During the time specified in the schedule, or when the tracked object fails, traffic flowing to the interface will be migrated to the backup interface. In such a case you need to select a backup interface from the Backup interface drop-down list and type the time into the Migrating time box. (Migrating time, 0 to 60 minutes, is the period during which traffic is migrated to the backup interface before the primary interface is switched to the backup interface. During the migrating time, traffic is migrated from the primary interface to the backup interface smoothly. By default the migrating time is set to 0, i.e., all the traffic will be migrated to the backup interface immediately.)

In the RIP tab, configure RIP for the interface.

Option	Description
Authentication mode	Specifies a packet authentication mode for the system, including plain text (the default) and MD5. The plain text authentication, during which unencrypted string is transmitted together with the RIP packet, cannot assure security, so it cannot be applied to the scenarios that require high security.
Authentication string	Specifies a RIP authentication string for the interface.
Transmit version	Specifies a RIP information version number transmitted by the interface. By default V1&V2 RIP information will be transmitted.
Receive version	Specifies a RIP information version number transmitted by the interface. By default V1&V2 RIP information will be transmitted.
Split horizon	Select the Enable checkbox to enable split horizon. With this function enabled, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent.

3. Click **OK**.

Creating a Tunnel Interface

To create a tunnel interface:

1. Select **Network > Interface**.
2. Select **New > Tunnel Interface**.

The screenshot shows the 'Tunnel Interface' configuration window with the 'Basic' tab selected. The configuration includes:

- Interface Name:** tunnel (1-1024)
- Description:** (0-63) chars
- Binding Zone:** Layer 2 Zone, **Layer 3 Zone** (selected), TAP, No Binding
- Zone:** mgt
- HA sync:** ☒ Enable
- IP Configuration:**
 - Type: **Static IP** (selected), DHCP, PPPoE
 - IP Address:
 - Net mask:
 - ☐ Set as Local IP
 - ☐ Enable DNS Proxy (Proxy selected, Proxy-Trans)
 - ☐ Enable DNS Bypass
 - Advanced, DHCP...
- Management:** Telnet, SSH, Ping, HTTP, HTTPS, SNMP
- Routing:** Reverse Route: Enable, Close, **Auto** (selected)
- WAP traffic distribution:** ☐ Enable

In the Basic tab, configure the following.

Option	Description
Interface Name	Specifies a name for the tunnel interface.
Description	Enter descriptions for the tunnel interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 zone. If TAP is selected, the interface will bind to a tap zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Select this check box to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not selecting this check box disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In a HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Enable DNS Proxy: Select this check box to enable DNS proxy for the interface.
	<ul style="list-style-type: none"> When the general DNS proxy is in use, the client in the network will still get DNS replies from the DNS server configured on itself. If the DNS server address is configured as an interface address of Hillstone device, the device will work as a DNS server; When the transparent DNS proxy is in use, the Hillstone device will reply all DNS requests. In such a case, there is no need to edit DNS configuration on each client. DNS service can be easily controlled by modifying the device's DNS configuration.
	Enable DNS Bypass: Select this check box to enable DNS bypass for the interface.
	Advanced: <ul style="list-style-type: none"> Management IP: Specifies a management IP for the interface. Type the IP address into the box. Secondary IP: Specifies secondary IPs for the interface. You can specify up to 6 secondary IP addresses.
Auto-obtain	DHCP: In the DHCP Configuration dialog, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 77 .
	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.
	Advanced: <ul style="list-style-type: none"> Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also learn DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server according to its priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20.
Management	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
	Select one or more management method check boxes to configure the interface management method.
Reverse Route	Enable or Disable reverse route as needed:

Option	Description
	<ul style="list-style-type: none"> • Enable: Enforces to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Tunnel Binding	<p>Bind the interface to a IPsec VPN tunnel or a SSL VPN tunnel. One tunnel interface can be bound to multiple IPsec VPN tunnels, while only to one SSL VPN tunnel.</p> <ul style="list-style-type: none"> • IPsec VPN: Select IPsec VPN radio button. Specifies a name for the IPsec VPN tunnel that is bound to the interface. Then select a next-hop address for the tunnel, which can either be the IP address or the egress IP address of the peering tunnel interface. This parameter, which is 0.0.0.0 by default, will only be valid when multiple IPsec VPN tunnels is bound to the tunnel interface. • SSL VPN: Select SSL VPN radio button. Specifies a name for the SSL VPN tunnel that is bound to the interface.
Proactive WebAuth	<p>Select the Enable check box to enable proactive webauth function and Specify the AAA server.</p> <p>After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.</p>

3. In the **IPv6 Configuration** tab, configure the following.

Option	Description
Enable	Enable IPv6 in the interface.
IPv6 Address	Specifies the IPv6 address prefix.
Prefix Length	Specifies the prefix length.
Autoconfig	<p>Select the checkbox to enable Auto-config function. In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address.</p> <ul style="list-style-type: none"> • Set Default Route - If the interface is configured with a default router, this option will generate a default route to the default router.
Advanced	

Option	Description
Static	Click Add button to add several IPv6 address, at most 5 IPv6 addresses.. Click Delete button to delete IPv6 address.
Dynamic	Shows IPv6 address which is dynamic.
Link-local	Specifies link-local address. Link-local address is used for communication between adjacent nodes of a single link. For example, communication between hosts when there are no routers on the link. By default system will generate a link-local address for the interface automatically if the interface is enabled with IPv6 (in the interface configuration mode, use the command <code>ipv6 enable</code>). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one.
MTU	Specifies an IPv6 MTU for an interface.
DAD Attempts	Specifies NS packet attempt times. The value range is 0 to 20. Value 0 indicates DAD is not enabled on the interface. If system does not receive any NA response packets after sending NS packets for the attempt times, it will verify that the IPv6 address is an unique available address. DAD (Duplicate Address Detection) is designed to verify the uniqueness of IPv6 addresses. This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving a NS packet, if any other host on the link finds that the address of the NS requester is duplicated, it will send a NA (Neighbor Advertisement) packet advertising that the address is already in use, and then the NS requester will mark the address as duplicate, indicating that the address is an invalid IPv6 address.
ND Interval	Specifies an interval for sending NS packets.
ND Reachable Time	Specifies reachable time. After sending an NS packet, if the interface receives acknowledgment from a neighbor within the specified time, it will consider the neighbor as reachable. This time is known as reachable time.
Hop Limit	Specifies the hop limit. Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface.
ND RA Suppress	Select the checkbox to disable RA suppress on LAN interfaces. By default, FDDI interface configured with IPv6 unicast route will send RA packets automatically, and interfaces of other types will not send RA packets.
Manage IP/MASK	Specifies the manage IP/MASK.

4. "In the Properties tab, configure properties for the interface." on Page 49
5. "In the Advanced tab, configure advanced options for the interface." on Page 49
6. "In the RIP tab, configure RIP for the interface." on Page 50
7. Click **OK**.

Creating a Virtual Forward Interface

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To create a virtual forward interface, take the following steps:

1. Select **Network > Interface**.
2. Select **New > Virtual Forward Interface**.

The screenshot shows the 'Virtual Forward Interface' configuration window with the 'Basic' tab selected. The configuration includes:

- Interface Name:** aggregate3 (1-1)
- Description:** (0-63) chars
- Binding Zone:** Layer 2 Zone, **Layer 3 Zone** (selected), TAP, No Binding
- Zone:** mgt
- IP Configuration:**
 - Type: **Static IP** (selected), DHCP, PPPoE
 - IP Address:
 - Net mask:
 - ☐ Set as Local IP
 - ☐ Enable DNS Proxy, **Proxy** (selected), Proxy-Trans
 - ☐ Enable DNS Bypass
 - Advanced, DHCP... (selected), DDNS
- Management:**
 - ☐ Telnet, ☐ SSH, ☐ Ping, ☐ HTTP, ☐ HTTPS, ☐ SNMP
- Routing:**
 - Reverse Route: ☐ Enable, ☐ Close, **Auto** (selected)
 - WAP traffic distribution: ☐ Enable

In the **Basic** tab, configure the following.

Option	Description
Interface Name	Specifies a name for the virtual forward interface.
Description	Enter descriptions for the virtual forward interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 zone. If TAP is selected, the interface will bind to a tap zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In a HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Enable DNS Proxy: Select this check box to enable DNS proxy for the interface.
	<ul style="list-style-type: none"> When the general DNS proxy is in use, the client in the network will still get DNS replies from the DNS server configured on itself. If the DNS server address is configured as an interface address of Hillstone device, the device will work as a DNS server; When the transparent DNS proxy is in use, all DNS requests will be replied by the Hillstone device. In such a case, there is no need to edit DNS configuration on each client. DNS service can be easily controlled by modifying the device's DNS configuration.
	Enable DNS Bypass: Select this check box to enable DNS bypass for the interface.
	Advanced: <ul style="list-style-type: none"> Management IP: Specifies a management IP for the interface. Type the IP address into the box. Secondary IP: Specifies secondary IPs for the interface. You can specify up to 6 secondary IP addresses.
Auto-obtain	DHCP: In the DHCP Configuration dialog, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 77 .
	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.
	Advanced: <ul style="list-style-type: none"> Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also learn DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server according to its priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20.
Management	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
	Select one or more management method check boxes to configure the interface management method.
Reverse Route	Enable or Disable reverse route as needed:

Option	Description
	<ul style="list-style-type: none"> • Enable: Enforces to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
WAP Traffic Distribution	<p>Select the Enable check box and configure as follows:</p> <ul style="list-style-type: none"> • Destination IP Replacement: Select the Enable check box, and specify the logs you need to record. If All is selected in WAP Log Record section, system will record all the traffic logs; while if Destination IP Replacement radio button is selected, system will record logs for the translated traffic. • Destination Service Port 1/Destination Service Port 2: Specifies the HTTP port number for the WAP gateway.
Proactive WebAuth	<p>Select the Enable check box to enable proactive webauth function and Specify the AAA server.</p> <p>After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.</p>

3. "In the IPv6 Configuration tab, configure the following." on Page 53
4. "In the Properties tab, configure properties for the interface." on Page 49
5. "In the Advanced tab, configure advanced options for the interface." on Page 49
6. "In the RIP tab, configure RIP for the interface." on Page 50
7. Click **OK**.

Creating a Loopback Interface

To create a loopback interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Loopback Interface**.

In the **Basic** tab, configure the following.

Option	Description
Interface Name	Specifies a name for the loopback interface.
Description	Enter descriptions for the loopback interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 zone. If TAP is selected, the interface will bind to a tap zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Select this check box to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not selecting this check box disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuration	
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In a HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Enable DNS Bypass: Select this check box to enable DNS bypass for the interface.
	DHCP: In the DHCP Configuration dialog, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 77 . DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
Auto-obtain	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
Management	Select one or more management method check boxes to configure the interface management method.

Option	Description
Reverse Route	<p>Enable or Disable reverse route as needed:</p> <ul style="list-style-type: none"> • Enable: Enforces to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Proactive WebAuth	<p>Select the Enable check box to enable proactive webauth function and Specify the AAA server.</p> <p>After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.</p>

3. "In the IPv6 Configuration tab, configure the following." on Page 53
4. "In the Properties tab, configure properties for the interface." on Page 49
5. "In the Advanced tab, configure advanced options for the interface." on Page 49
6. "In the RIP tab, configure RIP for the interface." on Page 50
7. Click **OK**.

Creating an Aggregate Interface

To create an aggregate interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Aggregate Interface**.

3. In the Basic tab, configure the following.

Option	Description										
Interface Name	Specifies a name for the aggregate interface.										
Description	Enter descriptions for the aggregate interface.										
Binding Zone	<p>Specifies the zone type.</p> <p>If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone.</p> <p>If TAP is selected, the interface will bind to a tap zone.</p> <p>If No Binding is selected, you should also select a VLAN/aggregate interface/redundant interface:</p> <table> <tr> <th>Belong to</th><th>Description</th></tr> <tr> <td>VLAN</td><td> <p>Acess The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</p> <p>Trunk The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</p> </td></tr> <tr> <td>Aggregate Interface</td><td>The interface you specified belongs to an aggregate interface. Choose an aggregate interface which the aggregate interface belongs to from the Interface Group drop-down list.</td></tr> <tr> <td>Redundant Interface</td><td>This interface belongs to a redundant interface. Select that redundant interface from the Interface Group drop-down list.</td></tr> <tr> <td>None</td><td>This interface does not belong to any object.</td></tr> </table>	Belong to	Description	VLAN	<p>Acess The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</p> <p>Trunk The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</p>	Aggregate Interface	The interface you specified belongs to an aggregate interface. Choose an aggregate interface which the aggregate interface belongs to from the Interface Group drop-down list.	Redundant Interface	This interface belongs to a redundant interface. Select that redundant interface from the Interface Group drop-down list.	None	This interface does not belong to any object.
Belong to	Description										
VLAN	<p>Acess The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</p> <p>Trunk The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</p>										
Aggregate Interface	The interface you specified belongs to an aggregate interface. Choose an aggregate interface which the aggregate interface belongs to from the Interface Group drop-down list.										
Redundant Interface	This interface belongs to a redundant interface. Select that redundant interface from the Interface Group drop-down list.										
None	This interface does not belong to any object.										
Zone	Select a security zone from the Zone drop-down list.										
LACP	<ul style="list-style-type: none"> Forced: Aggregates multiple physical interfaces to form an aggreg- 										

Option	Description
	<p>ate interface. These physical interfaces will share the traffic passing through the aggregate interface equally.</p> <ul style="list-style-type: none"> Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are: <ul style="list-style-type: none"> System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be. Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby. Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregation group will change to Standby automatically and will not forward any traffic.
HA sync	Select this check box to enable HA sync function. The primary device will synchronize its information with the backup device.
IP Configuration	
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In a HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Enable DNS Bypass: Select this check box to enable DNS bypass for the interface.
	<p>DHCP: In the DHCP Configuration dialog, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 77.</p> <p>DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81.</p>
Auto-obtain	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see " DDNS " on Page 81.
PPPoE	<p>Obtain IP through PPPoE. Configure the following options:</p> <ul style="list-style-type: none"> User - Specifies a username for PPPoE. Password - Specifies PPPoE user's password. Confirm password - Enter the password again to confirm. Idle interval - If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, the system will disconnect the Internet connection; if the interface requires Internet access, the system will connect to the Internet automatically. The

Option	Description
	<p>value range is 0 to 10000 minutes. The default value is 30.</p> <ul style="list-style-type: none"> • Re-connect interval - Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled. • Set gateway information from PPPoE server as the default gateway route - With this checkbox selected, system will set the gateway information provided by PPPoE server as the default gateway route.
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	<p>Enable or Disable reverse route as needed:</p> <ul style="list-style-type: none"> • Enable: Enforces to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
WAP Traffic Distribution	<p>Select the Enable check box and configure as follows:</p> <ul style="list-style-type: none"> • Destination IP Replacement: Select the Enable check box, and specify the logs you need to record. If All is selected in WAP Log Record section, system will record all the traffic logs; while if Destination IP Replacement radio button is selected, system will record logs for the translated traffic. • Destination Service Port 1/Destination Service Port 2: Specifies the HTTP port number for the WAP gateway.
Proactive WebAuth	<p>Select the Enable check box to enable proactive webauth function and Specify the AAA server.</p> <p>After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.</p>

4. "In the IPv6 Configuration tab, configure the following." on Page 53
5. "In the Properties tab, configure properties for the interface." on Page 49
6. "In the Advanced tab, configure advanced options for the interface." on Page 49
7. "In the RIP tab, configure RIP for the interface." on Page 50

8. In the Load Balance tab, configure a load balance mode for the interface. "Flow-based" means enabling automatic load balance based on the flow. This is the default mode. "Tuple" means enabling load based on the source/destination IP, source/destination MAC, source/destination interface or protocol type of packet, or the combination of the selected items.
9. Click **OK**.

Creating a Redundant Interface

To create a redundant interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Redundant Interface**.

3. "In the Basic tab, configure the following." on Page 60
4. "In the IPv6 Configuration tab, configure the following." on Page 53
5. "In the Properties tab, configure properties for the interface." on Page 49
6. "In the Advanced tab, configure advanced options for the interface." on Page 49
7. "In the RIP tab, configure RIP for the interface." on Page 50
8. Click **OK**.

Creating an Ethernet Sub-interface/an Aggregate Sub-interface/a Redundant Sub-interface

To create an ethernet sub-interface/an aggregate sub-interface/a redundant sub-interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Ethernet Sub-interface/Aggregate Sub-interface/Redundant Sub-interface**.
3. **In the Basic tab, configure the following.**

Option	Description
Interface Name	Specifies a name for the virtual forward interface.
Description	Enter descriptions for the virtual forward interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from

Option	Description
	the Zone drop-down list, and the interface will bind to a Layer 3 zone. If TAP is selected, the interface will bind to a tap zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In a HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Enable DNS Bypass: Select this check box to enable DNS bypass for the interface.
	DHCP: In the DHCP Configuration dialog, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 77 .
	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
Auto-obtain	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
PPPoE	Obtain IP through PPPoE. Configure the following options: (Effective only when creating a aggregate sub-interface) <ul style="list-style-type: none"> • User - Specifies a username for PPPoE. • Password - Specifies PPPoE user's password. • Confirm password - Enter the password again to confirm. • Idle interval -If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, the system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30. • Re-connect interval - Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled. • Set gateway information from PPPoE server as the default gateway route - With this checkbox selected, system will set the gateway information provided by PPPoE server as the default gateway route.
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	Enable or Disable reverse route as needed: <ul style="list-style-type: none"> • Enable: Enforces to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the

Option	Description
	<p>ingress interface that initializes the packets.</p> <ul style="list-style-type: none"> Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
WAP Traffic Distribution	<p>Select the Enable check box and configure as follows:</p> <ul style="list-style-type: none"> Destination IP Replacement: Select the Enable check box, and specify the logs you need to record. If All is selected in WAP Log Record section, system will record all the traffic logs; while if Destination IP Replacement radio button is selected, system will record logs for the translated traffic. Destination Service Port 1/Destination Service Port 2: Specifies the HTTP port number for the WAP gateway.
Proactive WebAuth	<p>Select the Enable check box to enable proactive webauth function and Specify the AAA server.</p> <p>After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.</p>

4. "In the IPv6 Configuration tab, configure the following." on Page 53
5. "In the Properties tab, configure properties for the interface." on Page 49
6. "In the Advanced tab, configure advanced options for the interface." on Page 49
7. "In the RIP tab, configure RIP for the interface." on Page 50
8. Click **OK**.

Creating a VSwitch Interface/a VLAN Interface

To create a VSwitch interface/a VLAN interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > VSwitch Interface/VLAN Interface**.
3. "In the Basic tab, configure the following." on Page 55
4. "In the IPv6 Configuration tab, configure the following." on Page 53
5. "In the Properties tab, configure properties for the interface." on Page 49
6. "In the Advanced tab, configure advanced options for the interface." on Page 49
7. "In the RIP tab, configure RIP for the interface." on Page 50
8. Click **OK**.

Editing an Interface

To edit an interface, take the following steps:

1. Select **Network > Interface**.
2. Select the interface you want to edit from the interface list and click **Edit**.
3. In the **Basic** tab, configure the following.

Option	Description						
Interface Name	Specifies a name for the interface.						
Description	Enter descriptions for the interface.						
Binding Zone	<p>Specifies the zone type.</p> <p>If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone.</p> <p>If TAP is selected, the interface will bind to a tap zone.</p> <p>If No Binding is selected, you should also select a VLAN/aggregate interface/redundant interface:</p> <table><tr><td>Belong to</td><td>Description</td></tr><tr><td>VLAN</td><td><p>Acess mode (one VLAN) The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</p><p>Trunk mode (multiple VLANs) The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</p></td></tr><tr><td>Aggregate Interface</td><td><p>The interface you specified belongs to a aggregate interface.</p><ul style="list-style-type: none">• Interface Group: Choose an aggregate interface which the aggregate interface belongs to from Interface Group drop-down list.• Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority.• Port timeout mode: The LACP timeout refers to the time interval for the members The system supports Fast (1 second) and Slow (30 seconds, the default value).waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the</td></tr></table>	Belong to	Description	VLAN	<p>Acess mode (one VLAN) The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</p> <p>Trunk mode (multiple VLANs) The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</p>	Aggregate Interface	<p>The interface you specified belongs to a aggregate interface.</p> <ul style="list-style-type: none">• Interface Group: Choose an aggregate interface which the aggregate interface belongs to from Interface Group drop-down list.• Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority.• Port timeout mode: The LACP timeout refers to the time interval for the members The system supports Fast (1 second) and Slow (30 seconds, the default value).waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the
Belong to	Description						
VLAN	<p>Acess mode (one VLAN) The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</p> <p>Trunk mode (multiple VLANs) The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</p>						
Aggregate Interface	<p>The interface you specified belongs to a aggregate interface.</p> <ul style="list-style-type: none">• Interface Group: Choose an aggregate interface which the aggregate interface belongs to from Interface Group drop-down list.• Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority.• Port timeout mode: The LACP timeout refers to the time interval for the members The system supports Fast (1 second) and Slow (30 seconds, the default value).waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the						

Option	Description
	status of the local member will change from Active to Selected, and stop traffic forwarding.
	<div>Redundant Interface</div> <div>This interface belongs to a redundant interface. Select that redundant interface from the Interface Group drop-down list.</div>
	<div>None</div> <div>This interface does not belong to any object.</div>
LACP	<ul style="list-style-type: none"> Forced: Aggregates multiple physical interfaces to form an aggregate interface. These physical interfaces will share the traffic passing through the aggregate interface equally. Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are: <ul style="list-style-type: none"> System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be. Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby. Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregation group will change to Standby automatically and will not forward any traffic.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In a HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Enable DNS Bypass: Select this check box to enable DNS bypass for the interface.
	DHCP: In the DHCP Configuration dialog, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 77 .
	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
Auto-obtain	DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81 .
PPPoE	User: Specifies a username for PPPoE.

Option	Description
	<p>Password: Specifies PPPoE user's password.</p> <p>Confirm Password: Enter the password again to confirm.</p> <p>Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.</p> <p>Re-connect Interval: Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.</p> <p>Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.</p> <p>Advanced</p> <p>Access concentrator: Specifies a name for the concentrator.</p> <p>Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.</p> <p>Netmask: Specifies a netmask for the IP address obtained via PPPoE.</p> <p>Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.</p> <p>Service: Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically.</p> <p>Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.</p> <p>Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1.</p> <p>DDNS: In the DDNS Configuration dialog, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 81.</p>
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	
WAP Traffic Distribution	<p>Select the Enable check box and configure as follows:</p> <ul style="list-style-type: none"> Destination IP Replacement: Select the Enable check box, and specify the logs you need to record. If All is selected in WAP Log Record section, system will record all the traffic logs; while if Destination IP Replacement radio button is selected, system will record logs for the translated traffic. Destination Service Port 1/Destination Service Port 2: Specifies the HTTP port number for the WAP gateway.
Proactive WebAuth	Select the Enable check box to enable proactive webauth function and Specify the AAA server.

Option	Description
	After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.

4. "In the IPv6 Configuration tab, configure the following." on Page 53

5. In the Properties tab, configure properties for the interface.

Property	Description
Duplex	Specifies a duplex working mode for the interface. Options include auto, full duplex and half duplex. Auto is the default working mode, in which system will select the most appropriate duplex working mode automatically. 1000M half duplex is not supported.
Rate	Specifies a working rate for the interface. Options include Auto, 10M, 100M and 1000M. Auto is the default working mode, in which system will detect and select the most appropriate working mode automatically. 1000M half duplex is not supported.
Combo type	This option is applicable to the Combo port of copper port + fiber port. If both the copper port and the fiber port are plugged with cable, the fiber port will be prioritized by default; if the copper port is used at first, and the cable is plugged into the fiber port, and the fiber port will be used for data transmission after reboot. You can specify how to use a copper port or fiber port. For detailed options, see the following instructions: <ul style="list-style-type: none"> • Auto: The above default scenario. • Copper forced: The copper port is enforced. • Copper preferred: The copper port is prioritized. • Fiber forced: The fiber port is enforced. • Fiber preferred: The fiber port is prioritized. With this option configured, the device will migrate the traffic on the copper port to the fiber port automatically without reboot.
MTU	Specifies a MTU for the interface. The value range is 1280 to 1500/1800 bytes. The default value is 1500. The max MTU may vary in different Hillstone models.
ARP Learning	Select the Enable checkbox to enable ARP learning.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.
MAC clone	Select the MAC clone check box to enable the MAC clone function. System clones a MAC address to the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will restore the default MAC address.

6. "In the Advanced tab, configure advanced options for the interface." on Page 49

7. "In the RIP tab, configure RIP for the interface." on Page 50

8. Click **OK**.



Note:

- Before deleting an aggregate/redundant interface, you must cancel other interfaces' bindings to it, aggregate/redundant sub-interface's configuration, its IP address configuration and its binding to the security zone.
- An Ethernet interface can only be edited but cannot be deleted.
- When a VSwitch interface is deleted, the corresponding VSwitch will be deleted as well.

MGT Interface

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To facilitate the management of the device and meet the requirement of separating the management traffic from the data traffic, the system has an independent management interface (MGT Interface). By default, the management interface belongs to the trust zone and the trust-vr virtual router. To separate the traffic of the management interface from the traffic of other interfaces completely, you can add the management interface to the mgt zone. The mgt zone belongs to the mgt-vr virtual router, the information of routing, ARP table are independent.

Configuring a MGT Interface

To configure a MGT interface, take the following steps:

1. Select **Network > MGT Interface**.
2. Specify the zone for the management interface in the Zone drop-down list. You can only select a Layer 3 zone.
3. Specify the method of obtaining IP address in the IP Configuration section. "Static IP" means specifying a static IP address and the netmask. Click **Advanced** to specify the secondary IP address into the text box. You can specify up to 6 secondary IP addresses. "Auto-obtain" means obtaining the IP address through DHCP.
4. Specify the management methods by selecting the "Telnet/SSH/Ping/HTTP/HTTPS/SNMP" check boxes of the desired management methods.
5. Specify the mode and rate of the management interface. If you select the Auto duplex transmission mode , you can only select the Auto rate.
6. Select the Shut Down check box to shut down the management interface.
7. Click **OK**.

VLAN

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

VLAN, the abbreviation for Virtual Local Area Network, is defined in IEEE 802.1Q. VLAN has the following features:

- A physical LAN can be divided into multiple VLANs, and a VLAN might include devices from multiple physical networks.
- A VLAN is virtually a broadcast domain. Layer 2 packets between VLANs are isolated. Communication between VLANs can only be implemented by a Layer 3 route technique (through routers, Layer 3 switches, or other Layer 3 network devices).

VLANs are distinguished by VLAN numbers. The value range is 1 to 4094. System reserves 32 VLAN numbers (224 to 255) for BGroup, but the unused numbers within the range are also available to VLANs.

Configuring a VLAN

To create a VLAN, take the following steps:

1. Select **Network > VLAN**.
2. Click **New**.

In the VLAN Configuration dialog, type a number in the VLAN ID text box, the value range is from 1 to 4094.

3. Click **OK**.

DNS

DNS, the abbreviation for Domain Name System, is a computer and network service naming system in form of domain hierarchy. DNS is designed for TCP/IP network to query for Internet domain names (e.g., www.xxxx.com) and translate them into IP addresses (e.g., 10.1.1.1) to locate related computers and services.

The security device's DNS provides the following functions:

- **Server:** Configures DNS servers and default domain names for the security device.
- **Proxy:** The security device acts as a DNS proxy server and provides proxy service for the connected PCs and other clients. Besides, the security device can also choose different DNS servers according to domain names.
- **Analysis:** Sets retry times and timeout for device's DNS service.
- **Cache:** DNS mappings to cache can speed up query. You can create, edit and delete DNS mappings.
- **NBT Cache:** Displays NBT cache information.

Configuring a DNS Server

You can configure a DNS server for system to implement DNS resolution. To create a DNS server, take the following steps:

1. Select **Network > DNS > DNS Server**.
2. Click **New** in the DNS Server section.
3. In the DNS Server Configuration dialog, type the IP address for the DNS server into the Server IP box.
4. Select a VRouter from the VR drop-down list. The default VRouter is trust-vr.
5. Select an interface from the Egress Interface drop-down list. This parameter is mainly used for multi-egress DNS agents. If the interface is only for this device's DNS, you can keep the default "---".
6. Click **OK**.

Configuring a DNS Proxy

To enable a DNS proxy, take the following steps:

1. Configure a DNS proxy list that contains domain names and corresponding DNS servers.
2. Enable DNS proxy on an interface of the device (For more details, see ["Configuring an Interface" on Page 47](#)).
3. Connect the client to the interface with DNS proxy enabled.

To create a DNS proxy, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Click **New** in the DNS Proxy section.
3. In the DNS Proxy Configuration dialog, specify a suffix for a domain name in the Domain Type section.
4. In the Domain Server section, specify a DNS server or servers. "Use system" means using the DNS server bundled with system. "User-defined" means defining IP address for the server. Click **User-defined** and select a VRouter from the VR drop-down list, then type the IP address for the DNS servers into the boxes below (6 servers at most).
5. Click **OK**.

The multi-egress DNS proxy supports DNS management, which provides load balancing for the configured egress interfaces of DNS servers. Then system sends DNS request packets out from the egress interface with lower bandwidth utilization. Enable "DNS Balance Configuration" to activate this function. For detailed information, refer to [Configuring outbound LLB](#).

Configuring an Analysis

Analysis configuration includes DNS requests' retry times and timeout.

- **Retry:** If there is no response from the DNS server after the timeout, system will send the request again; if there is still no response from the DNS server after the specified retry times (i.e. the number of times to repeat the DNS request), system will send the request to the next DNS server.
- **Timeout:** System will wait for the DNS server's response after sending the DNS request and will send the request again if no response returns after a specified time. The period of waiting for a response is known as timeout.

To configure the retry times and timeout for DNS requests, take the following steps:

1. Select **Network > DNS > Analysis**
2. Select the retry times radio button.
3. Select the timeout values radio button.
4. Type the value in the TTL text box to specify the survival time of the response message for the device's DNS.
5. Click **Apply**.

Configuring a DNS Cache

When using DNS, system might store the DNS mappings to its cache to speed up the query. There are three ways to obtain DNS mappings:

- **Dynamic:** Obtains from DNS response.
- **Static:** Adds DNS mappings to cache manually.
- **Register:** DNS hosts specified by some modules of security devices, such as NTP, AAA, etc.

For convenient management, DNS static cache supports group function, which means users make the multiple domain hosts with the same IP address and virtual router is a DNS static cache group.

To add a static DNS mapping to cache, take the following steps:

1. Select **Network > DNS > Cache**
2. Click **New**.

Option	Description
Hostname	Specify the hostname of a DNS cache group. You can click to add or click button to delete the specified hostname. The maximum number of domain hosts is 128, and the maximum length of each hostname is 255 characters.
IP	Specify the host IPv4 address of a DNS cache group. You can click to add or click button to delete the specified IP. The maximum number of host IP address is 8, and the earlier configured IP will be matched first.
Virtual Router	Select a VRouter.

3. Click **OK**.



Note:

- Only DNS static cache group can support new, edit and delete operation , while dynamic and register cache cannot .
- The DNS dynamic cache can be deleted by command or the lifetime reset. For detailed information , refer to **StoneOS CLI User Guide** and [download PDF](#) on website.
- User can clear the register cache only by deleting the defined hosts in function module.
- DNS static cache is superior to dynamic and register cache, which means the static cache will cover the same existed dynamic or register cache.

NBT Cache

System supports NetBIOS name resolution. With this function enabled, system can automatically obtain all the NetBIOS host names registered by the hosts within the managed network, and store them in the cache to provide IP address to NetBIOS host name query service for other modules.

Enabling a NetBIOS name resolver is the pre-requisition for displaying host names in NAT logs. For more information on how to display host names in the NAT logs, see "[Log Configuration](#)" on [Page 451](#).

To enable NetBIOS for a zone, select the NBT cache check box when creating or editing the zone. For more details, see ["Security Zone" on Page 44](#). The security zone with NetBIOS enabled should not be the zone that is connected to WAN. After NetBIOS is enabled, the query process might last for a while, and the query result will be added to the NetBIOS cache table. System will perform the query again periodically and update the result.



Note: Only when PCs have NetBIOS enabled can their host names be queried. For more information on how to enable NetBIOS, see the detailed instructions of your PC's Operating System.

To clear NBT cache, take the following steps:

1. Select **Network > DNS > NBT Cache**.
2. Select a VRouter from the VR drop-down list to display the NBT cache in that VRouter.
3. Select a NBT cache entry from the list and click **Delete**.

DHCP

DHCP, the abbreviation for Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for subnetworks automatically, thus reducing requirement on network administration. Besides, DHCP can avoid address conflict to assure the re-allocation of idle resources.

System supports DHCP client, DHCP server and DHCP relay proxy.

- DHCP client: The interface can be configured as a DHCP client and obtain IP addresses from the DHCP server. For more information on configuring a DHCP client, see ["Configuring an Interface" on Page 47](#).
- DHCP server: The interface can be configured as a DHCP server and allocate IP addresses chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: The interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

The security devices are designed with all the above three DHCP functions, but an individual interface can be only configured with one of the above functions.

Configuring a DHCP Server

To create a DHCP server, take the following steps:

1. Select **Network > DHCP**.
2. Select **New > DHCP Server**.

The screenshot shows the 'DHCP Configuration' dialog box with the 'Basic' tab active. The 'Interface' is set to 'vswitchif1' with a dropdown arrow and the IP '25.1.1.2'. Below are input fields for 'Gateway', 'Netmask', 'DNS 1', and 'DNS 2'. The 'Address Pool' section has 'Start IP' and 'End IP' fields. There are 'Add' and 'Delete' buttons above a table with columns 'Start IP' and 'End IP'. At the bottom are 'OK' and 'Cancel' buttons.


3. In the DHCP Configuration dialog, configure as following:

Option	Description
Interface	Configures a interface which enables the DHCP server.
Gateway	Configures a gateway IP for the client.
Netmask	Configures a netmask for the client.
DNS1	Configures a primary DNS server for the client. Type the server's IP address into the box.
DNS2	Configures an alternative DNS server for the client. Type the server's IP address into the box.
Address pool	Configures an IP range in the address pool. The IPs within this range will be allocated. Take the following steps:

Option	Description
	<ol style="list-style-type: none"> 1. Type the start IP and end IP into the Start IP and End IP box respectively. 2. Click Add to add an IP range which will be displayed in the list below. 3. Repeat the above steps to add more IP ranges. To delete an IP range, select the IP range you want to delete from the list and click Delete.

4. Configure Reserved Address (IP addresses in the Reserved Address, within the IP range of the address pool, are reserved for the DHCP server and will not be allocated).
To configure a reserved address, click the **Reserved Address** tab, type the start and end IP for an IP range into the Start IP and End IP box respectively, and then click **Add**. To delete an IP range, select the IP range you want to delete from the list and then click **Delete**.
5. Configure IP-MAC Binding. If the IP is bound to a MAC address manually, the IP will only be allocated to the specified MAC address.
To configure an IP-MAC Binding, click the **IP-MAC Binding** tab and type the IP and MAC address into the IP address and MAC box respectively, type the description in the Description text box if necessary, and then click **Add**. Repeat the above steps to add multiple entries. To delete an IP-MAC Binding, select an entry from the list and click **Delete**.

6. **In the Option tab, configure the options supported by DHCP server**

Option	Description
43	<p>Option 43 is used to exchange specific vendor specific information (VSI) between DHCP client and DHCP server. The DHCP server uses option 43 to assign Access Controller (AC) addresses to wireless Access Point (AP), and the wireless AP use DHCP to discover the AC to which it is to connect.</p> <ol style="list-style-type: none"> 1. Select 43 from the Option drop-down list. 2. Select the type of the VSI, ASCII or HEX. When selecting ASCII, the VSI matching string must be enclosed in quotes if it contains spaces. 3. Enter the VSI in the Sign text box. 4. Click Add. 5. Click OK to save the settings. <div style="border: 1px solid #00a09a; padding: 10px; margin-top: 10px;">  <p>Note: If the VCI matching string has been configured, first of all, you need to verify the VCI carried by the option 60 field in client's DHCP packets. When the VCI matches the configured one, the IP address, option 43 and corresponding information will be offered. If not, DHCP server will drop client's DHCP packets and will not reply to the client.</p> </div>
49	<p>After you configure the option 49 settings, the DHCP client can obtain the list of the IP addresses of systems that are running the X window System Display Manager.</p> <p>To configure the option 49 settings:</p>

Option	Description
	<ol style="list-style-type: none"> 1. Select 49 from the Option drop-down list. 2. Enter the IP address of the system that is running the X window System Display Manager into the IP address box. 3. Click Add. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click Delete.
60	<p>After configuring the VCI carried by option 60 for DHCP server, the DHCP packets sent by the DHCP server will carry this option and the corresponding VCI.</p> <ol style="list-style-type: none"> 1. Select 60 from the Option drop-down list. 2. Select the type of the VCI, ASCII or HEX. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces. 3. Enter the VCI in the Sign text box. 4. Click Add. 5. Click OK to save the settings.
138	<p>The DHCP server uses option 138 to carry a list of 32-bit (binary) IPv4 addresses indicating one or more CAPWAP ACs available to the WTP. Then the WTP discovers and connects to the AC according to the provided AC list.</p> <ol style="list-style-type: none"> 1. Select 138 from the Option drop-down list. 2. Enter the AC IP address in the IP address text box. 3. Click Add. <p>You can add up to four AC IP addresses.</p> <p>If you do not set the option 138 for the DHCP server or the DHCP client does not request option 138, DHCP server will not offer the option 138 settings.</p>

7. Click the **Advanced** tab to configure the DHCP server's advanced options.

Option	Description
Domain	The domain name configured by the DHCP client.
Lease	<p>Specifies a lease time. The value range is 300 to 1048575 seconds. The default value is 3600. Lease is the period during which a client is allowed to use an IP address, starting from the time the IP address is assigned. After the lease expires, the client will have to request an IP address again from the DHCP server.</p>
Auto configure	<p>Enables automatic configuration. Select an interface with DHCP client enabled on the same gateway from the drop-down list. "----" indicates auto configure is not enabled.</p> <p>Auto configure will activate function in the following condition: Another interface with DHCP configured on the device enables DHCP client. When auto configure is enabled, if the DHCP server (Hillstone device) does not have DNS, WINS or domain name configured, the DHCP client (DHCP) will dispatch the DNS, WINS and domain name information obtained from a connected DHCP server to the host that obtains such information from the DHCP server (Hillstone device). However, the DNS, WINS and</p>

Option	Description
	domain name that are configured manually still have the priority.
WINS1	Configures a primary WINS server for the client. Type the server's IP address into the box.
WINS2	Configures an alternative WINS server for the client. Type the server's IP address into the box.
SMTP server	Configures a SMTP server for the client. Type the server's IP address into the box.
POP3 server	Configures a POP3 server for the client. Type the server's IP address into the box.
News server	Configures a news server for the client. Type the server's IP address into the box.
Relay agent	<p>When the device1 with DHCP server enabled is connected to another device2 with DHCP relay enabled, and the PC obtains device1's DHCP information from device2, then only when the relay agent's IP address and netmask are configured on device1 can the DHCP information be transmitted to the PC successfully.</p> <p>Relay agent: Type relay agent's IP address and netmask, i.e., the IP address and netmask for the interface with relay agent enabled on device2.</p>
VCI-match-string	<p>The DHCP server can verify the VCI carried by option 60 in the client's DHCP packets. When the VCI in the client's DHCP packet matches the VCI matching string you configured in the DHCP server, the DHCP server will offer the IP address and other corresponding information. If not, the DHCP server will drop the client's DHCP packets and will not reply to the client. If you do not configure a VCI matching string for the DHCP server, it will ignore the VCI carried by option 60.</p> <ol style="list-style-type: none"> 1. Select the type of the VCI matching string, ASCII or HEX. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces. 2. Enter the VCI matching string in the text box.

8. Click **OK**.

Configuring a DHCP Relay Proxy

The device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client.

To create a DHCP relay proxy, take the following steps:

1. Select **Network > DHCP**.
2. Click **New > DHCP Relay Proxy**.
3. In the DHCP Relay Proxy dialog, select an interface to which the DHCP Relay Proxy will be applied from the Interface drop-down list.
4. Type the IP addresses of DHCP servers into the Server 1/Server 2/Server 3 boxes.
5. Click **OK**.

DDNS

DDNS (Dynamic Domain Name Server) is designed to resolve fixed domain names to dynamic IP addresses. Generally you will be allocated with a dynamic IP address from ISP each time you connect to the Internet, i.e., the allocated IP addresses for different Internet connections will vary. DDNS can bind the domain name to your dynamic IP address, and the binding between them will be updated automatically each time you connect to the Internet.

In order to enable DDNS, you will have to register in a DDNS provider to obtain a dynamic domain name. Hillstone devices support the following 5 DDNS providers, and you can visit one of the following websites to complete the registration:

- dyndns.org: <http://dyndns.com/dns>
- 3322.org: <http://www.pubyun.com>
- no-ip.com: <http://www.noip.com>
- Huagai.net: <http://www.ddns.com.cn>
- ZoneEdit.com: <http://www.zoneedit.com>

Configuring a DDNS

To create a DDNS, take the following steps:

1. Select **Network > DDNS**.
2. Click **New**.

DDNS Configuration

Basic

DDNS Name: (1-31) characters

Interface: (dropdown)

Hostname: (1-127) characters

Provider

Provider: (dropdown)

Server Name: (1-255) characters

Server Port: (1-65535), default: 80

User

User: (1-49) characters

Password: (1-31) characters

Confirm Password:

Update Interval

Minimum Update Interval: (5-120) minutes, default: 5

Maximum Update Interval: (24-8760) hours, default: 24

OK Cancel

3. In the DDNS Configuration dialog, configure as follows:

Option	Description
DDNS name	Specifies the name of DDNS.
Interface	Specifies the interface to which DDNS is applied.
Host name	Specifies the domain name obtained from the DDNS provider.
Provider	Specifies a DDNS provider. Choose one from the drop-down list.
Server name	Specifies a server name for the configured DDNS.
Server port	Specifies a server port number for the configured DDNS. The value range is 1 to 65535.
Username	Specifies the username registered in the DDNS provider.
Password	Specifies the corresponding password.
Confirm password	Enter the password again to confirm.
Min update interval	When the IP address of the interface with DDNS enabled changes, system will send an update request to the DDNS server. If the server does not respond to the request, system will send the request again according to the configured min update interval. For example, if the min update interval is set to 5 minutes, then system will send the second request 5 minutes after the first request failure; if it fails again, system will send the third request 10 (5x2) minutes later; if it fails again, and system will send the forth request 20 (10*2) minutes later, and so forth. The value will not increase anymore when reaching 120 minutes. That is, system will send the request at a fixed interval of 120 minutes. The default value is 5.
Max update interval	In case the IP address has not changed, system will send an update request to the DDNS server at the max update interval. Type the max update interval into the box. The value range is 24 to 8760 hours. The default value is 24.

4. Click **OK**.



Note: The Server name and Server port in the configuration options must be the corresponding name and port of the DDNS server. Do not configure these options if the exact information is unknown. The server will return the name and port information automatically after connection to the DDNS server has been established successfully.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, combines PPP protocol and Ethernet to implement access control, authentication, and accounting on clients during an IP address allocation.

The implementation of PPPoE protocol consists of two stages: discovery stage and PPP session stage.

- Discovery stage: The client discovers the access concentrator by identifying the Ethernet MAC address of the access concentrator and establishing a PPPoE session ID.
- PPP session stage: The client and the access concentrator negotiate over PPP. The negotiation procedure is the same with that of a standard PPP negotiation.

Interfaces can be configured as PPPoE clients to accept PPPoE connections.

Configuring PPPoE

To create a PPPoE instance, take the following steps:

1. Select **Network > PPPoE**.
2. Click **New**.

PPPoE Configuration

PPPoE Name :

(1-31) characters

Interface :

Username :

(1-31) characters

Password :

(1-31) characters

Confirm Password :

Idle Interval :

30

(1-31) characters

Re - connect Interval :

0

(0-10000)secs

Access Concentrator :

(1-31) characters

Authentication :

☒ Any ☐ CHAP ☐ PAP

Netmask :

255.255.255.255

Distance :

1

1-255

Weight :

1

1-255

Service :

(1-31) characters

Static IP :

OK

Cancel

3. In the PPPoE Configuration dialog, configure as follows.

Option	Description
PPPoE Name	Specifies a name for the PPPoE instance.
Interface	Select an interface from the drop-down list.
Username	Specifies a username.
Password	Specifies the corresponding password.
Conform pass-word	Enter the password again to confirm.
Idle Interval	Automatic connection. If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, system will disconnect

Option	Description
	the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.
Re-connect Interval	If the PPPoE connection disconnects for any reason for a certain period, i.e. the specified re-connect interval, system will try to re-connect automatically. The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.
Access Concentrator	Specifies a name for the concentrator.
Authentication	The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). To configure a PPPoE authentication method, click the authentication you want to select. The configured authentication must be the same with that configured in the PPPoE server.
Netmask	Specifies a netmask for the IP address obtained via PPPoE.
Distance	Specifies a route distance. The value range is 1 to 255. The default value is 1.
Weight	Specifies a route weight. The value range is 1 to 255. The default value is 1.
Service	Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically.
Static IP	You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the Static IP box.

4. Click **OK**.

Virtual Wire

The system supports the VSwitch-based Virtual Wire. With this function enabled and the Virtual Wire interface pair configured, the two Virtual Wire interfaces form a virtual wire that connects the two subnetworks attached to the Virtual Wire interface pair together. The two connected subnetworks can communicate directly on Layer 2, without any requirement on MAC address learning or other sub network's forwarding. Furthermore, controls of policy rules or other functions are still available when Virtual Wire is used.

Virtual Wire operates in two modes, which are Strict and Non-Strict mode respectively, as detailed below:

- **Strict Virtual Wire mode:** Packets can only be transmitted between Virtual Wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to Virtual Wire can neither manage devices nor access Internet over this interface.
- **Non-Strict Virtual Wire mode:** Packets can be transmitted between Virtual Wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between Virtual Wire interfaces, and does not affect Layer 3 packets' forwarding.

The table below lists packet transmission conditions in Strict Virtual Wire and Non-Strict Virtual Wire mode. You can choose an appropriate Virtual Wire mode according to the actual requirement.

Packet	Strict	Non-strict
Egress and ingress are interfaces of one Virtual Wire interface pair	Allow	Allow
Ingress is not Virtual Wire's interface	Deny	Deny
Egress and ingress are interfaces of different Virtual Wire interface pairs	Deny	Deny
Ingress of to-self packet is a Virtual Wire's interface	Deny	Allow
Ingress is Virtual Wire's interface, and egress is a Layer 3 interface	Deny	Allow

Configuring a Virtual-Wire

To create a Virtual-Wire, take the following steps:

1. Select **Network > Virtual-Wire**.
2. Click **New**.
3. In the Virtual-Wire Configuration dialog, select a virtual switch from the VSwitch drop-down list.
4. In the Interface 1 drop-down list, specify an interface for the virtual wire interface pair. The two interfaces in a single virtual wire interface pair must be different, and one interface cannot belong to two different virtual wire interface pairs simultaneously.
5. In the Interface 2 drop-down list, specify an interface for the virtual wire interface pair. The two interfaces in a single virtual wire interface pair must be different, and one interface cannot belong to two different virtual wire interface pairs simultaneously.
6. Click **OK**.

Configuring the Virtual Wire Mode

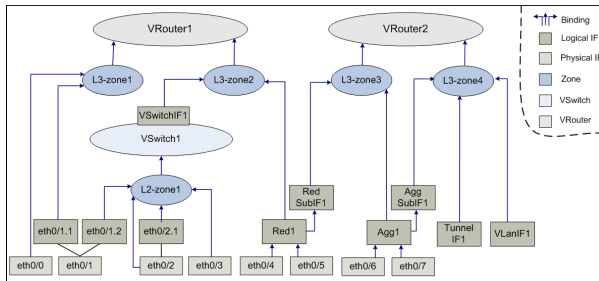
To configure a virtual wire mode, take the following steps:

1. Select **Network > Virtual-Wire**.
2. Click **Virtual-Wire Mode**.
3. In the Virtual-Wire Mode Configuration dialog, select a virtual switch from the VSwitch drop-down list.

4. Specify a virtual wire mode from one of the following options:
 - Strict - Packets can only be transmitted between virtual wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to the virtual wire can neither manage devices nor access Internet over this interface.
 - Non-strict - Packets can be transmitted between virtual wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between virtual wire interfaces, and does not affect Layer 3 packets' forwarding.
 - Disabled - Disables the virtual wire.
5. Click **OK**.

Virtual Router

Virtual Router (VRouter) is known as VR in system. VR acts as a router, and different VRs have their own independent routing tables. A VR named "trust-vr" is implemented with the system, and by default, all of the Layer 3 security zones are bounded to the trust-vr automatically. Hillstone devices support multiple VRs, and the max amount of supported VRs may vary with different hardware platforms. Multiple VRs divide a device into multiple virtual routers, and each router utilizes and maintains their independent routing table. In such a case one device is acting as multiple routers. Multiple VRs allow a device to achieve the effects of the address isolation between different route zones and address overlapping between different VRs, as well as to avoid route leaking to some extent, enhancing route security of network. For more information about the relationship between interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationship between them are:

- Interfaces are bound to security zones. Those that are bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One interface can be only bound to one security zone; the primary interface and sub interface can belong to different security zones.
- Security zones are bound to a VSwitch or VRouter. Layer 2 security zones are bound to a VSwitch (by default the pre-defined Layer 2 security zone is bound to the default VSwitch1), and Layer 3 security zones are bound to a VRouter (by default the pre-defined Layer 3 security zone is bound to the default trust-vr), thus realizing the binding between the interfaces and VSwitch or VR. One security zone can be only bound to one VSwitch or VR.

Creating a Virtual Router

To create a Virtual Router, take the following steps:

1. Select **Network > Virtual Router > Virtual Router**.
2. Click **New**.
3. Type the name into the Virtual Router name box.
4. Select the **Enable** check box for Vsys Share to share the Virtual Router between different virtual systems.
5. Click **OK**.

Global Configuration

Virtual Router's global configuration is the configuration for multiple Virtual Routers. To configure Multi-Virtual Router, take the following steps:

1. Select **Network > Virtual Router > Global Configuration**.
2. Select the **Enable** check box for Multi-Virtual Router.
3. Click **Apply**.

**Note:**

- After Multi-Virtual Router is enabled or disabled, system must reboot to make it take effect. After rebooting, system's max concurrent sessions will decrease by 15% if the function is enabled, or restore to normal if the function is disabled. When AV and Multi-Virtual Router are enabled simultaneously, the max concurrent session will further decrease by 50% (with AV enabled, the max concurrent session will decrease by half). The formula is:
Actual max concurrent sessions = original max concurrent sessions*(1-0.15)*(1-0.5).
- If Multi-Virtual Router is enabled, traffic can traverse up to 3 Virtual Routers, and any traffic that has to traverse more than 3 Virtual Routers will be dropped.

Virtual Switch

System might allow packets between some interfaces to be forwarded in Layer 2 (known as transparent mode), and packets between some interfaces to be forwarded in Layer 3 (known as routing mode), specifically depending on the actual requirement. To facilitate a flexible configuration of hybrid mode of Layer 2 and Layer 3, system introduces the concept of Virtual Switch (VSwitch). By default system uses a VSwitch known as VSwitch1. Each time you create a VSwitch, system will create a corresponding VSwitch interface (VSwitchIF) for the VSwitch automatically. You can bind an interface to a VSwitch by binding that interface to a security zone, and then binding the security zone to the VSwitch.

A VSwitch acts as a Layer 2 forwarding zone, and each VSwitch has its own independent MAC address table, so the packets of different interfaces in one VSwitch will be forwarded according to Layer 2 forwarding rules. You can configure policy rules conveniently in a VSwitch. A VSwitchIF virtually acts as a switch uplink interface, allowing packets forwarding between Layer 2 and Layer 3.

Creating a VSwitch

To create a VSwitch, take the following steps:

1. Select **Network > VSwitch**.
2. Click **New**.

Options are described as follows.

Option	Description
VSwitch Name	Specifies a name for the VSwitch.
Vsys Shared	Select the Enable check box and then system will share the VSwitch with different VSYS.
Virtual-Wire Mode	<p>Specifies a Virtual-Wire mode for the VSwitch, including (for specific information on Virtual Wire, see "Virtual Wire" on Page 85)</p> <ul style="list-style-type: none">• Strict - Packets can only be transmitted between Virtual Wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to Virtual Wire can neither manage devices nor access Internet over this interface.• Non-strict - Packets can be transmitted between Virtual Wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between Virtual Wire interfaces, and does not affect Layer 3 packets' forwarding.• Disabled - Disables Virtual Wire.
IGMP Snooping	Enables IGMP snooping on the VSwitch.
Forward Tagged Packets	Enables VLAN transparent so that the device can transmit VLAN tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID after passing through the device.
Forward Double Tagged Packets	Enables VLAN transparent so that the device can transmit VLAN double tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID after passing through the device.
Drop Unknown Multicast Packets	Drops the packets sent to unknown multicast to save bandwidth.

3. Click **OK**.

Port Mirroring

Some low-end platforms do not support port mirroring.

The device is designed with port mirroring on Ethernet interfaces. This function allows users to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.

To configure port mirroring, take the following steps:

1. Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.
2. Configure a destination interface.

To configure the destination interface of port mirroring:

1. Select **Network > Port Mirroring**.
2. Select an interfaces from the Destination Interface drop-down list, and click **OK**. All the source and destination interface will be listed in the table below.

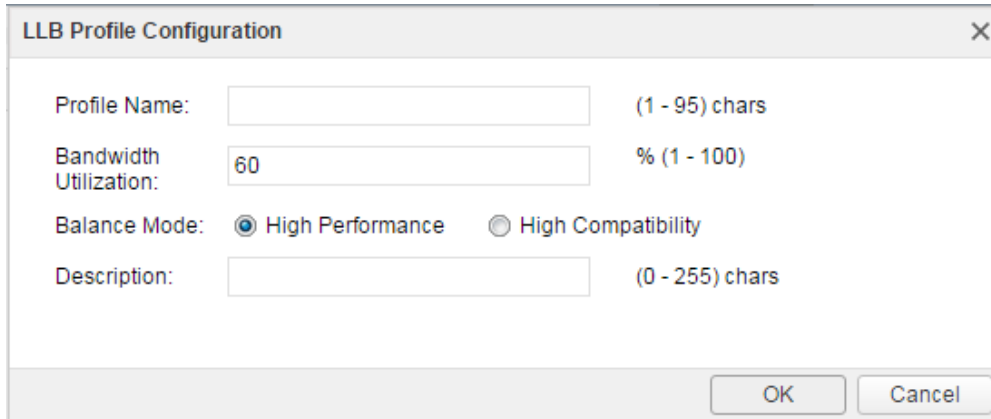
Outbound Link Load Balancing

For Outbound LLB, the system can intelligently oute and dynamically adjust the traffic load of each link by monitoring the delay, jitter, packet loss rate and bandwidth utilization of each link in real-time. You can configure a flexible LLB profile to bind to the route (the current system only supports DBR and PBR), forming LLB rules to implement outbound dynamic link load balancing, and thus make efficient use of network bandwidth.

Configuring LLB Profile

The LLB profile contains the parameters of the load balancing algorithm, such as bandwidth utilization threshold, probe switch, probe mode, and equalization direction.

1. Select **Network > Outbound > Profile**.
2. Click **New**.



The image shows a dialog box titled "LLB Profile Configuration" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Profile Name:** A text input field with a character limit of "(1 - 95) chars".
- Bandwidth Utilization:** A text input field containing the value "60" and a unit indicator "% (1 - 100)".
- Balance Mode:** Two radio button options: "High Performance" (which is selected) and "High Compatibility".
- Description:** A text input field with a character limit of "(0 - 255) chars".

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

3. In the LLB Profile Configurion, configure as follows:

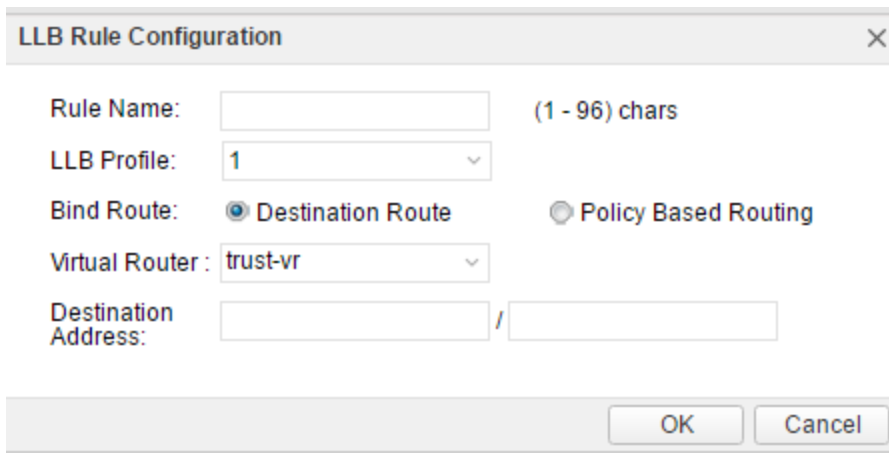
Option	Description
Profile Name	Specifies the Profile name whose length range is 1-96 characters.
Bandwidth Utilization	Specifies the bandwidth utilization threshold of the interface. When the rate does not exceed the threshold by the interface bandwidth, the system will only analysis delay, jitter and packet loss rate to dynamically adjust the routing link; when the rate exceeds the threshold by the interface bandwidth,system will analysis of each link bandwidth utilization rate of the parameters at the same time to adjust the routing method. Value ranges from 0 to 100 (0% to 100%) and defaults to 60.
Subnet Mask	Specifies the destination IP segment of the detect task. System carries out real-time monitoring of the traffic flow of the network segment, and adjusts the traffic load balance according to the monitoring and statistical results. It ranges from 8 to 32 and defaults to 28.
Balance Mode	<p>There are two equalization modes: High Performance and High Compatibility.</p> <ul style="list-style-type: none"> • High Performance - In this mode, system adjusts link to keep the link balance as fast as possible • High Compatibility - When the link load changes, system does not switch the link frequently, but ensures that the service is as far as possible on the previous link. This mode is suitable for services that are sensitive to link switching, such as banking services, only when the previous link is overloaded.
Description	Configure Additional details for the LLB profile.

4. Click **OK**.

Configuring LLB Rule

The LLB Profile and the route is bound by the formation of LLB rules that currently support binding destination routing (DBR) and policy-based routing (PBR).

1. Select **Network > Outbound > Rule**.
2. Click **New**.



The image shows a 'LLB Rule Configuration' dialog box. It contains the following fields and options:

- Rule Name:** A text input field with a placeholder '(1 - 96) chars'.
- LLB Profile:** A dropdown menu showing '1'.
- Bind Route:** Two radio buttons: 'Destination Route' (selected) and 'Policy Based Routing'.
- Virtual Router:** A dropdown menu showing 'trust-vr'.
- Destination Address:** Two text input fields separated by a slash, for IP address and subnet mask.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

3. In the LLB Rule Configuration, configure the following:

Option	Description
Rule Name	Specifies the Rule name,length of 1-96 characters
Profile Name	Specifies the bandwidth utilization threshold. It is in the range of 0-100 (0% -100%) and defaults to 60.
Bind Route	Specify the route to be bound in the rule:Destination Route or Policy Based Route. <ul style="list-style-type: none"> Destination Route - When this option is selected, specify the Vrouter and destination address of the destination route. Policy Based Route - Select this option to specify the name and id of the policy route.

4. Click **OK**.

Configuring DNS Balance

When the LLB DNS balancing function is enabled, system will balance the load of the outgoing interfaces of all of the configured DNS servers. The DNS request packets will be redirected to the link with the lower load.

To enable DNS Balance, take the following steps:

1. Select **Network >Outbound >DNS Balance Configuration**.
2. Select **Enable**. System will enable DNS Balance.



Note: To enable LLB DNS equalization, you must first enable the DNS transparent proxy function.

Inbound Link Load Balancing

After enabling the LLB for inbound traffic, the system will resolve domains of different IPs based on the sources of the DNS requests and return IPs for different ISPs to the corresponding users who initiate the requests, which reduces access across ISPs. Such a resolution method is known as SmartDNS.

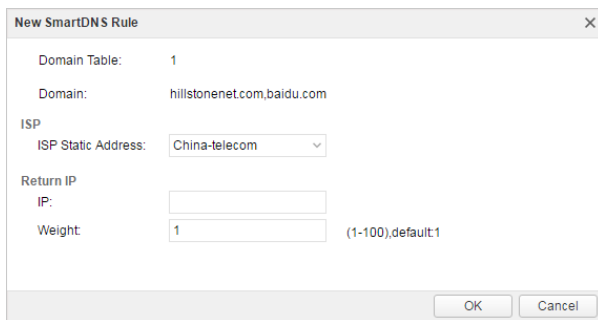
You can enable inbound LLB by the following steps:

1. Enable SmartDNS. This is the prerequisite for the implementation of inbound LLB.
2. Configure a SmartDNS rule table. The smart domain-to-IP resolution is implemented based on the rule table.

Creating a SmartDNS Rule Table

To create a SmartDNS rule table, take the following steps:

1. Select **Network > Inbound**.
2. Click **New > Domain Table**.
3. In the Domain Configuration dialog, type a domain table name into Domain Table text box.
4. Type a domain name into Domain text box. Separate multiple domain names with comma. Each rule table supports up to 64 domain names (case insensitive).
5. Click **OK**.
6. In the Inbound LLB page, click the domain table name you already created and then click **New > SmartDNS Rule**.



In the New SmartDNS Rule, configure the following:

Option	Description
ISP Static Address	Select a predefined or user-defined ISP from the drop-down list. If the source address matches any address entry of the ISP, system will return the specified IP.
Return IP	Specifies the return IP for different request sources. Options include: <ul style="list-style-type: none">• IP - Specifies the return IP. You can configure up to 64 IPs for a domain name.• Weight - Specifies the weight of the return IP. The value range is 1 to 100. The default value is 1. In the SmartDNS rule table, one domain name might correspond to multiple IPs. System will sort the IPs based on the weight and then return to the users.

7. Click **OK**.



Note: The ISP route being referenced by the SmartDNS rule table cannot be deleted.

Application Layer Gateway (ALG)

Some applications use multi-channels for data transmission, such as the commonly used FTP. In such a condition the control channel and data channel are separated. Devices under strict security policy control may set strict limits on each data channel, like only allowing FTP data from the internal network to the external network to transfer on the well-known port TCP 21. Once in the FTP active mode, if a FTP server in the public network tries to initiate a connection to a random port of the host in the internal network, devices will reject the connection and the FTP server will not work properly in such a condition. This requires devices to be intelligent enough to properly handle the randomness of legitimate applications under strict security policies. In FTP instances, by analyzing the transmission information of the FTP control channel, devices will be aware that the server and the client reached an agreement, and open up a temporary communication channel when the server takes the initiative to connect to a port of the client, thus assuring the proper operation of FTP.

The system adopts the strictest NAT mode. Some VoIP applications may work improperly after NAT due to the change of IP address and port number. The ALG mechanism can ensure the normal communication of VoIP applications after the NAT. Therefore, the ALG supports the following functions:

- Ensures normal communication of multi-channel applications under strict security policy rules.
- Ensures the proper operation of VoIP applications such as SIP and H.323 in NAT mode, and performs monitoring and filtering according to policies.

Enabling ALG

The system allows you to enable or disable ALG for different applications. Devices support ALG for the following applications: FTP, HTTP, MSRPC, PPTP, Q.931, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, TFTP, DNS, and Auto. You can not only enable ALG for applications, but also specify H323's session timeout.

To enable the ALG for applications, take the following steps:

1. Select **Network > Application Layer Gate**.
2. In the Application Layer Gateway dialog, select the applications that require ALG.

ALG can guarantee the normal communication of multi-channel application programs and VoIP application.

Select the ALG to be enabled:

ALG	Status	Description
FTP	<input checked="" type="checkbox"/>	FTP ALG
HTTP	<input checked="" type="checkbox"/>	HTTP ALG
MS-RPC	<input checked="" type="checkbox"/>	MS-RPC ALG
PPTP	<input checked="" type="checkbox"/>	PPTP ALG
Q.931	<input checked="" type="checkbox"/>	Q.931 ALG
RAS	<input checked="" type="checkbox"/>	RAS ALG
RSH	<input checked="" type="checkbox"/>	RSH ALG
RTSP	<input checked="" type="checkbox"/>	RTSP ALG
SIP	<input checked="" type="checkbox"/>	SIP ALG
SQLNetV2	<input checked="" type="checkbox"/>	SQLNetV2 ALG
SUN-RPC	<input checked="" type="checkbox"/>	SUN-RPC ALG
TFTP	<input checked="" type="checkbox"/>	TFTP ALG
DNS	<input type="checkbox"/>	DNS ALG

H.323 session timeout: (60~1800)sec. Default:60

3. To modify H323's session timeout, type the value into the **H323 session timeout** box. The value range is 60 to 1800 seconds. The default value is 60.
4. Click **OK** to save your changes.

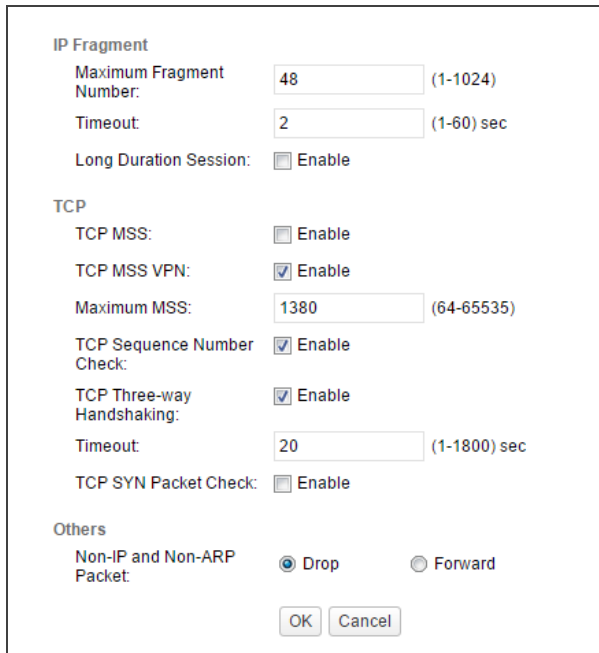
Global Network Parameters

Global network parameter configuration includes IP fragment, TCP packet processing methods and other options.

Configuring Global Network Parameters

To configure global network parameters, take the following steps:

1. Select **Network > Global Network Parameters > Global Network Parameters**.



The screenshot shows a configuration window titled "Global Network Parameters". It is divided into three sections: "IP Fragment", "TCP", and "Others".

- IP Fragment:**
 - Maximum Fragment Number: 48 (range 1-1024)
 - Timeout: 2 (range 1-60) sec
 - Long Duration Session: ☐ Enable
- TCP:**
 - TCP MSS: ☐ Enable
 - TCP MSS VPN: ☒ Enable
 - Maximum MSS: 1380 (range 64-65535)
 - TCP Sequence Number Check: ☒ Enable
 - TCP Three-way Handshaking: ☒ Enable
 - Timeout: 20 (range 1-1800) sec
 - TCP SYN Packet Check: ☐ Enable
- Others:**
 - Non-IP and Non-ARP Packet: ☒ Drop ☐ Forward

At the bottom, there are "OK" and "Cancel" buttons.

2. **Configure the following parameters.**

Option	Description
IP Fragment	
Maximum Fragment Number	Specifies a maximum fragment number for every IP packet. The value range is 1 to 1024. The default value is 48. Any IP packet that contains more fragments than this number will be dropped.
Timeout	Specifies a timeout period of fragment reassembling. The value range is 1 to 30. The default value is 2. If the Hillstone device has not received all the fragments after the timeout, the packet will be dropped.
Long Duration Session	Enables or disables long duration session. If this function is enabled, specify long duration session's percentage in the Percentage text box below. The default value is 10, i.e., 10% of long duration session in the total sessions.
TCP	
TCP MSS	Specifies a MSS value for all the TCP SYN/ACK packets. Select the Enable check box, and type the value into the Maximum MSS text box below.
Maximum MSS	Type the max MSS value into the Maximum MSS text box below. The value range is 64 to 65535. The default value is 1448.
TCP MSS VPN	Specifies a MSS value for IPSec VPN's TCP SYN packets. Select the Enable check box, and type the value into the Maximum MSS text box below.
Maximum MSS	Type the max MSS value for IPSEC VPN into the Maximum MSS text box below. The value range is 64 to 65535. The default value is 1380.
TCP Sequence Number Check	Configures if the TCP sequence number will be checked. When this function is enabled, if the TCP sequence number exceeds TCP window, that TCP packet will be dropped.
TCP Three-way Handshaking	Configures if the timeout of TCP three-way handshaking will be checked. Select the Enable check box to enable this function, and specify a timeout value in the Timeout text box below. The value range is 1 to 1800 seconds. The default value is 20. If the three-way handshaking has not been completed after timeout, the connection will be dropped.
TCP SYN Packet Check	Select the Enable check box to enable this function, and only when a packet is a TCP SYN packet can a connection be established.
Others	
Non-IP and Non-ARP Packet	Specifies how to process packets that are neither IP nor ARP.

3. Click **OK**.

Configuring Protection Mode

To configure the protection mode, take the following steps:

1. Select **Network > Global Network Parameters > Protection Mode**.
2. Click **Protection Mode** tab, and configure the traffic working mode.

Protection Mode

☒ Log & reset
 ☐ Log only

Log messages and reset or block.

 Log messages and do not reset or block.

- Log & reset - System not only generates protocol anomaly alarms and attacking behavior logs, but also blocks attackers or resets connections.

- Log only - System only generates protocol anomaly alarms and attacking behavior logs, but will not block attackers or reset connections.



Note: Log & reset mode is recommended. In this mode, the security performance of the device can take effect normally. If log only mode is selected, system can only record logs, and functions which can block traffic in system will be invalid, including policy, IPS, AV, QoS, etc.

Chapter 6 Advanced Routing

Routing is the process of forwarding packets from one network to the destination address in another network. Router, a packet forwarding device between two networks, is designed to transmit packets based on the various routes stored in routing tables. Each route is known as a routing entry.

Hillstone devices are designed with Layer 3 routing. This function allows you to configure routing options and forward various packets via VRouter. System implements with a default VRouter trust-vr, and also supports multiple VRouters (multi-VR).

Hillstone devices support destination routing, ISP routing, Source-Based Routing (SBR), Source-Interface-Based Routing (SIBR), Destination-Interface-Based Routing (DIBR), Policy-Based Routing (PBR), dynamic routing (including RIP, OSPF and BGP) and Equal Cost MultiPath Routing (ECMP).

- Destination Routing: A manually-configured route which determines the next routing hop according to the destination IP address.
- DIBR: A manually-configured route which determines the next routing hop according to the destination IP address and ingress interface.
- SBR: Source IP based route which selects routers and forwards data according to the source IP address.
- SIBR: Source IP and ingress interface based route.
- ISP Profile: Add a subnet to an ISP.
- ISP Routing: A kind of route which determines the next hop based on different ISPs.
- PBR: A route which forwards data based on the source IP, destination IP address and service type.
- Dynamic Routing: Selects routers and forwards data according to the dynamic routing table generated by dynamic routing protocols (RIP, OSPF or BGP).
- ECMP: Load balancing traffic destined to the same IP address or segment in multiple routes with equal management distance.

When forwarding the inbound packets, the device will select a route in the following sequence: PBR > SIBR > SBR > DIBR > Destination routing/ISP routing/Proximity routing/Dynamic routing.

Routing supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry for the routing rule.

Related Topics:

- ["Destination Route" on Page 101](#)
- ["Destination-Interface Route" on Page 102](#)
- ["Source Route" on Page 104](#)
- ["Source-Interface Route" on Page 106](#)
- ["ISP Profile" on Page 108](#)
- ["ISP Route" on Page 110](#)
- ["Policy-based Route" on Page 112](#)
- ["RIP" on Page 120](#)

Destination Route

The destination route is a manually-configured route entry that determines the next routing hop based on the destination IP address. Usually a network with comparatively a small number of outbound connections or stable Intranet connections will use a destination route. You can add a default route entry at your own choice as needed.

Creating a Destination Route

To create a destination route, take the following steps:

- 1. Select **Network > Routing > Destination Route**.
- 2. Click **New**.

In the Destination Route Configuration dialog box, enter values.

Destination Route Configuration

Virtual Router:

trust-vr

Destination:

Subnet Mask:

Next Hop:

Gateway

Virtual Router in current Vsys

Interface

Virtual Router in other Vsys

Gateway:

Schedule:

Precedence:

1

(1-255) , default: 1

Weight:

1

(1-255) , default: 1

Description:

(0-63) chars

OK

Cancel

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Destination	Type the IP address for the route into the text box.
Subnet Mask	Type the corresponding subnet mask into the text box.
Next Hop	<div>To specify the type of next hop, click Gateway, Current VRouter, Interface, or Other VRouter.</div> <div><ul style="list-style-type: none">• Gateway: Type the IP address into the Gateway text box.• Current VRouter: Select a name from the drop-down list.• Interface: Select a name from the Interface drop-down list. Type the IP address into the Gateway text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.• Other VRouter: Select a name from the Vsys drop-down list. Select a name from the Virtual Router drop-down list.</div>
Schedule	<div>Specifies a schedule when the rule will take effect. Select a desired schedule from the Schedule drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration.</div> <div>To create a new schedule, click New Schedule.</div>
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255.

Option	Description
	The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the text box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

3. Click **OK**.

Destination-Interface Route

Destination interface route is designed to select a route and forward data based on the Destination IP address and ingress interface of a packet.

Creating a Destination-Interface Route

To create a Destination-Interface route, take the following steps:

1. Select **Network > Routing > Destination Interface Route**.
2. Click **New**.

In the Destination Interface Route Configuration dialog box, enter values.

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Ingress Interface	Select an interface for the route from the drop-down list.
Destination IP	Type the Destination IP for the route into the textbox.
Subnet Mask	Type the corresponding subnet mask into the textbox.
Next Hop	<p>To specify the type of next hop, click Gateway, Virtual Router in current Vsys, Interface, or Virtual Router in other Vsys.</p> <ul style="list-style-type: none"> • Gateway: Type the IP address into the Gateway text box. • Virtual Router in current Vsys: Select a name from the Virtual Router drop-down list. • Interface: Select a name from the Interface drop-down list. Type

Option	Description
	<p>the IP address into the Gateway text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.</p> <ul style="list-style-type: none"> Virtual Router in other Vsys: Select a name from the Vsys drop-down list. Select a name from the Virtual Router drop-down list.
Schedule	<p>Specifies a schedule when the rule will take effect. Select a desired schedule from the Schedule drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration.</p> <p>To create a new schedule, click New Schedule.</p>
Precedence	<p>Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.</p>
Weight	<p>Type the weight for the DIBR into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.</p>
Description	<p>Type the description information into the Description text box if necessary.</p>

3. Click **OK**.

Source Route

Source route is designed to select a router and forward data based on the source IP address of a packet.

Creating a Source Route

To create a source route, take the following steps:

- 1. Select **Network > Routing > Source Route**.
- 2. Click **New**.

In the Source Route Configuration dialog box, enter values.

Source Route Configuration

Virtual Router:

trust-vr

Source IP:

Subnet Mask:

Next Hop:

Gateway

Virtual Router in current Vsys

Interface

Virtual Router in other Vsys

Gateway:

Schedule:

Precedence:

1

(1-255) , default: 1

Weight:

1

(1-255) , default: 1

Description:

(0-63) chars

OK

Cancel

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Source IP	Type the source IP for the route into the box.
Subnet Mask	Type the corresponding subnet mask into the box.
Next Hop	<div>To specify the type of next hop, click Gateway, Virtual Router in current Vsys, Interface, or Virtual Router in other Vsys.</div> <ul style="list-style-type: none">• Gateway: Type the IP address into the Gateway text box.• Virtual Router in current Vsys: Select a name from the drop-down list.• Interface: Select a name from the Interface drop-down list. Type the IP address into the Gateway text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.• Virtual Router in other Vsys: Select a name from the Vsys drop-down list. Select a name from the Virtual Router drop-down list.
Schedule	<div>Specifies a schedule when the rule will take effect. Select a desired schedule from the Schedule drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration.</div> <div>To create a new schedule, click New Schedule.</div>
Precedence	Type the route precedence into the box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.

Option	Description
Weight	Type the weight for the route into the box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

3. Click **OK**.

Source-Interface Route

Source interface route is designed to select a router and forward data based on the source IP address and ingress interface of a packet.

Creating a Source-Interface Route

To create a Source-Interface route, take the following steps:

- 1. Select **Network > Routing > Source Interface Route**.
- 2. Click **New**.

In the Source Interface Route Configuration dialog box, enter values.

Source Interface Route Configuration

Virtual Router:trust-vr

Ingress Interface:ethernet0/0

Source IP:

Subnet Mask:

Next Hop:

Gateway

Virtual Router in current Vsys

Interface

Virtual Router in other Vsys

Gateway:

Schedule:-----

Precedence:1(1-255), default: 1

Weight:1(1-255), default: 1

Description:(0-63) chars

OK

Cancel

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Ingress Interface	Select an interface for the route from the drop-down list.
Source IP	Type the source IP for the route into the textbox.
Subnet Mask	Type the corresponding subnet mask into the textbox.
Next Hop	<div>To specify the type of next hop, click Gateway, Virtual Router in current Vsys, Interface, or Virtual Router in other Vsys.<ul style="list-style-type: none">• Gateway: Type the IP address into the Gateway text box.• Virtual Router in current Vsys: Select a name from the Virtual Router drop-down list.• Interface: Select a name from the Interface drop-down list. Type the IP address into the Gateway text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.• Virtual Router in other Vsys: Select a name from the Vsys drop-down list. Select a name from the Virtual Router drop-down list.</div>
Schedule	<div>Specifies a schedule when the rule will take effect. Select a desired schedule from the Schedule drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration.</div> <div>To create a new schedule, click New Schedule.</div>

Option	Description
Precedence	Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the ISP route into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

3. Click **OK**.

ISP Profile

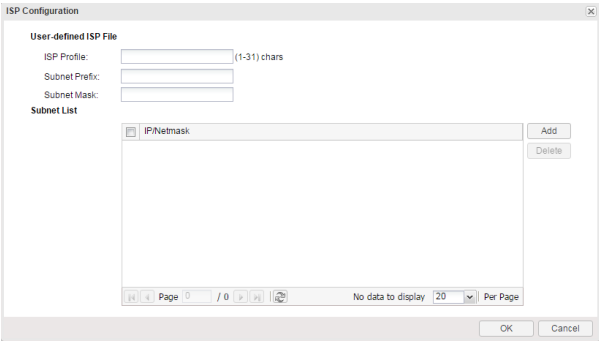
To configure an ISP route, you need to first add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload profiles that contain different ISP information.

Creating an ISP Profile

To create an ISP Profile, take the following steps:

- 1. Select **Network > Routing > ISP Profile**.
- 2. Click **New**.

In the ISP Configuration dialog box, enter values.

The ISP Configuration dialog box contains a section for 'User-defined ISP File' with three text input fields: 'ISP Profile:' (with a '(1-31) chars' hint), 'Subnet Prefix:', and 'Subnet Mask:'. Below these is a 'Subnet List' table with one row containing '192.168.1.0/24'. To the right of the table are 'Add' and 'Delete' buttons. At the bottom, there is a pagination bar showing 'Page 0 / 0', 'No data to display', and '20 Per Page'. 'OK' and 'Cancel' buttons are at the very bottom.

Option	Description
ISP Profile	Type the name for the new ISP profile into the textbox.
Subnet Prefix	Type the IP address for the subnet into the textbox.
Subnet Mask	Type the subnet mask into the textbox.
Add	Add the subnet to the ISP profile. The subnet will be displayed in the ISP subnet list below. If needed, repeat the steps to add multiple subnets for the ISP profile.
Delete	Delete the selected ISP profiles.

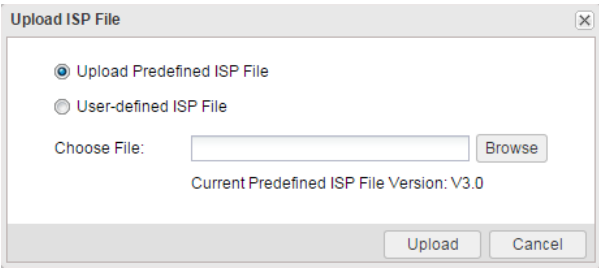
- 3. Click **OK**.

Uploading an ISP Profile

To upload an ISP Profile, take the following steps:

- 1. Select **Network > Routing > ISP Profile**.
- 2. Click **Upload**.

In the Upload ISP File dialog box, enter values.

The Upload ISP File dialog box has two radio buttons: 'Upload Predefined ISP File' (which is selected) and 'User-defined ISP File'. Below the radio buttons is a 'Choose File:' label followed by a text input field and a 'Browse' button. Below that, it says 'Current Predefined ISP File Version: V3.0'. At the bottom are 'Upload' and 'Cancel' buttons.

Option	Description
Upload Pre-defined IPS File	<p>To update the predefined IPS file:</p> <ol style="list-style-type: none"> 1. Select Upload Predefined IPS File. 2. Click Browse to select an IPS profile in your PC.
User-defined IPS File	<p>To update the user-defined IPS file:</p> <ol style="list-style-type: none"> 1. Select Upload Predefined IPS File. 2. Click Browse to select an IPS profile in your PC.

3. Click **Upload** to upload the selected ISP profile to device.

Saving an ISP Profile

To save an ISP Profile, take the following steps:

1. Select **Network > Routing > ISP Profile**.
2. Click **Save**.
3. In the Save User-defined ISP Configuration dialog box, select an ISP profile from the **ISP profile** drop-down list.
4. Click **Save** to save the profile to a specified location in PC.

ISP Route

Generally many users might apply for multiple lines for load balancing purpose. However, a typical balance will not have the function based on the traffic's direction. For such a scenario, the device provides the ISP route, which allows traffic from different ISPs to take their proprietary routes, thus accelerating network access.

To configure an ISP route, first you need to add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload profiles that contain different ISP information.

Creating an ISP Route

To create an ISP route, take the following steps:

- 1. Select **Network > Routing > ISP Route**.
- 2. Click **New**.

In the ISP Configuration dialog box, enter values.

ISP Route Configuration

ISP Profile:

China-telecom

Virtual Router:

trust-vr

Next Hop:

Gateway

Virtual Router in current Vsys

Interface

Virtual Router in other Vsys

Gateway:

Schedule:

Precedence:

10

(1-255) , default: 10

Weight:

1

(1-255) , default: 1

Description:

(0-63) chars

OK

Cancel

Option	Description
ISP Profile	Select an ISP profile name from the drop-down list.
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Next hop	<div>To specify the type of next hop, click Gateway, Current VRouter, Interface, or Other VRouter.</div> <div><ul style="list-style-type: none">• Gateway: Type the IP address into the Gateway text box.• Current VRouter: Select a name from the Virtual Router drop-down list.• Interface: Select a name from the Interface drop-down list. Type the IP address into the Gateway text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.• Other VRouter: Select a name from the Vsys drop-down list. Select a name from the Virtual Router drop-down list.</div>
Schedule	<div>Specifies a schedule when the rule will take effect. Select a desired schedule from the Schedule drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration.</div> <div>To create a new schedule, click New Schedule.</div>
Precedence	Type the route precedence into the textbox. The smaller the parameter is,

Option	Description
	the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 10. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the ISP route into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

3. Click **OK**.

Policy-based Route

Policy-based Route (PBR) is designed to select a router and forward data based on the source IP address, destination IP address and service type of a packet.

Creating a Policy-based Route

To create a Policy-based route, take the following steps:

- 1. Select **Network > Routing > Policy based Routing**.
- 2. Click **New**. Select **PBR** from the drop-down list.

In the Policy-based Route Configuration dialog box, configure the following.

Policy-based Route Configuration

PBR Name:

(1-31) characters

Virtual Router:

trust-vr

Type:

☒ Zone

☐ Virtual Router

☐ Interface

☐ No Binding

Bind To:

trust

OK

Cancel

Option	Description
PBR name	Specifies a name for the policy-based route.
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Type	<div>Specifies the object type that the policy-based route binds to. You can select Zone, Virtual Router, Interface or No Binding.</div> <ul style="list-style-type: none">• Zone: Click this option button and select a zone from the Zone drop-down list.• Virtual Router: Click this option button and show the virtual router that the policy-based route bind to.• Interface: Click this option button and select a interface from the Interface drop-down list.• No Binding: This policy-based route is no binding.



- 3. Click **OK**.




Creating a Policy-based Route Rule

To create a Policy-based Route rule, take the following steps:

1. Select **Network > Routing > Policy Based Routing**.
2. Click **New**. Select **Rule** from the drop-down list.

In the Rule Condition tab, configure the following.

Option	Description
PBR name	Specifies a name for the policy-based route.
Description (Optional)	Type information about the PBR rule.
Source	
Address	<p>Specifies the source addresses of PBR rule.</p> <ol style="list-style-type: none"> 1. Select an address type from the Address drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click  to add the addresses to the right pane. 4. After adding the desired addresses, click the blank area in this dialog to complete the source address configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • When selecting the Address Book type, you can click Add to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the any check box.
User	<p>Specifies a role, user or user group for the PBR rule.</p> <ol style="list-style-type: none"> 1. From the User drop-down menu, select the AAA server which the users and user groups belongs to. To specify a role, select Role from the AAA Server drop-down list. 2. Based on different types of AAA server, you can execute one or more actions: search a user/user group/role, expand the user-/user group list, enter the name of the user/user group. 3. After selecting users/user groups/roles, click  to add them to the right panes. 4. After adding the desired objects, click the blank area in this dialog to complete the user configuration.

Option	Description
Destination	
Address	<p>Specifies the destination addresses of PBR rule.</p> <ol style="list-style-type: none"> 1. Select an address type from the Address drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click  to add the addresses to the right panes. 4. After adding the desired addresses, click the blank area in this dialog to complete the destination address configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • When selecting the Address Book type, you can click Add to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the any check box.
Other	
Host Book	<p>Specifies the Host-book of PBR rule. Select an Host-book from the Host Book drop-down list.</p>
Service	<p>Specifies a service or service group.</p> <ol style="list-style-type: none"> 1. From the Service drop-down menu, select a type: Service, Service Group. 2. You can search the desired service/service group, expand the service/service group list. 3. After selecting the desired services/service groups, click  to add them to the right panes. 4. After adding the desired objects, click the blank area in this dialog to complete the service configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • To add a new service or service group, click Add. • The default service configuration is any. To restore the configuration to this default one, select the any check box.
Application	<p>Specifies an application/application group/application filters.</p> <ol style="list-style-type: none"> 1. From the Application drop-down menu, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click  to add them to the right panes. 3. After adding the desired objects, click the blank area in this dialog to complete the application configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • To add a new application group, click New AppGroup. • To add a new application filter, click New AppFilter.

Option	Description
Schedule	Specifies a schedule when the PBR rule will take effect. Select a desired schedule from the Schedule drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click New Schedule .
Record log	Select the Enable check box to enable the logging function for PBR rules.

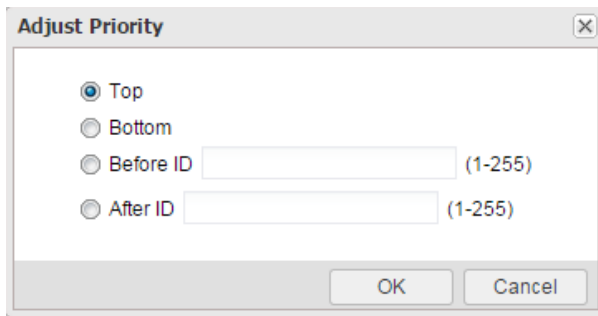
In the Next Hop tab, configure the following.

Option	Description
Set Next-hop	To specify the type of next hop, click IP Address , Virtual Router in current Vsys , Interface , or Virtual Router in other Vsys . <ul style="list-style-type: none"> IP Address: Type IP address into the IP address text box and specify the weight into the Weight text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value. Virtual Router in current Vsys: Select a name from the Next-Hop Virtual Router drop-down list and specify the weight into the Weight text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value. Interface: Select an interface from the Interface drop-down list and specify the weight into the Weight text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value. Virtual Router in other Vsys: Check the radio button to specify a virtual router in the current VSYS as the next hop. Select a virtual router from the Virtual Router drop-down list and specify the weight into the Weight text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value.
Track Object	Select the track object from the drop-down list. See "Track Object" on Page 267 .
Weight	Specifies the weight for the next hop. The value range is 1 to 255. The default value is 1. If a PBR rule is configured with multiple next hops, system will distribute the traffic in proportion to the corresponding weight.
Add	Click to add the specified next hop.
Delete	Select next-hop entries from the next hop table and click this button to delete.

Adjusting Priority of a PBR Rule

To adjust priority of a Policy-based Route rule, take the following steps:

1. Select **Network > Routing > Policy Based Routing**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.
3. Select the rule you want to adjust priority from the list below, click **Priority**.
4. In the Adjust Priority dialog box, enter values.



The 'Adjust Priority' dialog box contains four radio button options: 'Top' (selected), 'Bottom', 'Before ID' (with a text input field and '(1-255)' label), and 'After ID' (with a text input field and '(1-255)' label). At the bottom are 'OK' and 'Cancel' buttons.

Option	Description
Top	Click this option button to move the PBR rule to the top.
Bottom	Click this option button to move the PBR rule to the bottom.
Before ID	Click this option button and type the ID into the box to move the PBR rule to the position before the ID.
After ID	Click this option button and type the ID into the box to move the PBR rule to the position after the ID.



Note: Each PBR rule is labeled with a unique ID. When traffic flows into a Hillstone device, the device will query for PBR rules by turn, and process the traffic according to the first matched rule. However, the PBR rule ID is not related to the matching sequence during the query. You can move a PBR rule's location up or down at your own choice to adjust the matching sequence accordingly.

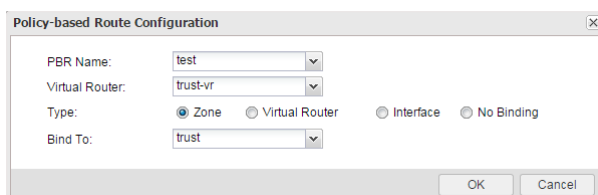
Applying a Policy-based Route

You can apply a policy-based route by binding it to an interface, virtual router or zone.

To apply a policy-based route, take the following steps:

1. Select **Network > Routing > Policy Based Routing**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.
3. Click **Bind to**.

In the Policy-based Route Configuration dialog box, enter values.



The 'Policy-based Route Configuration' dialog box shows 'PBR Name' set to 'test', 'Virtual Router' set to 'trust-vr', 'Type' with radio buttons for 'Zone' (selected), 'Virtual Router', 'Interface', and 'No Binding', and 'Bind To' set to 'trust'. 'OK' and 'Cancel' buttons are at the bottom.

Option	Description
PBR Name	Select a route from the PBR name drop-down list.
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Type	Specifies the object type that the policy-based route binds to. You can

Option	Description
	<p>select Zone, Virtual Router, Interface or No Binding.</p> <ul style="list-style-type: none"> • Zone: Click this option button and select a zone from the Zone drop-down list. • Virtual Router: Click this option button and show the virtual router that the policy-based route binds to. • Interface: Click this option button and select a interface from the Interface drop-down list. • No Binding: This policy-based route is no binding.

4. Click **OK**.

DNS Redirect

System supports the DNS redirect function, which redirects the DNS requests to a specified DNS server. For more information about specifying IP addresses of the DNS server, see [Configuring a DNS Server](#). Currently, the DNS redirect function is mainly used to redirect the video traffic for load balancing. With the policy based route working together, system can redirect the Web video traffic to different links, improving the user experience.

To enable the DNS redirect function, take the following steps:

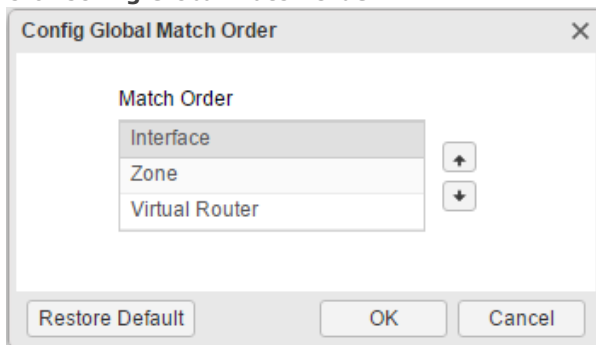
1. Select **Network > Routing > Policy Based Routing**.
2. Click **Enable DNS Redirect**.



Configuring the Global Match Order

By default, if the PRB rule is bound to both an interface , VRouter and the security zone the interface belongs to, the traffic matching sequence will be: Interface > Zone > VRouter. You can configure the global match order of PBR.

To configure the global match order, take the following steps:

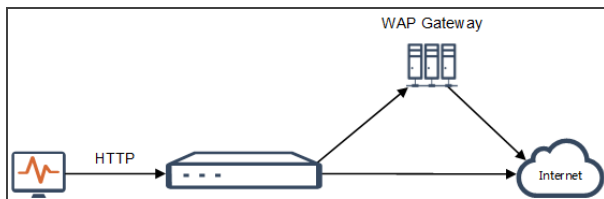
1. Select **Network > Routing > Policy Based Routing**.
2. Click **Config Global Match Order**.



3. Select the items that need to be adjusted, and click  and .
4. To restore the default matching sequence, click **Restore Default**.
5. Click **OK**.

WAP Traffic Distribution

The WAP traffic distribution function is designed to distribute the HTTP flow through the WAP gateway to relieve the traffic.



As shown in the topology above, the device that enabled WAP traffic distribution is deployed in front of the WAP server. When the HTTP traffic goes through the device, the system analyzes the traffic, and then distributes the flow to the WAP gateway or the Internet according to the configuration of the device. Normally, you will want to distribute your business service traffic to the WAP gateway, and allocate other traffic (e.g. Internet surfing or downloading) to the Internet.

The WAP traffic distribution function adopts a policy-based route rule. When the HTTP traffic of an interface matches a policy-based route rule, system will distribute the traffic to the specified next-hop IP address according to the PBR rule. For the traffic distributed to the Internet, you need to enable the IP replacement function. Because the original destination is the WAP gateway address, to enable accessibility, translating the original address to the actual destination is necessary.

To configure WAP traffic distribution, take the following steps:

- Enabling WAP traffic distribution.
- Configuring a DNS Server.
- Creating Host-book.
- Creating a Policy-based Route Rule.
- Checking WAP traffic distribution statistics.

Enabling WAP Traffic Distribution

To enable WAP traffic distribution on a specified interface, take the following steps:

1. Select Network > Interface and double click the interface you want.
2. Under the Basic tab, select the check box of **WAP traffic distribution**. For more information about the Host-book, see ["Configuring an Interface" on Page 47](#).

Configuring a DNS Server

The DNS server can be used to analyze the real destination IP address. For more information about the DNS server, see ["DNS" on page 76](#). A domain name can correspond to multiple IP addresses, so system can only support the first IP address that is analyzed.

Creating Host Book

To use the WAP traffic distribution function, you need to add a host book into the policy-based route rule. When the HTTP traffic matches the policy-based route rule, system will distribute the traffic to the WAP gateway or the Internet according to the PBR rule and whether the domain entry matches. For more information about the Host-book, see ["Host Book" on Page 236](#).

Creating a Policy-based Route Rule

To apply the host book domain entry in the policy-based route rule, bind the policy-based route rule to the interface that enabled the WAP traffic distribution function. For more information about the policy-based route, see ["Policy-based Route" on Page 112](#).

Video Streaming Redirection

You can redirect HTTP video streaming to a designated link to ensure a better streaming speed. The configuration of video streaming redirection combines multiple modules. The configuration logic is introduced here.

To configure video streaming redirection, take the following steps:

1. Configuring application identification: set up traffic control based on the data type.
2. Enabling video streaming redirection: enable WAP traffic distribution and assign the port number used for certain website's HTTP video. IP replacement is not needed.
3. Configuring PBR: Create a policy based route and adding the APP or services for video streaming, then binding this route rule to the interface which enables video streaming redirection.

RIP

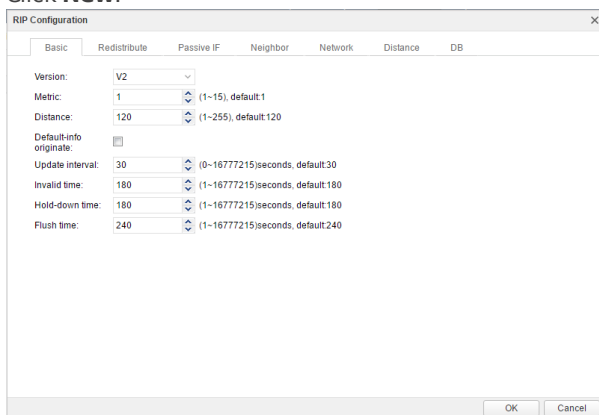
RIP, Routing Information Protocol, is an internal gateway routing protocol that is designed to exchange routing information between routers. Currently, devices support both RIP versions, i.e., RIP-1 and RIP-2.

RIP configuration includes basic options, redistribute, Passive IF, neighbor, network and distance. You will also need to configure RIP parameters for different interfaces, including RIP version, split horizon, and authentication mode.

Creating RIP

To create RIP, take the following steps:

1. Select **Network > Routing > RIP**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.
3. Click **New**.



In the Basic tab, configure the following.

Option	Description
Version	Specifies a RIP version. Hillstone devices support RIP-1 and RIP-2. RIP-1 transmits packets by broadcasting, while RIP-2 transmits packet by multicasting. Select a version from the drop-down list. The default version is RIP-2.
Metric	Specifies a default metric. The value range is 1 to 15. If no value is specified, the value of 1 will be used. RIP measures the distance to the destination network by hops. This distance is known as metric. The metric from a router to a directly connected network is 1, increment is 1 for every additional router between them. The max metric is 15, and the network with metric larger than 15 is not reachable. The default metric will take effect when the route is redistributed.
Distance	Specifies a default distance. The value range is 1 to 255. If no value is specified, the value of 120 will be used.
Information originate	Specifies if the default route will be redistributed to other routers with RIP enabled. By default RIP will not redistribute the default route. Select the check box to redistribute the default route.
Update interval	Specifies an interval in which all RIP routes will be sent to all the neighbors. The value range is 0 to 16777215 seconds. The default value is 30.
Invalid time	If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The value range is 1 to 16777215 seconds. The default value is 180.
Holddown time	If the metric becomes larger (e.g., from 2 to 4) after a route has been

Option	Description
	updated, the route will be assigned with a holddown time. During the holddown time, the route will not accept any update. The value range is 1 to 16777215 seconds. The default value is 180.
Flush time	System will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the end of flush time, it will be deleted from the RIP information database. The value range is 1 to 16777215 seconds. The default value is 240.

In the Redistribute tab, configure the following.

Option	Description
Protocol	Select a protocol type for the route from the Protocol drop-down list. The type can be Connected, Static, OSPF or BGP.
Metric	Type the metric for the route into the Metric box. If no value is specified, system will use the default metric value.
Add	Click Add to add the Redistribute route entry. All the entries that have been added will be displayed in the Redistribute Route list below.
Delete	Repeat the above steps to add more Redistribute route entries. To delete a Redistribute route entry, select the entry you want to delete from the list, and click Delete .

In the Passive IF tab, configure the following.

Option	Description
Interface	Select a passive interface from the Interface drop-down list.
Add	Click Add to add the passive interface. All the interfaces that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more Passive IFs. To delete a Passive IF, select the entry you want to delete from the list, and click Delete .

In the Neighbor tab, configure the following.

Option	Description
Neighbor IP	Type the neighbor IP into the Neighbor IP box.
Add	Click Add to add the neighbor IP. All the neighbor IPs that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more neighbor IPs. To delete a neighbor IP, select the entry you want to delete from the list, and click Delete .

In the Network tab, configure the following.

Option	Description
Network(IP/net-mask)	Type the IP address and netmask into the Network(IP/netmask) box.
Add	Click Add to add the network. All the networks that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more networks. To delete a network, select the entry you want to delete from the list, and click Delete .

In the Distance tab, configure the following.

Option	Description
Distance	Type the distance into the Distance box. The priority of the specified distance is higher than the default distance.
Network(IP/net-mask)	Type the IP prefix and netmask into the Network(IP/netmask) box.
Add	Click Add to add the distance. All the distances that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more distances. To delete a distance, select the entry you want to delete from the list, and click Delete .

In the DB tab, view the database of the RIP route .

All the route entries that can reach target network are stored in the database.

4. Click **OK**.



Note: Configuration for RIP on Hillstone device's interfaces includes: RIP version, split horizon and authentication mode. For more information on how to configure RIP on an interface, see ["Configuring an Interface" on Page 47](#).

Chapter 7 Authentication

Authentication is one of the key features for a security product. When a security product enables authentication, the users and hosts can be denied or allowed to access certain networks.

From a user's point of view, authentication is divided into the following categories:

- If you are a user from an internal network who wants to access the Internet, you can use:
 - ["Web Authentication" on Page 124](#)
 - ["Single Sign-On" on Page 131](#)
 - ["PKI" on Page 147](#)
- If you are a user from the Internet who wants to visit an internal network (usually with VPN), you can use:
 - ["SSL VPN" on Page 172](#)
 - ["IPSec VPN" on Page 153](#) (IPSec VPN (with radius server)+Xauth)
 - ["L2TP VPN" on Page 228](#) (L2TP over IPsec VPN)

Authentication Process

A user uses his/her terminal to connect to the firewall. The firewall calls the user data from the AAA server to check the user's identity.



- User (authentication applicant): The applicant initiates an authentication request, and enters his/her username and password to prove his/her identity.
- Authentication system (i.e. the firewall in this case): The firewall receives the username and password and sends the request to the AAA server. It is an agent between the applicant and the AAA server.
- ["AAA Server" on Page 249](#): This server stores user information like the username and password, etc. When the AAA server receives a legitimate request, it will check if the applicant has the right to the user network services and send back the decision. For more information, refer to ["AAA Server" on Page 249](#). AAA server has the following four types:
 - [Local server](#)
 - [Radius server](#)
 - [LDAP server](#)
 - [AD server](#)
 - [TACACS+server](#)

Web Authentication

Web authentication is used to identify the user who wants to visit the Internet. When Web authentication is enabled, the browser on the PC which is trying to access the Internet will show a login request. You need to input your user-name and password. When your information is correct, system will allocate your PC and IP address and give you a role that controls your authority.

- General Web authentication (WebAuth): a general Web authentication means that an authentication page will appear to check your information.
- "Single Sign-On" on Page 131: Single Sign On is a simplified WebAuth method. The authentication applicant will not be required to open an authentication page. When a user is a legitimate applicant in the AAA server, he/she can pass the identification automatically. For SSO, the AAA server type must be Active Directory server.

Using WebAuth Wizard

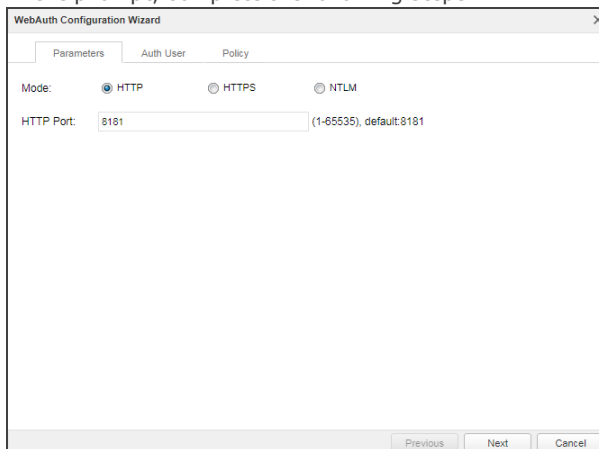
WebAuth wizard is the most convenient way to configure WebAuth.

The prerequisite for using the wizard is that you have already added AAA server in system and users are also added in that AAA server (refer to "AAA Server" on Page 249).

1. Select **Network > WebAuth > WebAuth**.
2. Click **WebAuth Wizard** on the right top corner.



3. In the prompt, complete the following steps.



Follow the steps in the wizard to complete authentication settings.

Parameters	
Mode	<p>Specify an authentication methods: HTTP, HTTPS or NTLM.</p> <ul style="list-style-type: none">• If you select HTTP or HTTPS, the auth user will be required to enter his/her username and password. HTTP and HTTPS indicate the protocol when transmitting the user's credentials between the client and the AAA server. HTTPS is encrypted, and can avoid information leakage.• If you select NTLM, auth user will not need to open an authen-

Parameters	
	entication page. System gets the user's PC login credential and send it to AAA server.
Auth User	
AAA Server	Specify the AAA server. Make sure that your selected AAA server has already set up all of the user's credentials and the server has been added in StoneOS system. Refer to "AAA Server" on Page 249 .
Policy	
Src Zone	Specify the source zone where auth users are from.
Dst Zone	Specify the destination zone where the auth users will visit.
DNS Zone	Specify the DNS zone.
When you click OK, system will automatically generate three security policies which are used for web auth. If you wish to customize some parts of this authentication process, like limit accessing time, you can modify the security policies. Refer to "Security Policy" on Page 296 .	

4. Click **OK**.

After WebAuth is configured, the users who matched the WebAuth policy are recommended to input the correct user-name and password, and then the users can access the network. System takes actions to avoid illegal users from getting usernames and passwords by brute-force. If one fails to log in through the same host three times in two minutes, that host will be blocked for 2 minutes.

Configuring Global Parameters for WebAuth

Global parameters apply to all WebAuth policies.

To configure WebAuth global parameters, take the following steps:

1. Select **Network > WebAuth > WebAuth**.

2. Under the WebAuth tab, select the radio button of the authentication method you want.

Under different mode, the configuration options will vary.

Authentication Mode	
Mode	Specify an authentication methods: HTTP, HTTPS or NTLM. <ul style="list-style-type: none"> If you select HTTP or HTTPS, the auth user will be required to enter his/her username and password. HTTP and HTTPS indicate the protocol when transmitting user's credential between the client and the AAA server. HTTPS is encrypted, and can avoid information leakage. If you select NTLM, auth user will not need to open an authentication page. System gets the user's PC login credential and send

Authentication Mode	
	<p>it to AAA server. Refer to "NTLM Authentication" on Page 127.</p> <ul style="list-style-type: none"> If you do not allow webauth, select Disable.
HTTP port	Specifies the HTTP protocol transmission port number of the authentication server. The range is 1 to 65535, and the default value is 8181.
HTTPS port	Specifies the HTTPS protocol transmission port number of the authentication server. The range is 1 to 65535, and the default value is 44433.
HTTPS trust domain	Specifies the HTTPS trust domain. This domain is previously created in PKI and has imported international CA certified certificate.
When NTLM Fails	<p>This option is used for NTLM authentication. It will define the next action when user fails to pass SSO login.</p> <p>Select Use HTTP Mode, and the next step is to use HTTP web-auth to continue authentication.</p> <p>Select Deny, and the users will fail to login in.</p>
User Login	
Multiple login	<p>If you disable multiple login, one account cannot login if it has already logged in elsewhere. You can choose to kick out the first login visitor or you can disable the second login.</p> <p>If you allow multiple login, more than one clients can login with the same account. But you can still set up the maximum number of clients using one account.</p>
Advanced	
Idle interval	The maximum time length of an inactive account after it has logs in.
Client Heartbeat Timeout	When the authenticator sends a request to ask the client to submit his/her username, the client need to respond within a specified period. If the client does not respond before timeout, system will resend the authentication request message.
Re-Auth Interval	When the client is authorized to access network, the authenticator can re-authenticate the client.
Forced Re-login Interval	If the forced re-login function is enabled, users must re-login after the configured interval ends.
Proxy Port	Specify the port number for HTTPS, HTTPS and SSO proxy server. The port number applies to all. If it changes in any page, the other mode will also use the new port. The range is 1 to 65535.
Popup URL	The popup URL function redirects the client to the specified URL after successful authentication. You need to turn off the pop-up blocker of your web browser to ensure this function can work properly. The format of URL should be "http://www.abc.com" or "https://www.abc.com".



Note:

- If the WebAuth success page is closed, you can log out not only by timeout, but also by visiting the WebAuth status page (displaying online users, online times and logout button). You can visit it through "http(https):// IP-Address: Port-Number". In the URL, IP-Address refers to the IP address of the WebAuth interface, and Port-Number refers to HTTP/HTTPS port. By default, the HTTP port is 8181, the HTTPS port is 44433. The WebAuth status page will be invalid if there are no online users on the client or the WebAuth is disabled.
- You can specify the username and password in the URL address. When the specified redirect URL is the application system page with the authentication needed in the intranet, you do not need the repeat authentication and can access the application system. The corresponding keywords are \$USER, \$PWD, or \$HASHPWD. Generally, you can select one keyword between \$PWD and \$HASHPWD. The format of the URL is "URL" + "username=\$USER&password=\$PWD".
- When entering the redirect URL in CLI, add double quotations to the URL address if the URL address contains question mark. For example, "http://192.10.5.201/oa/-login.do?username=\$USER&password=\$HASHPWD"

3. Click **Apply**.

NTLM Authentication

This method still needs to trigger the browser, and the browser will send user information to the AD server automatically.

The configuration of NTLM is the same with WebAuth, refer to ["Using WebAuth Wizard" on Page 124](#). After finishing the WebAuth wizard, take the following two steps for NTLM:

Step 1: Configuring NTLM for StoneOS

1. Select **Network > WebAuth > WebAuth** to enter the WebAuth page.



2. Select the **NTLM** radio button, the following parameters appear:

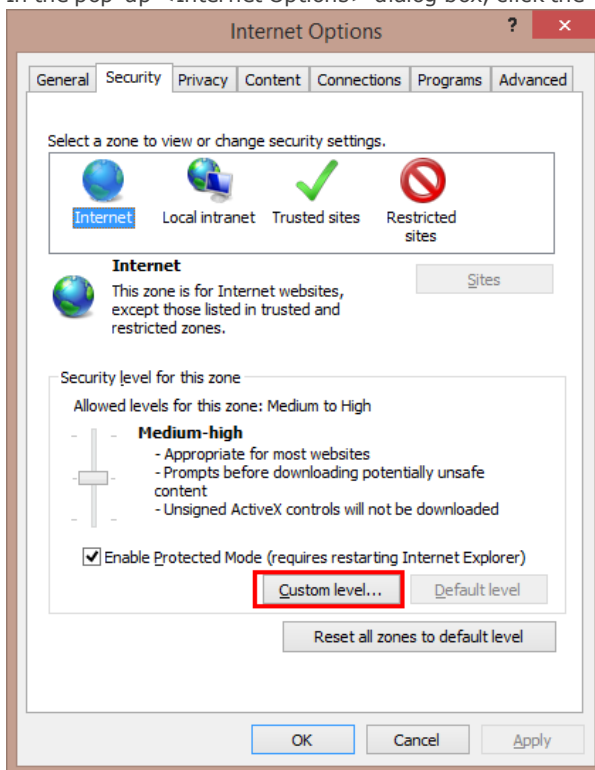
Authentication Mode	
When NTLM fails	If you select Use HTTP Mode , when a user fails to authenticate through NTLM, the user still can manually input user name and password in the browser page to authenticate again.
User Login	
Multiple login: Disable	<ul style="list-style-type: none"> • If select Replace, system only permits one user login, the user logged in will be kicked out by the user logging in. • If select Refuse New Login, system will disable the same user to log in again.
Multiple login: Enable	<ul style="list-style-type: none"> • If select Unlimited, system will not limit the concurrent login number of the same user. • If select Maximum, system will configure the maximum concurrent login number of the same user.

Authentication Mode	
Advanced	
Idle interval	The longest time that the authentication user can keep online without any traffic.
Force Re-login Interval	The time interval that system forces the login user to authenticate again.
Proxy port	Specifies the proxy port number of SSO proxy server. The range is 1 to 65535.

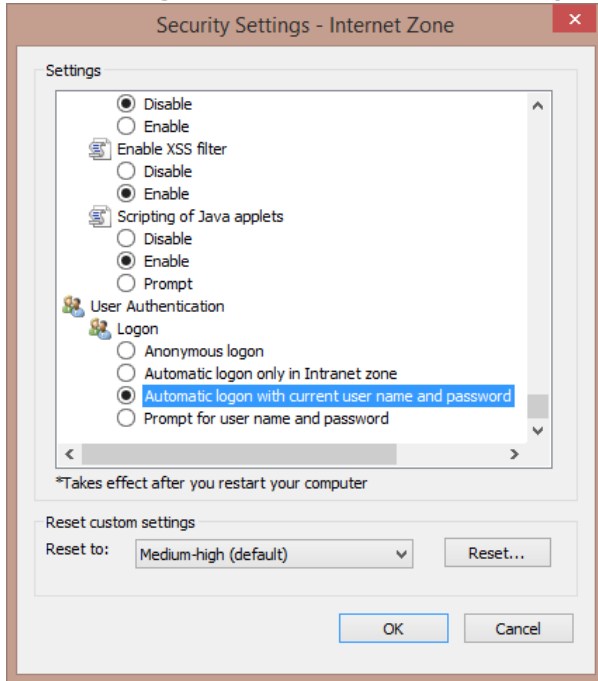
3. Click **Apply**.

Step 2: Configuring settings for User Browser

1. On the PC terminal of a user , open a browser (take IE as an example).
2. On the menu bar of IE browser, select **Tools > Internet options**.
3. In the pop-up <Internet Options> dialog box, click the <Security> tab, and click **Custom level...**.



4. In the pop-up <Security Settings - Internet Zone> dialog box, enter **User Authentication>Logon** and select **Automatic logon with current user name and password**.

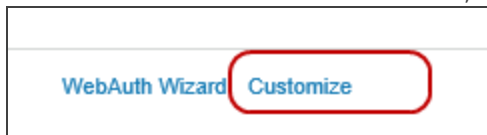


5. Click **OK**.

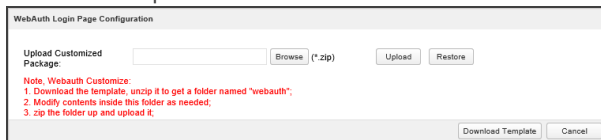
Modifying WebAuth Page

The WebAuth page is the redirected page when an authenticated user opens the browser. By default, you need to enter his/her username and password in the WebAuth page. If you select the SMS mode, you need to enter the phone number and SMS code in the WebAuth page.

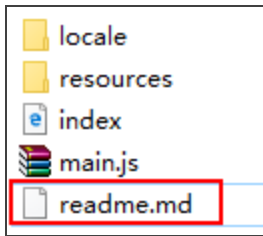
1. Select **Network > WebAuth > WebAuth**, and click **Customize** on the right top corner.



2. In the prompt, click **Download Template** to download the zip file "webauth" of the default WebAuth login page, and then unzip the file.



3. Open the source file and modify the content(including style, picture, etc.)according to the requirements. For more detailed information, see the file of **readme.md**.



4. Compress the modified file and click **Upload** to upload the zip file to system.



Note:

- The WebAuth login page you already specified will be invalid after you upgrade the version from the old to 5.5R5.
- The zip file should comply with the following requirements: the file format should be zip; the maximum number of the file in the zip file is 50; the upper limit of the zip file is 1M; the zip file should contain "index.html".
- System can only save one file of the default template page and the customized page. When you upload the new customized page file, the old file will be covered. You are suggested to back up the old file.

Single Sign-On

When the user authenticates successfully for one time, system will obtain the user's authentication information. Then the user can access the Internet without authentication later.

SSO can be realized through three methods, which are independent from each other, and they all can achieve the "no-sign-on"(don't need to enter a user name and password) authentication.

Method	Installing Software or Script	Description
SSO Radius	---	After enabling SSO Radius function, system can receive the accounting packets that based on Radius standard protocol. System will obtain user authentication information, update online user information and manage user's login and logout according to the packets.
AD Scripting	Logonscript.exe	This method needs to install the script "Logonscript.exe" on the AD server. The triggered script can also send user information to StoneOS. This method is recommended if you have a higher accuracy requirement for statistical monitoring and don't mind to change the AD server.
AD Polling	---	After enabling the AD Polling function, system will regularly query the AD server to obtain the login user information and probe the terminal PC to verify whether the users are still online, thus getting correct authentication user information to achieve SSO. This method is recommended if you don't want to change the AD server.
SSO Monitor	---	After enabling SSO Monitor, StoneOS will build connection with the third-party authentication server through SSO-Monitor protocol, as well as obtain user online status and information of the group that user belongs to. System will also update the mapping information between user name and IP in real time for online user.
AD Agent	AD Security Agent	This method needs to install AD Security Agent software on the AD server or other PCs in the domain. The software can send user information to StoneOS. This method is recommended if you don't want to change the AD server.

Enabling SSO Radius for SSO

After enabling SSO Radius function, system can receive the accounting packets that based on Radius standard protocol. System will obtain user authentication information, update online user information and manage user's login and logout according to the packets.

To configure the SSO Radius function, take the following steps:

1. Click **Object>SSO Server>SSO Radius** and enter **SSO Radius** page. By default, SSO Radius is disabled.

SSO Radius: ☐

Port: (1024-65535), default: 1813

AAA Server:

Client: ?

IP Address	Shared Secret	User Timeout(minutes)
------------	---------------	-----------------------

+ -

Apply Cancel

2. Click ☒ checkbox to enable the SSO Radius function.
3. Specify the Port to receive Radius packets for StoneOS (Don't configure port in non-root VSYS). The range is 1024 to 65535. The default port number is 1813.
4. Specify the AAA Server that user belongs to. You can select the configured Local, AD or LDAP server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.
5. Specify the IP Address, Shared Secret and Idle Interval of SSO Radius client which is allowed to access system. You can configure up to 8 clients.
 - IP Address: Specify the IPv4 address of SSO Radius client. If the IPv4 address is 0.0.0.0, it means that system receives the packets sent from any Radius client.
 - Shared Secret: Specify the shared secret key of SSO Radius client. The range is 1 to 31 characters. System will verify the packet by the shared secret key, and parse the packet after verifying successfully. If system fails to verify the packet, the packet will be dropped. The packet can be verified successfully only when SSO Radius client is configured the same shared secret key with system or both of them aren't configured a shared secret key.
 - User Timeout(minutes): Configure the idle interval for the authentication information of Radius packet in the device. If there's no update or delete packet of the user during the idle interval, the device will delete the user authentication information. The range is 0 to 1440 minutes. The default value is 30. 0 means the user authentication information will never timeout.
6. Click **Apply** button to save all the configurations.

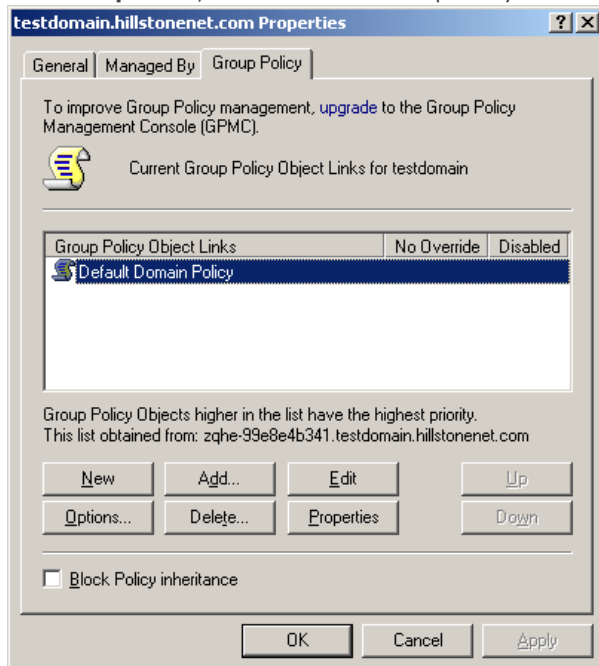
Using AD Scripting for SSO

Before using a script for SSO, make sure you have established your Active Directory server first. To use a script for SSO, take the following steps:

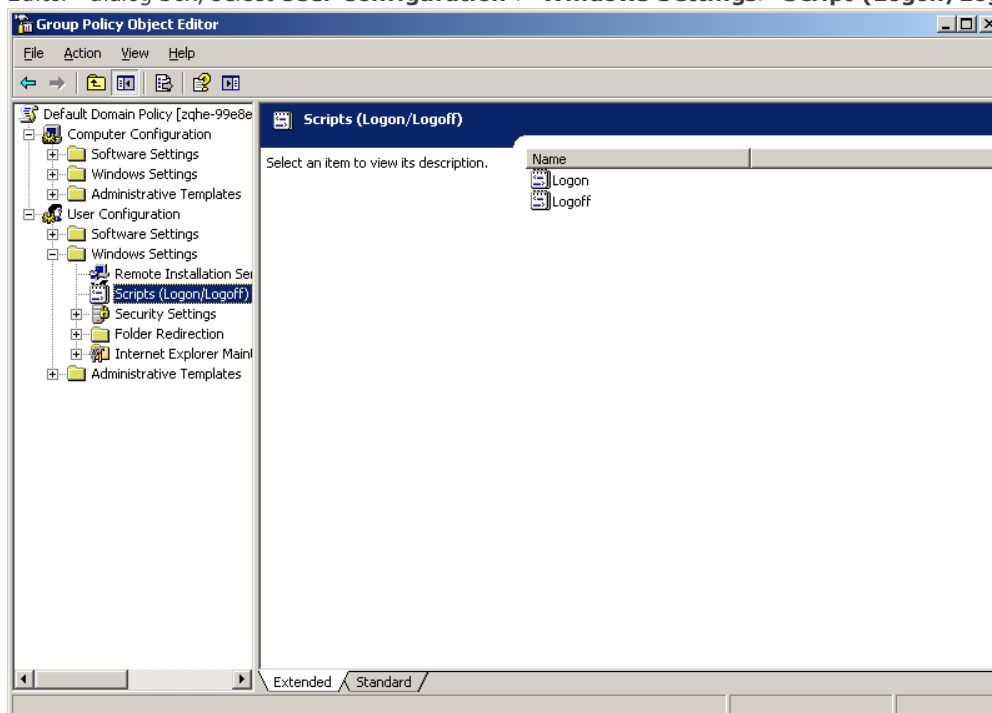
Step 1: Configuring the Script for AD Server

1. Open the AD Security Agent software(for detailed information of the software, see [Using AD Agent Software for SSO](#)). On the <AD Scripting> tab, click **Get AD Scripting** to get the script "Logonscript.exe" , and save it in a directory where all domain users can access.

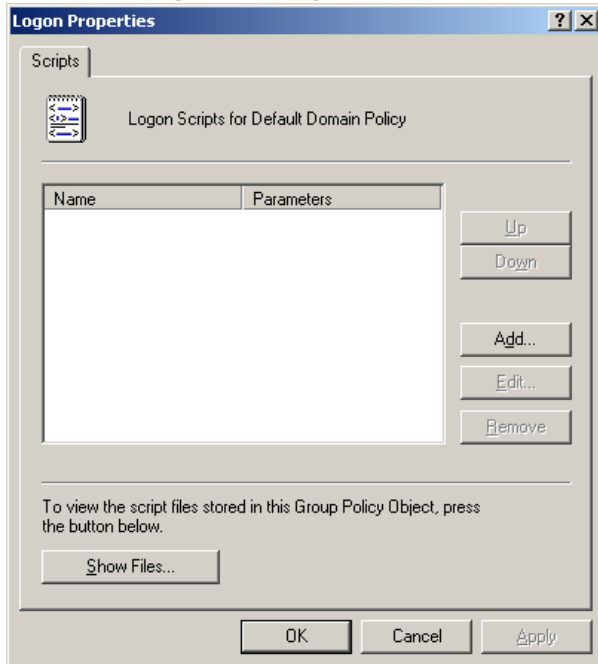
2. In the AD server, enter **Start** menu, and select **Management Tools > Active Directory User and Computer**.
3. In the pop-up <Active Directory User and Computer> dialog box, right-click the domain which will apply SSO to select **Properties**, and then click <Group Policy> tab.



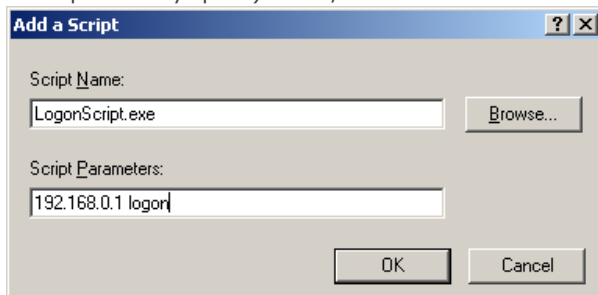
4. In the Group Policy list, double-click the group policy which will apply SSO. In the pop-up <Group Policy Object Editor> dialog box, select **User Configuration > Windows Settings> Script (Logon/Logout)**.



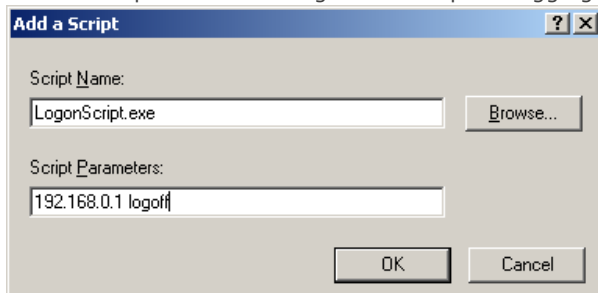
5. Double-click **Logon** on the right window, and click **Add** in the pop-up <logon properties> dialog box.



6. In the <Add a Script> dialog box, click **Browse** to select the logon script (logonscript.exe) for the Script Name; enter the authentication IP address of StoneOS and the text "logon" for the Script Parameters (the two parameters are separated by space). Then, click **OK**.



7. Take the steps of 5-6 to configure the script for logging out, and enter the text "logoff" in the step 6.



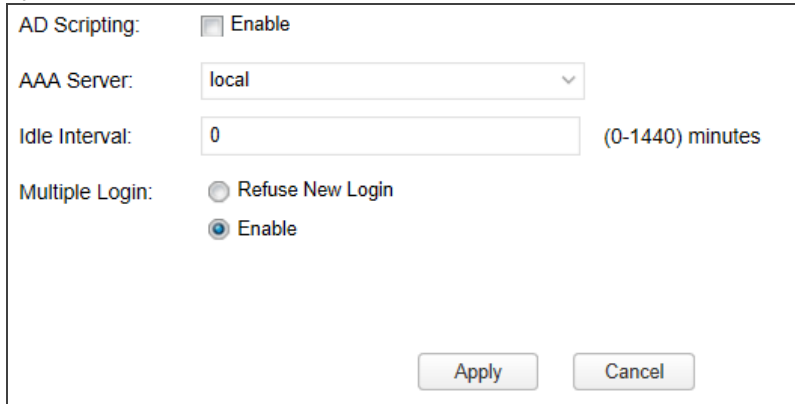
Note: The directory of saving the script should be accessible to all domain users, otherwise, when a user who does not have privilege will not trigger the script when logs in or out.

Step 2: Configuring AD Scripting for StoneOS

After the AD Scripting is enabled, the user can log in Hillstone device simultaneously when logging in the AD server successfully. System only supports AD Scripting of Active Directory server.

To configure the AD Scripting function, take the following steps:

1. Click **Object> SSO Server> AD Scripting** to enter the AD Scripting page. The AD Scripting function is disabled by default.




2. Select the **Enable** check box of AD Scripting to enable the function.
3. Specify the AAA Server that user belongs to. You can select the configured Local, AD or LDAP server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.
4. Specify the Idle Interval, which specifies the longest time that the authentication user can keep online without any traffic. After the interval timeout, StoneOS will delete the user authentication information. The value range is 0 to 1440 minutes. 0 means always online.
5. Allow or disable users with the same name to log in depends on needs.
 - **Enable**: Click to permit the user with the same name to log in from multiple terminals simultaneously.
 - **Refuse New Login**: Click to permit only one user with the same name to log in, and the user logged in will be kicked out by the user logging in.
6. Click **Apply** to save the changes.

After completing the above two steps, the script can send the user information to StoneOS in real time. When users log in or out, the script will be triggered and send the user behavior to StoneOS.

Using AD Polling for SSO

When the domain user logs in the AD server, the AD server will generate login logs. After enabling the AD Polling function, system will regularly query the AD server to obtain the user login information and probe the terminal PCs to verify whether the users are still online, thus getting correct authentication user information to achieve SSO.

Before using AD Polling for SSO, you should make sure that the Active Directory server is set up first. To use AD Polling for SSO, take the following steps:

1. Click **Object>SSO Client>AD Polling** to enter the AD Polling page.
2. Click the  **New** button on the upper left corner of the page, and the **AD Polling Configuration** dialog box pops up.

AD Polling Configuration

Name:

(1-31) chars

Status:

☐ Enable

Host:

(1-31) chars

Virtual Router:

trust-vr

Account:

(1-31) chars

Password:

(1-31) chars

AAA Server:

local

AD Polling Interval:

2

(1-3600) seconds

Client Probing Interval:

0

(0-1440) minutes ?

Force Timeout:

600

(0-144000) minutes ?

OK

Cancel

In the AD Polling Configuration dialog box, configure the following:

Option	Description
Name	Specifies the name of the new AD Polling profile. The range is 1 to 31 characters
Status	<p>Click Enable checkbox to enable the AD Polling function. After enabling, system will query the AD server to obtain the user information and probe the terminal PC to verify whether the online users are online regularly. When queries for the first time, system will obtain the online user information on the AD server in the previous 8 hours .</p> <p>If fails to obtain the previous information, system will obtain the following online user information directly.</p>
Host	Enter the IP address of authentication AD server in the domain. You can only select AD server. After specifying the authentication AD server, when the domain users log in the AD server, the AD server will generate the login logs. The range is 1 to 31 characters.
Virtual Router	Select the virtual router that the AD server belongs to in the drop-down list.
Account	Enter a domain user name to log in the AD server. The format is domain\username, and the range is 1 to 63 characters. The user is required to have permission to query security logs on the AD server, such as the user of Administrator whose privilege is Domain Admins on the AD server.

Option	Description
Password	Enter a password corresponding to the domain user name. The range is 1 to 31 characters.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see " AAA Server " on Page 249. You are suggested to select the configured authentication AD server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role,.
AD Polling Interval	Configure the interval for regular AD Polling probing. System will query the AD server to obtain the online user information at interval. The range is 1 to 3600 seconds, and the default value is 2 seconds. You are suggested to configure 2 to 5 seconds to ensure to obtain online user information in real time.
Client Probing Interval	Configure the interval for regular client probing. System will probe whether the user is still online through WMI at interval, and kick out the user if cannot be probed. The range is 0 to 1440 minutes, and the default value is 0 minute(the function is disabled). You are suggested to configure a larger probing interval to save the system performance, if you have low requirements for the offline users.
Force Timeout	Configure the forced logout time. When the user's online time exceeds the configured timeout time, system will kick out the user and force the user to log out. The range is 0 (the function is disabled) to 144000 minutes, and the default value is 600 minutes.

3. Click **OK** button to finish the configuration of AD Polling.



Note:

- When system is restarted or the configuration of AD Polling (except the account, password and force timeout) is modified, system will clear the existed user information and obtain the user information according to the new configuration.
- To realize the AD Polling function, you need to enable the WMI of the PC where the AD server is located and the terminal PC. By default, the WMI is enabled. To enable WMI, you need to enter the **Control Panel >Administrative Tools> Services** and enable the WMI performance adapter.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the RPC service and remote management should be enabled. By default, the RPC service and remote management is enabled. To enable the RPC service, you need to enter the **Control Panel >Administrative Tools> Services** and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command **netsh firewall set service RemoteAdmin**.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel**




>**System and Security**> **Windows Firewall** >**Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.

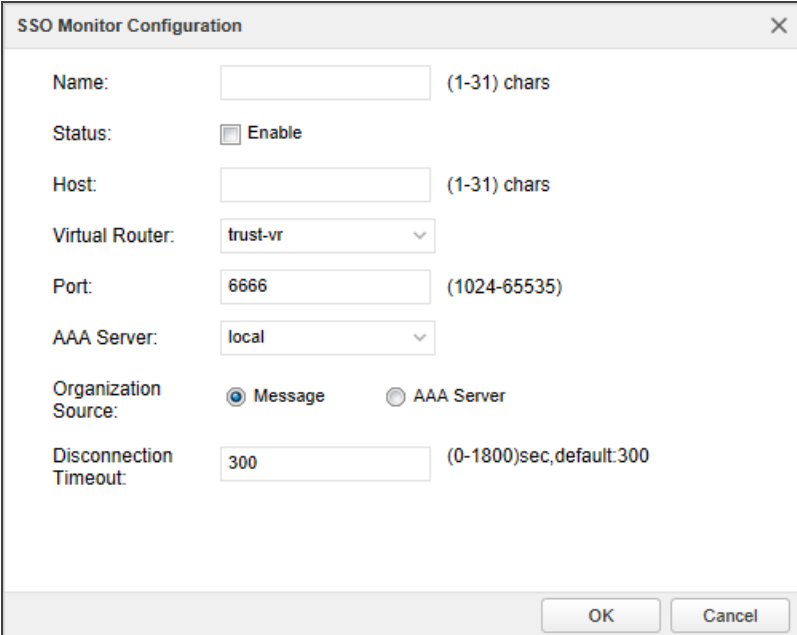
- To use the offline function, you should make sure that the time of the PC where the AD server is located and the terminal PCs is the same. To enable the function of Synchronize with an Internet time server, select **Control Panel > Clock, Language, and Region > Date and Time**, and the Date and Time dialog box pops up. Then, click **Internet Time** tab, and check **Synchronize with an Internet time server**.

Using SSO Monitor for SSO

When user logs in through the third-party authentication server, the authentication status will be saved on the server. StoneOS will build connection with the third-party authentication server through SSO-Monitor protocol, as well as obtain user online status and information of group that user belongs to.

To use SSO Monitor for SSO, take the following steps:

1. Click **Object>SSO Client>SSO Monitor** to enter **SSO Monitor** page.
2. Click the  **New** button and the **SSO Monitor Configuration** dialog box pops up.



The SSO Monitor Configuration dialog box contains the following fields and options:

- Name:** Text input field with a character count of (1-31) chars.
- Status:** Check box labeled **Enable**.
- Host:** Text input field with a character count of (1-31) chars.
- Virtual Router:** Dropdown menu with the value **trust-vr**.
- Port:** Text input field with the value **6666** and a character count of (1024-65535).
- AAA Server:** Dropdown menu with the value **local**.
- Organization Source:** Radio buttons for **Message** (selected) and **AAA Server**.
- Disconnection Timeout:** Text input field with the value **300** and a character count of (0-1800)sec, default:300.

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

In the SSO Monitor Configuration dialog box, configure the following:

Name	Specify the name of the new SSO Monitor. The range is 1 to 31 characters.
Status	Click Enable checkbox to enable the SSO Monitor function. After enabling the function, system will build connection with the third-party authentication server through SSO-Monitor protocol, as well as obtain user online status and information of group that user belongs to. The machine will generate authentication user according to the authentication information.
Host	Enter the IP address of the authentication server. The range is 1 to 31 characters. You can select the third-party custom authentication server which supports SSO-Monitor protocol. After specifying the authentication server, when user logs in the specified server, the server will save user's authentication information.
Virtual Router	Select the virtual router that the authentication server belongs to in the drop-down list.
Port	Specifies the port number of the third-party authentication server. System will obtain user information through the port number. The default number is 6666. The range is 1024 to 65535.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see "AAA Server" on Page 249 for configuration method. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.
Organization Source	Select the method to synchronize user organization structure with system, including Message and AAA Server. When Message is selected, StoneOS will use the user group of authentication information as the group that user belongs to. It's usually used in the scenario of the third-party authentication server saving user group. When AAA Server is selected, StoneOS will use the user organization structure of AAA server as the group that user belongs to. It's usually used in the scenario of the third-party authentication server being authenticated by AAA server and the user organization structure being saved in the AAA server.
Disconnection Timeout	Configure the disconnection timeout. When StoneOS disconnects with the third-party authentication server due to timeout, system will wait during the disconnection timeout. If system still fails to connect within the configured time, it will delete online users. The range is 0 to 1800 seconds. The default value is 300. 0 means the user authentication information will never timeout.

3. Click **OK** button to finish SSO Monitor configuration.



Note: You can configure different numbers of SSO Monitor on different servers. When the configured number exceeds the limit, system will pop up the alarm information.

Using AD Agent Software for SSO

Before using AD Security Agent for SSO, make sure you have established your Active Directory server first. To use AD Security Agent for SSO, take the following steps:

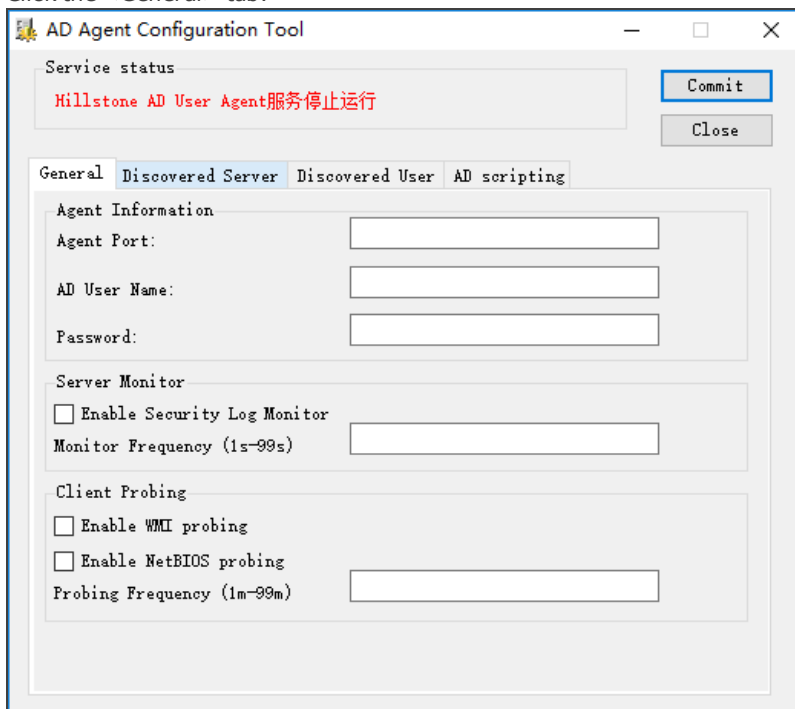
Step 1: Installing and Running AD Security Agent on a PC or Server

AD Security Agent can be installed on an AD server or a PC in the domain. If you install the software on an AD server, the communication only includes "AD Security Agent → StoneOS"; If you install the software on a PC in the domain, the communication includes both process in the following table. The default protocol and port used in the communication are described as follows:

Communication direction		AD Security Agent→AD Server	AD Security Agent→StoneOS
Protocol		TCP	TCP
Port	StoneOS	---	6666
	AD Security Agent	1935、1984	6666
	AD Server	445	---

To install the AD Security Agent to an AD server or a PC in the domain, take the following steps:

1. Click <http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-adagent> to download an AD Security Agent software, and copy it to a PC or a server in the domain.
2. Double-click `ADAgentSetup.exe` to open it and follow the installation wizard to install it.
3. Start AD Security Agent through one of the two following methods:
 - Double-click the `AD Agent Configuration Tool` shortcut on the desktop.
 - Click **Start** menu, and select **All app > Hillstone AD Agent > AD Agent Configuration Tool**.
4. Click the <General> tab.



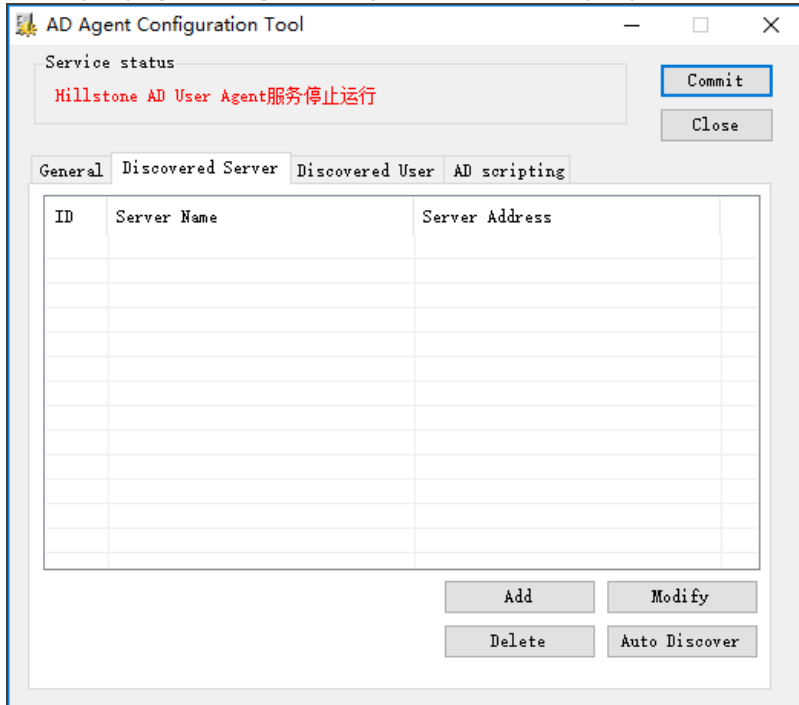
On the <General> tab, configure these basic options.

Option	Description
Agent Port	Enter agent port number. AD Security Agent uses this port to communicate with StoneOS. The range is 1025 to 65535. The

Option	Description
	default value is 6666. This port must be the same with the configured monitoring port in StoneOS, otherwise, the AD Security Agent and StoneOS cannot communicate with each other.
AD User Name	Enter user name to log in the AD server. If AD Security Agent is running on the other PCs of the domain, this user should have high privilege to query event logs in AD server, such as the user of Administrator whose privilege is Domain Admins on AD server.
Password	Enter the password that matched with the user name. If the AD Security Agent is running on the device where the AD server is located, the user name and password can be empty.
Server Monitor	
Enable Security Log Monitor	Select to enable the function of monitoring event logs on AD Security Agent. The default query interval is 5 seconds. The function must be enabled if the AD Security Agent is required to query user information.
Monitor Frequency	Specifies the polling interval for querying the event logs on different AD servers. The default value is 5 seconds. When finishing the query of a AD server, the AD Security Agent will send the updated user information to system.
Client probing	
Enable WMI probing	<p>Select the check box to enable WMI probing.</p> <ul style="list-style-type: none"> To enable WMI to probe the terminal PCs, the terminal PCs must open the RPC service and remote management. To enable the RPC service, you need to enter the Control Panel >Administrative Tools> Services and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command netsh firewall set service RemoteAdmin. WMI probing is an auxiliary method for security log monitor. which will probe all IPs in Discovered Users list. When the probed domain name does not match with the stored name, the stored name will be replaced by the probed name.
Probing Frequency	Specifies the interval of active probing action. The range is 1 to 99 minutes and the default value is 20 minutes.

- On the <Discovered Server> tab, click **Auto Discover** to start automatic scanning the AD servers in the domain. Besides, you can click **Add** to input IP address of server to add it manually.

When querying event logs in multiple AD servers, the query order is from top to bottom in the list.



6. Click the <Discovered User> tab to view the corresponding relationship between the user name and user address that has been detected.
7. On the <AD Scripting> tab, click **Get AD Scripting** to get the script "Logonscript.exe". (For introduction and installation of this script, refer to "Using AD Scripting for SSO" on Page 132) .
8. Click **Commit** to submit all settings and start AD Security Agent service in the mean time.



Note: After you have committed, AD Agent service will be running in the background all the time. If you want to modify settings, you can edit in the **AD Agent Configuration Tool** and click **Commit**. The new settings can take effect immediately.

Step 2: Configuring AD server for StoneOS

To ensure that the AD Security Agent can communicate with StoneOS, take the following steps to configure the AD server:

1. Click **Object>AAA Server** to enter the AAA server page.
2. Choose one of the following two methods to enter the Active Directory server configuration page:
 - Click the **+ New** button on the upper left corner of the page, and choose **Active Directory Server** in the drop-down list.
 - Choose the configured AD server and click the **Edit** button on the upper left corner of the page.

Basic Configuration:

Server Name: test (1-31) chars

Server Address: 192.168.2.2 (1-31) chars

Virtual Router: trust-vr

Port: 389 (1-65535), default: 389

Base-dn: dc=abc, dc=xyz, dc=com (1-127) chars

Login-dn: cn=administrator, cn=users, dc=abc (0-127) chars

sAMAccountName: administrator (0-63) chars

Authentication Mode: ☒ Plain Text ☐ MD5

Password: ••••• (1-31) chars

Optional:

Role mapping rule: -----

Backup Server 1: Domain/IP

Virtual Router 1: -----

Backup Server 2: Domain/IP

Virtual Router 2: -----

Synchronization: ☒ Enable

Auto Synchronization: ☒ Interval Synchronization 30 (30-1440)min, default: 30
☐ Daily Synchronization :
☐ Once Synchronization

Synchronous Operation Mode: ☒ Group Synchronization
☐ Organization Structure(OU) Synchronization

OU maximum depth: 12 (1-12), Default: 12

User Filter: (0-120) chars ⓘ

Security Agent: ☒ Enable When the security agent is enabled the system will perform single sign-on(SSO).

Agent Port: 6666 (1025-65535), default: 6666

Disconnection Timeout: 300 (0-1800)sec, default: 300

Backup Authentication Server: -----

3. For basic configuration of AD server, see [Configuring Active Directory Server](#).

The following configurations should be matched with the AD Security Agent:

- **Server Address:** Specify the IP address or domain name of AD server. It should be the same with the IP address of the device installed AD Security Agent.
- **Security Agent:** Check the checkbox to enable SSO function, and the server can send the user online information to StoneOS.
 - **Agent Port:** Specify the monitoring port. StoneOS communicates with the AD Security Agent through this port. The range is 1025 to 65535. The default value is 6666. This port should be the same with the configured port of AD Security Agent, or system will fail to communicate with the AD Agent.
 - **Disconnection Timeout:** Specifies the timeout time of deleting user binding information. The range is 0 to 1800 seconds. The default value is 300 seconds. 0 means never timeout.

4. Click **OK** to finish the related configuration of AD server.

After completing the above two steps, when domain user logs in the AD server, the AD Security Agent will send the user name, address and online time to the StoneOS.

802.1x

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

802.1X is a standard defined by IEEE for Port-based Network Access Control. It uses Layer-2 based authentication (protocol: EAPOL, Extensible Authentication Protocol over LAN) to verify the legality of the users accessing the network through LAN. Before authentication, the security device only allows the 802.1X message to pass through the port. After authentication, all of the normal traffic can pass through.

The AAA servers for 802.1x are Local server and Radius server. Other types of AAA servers like AD or LDAP server do not support 802.1x.

The authenticating process is the same with other authentication, please refer to "[Chapter 7 Authentication](#)" on [Page 123](#).

Configuring 802.1x

A complete configuration for 802.1x authentication includes the following points:

- Prerequisite: Before configuration, you should already have the AAA server you want (only local or Radius server is supported for 802.1x). The AAA server has been added in the firewall system (refer to AAA server), and the interface or VLAN for authentication has been bound to a security zone (refer to interface or vlan).
- Configuration key steps:
 1. Creating a 802.1x profile.
 2. Creating a security policy to allow accessing.
- In the user's PC, modify the network adapter's properties: If the computer is connected to the 802.1x interface, this computer should enable its authentication function on its LAN port (right click **LAN** and select **Properties**, in the prompt, under the <Authentication> tab, select **MD5-Challenge** or **Microsoft: Protected EAP (PEAP)**, and click **OK** to confirm.)



Note: Early versions of Windows have enabled 802.1x by default, but Windows 7 and Window 8 do not have this feature enabled. To enable 802.1x, please search online for a solution that suits your system.

Creating 802.1x Profile

To create a 802.1x profile, take the following steps:

1. Select **Network > 802.1x > 802.1x**.
2. Click **New** and a prompt appears.

Under the Basic tab and Advanced tab, enter values

Basic	
802.1x Name	Enter a name for the 802.1x profile
Interface	Select the interface for 802.1x authentication. It should be a Layer-2 interface or a VLAN interface.
AAA Server	Select the AAA server for 802.1x authentication. It should be a local server or a Radius server.
Access Mode	Select an access mode. If you select Port and one of the clients connected to 802.1x interface has passed authentication, all clients can access the Internet. If you select MAC , every client must pass authentication before using Internet.
Advanced	
Port authorized	<p>If you select Auto, system will allow users who have successfully passed authentication to connect to network;</p> <p>If you select Force-unauthorized, system will disable the authorization of the port; as a result, no client can connect to the port, so there is no way to connect to the network.</p>
Re-auth period	Enter a time period as the re-authentication time. After a user has successfully connected to the network, system will automatically re-auth the user's credentials. The range is from 0 to 65535 seconds. If the value is set to 0, this function is disabled.
Quiet period	If the authentication fails, it will take a moment before system can process the authenticating request from the same client again. The range is 0 to 65535 seconds, and the default value is 60 seconds. If this value is set to 0, system will not wait, and will immediately process the request from the same client.
Retry times	Specifies a number for retry times. If the authentication system does not receive any response from the client, system will try to require user's credentials again. When system has tried for the specified times, it will stop trying. The range is 1 to 10 times, and the default is 2 times.
Sever timeout	Specifies a server timeout value. The authenticator transmits the client's credentials to the authentication server. If the server does not answer the authenticator within a specified time, the authenticator will resend request to the authentication server. The range is 1 to 65535 seconds, the default value is 30 seconds.
Client timeout	When the authenticator sends a request to ask the client to submit his/her username, the client needs to respond within a specified period. If the client does not respond before timeout, system will resend the authentication request message. The range is 1 to 65535 seconds, and the default value is 30 seconds.

3. Click **OK**.

802.1x Global Configuration

Global parameters apply to all 802.1x profiles.

To configure global parameters, take the following steps:

1. Select **Network > 802.1x> Global Configuration**.

The dialog box contains the following fields and controls:

- Max user number:** A text input field with the value "1000" and a range indicator "(1-1000)default1000".
- Multiple login:** A dropdown menu currently showing "Disable".
- Behavior:** Two radio buttons: "Replace" (unselected) and "Refuse" (selected).
- Re-Auth time:** A text input field with the value "300" and a range indicator "(180-86,400) secs".
- At the bottom are "OK" and "Cancel" buttons.

In the Global Configuration dialog box, specify the parameters that will be applicable for all 802.1x profiles.

Option	Description
Max user number	The maximum user client number for a authentication port.
Multiple login	<p>You may choose to allow or disable one account to login from different clients.</p> <ul style="list-style-type: none">• Disable: If you select Disable, one account can only login from one client simultaneously. Then, when you want to kick off the old login user, you should select Replace; if you want to disallow new login user, select Refuse.• Enable: If you select Enable, different clients can use one account to login. If you do not limit the login client number, select Unlimited; if you want to set up a maximum login number, select Max attempts and enter a value for maximum user client number.
Re-Auth time	Specify a time for authentication timeout value. If the client does not respond within the timeout period, the client will be required to re-enter its credentials. The range is 180 to 86400 seconds, the default value is 300 seconds.

2. Click **OK**.

Viewing Online Users

To view which authenticated users are online:

1. Select **Network > 802.1x > Online user**.
2. The page will show all online users. You can set up filters to view results that match your conditions.

PKI

PKI (Public Key Infrastructure) is a system that provides public key encryption and digital signature service. PKI is designed to automate secret key and certificate management, and assure the confidentiality, integrity and non-repudiation of data transmitted over the Internet. The certificate of PKI is managed by a public key by binding the public key with a respective user identity by a trusted third-party, thus authenticating the user over the Internet. A PKI system consists of Public Key Cryptography, CA (Certificate Authority), RA (Certificate Authority), Digital Certificate and related PKI storage library.

PKI terminology:

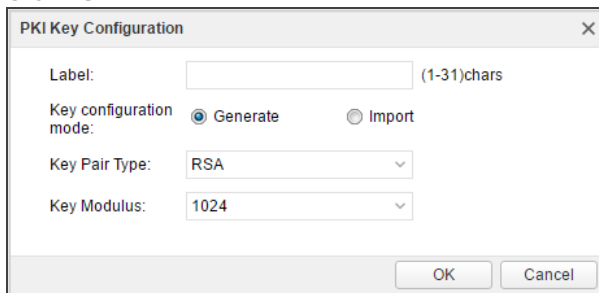
- **Public Key Cryptography:** A technology used to generate a key pair that consists of a public key and a private key. The public key is widely distributed, while the private key is only known to the recipient. The two keys in the key pair complement each other, and the data encrypted by one key can only be decrypted by the other key of the key pair.
- **CA:** A trusted entity that issues digital certificates to individuals, computers or any other entities. CA accepts requests for certificates and verifies the information provided by the applicants based on certificate management policy. If the information is legal, CA will sign the certificates with its private key and issue them to the applicants.
- **RA:** The extension to CA. RA forwards requests for a certificate to CA, and also forwards the digital certificate and CRL issued by CA to directory servers in order to provide directory browsing and query services.
- **CRL:** Each certificate is designed with expiration. However, CA might revoke a certificate before the date of expiration due to key leakage, business termination or other reasons. Once a certificate is revoked, CA will issue a CRL to announce the certificate is invalid, and list the series number of the invalid certificate.

PKI is used in the following two situations:

- **IKE VPN:** PKI can be used by IKE VPN tunnel.
- **HTTPS/SSH:** PKI applies to the situation where a user accesses a Hillstone device over HTTPS or SSH.
- **"Sandbox" on Page 376:** Support the verification for the trust certification of PE files.

Creating a PKI Key

1. Select **System > PKI > Key**.
2. Click **New**.



In the PKI Key Configuration dialog, configure the following.

Option	Description
Label	Specifies the name of the PKI key. The name must be unique.
Key configuration mode	Specifies the generation mode of keys, which includes Generate and Import.
Key Pair Type	Specifies the type of key pair, either RSA or DSA.
Key modulus	Specifies the modulus of the key pair. The options are 1024 (the default value), 2048, 512 and 768 bits.

Option	Description
Import Key	Browse your local file system and import the key file.

3. Click **OK**.

Creating a Trust Domain

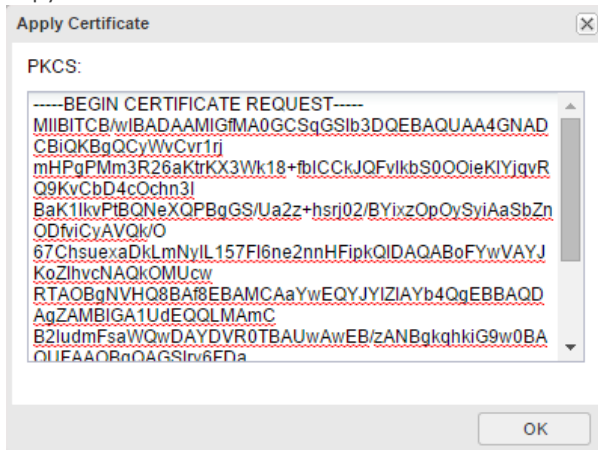
1. Select **System > PKI > Trust Domain**.
2. Click New.

In the **Basic** tab, configure values for basic properties.

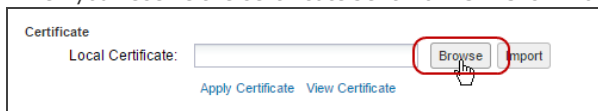
Option	Description
Basic	
Trust Domain	Enter the name of the new trust domain.
Enrollment Type	Use one of the two following methods: <ul style="list-style-type: none"> • Select Manual Input, and click Browse to find the certificate and click Import to import it into system. • Select Self-signed Certificate, and the certificate will be generated by the device itself.
Key Pair	Select a key pair.
Subject	
Name	Enter a name of the subject.
Country (Region)	Enter the name of applicant's country or region. Only an abbreviation of two letters are allowed, like CN.
Location	Optional. The location of the applicant.
State/Province	Optional. State or province name.
Organization	Optional. Organization name.
Organization unit	Optional. Department name within applicant's organization.

3. Click **Apply Certificate**, and a string of code will appear.

- Copy this code and send it to CA via email.



- When you receive the certificate sent from CA. Click Browse to import the certificate.



- (Optional) In the CRL tab, configure the following.

Certification Revocation List	
Check	<ul style="list-style-type: none"> No Check - System does not check CRL. This is the default option. Optional - System accepts certificating from peer, no matter if CRL is available or not. Force - System only accepts certificating from peer when CRL is available.
URL 1-3	<p>The URL address for receiving CRL. At most 3 URLs are allowed, and their priority is from 1 to 3.</p> <ul style="list-style-type: none"> Select http:// if you want to get CRL via HTTP. Select ldap:// if you want to get CRL via LDAP. If you use LDAP to receive CRL, you need to enter the login-DN of LDAP server and password. If no login-DN or password is added, the transmission will be anonymous.
Auto Update	Update frequency of CRL list.
Manual Update	Get the CRL immediately by clicking Obtaining CRL .

- Click **OK**.

Importing/Exporting Trust Domain

To simplify configurations, you can export certificates (CA or local) and private key (in the format of PKSC12) to a computer and import them to another device.

To export a PKI trust domain, take the following steps:

- Select **System > PKI > Trust Domain Certificate**.
- Select a domain from drop-down menu.
- Select the radio button of the item you want to export, and click **Export**.

If you choose PKCS, you need to set up password.

4. Click **OK**, and select a storage path to save the item.

To import the saved trust domain to another device, take the following steps:

1. Log in the other device, select **System > PKI > Trust Domain Certificate**.
2. Select a domain from drop-down menu.
3. Select the radio button of the item you want to import, and click **Import**.
If you choose PKCS, you need to enter the password when it was exported.
4. Click **Browse** and find the file to import.
5. Click **OK**. The domain file is imported.

Importing Trust Certification

System will not detect the PE file whose certification is trusted. To import trust certification of PE files, take the following steps:

1. Select **System > PKI > Credible Root Certificate**.
2. Click **Import** and choose a certificate file in your PC.
3. Click OK and then the file will be imported.

Online Users

To view the online authenticated users, take the following steps:

1. Select **Network > WebAuth > Online Users**.
2. The page will show all online users. You can set up filters to views results that match your conditions.

Authentication Type:		All	+ Filter
		All	
<input type="checkbox"/>	Username	WebAuth(HTTP/H...	
		WebAuth(SMS)	
		WebAuth(NTLM)	

Chapter 8 VPN

System supports the following VPN functions:

- ["IPSec VPN" on Page 153](#): IPSec is a security framework defined by the Internet Engineering Task Force (IETF) for securing IP communications. It is a Layer 3 virtual private network (VPN) technology that transmits data in a secure tunnel established between two endpoints.
- ["SSL VPN" on Page 172](#): SSL provides secure connection services for TCP-based application layer protocols by using data encryption, identity authentication, and integrity authentication mechanisms.
- ["L2TP VPN" on Page 228](#): L2TP is one protocol for VPDN tunneling. VPDN technology uses a tunneling protocol to build secure VPNs for enterprises across public networks. Branch offices and traveling staff can remotely access the headquarters' Intranet resources through a virtual tunnel over public networks.

IPSec VPN

IPSec is a widely used protocol suite for establishing a VPN tunnel. IPSec is not a single protocol, but a suite of protocols for securing IP communications. It includes Authentication Headers (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE) and some authentication methods and encryption algorithms. IPSec protocol defines how to choose the security protocols and algorithms, as well as the method for exchanging security keys among communicating peers, while offering the upper layer protocols with network security services, including access control, data source authentication, data encryption, etc.

Basic Concepts

- Security association
- Encapsulation modes
- Establishing SA
- Using IPSec VPN

Security Association (SA)

IPSec provides encrypted communication between two peers which are known as IPSec ISAKMP gateways. Security Association (SA) is the basis and essence of IPSec. SA defines some factors of communication peers like the protocols, operational modes, encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), shared keys of data protection in particular flows and the life cycle of SA, etc.

SA is used to process data flow in one direction. Therefore, in a bi-directional communication between two peers, you need at least two security associations to protect the data flow in both of the directions.

Encapsulation Modes

IPSec supports the following IP packet encapsulation modes:

- Tunnel mode - IPSec protects the entire IP packet, including both the IP header and the payload. It uses the entire IP packet to calculate an AH or ESP header, and then encapsulates the original IP packet and the AH or ESP header with a new IP header. If you use ESP, an ESP trailer will also be encapsulated. Tunnel mode is typically used for protecting gateway-to-gateway communications.
- Transport mode - IPSec only protects the IP payload. It only uses the IP payload to calculate the AH or ESP header, and inserts the calculated header between the original IP header and payload. If you use ESP, an ESP trailer is also encapsulated. The transport mode is typically used for protecting host-to-host or host-to-gateway communications.

Establishing SA

There are two ways to establish SA: manual and IKE auto negotiation (ISAKMP).

- Manually configuring SA is complicated as all the information will be configured by yourself and some advanced features of IPSec are not supported (e.g. timed refreshing), but the advantage is that manually configured SA can independently fulfill IPSec features without relying on IKE. This method applies to a situation with a small number of devices or an environment of static IP addresses.
- IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic networks. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPSec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

Using IPSec VPN

To apply VPN tunnel feature in the device, you can use policy-based VPN or route-based VPN.

- Policy-based VPN - Applies the configured VPN tunnel to a policy so that the data flow which conforms to the policy settings can pass through the VPN tunnel.
- Route-based VPN - Binds the configured VPN tunnel to the tunnel interface and define the next hop of static route as the tunnel interface.

Configuring an IKE VPN

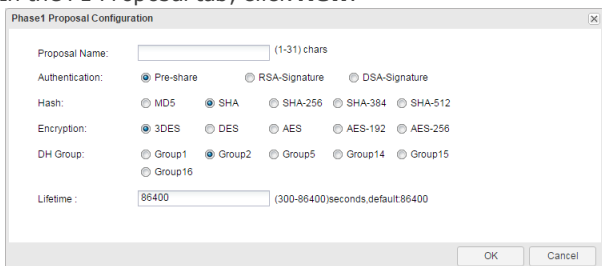
IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic network. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPsec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

To configure an IKE VPN, you need to confirm the Phase 1 proposal, the Phase 2 proposal, and the VPN peer. After confirming these three contents, you can proceed with the configuration of IKE VPN settings.

Configuring a Phase 1 Proposal

The P1 proposal is used to negotiate the IKE SA. To configure a P1 proposal, take the following steps:

1. Select **Network > VPN > IPsec VPN**.
2. In the P1 Proposal tab, click **New**.

The image shows a 'Phase1 Proposal Configuration' dialog box. It has a title bar with a close button. Inside, there are several fields and radio buttons. 'Proposal Name' is a text field with '(1-31) chars' as a hint. 'Authentication' has three radio buttons: 'Pre-share' (selected), 'RSA-Signature', and 'DSA-Signature'. 'Hash' has five radio buttons: 'MD5', 'SHA' (selected), 'SHA-256', 'SHA-384', and 'SHA-512'. 'Encryption' has five radio buttons: '3DES' (selected), 'DES', 'AES', 'AES-192', and 'AES-256'. 'DH Group' has six radio buttons: 'Group1', 'Group2' (selected), 'Group5', 'Group14', and 'Group15'. 'Lifetime' is a text field with '86400' and '(300-86400)seconds,default:86400' as a hint. At the bottom right are 'OK' and 'Cancel' buttons.

In the Phase1 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Proposal Name	Specifies the name of the Phase1 proposal.
Authentication	Specifies the IKE identity authentication method. IKE identity authentication is used to verify the identities of both communication parties. There are three methods for authenticating identity: pre-shared key, RSA signature and DSA signature. The default value is pre-shared key. For pre-shared key method, the key is used to generate a secret key and the keys of both parties must be the same so that it can generate the same secret keys.
Hash	Specifies the authentication algorithm for Phase1. Select the algorithm you want to use. <ul style="list-style-type: none">• MD5 – Uses MD5 as the authentication algorithm. Its hash value is 128-bit.• SHA – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm.• SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit.• SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit.• SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
Encryption	Specifies the encryption algorithm for Phase1. <ul style="list-style-type: none">• 3DES - Uses 3DES as the encryption algorithm. The key length is

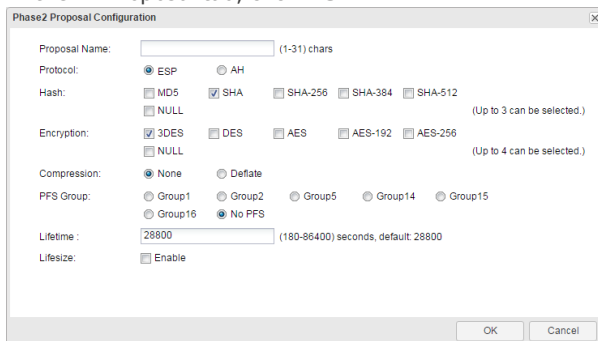
Option	Description
	<p>192-bit. This is the default encryption algorithm.</p> <ul style="list-style-type: none"> • DES – Uses DES as the encryption algorithm. The key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit.
DH Group	<p>Specifies the DH group for Phase1 proposal.</p> <ul style="list-style-type: none"> • Group1 – Uses Group1 as the DH group. The key length is 768-bit. • Group2 – Uses Group2 as the DH group. The key length is 1024-bit. Group2 is the default value. • Group5 – Uses Group5 as the DH group. The key length is 1536-bit. • Group14 – Uses Group14 as the DH group. The key length is 2048-bit. • Group15 – Uses Group5 as the DH group. The key length is 3072-bit. • Group16 – Uses Group5 as the DH group. The key length is 4096-bit.
Lifetime	<p>Specifies the lifetime of SA Phase1. The value range is 300 to 86400 seconds. The default value is 86400. Type the lifetime value into the Lifetime box. When the SA lifetime runs out, the device will send a SA P1 deleting message to its peer, notifying that the P1 SA has expired and it requires a new SA negotiation.</p>

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

Configuring a Phase 2 Proposal

The P2 proposal is used to negotiate the IPsec SA. To configure a P2 proposal, take the following steps:

1. Select **Network > VPN > IPsec VPN**.
2. In the P2 Proposal tab, click **New**.



The image shows the 'Phase2 Proposal Configuration' dialog box. It contains the following fields and options:

- Proposal Name:** A text box with a placeholder '(1-31) chars'.
- Protocol:** Radio buttons for ESP (selected) and AH.
- Hash:** Checkboxes for MD5, SHA (selected), SHA-256, SHA-384, and SHA-512. A note says '(Up to 3 can be selected.)'.
- Encryption:** Checkboxes for 3DES (selected), DES, AES, AES-192, and AES-256. A note says '(Up to 4 can be selected.)'.
- Compression:** Radio buttons for None (selected) and Deflate.
- PFS Group:** Radio buttons for Group1, Group2, Group5, Group14, Group15, and No PFS (selected).
- Lifetime:** A text box with '28800' and a note '(180-86400) seconds, default: 28800'.
- Lifesize:** A checkbox labeled 'Enable'.

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

In the Phase2 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Proposal Name	Specifies the name of the Phase2 proposal.
Protocol	Specifies the protocol type for Phase2. The options are ESP and AH. The default value is ESP.
Hash	<p>Specifies the authentication algorithm for Phase2. Select the algorithm you want to use.</p> <ul style="list-style-type: none"> • MD5 – Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit. • Null – No authentication.
Encryption	<p>Specifies the encryption algorithm for Phase2.</p> <ul style="list-style-type: none"> • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm. The key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit. • Null – No authentication.
Compression	Specifies the compression algorithm for Phase2. By default, no compression algorithm is used.
PFS Group	<p>Specifies the PFS function for Phase2. PFS is used to protect DH algorithm.</p> <ul style="list-style-type: none"> • No PFS - Disables PFS. This is the default value. • Group1 – Uses Group1 as the DH group. The key length is 768-bit. • Group2 – Uses Group2 as the DH group. The key length is 1024-bit. Group2 is the default value. • Group5 – Uses Group5 as the DH group. The key length is 1536-bit. • Group14 – Uses Group14 as the DH group. The key length is 2048-bit.

Option	Description
	<ul style="list-style-type: none"> Group15 – Uses Group5 as the DH group. The key length is 3072-bit. Group16 – Uses Group5 as the DH group. The key length is 4096-bit.
Lifetime	You can evaluate the lifetime by two standards which are the time length and the traffic volume. Type the lifetime length of P2 proposal into the box. The value range is 180 to 86400 seconds. The default value is 28800.
Lifeseize	Select Enable to enable the P2 proposal traffic-based lifetime. By default, this function is disabled. After selecting Enable, specifies the traffic volume of lifetime. The value range is 1800 to 4194303 KBs. The default value is 1800. Type the traffic volume value into the box.

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

Configuring a VPN Peer

To configure a VPN peer, take the following steps:

1. Select **Network > VPN > IPsec VPN**.
2. In the VPN Peer List tab, click **New**.

In the VPN Peer Configuration dialog box, configure the corresponding options.

Basic	
Name	Specifies the name of the ISAKMP gateway.
Interface	Specifies interface bound to the ISAKMP gateway.
Interface Type	Select the interface type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type interface.
Mode	Specifies the mode of IKE negotiation. There are two IKE negotiation modes: Main and Aggressive . The main mode is the default mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in the situation where the IP address of the center device is static and the IP address of client device is dynamic.
Type	Specifies the type of the peer IP. If the peer IP is static, type the IP address into the Peer IP box; if the peer IP type is user group, select the AAA server you need from the AAA Server drop-down list.
Local ID	Specifies the local ID. System supports five types of ID: FQDN, U-FQDN, Asn1dn (only for license), KEY-ID and IP. Select the ID type you want, and then type the content for this ID into the Local ID box or the Local IP box.
Peer ID	Specifies the peer ID. System supports five types of ID: FQDN, U-FQDN,

Basic	
	Asn1dn (only for license), KEY-ID and IP. Select the ID type you want, and then type the content for this ID into the Peer ID box or the Peer IP box.
Proposal1/2/3/4	Specifies a P1 proposal for ISAKMP gateway. Select the suitable P1 proposal from the Proposal1 drop-down list. You can define up to four P1 proposals for an ISAKMP gateway
Pre-shared Key	If you choose to use pre-shared key to authenticate, type the key into the box.
Trust Domain	If you choose to use RSA signature or DSA signature, select a trust domain.
User Key	Click Generate . In the Generate the User Key dialog box, type the IKE ID into the IKE ID box, and then click Generate . The generated user key will be displayed in the Generate Result box. PnPVPN client uses this key as the password to authenticate the login users.

3. If necessary, click the **Advanced** tab to configure some advanced options.

In the Advanced tab, configure the corresponding options.

Advanced	
Connection Type	Specifies the connection type for ISAKMP gateway. <ul style="list-style-type: none"> • Bidirection - Specifies that the ISAKMP gateway serves as both the initiator and responder. This is the default value. • Initiator - Specifies that the ISAKMP gateway serves as the only initiator. • Responder - Specifies that the ISAKMP gateway serves as the only responder.
NAT Traversal	This option must be enabled when there is a NAT device in the IPSec or IKE tunnel and the device implements NAT. By default, this function is disabled.
Any Peer ID	Makes the ISAKMP gateway accept any peer ID and not check the peer IDs.
Generate Route	Select the Enable check box to enable the auto routing function. By default, this function is disabled. This function allows the device to automatically add routing entries which are from the center device to the branch, avoiding the problems caused by manual configured routing.
DPD	Select the Enable check box to enable the DPD (Delegated Path Discovery) function. By default, this function is disabled. When the responder does not receive the peer's packets for a long period, it can enable DPD and initiate a DPD request to the peer so that it can test if the ISAKMP gateway exists. <ul style="list-style-type: none"> • DPD Interval - The interval of sending DPD request to the peer. The value range is 1 to 10 seconds. The default value is 10 seconds. • DPS Retries - The times of sending DPD request to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD retries. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 10 times. The default value is 3.
Description	Type the description for the ISAKMP gateway.
XAUTH	Select Enable to enable the XAUTH server in the device. Then select an

Advanced	
	address pool from the drop-down list. After enabling the XAUTH server, the device can verify the users that try to access the IPsec VPN network by integrating the configured AAA server.

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

Configuring an IKE VPN

Use IKE to negotiate IPsec SA automatically. To configure IKE VPN, take the following steps:

1. Select **Network > VPN > IPsec VPN**.
2. In the IKE VPN List tab, click **New**.

In the Basic tab, configure the corresponding options.

Peer	
Peer Name	Specifies the name of the ISAKMP gateway. To edit an ISAKMP gateway, click Edit .
Information	Shows the information of the selected peer.
Tunnel	
Name	Type a name for the tunnel.
Mode	Specifies the mode, including tunnel mode and transport mode.
P2 Proposal	Specifies the P2 proposal for tunnel.
Proxy ID	Specifies ID of Phase 2 for the tunnel which can be Auto or Manual. <ul style="list-style-type: none"> • Auto - The Phase 2 ID is automatically designated. • Manual - The Phase 2 ID is manually designated. Manual configuration of P2 ID includes the following options: <ul style="list-style-type: none"> • Local IP/Netmask - Specifies the local ID of Phase 2. • Remote IP/Netmask - Specifies the Phase 2 ID of the peer device. • Service - Specifies the service.

3. If necessary, click the **Advanced** tab to configure some advanced options.

In the Advanced tab, configure the corresponding options.

Advanced	
DNS1/2	Specifies the IP address of the DNS server allocated to the client by the PnPVPN server. You can define one primary DNS server and a backup DNS server.
WINS1/2	Specifies the IP address of WINS server allocated to the client by the PnPVPN server. You can define one primary WINS server and a backup WINS server.
Enable Idle Time	Select the Enable check box to enable the idle time function. By default, this function is disabled. This time length is the longest time the tunnel can exist without traffic passing through. When the time is over, SA will be cleared.
DF-Bit	<p>Select the check box to allow the forwarding device to execute IP packet fragmentation. The options are:</p> <ul style="list-style-type: none"> • Copy - Copies the IP packet DF options from the sender directly. This is the default value. • Clear - Allows the device to execute packet fragmentation. • Set - Disallows the device to execute packet fragmentation.
Anti-Replay	<p>Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled.</p> <ul style="list-style-type: none"> • Disabled - Disables this function. • 32 - Specifies the anti-replay window as 32. • 64 - Specifies the anti-replay window as 64. • 128 - Specifies the anti-replay window as 128. • 256 - Specifies the anti-replay window as 256. • 512 - Specifies the anti-replay window as 512.
Commit Bit	Select the Enable check box to make the corresponding party configure the commit bit function, which can avoid packet loss and time difference. However, commit bit may slow the responding speed.
Accept-all-proxy-ID	This function is disabled by default. With this function enabled, the device which is working as the initiator will use the peer's ID as its Phase 2 ID in the IKE negotiation, and return the ID to its peer.
Auto Connect	<p>Select the Enable check box to enable the auto connection function. By default, this function is disabled. The device has two methods of establishing SA: auto and intrigued traffic mode. When it is auto mode, the device will check SA status every 60 seconds and initiate negotiation request when SA is not established; when it is in intrigued traffic mode, the tunnel will send negotiation request only when there is traffic passing through the tunnel. By default, the intrigued traffic mode is enabled.</p> <p>Note: Auto connection works only when the peer IP is static and the local device is the initiator.</p>
Tunnel Route	This item can be modified only after this IKE VPN is created. Click Choose to add one or more tunnel routes in the appearing Tunnel Route Configuration dialog box. You can add up to 128 tunnel routes.

Advanced	
Description	Type the description for the tunnel.
VPN Track	<p>Select the Enable check box to enable the VPN track function. The device can monitor the connectivity status of the specified VPN tunnel, and also allows backup or load sharing between two or more VPN tunnels. This function is applicable to both route-based and policy-based VPNs. The options are:</p> <ul style="list-style-type: none"> • Track Interval - Specifies the interval of sending Ping packets. The unit is second. • Threshold - Specifies the threshold for determining the track failure. If system did not receive the specified number of continuous response packets, it will identify a track as failure, i.e., the target tunnel is disconnected. • Src Address - Specifies the source IP address that sends Ping packets. • Dst Address - Specifies the IP address of the tracked object. • Notify Track Event - Select the Enable check box to enable the VPN tunnel status notification function. With this function enabled, for route-based VPN, system will inform the routing module about the information of the disconnected VPN tunnel and update the tunnel route once any VPN tunnel disconnection is detected; for policy-based VPN, system will inform the policy module about the information of the disconnected VPN tunnel and update the tunnel policy once any VPN tunnel disconnection is detected.

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

Configuring a Manual Key VPN

Manually configuring SA is complicated as all the information will be configured by yourself and some advanced features of IPSec are not supported (e.g. timed refreshing), but the advantage is that manually configured SA can independently fulfill IPSec features without relying on IKE. This method applies to a situation with a small number of devices or an environment of static IP addresses.

To create a manual key VPN, take the following steps:

- 1. Select **Network > VPN > IPSec VPN**.
- 2. In the Manual Key VPN Configuration section, click **New**.

Manual Key VPN Configuration

Basic

Tunnel Name:

(1-31) chars

Mode:

Tunnel

Transport

Peer IP:

Local SPI:

(Hex, 1-FFFF)

Remote SPI:

(Hex, 1-FFFFFFF)

Interface:

cellular0/0

Encryption

Protocol:

ESP

AH

Encryption:

None

3DES

AES

AES-192

AES-256

DES

Inbound Encryption Key:

(2-64, hex number)

Outbound Encryption Key:

(2-64, hex number)

Hash:

None

MD5

SHA-1

SHA-256

SHA-384

SHA-512

Inbound Hash Key:

(2-128, hex number)

Outbound Hash Key:

(2-128, hex number)

Compression:

None

Deflate

Description

Description:

(0-255) chars

OK

Cancel

In the Manual Key VPN Configuration dialog box, configure the corresponding options.

Basic	
Tunnel Name	Specifies the name of manually created key VPN.
Mode	Specifies the mode, including Tunnel and Transport. The tunnel mode is the default mode.
Peer IP	Specifies the IP address of the peer.
Local SPI	Type the local SPI value. SPI is a 32-bit value transmitted in AH and ESP header, which uniquely identifies a security association. SPI is used to seek corresponding VPN tunnel for decryption.
Remote SPI	Type the remote SPI value. Note: When configuring an SA, you should configure the parameters of both the inbound and outbound direction. Furthermore, SA parameters of the two ends of the tunnel should be totally matched. The local inbound SPI should be the same with the outbound SPI of the other end; the local outbound SPI should be the same with the inbound SPI of the other end.
Interface	Specifies the egress interface for the manual key VPN. Select the interface you want from the Interface drop-down list.
Interface Type	Select the interface type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type interface.

Basic	
Encryption	
Protocol	Specifies the protocol type. The options are ESP and AH. The default value is ESP.
Encryption	<p>Specifies the encryption algorithm.</p> <ul style="list-style-type: none"> • None – No authentication. • 3DES – Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm. The key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit.
Inbound Encryption Key	Type the encryption key of the inbound direction. You should configure the keys of both ends of the tunnel. The local inbound encryption key should be the same with the peer's outbound encryption key, and the local outbound encryption key should be the same with the peer's inbound encryption key.
Outbound Encryption Key	Type the encryption key of the outbound direction.
Hash	<p>Specifies the authentication algorithm. Select the algorithm you want to use.</p> <ul style="list-style-type: none"> • None – No authentication. • MD5 – Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA-1 – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
Inbound Hash Key	Type the hash key of the inbound direction. You should configure the keys of both ends of the tunnel. The local inbound hash key should be the same with the peer's outbound hash key, and the local outbound hash key should be the same with the peer's inbound hash key.
Outbound Hash Key	Type the hash key of the outbound direction.
Compression	Select a compression algorithm. By default, no compression algorithm is used.

Basic	
Description	
Description	Type the description for the manual key VPN.

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

Viewing IPsec VPN Monitoring Information

By using the ISAKMP SA table, IPsec SA table, and Dial-up User table, IPsec VPN monitoring function can show the SA negotiation results of IPsec VPN Phase1 and Phase2 as well as information of dial-up users.

To view the VPN monitoring information, take the following steps:

1. Select **Network > VPN > IPsec VPN**.
2. In the IKE VPN Configuration section, click **IPsec VPN Monitor**.

Options in these tabs are described as follows:

ISAKMP SA

Option	Description
Cookie	Displays the negotiation cookies which are used to match SA Phase 1.
Status	Displays the status of SA Phase1.
Peer	Displays the IP address of the peer.
Port	The port number used by the SA Phase1. 500 indicates that no NAT has been found during the SA Phase 1; 4500 indicates that NAT has been detected.
Algorithm	Displays the algorithm of the SA Phase1, including authentication method, encryption algorithm and verification algorithm.
Lifetime	Displays the lifetime of SA Phase1. The unit is second.

IPsec SA

Option	Description
ID	Displays the tunnel ID number which is auto assigned by the system.
VPN Name	Displays the name of VPN.
Direction	Displays the direction of VPN.
Peer	Displays the IP address of the peer.
Port	The port number used by the SA Phase2.
Algorithm	The algorithm used by the tunnel, including protocol type, encryption algorithm, verification algorithm and decryption algorithm.
SPI	Displays the local SPI and the peer SPI. The direction of inbound is local SPI, while outbound is peer SPI.
CPI	Displays the compression parameter index (CPI) used by SA Phase2.
Lifetime (s)	Displays the lifetime of SA Phase2 in seconds, i.e. SA Phase2 will restart negotiations after X seconds.
Lifetime (KB)	Displays the lifetime of SA Phase2 in KB, i.e. SA Phase2 will restart negotiations after X kilobytes of data flow.
Status	Displays the status of SA Phase2.

Dial-up User

Option	Description
Peer	Displays the statistical information of the peer user. Select the peer you want from the Peer drop-down list.
User ID	Displays the IKE ID of the user selected.
IP	Displays the corresponding IP address.
Encrypted Packets	Displays the number of encrypted packets transferred through the tunnel.

Option	Description
Encrypted Bytes	Displays the number of encrypted bytes transferred through the tunnel.
Decrypted Packets	Displays the number of decrypted packets transferred through the tunnel.
Decrypted Bytes	Displays the number of decrypted bytes transferred through the tunnel.

Configuring PnPVPN

IPSec VPN requires sophisticated operational skills and high maintenance cost. To relieve network administrators from the intricate work, system provides an easy-to-use VPN technology - PnPVPN (Plug-and-Play VPN). PnPVPN consists of two parts: PnPVPN Server and PnPVPN Client.

- PnPVPN Server: Normally deployed in the headquarters and maintained by an IT engineer, the PnPVPN Server sends most of the configuration commands to the clients. The device usually works as a PnPVPN Server and one device can serve as multiple servers.
- PnPVPN Client: Normally deployed in the branch offices and controlled remotely by a headquarters engineer, the PnPVPN Client can obtain configuration commands (e.g. DNS, WINS, DHCP address pool, etc.) from the PnPVPN Server with simple configurations, such as client ID, password, and server IP settings.

The device can serve as both a PnPVPN Server and a PnPVPN Client. When working as a PnPVPN Server, the maximum number of VPN instance and the supported client number of each device may vary according to the platform series.

PnPVPN Workflow

The workflow for PnPVPN is as follows:

1. The client initiates a connection request and sends his/her own ID and password to the server.
2. The server verifies the ID and password when it receives the request. If the verification succeeds, the server will send the configuration information, including DHCP address pool, DHCP mask, DHCP gateway, WINS, DNS and tunnel routes, etc., to the client.
3. The client distributes the received information to corresponding functional modules.
4. The client PC automatically gains an IP address, IP mask, gateway address and other network parameters and connects itself to the VPN.

PnPVPN Link Redundancy

The PnPVPN server supports dual VPN link dials for a PnPVPN client, and automatically generates the routing to the client. Also, it can configure the VPN monitor for the client. Two ISAKMP gateways and two tunnel interfaces need to be configured in the server. The two VPN tunnels need to refer different ISAKMP gateways and be bound to different tunnel interfaces.

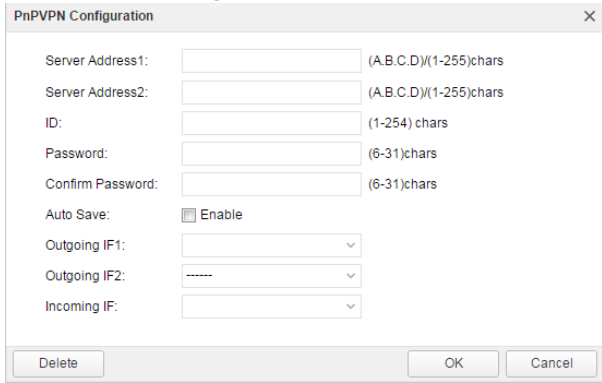
The client supports to configure dual VPN dials and redundant routing. When the two VPN tunnels are negotiating with the server, the client generates routes with different priority according to the tunnel routing configuration at the server side. The high priority tunnel acts as the master link and the tunnel with low priority as the backup link, so as to realize redundant routing. The master VPN tunnel will be in the active state first. When master tunnel is interrupted, the client will use the backup tunnel to transfer the data. When the master tunnel restores to be normal, it will transfer the data again.

Configuring a PnPVPN Client

To configure a PnPVPN client, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. In the IKE VPN Configuration section, click **PnPVPN Client**.

The image shows a 'PnPVPN Configuration' dialog box with a close button (X) in the top right corner. It contains several input fields and a checkbox. The fields are: 'Server Address1:' with a text box and '(A.B.C.D)/(1-255)chars' hint; 'Server Address2:' with a text box and '(A.B.C.D)/(1-255)chars' hint; 'ID:' with a text box and '(1-254) chars' hint; 'Password:' with a text box and '(6-31)chars' hint; 'Confirm Password:' with a text box and '(6-31)chars' hint; 'Auto Save:' with a checked checkbox and 'Enable' text; 'Outgoing IF1:' with a dropdown menu; 'Outgoing IF2:' with a dropdown menu showing '-----'; and 'Incoming IF:' with a dropdown menu. At the bottom are three buttons: 'Delete', 'OK', and 'Cancel'.

In the PnPVPN Configuration dialog box, configure the following options.

Option	Description
Server Address1	Type the IP address of PnPVPN Server into the box. PnPVPN client supports dual link dials to the server side. This option is required.
Server Address2	Type the IP address of PnPVPN Server into the box. The server address 1 and the server address 2 can be the same or different. It is optional.
ID	Specifies the IKE ID assigned to the client by the server.
Password	Specifies the password assigned to the client by the server.
Confirm Password	Enter the password again to confirm.
Auto Save	Select Enable to auto save the DHCP and WINS information released by the PnPVPN Server.
Outgoing IF1	Specifies the interface connecting to the Internet. This option is required.
Outgoing IF2	Specifies the interface connecting to the Internet. The IF1 and the IF2 can be the same or different. It is optional.
Incoming IF	Specifies the interface on the PnPVPN Client accessed by the Intranet PC or the application servers.

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



Note:

- Server Addresses1 and Outgoing IF1 both need to be configured. If you want to configure a backup link, you need to configure both the Server Address2 and Outgoing IF2.
- If the server addresses or the Outgoing IFs are different, two separate VPN links will be generated.
- The configuration of the two servers can be configured on one device, and can also be configured on two different devices. If you configure it on two devices, you need to configure AAA user on the two devices. The DHCP configuration for the AAA user should be the same, otherwise it might cause that the client and server negotiate successfully, but the traffic is blocked.

Configuring IPSec-XAUTH Address Pool

XAUTH server assigns the IP addresses in the address pool to users. After the client has established a connection to the XAUTH server successfully, the XAUTH server will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and will assign them to the client.

XAUTH server provides fixed IP addresses by creating and implementing IP binding rules that consist of a static IP binding rule and an IP-role binding rule. The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, system will assign the binding IP to the client. The IP-role binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, system will assign an IP address within the IP range to the client.

When the XAUTH server is allocating IP addresses in the address pool, system will check the IP binding rule and determine how to assign IP addresses to the client based on the specific checking order below:

1. Check if the client is configured with any static IP binding rule. If so, assign the binding IP address to the client; otherwise, check the other configuration. Note if the binding IP address is in use, the user will be unable to log in.
2. Check if the client is configured with any IP-role binding rule. If so, assign an IP address within the binding IP range to the client; otherwise, the user will be unable to log in.



Note: The IP addresses defined in the static IP binding rule and IP-role binding rule should not be overlapped.

To configure the IPSec-XAUTH address pool, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. At the top-right corner, Select **IPSec-XAUTH Address Pool**.
3. In the XAUTH Address Pool Configuration dialog box, click **New**.

In the Basic tab, configure the corresponding options.

Option	Description
Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved Start IP	Specifies the reserved start IP of the address pool.
Reserved End IP	Specifies the reserved end IP of the address pool.
Netmask	Specifies the netmask of the IP address.
DNS1/2	Specifies the DNS server IP address for the address pool. It is optional. At most two DNS servers can be configured for one address pool.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to two WIN servers can be configured for one address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the User box.
IP	Type the IP address into the IP box.
Add	Click Add to add the item that binds the specified user to the IP address.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Select a role from the Role drop-down list.
Start IP	Type the start IP address into the Start IP box.
End IP	Type the end IP address into the End IP box.
Add	Click Add to add the item that binds the specified role to the IP address range.
Up/Down/Top/Bottom	Move the selected IP-role binding rule . For the user that is bound to multiple roles that are also configured with their corresponding IP-role binding rules, system will query the IP-role binding rules in order, and assign an IP address based on the first matched rule.

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

SSL VPN

The device provides an SSL based remote access solution. Remote users can access the intranet resource safely through the provided SSL VPN.

SSL VPN consists of two parts: SSL VPN server and SSL VPN client. The device configured as the SSL VPN server provides the following functions:

- Accept client connections.
- Allocate IP addresses, DNS server addresses, and WIN server addresses to SSL VPN clients.
- Authenticate and authorize clients.
- Perform host checking to client.
- Encrypt and forward IPsec data.

By default, the concurrent online client number may vary on different platform series. You can expand the supported number by purchasing the corresponding license.

After successfully connecting to the SSL VPN server, the SSL VPN client secures your communication with the server. The following SSL VPN clients are available:

- "SSL VPN Client for Windows" on Page 190
- "SSL VPN Client for Android" on Page 208
- "SSL VPN Client for iOS" on Page 212
- "SSL VPN Client for Mac OS" on Page 217
- "SSL VPN Client for Linux" on Page 220

Configuring an SSL VPN

To configure an SSL VPN, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. In the SSL VPN page, click **New**.

SSL VPN Configuration

Name/Access User Interface Tunnel Route Binding Resource

Welcome to the SSL VPN Configuration Wizard

Secure Connect VPN(SSL VPN) is a simple and easy-to-use remote connection method integrated on the Security device. It is based on the SSL login technique and provides a secure visit to private networks

SSL VPN Name: (1-31)chars

Assigned Users

Select the AAA server for user authentication.

AAA Server: [View AAA Server](#)

Domain: (1-31) chars

Verify User Domain Name: ☒ Enable

AAA Server	Domain	Verify User Domain Name
------------	--------	-------------------------

In the Name/Access User tab, configure the corresponding options.

Option	Description
SSL VPN Name	Type the name of the SSL VPN instance

Option	Description
Assigned Users	
AAA Server	Select an AAA server from the AAA Server drop-down list. You can click View AAA Server to view the detailed information of this AAA server.
Domain	Type the domain name into the Domain box. The domain name is used to distinguish the AAA server.
Verify User Domain Name	After enabling this function, system will verify the username and its domain name.
Add	Click Add to add the assigned users. You can repeat to add more items.

In the Interface tab, configure the corresponding options.

Access Interface	
Egress Interface1	Select the interface from the drop-down list as the SSL VPN server interface. This interface is used to listen to the request from the SSL VPN client.
Egress Interface2	Select the interface from the drop-down list. This interface is needed when the optimal path detection function is enabled.
Service Port	Specifies the SSL VPN service port number.
Tunnel Interface	
Tunnel Interface	Specifies the tunnel interface used to bind to the SSL VPN tunnel. Tunnel interface transmits traffic to/from SSL VPN tunnel. <ul style="list-style-type: none"> Select a tunnel interface from the drop-down list, and then click Edit to edit the selected tunnel interface. Click New in the drop-down list to create a new interface.
Information	Shows the zone, IP address, and netmask of the selected tunnel interface.
Address Pool	
Address Pool	Specifies the SSL VPN address pool. <ul style="list-style-type: none"> Select an address pool from the drop-down list, and then click Edit to edit the selected address pool. Click New in the drop-down list to create a new address pool.
Information	Shows the start IP address, end IP address, and mask of the address pool.


In the Tunnel Route tab, configure the following options.

Tunnel Route	
Specify the destination network segment that you want to access through SCVPN tunnel. The specified destination network segment will be distributed to the VPN client, then the client uses it to generate the route to the specified destination.	
IP	Type the destination IP address.
Mask	Type the netmask of the destination IP address.
Metric	Type the metric value.
Add	Click Add to add this route. You can repeat to add more items.
Delete	Click Delete to delete the selected route.
Enable domain name	
Specify the destination domain name that you want to access through SCVPN tunnel.	

After selecting the **Enable domain name** check box, system will distribute the specified domain names to the VPN client, and the client will generate the route to the specified destination according to the resolving results from the DNS.

Domain	Specify the URL of the domain name. The URL cannot exceed 63 characters and it cannot end with a dot (.). Both wildcards and a single top level domain, e.g. .com and .com are not supported.
Add	Click Add to add the domain name to the list and you can add up to 64 domain names.
Delete	Click Delete to delete the selected domain name.
Domain route max entries	The maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The value ranges from 1 to 10000.

In the Binding Resource tab, configure the binding relationship between user groups and resources.

Binding Resource	
Resource List	Types or selects an existing resource name.
User	<p>Specifies a user group name.</p> <ol style="list-style-type: none"> 1. From the User drop-down menu, select the AAA servers where user groups reside. Currently, only the local authentication server and the RADIUS server are available. 2. Based on different types of AAA server, you can execute one or more actions: search a user group, expand the user group list, and enter the name of the user group. 3. After selecting user groups, click  to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog to complete the configuration. <p>Note:</p> <ul style="list-style-type: none"> • A user group can be bound with multiple resources, and a resource can also be bound with multiple user groups. • Only 32 binding entries can be configured in an SSL VPN instance.
Add	Click Add to add binding entries for resources and user groups to the list below. You can repeat to add more items.
Delete	Click Delete to delete the selected item.

3. If necessary, click **Advanced** to configure the advanced functions, including parameters, client, host security, SMS authentication, and optimized path.

In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	<p>Specifies the SSL protocol version. Any indicates one of SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2 or GMSSLv1.0 protocol will be used.</p> <p>If tlsv1.2 or any is specified to the SSL protocol in SSL VPN server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the tlsv1.2 protocol before the digital certificate authentication via SSL VPN client, so that the SSL VPN server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system</p>

	<p>which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows:</p> <ol style="list-style-type: none"> 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. openssl pkcs12 -in oldcert.pfx -out cert.pem 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports tls1.2 protocol. openssl pkcs12 -export -in cert.pem -out newcert.pfx -CSP "Microsoft Enhanced RSA and AES Cryptographic Provider" 3. Import the newly generated .pfx format certificate into your browser or USB Key. <p>After the above operation, you have to log into SSL VPN server with SSL VPN client whose version is 1.4.6.1239 or later.</p>
Trust Domain	Specifies the trust domain. When the GMSSLv1.0 protocol is used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must config this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Encryption	Specifies the encryption algorithm of the SSL VPN tunnel. The default value is 3DES. NULL indicates no encryption. When using the GMSSLv1.0 protocol, you're recommended to select SM4 for the encryption algorithm.
Hash	Specifies the hash algorithm of the SSL VPN tunnel. The default value is SHA-1. NULL indicates no hash. When using the GMSSLv1.0 protocol, you're recommended to select SM3 for the hash algorithm.
Compression	Specifies the compression algorithm of the SSL VPN tunnel. By default, no compression algorithm is used.
Client Connection	
Idle Time	Specifies the time that a client stays online without any traffic with the server. After waiting for the idle time, the server will disconnect from the client. The value range is 15 to 1500 minutes. The default value is 30.
Multiple Login	This function permits one client to sign in more than one place simultaneously. Select the Enable check box to enable the function.
Multiple Login Times	Type the login time into the Multiple Login Times box. The value range is 0 to 99,999,999. The value of 0 indicates no login time limitation.
Advanced Parameters	
Anti-Replay	The anti-replay function is used to prevent replay attacks. The default value is 32.
DF-Bit	<p>Specifies whether to permit packet fragmentation on the device forwarding the packets. The actions include:</p> <ul style="list-style-type: none"> • Set - Permits packet fragmentation. • Copy - Copies the DF value from the destination of the packet. It is the default value. • Clear - Forbids packet fragmentation.

Port (UDP)	Specifies the UDP port number for the SSL VPN connection.
------------	---

In the Client tab, configure the corresponding options.

Client Configuration	
Redirect URL	<p>This function redirects the client to the specified redirected URL after a successful authentication. Type the redirected URL into the box. The value range is 1 to 255 characters. HTTP (http://) and HTTPS (https://) URLs are supported. Based on the type of the URL, the corresponding fixed format of URL is required. Take the HTTP type as the example:</p> <ul style="list-style-type: none"> For the UTF-8 encoding page - The format is URL+user-name=\$USER&password=\$PWD, e.g., http://www.-abc.com/oa/login.do?username=\$USER&password=\$PWD For the GB2312 page - The format is URL+user-name=\$GBUSER&password=\$PWD, e.g., http://www.-abc.com/oa/login.do?username=\$GBUSER&password=\$PWD Other pages: - Type the URL directly, e.g., http://www.abc.com
Title	Specifies the description for the redirect URL. The value range is 1 to 31 bytes. This title will appear as a client menu item.
Delete privacy data after disconnection	Select Enable to delete the corresponding privacy data after the client's disconnection.
Digital Certificate Authentication	
Authentication	<p>Select the Enable check box to enable this function. There are two options available:</p> <ul style="list-style-type: none"> Username/Password + Digital Certificate - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate, and also type the correct username and password. The USB Key certificate users also need to type the USB Key password. Digital Certificate only - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate. The USB Key certificater users also need to type the USB Key password. No username or user's password is required. <p>When Digital Certificate only is selected:</p> <ul style="list-style-type: none"> System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see "Role" on Page 264. System does not allow the local user to change the password. System does not support SMS authentication. The client will not re-connect automatically if the USB Key is removed.
Download URL	When USB Key authentication is enabled, you can download the UKey driver from this URL.
Trust Domain Sub-	To configure the trust domain and the subject & username checking function:

ject&Username Checking CN Matching OU Matching	<ol style="list-style-type: none"> 1. From the Trust domain drop-down list, select the PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed. 2. If necessary, select the Subject&Username Checking check box to enable the subject & username check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check whether the subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the CN Match box and the OU box to determine whether matches them. 3. Click Add. The configured settings will be displayed in the list below. To delete an item, select the item you want to delete from the list, and then click Delete.
---	--

In the SMS Authentication tab, configure the corresponding options.

SMS Authentication	
SMS Authentication	<p>Select the Enable check box to enable the function.</p> <ul style="list-style-type: none"> • Specify the lifetime of the SMS authentication code. Type the lifetime value into the Lifetime of SMS Auth Code box.
SMS Test	To check whether the device works normally, specify a mobile phone number in the box and then click Send .

In the Host Checking/Binding tab, configure the corresponding options.

Host Checking	
Creates a host checking rule to perform the host checking function. Before creating a host checking rule, you must first configure the host checking profile in " Configuring a Host Checking Profile " on Page 187.	
Role	Specifies the role to which the host checking rule will be applied. Select the role from the Role drop-down list. Default indicates the rule will take effect to all the roles.
Host Checking Name	Specifies the host checking profile. Select the profile from the Host Checking Name drop-down list.
Guest Role	Select the guest role from the Guest Role drop-down list. The user will get the access permission of the guest role when the host checking fails. If Null is selected, system will disconnect the connection when the host checking fails.
Periodic Checking	Specify the checking period. System will check the status of the host automatically according to the host checking profile in each period.
Add	Click Add . The configured settings will be displayed in the table below.
Delete	To delete an item, select the item you want to delete from the list, and then click Delete .
Host Binding	
Enable Host Binding	<p>Select the Enable Host Binding check box to enable the function. By default, one user can only log in one host. You can change the login status by configuring the following options.</p> <ul style="list-style-type: none"> • Allow one user to login through multiple hosts. • Allow multiple users to login on one host.

	<ul style="list-style-type: none"> Automatically add the user-host ID entry into the binding list at the first login. <p>Note: To use the host binding function, you still have to configure it in the host binding configuration page. For more information about host binding, see "Host Binding" on Page 183.</p>
--	--

In the Optimized Path tab, configure the corresponding options.

Option	Description
Optimal path detection can automatically detect which ISP service is better, giving remote users a better user experience.	
No Check	Do not detect.
Client	The client selects the optimal path automatically by sending UDP probe packets.
The device	<p>When the client connects to the server directly without any NAT device, this is the detection process:</p> <ol style="list-style-type: none"> The server recognizes the ISP type of the client according to the client's source address. The server sends all of the sorted IP addresses of the egress interfaces to the client. The client selects the optimal path. <p>When the client connects to the server through a NAT device, this is the detection process:</p> <ol style="list-style-type: none"> The server recognizes the ISP type of the client according to the client's source address. The server sends all of the sorted NAT IP addresses of the external interfaces to the client. The client selects the optimal path.
NAT Mapping Address and Port	If necessary, in the NAT mapping address and port section, specify the mapped public IPs and ports of the server referenced in the DNAT rules of the DNT device. When the client connects to the server through the DNAT device, the NAT device will translate the destination address of the client to the server's egress interface address. Type the IP address of the NAT device's external interface and the HTTPS port number (You are not recommended to specify the HTTPS port as 443, because 443 is the default HTTPS port of WebUI management). You can configure up to 4 IPs.

- Click **Done** to save the settings.

To view the SSL VPN online users, take the following steps:

- Select **Configure > Network > SSL VPN**.
- Select an SSL VPN instance.
- View the detailed information of the online users in the table.

Configuring Resource List

Resource list refers to resources configured in system that can be easily accessible by users. Each resource contains multiple resource items. The resource item is presented in the form of a resource item name followed by a URL in your default browser page. After the SSL VPN user is authenticated successfully, the authentication server will send the user group information of the user to the SSL VPN server. Then, according to the binding relationship between the

user group and resources in the SSL VPN instance, the server will send a resource list in which the user can access to the client. After that, the client will analyze and make the IE browser in system pop up a page to display the received resource list information, so that the user can access the private network resource directly by clicking the URL link. The resource list page pops up only after the authentication is passed. If a user does not belong to any user group, the browser will not pop up the resource list page unless authentication is passed.

To configure resource list for SSL VPN:

- 1. Select **Network > VPN > SSL VPN**.
- 2. Click **Resources List** at the top-right corner.
- 3. Click **New**.

Resources Configuration

Name:

(1-31) chars

Resource Item

Name:

1-63 chars

URL:

1-255 chars

Name

URL

Add

Delete

up

down

top

bottom

OK

Cancel

In the Resources Configuration dialog box, configure the corresponding options.

Option	Description
Name	Enters a name for the new resource.
Resource Item	
Name	Enters a name for a new resource item. Names of resource items in different resources can not be the same.
URL	Enters a URL for a new resource item.
Add	Click Add to add this binding item to the list below. Note: The number of resource items that can be added in a resource ranges from 0 to 48. The total number of resource items that can be added in all resources can not exceed 48.
Delete	To delete a rule, select the rule you want to delete from the list and click Delete .
Up/Down/Top/Bottom	You can move the location for items at your own choice to adjust

the presentation sequence accordingly.

4. Click **OK**, the new resource will be displayed in the resource list.
At most 3 resource items can be displayed in the resource list for each resource, and the other items will be displayed as "...". You can click **Edit** or **Delete** button to edit or delete the selected resource.



Note:

- Less than 48 resources can be configured in a SSL VPN instance.
- The resource list function is only available for Windows SSL VPN clients.

Configuring an SSL VPN Address Pool

The SSL VPN servers allocate the IPs in the SSL VPN address pools to the clients. After the client connects to the server successfully, the server will fetch an IP address along with other related parameters (e.g., DNS server address, and WIN server address) from the SSL VPN address pool and then allocate the IP and parameters to the client.

You can create an IP binding rule to meet the fixed IP requirement. The IP binding rule includes the IP-user binding rule and the IP-role binding rule. The IP-user binding rule binds the client to a fixed IP in the configured address pool. When the client connects to the server successfully, the server will allocate the binding IP to the client. The IP-role binding rule binds the role to an IP range in the configured address pool. When the client connects to the server successfully, the server will select an IP from the IP range and allocate the IP to the client.

After the client successfully connects to the server, the server will check the binding rules in a certain order to determine which IP to allocate. The order is shown as below:

- Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.
- Check whether the IP-role binding rule is configured for the client. If yes, get an IP from the IP range and allocate to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.



Note: IP addresses in the IP-user binding rule and the IP address in the IP-role binding rules should not overlap.

To configure an address pool, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. Click **Address Pool** at the top-right corner.

3. Click **New**.

In the **Basic** tab, configure the following options.

Option	Description
Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved Start IP	Specifies the reserved start IP of the address pool.
Reserved End IP	Specifies the reserved end IP of the address pool.
Mask	Specifies the netmask in the dotted decimal format.
DNS1/2/3/4	Specifies the DNS server IP address for the address pool. It is optional. 4 DNS servers can be configured for one address pool at most.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to 2 WIN servers can be configured for one address pool.

In the **IP User Binding** tab, configure the corresponding options.

Option	Description
User	Type the user name into the User box.
IP	Type the IP address into the IP box.
Add	Click Add to add this IP user binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click Delete .

In the **IP Role Binding** tab, configure the corresponding options.

Option	Description
Role	Type the role name into the Role box.
Start IP	Type the start IP address into the Start IP box.
End IP	Type the end IP address into the End IP box.
Add	Click Add to add this IP role binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click Delete .

Up/Down/Top/Bottom System will query IP role binding rules by turn, and allocate the IP address according to the first matched rule. You can move the location up or down at your own choice to adjust the matching sequence accordingly.

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

Configuring SSL VPN Login Page

You can customize the title and background of the SSL VPN login page. The default title is **Login** and the login page is shown as below:



To customize the SSL VPN login page, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top-right corner, click **Login Page Configuration**.
3. Click **Browse** to select the background picture. The selected pictures must be zipped, and the file name must be **Login_box_bg_en.gif** for English pages. The picture size must be 624px*376px.
4. Click **Upload** to upload the background picture to system. After uploading successfully, you will have completed the background picture modification.
5. Enter the title in the **Authentication Page Title** box to customize the title of the login page.
6. Click **OK** to save the settings. Clicking **Cancel** will only affect the authentication page title modification.

If you want to use the default authentication title **Login**, click **Clear Page Title**. Then click **OK**. If you want to restore the default picture, click **Restore Default Background** and select **English** in the pop-up dialog. Then click **OK**.

Host Binding

The host binding function verifies that the hosts are running the SSL VPN clients according to their host IDs and user information. The verification process is:

1. When an SSL VPN user logs in via the SSL VPN client, the client will collect the host information of main board serial number, hard disk serial number, CUP ID, and BIOS serial number.
2. Based on the above information, the client performs the MD5 calculation to generate a 32-digit character, which is named host ID.
3. The client sends the host ID and user/password to the SSL VPN server.
4. The SSL VPN server verifies the host according to the entries in the host unbinding list and host binding list, and deals with the verified host according to the host binding configuration.

The host unbinding list and host binding list are described as follows:

- Host unbinding list: The host unbinding list contains the user-host ID entries for the first-login users.
- Host binding list: The host binding list contains the user-host ID entries for the users who can pass the verification. The entries in the host unbinding list can be moved to the host binding list manually or automatically for the first login. When a user logs in, the SSL VPN server will check whether the host binding list contains the user-host ID entry of the login user. If there is a matched entry in the host binding list, the user will pass the verification and the sever will go on checking the user/password. If there is no matched entry for the login user, the connection will be disconnected.

Configuring Host Binding

Configuring host binding includes host binding/unbinding configurations, super user configurations, shared host configurations, and user-host binding list importing/exporting.

Configuring Host Binding and Unbinding

To add a binding entry to the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Checking/Binding** to visit the Host Checking/Binding page.
2. Click **Host Binding**.
3. With the Binding and Unbinding tab active, select the entries you want to add to the Host Unbinding List.
4. Click **Add** to add the selected entries to the Host Binding List.

To delete a binding entry from the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Checking/Binding** to visit the Host Checking/Binding page.
3. Click **Host Binding**.
4. With the Binding and Unbinding tab active, select the entries you want to delete from the Host binding List.
5. Click **Unbinding** to remove the selected entries from this list.

Configuring a Super User

The super user won't be controlled by the host checking function, and can log into any host. To configure a super user, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Checking/Binding** to visit the Host Checking/Binding page.

- Click **Host Binding**.
- With the User Privilege tab active, click **New**.

In the New dialog box, configure the corresponding options.

Option	Description
User	Specifies the name of the user.
Super User	Select the Enable check box to make it a super user.
Pre-approved Number	If system allows one user to login from multiple hosts, and the option of automatically adding the user-host ID entry into the host binding list at the first login is enabled, then by default system only records the user and first login host ID entry to the host binding list. For example, if the user logs in from other hosts, the user and host ID will be added to the host unbinding list. This pre-approved number specifies the maximum number of user-host ID entries for one user in the host binding list.

- Click **OK** to save the settings.

Configuring a Shared Host

Clients that log in from the shared host won't be controlled by the host binding list. To configure a shared host, take the following steps:

- Select **Network > VPN > SSL VPN**.
- At the top right corner, click **Host Checking/Binding** to visit the Host Checking/Binding page.
- Click **Host Binding**.
- With the Host ID Privilege tab active, click **New**.

In the New dialog box, configure the corresponding options.

Option	Description
Host ID	Type the host ID into the Host ID box.
Shared Host	Select the Enable check to make it a shared host. By default, this check box is selected.

5. Click **OK** to save the settings.

Importing/Exporting Host Binding List

To import the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Checking/Binding** to visit the Host Checking/Binding page.
3. Click **Host Binding**.
4. With the Binding and Unbinding tab active, click **Import**.
5. Click **Browse** to find the binding list file and click **Upload**.

To export the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Checking/Binding** to visit the Host Checking/Binding page.
3. Click **Host Binding**.
4. With the Binding and Unbinding tab active, click **Export**.
5. Select a path to save the host binding list.

Host Checking

The host checking function checks the security status of the hosts running SSL VPN clients, and according to the check result, the SSL VPN server will determine the security level for each host and assign corresponding resource access right based on their security level. It a way to assure the security of SSL VPN connection. The checked factors include the operating system, IE version, and the installation of some specific software.

The factors to be checked by the SSL VPN server are displayed in the list below:

Factor	Description
Operating system	• Operating system, e.g., Windows 2000, Windows 2003, Windows XP, Windows Vista, Windows 7m Windows 8, etc.
	• Service pack version, e.g., Service Pack 1
	• Windows patch, e.g., KB958215, etc.
	• Whether the Windows Security Center and Automatic Updates are enabled.
	• Whether the installation of AV software is compulsory, and whether the real-time monitor and the auto update of the signature database are enabled.
	• Whether the installation of anti-spyware is compulsory, and whether the real-time monitor and the online update of the signature database are enabled.
Other configurations	• Whether the personal firewall is installed, and whether the real-time protection is enabled.
	Whether the IE version and security level reach the specified requirements.
	Whether the specified processes are running.
	Whether the specified services are installed.
	Whether the specified services are running.
	Whether the specified registry key values exist.
	Whether the specified files exist in the system.

Role Based Access Control and Host Checking Procedure

Role Based Access Control (RBAC) means that the permission of the user is not determined by his user name, but his role. The resources can be accessed by a user after the login is determined by his corresponding role. So role is the bridge connecting the user and permission.

The SSL VPN host checking function supports RBAC. And the concepts of primary role and guest role are introduced in the host checking procedure. The primary role determines which host checking profile (contains the host checking contents and the security level) will be applied to the user and what access permission can the user have if he passes the host checking. The guest role determines the access permissions for the users who fail the host checking.

The host checking procedure is shown as below

1. The SSL VPN client sends request for connection and passes the authentication.
2. The SSL VPN server sends the host checking profile to the client.
3. The client checks the host security status according to the items in the host checking profile. If it fails the host checking, system will be notified of the checking result.
4. The client sends the checking result back to the server.
5. The server disconnects the connection to the failed client or gives the guest role's access permission to the failed client.

The host checking function also supports dynamic access permission control. On one side, when the client's security status changes, the server will send a new host checking profile to the client to make him re-check; on the other side, the client can perform security checks periodically. For example, if the AV software is disabled and is detected by the host checking function, the role assigned to the client may change as will the access permissions.

Configuring a Host Checking Profile

To configuring host checking profile, take the following steps:

- 1. Select **Network > VPN > SSL VPN**.
- 2. At the top right corner, click **Host Checking/Binding** to visit the Host Checking/Binding page.
- 3. In the Host Checking tab, click **New** to create a new host checking rule.

Host Compliance Check Configuration

BasicAdvanced

Name:

(1-31) chars

OS Version:

NO Check

Patch1:

(0-64) chars

Patch2:

(0-64) chars

Patch3:

(0-64) chars

Patch4:

(0-64) chars

Patch5:

(0-64) chars

Lowest IE Version:

☒ NO Check

☐ IE6.0

☐ IE7.0

☐ IE8.0

☐ IE9.0

☐ IE10.0

☐ IE11.0

Lowest IE Security Level:

☒ NO Check

☐ Medium

☐ Medium-High

☐ High

The host compliance check function will only affect the SSL VPN client for Windows OS.

OK

Cancel

In the Basic tab, configure the corresponding options.

Option	Description
Hostname	Specifies the name of the host checking profile.
OS Version	Specifies whether to check the OS version on the client host. Click one of the following options: <ul style="list-style-type: none">No Check: Do not check the OS version.Must Match: The OS version running on the client host must be the same as the version specified here. Select the OS version and service pack version from the drop-down lists respectively.At Least: The OS version running on the client host should not be lower than the version specified here. Select the OS version and service pack version from the drop-down lists respectively.
Patch1/2/3/4/5	Specifies the patch that must be installed on the client host. Type the patch name into the box. Up to 5 patches can be specified.
Lowest IE Version	Specifies the lowest IE version in the Internet zone on the client host. The IE version running on the client host should not be lower than the version specified here.
Lowest IE Security Level	Specifies the lowest IE security level on the client host. The IE security level on the host should not be lower than the level specified here.

In the Advanced tab, configure the corresponding options.

Option	Description
--------	-------------

Security Center	Checks whether the security center is enabled on the client host.
Auto Update	Checks whether the Windows auto update function is enabled.
Anti-Virus Software	Checks the status and configurations of the anti-virus software: <ul style="list-style-type: none"> • Installed: The client host must have the AV software installed. • Monitor: The client host must enable the real-time monitor of the AV software. • Virus Signature DB Update: The client host must enable the signature database online update function.
Anti-spyware Software	Checks the status and configurations of the anti-spyware software: <ul style="list-style-type: none"> • Installed: The client host must have the anti-spyware installed. • Monitor: The client host must enable the real-time monitor of the anti-spyware. • Virus Signature DB Update: The client host must enable the signature database online update function.
Firewall	Checks the status and configurations of the firewall: <ul style="list-style-type: none"> • Installed: The client host must have the personal firewall installed. • Monitor: The client host must enable the real-time monitor function of the personal firewall.
Registry Key Value	
Key1/2/3/4/5	Checks whether the key value exists. Up to 5 key values can be configured. The check types are: <ul style="list-style-type: none"> • No Check: Do not check the key value. • Exist: The client host must have the key value. Type the value into the box. • Do not Exist: The client cannot have the key value. Type the value into the box.
File Path Name	
File1/2/3/4/5	Checks whether the file exists. Up to 5 files can be configured. The check types are: <ul style="list-style-type: none"> • No Check: Do not check file. • Exist: The client host must have the file. Type the value into the box. • Do not Exist: The client cannot have the file. Type the value into the box.
Running Process Name	
Process1/2/3/4/5	Checks whether the process is running. Up to 5 processes can be configured. The check types are: <ul style="list-style-type: none"> • No Check: Do not check the process. • Exist: The client host must have the process run. Type the process name into the box.

	<ul style="list-style-type: none"> Do not Exist: The client cannot have the process run. Type the process name into the box.
Installed Service Name	
Service1/2/3/4/5	<p>Checks whether the service is installed. Up to 5 services can be configured. The check types are:</p> <ul style="list-style-type: none"> No Check: Do not check the service. Exist: The client host must have the service installed. Type the service name into the box. Do not Exist: The client host cannot have the service installed. Type the service name into the box.
Running Service name	
Service1/2/3/4/5	<p>Checks whether the service is running. Up to 5 services can be configured. The check types are:</p> <ul style="list-style-type: none"> No Check: Do not check the service. Exist: The client host must have the service run. Type the service name into the box. Do not Exist: The client host cannot have the service run. Type the service name into the box.

- Click **OK** to save the settings.

SSL VPN Client for Windows

SSL VPN client for Windows is named Hillstone Secure Connect. Hillstone Secure Connect can be run with the following operating systems: Windows 2000/2003/XP/Vista/Windows 7/Windows 8/Windows 2008/Windows 10/Windows 2012. The encrypted data can be transmitted between the SSL VPN client and SSL VPN server after a connection has been established successfully. The functions of the client are:

- Get the interface and the route information of the PC on which the client is running.
- Show the connecting status, statistics, interface information, and route information.
- Show SSL VPN log messages.
- Upgrade the client software.
- Resolve the resource list information received from the server.

This section mainly describes how to download, install, start, uninstall the SSL VPN client, and its GUI and menu. The method for downloading, installing and starting the client may vary from the authentication methods configured on the server. The SSL VPN server supports the following authentication methods:

- Username/Password
- Username/Password + Digital Certificate
- Digital Certificate only

Downloading and Installing Secure Connect

When using the SSL VPN client for the first time, you need to download and install the client software Hillstone Secure Connect. This section describes three methods for downloading and installing the client software based on three available authentication methods. For the Username/Password + Digital Certificate authentication, the digital certificate can either be the USB Key certificate provided by the vendor, or the file certificate provided by the administrator.

Using Username/Password Authentication

When the Username/Password authentication is configured on the server, take the following steps to download and install the SSL VPN client software - Hillstone Secure Connect:

1. Visit the following URL with a web browser: <https://IP-Address:Port-Number>. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN instance.
2. In the SSL VPN login page (shown in Figure 1), type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**.
 - If the local authentication server is configured on the device, the username and password should already be configured on the device.
 - If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, and the user logs in for the first time, the username should be the username configured on the Radius server, and the password should be the dynamic Token password bound to the user. Click **Login**, and in the PIN Setting page (shown in Figure 2), set a PIN (4 to 8 digits). After the PIN has been set successfully, you will be prompted to login again with the new password (shown in Figure 3). Click **Login again** to return to the login page, type the correct username and new password, and click **Login**. The new password is PIN + dynamic Token password. For example, if the PIN is set to 54321, and the dynamic Token password is 808771, then the new password is 54321808771.
 - If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, but the user is not logging in for the first time, the username should be the username configured on the Radius server, and the password should be PIN + dynamic Token password.

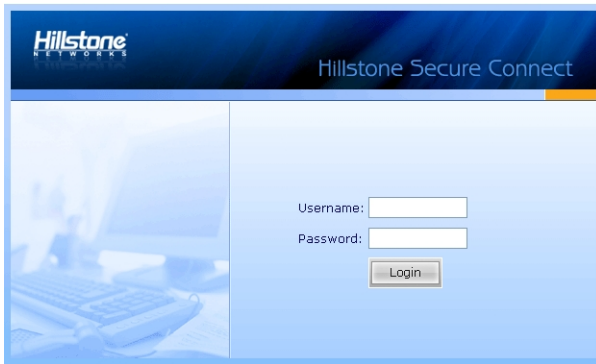


Figure 1



Figure 2

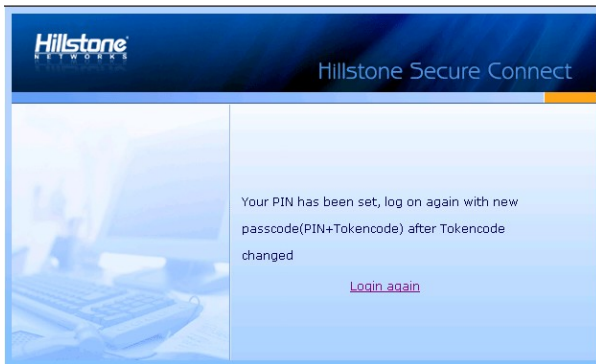


Figure 3

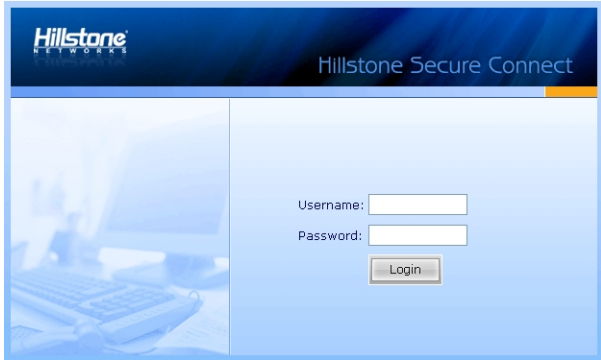
3. If SMS authentication is enabled on the SSL VPN server, the SMS Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.
 - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
 - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.
4. After logging in, IE will download the client software automatically, and you can install it by following the prompts; for other web browsers, e.g., Firefox, you should click **Download** to download the client software scvpn.exe first, and then double click it to install.

A virtual network adapter will be installed on your PC together with Secure Connect. It is used to transmit encrypted data between the SSL VPN server and client.

Using Username/Password + Digital Certificate Authentication

When the Username/Password + Digital Certificate authentication is configured on the server, take the following steps to download and install the SSL VPN client software - Hillstone Secure Connect:

1. Insert the USB Key to the USB port of the PC, or import the file certificate provided by the administrator manually.
2. Visit the following URL with a web browser: `https://IP-Address:Port-Number`. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN instance.
3. In the Select Digital Certificate dialog box, select the certificate you want and click **OK**. If USB Key certificate is selected, in the pop-up dialog box, provide the UKey PIN code (1111 by default) and click **OK**.
4. In the SSL VPN login page shown below, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user should be configured before in the device.



5. If SMS authentication is enabled on the SSL VPN server, the SMS Authentication dialog box will appear. Type the authentication code and click **Authenticate**. If you have not received the authentication code within one minute, you can re-apply.
 - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
 - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.
6. After logging in, IE will download the client software automatically, and you can install it by following the prompts; for other web browsers, e.g., Firefox, you should click **Download** to download the client software scvpn.exe first, and then double click it to install.

A virtual network adapter will be installed on your PC together with Secure Connect. It is used to transmit encrypted data between the SSL VPN server and client.

Using Digital Certificate Only

When only the Digital Certificate authentication is configured on the server, take the following steps to download and install the SSL VPN client software - Hillstone Secure Connect:

1. Insert the USB Key to the USB port of the PC, or import the file certificate provided by the administrator manually.
2. Visit the following URL with a web browser: `https://IP-Address:Port-Number`. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN instance.
3. In the Select Digital Certificate dialog box, select the certificate you want and click **OK**. If USB Key certificate is selected, in the Enter Password dialog box, provide the UKey user password (1111 by default) and click **OK**.
4. After logging in, IE will download the client software automatically, and you can install it by following the prompts; for other web browsers, e.g., Firefox, you should click **Download** to download the client software scvpn.exe first, and then double click it to install.

A virtual network adapter will be installed on your PC together with Secure Connect. It is used to transmit encrypted data between the SSL VPN server and client.

Starting Secure Connect

After installing Secure Connect on your PC, you can start it in two ways:

- Starting via Web
- Starting directly

Starting via Web

This section describes how to start Secure Connect via Web based on the three authentication methods configured on the server. For the Username/Password + Digital Certificate authentication, the digital certificate can either be the USB Key certificate provided by the vendor, or the file certificate provided by the administrator.

Using Username/Password Authentication

When the Username/Password authentication is configured on the server, take the following steps to start Secure Connect via web:

1. Type the URL `https://IP-Address:Port-Number` into the address bar of your web browser.
2. In the login page (shown in Figure 4), type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**.
 - If local authentication server is configured on the device, the username and password should be configured before on the device;
 - If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, and the user logs in for the first time, the username should be the username configured on the Radius server, and the password should be the dynamic Token password bound to the user. Click **Login**, and in the PIN Setting page (shown in Figure 5), set a PIN (4 to 8 digits). After the PIN has been set successfully, you will be prompted to login again with the new password (shown in Figure 6). Click **Login again** to return to the login page, type the correct username and new password, and click **Login**. The new password is PIN + dynamic Token password. For example, if the PIN is set to 54321, and the dynamic Token password is 808771, then the new password is 54321808771.
 - If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, but the user is not logging in for the first time, the username should be the username configured on the Radius server, and the password should be PIN + dynamic Token password.

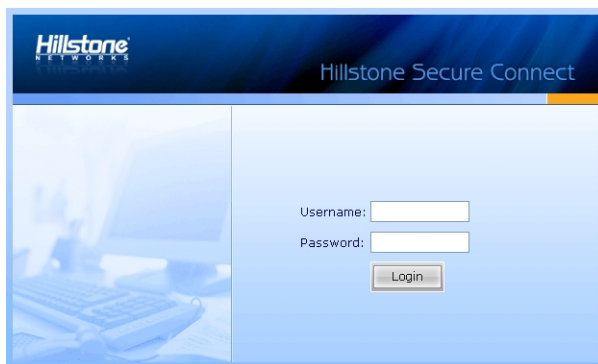


Figure 4

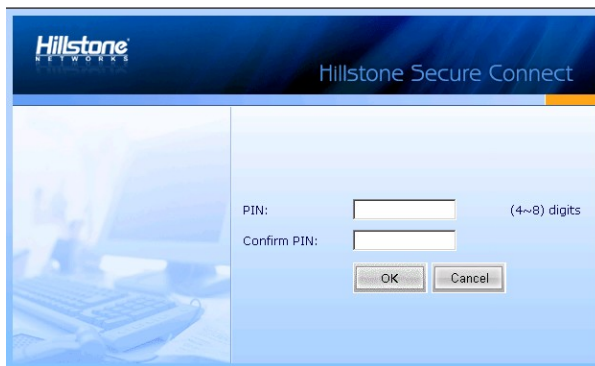


Figure 5

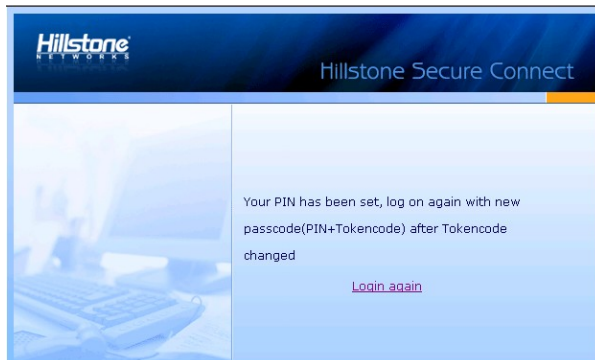



Figure 6

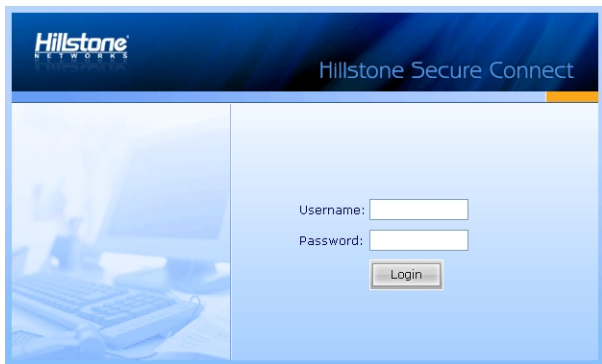
3. If the SMS authentication function is enabled, type the SMS authentication code into the box, and then click **Authenticate**. If you have not received the code within one minute, you can re-apply.
 - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
 - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

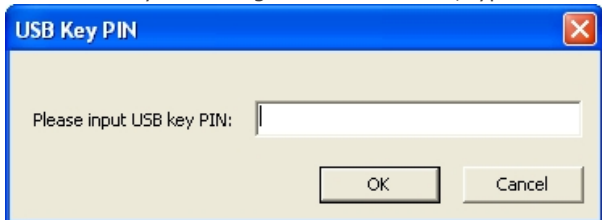
Using Username/Password + USB Key Certificate Authentication

When the Username/Password + Digital Certificate authentication for the USB Key certificate is configured on the server, to start Secure Connect via web, take the following steps:

1. Insert the USB Key to the USB port of the PC.
2. Type the URL `https://IP-Address:Port-Number` into the address bar of your web browser.
3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**. In the Enter Password dialog box, provide the UKey user password (1111 by default) and click **OK**.
4. In the SSL VPN login page shown below, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user should already be configured on the device.



5. If the SMS authentication function is enabled, type the SMS authentication code into the box, and then click **Authenticate**. If you have not received the code within one minute, you can re-apply.
 - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
 - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.
6. In the USB Key PIN dialog box shown below, type the UKey PIN (1111 by default), and click **OK**.

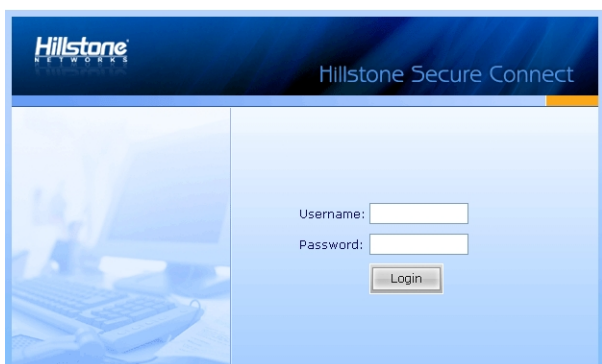


After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (🔒) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using Username/Password + File Certificate Authentication

When the Username/Password + Digital Certificate authentication for the file certificate is configured on the server, to start the Secure Connect via web, take the following steps:

1. Import the file certificate provided by the administrator manually.
2. Type the URL `https://IP-Address:Port-Number` into the address bar of your web browser.
3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**.
4. In the SSL VPN login page shown below, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user should already be configured on the device.



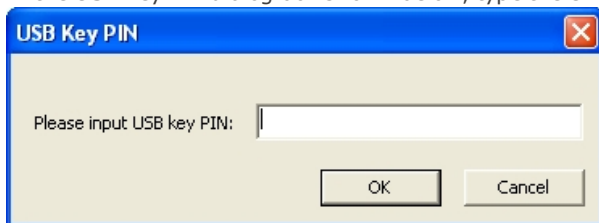
5. If the SMS authentication function is enabled, type the SMS authentication code into the box, and then click **Authenticate**. If you have not received the code within one minute, you can re-apply.
 - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
 - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (🔒) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using USB Key Certificate Only Authentication

When the Digital Certificate only authentication for the USB Key certificate is configured on the server, to start the Secure Connect via web, take the following steps:

1. Insert the USB Key to the USB port of the PC.
2. Type the URL https://IP-Address:Port-Number into the address bar of your web browser.
3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**. In the Enter Password dialog box, provide the UKey user password (1111 by default) and click **OK**.
4. In the USB Key PIN dialog box shown below, type the UKey PIN (1111 by default), and click **OK**.




After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (🔒) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using File Certificate Only Authentication

When the Digital Certificate only authentication for the file certificate is configured on the server, to start the Secure Connect via web, take the following steps:

1. Import the file certificate provided by the administrator manually.
2. Type the URL https://IP-Address:Port-Number into the address bar of your web browser.

3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

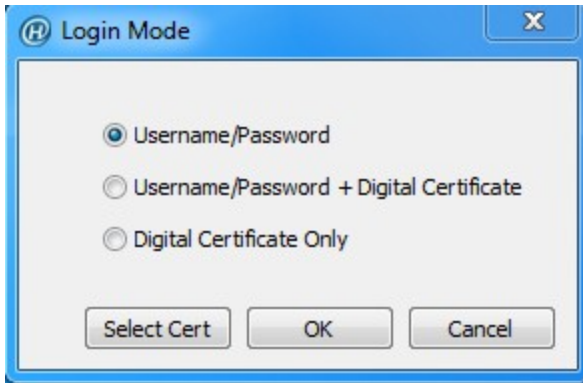
Starting Directly

This section describes how to start Secure Connect directly based on the three authentication methods configured on the server. For the Username/Password + Digital Certificate authentication, the digital certificate can either be the USB Key certificate provided by the vendor, or the file certificate provided by the administrator.

Using Username/Password Authentication

When the Username/Password authentication is configured on the server, to start the Secure Connect directly, take the following steps:

1. On your PC, double click the shortcut of Hillstone Secure Connect on your desktop.
2. In the Login dialog box, click **Mode**. In the Login Mode dialog shown below, click **Username/Password**, and then click **OK**.



3. In the Login dialog box of the Username/Password authentication mode (shown in Figure 7), configure the options to login.

Option	Description
Saved Con- nection	Provides the connection information you have filled before. Select a con- nection from the drop-down list.
Server	Enter the IP address of SSL VPN server.
Port	Enter the HTTPS port number of SSL VPN server.
Username	Enter the name of the login user.
Password	Enter the password of the login user.

- If the local authentication server is configured on the device, the username and password should already be configured on the device.
- If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, and the user logs in for the first time, the username should be the username configured on the Radius server, and the password should be the dynamic Token password bound to the user. Click **Login**, and in the PIN Setting page (shown in Figure 8), set a PIN (4 to 8 digits). After the PIN has been set successfully, you will be prompted to login again with the new password (shown in Figure 9). Click **Login again** to return to the login page, type the correct username and new password, and click **Login**. The new password is PIN + dynamic Token password. For example, if the PIN is set to 54321, and the dynamic Token password is 808771, then the new password is 54321808771.

- If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, but the user is not logging in for the first time, the username should be the username configured on the Radius server, and the password should be PIN + dynamic Token password.



Figure 7

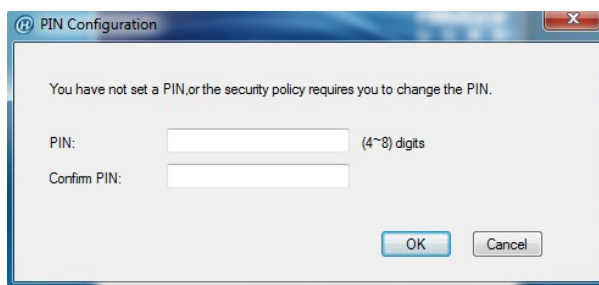


Figure 8

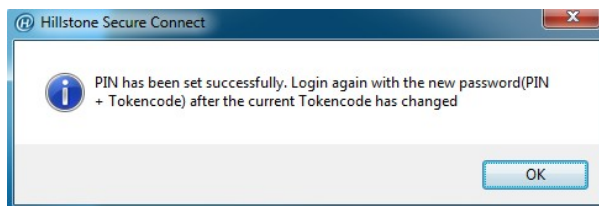
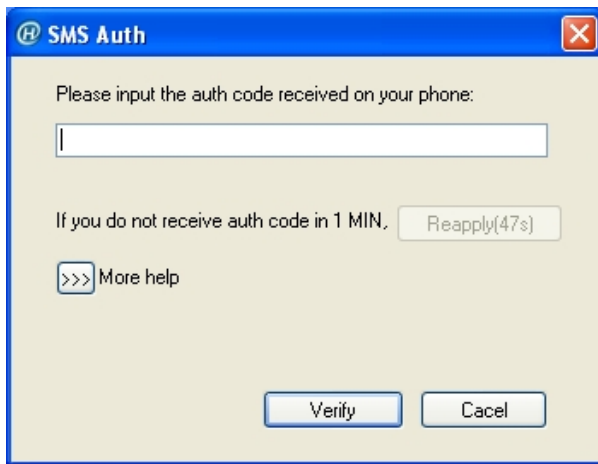



Figure 9

4. Click **Login**. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog (as shown below) and click **Verify**. If you have not received the authentication code within one minute, you can re-apply by clicking **Reapply**.

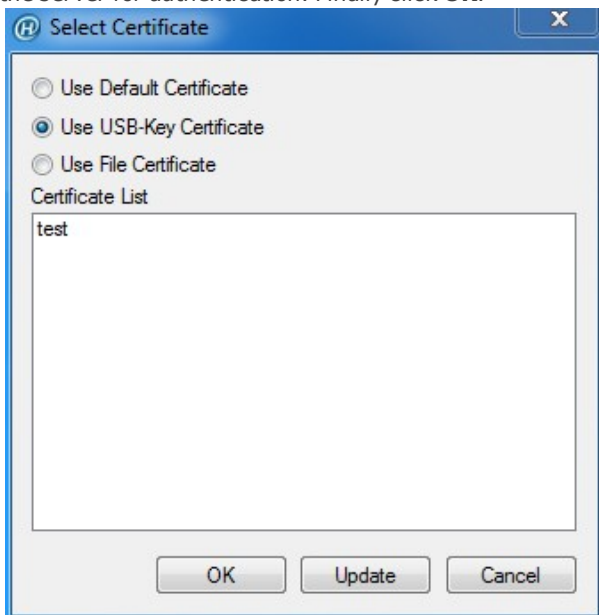


Finishing the above steps, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. And the encrypted communication between the client and server can be implemented now.

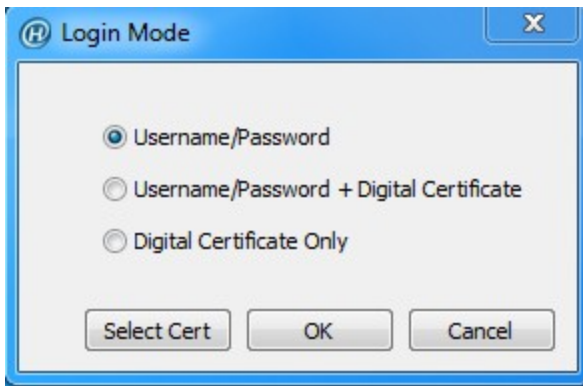
Using Username/Password + USB Key Certificate Authentication

When the Username/Password + Digital Certificate authentication is configured on the server, for the USB Key certificate, to start Secure Connect directly, take the following steps:

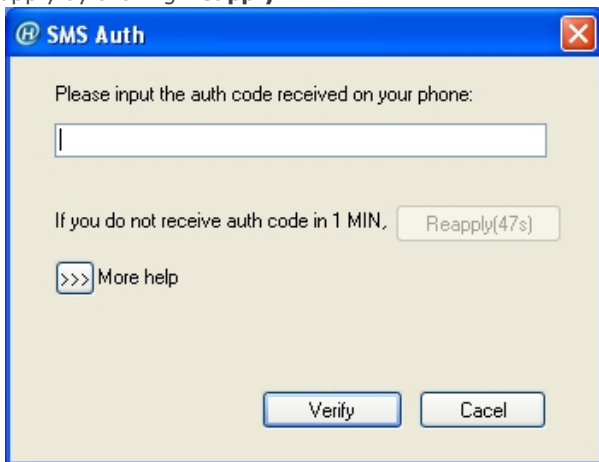
1. Insert the USB Key to the USB port of the PC.
2. In your PC, double click the shortcut to Hillstone Secure Connect on your desktop.
3. In the Login dialog box, click **Mode**. In the Login Mode dialog box, first click **Username/Password + Digital Certificate**, and if necessary, click **Select Cert**. In the Select Certificate dialog box shown below, select a USB Key certificate. If the USB Key certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.




4. In the Login dialog of the Username/Password + Digital Certificate authentication mode (as shown below), configure the options to login.



5. Click **Login**. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog (as shown below) and click **Verify**. If you have not received the authentication code within one minute, you can re-apply by clicking **Reapply**.

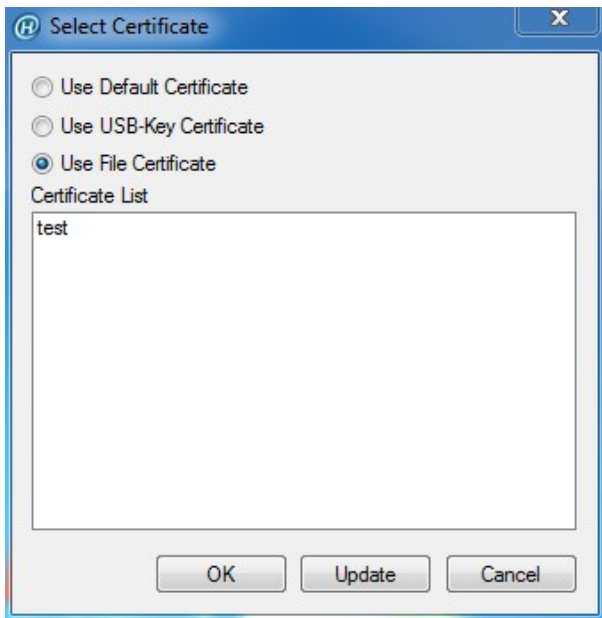


After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

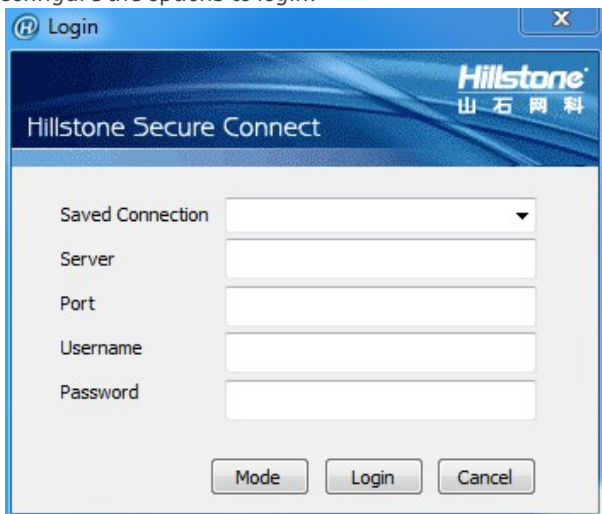
Using Username/Password + File Certificate Authentication

When the Username/Password + Digital Certificate authentication for the USB Key certificate is configured on the server, to start the Secure Connect directly, take the following steps:

1. Import the file certificate provided by the administrator manually.
2. On your PC, double click the shortcut to Hillstone Secure Connect on your desktop.
3. In the Login dialog box, click **Mode**. In the Login Mode dialog, first click **Username/Password + Digital Certificate**, and if necessary, click **Select Certificate**. In the Select Certificate dialog box shown below, select a file certificate. If the file certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.




4. In the Login dialog box of the Username/Password + Digital Certificate authentication mode (as shown below), configure the options to login.



5. Click **Login**. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog box (as shown below) and click **Verify**. If you have not received the authentication code in one minute, you can re-apply by clicking **Reapply**.

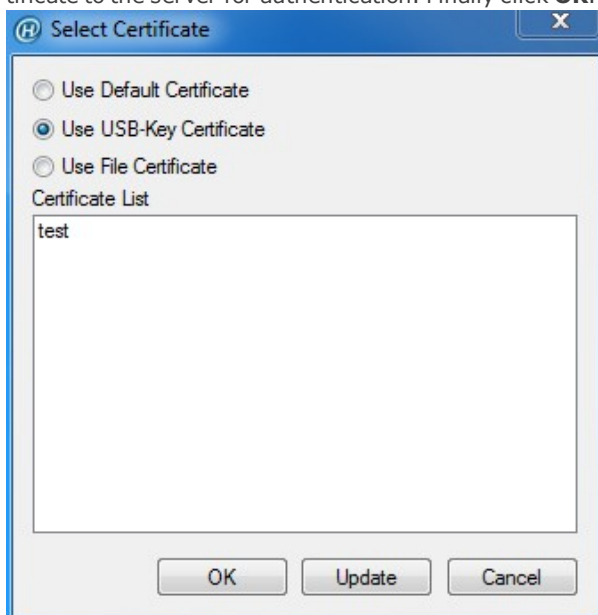


After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using USB Key Certificate Only

When the Username/Password + Digital Certificate authentication for the file certificate is configured on the server, to start the Secure Connect directly, take the following steps:


1. Insert the USB Key to the USB port of the PC.
2. On your PC, double click the shortcut to Hillstone Secure Connect on your desktop.
3. In the Login dialog box, click **Mode**. In the Login Mode dialog box, first click **Username/Password + Digital Certificate**, and if necessary, click **Select Certificate**. In the Select Certificate dialog box shown below, select a USB Key certificate. If the USB Key certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.



4. In the Login dialog box of the Username/Password + Digital Certificate authentication mode (as shown below), configure the options to login.



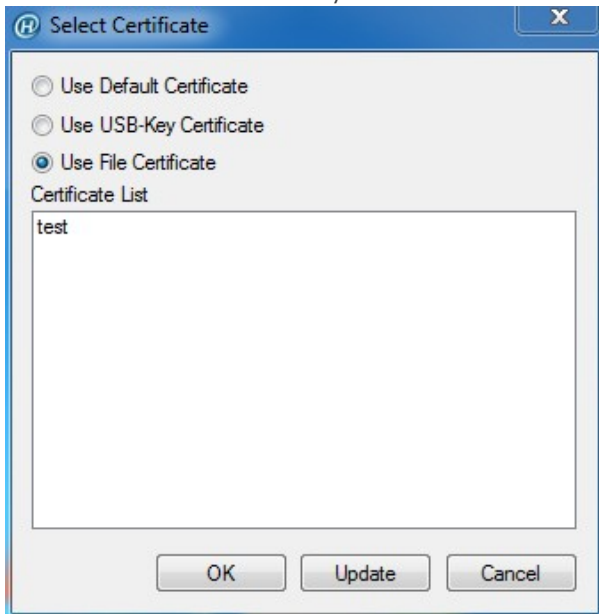
5. Finishing the above configuration, click **Login**.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

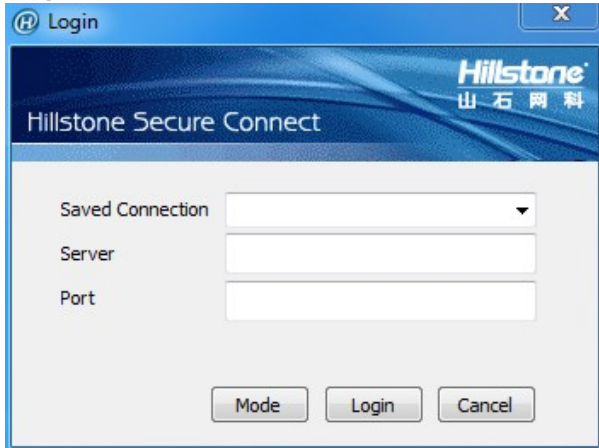
Using File Certificate Only

When the Digital Certificate Only authentication for the USB Key certificate is configured on the server, to start the Secure Connect directly, take the following steps:


1. Import the file certificate provided by the administrator manually.
2. On your PC, double click the shortcut to Hillstone Secure Connect on your desktop.
3. In the Login dialog box, click **Mode**. In the Login Mode dialog box, first click **Username/Password + Digital Certificate**, and if necessary, click **Select Certificate**. In the Select Certificate dialog box shown below, select a file certificate. If the file certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.




4. In the Login dialog box of the Digital Certificate Only authentication mode (as shown below), configure the options to login.



5. Finishing the above configuration, click **Login**.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Viewing Secure Connect GUI

Double click the Secure Connect icon () in the notification area, and the Network Information dialog box appears. This dialog box shows information about statistics, interfaces, and routes.

General

Descriptions of the options on the General tab:

Address Information	
Server	The IP address of the connected SSL VPN server.
Client	The IP address of the client.
Crypto Suite	
Cipher	The encryption algorithm and authentication algorithm used by SSL VPN.
Version	The SSL version used by SSL VPN.
Connection Status	
Status	The current connecting status between the client and server. The possible statuses are: connecting, connected, disconnecting, and disconnected.
IPCompress	
Algorithm	Shows the compression algorithm used by SSL VPN.
Tunnel Packets	
Sent	The number of sent packets through the SSL VPN tunnel.
Received	The number of received packets through the SSL VPN tunnel.
Tunnel Bytes	
Sent	The number of sent bytes through the SSL VPN tunnel.
Received	The number of received bytes through the SSL VPN tunnel.
Connected Time	

Address Information	
Duration	Shows the time period during which the client is online.
Compress Ratio	
Sent	Shows the length ratio of sent data after compression.
Received	Shows the length ratio of received data after compression.

Interface

Descriptions of the options on the Interface tab:


Option	Description
Adapter Name	The name of the adapter used to send SSL VPN encrypted data.
Adapter Type	The type of the adapter used to send SSL VPN encrypted data.
Adapter Status	The status of the adapter used to send SSL VPN encrypted data.
Physical Address	The MAC address of the interface used to send SSL VPN encrypted data.
IP Address Type	The type of the interface address used to send SSL VPN encrypted data.
Network Address	The IP address (allocated by SSL VPN server) of the interface used to send SSL VPN encrypted data.
Subnet Mask	The subnet mask of the interface used to send SSL VPN encrypted data.
Default Gateway	The gateway address of the interface used to send SSL VPN encrypted data.
DNS Server Address	The DNS server addresses used by the client.
WINS Address	The WINS server addresses used by the client.

Route

Description of the option on the Route tab:

Option	Description
Local LAN Routes	The routes used by the virtual network adapter.

Viewing Secure Connect Menu

Right-click the Secure Connect icon () in the notification area and the menu appears.

Descriptions of the menu items are as follows:

Option	Description
Network Information	Displays the related information in the Network Information dialog box.
Log	Shows Secure Connect log messages in the Log dialog box. This dialog box shows the main log messages. To view the detailed log messages, click Detail . Click Clear to remove the messages in the dialog box. Click OK to close the Log dialog box.
Debug	Configures Secure Connect's debug function in the Debug dialog box.
About	Shows Secure Connect related information in the About dialog box.
Connect	When Secure Connect is disconnected, click this menu item to connect.
Disconnect	When Secure Connect is connected, click this menu item to disconnect.
Option	Configures Secure Connect options, including login information, auto start, auto login, and so on. For more information, see "Configuring Secure Connect" on Page 206 .

Option	Description
Exit	Click Exit to exit the client. If the client is connected to the server, the connection will be disconnected.

Configuring Secure Connect

You can configure Secure Connect in the Secure Connect Options dialog box(click **Option** from the client menu). The configurations include:

- Configuring General Options
- Configuring a Login Entry

Configuring General Options

In the Secure Connect Options dialog box, select **General** from the navigation pane and the general options will be displayed.

Descriptions of the options:

Option	Description
Auto Start	Select this check box to autorun the SSL VPN client when the PC is started.
Auto Login	Select this check box to allow the specified user to login automatically when the PC is started. Select the auto login user from the Default Connection drop-down list.
Auto Reconnect	Select this check box to allow the client to reconnect to the SSL VPN server automatically after an unexpected disconnection.
Select Cert	Click the button to select a USB Key certificate in the Select Certificate dialog box. This option is available when the USB KEY authentication is enabled.

Configuring a Login Entry

Login entry contains the login information for clients. The configured login entries will be displayed in the Saved Connection drop-down list in the Login dialog box. You can login by simply choosing the preferred connection instead of filling up the options in the Login dialog box.

To add a login entry, take the following steps:

1. In the Secure Connect Options dialog box, select **Saved Connection** from the navigation pane and the login options will be displayed.

In the dialog box, configure the corresponding options.

Option	Description
Connection Name	Specifies the name for the connection to identify it. System will assign a name to the connection based on its server, port, and user automatically if this option is kept blank
Server	Specifies the IP address of the SSL VPN server.
Port	Specifies the HTTPS port number of the SSL VPN server.
Username	Specifies the login user.
Login Mode	Specifies the login mode. It can be one of the following options: <ul style="list-style-type: none">• Password (the username/password authentication method). If Password is selected, select Remember Password to make system remember the password and type the password into the Password box.• Password + UKey (the USB KEY authentication method). If Password + UKey is selected, select Remember PIN to make system remember the PIN number and type PIN number into the UKey PIN box.
Proximity Auto Detection	Select the option to enable the optimal path detection function. For more information about optimal path detection, see "Configuring an SSL VPN" on Page 172 .

2. Click **Apply**.

SSL VPN Client for Android

The SSL VPN client for Android is Hillstone Secure Connect. It can run on Android 4.0 and above. The functions of Hillstone Secure Connect contains the following items:

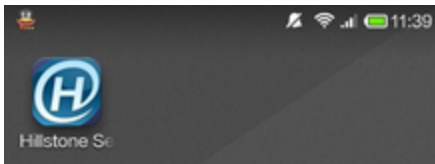
- Obtain the interface information of the Android OS.
- Display the connection status with the device, traffic statistics, interface information, and routing information.
- Display the log information of the application.

Downloading and Installing the Client

To download and install the client, take the following steps:

1. Visit <http://www.hillstonenet.com/our-products/next-gen-firewalls-e-series/> to download the installation file of the client.
2. Use your mobile phone to scan the QR code of the client for Android at the right sidebar, and the URL of the client displays.
3. Open the URL and download the Hillstone-Secure-Connect-Versione_Number.apk file.
4. After downloading successfully, find this file in your mobile phone.
5. Click it and the installation starts.
6. Read the permission requirements.
7. Click **Install**.


After the client being installed successfully, the icon of Hillstone Secure Connect appears in the desktop as shown below:



Starting and Logging into the Client

To start and log into the client, take the following steps:

1. Click the icon of Hillstone Secure Connect. The login page appears.
2. **Provide the following information and then click Login.**
 - Please Choose: Select a login entry. A login entry stores the login information and it facilitates your next login. For more information on login entry, see the Configuration Management section below.
 - Server: Enters the IP address or the server name of the device that acts as the VPN server.
 - Port: Enters the HTTPs port number of the device.
 - Username: Enters the username for logging into the VPN.
 - Password: Enters the corresponding password.
3. If the SSL VPN server enables the SMS authentication, the SMS authentication page will appear. In this page, enter the received authentication code and then submit it. If you do not receive the authentication code, you can request it after one minute.

After the client connecting to the SSL VPN server, the key icon () will appear at the notification area of your Android system.

GUI

After the client connects to the SSL VPN server, you can view the following pages: Connection Status page, Configuration Management page, Connection Log page, System Configuration page, and About Us page.

Connection Status

Click **Status** at the bottom of the page to enter into the **Connection Status** page and it displays the statistics and routing information:

- The Connection Time: Time period during which the client is online.
- Received Bytes: Shows the received bytes through the SSL VPN tunnel.
- Sent Bytes: Shows the sent bytes through the SSL VPN tunnel.
- Server: Shows the IP address or the server name of the device that client connects to.
- Port: Shows the HTTPs port number of the device.
- Account: Shows the username that logs into the VPN instance.
- Private Server Address: Shows the interface's IP address of the device that the client connects to.
- Client Private Address: Shows the IP address of the interface. This interface transmits the encrypted traffic and this IP address is assigned by the SSL VPN server.
- Address Mask: Shows the netmask of the IP address of the interface. This interface transmits the encrypted traffic.
- DNS Address: Shows the DNS Address used by the client.
- Routing Information: Shows the routing information for transmitting encrypted data.
- Disconnection Connection: Click this button to disconnect the current connection with the server.

Configuration Management


Click **VPN** at the bottom of the page to enter into the **Configuration Management** page. In this page, you can perform the following operations:

- Add/Edit/Delete a login entry
- Modify the login password
- Disconnect the connection with SSL VPN server
- Connect to the SSL VPN server

Adding a Login Entry

To facilitate the login process, you can add a login entry that stores the login information. The added login entry will display in the drop-down list of **Please Choose** in the login page. You can select a login entry and the login information will be filled in automatically.

To add a login entry, take the following steps:

1. In the Configuration Management page, click the  icon at the top-right corner.
2. **In the pop-up window, enter the following information:**
 - a. Connection Name: Enter a name as an identifier for this login entry

- b. **Server:** Enter the IP address or the server name of the device that acts as the VPN server.
 - c. **Port:** Enter the HTTPs port number of the device.
 - d. **Username:** Enter the username for logging into the VPN.
3. Click **Confirm** to save this login entry.

Editing a Login Entry

To edit a login entry, take the following steps:

1. In the login entry list, click the one that you want to edit and several buttons will appear.
2. Click **Edit** to make the Edit Configuration dialog box appear.
3. In the dialog box, edit the login entry.
4. Click **Confirm** to save the modifications.

Deleting a Login Entry

To delete a login entry, take the following steps:

1. In the login entry list, click the one that you want to delete and several buttons will appear.
2. Click **Delete**.
3. Click **Yes** in the pop-up dialog box to delete this login entry.

Modifying the Login Password

To modify the login password, take the following steps:

1. In the login entry list, click the one that you want to modify the password and several buttons will appear.
2. Click **Modify Password**.
3. Enter the current password and new password in the pop-up dialog box.
4. Click **Confirm** to save the settings.

Disconnecting the Connection or Logging into the Client

To disconnect the connection or log into the client, take the following steps:

1. In the login entry list, click a login entry and several buttons will appear.
2. If the connection status to this server is disconnected, you can click **Login** to log into the client; if the connection status is connected, you can click **Disconnect Connection** to disconnect the connection.
3. In the pop-up dialog box, confirm your operation.

Connection Log

Click **Log** at the bottom of the page to enter into the **Configuration Log** page. In this page, you can view the logs.

System Configuration

Click **Config** at the bottom of the page to enter into the **System Configuration** page. In this page, you can configure the following options:

- **Auto Reconnect:** After turning on this switch, the client will automatically reconnect to the server if the connection is disconnected unexpectedly.

- Show Notify: After turning on this switch, the client icon will display in the notification area.
- Allow To Sleep: After turning on this switch, the client can stay connected while the Android system is in the sleep status. With this switch turned off, the client might disconnect the connection and cannot stay connected for a very long time while the Android system is in the sleep status.
- Auto Login: After turning on this switch, the client will automatically connect to the server when it starts. The server is the one that the client connects to the last time.
- Remember The Password: After turning on this switch, the client will remember the password and automatically fill in the login entry.
- Exit: Click **Exit** to exit this application.

About Us

Click **About** at the bottom of the page to enter the About US page. This page displays the version information, contact information, copyright information, etc.

SSL VPN Client for iOS

The SSL VPN client for iOS is called Hillstone BYOD Client (HBC) and it supports iOS 6.0 and higher versions. HBC mainly has the following functions:

- Simplify the VPN creation process between the Apple device and the Hillstone device
- Display the VPN connection status between the Apple device and the Hillstone device
- Display the log information

To use the SSL VPN client for iOS, download and install the **Hillstone BYOD Client** app from the App Store.

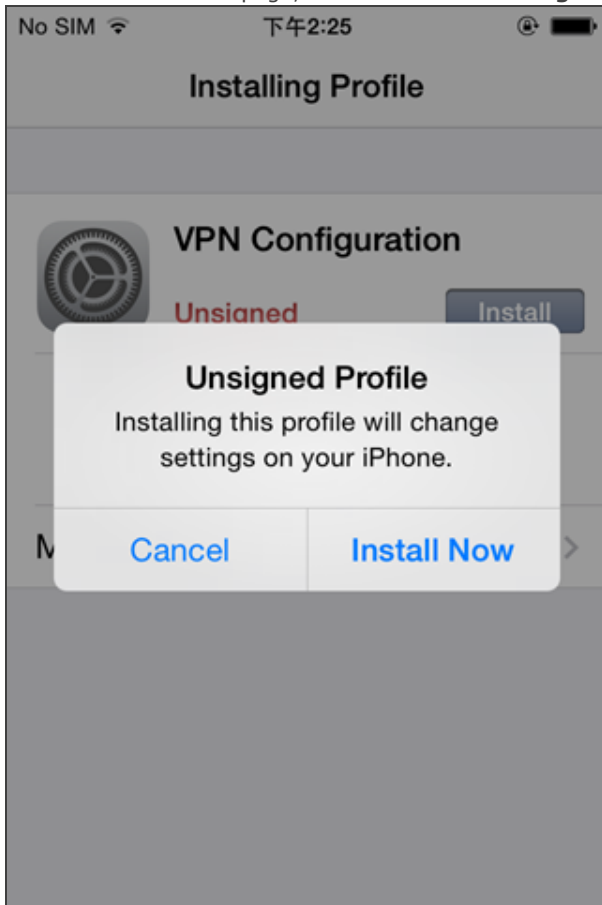
Deploying VPN Configurations

For the first-time logon, you need to deploy the VPN configurations, as shown below:

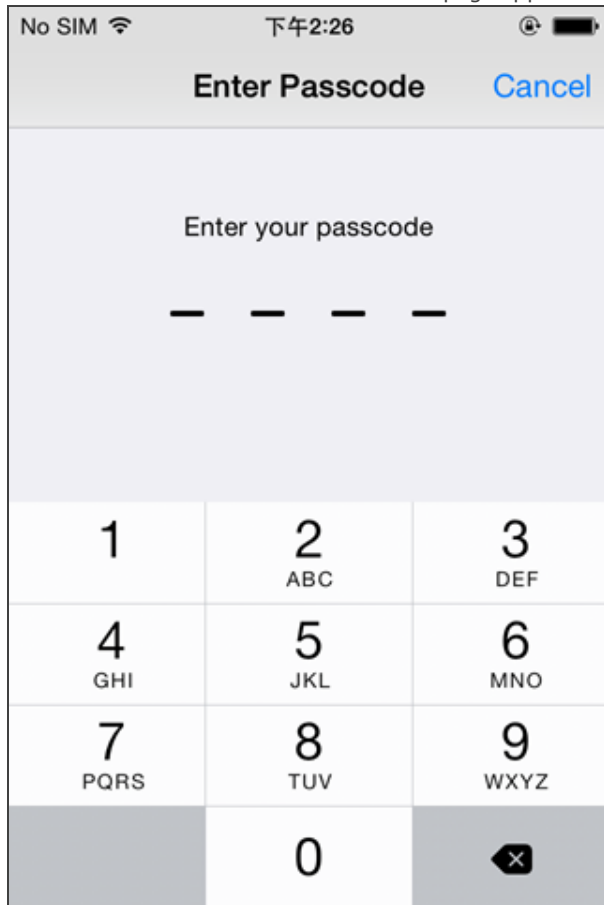
1. Click the HBC icon located at the desktop of iOS. The login page of HBC appears.
2. **In the login page, specify the following information and then click Login.**
 - Connection: Enter a name for this newly created connection instance.
 - Server: Enter the IP address or the server name of the device that acts as the VPN server.
 - Port: Enter the HTTPs port number of the device.
 - Username: Enter the username for logging into the VPN.
 - Password: Enter the corresponding password.
3. After logging the VPN server successfully, the **Install Profile** page pops up and the deployment process starts automatically.



4. In the **Install Profile** page, click **Install**. The **Unsigned Profile** window pops up.



5. Click **Install Now**. The **Enter Passcode** page appears.



6. Enter your passcode. The passcode is the one for unlocking your iOS screen. With the correct passcode entered, iOS starts to install the profile.

7. After completing the installation, click **Done** in the **Profile Installed** page.



The profile deployed is for the instance with the above parameters (connection, server, port, username, and password). If the value of one parameter changes, you need to deploy the VPN configuration profile again.

Connecting to VPN

After the VPN configuration deployment is finished, take the following steps to connect to VPN:

1. Start HBC.
2. In the login page, enter the required information. The value of these parameters should be the ones that you have specified in the above section of Deploying VPN Configurations. If one of the parameter changes, you need to re-deploy the VPN configuration.
3. Click **Login**. HBC starts to connect to the Hillstone device.
4. Start **Settings** of iOS and navigate to **VPN**.
5. In the **VPN** page, select the configuration that has the same name as the one you configured in the section of Deploying VPN Configuration.
6. Click the **VPN** switch. iOS starts the VPN connection.
7. In this **VPN** page, when the **Status** value is **Connected**, it indicates the VPN between the iOS device and the Hillstone device has been established.

Introduction to GUI

After logging into HBC, you can view the following pages: Connection Status, Connection Log, and About US.

Connection Status

Click **Connection** at the bottom of the page to enter into the **Connection Status** page and it displays the current connection status. You can configure the following options:

- Remember password: Remembers the password for this connection instance.
- Import configuration: If HBC can connect to the Hillstone device successfully but the iOS VPN connection fails, you need to re-deploy the VPN configurations. After turning on this **Import configuration** switch, HBC will re-deploy the VPN configurations when you log in for the next time.

Connection Log

Click **Log** at the bottom of the page to enter into the **Connection Log** page and it displays the connection log messages.

About US

Click **About** at the bottom of the page to enter the **About Us** page and it displays the information of version, copyright, etc.

SSL VPN Client for Mac OS

The SSL VPN client for Mac OS is Hillstone Secure Connect. It can run on Mac OS X 10.6.8 and above. The encrypted data can be transmitted between the SSL VPN client and SSL VPN server after a connection has been established successfully. The functions of the client are:

- Establish the SSL VPN connection with the SSL VPN server.
- Show the connection status, traffic statistics, and route information.
- Show log messages.

Downloading and Installing Client

Visit <http://www.hillstonenet.com/our-products/next-gen-firewalls-e-series/> to download the installation file of the client.

After downloading the installation file, double-click it. In the pop-up, drag SCVPN to Applications to perform the installation.




To open the installation file, you must have the administrator permission and select **Anywhere** in **System Preferences > Security & Privacy > General > Allow apps downloaded from**.

Starting Client and Establishing Connection

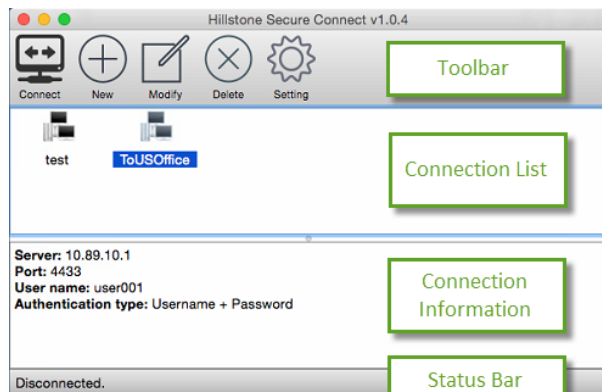
To start the client and establish the connection with the server side, take the following steps:

1. In Mac OS, select **Launchpad > SCVPN**. The client starts.
2. Click **New**. The **Create connection profile** window appears.
3. Provide the following information and then click **OK**.
 - **Name**: Specify a name for this VPN connection.
 - **Description**: Specify the description for this VPN connection.
 - **Server**: Enter the IP address or the server name of the device that acts as the VPN server.
 - **Port**: Enter the HTTPs port number of the device.
 - **User name**: Enter the login name.
 - **Password**: Enter the corresponding password.
 - **Remember password** : Select this check box to remember the password.
4. Select the connection name in the connection list.
5. In the toolbar, click **Connect**. If you do not select **Remember password** in step 3, enter the password in the pop-up and then click **OK**.

After the client connects to the SSL VPN server, the status bar displays **Connection established**. Meanwhile, the notification area of Mac displays . The encrypted data can be transmitted between the SSL VPN client and SSL VPN server now.

GUI

The GUI of the client includes four areas: toolbar, connection list, connection information, and status bar.



Toolbar

In the toolbar, you can perform the following actions:

- **Connect**: Select a connection from the connection list and then click **Connect**. The client starts to establish the connection with server side.
- **New**: Create a new connection. For details, see Starting Client and Establishing Connection.
- **Modify**: Select a connection from the connection list and then click **Modify**. For details of modifying the parameters, see Starting Client and Establishing Connection.
- **Delete**: Select a connection from the connection list and then click **Delete** to delete this connection.

- **Settings:** Set to minimize the client when the connection is established and select whether to check the update of the client when it starts.
- **Cancel:** Click this button to cancel the connection. When the client is connecting to the server side, this button will display.
- **Disconnect:** Disconnect the current connection. After the connection is established, this button will display.
- **Info:** View the channel information and the route information of the current connection. After the connection is established, this button displays.

Connection List

Displays all created connections.

Connection Information

When selecting a connection in the connection list, the connection information area displays the corresponding information of this connection.

After establishing the connection, the connection information area displays the connection duration, server IP address, the IP assigned to the client, the number of packets sent/received through the SSL VPN tunnel, and the bytes sent/received through the SSL VPN tunnel.

Status Bar

Displays the connection status.

Menu

The **SCVPN** item in the menu includes the following options:

- **About SCVPN:** Displays the information of this client.
- **Quit SCVPN:** Quit the client.

The **Logging** item in the menu includes the following options:

- **View:** View the logs.
- **Level:** Select the log level. When selecting the lower level in the menu, the displayed logs will include the logs of upper level. However, when selecting the upper level in the menu, the displayed logs will not include the logs of lower level.

SSL VPN Client for Linux

The SSL VPN client for Linux is Hillstone Secure Connect. It can run on the following operation system.

- 64-bit desktop version of Ubuntu12.04 (GNOME desktop);
- 64-bit desktop version of Ubuntu14.04(GNOME desktop);
- 64-bit desktop version of Ubuntu Kylin16.04(default desktop);
- 64-bit desktop version of CentOS6.5(GNOME desktop);



Note: Hillstone Secure Connect needs to exactly match one of the above Linux systems and use the specified desktop, otherwise the client cannot be installed.

The encrypted data can be transmitted between the SSL VPN client and SSL VPN server after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC on which the client is running.
- Show the connection status, traffic statistics, and route information.
- Show log messages.

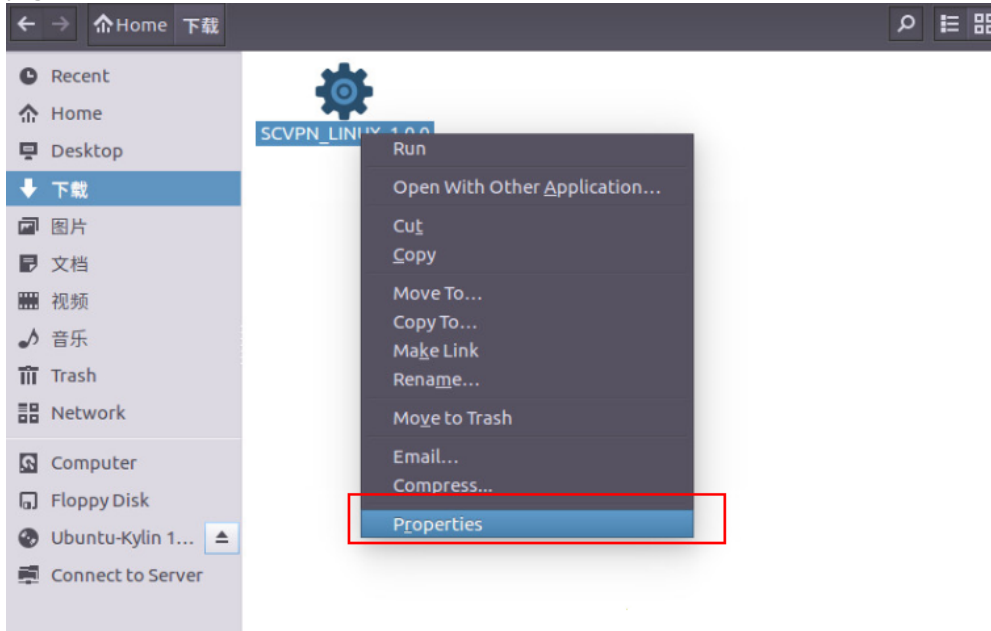
Take 64-bit Ubuntu Kylin16.04 desktop as an example to introduce downloading and installing client, starting client and establishing connection, upgrading and uninstalling client, the client GUI and menu. The client configuration of other three Linux systems can refer to 64-bit Ubuntu Kylin16.04 desktop.

Downloading and Installing Client

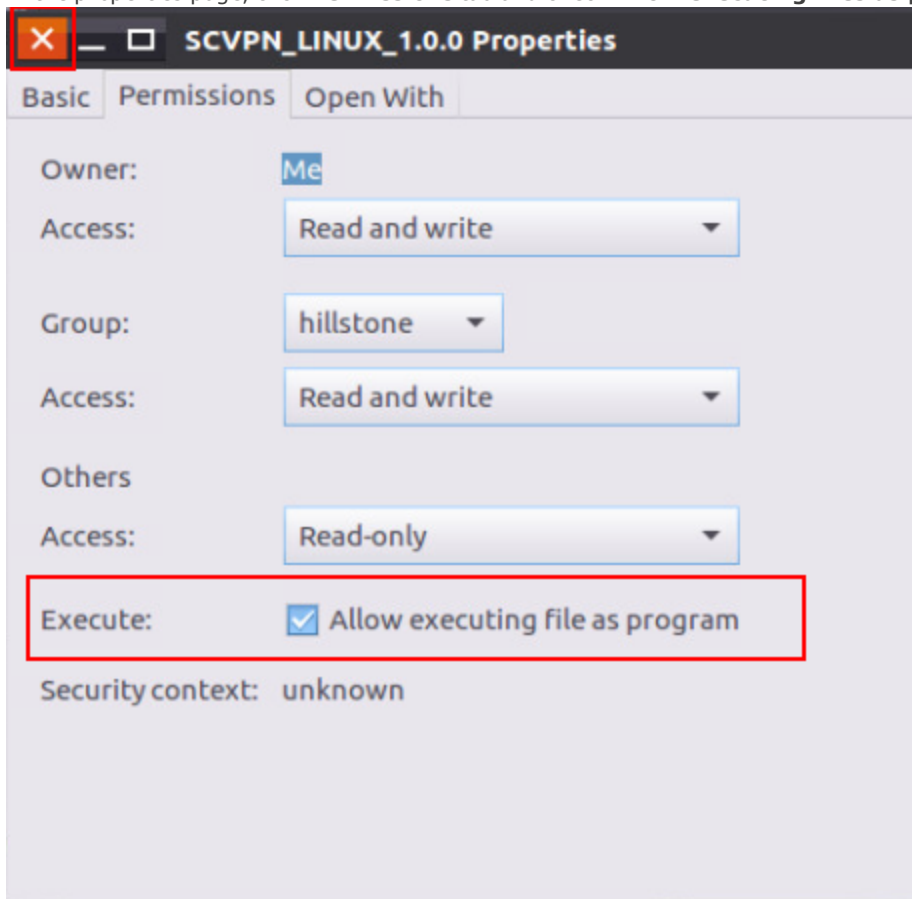
Downloading and installing Hillstone Secure Connect, take the following steps:

1. Visit <http://www.hillstonenet.com/our-products/next-gen-firewalls-e-series/> to download the installation file of the client.

2. After downloading the installation file, right-click the client icon and select **Properties** to go to the properties page.



3. In the properties page, click **Permissions** tab and check **Allow executing files as program**, then close it.

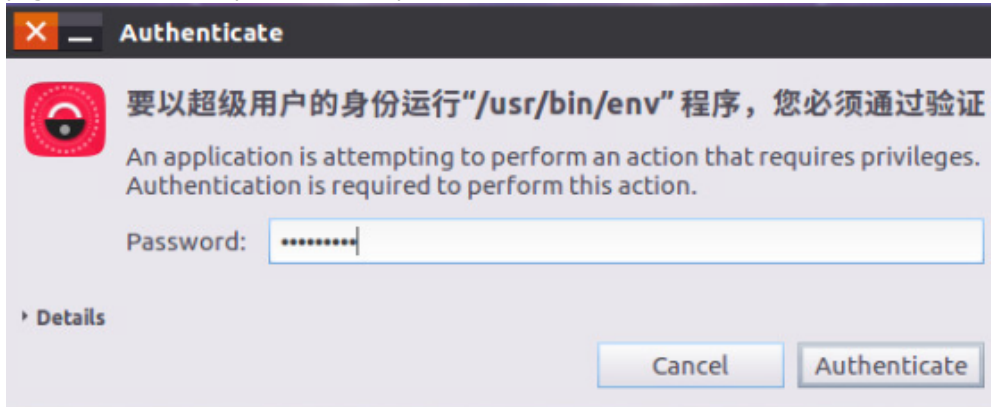


4. Double-click the client icon and follow the setup wizard to complete the installation.

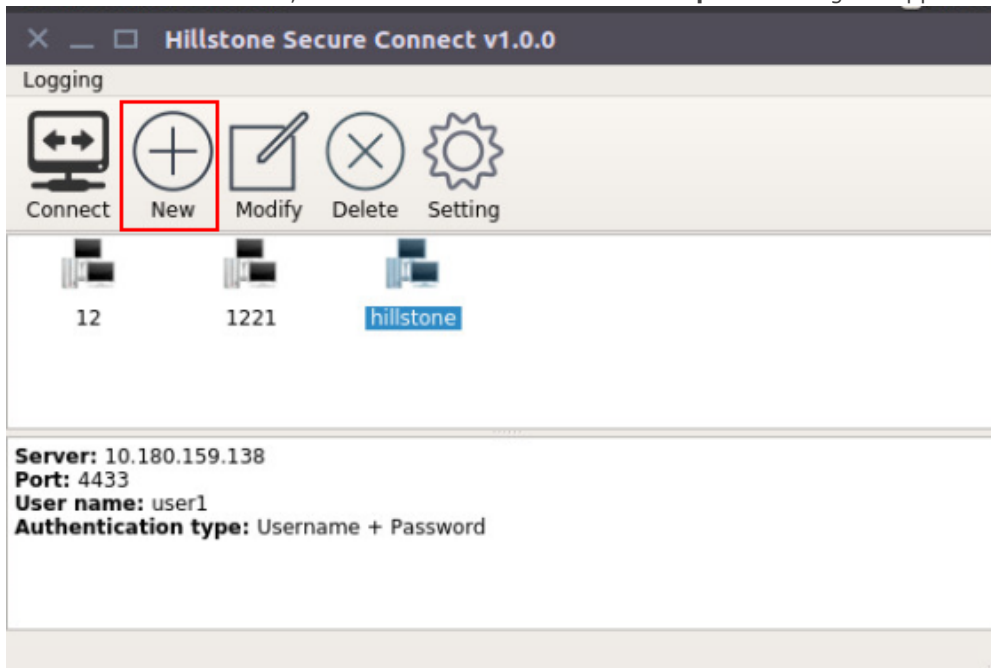
Starting Client and Establishing Connection

To start the client and establish the connection with the server side, take the following steps:

1. Double-click the SCVPN icon on the desktop of the Linux system, and system enters the super user authentication page. Then enter the password of super user , and click **Authenticate** to enter the main interface of the client.



2. In the client main interface, click **New**. The **Create connection profile** dialog box appears.



3. Provide the following information and then click OK.

Create connection profile

Name:

Description:

Host:

Port:

Authentication

User name:

Password:

☒ Remember password

- **Name:** Specify a name for this VPN connection.
- **Description:** Specify the description for this VPN connection.
- **Server:** Enter the IP address or the server name of the device that acts as the VPN server.
- **Port:** Enter the HTTPs port number of the device.
- **User name:** Enter the login name. For detailed information, refer to ["User" on Page 259](#).
- **Password:** Enter the corresponding password.
- **Remember password :** Select this check box to remember the password.

4. Select the connection name in the connection list. In the toolbar, click **Connect**. If you do not select **Remember password** in step 3, enter the password in the pop-up and then click **OK**.



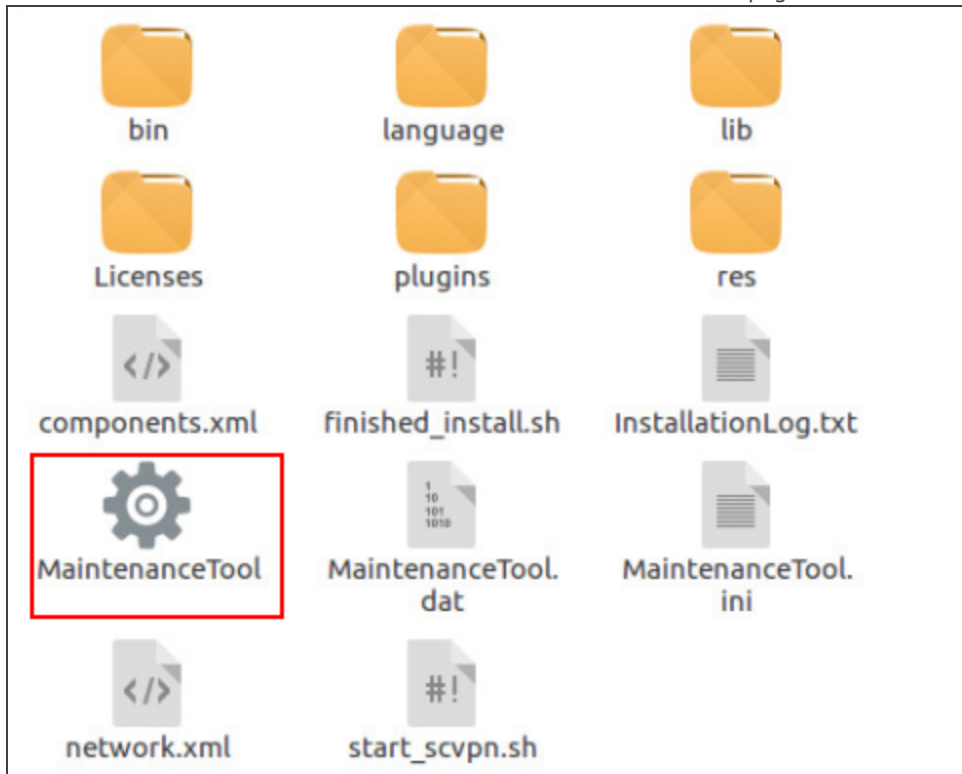
5. After the client connecting to the SSL VPN server, the status bar displays **Connection established**. The encrypted data can be transmitted between the SSL VPN client and SSL VPN server now.



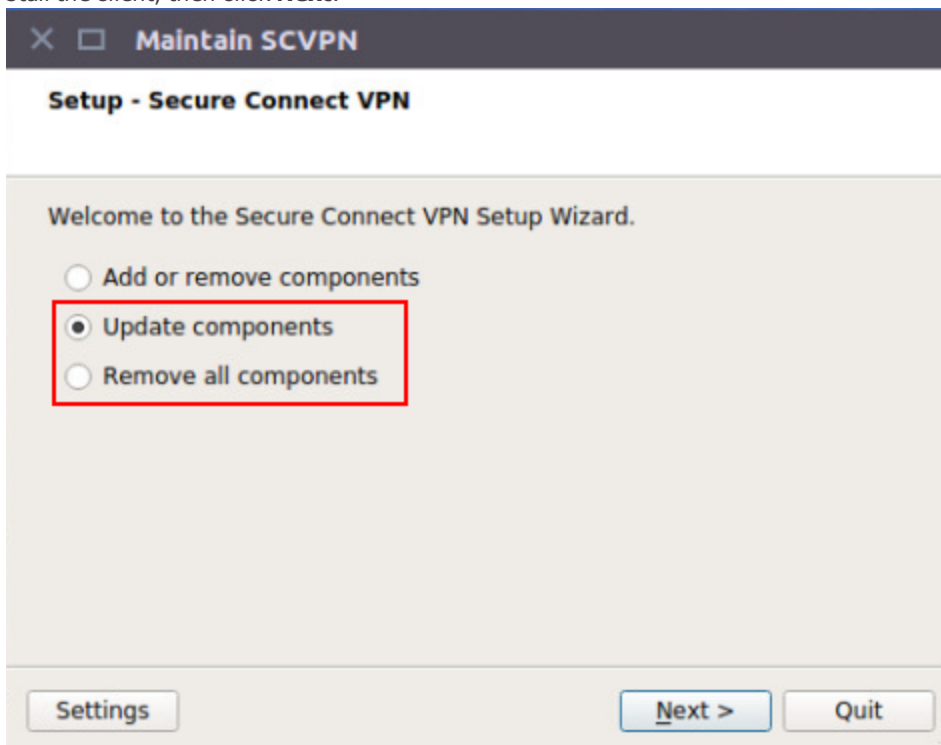
Upgrading and Uninstalling Client

To update and uninstall the SSL VPN Client, take the following steps:

1. Double-click the MaintenanceTool icon to enter the **Maintain SCVPN** page.



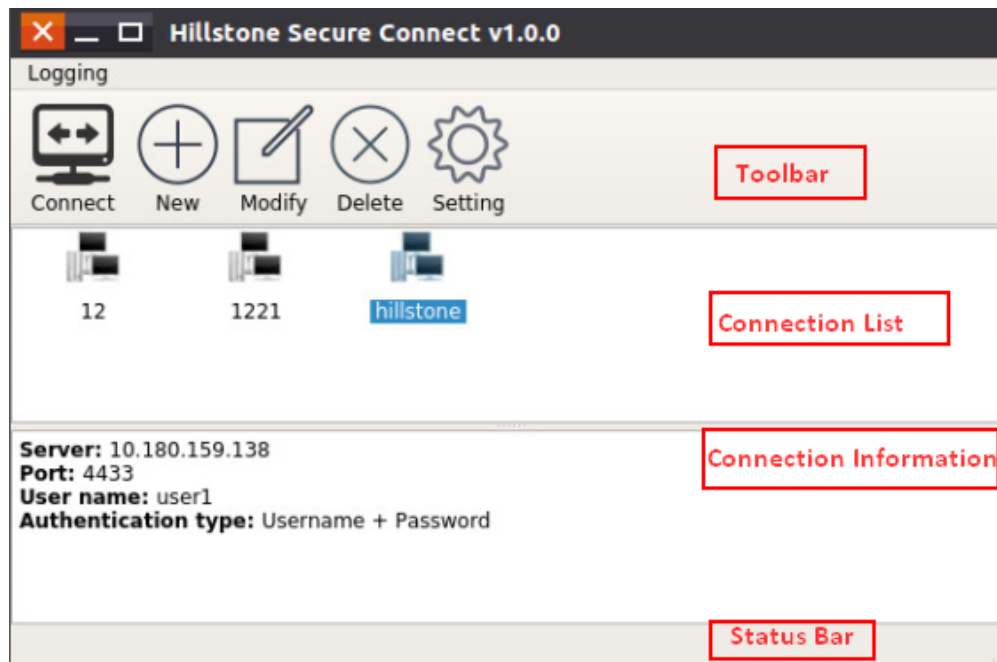
2. In the **Maintain SCVPN** page, select **Update components** or **Remove all components** to upgrade or uninstall the client, then click **Next**.



3. Follow the setup wizard to complete the upgrade or uninstall of client.

GUI

The GUI of the client includes four areas: toolbar, connection list, connection information, and status bar.



Toolbar

In the toolbar, you can perform the following actions:

- **Connect:** Select a connection from the connection list and then click **Connect**. The client starts to establish the connection with server side.
- **New:** Create a new connection. For details, see [Starting Client and Establishing Connection](#).
- **Modify:** Select a connection from the connection list and then click **Modify**. For details about modifying the parameters, see [Starting Client and Establishing Connection](#).
- **Delete:** Select a connection from the connection list and then click **Delete** to delete this connection.
- **Settings:** Set to minimize the client when the connection is established
- **Cancel:** Click this button to cancel the connection. When the client is connecting to the server side, this button is displayed. For more information, see [Starting Client and Establishing Connection](#).
- **Disconnect:** Disconnect the current connection. After the connection is established, this button is displayed. For more information, see [Starting Client and Establishing Connection](#).
- **Info:** View the channel information and the route information of the current connection. After the connection is established, this button is displayed. For more information, see [Starting Client and Establishing Connection](#).

Connection List

Displays all created SSL VPN connections, and uses different icons to distinguish between the connected and the unconnected.

Connection Information

When selecting a connection in the connection list, the connection information area displays the corresponding information of this connection.

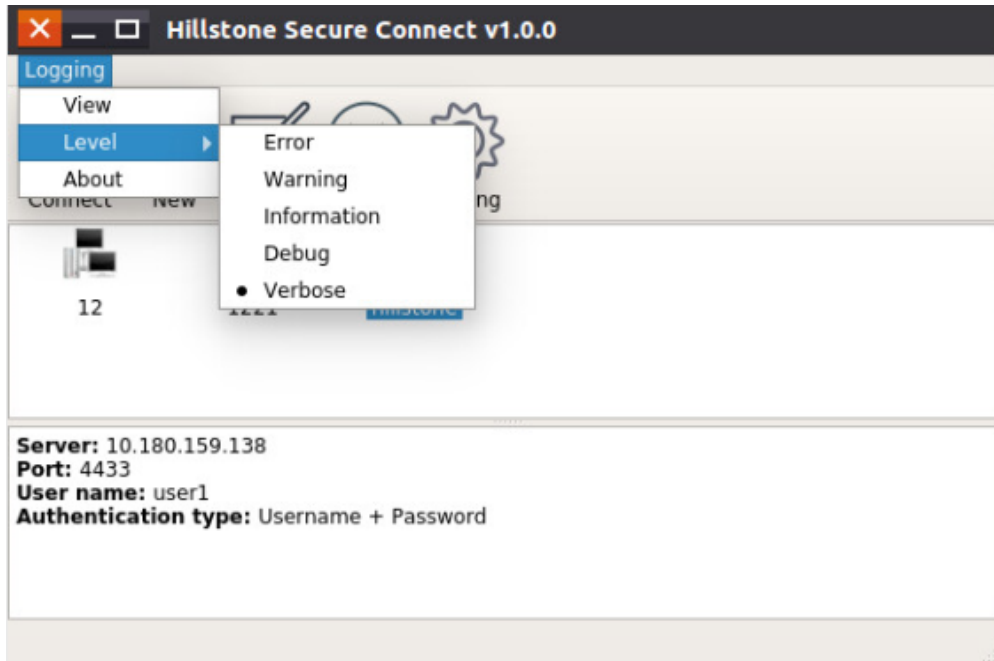
- When the client doesn't connect or has connected to the server, the connection information area displays the server IP address, the port number, the user name and the authentication type.
- After establishing the connection, the connection information area displays the connection duration, server IP address, the IP assigned to the client, the number of packets sent/received through the SSL VPN tunnel, and the bytes sent/received through the SSL VPN tunnel.

Status Bar

Displays the connection status and the connection progress when connecting to the server. For more information, see [Starting Client and Establishing Connection](#).

Menu

Click the **logging** menu in the top-left corner of the client interface .



- View: View the logs.
- Level: Select the log level. When selecting a level in the menu, system will display the logs of upper levels and will not display the logs of lower levels.
- About: Display the version information, copyright information and other relevant information.

L2TP VPN

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

L2TP (Layer Two Tunneling Protocol) is a VPN technique that allows dial-up users to launch VPN connection from L2TP clients or L2TP access concentrators (LAC), and connect to a L2TP network server (LNS) via PPP. After the connection has been established successfully, LNS will assign IP addresses to legal users and permit them to access the private network.

The device acts as a LNS in the L2TP tunnel network. The device accepts connections from L2TP clients or LACs, implements authentication and authorization, and assigns IP addresses, DNS server addresses and WINS server addresses to legal users.

L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPsec, and encrypt data by IPsec, thus assuring the security during the data transmitted through the L2TP tunnel.

Configuring an L2TP VPN

To create an L2TP VPN instance, take the following steps:

- 1. Select **Network > VPN > L2TP VPN**.
- 2. In the L2TP VPN page, click **New**.

In the **Name/Access User** tab, configure the corresponding options.

Option	Description
L2TP VPN Name	Type the name of the L2TP VPN instance
Assigned Users	
AAA Server	Select an AAA server from the AAA Server drop-down list. You can click View AAA Server to view the detailed information of this AAA server.
Domain	Type the domain name into the Domain box. The domain name is used to distinguish the AAA server.
Verify User Domain Name	After this function is enable, system will verify the username and its domain name.
Add	Click Add to add the assigned users. You can repeat to add more items.

In the **Interface/Address Pool/IPSec Tunnel** tab, configure the corresponding options.

Access Interface	
Egress Interface	Select the interface from the drop-down list as the L2TP VPN server interface. This interface is used to listen to the request from L2TP clients.

Tunnel Interface	
Tunnel Interface	<p>Specifies the tunnel interface used to bind to the L2TP VPN tunnel. Tunnel interface transmits traffic to/from L2TP VPN tunnel.</p> <ul style="list-style-type: none"> • Select a tunnel interface from the drop-down list, and then click Edit to edit the selected tunnel interface. • Click New in the drop-down list to create a new interface.
Information	Shows the zone, IP address, and netmask of the selected tunnel interface.
Address Pool	
Address Pool	<p>Specifies the L2TP VPN address pool.</p> <ul style="list-style-type: none"> • Select an address pool from the drop-down list, and then click Edit to edit the selected address pool. • Click New in the drop-down list to create a new address pool. <p>For more information about creating/editing address pools, see "Configuring an L2TP VPN Address Pool" on Page 230.</p>
Information	Shows the start IP address, end IP address, and mask of the address pool.
L2TP over IPSec	
L2TP over IPSec	<p>Select a referenced IPSec tunnel from the drop-down list. L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPSec, and encrypt data by IPSec, thus assuring the security for the data transmitted through the L2TP tunnel..</p>

3. If necessary, click **Advanced** to configure the advanced functions.

In the **Parameters** tab, configure the corresponding options.

Security	
Tunnel Authentication	Click Enable to enable tunnel authentication to assure the security of the connection. The tunnel authentication can be launched by either LNS or LAC. The tunnel cannot be established unless the both ends are authenticated, i.e., the secret strings of the two ends are consistent.
AVP Hidden	Click Enable to enable AVP hidden. L2TP uses AVP (attribute value pair) to transfer and negotiate several L2TP parameters and attributes. By default AVP is transferred in plain text. For data security consideration, you can encrypt the data by the secret string to hide the AVP during the transmission.
Secret	Specifies the secret string that is used for LNS tunnel authentication.
Peer	Specifies the host name of LAC. If multiple LACs are connected to LNS, you can specify different secret strings for different LACs by this parameter.
Add	Click Add to add the configured secret and peer name pair to the list.
Client Connection	
Accept Client IP	Click Enable to allow the accepting of IP address specified by the client. By default the client IP is selected from the address pool, and allocated by LNS automatically. If this function is enabled, you can specify an IP address. However, this IP address must belong to the specified address pool, and be consistent with the username and role. If the specified IP is already in use, system will not allow the user to log on.
Multiple Login	Click Enable to allow a user to log on and be authenticated on different hosts simultaneously.

Hello Interval	Specifies the interval at which Hello packets are sent. LNS sends Hello packets to the L2TP client or LAC regularly, and will drop the connection to the tunnel if no response is returned after the specified period.
LNS Name	Specifies the local name of LNS.
Tunnel Windows	Specifies the window size for the data transmitted through the tunnel.
Control Packet Transmit Retry	Specifies the retry times of control packets. If no response is received from the peer after the specified retry times, system will determine the tunnel connection is disconnected.
PPP Configuration	
LCP Interval Transmit Retry	Specifies parameters for LCP Echo packets used for PPP negotiation. The options are: <ul style="list-style-type: none"> Interval: Specifies the interval at which LCP Echo packets are sent. Transmit Retry: Specifies the retry times for sending LCP Echo packets. If LNS has not received any response after the specified retry times, it will determine the connection is disconnected.
PPP Authentication	Specifies a PPP authentication protocol. The options are: <ul style="list-style-type: none"> PAP: Uses PAP for PPP authentication. CHAP: Uses CHAP for PPP authentication. This is the default option. Any: Uses CHAP for PPP authentication by default. If CHAP is not supported, then uses PAP.

4. Click **Done** to save the settings.

Configuring an L2TP VPN Address Pool

LNS assigns the IP addresses in the address pool to users. After the client has established a connection to LNS successfully, LNS will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and assign them to the client.

L2TP provides fixed IP addresses by creating and implementing IP binding rules.

- The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, system will assign the binding IP to the client.
- The IP-role binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, system will assign an IP address within the IP range to the client.

When LNS is allocating IP addresses in the address pool, system will check the IP binding rule and determine how to assign IP addresses for the client based on the specific checking order below:

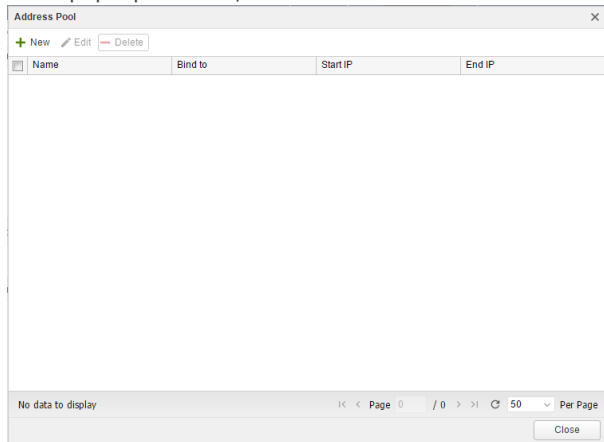


Note: The IP addresses defined in the static IP binding rule and IP-role binding rule should not be overlapped.

To create an address pool, take the following steps:

1. Select **Network > VPN > L2TP VPN**.
2. At the top-right corner, click **Address Pool**.

3. In the pop-up window, click **New**.



In the Basic tab, configure the corresponding options.

Option	Description
Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved Start IP	Specifies the reserved start IP of the address pool.
Reserved End IP	Specifies the reserved end IP of the address pool.
DNS1/2	Specifies the DNS server IP address for the address pool. It is optional. Up to 2 DNS servers can be configured for one address pool.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to 2 WIN servers can be configured for one address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the User box.
IP	Type the IP address into the IP box.
Add	Click Add to add this IP user binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click Delete .

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Type the role name into the Role box.
Start IP	Type the start IP address into the Start IP box.
End IP	Type the end IP address into the End IP box.
Add	Click Add to add this IP role binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click Delete .
Up/Down/Top/Bottom	System will query for IP role binding rules by turn, and allocate the IP address according to the first matched rule. You can move the location up or down at your own choice to adjust the matching sequence accordingly.

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

Viewing L2TP VPN Online Users

To view the L2TP VPN online users, take the following steps:

1. Select **Network > VPN > L2TP VPN**.
2. Select an L2TP VPN instance.
3. View the detailed information of the online users in the table.

Option	Description
Name	Displays the name of L2TP VPN.
Login Time	Displays the login time of the L2TP VPN online user.
Public IP	Displays the public IP of the L2TP VPN online user.
Private IP	Displays the private IP of the L2TP VPN online user.
Operation	Displays the executable operation of the L2TP VPN online user.

Chapter 9 Object

This chapter describes the concept and configuration of objects that will be referenced by other modules in system, including:

- **"Address" on Page 234:** Contains address information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, session limit rules, etc.
- **"Host Book" on Page 236:** A collection of one domain name or several domain names.
- **"Service Book" on Page 237:** Contains service information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, etc.
- **"Application Book" on Page 241:** Contains application information, and it can be used by multiple modules, such as policy rules, NAT rules, QoS, etc.
- **"SLB Server Pool " on Page 245:** Describes SLB server configurations.
- **"Schedule" on Page 247:** Specifies a time range or period. The functions (such as policy rules, QoS rules, host blacklist, connections between the PPPoE interface and Internet) that use the schedule will take effect in the time range or period specified by the schedule.
- **"AAA Server" on Page 249:** Describes how to configure an AAA server.
- **"User" on Page 259:** Contains information about the functions and services provided by a Hillstone device, and users authenticated and managed by the device.
- **"Role" on Page 264:** Contains role information that associates users to privileges. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.
- **"Track Object" on Page 267:** Tracks if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.
- **"Send Object" on Page 269:** After configuring the alarm rules, system will report the warning events to the recipient by sending a warning email or message.
- **"URL Filter" on Page 270:** URL filter controls the access to some certain websites and records log messages for the access actions.

Address

IP address is an important element for the configurations of multiple modules, such as policy rules, NAT rules and session limit rules. Therefore, system uses an address book to facilitate IP address reference and flexible configuration. You can specify a name for an IP range, and only the name is referenced during configuration. The address book is the database in system that is used to store the mappings between IP ranges and the corresponding names. The mapping entry between an IP address and its name in the address book is known as an address entry.

System provides a global address book. You need to specify an address entry for the global address book. When specifying the address entry, you can replace the IP range with a DNS name. Interfaces of the configured IPs will be used as address entries and added to the address book automatically. You can use them for NAT conveniently. Furthermore, an address entry also has the following features:

- All address books contain a default address entry named **Any** and **private_network**. The IP address of **Any** is 0.0.0.0/0, which is any IP address. **Any** can neither be edited nor deleted. The IP addresses of **private_network** are 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, that all private network address. The **private_network** can be edited and deleted.
- One address entry can contain another address entry in the address book.
- If the IP range of an address entry changes, StoneOS will update other modules that reference the address entry automatically.

Address book supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry.

Creating an Address Book

To create an address book, take the following steps:

1. Click **Object>Address Entry**.
2. Click **New**.

In Address Configuration dialog box, enter the address entry configuration.

Basic	
Name	Type the address entry name into the Name box.
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type IP. If IPv6 is selected, all the IP/netmask, IP range, address entry configured should be in the IPv6 format.
Member	
Member	Select an address entry member from the drop-down list, and configure IP/netmask, IP range, Host name, Address entry, or Country/Region as needed.

Basic	
	<ul style="list-style-type: none"> • The Country/Region member is supported in the address entry of the IPv4 type. • Only the security policy and the policy-based route support the address entry with the Country/Region member added. • The address entry with the Country/Region member added does not support the Excluded Member settings.
Add	Click Add to add the configured member to the list below. If it is needed, repeat the above steps to add more members.
Delete	Delete the selected address entry from the list.
Excluded Member	
Member	Specify the excluded member. Select an address entry member from the drop-down list, and configure IP/netmask, IP range, Host name or Address entry as needed. Note: Excluded members' address range need to be in the address range of the members, otherwise the configuration cannot be completed.
Add	Click Add to add the configured excluded member to the list below. If needed, repeat the above steps to add more excluded members.
Delete	Delete the selected excluded member entry from the list.

3. Click OK.

Viewing Details

To view the details of an address entry, take the following steps, including the name, member, description and reference:

1. Click **Object>Address Entry**.
2. In the Address Book dialog box, select an address entry from the member list, and view the details under the list.

Host Book

You can specify a name to be a collection of one domain name or several domain names, and reference this host book when configuring. Host book is the database to store the relationships of domain integrations and the specified names in system.

The entry of the relationship of domain integrations and the specified name is called host entry.



- Note:**
- The maximum number of host entries is one fourth of the maximum number of address entries.
 - Up to one host entry can be configured for each PBR rule.

Creating a Host Book

To create a host book, take the following steps:

1. Select **Object > Host Book**.
2. Click **New**.

Configure the following options.

Option	Description
Name	Type a name for the host book.
Member	Specifies the host entry member. Enter IP address or domain name in the Member text box and then click Add . If needed, you can add multiple host entries in the host book. Select the host entry you want to delete and click Delete , then the selected entry will be removed.
Description	Type the description of host book.

3. Click **OK**.

Service Book

Service is an information stream designed with protocol standards. Service has some specific distinguishing features, like corresponding protocol, port number, etc. For example, the FTP service uses TCP protocol, and its port number is 21. Service is an essential element for the configuration of multiple StoneOS modules including policy rules, NAT rules, QoS rules, etc.

System ships with multiple predefined services/service groups. Besides, you can also customize user-defined services/service groups as needed. All these service/service groups are stored in and managed by StoneOS service book.

Predefined Service/Service Group

System ships with multiple predefined services, and identifies the corresponding application types based on the service ports. The supported predefined services may vary from different Hillstone device models. Predefined service groups contain related predefined services to facilitate user configuration.

User-defined Service

Except for the above predefined services, you can also create your own user-defined services easily. The parameters that will be specified for the user-defined service entries include:

- Name
- Protocol type
- The source and destination port for TCP or UDP service, and the type and code value for ICMP service.

User-defined Service Group

You can organize some services together to form a service group, and apply the service group to StoneOS policies directly to facilitate management. The service group has the following features:

- Each service of the service book can be used by one or more service groups.
- A service group can contain both predefined services and user-defined services.
- A service group can contain another service group. The service group of StoneOS supports up to 8 layers of nests.

The service group also has the following limitations:

- The name of a service and service group should not be identical.
- A service group being used by any policy cannot be deleted. To delete such a service group, you must first end its relationship with the other modules.
- If a user-defined service is deleted from a service group, the service will also be deleted from all of the service groups using it.

Configuring a Service Book

This section describes how to configure a user-defined service and service group.

Configuring a User-defined Service

- 1. Select **Object > Service Book > Service**.
- 2. Click **New**.

Service Configuration

Service:

(1-95) chars

Member:

+ New

Edit

Delete

Protocol

Destination Port

Source Port

Description:


(0-255) chars

OK

Cancel

Configure the following options.

Service Configuration					
Service	Type the name for the user-defined service into the textbox.				
Member	<div><div>Specify a protocol type for the user-defined service. The available options include TCP, UDP, ICMP and Others. If needed, you can add multiple service items.</div><div>Click New and the parameters for the protocol types are described as follows:</div><div><table><tr><td>TCP/UDP</td><td><div><div>Destination port:</div><ul style="list-style-type: none">Min - Specifies the minimum port number of the specified service entry.Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535.<div>Source port:</div><ul style="list-style-type: none">Min - Specifies the minimum port number of the specified service entry.Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535.<div><div></div><div>Note: The minimum port number cannot exceed the maximum port number.</div></div></div></td></tr><tr><td>ICMP</td><td>Type: Specifies an ICMP type for the service entry. The value range is 3 (Destination-Unreachable), 4 (Source</td></tr></table></div></div>	TCP/UDP	<div><div>Destination port:</div><ul style="list-style-type: none">Min - Specifies the minimum port number of the specified service entry.Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535.<div>Source port:</div><ul style="list-style-type: none">Min - Specifies the minimum port number of the specified service entry.Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535.<div><div></div><div>Note: The minimum port number cannot exceed the maximum port number.</div></div></div>	ICMP	Type: Specifies an ICMP type for the service entry. The value range is 3 (Destination-Unreachable), 4 (Source
TCP/UDP	<div><div>Destination port:</div><ul style="list-style-type: none">Min - Specifies the minimum port number of the specified service entry.Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535.<div>Source port:</div><ul style="list-style-type: none">Min - Specifies the minimum port number of the specified service entry.Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535.<div><div></div><div>Note: The minimum port number cannot exceed the maximum port number.</div></div></div>				
ICMP	Type: Specifies an ICMP type for the service entry. The value range is 3 (Destination-Unreachable), 4 (Source				

Service Configuration	
	<p>Quench), 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp) and 15 (Information).</p> <p>Min Code: Specifies a minimum value for ICMP code. The value range is 0 to 5.</p> <p>Max Code: Specifies a maximum value for ICMP code. The value range is 0 to 5.</p> <div style="border: 1px solid #00a09a; padding: 10px; margin-top: 10px;">  <p>Note: The minimum port number cannot exceed the maximum port number.</p> </div>
	<p>Others Protocol: Specifies a protocol number for the service entry. The value range is 1 to 255.</p>
Description	If it's needed, type the description for the service into the text box.

3. Click **OK**.

Configuring a User-defined Service Group

- 1. Select **Object > Service Book > Service Group**.
- 2. Click **New**.

Service Group Configuration

Name: (1-31) chars

Description: (0-255) chars

Type: Service

Search

User-defined

Pre-defined

OK

Cancel

Configure the following options.

Service Group Configuration	
Name	Type the name for the user-defined service group into the text box.
Description	If needed, type the description for the service into the text box.
Member	<div>Add services or service groups to the service group. System supports at most 8-layer nested service group.</div> <div>Expand Pre-defined Service or User-defined Service from the left pane, select services or service groups, and then click Add to add them to the right pane. To remove a selected service, select it from the right pane,</div>

Service Group Configuration

and then click **Remove**.

3. Click **OK**.

Viewing Details

To view the details of a service entry, take the following steps, including the name, protocol, destination port and reference:

1. Click **Object>Service Book > Service**.
2. In the service dialog box, select an address entry from the member list, and view the details under the list.

Application Book

Application has some specific features, like corresponding protocol, port number, application type, etc. Application is an essential element for the configuration of multiple device modules including policy rules, NAT rules, application QoS management, etc.

System ships with multiple predefined applications and predefined application groups. Besides, you can also customize user-defined application and application groups as needed. All of these applications and applications groups are stored in and managed by StoneOS application book.

If IPv6 is enabled, IPv6 applications will be recognized by StoneOS.

Editing a Predefined Application

You can view and use all the supported predefined applications and edit TCP timeout, but cannot delete any of them. To edit a predefined application, take the following steps:

- 1. Select **Object > APP Book > Application**.
- 2. Select the application you want to edit from the application list, and click **Edit**.
- 3. In the Application Configuration dialog box, edit TCP timeout for the application.

Creating a User-defined Application

You can create your own user-defined applications. By configuring the customized application signature rules, system can identify and manage the traffic that crosses into the device, thus identifying the type of the traffic.

To create a user-defined application, take the following steps:

- 1. Select **Object > APP Book > Application**.
- 2. Click **New**.

The screenshot shows the 'User Defined Application Configuration' dialog box. It contains the following elements:

- Name:** A text input field with a character limit of (1-95) chars.
- Description:** A text input field with a character limit of (0-255) chars.
- Timeout:** A section with four rows, each for a protocol: TCP, UDP, ICMP, and Others. Each row has a checkbox, a numeric input field, and a unit dropdown menu (all currently set to 'second'). To the right of these are character limits: (1-65535) for each protocol and (1-65535) for Others.
- Signature:** A section with a list box and 'Add' and 'Remove' buttons.
- New Signature Rule:** A button at the bottom left of the Signature section.
- OK** and **Cancel** buttons at the bottom right.

Configure the following options.

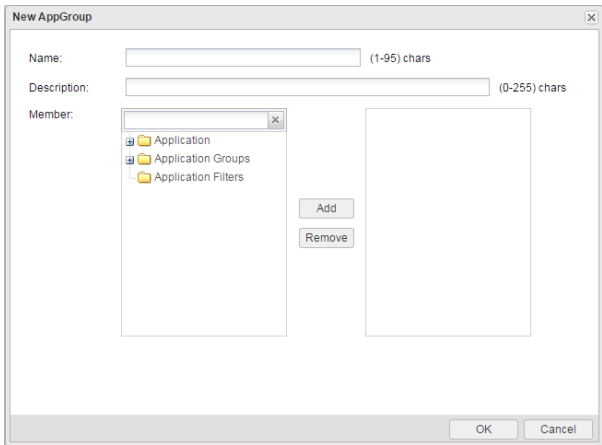
Option	Description
Name	Specify the name of the user-defined application.
Description	Specify the description of the user-defined application.
Timeout	Configure the application timeout value. If not, system will use the default value of the protocol.
Signature	Select the signature of the application and then click Add . To create a new signature, see " Creating a Signature Rule " on Page 242.

- 3. Click **OK**.

Creating a User-defined Application Group

To create a user-defined application group, take the following steps:

- 1. Select **Object > APP Book > Application Groups**
- 2. Click **New**.



Configure the following options.

Option	Description
Name	Specifies a name for the new application group.
Description	Specifies the description for the application group.
Member	<p>Add applications or application groups to the application group. System supports at most 8-layer nested application group.</p> <p>Expand Application or Application Group from the left pane, select applications or application groups, and then click Add to add them to the right pane. To remove a selected application or application group, select it from the right pane, and then click Remove.</p>

- 3. Click **OK**.

Creating an Application Filter Group

Application Filter Group allows you to create a group to filter applications according to application category, sub-category, technology, risk, and attributes.

To create an application filter group, take the following steps:

- 1. Select **Object > APP Book > Application Filters**.
- 2. Click **New**.
- 3. Type an application filter group name in the Name text box.
- 4. Specifies the filter condition. Choose the category, subcategory, technology, risk and characteristic by sequence in the drop-down list. You can click Clear Filter to clear all the selected filter conditions according to your need.
- 5. Click **OK**.

Creating a Signature Rule

By configuring the customized application signature rules, system can identify and manage the traffic that crosses into the device. When the traffic matches all of the conditions defined in the signature rule, it hits this signature rule. Then system identifies the application type.

If IPv6 is enabled, traffic of IPv6 address will be recognized by StoneOS.

To create a new signature rule, take the following steps:

- 1. Select **Object > APP Book > Signature Rule**.
- 2. Click **New**.

Signature Rule Configuration

Type

☒ IPv4☐ IPv6

Source

Zone:

Any

Address:

Destination

Address:

Protocol

☒ Enable

Type:

☒ TCP☐ UDP☐ ICMP☐ Others

Destination Port: Min:Max:

Source Port: Min:Max:

Action

App-Signature Rule:

☒ Enable

Continue Dynamic Identification:

☐ Enable

OK

Cancel

Configure the following options.

Option	Description
Type	Specify the IP address type, including IPv4 and IPv6 address. If IPv6 is enabled, traffic of IPv6 address will be recognized by StoneOS.
Source	
Zone	Specify the source security zone of the signature rule.
Address	Specify the source address. You can use the Address Book type or the IP/Netmask type.
Destination	
Address	Specify the source address. You can use the Address Book type or the IP/Netmask type.
Protocol	
Enable	Select the Enable check box to configure the protocol of the signature rule.
Type	<div>When selecting TCP or UDP,</div> <div><ul style="list-style-type: none">Destination Port: Specify the destination port number of the user-defined application signature. If the destination port number is within a range, system will identify the value of min-port as the minimum port number and identify the value of max-port as the maximum port number. The range of destination port number is 0 to 66535. The port number cannot be 0. For example, the destination port number is in the range of 0 to 20, but it cannot be 0.Source Port: Specify the source port number of the user-defined application signature. If the source port number is within a range, system will identify the value of min-port as the minimum port number and identify the value of max-port as the maximum port number. The range of source port number is 0 to 66535.</div> <div>When selecting ICMP:</div>

Option	Description
	<ul style="list-style-type: none"> Type: Specify the value of the ICMP type of the application signature. The options are as follows: 3 (Destination-Unreachable), 4 (Source Quench), 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp), 15 (Information), and any (any represents all of the above values). Min Code: Specify the value of the ICMP code of the application signature. The ICMP code is in the range of 0 to 5. The default value is 0-5. <p>When selecting Others:</p> <ul style="list-style-type: none"> Protocol: Specifies the protocol number of the application signature. The protocol number is in the range of 1 to 255.
Action	
App-Signature Rule	Select Enable to make this signature rule take effect after the configurations. Otherwise, it will not take effect.
Continue Dynamic Identification	Without selecting this check box, if the traffic satisfies the user-defined signature rule and system has identified the application type, system will not continue identifying the application. To be more accurate, you can select this check box to set the system to continue dynamically identification.

3. Click **OK**.

Viewing Details

To view the details of an application entry, including the name, category, risk and reference, take the following steps:

1. Click **Object>APP Book > Application**.
2. In the application dialog box, select an address entry from the member list, and view the details under the list.

SLB Server Pool

The SLB function uses the load balancing algorithm to distribute the traffic and this utilizes the resources of the intranet servers. You can use the following methods to balance the server load:

- Distribute the traffic to the specified port of each intranet server. This is applicable to the scenario that different intranet servers provide the same service via specified port at the same time.
- Distribute the traffic to different ports of an intranet server. This is applicable to the scenario that an intranet server provides the same service by running the same process at different ports.
- Combine the above two methods.

Configuring SLB Server Pool and Track Rule

To configure an SLB server pool and track rule, take the following steps:

1. Select **Object > SLB Server Pool**.
2. Click **New**. The SLB Server Pool Configuration dialog box appears.

The screenshot shows the 'SLB Server Pool Configuration' dialog box. It contains the following fields and controls:

- Name:** A text input field with a '(1-31)chars' hint.
- Algorithm:** A dropdown menu set to 'Weighted hashing'.
- Sticky:** A checkbox.
- Member:** A dropdown menu set to 'IP range'.
- Port:** A text input field with a '(1-65535)' hint.
- Maximum sessions:** A text input field with a '0' value and a '(0~1000000000)' hint.
- Weight:** A text input field with a '(1-255)' hint.
- Members List:** A table with columns 'Member', 'Port', 'Weight', and 'Maximum sessions'. It has 'Add' and 'Delete' buttons.
- Track:** A section with 'Track type' (set to 'PING') and 'Port' (with a '(1-65535)' hint).
- Buttons:** 'OK' and 'Cancel' at the bottom right.

In the SLB Server Pool Configuration dialog box, configure the following options.

Option	Description
Name	Specifies the name of the SLB server pool
Algorithm	Select an algorithm for load balancing.
Member	
Member	Specifies the member of the pool. You can type the IP range or the IP address and the netmask.
Port	Specifies the port number of the server.
Maximum Sessions	Specifies the allowed maximum sessions of the server. The value ranges from 0 to 1,000,000,000. The default value is 0, which represents no limitation.
Weight	Specifies the traffic forwarding weight during the load balancing. The value ranges from 1 to 255.
Add	Add the SLB address pool member to the SLB server pool. You can add up to 256 members.
Track	
Track Type	Selects a track type.
Port	Specifies the port number that will be tracked. The value ranges from 0 to 65535. <ul style="list-style-type: none">• When the members in the SLB server pool have the same IP address and different ports, you don't need to specify the port

Option	Description
	<p>when configuring the track rule. System will track each IP address and its port in the SLB server pool.</p> <ul style="list-style-type: none"> When there is a member whose port is not configured exists in the SLB sever pool, you must specify the port when configuring the track rule. System will track the specified port of the IP addresses in the SLB server pool. When the members in the SLB server pool are all configured with IP addresses and ports and these configured IP addresses are different from each other, you can select whether to specify the port when configuring the track rule. If specified, system will track the specified port of these IP addresses. If not, system will track the configured ports of the IP addresses of the members.
Interval	Specifies the interval between each Ping/TCP/UDP packet. The unit is second. The value ranges from 3 to 255.
Retries	Specifies a retry threshold. If no response packet is received after the specified times of retries, System will determine this track entry fails, i.e., the track entry is unreachable. The value range is 1 to 255.
Weight	Specifies a weight for the overall failure of the whole track rule if this track entry fails. The value range is 1 to 255.
Add	Click Add to add the configured track rule to the list.
Threshold	Types the threshold for the track rule into the Threshold box. The value range is 1 to 255. If the sum of weights for failed entries in the track rule exceeds the threshold, system will conclude that the track rule fails.
Description	Types the description for this track rule.

- Click **OK** to save the settings.

Viewing Details of SLB Pool Entries

To view the details of the servers in the SLB pool, take the following steps:

- Click **Object > SLB Server Pool**.
- Select an SLB pool entry.
- In the Server List tab at the bottom of this page, view the information of the servers that are in this SLB pool.
- In the Monitoring tab, view the information of the track rules.
- In the Referenced tab, view the DNAT rules that use the SLB pool.

Schedule

System supports a schedule. This function allows a policy rule to take effect in a specified time and controls the duration of the connection between a PPPoE interface and the Internet. The schedule consists of a periodic schedule and an absolute schedule. The periodic schedule specifies a time point or time range for periodic schedule entries, while the absolute schedule decides a time range in which the periodic schedule will take effect.

Periodic Schedule

Periodic schedule is the collection of periods specified by all of the schedule entries within the schedule. You can add up to 16 schedule entries to a periodic schedule. These entries can be divided into 3 types:

- Daily: The specified time of every day, such as Everyday 09:00 to 18:00.
- Days: The specified time of a specified day during a week, such as Monday Tuesday Saturday 09:00 to 13:30.
- Period: A continuous period during a week, such as from Monday 09:30 to Wednesday 15:00.

Absolute Schedule

An absolute schedule is a time range in which a periodic schedule will take effect. If no absolute schedule is specified, the periodic schedule will take effect as soon as it is used by some module.

Creating a Schedule

To create a schedule, take the following steps:

1. Select **Object > Schedule**.
2. Click **New**.

The screenshot shows the 'Schedule Configuration' dialog box. At the top, there is a 'Name' field with a placeholder '(1-31)chars'. Below this is the 'Days' section, which states 'Periodic schedule is the sum of time periods'. It contains a list box with a 'Time' entry, and 'Add' and 'Delete' buttons. The 'Timeframe' section explains that it is a range of time for the periodic schedule to take effect. It includes 'Start Time' and 'End Time' fields, each with a clock icon and a dropdown arrow. At the bottom are 'OK' and 'Cancel' buttons.

Configure the following options.

Schedule Configuration Dialog Box		
Name	Specifies a name for the new schedule.	
Add	Specifies a type for the periodic schedule in Add Periodic Schedules section.	
	Type	<ul style="list-style-type: none">• Daily - The specified time of every day. Click this radio button, and then, in the Time section, select a start time and end time from the Start time and End time drop-down list respectively.

Schedule Configuration Dialog Box		
		<ul style="list-style-type: none"> • Days - The specified time of a specified day during a week. Click this radio button, and then select a day/days in the Days and Time section, and finally select a start time and end time from the Start time and End time drop-down list respectively. • Period - A continuous period during a week. Click this radio button, and then in the Duration section select a start day/time and end day/time from the Start time and End time drop-down list respectively.
	Preview	Preview the detail of the configured periodic schedule in the Preview section.
Delete	Select the entry you want to delete from the period schedule list below, and click Delete .	
Absolute Schedule	The absolute schedule decides a time range in which the periodic schedule will take effect. Without configuring an absolute schedule, the periodic schedule will take effect as soon as it is used by some module.	

3. Click **OK**.

AAA Server

An AAA server is a server program that handles user requests to access computer resources, and for an enterprise, this server provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.

Here in StoneOS system, authentication supports the following five types of AAA server:

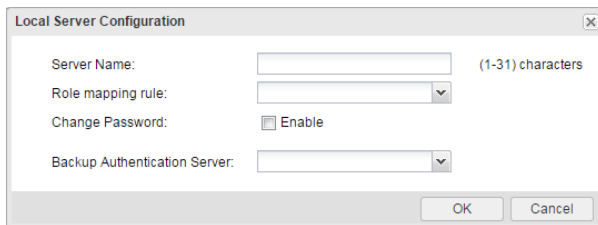
- Local server: a local server is the firewall itself. The firewall stores user identity information and handles requests. A local server authentication is fast and cheap, but its storage space is limited by the firewall hardware size.
- External servers:
 - [Radius Server](#)
 - [LDAP Server](#)
 - [Active-Directory Server](#)
 - [TACACS+ Server](#)

According to the type of authentication, you need to choose different AAA servers:

- "Single Sign-On" on Page 131: Only an AD server supports SSO.
- "802.1x" on Page 144 and "Configuring IPsec-XAUTH Address Pool" on Page 170: Only local and Radius servers support these two types of authentication.
- Other authentication methods mentioned in this guide: all four servers can support the other authentication methods.

Configuring a Local AAA Server

1. Select **Object > AAA Server**, and click **New > Local Server**.
2. The Local Server dialog box opens.



In the prompt, configure the following.

Option	Description
Server Name	Type the name for the new server into the text box.
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Change Password	If needed, select the Enable checkbox. With this function enabled, system allows users to change their own passwords after the successful WebAuth or SCVPN authentication.
Backup Authentication Server	To configure a backup authentication server, select a server from the drop-down list. After configuring a backup authentication server for the local server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails

Option	Description
	on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.

3. Click **OK**.

Configuring Radius Server

1. Select **Object > AAA Server**, and select **New > Radius Server**.
2. The Radius Sever dialog box opens.

In the prompt, configure the following.

Basic Configuration	
Server Name	Specifies a name for the Radius server.
Server Address	Specifies an IP address or domain name for the Radius server.
Virtual Router	Specifies a VR for the Radius server.
Port	Specifies a port number for the Radius server. The value range is 1024 to 65535. The default value is 1812.
Password	Specifies a password for the Radius server. You can specify at most 31 characters.
Optional	
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
Virtual Router-1/Virtual Router2	Specifies a VR for the backup server.
Retries	Specifies a retry time for the authentication packets sent to the AAA server. The value range is 1 to 10. The default value is 3.
Timeout	Specifies a timeout for the server response. The value range is 1 to 30 seconds. The default value is 3.
Backup Auth Server	Specifies a backup authentication server. After configuring a backup authentication server for the Radius server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.
Enable Account	Select the Enable Account checkbox to enable accounting for the Radius server, and then configure options in the sliding out area.
	Server Address Specifies an IP address or domain name for the accounting server.
	Virtual Router Specifies a VR for the accounting server.
	Port Specifies a port number for the accounting server. The value range is 1024 to 65535. The default value is 1813.
	Password Specifies a password for the accounting server.
	Confirm Password Enter the password again to confirm.
	Backup server 1/Backup server 2 Specifies an IP address or domain name for backup server 1 or backup server 2.
	Virtual Router1/Virtual Router2 Specifies a VR for the backup server.

3. Click **OK**.

Configuring Active Directory Server

1. Select **Object > AAA Server**, and then select **New > Active Directory Server**.
2. The Active Directory Server dialog box opens.

Active Directory Server Configuration

Basic Configuration:

Server Name:

(1-31) chars

Server Address:

(1-31) chars

Virtual Router:

trust-vr

Port:

389

(1-65535), default: 389

Base-dn:

(1-127) chars

Login-dn:

(0-255) chars

sAMAccountName:

(0-63) chars

Authentication Mode:

Plain Text

☒ MD5

Password:

(1-31) chars

Optional:

Role mapping rule:

Backup Server 1:

Domain/IP

Virtual Router 1:

Backup Server 2:

Domain/IP

Virtual Router 2:

Synchronization:

☒ Enable

Auto Synchronization:

☒ Interval Synchronization

☐ Daily Synchronization

☐ Once Synchronization

30

:

(30-1440)min, default: 30

Synchronous Operation Mode:

☒ Group Synchronization

☐ Organization Structure(OU) Synchronization

OU maximum depth:

12

(1-12), Default: 12

User Filter:

(0-120) chars ⓘ

Security Agent:

☐ Enable

When the security agent is enabled the system will perform single sign-on(SSO).

Agent Port:

6666

(1025-65535), default: 6666

Disconnection Timeout:

300

(0-1800)sec, default: 300

Backup Authentication Server:

Test Connectivity

OK

Cancel

In the prompt, configure the following.

Basic Configuration	
Server Name	Specifies a name for the Active Directory server.
Server Address	Specifies an IP address or domain name for the Active Directory server.
Virtual Router	Specifies a VR for the Active Directory server.
Port	Specifies a port number for the Active Directory server. The value range is 1 to 65535. The default value is 389.
Base-dn	<p>Specifies a Base-dn for the AD server. The Base-dn is the starting point at which your search will begin when the AD server receives an authentication request.</p> <p>For the example of abc.xyz.com as described above, the format for the Base-dn is "dc=abc,dc=xyz,dc=com".</p>
Login-dn	<p>Specifies authentication characteristics for the Login-dn (typically a user account with query privilege pre-defined by the AD server).</p> <p>When the authentication mode is plain, the Login-dn should be configured. DN (Distinguished name) is a username of the AD server who has a privilege to read user information. The format of the DN is "cn=xxx, DC=xxx,...". For example, the server domain is abc.xyz.com, and the AD server admin name is administrator who</p>

Basic Configuration	
	locates in Users directory. Then the login-dn should be "cn=a-administrator,cn=users,dc=abc,dc=xyz,dc=com".
sAMAccountName	<p>When the authentication mode is MD5, the sAMAccountName should be configured. sAMAccountName is a username of the AD server who has a privilege to read user information.</p> <p>The format of sAMAccountName is "xxx". For example, the AD server admin name is administrator , and then the sAMAccountName should be "administrator".</p>
Authentication Mode	<p>Specifies an authentication or synchronization method (either plain text or MD5). The default method is MD5.</p> <p>If the sAMAccountName is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating the user.</p>
Password	Specifies a password for the AD server.
Optional	
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for users who have been authenticated to the server according to the specified role mapping rule.
Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
Virtual Router1/Virtual Router2	Specifies a VR for the backup server.
Synchronization	Check the checkbox to enable the synchronization function; clear the checkbox to disable the synchronization function, and the system will stop synchronizing and clear the existing user information. By default, system will synchronize the user information on the configured Active-Directory server with the local server every 30 minutes.
Automatic Synchronization	Click the radio button to specify the automatic synchronization.
	<div>Interval Synchronization</div> <div>Specifies the time interval for automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.</div>
	<div>Daily Synchronization</div> <div>Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates hour and minute respectively.</div>
	<div>Once Synchronization</div> <div>If this parameter is specified, system will synchronize automatically when the configuration of Active-Directory server is modified. After executing this command , system will synchronize the user information immediately.</div>
Synchronous Oper-	Specifies user synchronization mode, including Group Syn-

Basic Configuration					
ation Mode	chronization and OU Synchronization. By default, the user information will be synchronized with the local server based on the group.				
OU maximum depth	<p>Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12.</p> <p>OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized with the local server.</p>				
User Filter	<p>Specifies the user-filter conditions. System can only synchronize and authenticate users that are in accordance with the filtering condition on the authentication server. The length is 0 to 120 characters. For example, if the condition is configured to "memberOf=CN=Admin,DC=test,DC=com" , system only can synchronize or authenticate user whose DN is "memberOf=CN=Admin,DC=test,DC=com" . The commonly used operators are: =(equals a value)、&(and) 、 (or)、!(not)、*(Wild-card: when matching zero or more characters)、~=(fuzzy query.)、>=Be greater than or equal to a specified value in lexicographical order.)、 <=(Be less than or equal to a specified value in lexicographical order.).</p>				
Security Agent	<p>Select the Enable check box to enable the Security Agent. With this function enabled, system will be able to obtain the mappings between the usernames of the domain users and IP addresses from the AD server, so that the domain users can gain access to network resources. In this way "Single Sign-On" on Page 131 is implemented. Besides, by making use of the obtained mappings, system can also implement other user-based functions, like security statistics, logging, behavior auditing, etc. To enable the Security Agent on the AD server, you first need to install and run the Security Agent on the server. Afterwards, when a domain user is logging in or logging off, the Security Agent will log the user's username, IP address, current time, and other information, and it will add the mapping between the username and the IP address to system. In this way the system can obtain every online user's IP address.</p>				
	<table><tr><td>Agent Port</td><td>Specify the monitoring port. StoneOS communicates with the AD Agent through this port. The range is 1025 to 65535. The default value is 6666. This port must be matched with the configured port of AD Agent, or system will fail to communicate with the AD Agent.</td></tr><tr><td>Disconnection Timeout</td><td>Specifies the disconnection timeout. The value range is 0 to 1800 seconds. The default value is 300. The value of 0 indicates never timeout.</td></tr></table>	Agent Port	Specify the monitoring port. StoneOS communicates with the AD Agent through this port. The range is 1025 to 65535. The default value is 6666. This port must be matched with the configured port of AD Agent, or system will fail to communicate with the AD Agent.	Disconnection Timeout	Specifies the disconnection timeout. The value range is 0 to 1800 seconds. The default value is 300. The value of 0 indicates never timeout.
	Agent Port	Specify the monitoring port. StoneOS communicates with the AD Agent through this port. The range is 1025 to 65535. The default value is 6666. This port must be matched with the configured port of AD Agent, or system will fail to communicate with the AD Agent.			
Disconnection Timeout	Specifies the disconnection timeout. The value range is 0 to 1800 seconds. The default value is 300. The value of 0 indicates never timeout.				
Backup Authentication Server	<p>Specifies a backup authentication server. After configuring a backup authentication server for the Radius server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.</p>				

3. Click **OK**.

Configuring LDAP Server

1. Select **Object > AAA Server**, and then select **New > LDAP Server**.
2. The LDAP Server dialog box opens.

LDAP Server Configuration

Basic Configuration:

Server Name:

(1-31) chars

Server Address:

(1-31) chars

Virtual Router:

trust-vr

Port:

389

(1-65535), default: 389

Base-dn:

(1-127) chars

Login-dn:

(0-255) chars

Authid:

(0-63) chars

Authentication Mode:

Plain Text

☒ MD5

Password:

(1-31) chars

Optional:

Role mapping rule:

Backup Server 1:

Domain/IP

Virtual Router 1:

Backup Server 2:

Domain/IP

Virtual Router 2:

Synchronization:

☒ Enable

Auto Synchronization:

☒ Interval Synchronization

30

(30-1440)min, default: 30

☐ Daily Synchronization

☐ Once Synchronization

Synchronous Operation Mode:

☒ Group Synchronization

☐ Organization Structure(OU) Synchronization

OU maximum depth:

12

(1-12), Default: 12

User Filter:

(0-120) chars ⓘ

Naming Attribute:

uid

(1-63) chars

Group Naming Attribute:

uid

(1-63) chars

Member Attribute:

uniqueMember

(1-63) chars

Group Class:

groupOfUniqueNames

(1-63) chars

Backup Authentication Server:

Test Connectivity

OK

Cancel

In the prompt, configure the following.

Basic Configuration	
Server Name	Specifies a name for the LDAP server.
Server Address	Specifies an IP address or domain name for the LDAP server.
Virtual Router	Specifies a VR for the LDAP server.
Port	Specifies a port number for the LDAP server. The value range is 1 to 65535. The default value is 389.
Base-dn	Specifies the details for the Base-dn. The Base-dn is the starting point at which your search will begin when the LDAP server receives an authentication request.
Login-dn	Specifies authentication characteristics for the Login-dn (typically a user account with query privileges pre-defined by the LDAP server).
Authid	Specifies the Authid, which is a string of 1 to 63 characters and is case sensitive.
Authentication Mode	<div>Specifies an authentication or synchronization method (either plain text or MD5). The default method is MD5.</div> <div>If the Authid is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating</div>

Basic Configuration							
	user.						
Password	Specifies a password for the LDAP server. This should correspond to the password for Admin DN.						
Optional							
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.						
Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.						
Virtual Router-1/Virtual Router2	Specifies a VR for the backup server.						
Synchronization	Check the checkbox to enable the synchronization function; clear the checkbox to disable the synchronization function, and system will stop synchronizing and clear the existing user information. By default, system will synchronize the user information on the configured LDAP server with the local every 30 minutes.						
Automatic Synchronization	<p>Click the radio button to specify the automatic synchronization.</p> <table> <tr> <td>Interval Synchronization</td><td>Specifies the time interval for automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.</td></tr> <tr> <td>Daily Synchronization</td><td>Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates hour and minute respectively.</td></tr> <tr> <td>Once Synchronization</td><td>If this parameter is specified, system will synchronize automatically when the configuration of LDAP server is modified. After executing this command, system will synchronize user information immediately.</td></tr> </table>	Interval Synchronization	Specifies the time interval for automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.	Daily Synchronization	Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates hour and minute respectively.	Once Synchronization	If this parameter is specified, system will synchronize automatically when the configuration of LDAP server is modified. After executing this command, system will synchronize user information immediately.
Interval Synchronization	Specifies the time interval for automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.						
Daily Synchronization	Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates hour and minute respectively.						
Once Synchronization	If this parameter is specified, system will synchronize automatically when the configuration of LDAP server is modified. After executing this command, system will synchronize user information immediately.						
Synchronous Operation Mode	Specifies the user synchronization mode, including Group Synchronization and OU Synchronization. By default, the user information will be synchronized with the local server based on the group.						
OU maximum depth	<p>Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12.</p> <p>OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized with the local server.</p>						
User Filter	Specifies the user filters. System can only synchronize and authenticate users that match the filters on the authentication server. The length is 0 to 120 characters. For example, if the condition is configured to "(&((objectclass=inetOrgperson)(objectclass=person)))", system only can synchronize or authenticate users which are defined as inetOrgperson or						

Basic Configuration	
	person. The commonly used operators are as follows: =(equals a value)、&(and) 、 (or)、!(not)、*(Wildcard: when matching zero or more characters)、~=(fuzzy query.)、>=(Be greater than or equal to a specified value in lexicographical order.)、<=(Be less than or equal to a specified value in lexicographical order.).
Naming Attribute	Specifies a naming attribute for the LDAP server. The default naming attribute is uid.
Group Naming Attribute	Specifies a naming attribute of group for the LDAP server. The default naming attribute is uid.
Member Attribute	Specifies a member attribute for the LDAP server. The default member attribute is uniqueMember.
Group Class	Specifies a group class for the LDAP server. The default class is groupofuniquenames.
Backup Authentication Server	Specifies a backup authentication server. After configuring a backup authentication server for the LDAP server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.

3. Click **OK**.

Configuring TACACS+ Server

1. Select **Object > AAA Server**.
2. Click **New > TACACS+ Server**, and the <TACACS+ Server Configuration> dialog box will appear.

TACACS+ Server Configuration

Basic Configuration:

Server Name: (1-31) chars

Server Address: (1-31) chars

Virtual Router: (dropdown)

Port: (1-65535), default: 49

Secret: (1-31) chars

Optional:

Role mapping rule: (dropdown)

Backup Server 1: Domain/IP

Virtual Router 1: (dropdown)

Backup Server 2: Domain/IP

Virtual Router 2: (dropdown)

Configure values in the <TACACS+ Server Configuration> dialog box.

Basic Configuration	
Server Name	Enter a name for the TACACS+ server.
Server Address	Specify the IP address or host name for the TACACS+ server.
Virtual Router	Specify the VRouter of TACACS+ server.
Port	Enter port number for the TACACS+ server. The default value is 49. The value range is 1 to 65535.
Secret	Enter the shared secret to connect the TACACS+ server.

Basic Configuration	
Confirm Secret	Re-enter the shared key.
Optional	
Role mapping rule	Select a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Backup Server 1 (2)	Enter the domain name or IP address for the backup TACACS+ server.
Virtual Router 1 (2)	Select the VRouter for the backup server.

Connectivity Test

When AAA server parameters are configured, you can test if they are correct by testing server connectivity.

To test server connectivity, take the following steps:

1. Select **Object > AAA Server**, and click **New**.
2. Select your AAA server type, which can be Radius, AD, LDAP or TACACS+. The local server does not need the connectivity test.
3. After filling out the fields, click **Test Connectivity**.
4. For Radius or TACACS+ server, enter a username and password in the popped <Test Connectivity> dialog box. If the server is AD or LDAP, the login-dn and secret is used to test connectivity.

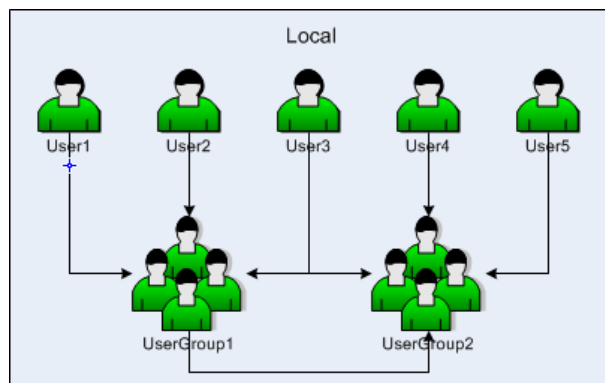
5. Click **Test Connectivity**. If "Test connectivity success" message appears, the AAA server settings are correct.

If there is an error message, here are the causes:

- Connect AAA server timeout: Wrong server address, port or virtual router.
- AAA server configuration error: Secret is wrong.
- Wrong name or password: Username or password for testing is wrong.

User

User refers to the user who uses the functions and services provided by the Hillstone device, or who is authenticated or managed by the device. The authenticated users consist of local user and external user. The local users are created by administrators. They belong to different local authentication servers, and are stored in system's configuration files. The external users are stored in external servers, such as AD server or LDAP server. System supports User Group to facilitate user management. Users belonging to one local authentication server can be allocated to different user groups, while one single user can belong to different user groups simultaneously; similarly, user groups belonging to one local authentication server can be allocated to different user groups, while one single user group can belong to different user groups simultaneously. The following diagram uses the default AAA server, Local, as an example and shows the relationship between users and user groups:



As shown above, User1, User2 and User3 belong to UserGroup1, while User3 also belongs to UserGroup2, and UserGroup2 also contains User4, User5 and UserGroup1.

Configuring a Local User

This section describes how to configure a local user and user group.

- Click the "Local server" drop-down box in the upper left corner of the page to switch the local user's server.
- Red **Expired**, orange **Will expire within a week** and yellow **Will expire within a month** colors are used to mark the expired users, expired within a week, expired within a month in the list.

Creating a Local User

To create a local user, take the following steps:

- Select **Object > User > Local User**.
- Click **New > User**.

User Configuration

Basic | VPN Options

Name: (1-63) chars

Password: (1-31) chars

Confirm Password:

Mobile + country code: (6-15) chars

Description: (0-127) chars

Group:

Expiration: ☐ Enable

If SMS authentication is enabled, SMS authentication code will be sent to the specified mobile phone.

In the Basic tab in User Configuration dialog box, configure the following.

Option	Description
Name	Specifies a name for the user.
Password	Specifies a password for the user.
Confirm password	Type the password again to confirm.
Mobile+country code	Specifies the user's mobile number. When users log into the SCVPN client, system will send the verification code to the mobile number.
Description	If needed, type the description of the user.
Group	Add the user to a selected usergroup. Click Choose , and in the Choose User Group dialog box, select the usergroup you want and click Add .
Expiration	Select the Enable check box to enable expiration for the user, and then specify a date and time. After expiration, the user cannot be authenticated, therefore cannot be used in system. By default expiration is not enabled.

In the VPN Options tab, configure network parameters for the PnPVPN client.

Option	Description
IKE ID	Specifies a IKE ID type for dial-up VPN users. If FQDN or ASN1 is selected, type the ID's content in the text box below.
DHCP Start IP	Specifies a start IP for the DHCP address pool.
DHCP End IP	Specifies an end IP for the DHCP address pool.
DHCP Netmask	Specifies a netmask for the DHCP address pool.
DHCP Gateway	Specifies a gateway for the DHCP address pool. The IP address of the gateway corresponds to the IP address of PnPVPN client's Intranet interface and PC's gateway address. The PC's IP address is determined by the segment and netmask configured in the above DHCP address pool. Therefore, the gateway's address and DHCP address pool should be in the same segment.

Option	Description
DNS1	Specifies an IP address for the DNS server. You can specify one primary DNS server (DNS1) and up to three alternative DNS servers.
DNS2	
DNS3	
DNS4	
WINS1	Specifies an IP address for the WINS server. You can specify one primary WINS server (WINS1) and one alternative WINS server.
WINS2	
Tunnel IP 1	Specifies an IP address for the master PnVPN client's tunnel interface. Select the Enable SNAT check box to enable SNAT.
Tunnel IP 2	Specifies an IP address for the backup PnVPN client's tunnel interface.

3. Click **OK**.

Creating a User Group

To create a user group, take the following steps:

1. Select **Object > User > Local User**.
2. Click **New > User Group**.
3. Type the name of the user group into the Name box.
4. Specify members for the user group. Expand User or User Group in the Available list, select a user or user group and click **Add** to add it to the Selected list on the right. To delete a selected user or user group, select it in the Selected list and then click **Remove**. One user group can contain multiple users or user groups, but system only supports up to 5 layers of nested user groups and does not support the loopback nest. Therefore, a user group should not nest the upper-layer user group it belongs to.
5. Click **OK**.

Import User Password List

Import user binding list to system, take the following steps:

1. Select **Object>User> Local User**.
2. Click **Import User Password List**, and the **Import User Password List** dialog box pops up.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK** to finish import.

Export User Password List

Export user binding list from system to local, take the following steps:

1. Select **Object>User> Local User**.
2. Click **Export User Password List**, and the **Export User Password List** dialog box pops up, and select the saved position in local.
3. Click **OK** to finish export.

**Note:**

- The user password in the import/export file is in encrypted text;.
- Please try to keep the import file format consistent with the export file.
- When importing, if the same user name exists under the same server, the original user password will be overwritten.

Configuring a LDAP User

This section describes how to configure a LDAP user.

Synchronizing Users

To synchronize users in a LDAP server, firstly, you need to configure a LDAP server, refer to ["Configuring LDAP Server" on Page 255](#). To synchronize users:

1. Select **Object > User > LDAP User**.
2. Select a server from the LDAP Server drop-down list, and click **Sync Users**.



Note: By default, after creating a LDAP server, system will synchronize the users of the LDAP server automatically, and then continue to synchronize every 30 minutes.

Configuring an Active Directory User

This section describes how to configure an active directory (AD) user.

Synchronizing Users

To synchronize users in an AD server to the device, first you need to configure an AD server, refer to ["Configuring Active Directory Server" on Page 252](#). To synchronize users, take the following steps:

1. Select **Object > User > AD User**.
2. Select an AD server from the Active Directory Server drop-down list, and click **Sync Users**.



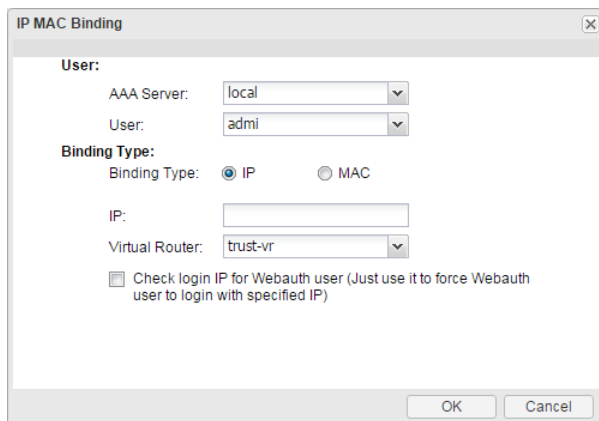
Note: By default, after creating an AD server, system will synchronize the users of the AD server automatically, and then continue to synchronize every 30 minutes.

Configuring a IP-User Binding

Adding User Binding

To bind an IP or MAC address to a user, take the following steps:

1. Select **Object > User > IP-User Binding** .
2. Click **Add User Binding**.



The dialog box is titled "IP MAC Binding". It contains the following fields and options:

- User:**
 - AAA Server: local (dropdown)
 - User: admi (dropdown)
- Binding Type:**
 - Binding Type: ☒ IP ☐ MAC
 - IP: (text box)
 - Virtual Router: trust-vr (dropdown)
 - ☐ Check login IP for Webauth user (Just use it to force Webauth user to login with specified IP)

At the bottom are "OK" and "Cancel" buttons.

Configure the following options.

User	
AAA Server	Select an AAA server from the drop-down list.
User	Select a user for the binding from the drop-down list.
Binding Type	
Binding Type	<p>By specifying the binding type, you can bind the user to a IP address or MAC address.</p> <ul style="list-style-type: none"> • IP - If IP is selected, type the IP address into the IP text box. And select a VR from the Virtual Router drop-down list. Select the Check WebAuth IP-User Mapping Relationship check box to apply the IP-User mapping only to the check for IP-user mapping during Web authentication if needed. • MAC - If MAC is selected, type the MAC address into the MAC text box. And select a VR from the Virtual Router drop-down list.

3. Click **OK**.

Import Binding

Import user binding list to system, take the following steps:

1. Select **Object>User> IP-User Binding**.
2. Click **Import** , and the **Import User Binding List** dialog box pops up.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK** to finish import.

Export Binding

Export user binding list from system to local, take the following steps:

1. Select **Object>User> IP-User Binding**.
2. Select the exported user category(include local,LDAP,AD and all users) in the **Export** drop-down list to pop up the export dialog box, and select the saved position in local.
3. Click **OK** to finish export.

Role

Roles are designed with certain privileges. For example, a specific role can gain access to some specified network resources, or make exclusive use of some bandwidth. In StoneOS, users and privileges are not directly associated. Instead, they are associated by roles.

The mappings between roles and users are defined by role mapping rules. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.

System supports role combination, i.e., the AND, NOT or OR operation on roles. If a role is used by different modules, the user will be mapped to the result role generated by the specified operation.

System supports the following role-based functions:

- Role-based policy rules: Implements access control for users of different types.
- Role-based QoS: Implements QoS for users of different types.
- Role-based statistics: Collects statistics on bandwidth, sessions and new sessions for users of different types.
- Role-based session limits: Implements session limits for specific users.
- SCVPN role-based host security detection: Implements control over accesses to specific resources for users of different types.
- Role-based PBR: Implements routing for users of different types.

Creating a Role

To create a role, take the following steps:

1. Select **Object > Role > Role**.
2. Click **New**.

Role Configuration

Role name:

(1~31) chars

Description:

(0~31) chars

OK

Cancel

Configure the following options.

Option	Description
Role Name	Type the role name into the Role Name box.
Description	Type the description for the role into the Description box.

3. Click **OK**.

Creating a Role Mapping Rule

To create a role mapping rule, take the following steps:

1. Select **Object > Role > Role Mapping** .
2. Click **New**.

3. Type the name for the rule mapping rule into the Name box.
4. In the Member section, select a role name from the first drop-down list, and then select a user, user group, certificate name (the CN field of USB Key certificate) or organization unit (the OU field of USB Key certificate) from the second drop-down list. If User, User group, CN or OU is selected, also select or enter the corresponding user name, user group name, CN or OU into the box behind.
5. Click **Add** to add to the role mapping list.
6. If needed, repeat Step 4 and Step 5 to add more mappings. To delete a role mapping, select the role mapping you want to delete from the mapping list, and click **Delete**.
7. Click **OK**.

Creating a Role Combination

To create a role combination, take the following steps:

1. Select **Object > Role > Role Combination**.
2. Click **New**.

Configure the following options.

Option	Description
First Prefix	Specifies a prefix for the first role in the role regular expression.
First Role	Select a role name from the First Role drop-down list to specify a name for the first role in the role regular expression.

Option	Description
Operator	Specifies an operator for the role regular expression.
Second Prefix	Specifies a prefix for the second role in the role regular expression.
Second Role	Select a role name from the Second Role drop-down list to specify a name for the second role in the role regular expression.
Result Role	Select a role name from the Result Role drop-down list to specify a name for the result role in the role regular expression.

3. Click **OK**.

Track Object

The devices provide the track object to track if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.

Creating a Track Object

To create a track object, take the following steps:

- 1. Select **Object > Track Object**.
- 2. Click **New**.

Configure the following options.

Option	Description
Name	Specifies a name for the new track object.
Threshold	Type the threshold for the track object into the text box. If the sum of weights for failed entries in the track object exceeds the threshold, system will conclude that the whole track object fails.
Track Type	<div>Select a track object type. One track object can only be configured with one type.</div> <div>Select Interface radio button:<ul style="list-style-type: none">Click Add in Add Track Members section and then configure the following options in the Add Interfaces dialog box:<ul style="list-style-type: none">Interface - Select a track interface from the drop-down list.Weight - Specifies a weight for the interface, i.e. the weight for overall failure of the whole track object if this track entry fails.</div> <div>Select HTTP Ping ARP DNS TCP radio button:<ul style="list-style-type: none">Click Add, select a packet type from the drop-down list, and then configure the following options in the Add HTTP/Ping/ARP/DNS/TCP Member dialog box:<ul style="list-style-type: none">IP/Host - Specifies an IP address or host name for the track object when the track is implemented by HTTP/Ping/TCP packets.</div>

Option	Description
	<p>IP - Specifies an IP address for the track object when the track is implemented by ARP packets.</p> <p>DNS - Specifies an IP address for the track object when the track is implemented by DNS packets.</p> <ul style="list-style-type: none"> • Weight - Specifies a weight for overall failure of the whole track object if this track entry fails. • Retries: Specifies a retry threshold. If no response packet is received after the specified times of retries, system will determine this track entry fails, i.e., the track entry is unreachable. The value range is 1 to 255. The default value is 3. • Interval - Specifies an interval for sending packets. The value range is 1 to 255 seconds. The default value is 3. • Egress Interface - Specifies an egress interface from which HTTP/Ping/ARP/DNS/TCP packets are sent. • Source Interface- Specifies a source interface for HTTP/Ping/ARP/DNS/TCP packets.
HA sync	Select this check box to enable HA sync function. The primary device will synchronize its information with the backup device.

3. Click **OK**.

Send Object

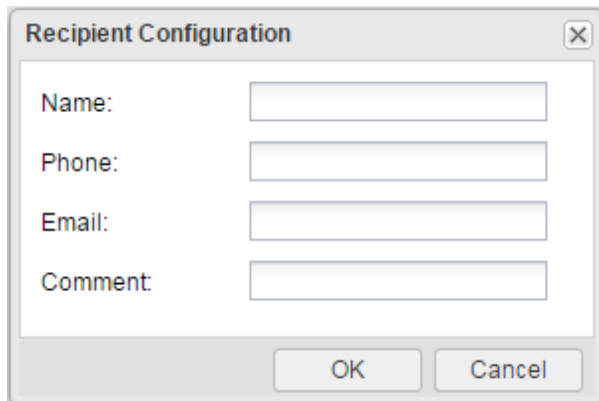
This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

After configuring the alarm rules, system will report the warning events to the recipient by sending a warning email or message. In the Send Object page , configure the recipient information.

Creating a Send Object

To create a send object, take the following steps:

1. Click **Object>Send Object**.
2. Click **New**.

A screenshot of a 'Recipient Configuration' dialog box. It has a title bar with a close button (X). Inside, there are four labeled text input fields: 'Name:', 'Phone:', 'Email:', and 'Comment:'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

In Recipient Configuration dialog box, configure the recipient information.

Option	Description
Name	Specify the recipient's name.
Phone	Specify the mobile phone number for receiving warning messages.
Email	Specify the email address for receiving warning emails.
Comment	Specify the comments of recipient.

Viewing Relevant Alarm Rules

In the Relevant Warning Rules window, you can view the warning rules that relate to a selected recipients after selecting recipients.

URL Filter

URL filter controls the access to some certain websites and records log messages for the access actions. URL filter helps you control the network behaviors in the following aspects:

- Access control to certain category of websites, such as gambling and pornographic websites.
- Access control to certain category of websites during the specified period. For example, forbid to access IM websites during the office hours.
- Access control to the website whose URL contains the specified keywords. For example, forbid to access the URL that contains the keyword of game.

If IPv6 is enabled, you can configure URL and keyword for both IPv4 and IPv6 address. How to enable IPv6, see [StoneOS_CLI_User_Guide_IPv6](#).

Configuring URL Filter

Configuring URL filter contains two parts:

- Create a URL filter rule
- Bind a URL filter rule to a security zone or policy rule

Part 1: Creating a URL filter rule

1. Select **Object > URL Filter**.
2. Click **New**.

The screenshot shows the 'URL Filter Rule Configuration' dialog box. It has a title bar with a close button. Inside, there's a 'Name:' field with a '(1-31) chars' hint. Below it are three radio buttons for 'Control Type': 'URL Category' (selected), 'URL Keyword Category', and 'Web Surfing Record'. There's an 'SSL Inspection:' section with an 'Enable' checkbox. A table with columns 'URL Category', 'Block', and 'Log' is present. The 'URL Category' column lists various categories like 'Advertisements & Pop-Ups', 'Alcohol & Tobacco', 'Anonymizers', 'Arts', 'Business', 'Transportation', 'Chat', 'Forums & Newsgroups', 'Compromised', and 'Computers & Technology'. The 'Block' and 'Log' columns have checkboxes for each category. At the bottom, there's an 'Other URLs:' section with 'Block Access' and 'Record Log' checkboxes. 'OK' and 'Cancel' buttons are at the bottom right.

URL Category	Block	Log
Advertisements & Pop-Ups	<input type="checkbox"/>	<input type="checkbox"/>
Alcohol & Tobacco	<input type="checkbox"/>	<input type="checkbox"/>
Anonymizers	<input type="checkbox"/>	<input type="checkbox"/>
Arts	<input type="checkbox"/>	<input type="checkbox"/>
Business	<input type="checkbox"/>	<input type="checkbox"/>
Transportation	<input type="checkbox"/>	<input type="checkbox"/>
Chat	<input type="checkbox"/>	<input type="checkbox"/>
Forums & Newsgroups	<input type="checkbox"/>	<input type="checkbox"/>
Compromised	<input type="checkbox"/>	<input type="checkbox"/>
Computers & Technology	<input type="checkbox"/>	<input type="checkbox"/>

In the **URL Filter Rule Configuration** dialog box, configure the following options.

Option	Description
Name	Specifies the name of the rule. You can configure the same URL filter rule name in different VSYSs.
Control Type	<p>Control types are URL Category, URL Keyword Category, and Web Surfing Record. You can select one type for each URL filter rule.</p> <p>URL Category controls the access to some certain category of website. The options are:</p> <ul style="list-style-type: none"> • SSL inspection: Select the Enable check box to enable SSL negotiation packets inspection. For HTTPS traffic, system can acquire the domain name of the site which you want to access from the SSL negotiation packets after this feature is configured. Then, system will perform URL filter in accordance with the domain name. If SSL proxy is configured at the same time, SSL negotiation packets inspection method will be preferred for URL filter. • New: Creates a new URL category. For more information about URL categories, see "User-defined URL DB" on Page 275. • Edit: Selects a URL category from the list, and click Edit to edit the selected URL category. • URL category: Shows the name of pre-defined and user-defined URL categories in the VSYS. • Block: Selects the check box to block access to the corresponding URL category. • Log: Selects the check box to log access to the corresponding URL category. • Other URLs: Specifies the actions to the URLs that are not in the list, including Block Access and Record Log. <p>URL Keyword Category controls the access to the website whose URL contains the specific keywords. Click the URL Keyword Category option to configure. The options are:</p> <ul style="list-style-type: none"> • New: Creates new keyword categories. For more information about keyword category, see "Keyword Category" on Page 278. • Edit: Select a URL keyword category from the list, and click Edit to edit the selected URL keyword categories. • Keyword category: Shows the name of the configured keyword categories. • Block: Selects the check box to block access to the website whose URL contains the specified keywords. • Log: Selects the check box to log the access to the website whose URL contains the specified keywords. • Other URLs: Specifies the actions to the URLs that do not contain the keywords in the list, including Block Access and Record Log.

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

Part 2: Binding a URL filter rule to a security zone or security policy rule

The URL filter configurations are based on security zones or policies.

- If a security zone is configured with the URL filter function, system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the URL filter function, system will perform detection on the traffic that is destined to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule are superior to that in a zone rule if they are specified at the same time, and the URL filter configurations in a destination zone are superior to that in a source zone if they are specified at the same time.
- To perform the URL filter function on the HTTPS traffic, see the policy-based URL filter.

To create the zone-based URL filter, take the following steps:

1. Create a zone. For more information about how to create this, refer to ["Security Zone" on Page 44](#).
2. In the Zone Configuration dialog box, select the Threat Protection tab.
3. Enable the threat protection that you need, and select the URL filter rules from the profile drop-down list below; you can click **Add Profile** from the profile drop-down list below to create a URL filter rule. For more information, see ["Part 1: Creating a URL filter rule" on Page 270](#).
4. Click **OK** to save the settings.

To create the policy-based URL filter, take the following steps:

1. Configure a security policy rule. For more information, see ["Configuring a Security Policy Rule" on Page 296](#).
2. In the Protection tab, select the **Enable** check box of URL Filter.
3. From the **Profile** drop-down list, select a URL filter rule. You can also click **Add Profile** to create a new URL filter rule.
4. To perform the URL filter function on the HTTPS traffic, you need to enable the SSL proxy function for this security policy rule. System will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the URL filter function on the decrypted traffic.

According to the various configurations of the security policy rule, system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled URL filter disabled	System decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the URL filter function on the decrypted traffic.
SSL proxy enabled URL filter enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filter function on the decrypted traffic.
SSL proxy disabled URL filter enabled	System performs the URL filter function on the HTTP traffic according to the URL filter profile. The HTTPS traffic will not be decrypted and system will transfer it.

If the SSL proxy and URL filter functions are enabled on a security policy rule but the control type of the selected URL filter rule is the Web surfing record, the system will not record the GET and POST methods and the posted contents via HTTPS.

If the zone which the security policy rule binds with is also configured with a URL filter, system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled URL filter disabled	URL filter enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filter function on the decrypted traffic according to the URL filter rule of the zone.
SSL proxy enabled URL filter enabled	URL filter enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filter function on the decrypted traffic according to the URL filter rule of the policy rule.
SSL proxy disabled URL filter enabled	URL filter enabled	System performs the URL filter function on the HTTP traffic according to the URL filter rule of the policy rule. The HTTPS traffic will not be decrypted and system will transfer it.

5. Click **OK** to save the settings.

If necessary, you can go on to configure the functions of ["Predefined URL DB" on Page 274](#), ["URL Lookup" on Page 277](#), and ["Warning Page" on Page 279](#).

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL categories.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database, including the URL category and the category type.
Warning Page	<ul style="list-style-type: none"> Block warning: When your network access is blocked, a warning page will prompt in the Web browser. Audit warning: When your network access is audited, a warning page will prompt in the Web browser.



Note:

- Only after cancelling the binding can you delete the URL filter rule.
- To get the latest URL categories, you are recommended to update the URL database first. For more information about URL database, see ["Predefined URL DB" on Page 274](#).

Viewing URL Hit Statistics

The URL access statistics includes the following parts:

- Summary: The statistical information of the top 10 user/IPs, the top 10 URLs, and the top 10 URL categories during the specified period of time are displayed.
- User/IP: The user/IP and detailed hit count are displayed.
- URL: The URL and detailed hit count are displayed.
- URL Category: The URL category and detailed hit count and traffic are displayed.

To view the URL hit statistics, see ["URL Hit" on Page 419](#) in Monitor.

Viewing Web Surfing Records

To view the Web surfing records, view "URL Logs" on Page 448. Before you view the Web surfing records, see "Log Configuration" on Page 451 to enable URL Log function.

Configuring URL Filter Objects

When using URL filter function, you need to configure the following objects:

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL categories.
User-defined URL DB	The user-defined URL database is defined by you and you can use it to specify the URL category.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword Category	Use the keyword category function to customize the keyword categories.
Warning Page	<ul style="list-style-type: none">Block warning: When your network access is blocked, a warning page will prompt in the Web browser.Audit warning: When your network access is audited, a warning page will prompt in the Web browser.

Predefined URL DB

System contains a predefined URL database.



Note: The predefined URL database is controlled by a license . Only after a URL license is installed, the predefined URL database can be used.

The predefined URL database provides URL categories for the configurations of a URL filter. It includes dozens of categories and tens of millions of URLs .

When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

Configuring Predefined URL Database Update Parameters

By default, system updates predefined URL database everyday. You can change the update parameters according to your own requirements. Currently, two default update servers are provided: update1.hillstonenet.com and update2.hillstonenet.com. Besides, you can update the predefined URL database from your local disk.

To change the update parameters, take the following steps:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the URL category database update section, you can view the current version of the database, perform the remote update, configure the remote update, and perform the local update.

URL Category Database Update

Current Version: 2.0.18

Remote Update:

☒ Enable Auto Update

Server 1: update1.hillstonenet.com Server 2: update2.hillstonenet.com Server 3:

Main Proxy Server: Port: Backup Proxy Server: Port:

Local Update:

3. Select **Enable Auto Update** to enable the automatic update function and then continue to specify the frequency and time. Click **OK** to save your settings.
4. Click **Configure Update Server** to configure the update server URL. In the pop-up dialog box, specify the URL or IP address of the update server, and select the virtual router that can connect to the server. To restore the URL settings to the default ones, click **Restore Default**.
5. Click **Configure Proxy Server**, then enter the IP addresses and ports of the main proxy server and the backup proxy server. When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature databases can update normally.
6. Click **OK** to save the settings.

Upgrading Predefined URL Database Online

To upgrade the URL database online, take the following steps:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the URL category database update section, click **Update** to update the predefined URL database.

Upgrading Predefined URL Database from Local

To upgrade the predefined URL database from local, take the following steps:

1. **System > Upgrade Management > Signature Database Update**
2. In the URL category database update section, click **Browse** to select the URL database file from your local disk.
3. Click **Upload** to update the predefined URL database.



Note: You can not upgrade the predefined URL database from local in non-root VSYS.

User-defined URL DB

Besides categories in predefined URL database, you can also create user-defined URL categories, which provides URL categories for the configurations of URL filter. When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL categories.



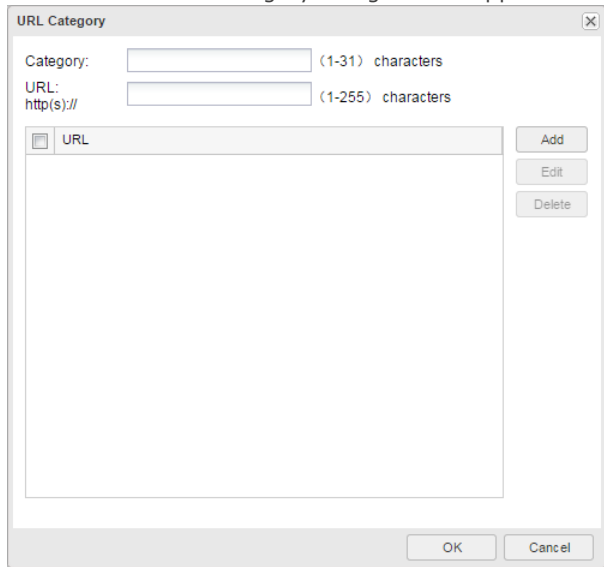
Note: You can not import your own URL lists into one of the predefined URL category in non-root VSYS.

Configuring User-defined URL DB

To configure a user-defined URL category, take the following steps:

1. Select **Policy > URL Filter**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.

3. Click **New**. The URL Category dialog box will appear.



4. Type the category name in the **Category** box. URL category name cannot only be a hyphen (-). And you can create at most 16 user-defined categories.
5. Type a URL into the **URL http://** box.
6. Click **Add** to add the URL and its category to the table.
7. To edit an existing one, select it and then click **Edit**. After editing it, click **Add** to save the changes.
8. Click **OK** to save the settings.

Importing User-defined URL

System supports to batch imported user-defined URL lists into the predefined URL category named custom1/2/3. To import user-defined URL, take the following steps:

1. Select **Object > URL Filter**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.
3. Select one of the predefined URL category(custom1/2/3), and then click **Import**.
4. In the Batch Import URL dialog box, click **Browse** button to select your local URL file. The file should be less than 1 M, and have at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address.
5. Click **OK** to finish importing.

Clearing User-defined URL

In the predefined URL category named custom1/2/3, clear a user-defined URL, take the following steps:

1. Select **Object > URL Filter**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.
3. Select one of the predefined URL categories(custom1/2/3), and then click **Clear**. The URL in the custom 1/2/3 will be cleared from the system.

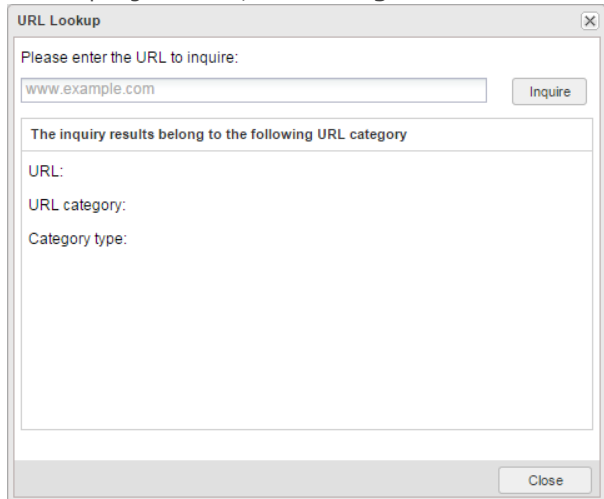
URL Lookup

You can inquire a URL to view the details by URL lookup, including the URL category and the category type.

Inquiring URL Information

To inquiry URL information, take the following steps:

1. Select **Policy > URL Filter**.
2. At the top-right corner, click **Configuration > URL Lookup**. The URL Lookup dialog box will appear.



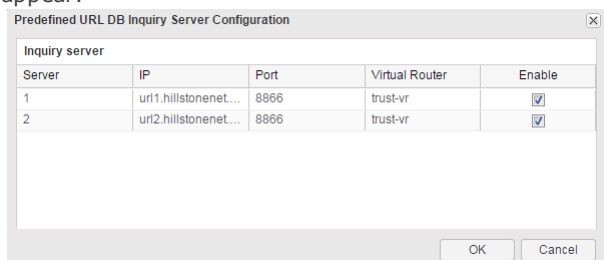
3. Type the URL into the **Please enter the URL to inquire** box.
4. Click **Inquire**, and the results will be displayed at the bottom of the dialog box.

Configuring URL Lookup Servers

URL lookup server can classify an uncategorized URL (URL is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. Two default URL lookup servers are provided: url1.hillstonenet.com and url2.hillstonenet.com. By default, the URL lookup servers are enabled.

To configure a URL lookup server, take the following steps:

1. Select **Policy > URL Filter**.
2. At the top-right corner, Select **Configuration > Predefined URL DB**. The Predefined URL DB dialog box will appear.
3. Click **Inquiry Server Configuration**. The Predefined URL DB Inquiry Server Configuration dialog box will appear.



Server	IP	Port	Virtual Router	Enable
1	url1.hillstonenet...	8866	trust-vr	<input checked="" type="checkbox"/>
2	url2.hillstonenet...	8866	trust-vr	<input checked="" type="checkbox"/>

4. In the Inquiry server section, double-click the cell in the IP/Port/Virtual Router column of Server1/2 and type a new value.

5. Select the check box in the **Enable** column to enable this URL lookup server.
6. Click **OK** to save the settings.

Keyword Category

You can customize the keyword category and use it in the URL filter function.

After configuring a URL filter rule, system will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of *times * trust value* of each keyword that belongs to the category. Then system compares the sum with the threshold 100 and performs the following actions according to the comparison result:

- If the sum is larger than or equal to category threshold (100), the configured category action will be triggered;
- If more than one category action can be triggered and there is block action configured, the final action will be Block;
- If more than one category action can be triggered and all the configured actions are Permit, the final action will be Permit.

For example, a URL filter rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

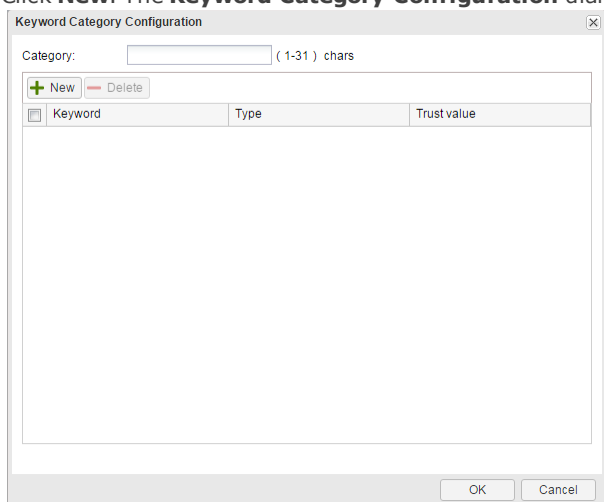
If system detects 1 occurrence of K1 and K2 each on a URL, then C1 trust value is $20*1 + 40*1 = 60 < 100$, and C2 trust value is $30*1 + 80*1 = 110 > 100$. As a result, the C2 action is triggered and the URL access is permitted.

If system detects 3 occurrences of K1 and 1 occurrence of K2 on a URL, then C1 trust value is $20*3 + 40*1 = 100$, and C2 trust value C2 is $30*3 + 80*1 = 170 > 100$. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.

Configuring a Keyword Category

To configure a keyword category, take the following steps:

1. Select **Policy > URL Filter**.
2. At the top-right corner, select **Configuration > Keyword Category**. The Keyword Category dialog box will appear.
3. Click **New**. The **Keyword Category Configuration** dialog box will appear.



4. Type the category name.

5. Click **New**. In the slide area, specify the keyword, character matching method (simple/regular expression), and trust value (100 by default).
6. Click **Add** to add the keyword to the list below.
7. Repeat the above steps to add more keywords.
8. To delete a keyword, select the keyword you want to delete from the list and click **Delete**.
9. Click **OK** to save your settings.

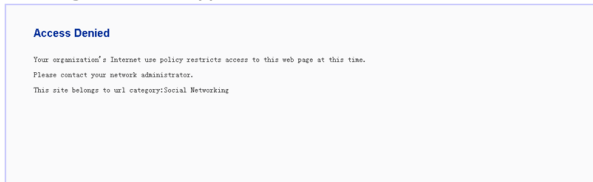
Warning Page

The warning page shows the user block information and user audit information.

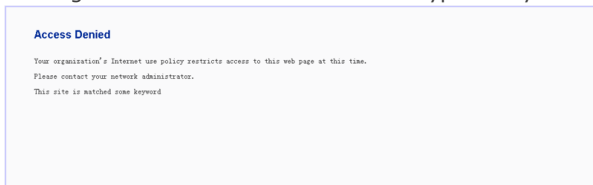
Configuring Block Warning

If the internet behavior is blocked by the URL filter function, the Internet access will be denied. The information of Access Denied will be shown in your browser, and some web surfing rules will be shown to you on the warning page at the same time. According to the different network behaviors, the default block warning page includes the following two situations:

- Visiting a certain type of URL.

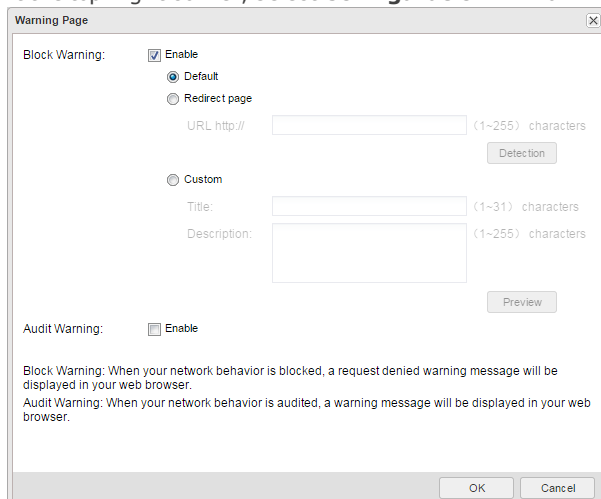


- Visiting the URL that contains a certain type of keyword category.



The block warning function is disabled by default. To configure the block warning function, take the following steps:

1. Click **Object > URL Filter**.
2. At the top-right corner, select **Configuration > Warning Page**. The Warning Page dialog box will appear.



3. In the Block Warning section, select **Enable**.

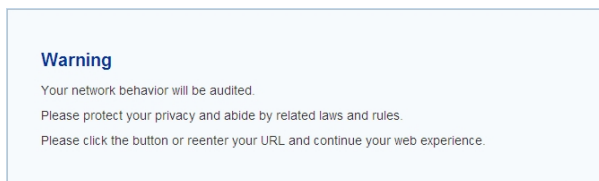
4. **Configure the display information in the blocking warning page.**

Option	Description
Default	Use the default blocking warning page as shown above.
Redirect page	Redirect to the specified URL. Type the URL in the URL http:// box. You can click Detection to verify whether the URL is valid.
Custom	Customize the blocking warning page. Type the title in the Title box and the description in the Description box. You can click Preview to preview the blocking warning page.

5. Click **OK** to save the settings.

Configuring Audit Warning

After enabling the audit warning function, when your network behavior matches the configured URL filter rule, your HTTP request will be redirected to a warning page where the audit and privacy protection information is displayed. See the picture below:



The audit warning function is disabled by default. To configure the audit warning function, take the following steps:

1. Select **Object > URL Filter**.

2. At the top-right corner, select **Configuration > Warning Page**. The Warning Page dialog box will appear.

3. In the Audit Warning section, select **Enable**.

4. **Configure the display information in the audit warning page.**

Option	Description
Default	Use the audit blocking warning page as shown above.
Custom	Customize the audit blocking warning page. Type the title in the Title box and the description in the Description box. You can click Preview to preview the audit warning page.

5. Click **OK** to save the settings.

Data Security

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

The data security function allows you to flexibly configure control rules to comprehensively control and audit (by behavior logs and content logs) on user network behavior.

Data security can audit and filter in the following network behaviors:

Function	Description
File filter	Checks the files transported through HTTP, FTP, SMTP, POP3 protocols and control them according to the file filter rules.
Network Behavior Record	Audits the IM applications behaviors and record log messages for the access actions.

Configuring Data Security Objects

When using the data security function, you need to configure the following objects for the data security rules:

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL DB	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword Category	Use the keyword category function to customize the keyword categories. You can use it to specify the keyword for the URL category/Web posting/email filter functions.
Warning Page	<ul style="list-style-type: none">Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser.Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
User Exception	Users that are not controlled by the internet behavior control rules.

Predefined URL DB

The system contains a predefined URL database.



Note: The predefined URL database is controlled by a license controlled. Only after a URL license is installed, the predefined URL database can be used.

The predefined URL database provides URL categories for the configurations of Web content/Web posting. It includes dozens of categories and tens of millions of URLs .

When identifying the URL category of a URL, the user-defined URL database has a higher priority than the predefined URL database.

Configuring Predefined URL Database Update Parameters

By default, the system updates predefined URL database everyday. You can change the update parameters according to your own requirements. Currently, two default update servers are provides: update1.hillstonenet.com and update2.hillstonenet.com. Besides, you can update the predefined URL database from your local disk.

To change the update parameters:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the URL category database update section, you can view the current version of the database, perform the remote update, configure the remote update, and perform the local update.

3. Select **Enable Auto Update** to enable the automatic update function. And then continue to specify the frequency and time. Click **OK** to save your settings.
4. Click **Configure Update Server** to configure the update server URL. In the pop-up dialog, specify the URL or IP address of the update server, and select the virtual router that can connect to the server. To restore the URL settings to the default ones, click **Restore Default**.
5. Click **Configure Proxy Server**, then enter the IP addresses and ports of the main proxy server and the backup proxy server. When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update normally.
6. Click **OK** to save the settings.

Upgrading Predefined URL Database Online

To upgrade the URL database online:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the URL category database update section, click **Update** to update the predefined URL database.

Upgrading Predefined URL Database from Local

To upgrade the predefined URL database from local:

1. **System > Upgrade Management > Signature Database Update**
2. In the URL category database update section, click **Browse** to select the URL database file from your local disk.
3. Click **Upload** to update the predefined URL database.

User-defined URL DB

Besides categories in predefined URL database, you can also create user-defined URL categories, which provides URL categories for the configurations of Web content/Web posting. When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

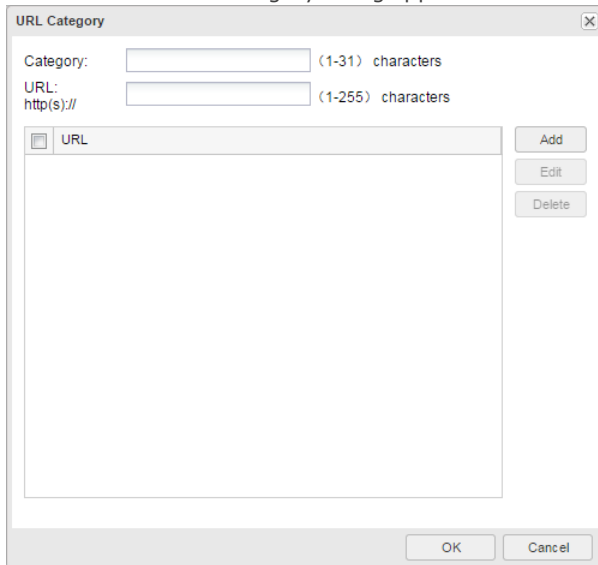
System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL category.

Configuring User-defined URL DB

To configure a user-defined URL category:

1. Select **Object >Data Security>Content Filter> Web Content/Web Posting**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.

3. Click **New**. The URL Category dialog appears.



4. Type the category name in the **Category** box. URL category name cannot only be a hyphen (-). And you can create at most 16 user-defined categories.
5. Type a URL into the **URL http://** box.
6. Click **Add** to add the URL and its category to the table.
7. To edit an existing one, select it and then click **Edit**. After editing it, click **Add** to save the changes.
8. Click **OK** to save the settings.

Importing User-defined URL

System supports to batch import user-defined URL lists into the predefined URL category named custom1/2/3. To import user-defined URL:

1. Select **Object > URL Filter**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.
3. Select one of the predefined URL category(custom1/2/3), and then click **Import**.
4. In the Batch Import URL dialog, click **Browse** button to select your local URL file. The file should be less than 1 M, and has at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address.
5. Click **OK** to finish importing.

Clearing User-defined URL

In the predefined URL category named custom1/2/3, clear user-defined URL:

1. Select **Object > URL Filter**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.
3. Select one of the predefined URL category(custom1/2/3), and then click **Clear**, the URL in the custom 1/2/3 will be cleared from the system.

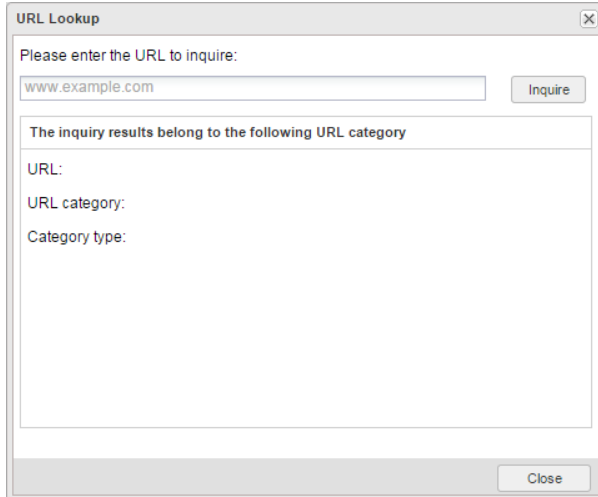
URL Lookup

You can inquire a URL to view the details by URL lookup, including the URL category and the category type.

Inquiring URL Information

To inquiry URL information:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting**.
2. At the top-right corner, click **Configuration > URL Lookup**. The URL Lookup dialog appears.



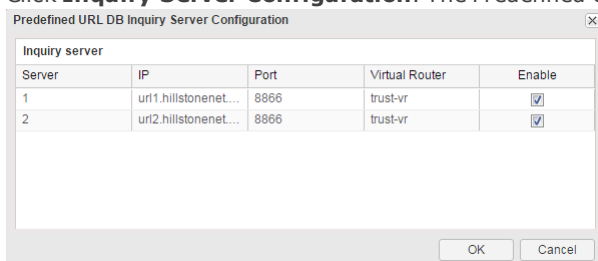
3. Type the URL into the **Please enter the URL to inquire** box.
4. Click **Inquire**, and the results will be displayed at the bottom of the dialog.

Configuring URL Lookup Servers

URL lookup server can classify an uncategorized URL (URL is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. Two default URL lookup servers are provided: url1.hillstonenet.com and url2.hillstonenet.com. By default, the URL lookup servers are enabled.

To configure a URL lookup server:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting**.
2. At the top-right corner, Select **Configuration > Predefined URL DB**. The Predefined URL DB dialog appears.
3. Click **Inquiry Server Configuration**. The Predefined URL DB Inquiry Server Configuration dialog appears.



Server	IP	Port	Virtual Router	Enable
1	url1.hillstonenet....	8886	trust-vr	<input checked="" type="checkbox"/>
2	url2.hillstonenet....	8886	trust-vr	<input checked="" type="checkbox"/>

4. In the Inquiry server section, double-click the cell in the IP/Port/Virtual Router column of Server1/2 and type a new value.

5. Select the check box in the **Enable** column to enable this URL lookup server.
6. Click **OK** to save the settings.

Keyword Category

You can customize the keyword category and use it in the internet behavior control function.

After configuring a internet behavior control rule, the system will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of *times* * *trust value* of each keyword that belongs to the category. Then the system compares the sum with the threshold 100 and performs the following actions according to the comparison result:

- If the sum is larger than or equal to category threshold (100), the configured category action will be triggered;
- If more than one category action can be triggered and there is block action configured, the final action will be Block;
- If more than one category action can be triggered and all the configured actions are Permit, the final action will be Permit.

For example, a web content rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

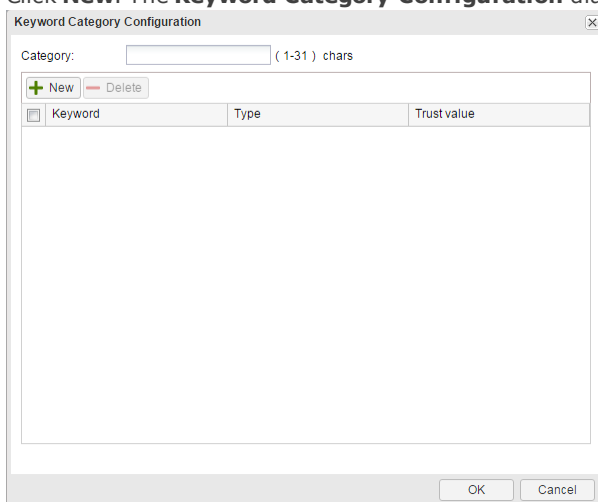
If the system detects 1 occurrence of K1 and K2 each on a web page, then C1 trust value is $20*1 + 40*1 = 60 < 100$, and C2 trust value is $30*1 + 80*1 = 110 > 100$. As a result, the C2 action is triggered and the web page access is permitted.

If the system detects 3 occurrences of K1 and 1 occurrence of K2 on a web page, then C1 trust value is $20*3 + 40*1 = 100$, and C2 trust value C2 is $30*3 + 80*1 = 170 > 100$. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.

Configuring a Keyword Category

To configure a keyword category:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter**.
2. At the top-right corner, Select **Configuration > Keyword Category**. The Keyword Category dialog appears.
3. Click **New**. The **Keyword Category Configuration** dialog appears.



4. Type the category name.

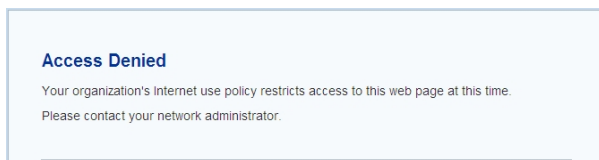
5. Click **New**. In the slide area, specify the keyword, character matching method (simple/regular expression), and trust value (100 by default).
6. Click **Add** to add the keyword to the list below.
7. Repeat the above steps to add more keywords.
8. To delete a keyword, select the keyword you want to delete from the list and click **Delete**.
9. Click **OK** to save your settings.

Warning Page

The warning page shows the user block information and user audit information.

Configuring Block Warning

If the internet behavior is blocked by the internet behavior control function, the Internet access will be denied. The information of Access Denied will be shown in your browser, and some web surfing rules will be shown to you on the warning page at the same time. See the picture below:

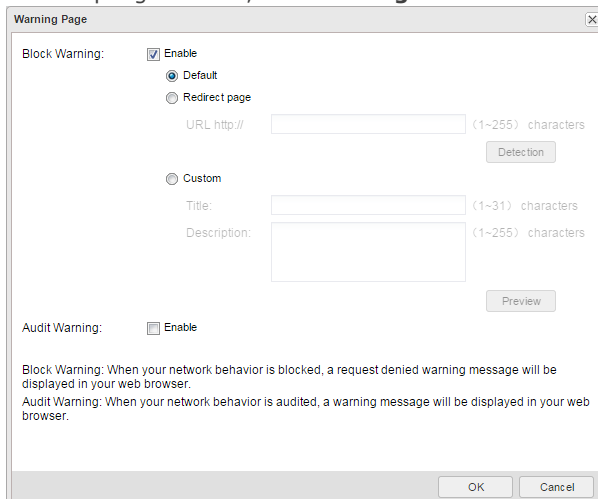


After enabling the block warning function, block warning information will be shown in the browser when one of the following actions is blocked:

- Visiting the web page that contains a certain type of keyword category
- Posting information to a certain type of website or posting a certain type of keywords
- HTTP actions of Connect, Get, Put, Head, Options, Post, and Trace. HTTP binary file download, such as .bat, .com. Downloading ActiveX and Java Applet.

The block warning function is enabled by default. To configure the block warning function:

1. Click **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > Warning Page**. The Warning Page dialog appears.



3. In the Block Warning section, select **Enable**.

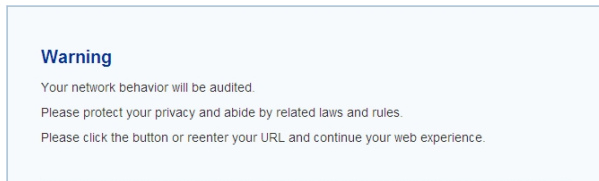
4. **Configure the display information in the blocking warning page.**

Option	Description
Default	Use the default blocking warning page as shown above.
Redirect page	Redirect to the specified URL. Type the URL in the URL http:// box. You can click Detection to verify whether the URL is valid.
Custom	Customize the blocking warning page. Type the title in the Title box and the description in the Description box. You can click Preview to preview the blocking warning page.

5. Click **OK** to save the settings.

Configuring Audit Warning

After enabling the audit warning function, when your internet behavior matches the configured internet behavior rules, your HTTP request will be redirected to a warning page, on which the audit and privacy protection information is displayed. See the picture below:



The audit warning function is disabled by default. To configure the audit warning function:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > Warning Page**. The Warning Page dialog appears.
3. In the Audit Warning section, select **Enable**.
4. Click **OK** to save the settings.

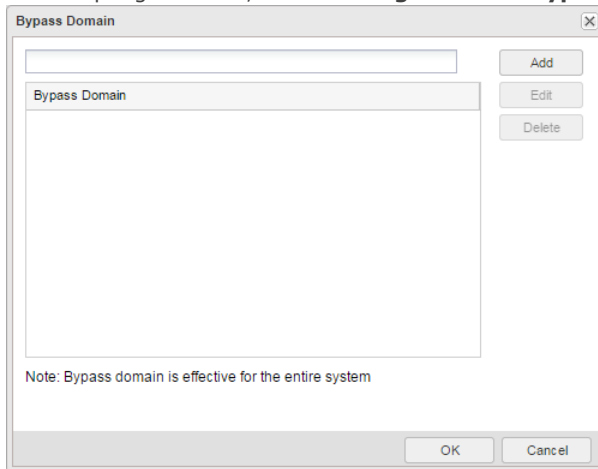
Bypass Domain

Regardless of internet behavior control rules, requests to the specified bypass domains will be allowed unconditionally.

To configure a bypass domain:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.

2. At the top-right corner, Select **Configuration > Bypass Domain**. The Bypass Domain dialog appears.



The Bypass Domain dialog box features a title bar with the text "Bypass Domain" and a close button (X). Below the title bar is a text input field. To the right of this field are three buttons: "Add", "Edit", and "Delete". Below the input field is a list box labeled "Bypass Domain". At the bottom of the dialog, there is a note that reads "Note: Bypass domain is effective for the entire system". At the very bottom are "OK" and "Cancel" buttons.

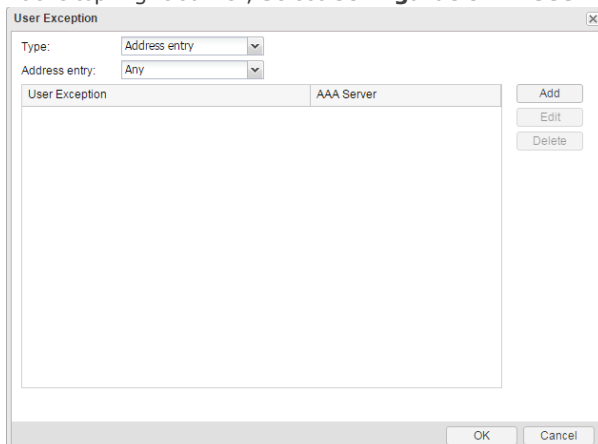
3. In the text box, type the domain name.
4. Click **Add**. The domain name will be added to the system and displayed in the bypass domain list.
5. Click **OK** to save the settings.

User Exception

The user exception function is used to specify the users who will not be controlled by the internet behavior control rules. The system supports the following types of user exception: IP, IP range, role, user, user group, and address entry.

To configure the user exception:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > User Exception**. The User Exception dialog appears.



The User Exception dialog box has a title bar with "User Exception" and a close button (X). It contains two dropdown menus: "Type:" with "Address entry" selected, and "Address entry:" with "Any" selected. Below these is a list box labeled "User Exception" which currently shows "AAA Server". To the right of the list box are "Add", "Edit", and "Delete" buttons. At the bottom are "OK" and "Cancel" buttons.

3. Select the type of the user from the **Type** drop-down list.
4. Configure the corresponding options.
5. Click **Add**. The user will be added to the system and displayed in the user exception list.
6. Click **OK** to save the settings.

File Filter

The file filter function checks the files transported through HTTP, FTP, SMTP, POP3 protocols and control them according to the file filter rules.

- Be able to check and control the files transported through GET and POST methods of HTTP, FTP, SMTP, and POP3.
- Support file type filter conditions.
- Support block, log, and permit actions.

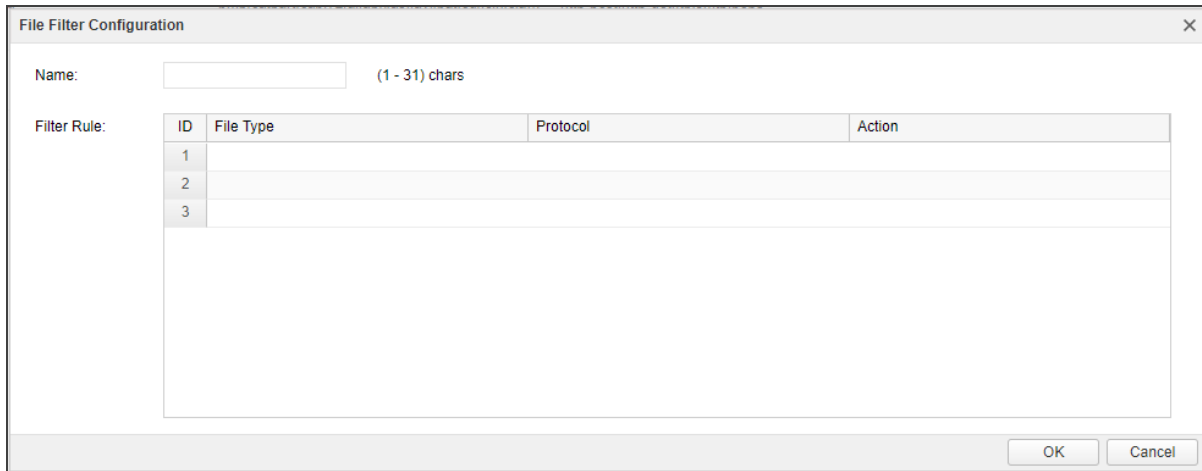
After you bind the file filter profile to a policy rule, the system will process the traffic that matches the rule according to the profile.

Creating File Filter Rule

Use the file filter rule to specify the protocol that you want to check, the filter conditions, and the actions.

To create a file filter rule:

1. Select **Object > Data Security > File Filter**.
2. Click **New**.



The dialog box titled "File Filter Configuration" contains a "Name:" label followed by a text input field and the text "(1 - 31) chars". Below this is a "Filter Rule:" label followed by a table. The table has four columns: "ID", "File Type", "Protocol", and "Action". The first three rows of the table are numbered 1, 2, and 3 in the "ID" column. The "File Type", "Protocol", and "Action" columns are empty for all three rows. At the bottom right of the dialog box are "OK" and "Cancel" buttons.

ID	File Type	Protocol	Action
1			
2			
3			

3. In the dialog box, enter values.

Option	Description
Name	Specifies the name of the file filter rule.
Filter Rule	
ID	The ID of file filter rule item. Each file filter rule contains 3 items. If one filter rule item is configured with the block action and the file happens to match this rule, then the system will block the uploading/downloading of this file.
File Type	<p>Specify the file type. Click on the column's cells and select from the drop-down menu. You can specify more than one file types. To control the file type that not supported, you can use the UNKNOWN type.</p> <p>When the transmitted file is a particular type, the system will trigger the actions. The file filter function can identify the following file types:</p> <p>7Z, AI, APK, ASF, AVI, BAT, BMP, CAB, CATPART, CDR, CIN, CLASS, CMD, CPL, DLL, DOC, DOCX, DPX, DSN, DWF, DWG, DXF, EDIT, EMF, EPS, EPUB, EXE, EXR, FLA, FLV, GDS, GIF, GZ, HLP, HTA, HTML, IFF, ISO, JAR, JPG, KEY, LNK, LZH, MA, MB, MDB, MDI, MIF, MKV, MOV, MP3, MP4, MPEG, MPKG, MSI, NUMBERS, OCX, PAGES, PBM, PCL, PDF, PGP, PIF, PL, PNG, PPT, PPTX, PSD, RAR, REG, RLA, RMVB, RPF, RTF, SGI, SH, SHK, STP, SVG, SWF, TAR, TDB, TIF, TORRENT, TXT, VBE, WAV, WEBM, WMA, WMF, WMV, WRI, WSF, XLS, XLSX, XML, XPM, ZIP, UNKNOWN</p>
Protocol	Specifies the protocols. http-get represents to check the files transported through the GET method of HTTP. http-post represents to check the files transported through the POST method of HTTP. ftp represents to check the files transported through FTP. smtp represents to check the files transported through SMTP. pop3 represents to check the files transported through POP3. You can specify more than one protocol types. This option is required.
Action	Specify the action to control the files that matches the filter conditions. You can specify block and log at the same time. This option is required.

4. Click **OK**.

Network Behavior Record

Network behavior record function audits the IM applications behaviors and record log messages for the access actions, includes:

- Audits the QQ, WeChat and sinaweibo user behaviors.
- Log the access behaviors.

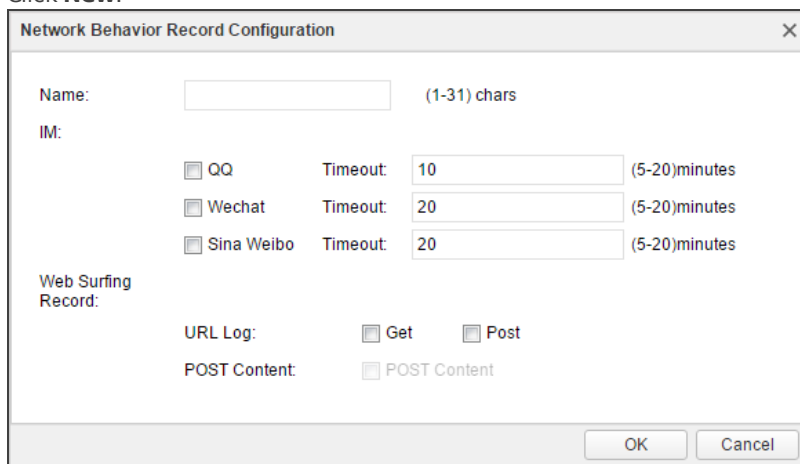
Configuring Network Behavior Recording

Configuring network behavior record contains two parts:

- Create a network behavior record rule
- Bind a network behavior record rule to a security zone or policy rule

Part 1: Creating a NBR rule

1. Select **Object > Data Security>Network Behavior Record**.
2. Click **New**.



The image shows a 'Network Behavior Record Configuration' dialog box. It has a title bar with a close button (X). The dialog contains the following fields and options:

- Name:** A text input field with a placeholder '(1-31) chars'.
- IM:** A section containing three rows of checkboxes and text input fields:
 - ☐ QQ Timeout: (5-20)minutes
 - ☐ Wechat Timeout: (5-20)minutes
 - ☐ Sina Weibo Timeout: (5-20)minutes
- Web Surfing Record:** A section containing two rows of checkboxes:
 - URL Log: ☐ Get ☐ Post
 - POST Content: ☐ POST Content

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

In the Network Behavior Record Configuration dialog box, enter values.

Option	Description
Name	Rule Name
IM	
QQ	<p>To audits the QQ behavior.</p> <ol style="list-style-type: none"> 1. Select the QQ checkbox. 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 10. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.
WeChat	<p>To audits the WeChat behavior.</p> <ol style="list-style-type: none"> 1. Select the Wechat checkbox. 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 20. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.
Sina Weibo	<p>To audits the sina weibo behavior.</p> <ol style="list-style-type: none"> 1. Select the Sina Weibo checkbox 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 20. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.
Web Surfing Record	
URL Log	<p>logs the GET and POST methods of HTTP.</p> <ul style="list-style-type: none"> • Get: Records the logs when having GET methods. • Post: Records the logs when having POST methods.
POST Content	Post Content: Records the posted content.

3. Click **OK**.

Part 2: Binding a network behavior record rule to a security zone or security policy rule

The network behavior record configurations are based on security zones or policies.

- If a security zone is configured with the network behavior record function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the network behavior record function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the network behavior record configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based network behavior record :

1. Create a zone. For more information about how to create, refer to ["Security Zone" on Page 44](#).
2. In the Zone Configuration dialog, select Data Security tab.
3. Enable the threat protection you need, and select a network behavior record rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create a network behavior record rule, see [Creating a network behavior record rule](#).
4. Click **OK** to save the settings.

To realize the policy-based network behavior record :

1. Configure a security policy rule. See ["Configuring a Security Policy Rule" on Page 296](#).
2. In the Data Security tab, select the **Enable** check box of network behavior record.
3. From the **Profile** drop-down list, select a network behavior record rule. You can also click **Add Profile** to create a new network behavior record rule.
4. Click **OK** to save the settings.



Note:

- You can export logs to a designated destination. Refer to ["Log Configuration" on Page 451](#)
- By default, a rule will immediately take effect after you click **OK** to complete configuration

Viewing Logs of Network Behavior Recording

To see the logs of network behavior recording, please refer to the ["Network Behavior Record Logs" on Page 450](#).

Chapter 10 Policy

The Policy module provides the following functions:

- Security policy: Security policy the basic function of devices that are designed to control the traffic forwarding between security zones/segments. By default all traffic between security zones/segments will be denied.
- NAT: When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets.
- QoS: QoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. QoS can assure the normal transmission of critical business traffic when the network is overloaded or congested.
- Session limit: The session limit function limits the number of sessions and controls the session rate to the source IP address, destination IP address, specified IP address, service, or role/user/user group, thereby protecting from DoS attacks and control the bandwidth of applications, such as IM or P2P.
- Global blacklist: After adding the IP addresses or services to the global blacklist, system will perform the block action to the IP address and service until the block duration ends.

Security Policy

Security policy is the basic function of devices that is designed to control the traffic forwarding between security zones/segments. Without security policy rules, the devices will deny all traffic between security zones/segments by default. After configuring the security policy rule, the device can identify what traffic between security zones or segments will be permitted, and the others will be denied.

The basic elements of policy rules:

- The source zone and address of the traffic
- The destination zone and address of the traffic
- The service type of the traffic
- Actions that the devices will perform when processing the specific type of traffic, including Permit, Deny, Tunnel, From tunnel, WebAuth, and Portal server.

Generally a security policy rule consists of two parts: filtering conditions and actions. You can set the filtering conditions by specifying traffic's source zone/address, destination zone/address, service type, and user. Each policy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a policy rule ID at your own choice. All policy rules in system are arranged in a specific order. When traffic flows into a device, the device will query for policy rules by turn, and processes the traffic according to the first matched rule.

The max global security policy rule numbers may vary in different models.

Security policy supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry for the policy rule.

This section contains the following contents:

- Configure a security policy rule
- View and search the security policy rules
- Manage the security policy rules: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, hit count check, and rule redundancy check.

Configuring a Security Policy Rule

To configure a security policy rule, take the following steps:



1. Select **Policy > Security Policy**.
2. At the top-left corner, click **New**. The Policy Configuration dialog box will appear.


The screenshot shows the 'Policy Configuration' dialog box with the 'Basic' tab selected. The dialog has four tabs: Basic, Protection, Data Security, and Options. The 'Basic' tab contains the following fields and options:

- Name:** A text input field with a placeholder '(0-95) chars'.
- Source:**
 - Zone:** A dropdown menu currently showing 'any'.
 - Address:** A dropdown menu currently showing 'any'.
 - User:** A dropdown menu.
- Destination:**
 - Zone:** A dropdown menu currently showing 'any'.
 - Address:** A dropdown menu currently showing 'any'.
- Service:** A dropdown menu currently showing 'any'.
- Application:** A dropdown menu.
- Action:** Three radio buttons: ☒ Permit, ☐ Deny, and ☐ Secured connection.
- Enable Web Redirect:** A checkbox that is currently unchecked.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

In the Basic tab, configure the corresponding options.

Option	Description
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware can configure the IPv6 type IP. If IPv6 is selected, all of the IP/netmask, IP range, and address entry should be configured in the IPv6 format.
Source Information	
Zone	Specifies a source zone.
Address	<p>Specifies the source addresses.</p> <ol style="list-style-type: none"> 1. After adding the desired addresses, click the blank area in this dialog box to complete the source address configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • When selecting the Address Book type, you can click Add to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the any check box.
User	<p>Specifies a role, user or user group for the security policy rule.</p> <ol style="list-style-type: none"> 1. From the User drop-down menu, select the AAA server where the users and user groups reside. To specify a role, select Role from the AAA Server drop-down list. 2. Based on the type of AAA server, you can execute one or more actions: search a user/user group/role, expand the user/user group list, enter the name of the user/user group. 3. After selecting users/user groups/roles, click  to add the them to the right pane. 4. After adding the desired objects, click the blank area in this dialog box to complete the user configuration.
Destination	
Zone	Specifies a destination zone.
Address	<p>Specifies the destination addresses.</p> <ol style="list-style-type: none"> 1. After adding the desired addresses, click the blank area in this dialog box to complete the destination address configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • When selecting the Address Book type, you can click Add to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the any check box.
Other Information	
Service	<p>Specifies a service or service group.</p> <ol style="list-style-type: none"> 1. From the Service drop-down menu, select a type: Service, Service Group. 2. You can search the desired service/service group, expand the service/service group list. 3. After selecting the desired services/service groups, click  to add them to the right pane.

Option	Description
	<p>4. After adding the desired objects, click the blank area in this dialog box to complete the service configuration.</p> <p>You can also perform other operations:</p> <ul style="list-style-type: none"> To add a new service or service group, click Add. The default service configuration is any. To restore the configuration to this default one, select the any check box.
Application	<p>Specifies an application/application group/application filters.</p> <ol style="list-style-type: none"> From the Application drop-down menu, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. After selecting the desired applications/application groups/application filters, click  to add them to the right pane. After adding the desired objects, click the blank area in this dialog box to complete the application configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> To add a new application group, click New AppGroup. To add a new application filter, click New AppFilter.
Action	
Action	<p>Specifies an action for the traffic that is matched to the policy rule, including:</p> <ul style="list-style-type: none"> Permit - Select Permit to permit the traffic to pass through. Deny - Select Deny to deny the traffic. WebAuth - Performs Web authentication on the matched traffic. Select WebAuth from the drop-down list after selecting the Security Connection option, and then select an authentication server from the following drop-down list. From tunnel (VPN) - For the traffic from a peer to local, if this option is selected, system will first determine if the traffic originates from a tunnel. Only such traffic will be permitted. Select From tunnel (VPN) from the drop-down list after selecting the Security Connection option, and then select a tunnel from the following drop-down list. Tunnel (VPN) - For the traffic from local to a peer, select this option to allow the traffic to pass through the VPN tunnel. Select Tunnel (VPN) from the drop-down list after selecting the Security Connection option, and then select a tunnel from the following drop-down list. Portal server - Performs portal authentication on the matched traffic. Select Portal server from the drop-down list after selecting the Security Connection option, and then type the URL address of the portal server.
Enable Web Redirect	<p>Enable the Web redirect function to redirect the HTTP request from clients to a specified page automatically. With this function enabled, system will redirect the page you are requesting over HTTP to a prompt</p>

Option	Description
	<p>page.</p> <ol style="list-style-type: none"> 1. Select the Enable Web Redirect check box. 2. Type a redirect URL into the Notification page URL box. <p>When using Web redirect function, you need to configure the Web authentication function. For more configurations, see "User Online Notification" on Page 305.</p>

In the Protection tab, configure the corresponding options.

Option	Description
Antivirus	Specifies an antivirus profile. The combination of security policy rule and antivirus profile enables the devices to implement fine-grained application layer policy control.
IPS	Specifies an IPS profile. The combination of security policy rule and IPS profile enables the devices to implement fine-grained application layer policy control.
Antispam	Specifies an anti-spam profile. The combination of security policy rule and anti-spam profile enables the devices to implement fine-grained application layer policy control.
URL Filter	Specifies a URL filter profile. The combination of security policy rule and URL filter profile enables the devices to implement fine-grained application layer policy control.
Sandbox	Specifies a sandbox profile. The combination of security policy rule and sandbox profile enables the devices to implement fine-grained application layer policy control.

In the Data Security tab, configure the corresponding options.

Option	Description
File Filter	Specifies a file filter profile. The combination of security policy rule and file filter profile enables the devices to implement fine-grained application layer policy control.
Content Filter	<ul style="list-style-type: none"> • Web Content: Specifies a web content profile. The combination of security policy rule and Web Content profile enables the devices to implement fine-grained application layer policy control. • Web Posting: Specifies a web posting profile. The combination of security policy rule and web posting profile enables the devices to implement fine-grained application layer policy control. • Email Filter: Specifies an email filter profile. The combination of security policy rule and email filter profile enables the devices to implement fine-grained application layer policy control. • HTTP/FTP Control: Specifies a HTTP/FTP control profile. The combination of security policy rule and HTTP/FTP control profile enables the devices to implement fine-grained application layer policy control.
Network Behavior Record	Specifies a NBR profile. The combination of security policy rule and NBR profile enables the devices to implement fine-grained application layer policy control.

In the **Options** tab, configure the corresponding options.

Option	Description
Schedule	Specifies a schedule when the security policy rule takes effect. Select a desired schedule from the Schedule drop-down list. This option supports fuzzy search. After selecting the desired schedules, click the blank area in this dialog box to complete the schedule configuration. To create a new schedule, click New Schedule .
QoS	Add the QoS tag to the matched traffic by typing the value into the box, which is used to control the traffic combined with the QoS. For more information about QoS configuration, see " Pipes " on Page 311 .
Log	You can log policy rule matching in the system logs according to your needs. <ul style="list-style-type: none"> For the policy rules of Permit, logs will be generated in two conditions: the traffic that is matched to the policy rules starts and ends its session. For the policy rules of Deny, logs will be generated when the traffic that is matched to the policy rules is denied. Select one or more check boxes to enable the corresponding log types. <ul style="list-style-type: none"> Deny - Generates logs when the traffic that is matched to the policy rules is denied. Session start - Generates logs when the traffic that is matched to the policy rules starts its session. Session end - Generates logs when the traffic that is matched to the policy rules ends its session.
SSL Proxy	Specifies a SSL proxy profile. The combination of security policy rule and SSL proxy profile enables the devices to decrypt the HTTPS traffic.
Position	Select a rule position from the Position drop-down list. Each policy rule is labeled with a unique ID or name. When traffic flows into a device, the device will query for the policy rules by turn, and processes the traffic according to the first matched rule. However, the policy rule ID is not related to the matching sequence during the query. The sequence displayed in policy rule list is the query sequence for policy rules. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name.
Description	Type descriptions into the Description box.

3. Click **OK** to save your settings.



Viewing and Searching Security Policy Rules

View the security policy rules in the policy rule list.



<div> <div> <div>New</div> <div>Edit</div> <div>Delete</div> <div>Copy</div> <div>Paste</div> <div>11 Move</div> </div> <div>Filter</div> </div>											
ID	Name	Source			Destination		Service	Application	Action	Session	Protection
		Zone	Address	User	Zone	Address					
1	a	any	any		any	any	any				
2	ab	any			any		any				

- Each column displays the corresponding configurations.
- Click the button under Session column in the Policy list, and then the Session Detail dialog box will appear. You

can view the current session status of the selected policy.

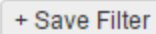

- Hover over your mouse on the configuration in a certain column. Then based on the configuration type, the WebUI displays either the  icon or the detailed configurations.
 - You can view the detailed configurations directly.
 - You can click the  icon. Based on the configuration type, the WebUI displays **Filter** or **Detail**. Click **Detail** to see the detailed configurations. Click **Filter** to all of the policy rules that have the same configuration as the one you are hovering over with your mouse.

Use the Filter to search for the policy rules that match the filter conditions.

1. Click **Policy > Security Policy**.
2. At the top-right corner, click **Filter**. Then a new row appears at the top.
3. Click **+Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value.
4. Press **Enter** to search for the policy rules that matches the filter conditions.
5. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.
6. To delete a filter condition, hover your mouse on that condition and then click the  icon. To close the filter, click the  icon on the right side of the row.

Source Zone:  Source: 

Save the filter conditions.

1. After adding the filter conditions, click the **+ Filter** after the next arrow, in the drop-down menu, click .
2. Specifies the name of the filter condition to save, the maximum length of name is 32 characters, and the name supports only Chinese and English characters and underscores.
3. Click the **Save** button on the right side of the text box.
4. To use the saved filter condition, double click the name of the saved filter condition.
5. To delete the saved filter condition, click  on the right side of the filter condition.



Note:

- You can add up to 20 filter conditions as needed.
- After the device has been upgraded, the saved filter condition will be cleared.

Managing Security Policy Rules

Managing security policy rules include the following matters: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, hit count check, and rule redundancy check.

Enabling/Disabling a Policy Rule

By default the configured policy rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule:

1. Select **Policy > Security Policy**.
2. Select the security policy rule that you want to enable/disable.
3. Click **More**, and then select **Enable** or **Disable** to enable or disable the rule.

The disabled rule will not display in the list. Click **More > Show Disabled Policies** to show them.

Cloning a Policy Rule

To clone a policy rule, take the following steps:

1. Select **Policy > Security Policy**.
2. Select the security policy rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up, select the desired position. Then the rule will be cloned to the desired position.

Adjusting Security Policy Rule Position

To adjust the rule position, take the following steps:

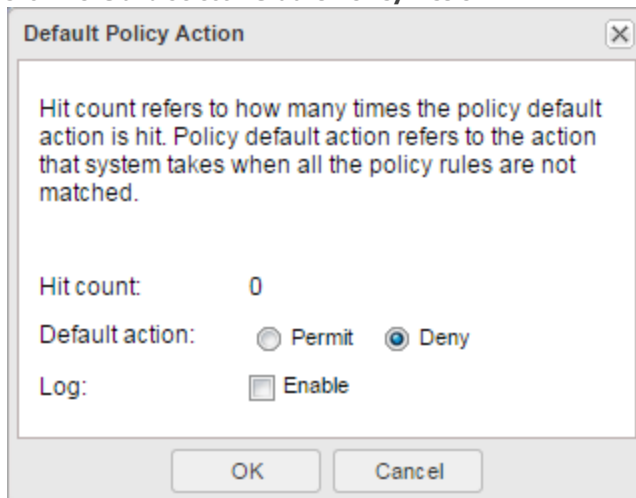
1. Select **Policy > Security Policy**.
2. Select the check box of the security policy whose position will be adjusted.
3. Click **Move**.
4. In the pop-up menu, type the rule ID or name, and click **Before ID**, **After ID**, **Before Name** or **After Name**. Then the rule will be moved before or after the specified ID or name.

Configuring Default Action

You can specify a default action for the traffic that is not matched with any configured policy rule. System will process the traffic according to the specified default action. By default system will deny such traffic.

To specify a default policy action, take the following steps:

1. Select **Policy > Security Policy**.
2. Click **More** and select **Default Policy Action**.



In the **Default Policy Action** dialog box, configure the following options.

Option	Description
Hit count	Shows the statistics on policy matching.
Default action	Specify a default action for the traffic that is not matched with any configured policy rule. <ul style="list-style-type: none">Click Permit to permit the traffic to pass through.Click Deny to deny the traffic.
Log	Configure to generate logs for the traffic that is not matched with any configured policy rule. By default system will not generate logs for such traffic. To enable log, select the Enable check box, and system will generate logs for such traffic.

- Click **OK** to save your changes.

Viewing and Clearing Policy Hit Count

System supports statistics on policy hit counts, i.e., statistics on the matching between traffic and policy rules. Each time the inbound traffic is matched with a certain policy rule, the hit count will increase by 1 automatically.

To view a policy hit count, click **Policy > Security Policy**. In the policy rule list, view the statistics on policy hit count under the Hit Count column.

To clear a policy hit count, take the following steps:

- Select **Policy > Security Policy**.
- Click **More** and select **Clearing Policy Hit Count**.

In the **Clearing Hit Count** dialog box, configure the following options.

Option	Description
All policies	Clears the hit counts for all policy rules.
Default policy	Clears the hit counts for the default action policy rules.
Policy ID	Clears the hit counts for a specified ID policy rule.
Name	Clears the hit counts for a specified name policy rule.

- Click **OK** to perform the hit count clearing.

Hit Count Check

System supports to check policy rule hit counts.

To check hit count, take the following steps:

- Select **Policy > Security Policy**.
- Click **More** and select **Hit Count Check**. After the check, the policy rules whose hit count is 0 will be highlighted. That means that the policy rule is not used in system.


Rule Redundancy Check

In order to make the rules in the policy effective, system provides a method to check the conflicts among rules in a policy. With this method, administrators can check whether the rules overshadow each other.

To start a rule redundancy check, take the following steps:

- Select **Policy > Security Policy**.
- Click **More** and select **Redundancy Check**. After the check, system will highlight the policy rule which is overshadowed.









Note: Status will be shown below the policy list when redundancy check is started. It is not recommended to edit a policy rule during the redundancy check. You can click  to stop the check manually.

Schedule Validity Check

In order to make sure that the policies based on schedule are effective, system provides a method to check the validity of policies. After checking the policy, the invalid policies based on schedule will be highlighted by yellow.

To check schedule validity:

1. Select **Policy > Security Policy** to enter the **Security Policy** page.
2. Click **More** and select **Schedule Validity Check**. After check, system will highlight the invalid policy based on schedule by yellow. Meanwhile, you can view the validity status in the policy list.

+ New Edit Delete Copy Paste Move More												
ID	Source			Destination		Service	Application	Action	Session	Protection	Options	Description
	Zone	Address	User	Zone	Address							
1	any	any		any	any	any						
6	any	any		any	any	any						

Showing Disabled Policies

To show disabled policies:

1. Select **Policy > Security Policy** to enter the **Security Policy** page.
2. Click **More** and select **Show Disabled Policies**. The disabled policies will be highlighted by green in the policy list.

+ New Edit Delete Copy Paste Move More													
ID	Source			Destination		Service	Application	Action	Session	Protection	Options	Description	Hit Count
	Zone	Address	User	Zone	Address								
1	any	any		any	any	any							0
2	any	any		any	any	any							0
3	any	any		any	any	any							0



Note:

- By default(the "Schedule Validity Check" and "Show Disabled Policies" are not selected), the policy list only displays the enabled policies which are not highlighted.
- When you select both "Schedule Validity Check" and "Show Disabled Policies", the policy is managed as follows:
 - The policy list will display the "Validity" column, which shows the validity status of policies.
 - The invalid policy based on schedule will be highlighted by yellow no matter if the policy is disabled or not.
 - If the valid policy based on schedule is disabled, it will be highlighted by green.

User Online Notification

The system provides the policy-based user online notification function. The user online notification function integrates WebAuth function and Web redirect function.

After configuring the user online notification function, system redirects your HTTP request to a new notification page when you visit the Internet for the first time. In the process, a prompt page (see the picture below) will be shown first, and after you click **continue** on this page, system will redirect your request to the specified notification page. If you want to visit your original URL, you need to type the URL address into the Web browser.



Before you enable the user online notification function, you must configure the WebAuth function. For more information about configuring WebAuth function, view ["Web Authentication" on Page 124](#).

Configuring User Online Notification

To configure the user online notification function, take the following steps:

1. Select **Policy > Security Policy**.
2. Select the security policy rule with which you want to enable the user online notification function. Generally, it is recommended to select the security policy rule which is under the WebAuth policy rule and whose action is permit to transmit the HTTP traffic.
3. Click **Edit**.
4. In the Basic tab, select the **Enable Web Redirect** check box and type the notification URL into the **Notification page URL** box.
5. Click **OK** to save the settings.

Configuring the Parameters of User Online Notification

The parameters are:

- Idle time: The time that an online user stays online without traffic transmitting. If the idle time is exceeded, the HTTP request will be redirected to the user online notification page again.
- Background picture: You can change the background picture on the prompt page.

To configure the parameters, take the following steps:

1. Select **Policy > Security Policy**.
2. Select the security policy rule with the user online notification function enabled.
3. Click **More** and select **Web Redirect Configuration**.
4. Type the idle time value into the **Idle time** box. The default value is 30 minutes. The range is 3 to 1440 minutes.

5. Change the background picture of the prompt page. Click **Browse** to choose the picture you want, and then click **Upload**. The uploaded picture must be zipped and named as web_redirect_bg_en.gif, with the size of 800px*600px.

Viewing Online Users

After configuring the user online notification function, you can get the information of online users from the Online Notification Users dialog box.

1. Select **Policy > Security Policy**.
2. Click **More** and select **Web Redirect IP List**.
3. **In the Web Redirect IP List dialog box, view the following information.**

Option	Description
IP address	The IP address of the online user.
Session number	Session number of the online user.
Interface	The source interface of the online user.
Lifetime (s)	The period of time during which the user is staying online.
Expiration (s)	The idle time of the user.

iQoS

System provides iQoS (intelligent quality of service) which guarantees the customer's network performance, manages and optimizes the key bandwidth for critical business traffic, and helps the customer greatly in fully utilizing their bandwidth resources.

iQoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. iQoS can assure the normal transmission of critical business traffic when the network is over-loaded or congested. iQoS is controlled by license. To use iQoS, apply and install the iQoS license.



Note: If you have configured QoS in the previous QoS function before upgrading the system to version 5.5, the previous QoS function will take effect. You still need to configure the previous QoS function in CLI. You cannot use the newest iQoS function in version 5.5 and the newest iQoS function will not display in the WebUI and will not take effect. If you have not configured the previous QoS function before upgrading the system to version 5.5, the system will enable the newest iQoS function in version 5.5. You can configure iQoS function in the WebUI and the previous QoS function will not take effect.

Implement Mechanism

The packets are classified and marked after entering system from the ingress interface. For the classified and marked traffic, system will smoothly forward the traffic through the shaping mechanism, or drop the traffic through the policing mechanism. If the shaping mechanism is selected to forward the traffic, the congestion management and congestion avoidance mechanisms will give different priorities to different types of packets so that the packets of higher priority can pass through the gateway earlier to avoid network congestion.

In general, implementing QoS includes:

- Classification and marking mechanism: Classification and marking is the process of identifying the priority of each packet. This is the first step of iQoS.
- Policing and shaping mechanisms: Policing and shaping mechanisms are used to identify traffic violation and make responses. The policing mechanism checks the traffic in real time and takes immediate actions according to the settings when it discovers a violation. The shaping mechanism works together with queuing mechanism. It makes sure that the traffic will never exceed the defined flow rate so that the traffic can go through that interface smoothly.
- Congestion management mechanism: Congestion management mechanism uses the queuing theory to solve problems in the congested interfaces. As the data rate can be different among different networks, congestion may happen to both wide area network (WAN) and local area network (LAN). Only when an interface is congested will the queuing theory begin to work.
- Congestion avoidance mechanism: Congestion avoidance mechanism is a supplement to the queuing algorithm, and it also relies on the queuing algorithm. The congestion avoidance mechanism is designed to process TCP-based traffic.

Pipes and Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes.

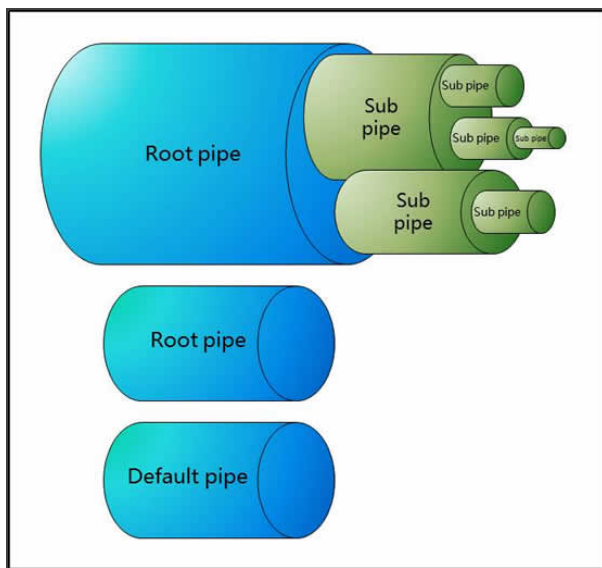
Pipes

By configuring pipes, the devices implement iQoS. Pipe, which is a virtual concept, represents the bandwidth of transmission path. System classifies the traffic by using the pipe as the unit, and controls the traffic crossing the pipes according to the actions defined for the pipes. For all traffic crossing the device, they will flow into virtual pipes according to the traffic matching conditions they match. If the traffic does not match any condition, they will flow into the default pipe predefined by the system.

Pipes, except the default pipe, include two parts of configurations: traffic matching conditions and traffic management actions:

- **Traffic matching conditions:** Defines the traffic matching conditions to classify the traffic crossing the device into matched pipes. System will limit the bandwidth to the traffic that matches the traffic matching conditions. You can define multiple traffic matching conditions to a pipe. The logical relation between each condition is OR. When the traffic matches a traffic matching condition of a pipe, it will enter this pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list in the Policy > iQoS page.
- **Traffic management actions:** Defines the actions adopted to the traffic that has been classified to a pipe. The data stream control includes the forward control and the backward control. Forward control controls the traffic that flows from the source to the destination; backward control controls the traffic flows from the destination to the source.

To provide flexible configurations, system supports the multiple-level pipes. Configuring multiple-level pipes can limit the bandwidth of different applications of different users. This can ensure the bandwidth for the key services and users. Pipes can be nested to at most four levels. Sub pipes cannot be nested to the default pipe. The logical relation between pipes is shown as below:

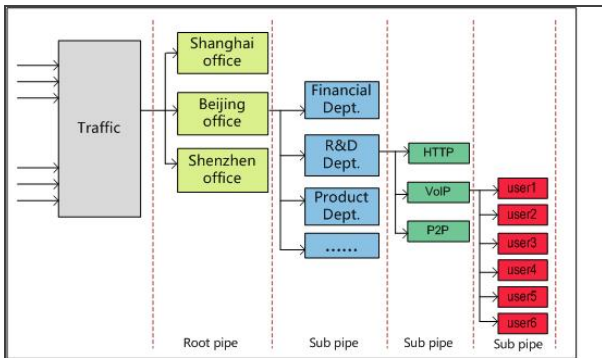


- You can create multiple root pipes that are independent. At most three levels of sub pipes can be nested to the root pipe.
- For the sub pipes at the same level, the total of their minimum bandwidth cannot exceed the minimum bandwidth of their upper-level parent pipe, and the total of their maximum bandwidth cannot exceed the maximum bandwidth of their upper-level parent pipe.
- If you have configured the forward or backward traffic management actions for the root pipe, all sub pipes that belong to this root pipe will inherit the configurations of the traffic direction set on the root pipe.
- The root pipe that is only configured the backward traffic management actions cannot work.

The following chart illustrates the application of multiple-level pipes in a company. The administrator can create the following pipes to limit the traffic:

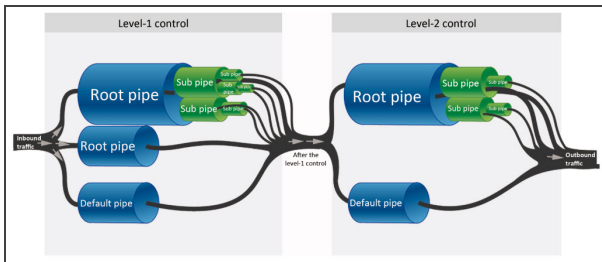
1. Create a root pipe to limit the traffic of the office located in Beijing.
2. Create a sub pipe to limit the traffic of its R&D department.
3. Create a sub pipe to limit the traffic of the specified applications so that each application has its own bandwidth.

4. Create a sub pipe to limit the traffic of the specified users so that each user owns the defined bandwidth when using the specified application.



Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes. Traffic that is dealt with by level-1 control flows into the level-2 control, and then system performs the further management and control according to the pipe configurations of level-2 control. After the traffic flowing into the device, the process of iQoS is shown as below:



According to the chart above, the process of traffic control is described below:

1. The traffic first flows into the level-1 control, and then system classifies the traffic into different pipes according to the traffic matching conditions of the pipe of level-1 control. The traffic that cannot match any pipe will be classified into the default pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list in the **Policy > iQoS** page. After the traffic flows into the root pipe, system classifies the traffic into different sub pipes according to the traffic matching conditions of each sub pipe.
2. According to the traffic management actions configured for the pipes, system manages and controls the traffic that matches the traffic matching conditions.
3. The traffic dealt with by level-1 control flows into the level-2 control. System manages and controls the traffic in level-2 control. The principles of traffic matching, management and control are the same as the one of the level-1 control.
4. Complete the process of iQoS.

Enabling iQoS

To enable iQoS, take the following steps:

1. Select **Policy > iQoS > Configuration**.
2. Select the **Enable iQoS** check box.
3. If you select the **Enable NAT IP matching** check box in **Level-1 Control** or **Level-2 Control**, system will use the IP addresses between the source NAT and the destination NAT as the matching items. If the matching is

successful, system will limit the speed of these IP addresses.



Note: Before enabling NAT IP matching, you must config the NAT rules. Otherwise, the configuration will not take effect.

4. Click **Apply** to save the configurations.

Pipes

By using pipes, devices implement iQoS. Pipes in different traffic control levels will take effect in different stages.

Configuring pipes includes the following sections:

1. Create the traffic matching conditions, which are used to capture the traffic that matches these conditions. If configuring multiple traffic matching conditions for a pipe, the logical relation between each condition is OR.
2. Create a white list according to your requirements. System will not control the traffic in the white list. Only root pipe and the default pipe support the white list.
3. Specify the traffic management actions, which are used to deal with the traffic that is classified into a pipe.
4. Specify the schedule. The pipe will take effect during the specified time period.

Basic Operations

Select **Policy > iQoS > Policy** to open the Policy page.

Level-1 Control		Level-2 Control				
+ New		- Delete		Edit		Disable
						Disable second level control
Pipe Name	Mode	Action	Schedule	Condition	Whitelist	
rootpipe		Forward: Pipe Bandwidth: 1000 Kbps Priority: 7				
asubpipe		Forward: Min Bandwidth: 100 Kbps Max Bandwidth: 500 Kbps Priority: 7				
asspipe		Forward: Min Bandwidth: 50 Kbps Max Bandwidth: 90 Kbps Priority: 7				
Default Pipe		Forward: Pipe Bandwidth: 1000 Kbps Limited by IP Source IP (Min Bandwidth: 10...				

You can perform the following actions in this page:

- Disable the level-2 traffic control: Click **Disable second level control**. The pipes in the level-2 traffic control will not take effect. The Level-2 Control tab will not appear in this page.
- View pipe information: The pipe list displays the name, mode, action, schedule, and the description of the pipes.
 - Click the icon to expand the root pipe and display its sub pipes.
 - Click the icon of the root pipe or the sub pipe to view the condition settings.
 - Click the icon of the root pipe to view the white list settings.
 - represents the root pipe is usable, represents the root pipe is unusable, represents the sub pipe is usable, represents the sub pipe is unusable, flow-two the gray text represents the pipe is disabled.
- Create a root pipe: Select the Level-1 Control or Level-2 Control tab, then click **New** in the menu bar to create a new root pipe.
- Create a sub pipe: Click the icon of the root pipe or the sub pipe to create the corresponding sub pipe.
- Click **Enable** in the menu bar to enable the selected pipe. By default, the newly-created pipe will be enabled.
- Click **Disable** in the menu bar to disable the selected pipe. The disabled pipe will not take effect.
- Click **Delete** to delete the selected pipe. The default pipe cannot be deleted.

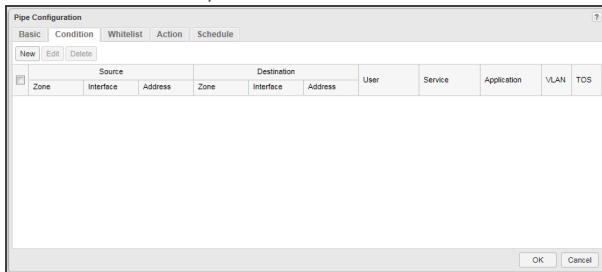
Configuring a Pipe

To configure a pipe, take the following steps:


1. According to the methods above, create a root pipe or sub pipe. The Pipe Configuration page appears.
2. **In the Basic tab, specify the basic pipe information.**




- Parent Pipe/Control Level: Displays the control level or the parent pipe of the newly created pipe.
- Pipe Name: Specify a name for the new pipe.
- Description: Specify the description of this pipe.
- QoS Mode: Shape, Policy, or Monitor.
 - The Shape mode can limit the data transmission rate and smoothly forward the traffic. This mode supports the bandwidth borrowing and priority adjusting for the traffic within the root pipe.
 - The Policy mode will drop the traffic that exceeds the bandwidth limit. This mode does not support the bandwidth borrowing and priority adjusting, and cannot guarantee the minimum bandwidth.
 - The Monitor mode will monitor the matched traffic, generate the statistics, and will not control the traffic.
- Bandwidth borrowing: All of the sub pipes in a root pipe can lend their idle bandwidth to the pipes that are lacking bandwidth. The prerequisite is that their bandwidth must be enough to forward the traffic in their pipes.
- Priority adjusting: When there is traffic congestion, system will arrange the traffic to enter the waiting queue. You can set the traffic to have higher priority and system will deal with the traffic in order of precedence.


3. In the Condition tab, click **New**.



In the Condition Configuration tab, configure the corresponding options.

Source Information	
Zone	Specify the source zone of the traffic. Select the zone name from the drop-down menu.
Interface	Specify the source interface of the traffic. Select the interface name from the drop-down menu.
Address	<p>Specify the source address of the traffic.</p> <ol style="list-style-type: none"> 1. Select an address type from the Address drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click  to add the addresses to the right pane. 4. After adding the desired addresses, click the blank area in this dialog box to complete the address configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • When selecting the Address Book type, you can click Add to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the any check box.

Destination Information	
Zone	Specify the destination zone of the traffic. Select the zone name from the drop-down menu.
Interface	Specify the destination interface of the traffic. Select the interface name from the drop-down menu.
Address	<p>Specify the destination address of the traffic.</p> <ol style="list-style-type: none"> 1. Select an address type from the Address drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click  to add the addresses to the right pane. 4. After adding the desired addresses, click the blank area in this dialog box to complete the address configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • When selecting the Address Book type, you can click Add to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the any check box.
User Information	<p>Specify a user or user group that the traffic belongs to.</p> <ol style="list-style-type: none"> 1. From the User drop-down menu, select the AAA server where the users and user groups reside. 2. Based on different types of AAA server, you can execute one or more actions: search a user/user group/role, expand the user-/user group list, and enter the name of the user/user group. 3. After selecting users/user groups/roles, click  to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog box to complete the user information configuration.
Service	<p>Specify a service or service group that the traffic belongs to.</p> <ol style="list-style-type: none"> 1. From the Service drop-down menu, select a type: Service, Service Group. 2. You can search the desired service/service group, expand the service/service group list. 3. After selecting the desired services/service groups, click  to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog box to complete the service configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • To add a new service or service group, click Add. • The default service configuration is any. To restore the configuration to this default one, select the any check box.
Application	Specify an application, application group, or application filters that the traffic belongs to.

	<ol style="list-style-type: none"> 1. From the Application drop-down menu, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click  to add them to the right pane. 3. After adding the desired objects, click the blank area in this dialog to complete the application configuration. <p>You can also perform other operations:</p> <ul style="list-style-type: none"> • To add a new application group, click New AppGroup. • To add a new application filter, click New AppFilter.
URL Category	<p>Specifies the URL category that the traffic belongs to.</p> <p>After the user specifies the URL category, the system matches the traffic according to the specified category.</p> <ol style="list-style-type: none"> 1. In the "URL category" drop-down menu, the user can select one or more URL categories, up to 8 categories. 2. After selecting the desired filters, click the blank area in this dialog to complete the configuration. <p>To add a new URL category, click the "New" button, the page will pop up "URL category" dialog box. In this dialog box, the user can configure the category name and URL.</p> <p>Select a URL category, click the "Edit" button, the page will pop up "URL category" dialog box. In this dialog box, the user can edit the URL in the category.</p>
Advanced	
VLAN	Specify the VLAN information of the traffic.
TOS	<p>Specify the TOS fields of the traffic; or click Configure to specify the TOS fields of the IP header of the traffic in the TOS Configuration dialog box.</p> <ul style="list-style-type: none"> • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum cost. • Reserved: Specify the normal service.

4. If you are configuring root pipes, you can specify the white list settings based on the description of configuring conditions.

5. **In the Action tab, configuring the corresponding actions.**

Forward (From source to destination)

The following configurations control the traffic that flows from the source to the destination. For the traffic that matches the conditions, system will perform the corresponding actions.

Pipe Bandwidth	<p>When configuring the root pipe, specify the pipe bandwidth.</p> <p>When configuring the sub pipe, specify the maximum bandwidth and</p>
----------------	--

	<p>the minimum bandwidth of the pipe:</p> <ul style="list-style-type: none"> • Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved and cannot be used by other pipes, select Enable Reserved Bandwidth. • Max Bandwidth: Specify the maximum bandwidth.
Limit type	<p>Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP:</p> <ul style="list-style-type: none"> • Type: Select the type of the bandwidth limitation: No Limit, Limit Per IP, or Limit Per User. <ul style="list-style-type: none"> • No Limit represents that system will not limit the bandwidth for each IP or each user. • Limit Per IP represents that system will limit the bandwidth for each IP. In the Limit by section, select Source IP to limit the bandwidth of the source IP in this pipe; or select Destination IP to limit the bandwidth of the destination IP in this pipe. • Limit Per User represents that system will limit the bandwidth for each user. In the Limit by section, specify the minimum/maximum bandwidth of the users. • When configuring the root pipe, you can select the Enable Average Bandwidth check box to make each source IP, destination IP, or user to share an average bandwidth.
Limit by	<p>When the Limit type is Limit Per IP or Limit Per User, you need to specify the minimum bandwidth or the maximum bandwidth:</p> <ul style="list-style-type: none"> • Min Bandwidth: Specify the minimum bandwidth. • Max Bandwidth: Specify the maximum bandwidth.
Advanced	
Priority	<p>Specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down menu. The smaller the value is, the higher the priority is. When a pipe has higher priority, system will first deal with the traffic in it and borrow the extra bandwidth from other pipes for it. The priority of the default pipe is 7.</p>
TOS	<p>Specify the TOS fields of the traffic; or click Configure to specify the TOS fields of the IP header of the traffic in the appeared TOS Configuration page.</p> <ul style="list-style-type: none"> • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost. • Reserved: Specify the normal service.
Limit Opposite Bandwidth	<p>Select the Limit Opposite Bandwidth check box to configure the value of limit-strength. The smaller the value, the smaller the limit.</p>

Backward (From condition's destination to source)

The following configurations control the traffic that flows from the destination to the source. For the traffic that matches the conditions, system will perform the corresponding actions.

Pipe Bandwidth	<p>When configuring the root pipe, specify the pipe bandwidth.</p> <p>When configuring the sub pipe, specify the maximum bandwidth and the minimum bandwidth of the pipe:</p> <ul style="list-style-type: none">• Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved and cannot be used by other pipes, select Enable Reserved Bandwidth.• Max Bandwidth: Specify the maximum bandwidth.
Limit type	<p>Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP:</p> <ul style="list-style-type: none">• Type: Select the type of the bandwidth limitation: No Limit, Limit Per IP, or Limit Per User.<ul style="list-style-type: none">• No Limit represents that system will not limit the bandwidth for each IP or each user.• Limit Per IP represents that system will limit the bandwidth for each IP. In the Limit by section, select Source IP to limit the bandwidth of the source IP in this pipe; or select Destination IP to limit the bandwidth of the destination IP in this pipe.• Limit Per User represents that system will limit the bandwidth for each user. In the Limit by section, specify the minimum/maximum bandwidth of the users.• When configuring the root pipe, you can select the Enable Average Bandwidth check box to make each source IP, destination IP, or user to share an average bandwidth.
Limit by	<p>When the Limit type is Limit Per IP or Limit Per User, you need to specify the minimum bandwidth or the maximum bandwidth:</p> <ul style="list-style-type: none">• Min Bandwidth: Specify the minimum bandwidth.• Max Bandwidth: Specify the maximum bandwidth.

Advanced

Priority	<p>Specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down menu. The smaller the value is, the higher the priority is. When a pipe has higher priority, system will first deal with the traffic in it and borrow the extra bandwidth from other pipes for it. The priority of the default pipe is 7.</p>
TOS	<p>Specify the TOS fields of the traffic; or click Configure to specify the TOS fields of the IP header of the traffic in the appeared TOS Configuration page.</p> <ul style="list-style-type: none">• Precedence: Specify the precedence.• Delay: Specify the minimum delay.• Throughput: Specify the maximum throughput.

	<ul style="list-style-type: none"> • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost. • Reserved: Specify the normal service.
Limit Opposite Bandwidth	Select the Limit Opposite Bandwidth check box to configure the value of limit-strength. The smaller the value, the smaller the limit.

6. In the Schedule tab, configure the time period when the pipe takes effect. Select the schedule from the drop-down list, or create a new one.
7. Click **OK** to save the settings.

Viewing Statistics of Pipe Monitor

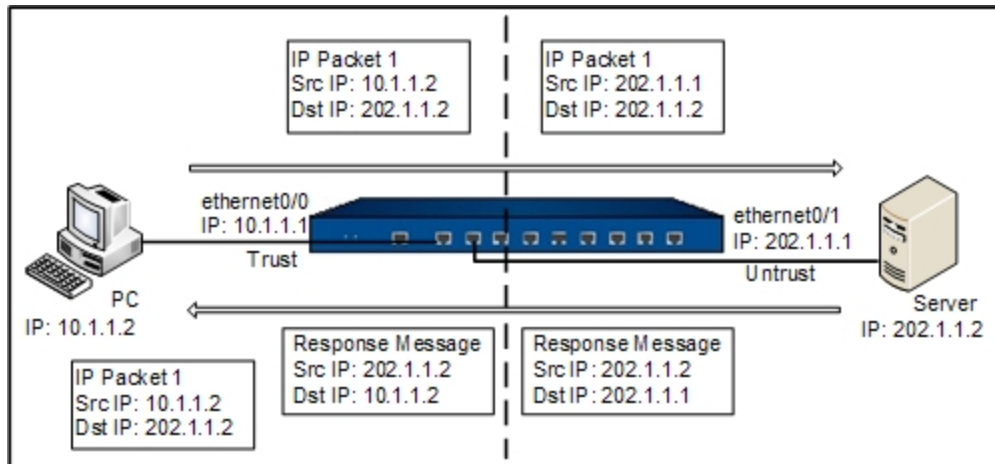
To view the statistics of pipe monitor, see "iQoS" on [Page 307](#).

NAT

NAT, Network Address Translation, translates the IP address within an IP packet header to another IP address. When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets. In practice, NAT is mostly used to allow the private network to access the public network, vice versa.

Basic Translation Process of NAT

When a device is implementing the NAT function, it lies between the public network and the private network. The following diagram illustrates the basic translation process of NAT.



As shown above, the device lies between the private network and the public network. When the internal PC at 10.1.1.2 sends an IP packet (IP packet 1) to the external server at 202.1.1.2 through the device, the device checks the packet header. Finding that the IP packet is destined to the public network, the device translates the source IP address 10.1.1.2 of packet 1 to the public IP address 202.1.1.1 which can get routed on the Internet, and then forwards the packet to the external server. At the same time, the device also records the mapping between the two addresses in its NAT table. When the response packet of IP packet 1 reaches the device, the device checks the packet header again and finds the mapping records in its NAT table, and replaces the destination address with the private address 10.1.1.2. In this process, the device is transparent to the PC and the Server. To the external server, it considers that the IP address of the internal PC is 202.1.1.1 and knows nothing about the private address 10.1.1.2. Therefore, NAT hides the private network of enterprises.

Implementing NAT

The devices translate the IP address and port number of the internal network host to the external network address and port number, and vice versa. This is the translation between the "private IP address + port number" and "public IP address + port number".

The devices achieve the NAT function through the creation and implementation of NAT rules. There are two types of NAT rules, which are source NAT rules (SNAT Rule) and destination NAT rules (DNAT Rule). SNAT translates source IP addresses, thereby hiding the internal IP addresses or sharing the limited IP addresses; DNAT translates destination IP addresses, and usually the IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device is translated to public IP addresses.

Configuring SNAT

To create an SNAT rule, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Click **New**. The SNAT Configuration dialog box will appear.

SNAT Configuration

Basic Advanced

Requirements

Virtual Router: trust-vr

Source Address: Address Entry Any

Destination Address: Address Entry Any

Ingress: All Traffic

Egress: All Traffic

Service: any

Translated to

Translated: ☒ Egress IP ☐ Specified IP ☐ No NAT

Mode: Dynamic port

Sticky: ☐ Enable

If "Sticky" is selected, all sessions of one source IP will be mapped to a fixed IP

Others

HA group: ☒ 0 ☐ 1

Description: (0-63) chars

OK Cancel

In the Basic tab, configure the following options.

Requirements	
Virtual Router	Specifies a VRouter for the SNAT rule. The SNAT rule will take effect when the traffic flows into this VRouter and matches the SNAT rule conditions.
Source Address	Specifies the source IP address of the traffic, including: <ul style="list-style-type: none">• Address Entry - Select an address entry from the drop-down list.• IP Address - Type an IP address into the box.• IP/Netmask - Type an IP address and its netmask into the box.
Destination Address	Specifies the destination IP address of the traffic, including: <ul style="list-style-type: none">• Address Entry - Select an address entry from the drop-down list.• IP Address - Type an IP address into the box.• IP/Netmask - Type an IP address and its netmask into the box.
Ingress	Specifies the ingress traffic, the default value is all traffic. <ul style="list-style-type: none">• All traffic - Specifies all traffic as the ingress traffic. Traffic from any ingress interfaces will continue to match this SNAT rule.• Ingress Interface - Specifies the ingress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not.
Egress	Specifies the egress traffic, the default value is all traffic. <ul style="list-style-type: none">• All traffic - Specifies all traffic as the egress traffic. Traffic from all egress interfaces will continue to match this SNAT rule.• Egress Interface - Specifies the egress interface of traffic. Select

Requirements	
	<p>an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not.</p> <ul style="list-style-type: none"> Next Virtual Router - Specifies the next virtual router of traffic. Select a virtual router from the drop-down list.
Service	<p>Specifies the service type of the traffic from the drop-down list.</p> <p>To create a new service or service group, click New Service or New Group.</p>
Translate to	
Translated	<p>Specifies the translated NAT IP address, including:</p> <ul style="list-style-type: none"> Egress IF IP - Specifies the NAT IP address to be an egress interface IP address. Specified IP - Specifies the NAT IP address to be a specified IP address. After selecting this option, continue to specify the available IP address in the Address drop-down list. No NAT - Do not implement NAT.
Mode	<p>Specifies the translation mode, including:</p> <ul style="list-style-type: none"> Static - Static mode means one-to-one translation. This mode requires the translated address entry to contain the same number of IP addresses as that of the source address entry. Dynamic IP - Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied. Dynamic port - Called PAT. Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is not enabled, the first address in the address entry will be used first; when the port resources of the first address are exhausted, the second address will be used. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the Enable check box behind Sticky to enable Sticky. You can also track if the public address after NAT is available, i.e., use the translated address as the source address to track if the destination website or host is accessible. Select the Enable check box behind Track to enable the function, and select a track object from the drop-down list.
Others	
HA Group	Specifies the HA group that the SNAT rule belongs to. The default setting is 0.
Description	Types the description.

In the **Advanced** tab, configure the corresponding options.

Option	Description
NAT Log	Select the Enable check box to enable the log function for this SNAT rule. The system will generate log information when there is traffic matching this NAT rule.
Position	<p>Specifies the position of the rule. Each SNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the SNAT rules in order, and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list:</p> <ul style="list-style-type: none"> • Bottom - The rule is located at the bottom of all the rules in the SNAT rule list. By default, system will put the newly-created SNAT rule at the bottom of all SNAT rules. • Top - The rule is located at the top of all the rules in the SNAT rule list. • Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. • After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	Specifies the method you get the rule ID. Each rule has its unique ID. It can be automatically assigned by system or manually assigned by yourself. If you select Manually assign , type an ID number into the box behind.

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

Enabling/Disabling a SNAT Rule

By default the configured SNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule:

1. Select **Policy > NAT > SNAT**.
2. Select the SNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Adjusting Priority

Each SNAT rule has a unique ID. When the traffic flows into the device, the device will search the SNAT rules in order and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching.

To adjust priority, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Select the rule you want to adjust its priority and click **Priority**.
3. In the Priority dialog box, move the selected rule to:
 - Top: The rule is moved to the top of all of the rules in the SNAT rule list.
 - Bottom: The rule is moved to the bottom of all of the rules in the SNAT rule list. By default, system will put the

newly-created SNAT rule at the bottom of all of the SNAT rules.

- Before ID: Specifies an ID number. The rule will be moved before the ID you specified.
- After ID: Specifies an ID number. The rule will be moved after the ID you specified.

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

Copying/Pasting a SNAT Rule

To copy/paste a SNAT rule, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Select the SNAT rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up, select the desired position. Then the rule will be cloned to the desired position.
 - Top: The rule is pasted to the top of all the rules in the SNAT rule list.
 - Bottom: The rule is pasted to the bottom of all the rules in the SNAT rule list.
 - Before the Rule Selected: The rule will be pasted before the Rule being selected.
 - After the Rule Selected: The rule will be pasted after the Rule being selected.

Exporting NAT444 Static Mapping Entries

You can export the NAT444 static mapping entries to a file . The exported file contains the ID, source IP address, translated IP address, start port, end port, and the protocol information.

To export the NAT444 static mapping entries, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Click **Export NAT444 Static Mapping Entries**.
3. Select a location to store the file and click **Save**.

The exported file is CSV format. It is recommended to export the file through the management interface.

Hit Count

The system supports statistics on SNAT rule hit counts, i.e., statistics on the matching between traffic and SNAT rules. Each time the inbound traffic is matched to a certain SNAT rule, the hit count will increment by 1 automatically.

To view a SNAT rule hit count, click **Policy > NAT > SNAT**. In the SNAT rule list, view the statistics on SNAT rule hit count under the Hit Count column.

Clearing NAT Hit Count

To clear a SNAT rule hit count, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Click **Hit Count**, and select **Clearing NAT Hit Count** in the pop-up list.
3. In the **Clearing NAT Hit Count** dialog box, configure the following options:
 - All NAT: Clears the hit counts for all NAT rules.
 - NAT ID: Clears the hit counts for a specified NAT rule ID.
4. Click **OK**.

Hit Count Check

System supports to check policy rule hit counts.

To check hit count, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Click **Hit Count**, and select **Hit Count Check** in the pop-up list. After the check, the NAT rules whose hit count is 0 will be highlight, that is to say, the NAT rule is not used in system.

Configuring DNAT

DNAT translates destination IP addresses, usually the IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device is translated to the public IP addresses.

Configuring an IP Mapping Rule

To configure an IP mapping rule, take the following steps:

- 1. Select **Policy > NAT > DNAT**.
- 2. Click **New** and select **IP Mapping**.

IP Mapping Configuration

Requirements

Virtual Router:

trust-vr

Destination Address:

Address Entry

Mapping

Translate to:

Address Entry

Others

HA group:

☒ 0

☐ 1

Description:

(0-63) characters

OK

Cancel

In the IP Mapping Configuration dialog box, configure the corresponding options.

Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Destination Address	Specifies the destination IP address of the traffic, including: <ul style="list-style-type: none">• Address Entry - Select an address entry from the drop-down list.• IP Address - Type an IP address into the box.• IP/Netmask - Type an IP address and its netmask into the box.
Mapping	
Translate to	Specifies the translated NAT IP address, including Address Entry , IP Address , and IP/Netmask . The number of the translated NAT IP addresses you specified must be the same as the number of the destination IP addresses of the traffic.
Others	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Description	Types the description.

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

Configuring a Port Mapping Rule

To configure a port mapping rule, take the following steps:

- 1. Select **Policy > NAT > DNAT**.

- Click **New** and select **Port Mapping**.

In the **Port Mapping Configuration** dialog, configure the corresponding options.

Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Destination Address	Specifies the destination IP address of the traffic, including: <ul style="list-style-type: none"> Address Entry - Select an address entry from the drop-down list. IP Address - Type an IP address into the box. IP/Netmask - Type an IP address and its netmask into the box.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click New Service or New Group .
Mapping	
Translate to	Specifies the translated NAT IP address, including Address Entry , IP Address , and IP/Netmask . The number of the translated NAT IP addresses you specified must be the same as the number of the destination IP addresses of the traffic.
Port Mapping	Types the translated port number of the Intranet server. The available range is 1 to 65535.
Others	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Description	Types the description.

- Click **OK** to save the settings.

Configuring an Advanced NAT Rule

You can create a DNAT rule and configure the advanced settings, or you can edit the advanced settings of an exiting DNAT rule.

To create a DNAT rule and configure the advanced settings, take the following steps:

- Select **Policy > NAT > DNAT**.
- Click **New** and select **Advanced Configuration**. To edit the advanced settings of an existing DNAT rule, select it and click **Edit**. The **DNAT configuration** dialog box will appear.

DNAT Configuration

Basic Advanced

Requirements

Virtual Router: trust-vr

Source Address: Address Entry Any

Destination Address: Address Entry Any

Service: any

Translated to

Action: ☒ NAT ☐ No NAT

Translate to: Address Entry Any

Translate Service Port to

Port: ☐ Enable Port: (1-65,535)

Load Balance: ☐ Enable If enabled, traffic will be balanced to different Intranet servers

Others

Redirect: ☐ Enable

HA group: ☒ 0 ☐ 1

Description: (0-63) chars

OK Cancel

In the Basic tab, configure the following options.

Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Source Address	Specifies the source IP address of the traffic, including: <ul style="list-style-type: none"> Address Entry - Select an address entry from the drop-down list. IP Address - Type an IP address into the box. IP/Netmask - Type an IP address and its netmask into the box.
Destination Address	Specifies the destination IP address of the traffic, including: <ul style="list-style-type: none"> Address Entry - Select an address entry from the drop-down list. IP Address - Type an IP address into the box. IP/Netmask - Type an IP address and its netmask into the box.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click New Service or New Group .
Translated to	
Action	Specifies the action for the traffic you specified, including: <ul style="list-style-type: none"> NAT - Implements NAT for the eligible traffic. No NAT - Do not implement NAT for the eligible traffic.
Translate to	When selecting the NAT option, you need to specify the translated IP address. The options include Address Entry , IP Address , IP/Netmask , and SLB Server Pool . For more information about the SLB Server Pool, view " SLB Server Pool " on Page 245 .
Translate Service Port to	
Port	Select Enable to translate the port number of the service that matches the conditions above.
Load Balance	Select Enable to enable the function. Traffic will be balanced to different Intranet servers.

Requirements	
Others	
Redirect	Select Enable to enable the function. When the number of this Translate to is different from the Destination Address of the traffic or the Destination Address address is any , you must enable the redirect function for this DNAT rule.
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Description	Types the description.

In the **Advanced** tab, configure the following options.

Track Server	
Track Ping Packets	After enabling this function, system will send Ping packets to check whether the Intranet servers are reachable.
Track TCP Packets	After enabling this function, System will send TCP packets to check whether the TCP ports of Intranet servers are reachable.
TCP Port	Specifies the TCP port number of the monitored Intranet server.
Others	
NAT Log	Enable the log function for this DNAT rule to generate the log information when traffic matches this NAT rule.
Position	Specifies the position of the rule. Each DNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the DNAT rules by sequence, and then implement DNAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the DNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list: <ul style="list-style-type: none"> Bottom - The rule is located at the bottom of all of the rules in the DNAT rule list. By default, the system will put the newly-created DNAT rule at the bottom of all of the SNAT rules. Top - The rule is located at the top of all of the rules in the DNAT rule list. Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	The ID number is used to distinguish between NAT rules. Specifies the method you get the rule ID. It can be automatically assigned by system or manually assigned by yourself.

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

Enabling/Disabling a DNAT Rule

By default the configured DNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Select the DNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Copying/Pasting a DNAT Rule

To copy/paste a DNAT rule, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Select the DNAT rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up, select the desired position. Then the rule will be cloned to the desired position.
 - Top: The rule is pasted to the top of all of the rules in the DNAT rule list.
 - Bottom: The rule is pasted to the bottom of all of the rules in the DNAT rule list.
 - Before the Rule Selected: The rule will be pasted before the Rule selected.
 - After the Rule Selected: The rule will be pasted after the Rule selected.

Adjusting Priority

Each DNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the DNAT rules in order, and then implement NAT of the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the DNAT rule list is the order of the rule matching.

To adjust priority, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Select the rule you want to adjust its priority and click **Priority**.
3. In the Priority dialog box, move the selected rule to:
 - Top: The rule is moved to the top of all of the rules in the DNAT rule list.
 - Bottom: The rule is moved to the bottom of all of the rules in the DNAT rule list. By default, system will put the newly-created DNAT rule at the bottom of all of the DNAT rules.
 - Before ID: Specifies an ID number. The rule will be moved before the ID you specified.
 - After ID: Specifies an ID number. The rule will be moved after the ID you specified.
4. Click **OK** to save the settings.

Hit Count

The system supports statistics on DNAT rule hit counts, i.e., statistics on the matching between traffic and DNAT rules. Each time the inbound traffic is matched to a certain DNAT rule, the hit count will increment by 1 automatically.

To view a DNAT rule hit count, click **Policy > NAT > DNAT**. In the DNAT rule list, view the statistics on DNAT rule hit count under the Hit Count column.

Clearing NAT Hit Count

To clear a DNAT rule hit count, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Click **Hit Count**, and select **Clearing NAT Hit Count** in the pop-up list.
3. In the **Clearing NAT Hit Count** dialog box, configure the following options:
 - All NAT: Clears the hit counts for all NAT rules.
 - NAT ID: Clears the hit counts for a specified NAT rule ID.
4. Click **OK**.

Hit Count Check

System supports to check policy rule hit counts.

To check hit count, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Click **Hit Count**, and select **Hit Count Check** in the pop-up list. After the check, the NAT rules whose hit count is 0 will be highlighted. This shows that the NAT rule is not being used in system.

SLB Server

View SLB server status: After you enabling the track function (PING track, TCP track, or UDP track), system will list the status and information of the intranet servers that are tracked.

View SLB server pool status: After you enabling the server load balancing function, system will monitor the intranet servers and list the corresponding status and information.

Viewing SLB Server Status

To view the SLB server status, take the following steps:

1. Select **Policy > NAT > SLB Server Status**.
2. You can set the filtering conditions according to the virtual router, SLB server pool, and server address and then view the information.

Option	Description
Server	Shows the IP address of the server.
Port	Shows the port number of the server.
Status	Shows the status of the server.
Current Sessions	Shows the number of current sessions.
DNAT	Shows the DNAT rules that uses the server.
HA Group	Shows the HA group that the server belongs to.

Viewing SLB Server Pool Status

To view the SLB server pool status, take the following steps:

1. Select **Policy > NAT > SLB Server Pool Status**.
2. You can set the filtering conditions according to the virtual router, algorithm, and server pool name and then view the information.

Option	Description
Name	Shows the name of the server pool name.
Algorithms	Shows the algorithm used by the server pool.
DNAT	Shows the DNAT rules that use the server.
Abnormal Server- /All Servers	Shows the number of abnormal servers and the total number of the servers.
Current Sessions	Shows the number of current sessions.

Session Limit

The devices support zone-based session limit function. You can limit the number of sessions and control the session rate to the source IP address, destination IP address, specified IP address, applications or role/user/user group, thereby protecting from DoS attacks and controlling the bandwidth of applications, such as IM or P2P.

Configuring a Session Limit Rule

To configure a session limit rule, take the following steps:

- 1. Select **Policy > Session Limit**.
- 2. Click **New**. The Session Limit Configuration dialog box will appear.

Session Limit Configuration

Zone: trust

Limit Conditions

☒ IP:
 IP: Any All IPs
 Source IP: Any All Source IPs
 Destination IP: Any All Destination IPs

☒ Application:
 Application:

☒ Role/User/User Group
 Role: User User Group: All Users
 Role:
 User Group:

☒ Schedule:
 Schedule:

Limit Types

Session Type:
 Session Number: 0 (0-212500;0:unlimited)
 New Connections/5s: (1-212500)

OK Cancel

- 3. Select the zone where the session limit rule is located.
- 4. **Configure the limit conditions.**

IP	
Select the IP check box to configure the IP limit conditions.	
IP	<div>Select the IP radio button and then select an IP address entry.</div> <ul style="list-style-type: none">• Select All IPs to limit the total number of sessions to all IP addresses.• Select Per IP to limit the number of sessions to each IP address.
Source IP	<div>Select the Source IP radio button and specify the source IP address entry and destination IP address entry. When the session's source IP and destination IP are both within the specified range, system will limit the number of session as follows:</div> <ul style="list-style-type: none">• When you select Per Source IP, system will limit the number of sessions to each source IP address.• When you select Per Destination IP, system will limit the number of sessions to each destination IP address.
Protocol	
Protocol	Limits the number of sessions to the protocol which has been setted in the textbox.
Application	
Application	Limits the number of sessions to the selected application.

IP	
Role/User/User Group	
Select the Role/User/User Group check box to configure the corresponding limit conditions.	
Role	Select the Role radio button and a role from the Role drop-down list to limit the number of sessions of the selected role.
User	Select the User radio button and a user from the User drop-down list to limit the number of sessions of the selected user.
User Group	Select the User Group radio button and a user group from the User Group drop-down list to limit the number of sessions of the selected user group. <ul style="list-style-type: none"> • Next to the User Group radio button, select All Users to limit the total number of sessions to all of the users in the user group. • Next to the User Group radio button, select Per User to limit the number of sessions to each user.
Schedule	
Schedule	Select the Schedule check box and choose a schedule you need from the drop-down list to make the session limit rule take effect within the time period specified by the schedule.

5. **Configure the limit types.**

Session Type	
Session Number	Specify the maximum number of sessions. The value range is 0 to 1048576. The value of 0 indicates no limitation.
New Connections/5s	Specify the maximum number of sessions created per 5 seconds. The value range is 1 to 1048576.

6. Click **OK** to save your settings.
7. Click **Switch Mode** to select a matching mode. If you select **Use the Minimum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is limited to the minimum number of sessions of all matched session limit rules; if you select **Use the Maximum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is the maximum number of sessions of all matched session limit rules.

Clearing Statistic Information

After configuring a session limit rule, the sessions which exceed the maximum number of sessions will be dropped. You can clear the statistical information of the dropped sessions of specified session limit rule according to your need.

To clear statistic information, take the following steps:

1. Select **Policy > Session Limit**.
2. Select the rule whose session's statistical information you want to clear.
3. Click **Clear**.

ARP Defense

StoneOS provides a series of ARP defense functions to protect your network against various ARP attacks, including:

- **ARP Learning:** Devices can obtain IP-MAC bindings in an Intranet from ARP learning, and add them to the ARP list. By default this function is enabled. The devices will always keep ARP learning on, and add the learned IP-MAC bindings to the ARP list. If any IP or MAC address changes during the learning process, the devices will add the updated IP-MAC binding to the ARP list. If this function is disabled, only IP addresses in the ARP list can access the Internet.
- **MAC Learning:** Devices can obtain MAC-Port bindings in an Intranet from MAC learning, and add them to the MAC list. By default this function is enabled. The devices will always keep MAC learning on, and add the learned MAC-Port bindings to the MAC list. If any MAC address or port changes during the learning process, the devices will add the updated MAC-Port binding to the MAC list.
- **IP-MAC-Port Binding:** If IP-MAC, MAC-Port or IP-MAC-Port binding is enabled, packets that are not matched to the binding will be dropped to protect against ARP spoofing or MAC address list attacks. The combination of ARP and MAC learning can achieve the effect of "real-time scan + static binding", and make the defense configuration more simple and effective.
- **Authenticated ARP:** Authenticated ARP is implemented on the ARP client Hillstone Secure Defender. When a PC with Hillstone Secure Defender installed accesses the Internet via the interface that enables Authenticated ARP, it will perform an ARP authentication with the device, for the purpose that the MAC address of the device being connected to the PC is trusted.
- **ARP Inspection:** Devices support ARP Inspection for interfaces. With this function enabled, StoneOS will inspect all ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list.
- **DHCP Snooping:** With this function enabled, system can create a binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and server.
- **Host Defense:** With this function enabled, the system can send gratuitous ARP packets for different hosts to protect them against ARP attacks.

Configuring ARP Defense

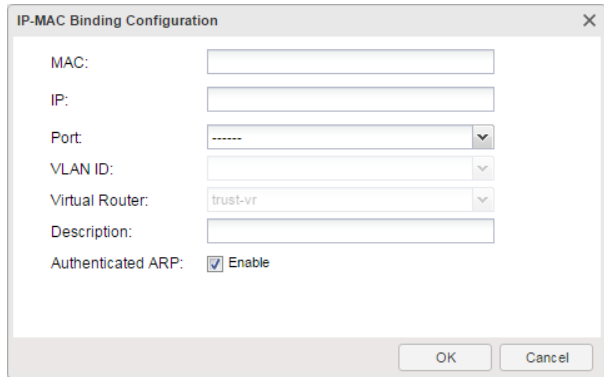
Configuring Binding Settings

Devices support IP-MAC binding, MAC-Port binding and IP-MAC-Port binding to reinforce network security control. The bindings obtained from ARP/MAC learning and ARP scan are known as dynamic bindings, and those manually configured are known as static bindings.

Adding a Static IP-MAC-Port Binding

To add a static IP-MAC-Port binding, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Click **New**.

A screenshot of the 'IP-MAC Binding Configuration' dialog box. It contains several input fields: 'MAC' (text box), 'IP' (text box), 'Port' (drop-down menu with '-----' selected), 'VLAN ID' (drop-down menu), 'Virtual Router' (drop-down menu with 'trust-vr' selected), and 'Description' (text box). At the bottom, there is a checkbox for 'Authenticated ARP' which is checked and labeled 'Enable'. 'OK' and 'Cancel' buttons are at the bottom right.

In the IP-MAC Binding Configuration, configure the corresponding settings.

Option	Description
MAC	Specify a MAC address.
IP	To enable the IP-MAC binding, specify an IP address.
Port	To enable the port binding, select a port from the drop-down list behind.
VLAN ID	If the port belongs to a VLAN, select the VLAN ID from the VLAN ID drop-down list.
Virtual Router	Select the virtual router that the binding item belongs to. By default, the binding item belongs to trust-vr.
Description	Specify the description for this item.
Authenticated ARP	Select Enable to enable the authenticated ARP function.

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

Obtaining a Dynamic IP-MAC-Port Bindings

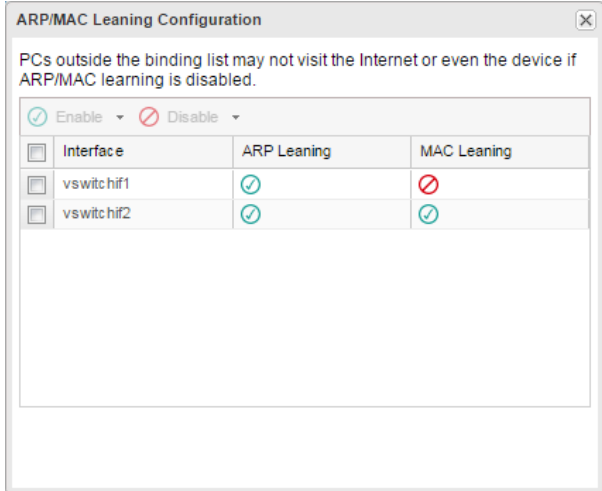
Devices can obtain dynamic IP-MAC-Port binding information from:

- ARP/MAC learning
- IP-MAC scan

To configure the ARP/MAC learning, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.

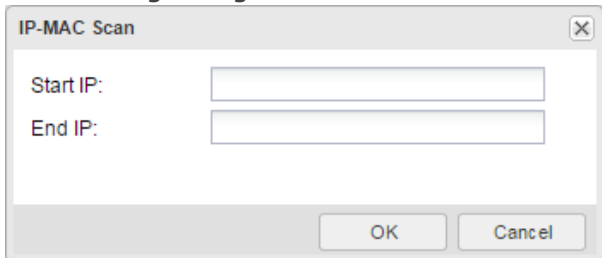
2. Select **Others** and click **ARP/MAC Learning** from the pop-up menu.



3. In the ARP/MAC Learning Configuration dialog box, select the interface that you want to enable the ARP/MAC learning function.
4. Click **Enable** and then select **ARP Learning** or **MAC Learning** in the pop-up menu. The system will enable the selected function on the interface you select.
5. Close the dialog box and return to the IP-MAC Binding tab.

To configure the ARP scan, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Binding Configuration** and then click **IP-MAC Scan** from the pop-up menu.



3. In the IP-MAC Scan dialog box, enter the start IP and the end IP.
4. Click **OK** to start scanning the specified IP addresses. The result will display in the table in the IP-MAC binding tab.

Bind the IP-MAC-Port Binding Item

To bind the IP-MAC-Port binding item, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Binding Configuration** and then click **Bind All** from the pop-up menu.
3. In the Bind All dialog box, select the binding type.
4. Click **OK** to complete the configurations.

To unbind an IP-MAC-Port binding item:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Binding Configuration** and then click **Unbind All** from the pop-up menu.
3. In the Unbind All dialog box, select the unbinding type.
4. Click **OK** to complete the configurations.

Importing/Exporting Binding Information

To import the binding information, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Others** and then click **Import** from the pop-up menu.
3. In the Import dialog box, click **Browse** to select the file that contains the binding information. Only the UTF-8 encoding file is supported.

To export the binding information, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Others** and then click **Export** from the pop-up menu.
3. Choose the binding information type.
4. Click **OK** to export the binding information to a file.

Configuring Authenticated ARP

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

The devices provide Authenticated ARP to protect the clients against ARP spoofing attacks. Authenticated ARP is implemented on the ARP client Hillstone Secure Defender. When a PC with Hillstone Secure Defender installed accesses the Internet via the interface that enables Authenticated ARP, it will perform an ARP authentication with the device to assure the MAC address of the device being connected to the PC is trusted. Besides, The ARP client is also designed with powerful anti-spoofing and anti-replay mechanisms to defend against various ARP attacks.



Note: The Loopback interface and PPPoE sub-interface are not designed with ARP learning, so these two interfaces do not support Authenticated ARP.

To use the Authenticated ARP function, you need to enable the Authenticated ARP function in the device and install the Hillstone Secure Defender in the PCs.

To enable the Authenticated ARP in the device, take the following steps:

1. Select **Policy > ARP Defense > ARP Defense**.
2. Select the interfaces on which you want to enable the Authenticated ARP function.



3. Click **Enable** and select **Force Authenticated ARP** to enable the authenticated ARP function.
4. Enable or disable **Force Install** as needed. If the **Force Install** option is selected, PCs cannot access the Internet via the corresponding interface unless the ARP client has been installed; if the **Force Install** option is not selected, only PCs with the ARP client installed are controlled by Authenticated ARP.

To install Hillstone Secure Defender in the PCs, take the following steps:

1. Enable Authenticated ARP for an interface, and also select the **Force Install** option for the interface.
2. When a PC accesses the Internet via this interface, the Hillstone Secure Defender's download page will pop up. Download HillstoneSecureDefender.exe as prompted.
3. After downloading, double-click **HillstoneSecureDefender.exe** and install the client as prompted by the installation wizard.

Configuring ARP Inspection

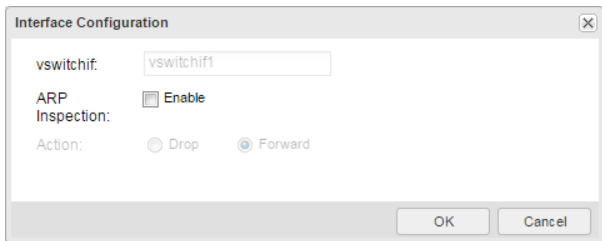
Devices support ARP Inspection for interfaces. With this function enabled, system will inspect all the ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list:

- If the IP address is in the ARP list and the MAC address matches, the ARP packet will be forwarded;
- If the IP address is in the ARP list but the MAC address does not match, the ARP packet will be dropped;
- If the IP address is not in the ARP list, continue to check if the IP address is in the DHCP Snooping list;
- If the IP address is in the DHCP Snooping list and the MAC address also matches, the ARP packet will be forwarded;
- If the IP address is in the DHCP Snooping list but the MAC address does not match, the ARP packet will be dropped;
- If the IP address is not in the DHCP Snooping, the ARP packet will be dropped or forwarded according to the specific configuration.

Both the VSwitch and VLAN interface of the system support ARP Inspection. This function is disabled by default.

To configure ARP Inspection of the VSwitch interface, take the following steps:

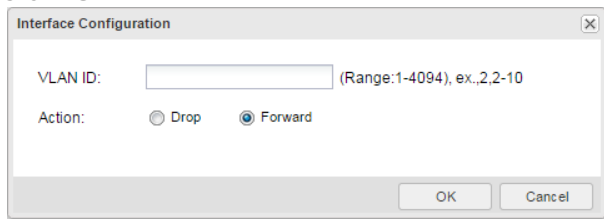
1. Select **Policy > ARP Defense > ARP Inspection**.
2. System already lists the existing VSwitch interfaces.
3. Double-click the item of a VSwitch interface.



4. In the Interface Configuration dialog box, select the **Enable** check box.
5. To drop the traffic whose sender's IP address is not in the ARP table, select **Drop**. To forward the traffic whose sender's IP address is not in the ARP table, select **Forward**.
6. Click **OK** to save the settings and close the dialog box.
7. For the interfaces belonging to the VSwitch interface, you can set the following options:
 - If you do not need the ARP inspection in the interface, in the Advanced Options section, double-click the interface and select **Do Not Inspect** option in the pop-up dialog box.
 - Configure the number of ARP packets received per second. When the ARP packet rate exceeds the specified value, the excessive ARP packets will be dropped. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.
8. Click **OK** to save the settings.

To configure the ARP inspection of the VLAN interface, take the following steps:

1. Select **Policy > ARP Defense > ARP Inspection**.
2. Click **New**.



3. In the Interface Configuration dialog box, specify the VLAN ID.
4. To drop the traffic whose sender's IP address is not in the ARP table, select **Drop**. To forward the traffic whose sender's IP address is not in the ARP table, select **Forward**.
5. For the interfaces belongs to the VLAN, you can set the following options:
 - If you do not need the ARP inspection in the interface, in the Advanced Options section, double-click the interface and select **Do Not Inspect** option in the pop-up dialog box.
 - Configure the number of ARP packets received per second. When the ARP packet rate exceeds the specified value, the excessive ARP packets will be dropped. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.
6. Click **OK** to save the settings.

Configuring DHCP Snooping

DHCP, Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for sub networks automatically. DHCP Snooping can create a binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and the server. When ARP Inspection is also enabled, the system will check if an ARP packet passing through can be matched to any binding on the list. If not, the ARP packet will be dropped. In the network that allocates addresses via DHCP, you can prevent against ARP spoofing attacks by enabling ARP inspection and DHCP Snooping.

DHCP clients look for the server by broadcasting, and only accept the network configuration parameters provided by the first reachable server. Therefore, an unauthorized DHCP server in the network might lead to DHCP server spoofing attacks. The devices can prevent DHCP server spoofing attacks by dropping DHCP response packets on related ports.

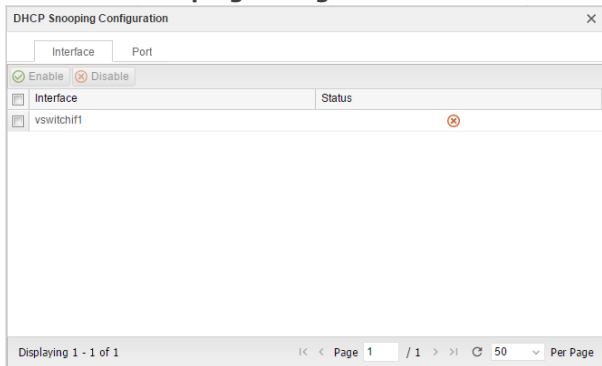
Besides, some malicious attackers send DHCP requests to a DHCP server in succession by forging different MAC addresses, and eventually lead to IP address unavailability to legal users by exhausting all the IP address resources. This kind of attacks is commonly known as DHCP Starvation. The devices can prevent against such attacks by dropping request packets on related ports, setting rate limit or enabling validity check.

The VSwitch interface of the system supports DHCP snooping. This function is disabled by default.

To configure DHCP snooping, take the following steps:

1. Select **Policy > ARP Defense > DHCP Snooping**.

2. Click **DHCP Snooping Configuration**.



3. In the Interface tab, select the interfaces that need the DHCP snooping function.

4. Click **Enable** to enable the DHCP snooping function.

5. In the Port tab, configure the DHCP snooping settings:

- Validity check: Check if the client's MAC address of the DHCP packet is the same as the source MAC address of the Ethernet packet. If not, the packet will be dropped. Select the interfaces that need the validity check and then click **Enable** to enable this function.
- Rate limit: Specify the number of DHCP packets received per second on the interface. If the number exceeds the specified value, system will drop the excessive DHCP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit. To configure the rate limit, double-click the interface and then specify the value in the **Rate** text box in the pop-up Port Configuration dialog box.
- Drop: In the Port Configuration dialog box, if the **DHCP Request** check box is selected, the system will drop all of the request packets sent by the client to the server; if the **DHCP Response** check box is selected, system will drop all the response packets returned by the server to the client.

6. Click **OK** to save the settings.

Viewing DHCP Snooping List

With DHCP Snooping enabled, system will inspect all of the DHCP packets passing through the interface, and create and maintain a DHCP Snooping list that contains IP-MAC binding information during the process of inspection. Besides, if the VSwitch, VLAN interface or any other Layer 3 physical interface is configured as a DHCP server, the system will create IP-MAC binding information automatically and add it to the DHCP Snooping list even if DHCP Snooping is not enabled. The bindings in the list contain information like legal users' MAC addresses, IPs, interfaces, ports, lease time, etc.

To view the DHCP snooping list, take the following steps:

1. Select **Policy > ARP Defense > DHCP Snooping**.
2. In the current page, you can view the DHCP snooping list.

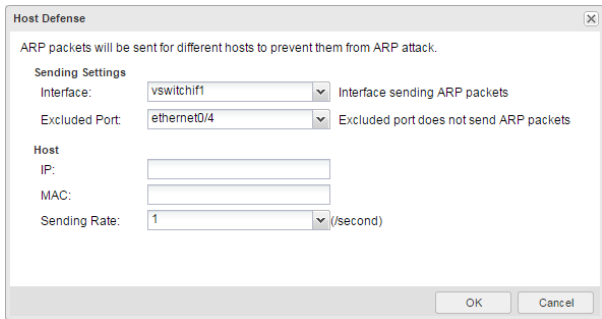
Configuring Host Defense

Host Defense is designed to send gratuitous ARP packets for different hosts to protect them against ARP attacks.

To configure host defense, take the following steps:

1. Select **Policy > ARP Defense > Host Defense**.

2. Click **New**.



The Host Defense dialog box is titled "Host Defense" and contains the following settings:

- Sending Settings**
 - Interface:** vswitchif1 (dropdown menu) with the label "Interface sending ARP packets"
 - Excluded Port:** ethernet0/4 (dropdown menu) with the label "Excluded port does not send ARP packets"
- Host**
 - IP:** (empty text field)
 - MAC:** (empty text field)
 - Sending Rate:** 1 (dropdown menu) with the label "(/second)"

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

In the Host Defense dialog box, configure the corresponding options.

Sending Settings	
Interface	Specify an interface that sends gratuitous ARP packets.
Excluded Port	Specify an excluded port, i.e., the port that does not send gratuitous ARP packets. Typically it is the port that is connected to the proxied host.
Host	
IP	Specify the IP address of the host that uses the device as a proxy.
MAC	Specify the MAC address of the host that uses the device as a proxy.
Sending Rate	Specify a gratuitous ARP packet that sends rate. The value range is 1 to 10/sec. The default value is 1.

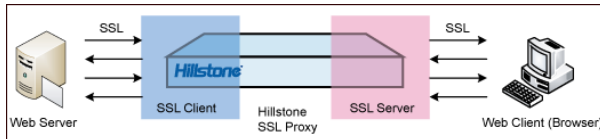
3. Click **OK** to save your settings and return to the Host Defense page.
4. Repeat Step 2 and Step 3 to configure gratuitous ARP packets for more hosts. You can configure the device to send gratuitous ARP packets for up to 16 hosts.

SSL Proxy

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS traffic. The SSL proxy function works in the following two scenarios:

The first scenario, the device works as the gateway of Web clients. The SSL proxy function replaces the certificates of encrypted websites with the SSL proxy certificate to get the encrypted information and send the SSL proxy certificates to the client's Web browser. During the process, the device acts as a SSL client and SSL server to establish connections to the Web server and Web browser respectively. The SSL proxy certificate is generated by using the device's local certificate and re-signing the website certificate. The process is described as below:



The second scenario, the device works as the gateway of Web servers. The device with SSL proxy enabled can work as the SSL server, use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), and send the decrypted traffic to the internal Web server.

Work Mode

There are three work modes. For the first scenario, the SSL proxy function can work in the Require mode and the Exempt mode; for the second scenario, the SSL proxy function can work in the Offload mode.

When the SSL proxy function works in the Require mode and the Exempt mode, it can perform the SSL proxy on specified websites.

For the websites that do not need SSL proxy, it dynamically adds the IP address and port of the websites to a bypass list, and the HTTPS traffic will be bypassed.

For the websites proxied by the SSL proxy function, the device will check the parameters of the SSL negotiation. When a parameter matches an item in the checklist, the corresponding HTTPS traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS traffic will be blocked by the device.
- If the action is Bypass, the HTTPS traffic will not be decrypted. Meanwhile, the device will dynamically add the IP address and port number of the Website to the bypass list, and the HTTPS traffic will be bypassed.

The device will decrypt the HTTPS traffic that is not blocked or bypassed.

When the SSL proxy function works in the Offload mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.

You can integrate SSL proxy function with the following:

- Integrate with the application identification function. Devices can decrypt the HTTPS traffic encrypted using SSL by the applications and identify the application. After the application identification, you can configure the policy rule, QoS, session limit, policy-based route.
- Integrate with the Web content function, Web post function, and email filter function. Devices can audit the actions that access the HTTPS website.
- Support unilateral SSL proxy in WebAuth. SSL client can use SSL connection during authentication stage. When authentication is completed, SSL proxy will no longer take effect, and the client and server communicate directly without SSL encryption.
- Integrate with AV, IPS, and URL. Devices can perform the AV protection, IPS protection, and URL filter on the decrypted HTTPS traffic.

Working as Gateway of Web Clients

To implement the SSL proxy, you need to bind a SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement the SSL proxy, take the following steps:

1. Configure the corresponding parameters of SSL negotiation, including the following items: specify the PKI trust domain of the device certificates, obtain the CN value of the subject field from the website certificate, configure the trusted SSL certificate list, and import a device certificate to the Web browser.
2. Configure a SSL proxy profile, including the following items: choose the work mode, set the website list (use the CN value of the Subject field of the website certificate), configure the actions to the HTTPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so on.
3. Bind a SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS traffic that matches the policy rule and is not blocked or bypassed by the device.

Configuring SSL Proxy Parameters

Configuring SSL proxy parameters includes the following items:

- Specify the PKI trust domain of the device certificate
- Obtain the CN value of the website certificate
- Configure a trusted SSL certificate list
- Import a device certificate to a Web browser


Specifying the PKI Trust Domain of Device Certificate

By default, the certificate of the default trust domain `trust_domain_ssl_proxy_2048` will be used to generate the SSL proxy certificate with the Web server certificate together, and then system will issue the generated SSL proxy certificate to the client. You can specify another PKI trust domain in system as the trust domain of the device certificate. The specified trust domain must have a CA certificate, local certificate, and the private key of the local certificate. To specify a trust domain, take the following steps:

1. Click **Policy > SSL Proxy**.
2. At the top-right corner of the page, click **Trust Domain Configuration**.
3. Select a trust domain from the Trust domain drop-down list.
 - The trust domain of `trust_domain_ssl_proxy` uses RSA and the modulus size is 1024 bits.
 - The trust domain of `trust_domain_ssl_proxy_2048` uses RSA and the modulus size is 2048 bits.
4. Click **OK** to save the settings.

Obtaining the CN Value

To get the CN value in the Subject field of the website certificate, take the following steps (take `www.gmail.com` as the example):

1. Open the IE Web browser, and visit `https://www.gmail.com`.
2. Click the **Security Report** button () next to the URL.
3. In the pop-up dialog box, click **View certificates**.
4. In the Details tab, click **Subject**. You can view the CN value in the text box.

Configuring a Trusted SSL Certificate List

The trusted SSL certificate list contains the well-known CA certificates in the industry, which are used to verify the validity of site certificates. For the valid certificates, system will send a SSL proxy certificate to the client browser; however, for the invalid certificates, system will send an internal certificate to the browser to inform you that the certificate of the website is invalid. You can import one or multiple trusted SSL certificates, or delete the specified trusted SSL certificate.

1. Click **Policy > SSL Proxy**.
2. At the top-right corner of the page, click **Trust SSL Certificate Configuration**.
 - In the pop-up dialog box, click **Import** to import a certificate.
 - In the pop-up dialog box, select a certificate and then click **Delete** to delete the selected certificate.
3. After the configurations, click **Close** to close the dialog box.

Importing Device Certificate to Client Browser

In the proxy process, the SSL proxy certificate will be used to replace the website certificate. However, there is no SSL proxy certificate's root certificate in the client browser, and the client cannot visit the proxy website properly. To address this problem, you have to import the root certificate (certificate of the device) to the browser.

To export the device certificate to local PC firstly, take the following steps:

1. Export the device certificate to local PC. Select **System > PKI**.
2. In the Management tab in the PKI Management dialog box, configure the options as below:
 - Trust domain: trust_domain_ssl_proxy or trust_domain_ssl_proxy_2048
 - Content: CA certificate
 - Action: Export
3. Click **OK** and select the path to save the certificate. The certificate will be saved to the specified location.

Then, import the device certificate to the client browser. Take Internet Explorer as an example:

1. Open IE.
2. From the toolbar, select **Tools > Internet** Options.
3. In the **Content** tab, click **Certificates**.
4. In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab.
5. Click **Import**. Import the certificate following the Certificate Import Wizard.

Configuring a SSL Proxy Profile

Configuring a SSL proxy profile includes the following items: choose the work mode, set the website list (use the CN value of the Subject field of the website certificate), configure the actions to the HTTPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so on. System supports up to 32 SSL proxy profiles and each profile supports up to 10,000 statistic website entries.

To configure a SSL proxy profile, take the following steps:

1. Click **Policy > SSL Proxy**.
2. At the top-left corner, click **New** to create a new SSL proxy profile.

In the Basic tab, configure the settings.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description.
Mode	<p>When the device works as the gateway of Web clients, the SSL proxy function can work in the Require mode or the Exempt mode.</p> <ul style="list-style-type: none"> In the Require mode, the device perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be bypassed. In the Exempt mode, the device does not perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be proxied by SSL proxy function.
Common Name	<p>Set the website list based on the work mode. When the SSL proxy is in the Require mode, set the websites that will be proxied by the SSL proxy function. When the SSL proxy is in the Exempt mode, set the websites that will not be proxied by the SSL proxy function and the device will perform the SSL proxy on other websites.</p> <p>To set the website list, specify the CN value of the subject field of the website certificate and then click Add.</p>
Warning	Select Enable to enable the warning page. When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, system notifies the users that their access to HTTPS websites are being monitored and asks the users to protect their privacy.

In the Decryption Configuration tab, configure the settings.

Option	Description
	After system completes the SSL negotiation, the traffic that is not blocked or bypassed will be decrypted. When the parameters match multiple items in the checklist and you configure difference actions to different items, the Block action will take effect. The corresponding HTTPS traffic will be blocked.
Key Modulus	Specify the key pair modulus size of the private/public keys that are associated with the SSL proxy certificate. You can select 1024 bits or 2048 bits.

Option	Description
Server certificate check	
Expired certificate	Check the certificate used by the server. When the certificate is overdue, you can select Block to block its HTTPS traffic, or select Bypass to bypass its HTTPS traffic, or select Decrypt to decrypt the HTTPS traffic.
Encryption mode check	
Unsupported version	<p>Check the SSL protocol version used by the server.</p> <ul style="list-style-type: none"> When system does not support the SSL protocol used by the SSL server, you can select Block to block its HTTPS traffic, or select Bypass to bypass its HTTPS traffic. When system supports the SSL protocol used by the SSL server, it will continue to check other items.
Unsupported encryption algorithms	<p>Check the encryption algorithm used by the server.</p> <ul style="list-style-type: none"> When system does not support the encryption algorithm used by the SSL server, you can select Block to block its HTTPS traffic, or select Bypass to bypass its HTTPS traffic. When system supports the encryption algorithm used by the SSL server, it will continue to check other items.
Client verification	<p>Check whether the SSL server verifies the client certificate.</p> <ul style="list-style-type: none"> When the SSL server verifies the client certificate, you can select Block to block its HTTPS traffic, or select Bypass to bypass its HTTPS traffic. When the SSL server does not verify the client certificate, it will continue to check other items.
Blocking SSL version	When the SSL server uses the specified version of SSL protocol, system can block its HTTPS traffic.
Blocking encryption algorithm	When the SSL server uses the specified encryption algorithm, system can block its HTTPS traffic.
Resource unavailable	When the decryption resource is not enough, system will bypass the HTTPS traffic. This action cannot be changed.

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

Working as Gateway of Web Servers

To implement SSL proxy, you need to bind a SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure a SSL proxy profile includes the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.
2. Bind a SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS traffic that matches the policy rule.

Configuring a SSL Proxy Profile

Configuring a SSL proxy profile includes the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.

To configure a SSL proxy profile, take the following steps:

1. Click **Policy > SSL Proxy**.

- At the top-left corner, click **New** to create a new SSL proxy profile.

The screenshot shows the 'SSL Proxy Configuration' dialog box with the 'Basic' tab selected. It contains the following elements:

- Name:** A text input field with a character count '(1-31) chars'.
- Description:** A text input field with a character count '(0-63) chars'.
- Mode:** Three radio buttons: 'require' (selected), 'exempt', and 'offload'.
- Common Name:** A text input field with the placeholder 'Enter a common name for the website certificate that needs decryption' and an 'Add' button.
- Common Name List:** A table with one header 'Common Name List' and an 'Add' button.
- Warning:** A checkbox labeled 'Enable' which is checked.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

In the Basic tab, configure the settings.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description.
Mode	When the device works as the gateway of Web servers, the SSL proxy function can work in the Offload mode.
Service Port	Specify the HTTP port number of the Web server.
Server Trust Domain	<p>Since the device will work as the SSL server and use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), you need to import the certificate and the key pair into a trust domain in the device. For more information about importing the certificate and the key pair, see "PKI" on Page 147.</p> <p>After you complete the importing, select the trust domain used by this SSL Profile.</p>
Warning	Select Enable to enable the warning page. When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, system notifies the users that their access to HTTPS websites are being monitored and asks the users to protect their privacy.

- Click **OK** to save the settings.

Binding a SSL Proxy Profile to a Policy Rule

After binding the SSL proxy profile to a policy rule, system will process the traffic that is matched to the rule according to the profile configuration. To bind the SSL proxy profile to a policy rule, see ["Security Policy" on Page 296](#).

Global Blacklist

After adding the IP addresses or services to the global blacklist, system will perform the block action to the IP address and service until the block duration ends. You can manually add IP addresses or services to the blacklist and system can also automatically add the IP addresses or services to the blacklist after you configure the IPS module.

Configuring global blacklist includes IP block settings and service block settings.

Configuring IP Block Settings

To configure the IP block settings, take the following steps:

- 1. Select **Policy > Global Blacklist > IP Block**.
- 2. Click **New**. The Block IP Configuration dialog box will appear.

Block IP Configuration

Virtual Router:

trust-vr

IP:

Blocked duration:

60

(60-3600 secs)

OK

Cancel

Configure the corresponding options.

Option	Description
Virtual Router	Selects the virtual router that the IP address belongs to.
IP	Types the IP address that you want to block. This IP address can be not only the source IP address, but also the destination IP address.
Blocked Duration	Types the duration that the IP address will be blocked. The unit is second. The value ranges from 60 to 3600. The default value is 60.

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

Configuring Service Block Settings

To configure the service block settings, take the following steps:

- 1. Select **Policy > Global Blacklist > Service Block**.
- 2. Click **New**. The Block Service Configuration dialog box will appear.

Block Service Configuration

Virtual Router:

trust-vr

Source IP:

Destination IP:

Destination port:

(0-65535)

Protocol:

TCP

(TCP,UDP)

Blocked duration:

60

(60-3600 secs)

OK

Cancel

Configure the corresponding options.

Option	Description
Virtual Router	Selects the virtual router that the IP address belongs to.
Source IP	Types the source IP address of the blocked service. The service block function will block the service from the source IP address to the destination IP address.
Destination IP	Types the destination IP address of the blocked service.
Port	Types the port number of the blocked service.
Protocol	Selects the protocol of the blocked service.
Blocked Duration	Types the duration that the IP address will be blocked. The unit is second. The value ranges from 60 to 3600. The default value is 60.

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

Chapter 11 Threat Prevention

Threat prevention is a device that can detect and block network threats. By configuring the threat prevention function, Hillstone devices can defend network attacks and reduce losses of the internal network.

Threat protections include:

- **Anti Virus:** It can detect the common file types and protocol types which are most likely to carry the virus and protect the network from them.. Hillstone devices can detect protocol types of POP3, HTTP, SMTP, IMAP4 and FTP, and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE , HTML, MAIL, RIFF and JPEG.
- **Intrusion Prevention:** It can detect and protect mainstream application layer protocols (DNS, FTP, POP3, SMTP, TELNET, MYSQL, MSSQL, ORACLE, NETBIOS), against web-based attacks and common Trojan attacks.
- **Attack Defense:** It can detect various types of network attacks, and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.
- **Abnormal Behavior Detection:** Traffic of sessions is detected based on the abnormal behavior detection signature database. When one detected object has multiple abnormal parameters, system will analyze the relationship among the abnormal parameters to see whether an abnormal behavior was formed.
- **Perimeter Traffic Filtering:** It can filter the perimeter traffic based on known IP of black/white list, and take block action on the malicious traffic that hits the blacklist.
- **Advanced Threat Detection:** It can intelligent analysis the suspicious traffic of Host, to detect malicious behavior and to identify APT (Advanced Persistent Threat) attack.
- **Anti-Spam:** It can filter the mails transmitted by SMTP and POP3 protocol through the cloud server, and discover the mail threats.

The threat protection configurations are based on security zones and policies.

- If a security zone is configured with the threat protection function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.



Note:

- Currently, you can only enable the Anti Virus and Intrusion Prevention function based on policies.
- Threat protection is controlled by a license. To use Threat protection, apply and install the Threat Protection(TP) license, 、 Anti Virus(AV) license or Intrusion Prevention System (IPS) license.

Threat Protection Signature Database

The threat protection signature database includes a variety of virus signatures, Intrusion prevention signatures, Perimeter traffic filtering signatures, 、 Abnormal behavior detection signature, and Advanced threat detection signatures. By default system updates the threat protection signature database everyday automatically. You can change the

update configuration as needed. Hillstone devices provide two default update servers: `update1.hillstonenet.com` and `update2.hillstonenet.com`. Hillstone devices support auto updates and local updates.

According to the severity, signatures can be divided into three security levels: critical, warning and informational. Each level is described as follows:

- Critical: Critical attacking events, such as buffer overflows.
- Warning: Aggressive events, such as over-long URLs.
- Informational: General events, such as login failures.

Anti Virus

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The system is designed with an Anti-Virus that is controlled by licenses to provide an AV solution featuring high speed, high performance and low delay. With this function configured in StoneOS, Hillstone devices can detect various threats including worms, Trojans, malware, malicious websites, etc., and proceed with the configured actions.

Anti Virus function can detect the common file types and protocol types which are most likely to carry the virus and protect the network from them. Hillstone devices can detect protocol types of POP3, HTTP, HTTPS, SMTP, IMAP4 and FTP, and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE , HTML, MAIL, RIFF and JPEG.

If IPv6 is enabled, Anti Virus function will detect files and protocols based on IPv6. How to enable IPv6, see [StoneOS_CLI_User_Guide_IPv6](#).

The virus signature database includes over 10,000 signatures, and supports both daily auto update and real-time local update. See "[Security Policy](#)" on [Page 296](#).



Note: Anti Virus is controlled by license. To use Anti Virus, apply and install the Anti Virus (AV) license.

Configuring Anti-Virus

This chapter includes the following sections:

- Preparation for configuring Anti-Virus function
- Configuring Anti-Virus function
- Configuring Anti-Virus global parameters

Preparing

Before enabling Anti-Virus, make the following preparations:

1. Make sure your system version supports Anti-Virus.
2. Import an Anti-Virus license and reboot. The Anti-Virus will be enabled after the rebooting.



Note:

- You need to update the Anti-Virus signature database before enabling the function for the first time. To assure a proper connection to the default update server, you need to configure a DNS server for StoneOS before updating.
- Except M8860/M8260/M7860/M7360/M7260, if Anti-Virus is enabled, the max amount of concurrent sessions will decrease by half.

Configuring Anti-Virus Function

The Anti-Virus configurations are based on security zones or policies.

- If a security zone is configured with the Anti-Virus function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.
- To perform the Anti-Virus function on the HTTPS traffic, see the policy-based Anti-Virus.

To realize the zone-based Anti-Virus, take the following steps:

1. Create a zone. For more information, refer to "[Security Zone](#)" on [Page 44](#).
2. In the Zone Configuration dialog, select Threat Protection tab.
3. Enable the threat protection you need and select an Anti-Virus rule from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list. To create an Anti-Virus rule, see [Configuring Anti-Virus Rule](#).
4. Click **OK** to save the settings.

To realize the policy-based Anti-Virus, take the following steps:

1. Create a security policy rule. For more information, refer to "[Security Policy](#)" on [Page 296](#).
2. In the Policy Configuration dialog box, select the Protection tab.

3. Select the **Enable** check box of **Antivirus**. Then select an Anti-Virus rule from the Profile drop-down list, or you can click **Add Profile** from the Profile drop-down list to create an Anti-Virus rule. For more information, see [Configuring Anti-Virus Rule](#).
4. To perform the Anti-Virus function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. System will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the Anti-Virus function on the decrypted traffic.

According to the various configurations of the security policy rule, system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled Anti-Virus disabled	System decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the Anti-Virus function on the decrypted traffic.
SSL proxy enabled Anti-Virus enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic.
SSL proxy disabled Anti-Virus enabled	System performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus profile. The HTTPS traffic will not be decrypted and the system will transfer it.

If the destination zone or the source zone specified in the security policy rule are configured with Anti-Virus as well, system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled Anti-Virus disabled	Anti-Virus enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the zone.
SSL proxy enabled Anti-Virus enabled	Anti-Virus enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the policy rule.
SSL proxy disabled Anti-Virus enabled	Anti-Virus enabled	System performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus rule of the policy rule. The HTTPS traffic will not be decrypted and system will transfer it.

5. Click **OK** to save the settings.

Configuring an Anti-Virus Rule

To configure an Anti-Virus rule, take the following steps:

1. Select **Object > Antivirus > Profile**.
2. Click **New**.

In the Anti-Virus Rules Configuration dialog box, enter the Anti-Virus rule configurations.

Option	Description
Rule Name	Specifies the rule name.
File Types	Specifies the file types you want to scan. It can be GZIP, JPEG, MAIL, RAR, HTML .etc
Protocol Types	<p>Specifies the protocol types (HTTP, SMTP, POP3, IMAP4, FTP) you want to scan and specifies the action the system will take after the virus is found.</p> <ul style="list-style-type: none"> • Fill Magic - Processes the virus file by filling magic words, i.e., fills the file with the magic words (Virus is found, cleaned) from the beginning to the ending part of the infected section. • Log Only - Only generates log. • Warning - Pops up a warning page to prompt that a virus has been detected. This option is only effective to the messages transferred over HTTP. • Reset Connection - If virus has been detected, system will reset connections to the files.
Capture	Select the Enable check box before Capture Packet to enable the capture function.
Malicious Website Access Control	Select the check box behind Malicious Website Access Control to enable the function.
Action	<p>Specifies the action the system will take after the malicious website is found.</p> <ul style="list-style-type: none"> • Log Only - Only generates log. • Reset Connection - If a malicious website has been detected, system will reset connections to the files. • Return to the Alarm Page - Pops up a warning page to prompt that a malicious website has been detected. This option is only effective to the messages transferred over HTTP.
Enable label e-mail	If an email transferred over SMTP is scanned, you can enable label email to scan the email and its attachment(s). The scanning results will be included in the mail body, and sent with the email. If no virus has been

Option	Description
	detected, the message of "No virus found" will be labeled; otherwise information related to the virus will be displayed in the email, including the filename, result and action. Type the end message content into the box. The range is 1 to 128.

3. Click **OK**.



Note: By default, according to virus filtering protection level, system comes with three default virus filtering rules: `predef_low`, `predef_middle`, `predef_high`. The default rule is not allowed to edit or delete.

Configuring Anti-Virus Global Parameters

To configure the AV global parameters, take the following steps:

1. Select **Object > Antivirus > Configuration**.

In AV Global Configuration section, enter the AV global configurations.

Option	Description
Antivirus	Select/clear the Enable check box to enable/disable Anti-Virus.
Max Decompression Layer	By default StoneOS can scan the files of up to 5 decompression layers. To specify a decompression layer, select a value from the drop-down list. The value range is 1 to 5.
Exceed Action	Specifies an action for the compressed files that exceed the max decompression layer. Select an action from the drop-down list: <ul style="list-style-type: none"> • Log Only - Only generates logs but will not scan the files. This action is enabled by default. • Reset Connection - If a virus has been detected, StoneOS will reset connections for the files.
Encrypted Compressed File	Specifies an action for encrypted compressed files: <ul style="list-style-type: none"> • ----- - Will not take any special anti-virus actions against the files, but might further scan the files according to the configuration. • Log Only - Only generates logs but will not scan the files. • Reset Connection - Resets connections for the files.

2. Click **OK**.

Intrusion Prevention System

IPS, Intrusion Prevention System, is designed to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration.

The IPS can implement a complete state-based detection which significantly reduces the false positive rate. Even if the device is enabled with multiple application layer detections, enabling IPS will not cause any noticeable performance degradation. Besides, StoneOS will update the signature database automatically everyday to assure its integrity and accuracy.

- IPS will support IPv6 address if the IPv6 function is enabled.
- By integrating with the SSL proxy function, IPS can monitor the HTTPS traffic.

The protocol detection procedure of IPS consists of two stages: signature matching and protocol parse.

- Signature matching: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, system will process the traffic according to the action configuration. This part of detection is configured in the **Select Signature** section.
- Protocol parse: IPS analyzes the protocol part of the traffic. If the analysis results show the protocol part containing abnormal contents, system will process the traffic according to the action configuration. This part of detection is configured in the **Protocol Configuration** section.



Note: Intrusion Prevention System is controlled by a license. To use Threat protection, apply and install the Intrusion Prevention System (IPS) license.

Signatures

The IPS signatures are categorized by protocols, and identified by a unique signature ID. The signature ID consists of two parts: protocol ID (1st bit or 1st and 2nd bit) and attacking signature ID (the last 5 bits). For example, in ID 605001, "6" identifies a Telnet protocol, and "00120" is the attacking signature ID. The 1st bit in the signature ID identifies protocol anomaly signatures, while the others identify attacking signatures. The mappings between IDs and protocols are shown in the table below:

ID	Protocol	ID	Protocol	ID	Protocol	ID	Protocol
1	DNS	7	Other-TCP	13	TFTP	19	NetBIOS
2	FTP	8	Other-UDP	14	SNMP	20	DHCP
3	HTTP	9	IMAP	15	MySQL	21	LDAP
4	POP3	10	Finger	16	MSSQL	22	VoIP
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

In the above table, Other-TCP identifies all the TCP protocols other than the standard TCP protocols listed in the table, and Other-UDP identifies all the UDP protocols other than the standard UDP protocols listed in the table.

Configuring IPS

This chapter includes the following sections:

- Preparation for configuring IPS function
- Configuring IPS function

Preparation

Before enabling IPS, make the following preparations:

1. Make sure your system version supports IPS.
2. Import an Intrusion Prevention System (IPS) license and reboot. The IPS will be enabled after the rebooting.



Note: Except M8860/M8260/M7860/M7360/M7260, if IPS is enabled, the max amount of concurrent sessions will decrease by half.

Configuring IPS Function

The IPS configurations are based on security zones or policies.

- To perform the IPS function on the HTTPS traffic, see the policy-based IPS.

To realize the zone-based IPS, take the following steps:

1. Create a zone. For more information, refer to ["Security Zone" on Page 44](#).
2. In the Zone Configuration dialog box, select Threat Protection tab.
3. Enable the IPS you need and select an IPS rules from the profile drop-down list below, or you can click **Add Profile** from the profile drop-down list below. To create an IPS rule, see [Configuring an IPS Rule](#).
4. Click a direction (Inbound, Outbound, Bi-direction). The IPS rule will be applied to the traffic that is matched with the specified security zone and direction.

To realize the policy-based IPS, take the following steps:

1. Create a policy rule. For more information, refer to ["Security Policy" on Page 296](#).
2. In the Policy Configuration dialog box, select the Protection tab.
3. Select the **Enable** check box of **IPS**. Then select an IPS rule from the Profile drop-down list, or you can click **Add Profile** from the Profile drop-down list to create an IPS rule. For more information, see [Configuring an IPS Rule](#).
4. To perform the IPS function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. System will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the IPS function on the decrypted traffic.

According to the various configurations of the security policy rule, system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled IPS disabled	System decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the IPS function on the decrypted traffic.
SSL proxy	System decrypts the HTTPS traffic according to the SSL proxy profile and

Policy Rule Configurations	Actions
enabled IPS enabled	performs the IPS function on the decrypted traffic.
SSL proxy disabled IPS enabled	System performs the IPS function on the HTTP traffic according to the IPS profile. The HTTPS traffic will not be decrypted and system will transfer it.

If the destination zone or the source zone specified in the security policy rule is configured with IPS as well, system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled IPS disabled	IPS enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS function on the decrypted traffic according to the IPS rule of the zone.
SSL proxy enabled IPS enabled	IPS enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS function on the decrypted traffic according to the IPS rule of the policy rule.
SSL proxy disabled IPS enabled	IPS enabled	System performs the IPS function on the HTTP traffic according to the IPS rule of the policy rule. The HTTPS traffic will not be decrypted and system will transfer it.

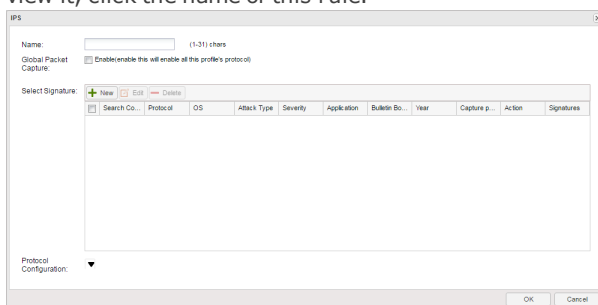
- Click **OK** to save the settings.

Configuring an IPS Rule

System has two default IPS rules: **predef_default** and **predef_loose**. The **predef_default** rule includes all the IPS signatures and its default action is reset. The **predef_loose** includes all the IPS signatures and its default action is log only.

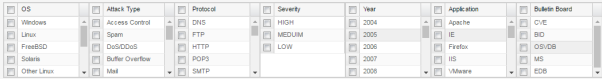
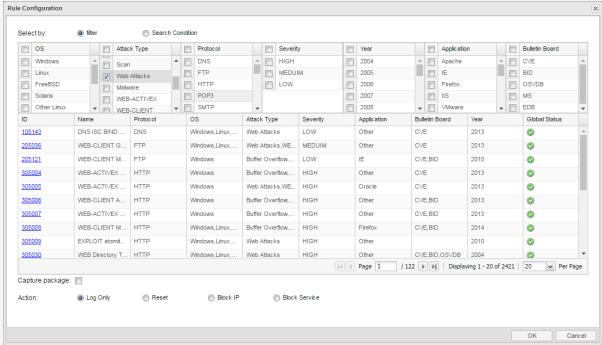
To configure an IPS rule, take the following steps:

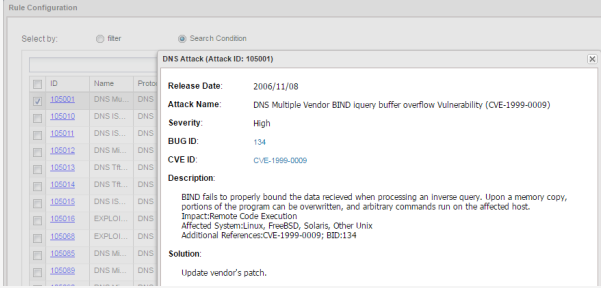
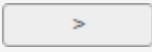
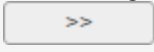


- Select **Object > Intrusion Prevention System > Profile**.
- Click **New** to create a new IPS rule. To edit an existing one, select the check box of this rule and then click **Edit**. To view it, click the name of this rule.




- Type the name into the Rule name box.
- According to your requirements, select the **Enable** check box of Global Packet Capture to capture packets.
- In the **Select Signature** area, the existing signature sets and their settings will be displayed in the table. Select the desired signature sets. You can also manage the signature sets, including New, Edit, and Delete.

Click New to create a new signature set rule.

Option	Description
<p>Creating a new signature set contains:</p> <ul style="list-style-type: none"> • Select By: Select the method of how to choose the signature set. There are two methods: Filter and Search Condition. • Capture package: Capture the abnormal packets that match the configured signature set. You can view them in the threat log. • Action: Specify the action performed on the abnormal traffic that match the signature set. 	
<p>Select By</p>	
<p>Filter</p>	<p>System categorizes the signatures according to the following aspects (aka main categories): affected OS, attack type, protocol, severity, released year, affected application, and bulletin board. A signature can be in several subcategories of one main category. For example, the signature of ID 105001 is in the Linux subcategory, the FreeBSD subcategory, and Other Linux subcategory at the same time.</p>  <p>With Filter selected, system displays the main categories and subcategories above. You can select the subcategories to choose the signatures in this subcategory. As shown below, after selecting the Web Attacks subcategory in the Attack Type main category, system will choose the signatures related to this subcategory. To view the detailed information of these chosen signatures, you can click the ID in the table.</p>  <p>When selecting main category and subcategory, note the following matters:</p> <ul style="list-style-type: none"> • You can select multiple subcategories of one main category. The logic relation between them is OR. • The logic relation between each main category is AND. • For example, you have selected Windows and Linux in OS and select HIGH in Severity. The chosen signatures are those whose severity is high and meanwhile whose affected operating system is either Windows or Linux.
<p>Search Condition</p>	<p>Enter the information of the signatures and press Enter to search the signatures. System will perform the fuzzy match-</p>

Option	Description
	<p>ing in the following field: attack ID, attack name, description, and CVE-ID.</p>  <p>In the search results displayed in the table, select the check box of the desired signatures. Then click  to add them to the right pane. The ID displayed in the right pane are the ones that are included in this signature set.</p> <p>To add all signatures in the left to the right, click .</p> <p>Use  or  to cancel the selected signatures or all signatures in the right.</p>
Capture Packet	
Capture Packet	Capture the abnormal packets that match the configured signature set. You can view them in the threat log.
Action	
Log Only	Record a log.
Reset	Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
Block IP	Block the IP address of the attacker. Specify a block duration. The value range is 60 to 3600 seconds, and the default value is 60.
Block Service	Block the service of the attacker. Specify a block duration. The value range is 60 to 3600 seconds, and the default value is 60.
<p>Note: You create several signature sets and some of them contain a particular signature. If the actions of these signature sets are different and the attack matches this particular signature, system will adopt the following rules:</p> <ul style="list-style-type: none"> • Always perform the stricter action on the attack. The signature set with stricter action will be matched. The strict level is: Block IP > Block Service > Rest > Log Only. If one signature set is Block IP with 15s and the other is Block Service with 30s, the final action will be Block IP with 30s. • If one signature set is configured with Capture Packet, system will capture the packets. • The action of the signature set created by Search Condition has higher priority than the action of the signature set created by Filter. 	

6. Click **OK** to complete signature set configurations.

7. In the Protocol Configuration area, click . The protocol configurations specify the requirements that the protocol part of the traffic must meet. If the protocol part contains abnormal contents, system will process the traffic according to the action configuration. System supports the configurations of HTTP, DNS, FTP, MSRPC, POP3, SMTP, SUNRPC, and Telnet.

In the HTTP tab, select the Protocol tab, and configure the following settings:

Option	Description
HTTP	Max Scan Length: Specify the maximum length of scanning when scanning the HTTP packets.
	Protocol Anomaly Detection: Select Enable to analyze the HTTP packets. If abnormal contents exist, you can: <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration.
	Banner Detection: Select the Enable check box to enable protection against HTTP server banners. <ul style="list-style-type: none"> • Banner information - Type the new information into the box that will replace the original server banner information.
	Max URI Length: Specify a max URI length for the HTTP protocol. If the URI length exceeds the limitation, you can: <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration.
	Allowed Methods: Specify the allowed HTTP methods.

To protect the Web server, select Web Server in the HTTP tab.

Protecting the Web server means system can detect the following attacks: SQL injection, XSS injection, external link check, ACL, and HTTP request flood and take actions when detecting them. A pre-defined Web server protection rule named **default** is built in. By default, this protection rule is enabled and cannot be disabled or deleted.

Configure the following settings to protect the Web server:

Option	Description
Name	Specify the name of the Web server protection rule.
Configure Domain	Specify domains protected by this rule. Click the link and the Configure Domain dialog box will appear. Enter the domain names in the Domain text box. At most 5 domains can be configured. The traffic to these domains will be checked by the protection rule.

Option	Description
	<p>The domain name of the Web server follows the longest match rule from the back to the front. The traffic that does not match any rules will match the default Web server. For example, you have configured two protection rules: rule1 and rule2. The domain name in rule1 is abc.com. The domain name in rule2 is email.abc.com. The traffic that visits news.abc.com will match rule1, the traffic that visits www.email.abc.com will match rule2, and the traffic that visits www.-abc.com.cn will match the default protection rule.</p>
CC URL Limit	<p>Select the Enable check box to enable the Web Server CC URL Restriction feature. When this function is enabled, system will block the traffic of this IP address, whose access frequency exceeds the threshold.</p> <ul style="list-style-type: none"> Threshold: Specifies the maximum number of times a single source IP accesses the URL path per minute. When the frequency of a source IP address exceeds this threshold, system will block the flow of the IP. The value ranges from 1 to 65535 times per minute. Block IP duration: Specifies the time to block IP. The default is 60 seconds, in the range of 60 to 3600 seconds. Over this time, system will release the blocked IP, this IP can re-visit the Web server. URL Path: Click the link and the Configure URL Path dialog appears. Enter the URL path in the URL text box to add or delete. After the configuration, all paths that contain the name of the path are also counted. System accesses the frequency statistics for HTTP requests that access these paths. If the access frequency of the HTTP request exceeds the threshold, the source IP of the request is blocked, and the IP will not be able to access the Web server. For example: configure '/home/ab', system will perform a frequency check on the 'access/home/ab/login' and '/home/BC/login' HTTP requests. URL path does not support the path format which contains the host name or domain name, for example: you can not configure www.baidu.-com/home/login.html, you should configure '/home/login.html', and 'www.baidu.com' should be configured in the corresponding Web server domain name settings. You can configure up to 32 URL paths. The length of each path is in the range of 1-255 characters.
SQL Injection Protection	<p>Select the Enable check box to enable SQL injection check.</p> <ul style="list-style-type: none"> Capture Packets: Capture the abnormal packets. You can view them in the threat log. Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. Sensitivity: Specifies the sensitivity for the SQL injection protection function. The higher the sensitivity is, the lower the false negative rate is. Check point: Specifies the check point for the SQL injection check.

Option	Description
	It can be Cookie, Cookie2, Post, Referer or URI.
XSS Injection Protection	<p>Select the Enable check box to enable XSS injection check for the HTTP protocol.</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. • Sensitivity: Specifies the sensitivity for the XSS injection protection function. The higher the sensitivity is, the lower the false negative rate is. • Check point: Specifies the check point for the XSS injection check. It can be Cookie, Cookie2, Post, Referer or URI.
External Link Check	<p>Select the Enable check box to enable external link check for the Web server. This function controls the resource reference from the external sites.</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • External link exception: Click this link, and the External Link Exception Configuration dialog box will appear. All the URLs configured on this dialog box can be linked by the Web sever. At most 32 URLs can be specified for one Web server. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
Referer check	<p>Select the check box to enable referer checking. System checks the headers of the HTTP packets and obtains the source site of the HTTP request. If the source site is in the Header Exception list, system will release it; otherwise, log or reset the connection. Thus controlling the Web site from other sites and to prevent chain of CSRF (Cross Site Request Forgery cross-site request spoofing) attacks occur.</p> <ul style="list-style-type: none"> • External link exception: Click the 'External link exception ' to open the <External link exception> dialog box, where the configured URL can refer to the other Web site. Each Web server can be configured with up to 32 URLs. • Action: Specify the action for the HTTP request for the chaining behavior, either "Log only" or "Reset". "
Iframe check	<p>Select the checkbox to enable iframe checking. System will identify if there are hidden iframe HTML pages by this function, then log it or reset its link.</p> <p>After iframe checking is enabled, system checks the iframe in the HTML page based on the specified iframe height and width, and when any height and width is less than or equal to the qualified value, system will identify as a hidden iframe attack, record, or reset connection that occurred.</p>

Option	Description
	<ul style="list-style-type: none"> Height: Specifies the height value for the iframe, range from 0 to 4096. Width: Specifies the width value of the iframe, range from 0 to 4096. Action: Specify the action for the HTTP request that hides iframe behavior, which is 'Only logged' or 'Reset'. Log Only - Record a log. Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
ACL	<p>Select the Enable check box to enable access control for the Web server. The access control function checks the upload paths of the web-sites to prevent the malicious code uploading from attackers.</p> <ul style="list-style-type: none"> ACL: Click this link, the ACL Configuration dialog appears. Specify websites and the properties on this dialog. "Static" means the URI can be accessed statically only as the static resource (images and text), otherwise, the access will handle as the action specified (log only/reset); "Block" means the resource of the website is not allowed to access. Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
HTTP Request Flood Protection	<p>Select the Enable check box to enable the HTTP request flood protection.</p> <ul style="list-style-type: none"> Request threshold: Specifies the request threshold. <ul style="list-style-type: none"> For the protected domain name, when the number of HTTP connecting request per second reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack, and will enable the HTTP request flood protection. For the protected full URL, when the number of HTTP connecting request per second towards this URL reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack towards this URL, and will enable the HTTP request flood protection. Full URL: Enter the full URLs to protect particular URLs. Click this link to configure the URLs, for example, www.example.com/index.html. When protecting a particular URL, you can select a statistic object. When the number of HTTP connecting request per second by the object reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack by this object, and will enable the HTTP request flood protection. <ul style="list-style-type: none"> x-forwarded-for: Select None, system will not use the value in x-forwarded-for as the statistic object. Select First, system will use the first value of the x-forwarded-for field as the statistic object. Select Last, system will use the last value of the x-forwarded-for field as the statistic object. Select All, system will use all values in x-forwarded-for as

Option	Description
	<p>the statistic object.</p> <ul style="list-style-type: none"> x-real-ip: Select whether to use the value in the x-real-ip field as the statistic field. <p>When the HTTP request flood attack is discovered, you can make the system take the following actions:</p> <ul style="list-style-type: none"> Authentication: Specifies the authentication method. System judges the legality of the HTTP request on the source IP through the authentication. If a source IP fails on the authentication, the current request from the source IP will be blocked. The available authentication methods are: <ul style="list-style-type: none"> Auto (JS Cookie): The Web browser will finish the authentication process automatically. Auto (Redirect): The Web browser will finish the authentication process automatically. Manual (Access Configuration): The initiator of the HTTP request must confirm by clicking OK on the returned page to finish the authentication process. Manual (CAPTCHA): The initiator of the HTTP request must be confirmed by entering the authentication code on the returned page to finish the authentication process. Crawler-friendly: If this check box is selected, system will not authenticate to the crawler. Request limit: Specifies the request limit for the HTTP request flood protection. After configuring the request limit, system will limit the request rate of each source IP. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, select the Record log check box. Proxy limit: Specifies the proxy limit for the HTTP request flood protection. After configuring the proxy limit, system will check whether each source belongs to the each source IP proxy server. If belongs to, according to configuration to limit the request rate. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, select the Record log check box. White List: Specifies the white list for the HTTP request flood protection. The source IP added to the white list will not check the HTTP request flood protection.

In the DNS tab, configure the following settings:

Option	Description
DNS	<p>Max Scan Length: Specify the maximum length of scanning when scanning the DNS packets.</p> <p>Protocol Anomaly Detection: Select Enable to analyze the DNS packets.</p>

Option	Description
	<p>If abnormal contents exist, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or send the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration.

In the FTP tab, configure the following settings:

Option	Description
FTP	<p>Max Scan Length: Specify the maximum length of scanning when scanning the FTP packets.</p> <p>Protocol Anomaly Detection: Select Enable to analyze the FTP packets. If abnormal contents exist, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Banner Detection: Select the Enable check box to enable protection against FTP server banners.</p> <ul style="list-style-type: none"> • Banner Information: Type the new information into the box that will replace the original server banner information. <p>Max Command Line Length: Specifies a max length (including carriage return) for the FTP command line. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max Response Line Length: Specifies a max length for the FTP response line. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Action for Brute-force: If the login attempts per minute fail for the times</p>

Option	Description
	<p>specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Select the Enable check box to enable brute-force.</p> <ul style="list-style-type: none"> • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • Block IP - Block the IP address of the attacker and specify a block duration. • Block Service - Block the service of the attacker and specify a block duration. • Block Time - Specifies the block duration.

In the MSRPC tab, configure the following settings:

Option	Description
MSRPC	<p>Max Scan Length: Specify the maximum length of scanning when scanning the MSRPC packets.</p> <p>Protocol Anomaly Detection: Select Enable to analyze the MSRPC packets. If abnormal contents exist, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max bind length: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max request length: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Action for Brute-force: If the login attempts per minute fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Select the Enable</p>

Option	Description
	<p>check box to enable brute-force.</p> <ul style="list-style-type: none"> • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • Block IP - Block the IP address of the attacker and specify a block duration. • Block Service - Block the service of the attacker and specify a block duration. • Block Time - Specifies the block duration.

In the POP3 tab, configure the following settings:

Option	Description
POP3	<p>Max Scan Length: Specify the maximum length of scanning when scanning the POP3 packets.</p> <p>Protocol Anomaly Detection: Select Enable to analyze the POP3 packets. If abnormal contents exist, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Banner Detection: Select the Enable check box to enable protection against POP3 server banners.</p> <ul style="list-style-type: none"> • Banner information - Type the new information into the box that will replace the original server banner information. <p>Max Command Line Length: Specifies a max length (including carriage return) for the POP3 command line. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max Parameter Length: Specifies a max length for the POP3 client command parameter. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration.

Option	Description
	<p>Max failure time: Specifies a max failure time (within one single POP3 session) for the POP3 server. If the failure time exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Action for Brute-force: If the login attempts per minute fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Select the Enable check box to enable brute-force.</p> <ul style="list-style-type: none"> • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • Block IP - Block the IP address of the attacker and specify a block duration. • Block Service - Block the service of the attacker and specify a block duration. • Block Time - Specifies the block duration.

In the SMTP tab, configure the following settings:

Option	Description
SMTP	<p>Max Scan Length: Specify the maximum length of scanning when scanning the SMTP packets.</p> <p>Protocol Anomaly Detection: Select Enable to analyze the SMTP packets. If abnormal contents exist, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Banner Detection: Select the Enable check box to enable protection against SMTP server banners.</p> <ul style="list-style-type: none"> • Banner information - Type the new information into the box that will replace the original server banner information. <p>Max Command Line Length: Specifies a max length (including carriage return) for the SMTP command line. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or

Option	Description
	<p>sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration.</p> <p>Max Path Length: Specifies a max length for the reverse-path and forward-path field in the SMTP client command. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max Reply Line Length: Specifies a max length reply length for the SMTP server. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max Text Line Length: Specifies a max length for the E-mail text of the SMTP client. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max Content Type Length: Specifies a max length for the content-type of the SMTP protocol. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max Content Filename Length: Specifies a max length for the filename of E-mail attachment. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log.

Option	Description
	<ul style="list-style-type: none"> • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Max Failure Time: Specifies a max failure time (within one single SMTP session) for the SMTP server. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Action for Brute-force: If the login attempts per minute fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Select the Enable check box to enable brute-force.</p> <ul style="list-style-type: none"> • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • Block IP - Block the IP address of the attacker and specify a block duration. • Block Service - Block the service of the attacker and specify a block duration. • Block Time - Specifies the block duration.

In the SUNRPC tab, configure the following settings:

Option	Description
SUNRPC	<p>Max Scan Length: Specify the maximum length of scanning when scanning the SUNRPC packets.</p> <p>Protocol Anomaly Detection: Select Enable to analyze the SUNRPC packets. If abnormal contents exist, you can:</p> <ul style="list-style-type: none"> • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Action for Brute-force: If the login attempts per minute fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Select the Enable check box to enable brute-force.</p> <ul style="list-style-type: none"> • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute.

Option	Description
	<ul style="list-style-type: none"> Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. Block Time - Specifies the block duration.

In the Telnet tab, configure the following settings:

Option	Description
Telnet	<p>Max Scan Length: Specify the maximum length of scanning when scanning the Telnet packets.</p> <p>Protocol Anomaly Detection: Select Enable to analyze the Telnet packets. If abnormal contents exist, you can:</p> <ul style="list-style-type: none"> Capture Packets: Capture the abnormal packets. You can view them in the threat log. Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Username/Password Max Length: Specifies a max length for the username and password used in Telnet. If the length exceeds the limits, you can:</p> <ul style="list-style-type: none"> Capture Packets: Capture the abnormal packets. You can view them in the threat log. Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. <p>Action for Brute-force: If the login attempts per minute fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Select the Enable check box to enable brute-force.</p> <ul style="list-style-type: none"> Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. Block Time - Specifies the block duration.

8. Click **Save** to complete the protocol configurations.

9. Click **OK** to complete the IPS rule configurations.

IPS Global Configuration

Configuring the IPS global settings includes:

- Enable the IPS function
- Specify how to merge logs
- Specify the work mode

Click **Object > Intrusion Prevention System > Configuration** to configure the IPS global settings.

Option	Description
IPS	Select/clear the Enable check box to enable/disable the IPS function.
Merge Log	<p>System can merge IPS logs which have the same protocol ID, the same VSYS ID, the same Signature ID, the same log ID, and the same merging type. Thus it can help reduce the number of logs and avoid receiving redundant logs. The function is disabled by default.</p> <p>Select the merging types in the drop-down list:</p> <ul style="list-style-type: none"> • ---- - Do not merge any logs. • Source IP - Merge the logs with the same Source IP. • Destination IP - Merge the logs with the same Destination IP. • Source IP, Destination IP - Merge the logs with the same Source IP and the same Destination IP.
Aggregate Time	Specifies the time granularity for IPS threat log of the same merging type (specified above) to be stored in the database. At the same time granularity, the same type of log is only stored once. It ranges from 10 to 600 seconds.
Mode	<p>Specifies a working mode for IPS:</p> <ul style="list-style-type: none"> • IPS - If attacks have been detected, StoneOS will generate logs, and will also reset connections or block attackers. This is the default mode. • Log only - If attacks have been detected, StoneOS will only generate logs, but will not reset connections or block attackers.

After the configurations, click **OK** to save the settings.

Signature List

Select **Object > Intrusion Prevention System > Signature List**. You can see the signature list.

Status:	Severity:	Year:	Operating System:	Type:	Attack Type:	Protocol Type:	Application:	Bulletin Board:	Search	Reset
Save Selection As:										
<div> <div>New</div> <div>Edit</div> <div>Delete</div> <div>Enable</div> <div>Disable</div> </div> <div>Load Database</div>										
ID	Name	CVE-ID	Protocol	OS	Attack Type	Severity	Application	Bulletin Board	Year	Global Status
105083	DNS Norton DNS CN...	CVE-2004-0444	DNS	Windows	Buffer Overflow	HIGH	Other	CVE	2010	✓
105084	DNS Red Hat Enterp...	CVE-2002-0029	DNS	Linux.FreeBSD,Other...	Buffer Overflow	HIGH	Other	CVE,BID	2010	✓
105088	DNS Multiple Vendor	CVE-2005-0036	DNS	Network Device	DoSDDoS	HIGH	Other	CVE	2010	✓
105099	DNS Microsoft ISA S...	CVE-2004-0892	DNS	Windows	Access Control	HIGH	Other	CVE,BID	2010	✓
105100	DNS Sun Java JRE...	CVE-2004-1503	DNS	Windows.Linux.Free...	DoSDDoS	HIGH	Other	CVE	2010	✓
105101	DNS Squid DNS Loo...	CVE-2005-0446	DNS	Windows.Linux.Free...	DoSDDoS	HIGH	Squid	CVE	2010	✓
105102	DNS Squid DNS Loo...	CVE-2005-0446	DNS	Windows.Linux.Free...	DoSDDoS	HIGH	Squid	CVE	2010	✓
105103	DNS Symantec Gate...	CVE-2005-0817	DNS	Windows.Solaris	DoSDDoS	HIGH	Other	CVE,BID	2010	✓
105104	DNS Multiple Vendor	CVE-1999-0009	DNS	Linux.FreeBSD,Solar...	Buffer Overflow	HIGH	Other	CVE,BID	2006	✓
105112	DNS ISC BIND CNA...	CVE-2011-2465	DNS	Windows.Linux	DoSDDoS	MEDIUM	Other	CVE	2012	✓
105113	DNS ISC BIND RRS...	CVE-2011-1910	DNS	Linux.FreeBSD,Solar...	DoSDDoS	MEDIUM	Other	CVE	2012	✓
105114	DNS Microsoft DNS...	CVE-2011-1966	DNS	Windows	Access Control	MEDIUM	Other	CVE,MS	2012	✓
105115	DNS Tftp32 DNS S...		DNS	Network Device	Buffer Overflow	MEDIUM	Other		2012	✓
105116	DNS Tftp32 DNS S...		DNS	Windows	Buffer Overflow	MEDIUM	Other	BID	2012	✓
105117	DNS ISC BIND RRS...	CVE-2011-1907	DNS	Windows	DoSDDoS	MEDIUM	Other	CVE	2012	✓
105118	EXPLOIT Microsoft F...	CVE-2011-1889	DNS	Windows	Access Control	MEDIUM	Other	CVE,MS	2013	✓
105120	EXPLOIT Oracle Se...	CVE-2010-0072	DNS	Windows	Buffer Overflow	LOW	Oracle	CVE,BID	2013	✓
105187	DNS Microsoft DNS...	CVE-2009-0093	DNS	Windows	DoSDDoS	LOW	Other	CVE	2014	✓
105190	DNS Microsoft Wind...	CVE-2006-3441	DNS	Other	Buffer Overflow	LOW	Other	CVE	2010	✓

The upper section is for searching signatures. The lower section is for managing signatures.

Searching Signatures

In the upper section, set the search conditions and then click **Search** to search the signatures that match the condition.

To clear all search conditions, click **Reset**. To save the search conditions, click **Save Selection As** to name this set of search conditions and save it.

Managing Signatures

You can view signatures, create a new signature, load the database, delete a signature, edit a signature, enable a signature, and disable a signature.

- View signatures: In the signature list, click the ID of a signature to view the details.
- Create a new signature: click **New**.

In the General tab, configure the following settings:

Option	Description
Name	Specifies the signature name.
Description	Specifies the signature descriptions.
Protocol	Specifies the affected protocol.
Flow	Specifies the direction. <ul style="list-style-type: none">• To_Server means the package of attack is from the server to the client.• To_Client means the package of attack is from the client to the server.• Any includes To_Server and To_Client.
Source Port	Specifies the source port of the signature. <ul style="list-style-type: none">• Any - Any source port.• Included - The source port you specified should be included. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.• Excluded - The source port you specified should be excluded. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.
Destination Port	Specifies the destination port of the signature. <ul style="list-style-type: none">• Any - Any destination port.• Included - The destination port you specified should be included. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.• Excluded - The destination port you specified should be excluded. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.
Dsize	Specifies the payload message size. Select "----", ">", "<" or "=" from the drop-down list and specifies the value in the text box. "----" means no setting of the parameters.
Severity	Specifies the severity of the attack.
Attack Type	Select the attack type from the drop-down list.
Application	Select the affected applications. "----" means all applications.

Option	Description
Operating System	Select the affected operating system from the drop-down list. "----" means all the operating systems.
Bulletin Board	Select a bulletin board of the attack.
Year	Specifies the released year of attack.
Detection Filter	Specifies the frequency of the signature rule. <ul style="list-style-type: none"> Track - Select the track type from the drop-down list. It can be by_src or by_dst. System will use the statistic of the source IP or the destination IP to check whether the attack matches this rule. Count - Specifies the maximum times the rule occurs in the specified time. If the attacks exceed the Count value, system will trigger rules and act as specified. Seconds - Specifies the interval value of the rule occurs.

In the **Content** tab, click **New** to specify the content of the signature:

Option	Description
Content	Specifies the signature content. Select the following check box if needed: <ul style="list-style-type: none"> HEX - Means the content is hexadecimal. Case Insensitive - Means the content is not case sensitive. URI - Means the content needs to match URI field of HTTP request.
Relative	Specifies the signature content location. <ul style="list-style-type: none"> If Beginning is selected, system will search from the header of the application layer packet. <ul style="list-style-type: none"> Offset: System will start searching after the offset from the header of the application layer packet. The unit is byte. Depth: Specifies the scanning length after the offset. The unit is byte. If Last Content is selected, system will search from the content end position. <ul style="list-style-type: none"> Distance: System will start searching after the distance from the former content end position. The unit is byte. Within: Specifies the scanning length after the distance. The unit is byte.

- Load the database: After you create a new signature, click **Load Database** to make the newly created signature take effect.
- Edit a signature: Select a signature and then click **Edit**. You can only edit the user-defined signature. After editing the signature, click **Load Database** to make the modifications take effect.
- Delete a signature: Select a signature and then click **Delete**. You can only delete the user-defined signature. After deleting the signature, click **Load Database** to make the deletion take effect.
- Enable/Disable signatures: After selecting signatures, click **Enable** or **Disable**.

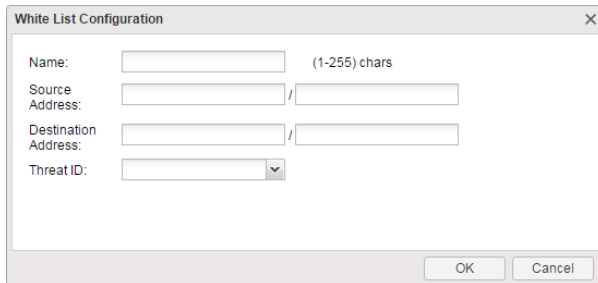
Configuring IPS White list

The device detects the traffic in the network in real time. When a threat is detected, the device generates alarms or blocks threats. With the complexity of the network environment, the threat of the device will generate more and more

warning, too much threat to the user can not start making the alarm, and many of them are false positives. By providing IPS whitelist, the system no longer reports alarms or blocks to the whitelist, thus reducing the false alarm rate of threats. The IPS whitelist consists of source address, destination address, and threat ID, and the user selects at least one item for configuration.

To configure an IPS white list :

1. Select **Policy > Intrusion Prevention System > White list**
2. Click **New**.



The image shows a 'White List Configuration' dialog box with the following fields:

- Name:** A text input field with a placeholder '(1-255) chars'.
- Source Address:** A text input field followed by a slash '/' and another text input field.
- Destination Address:** A text input field followed by a slash '/' and another text input field.
- Threat ID:** A dropdown menu.

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

In the White List Configuration dialog , enter the White List configurations.

Option	Description
Name	Specifies the white-list name.
Source Address	Specifies the source address of the traffic to be matched by IPS.
Destination Address	Specifies the destination address of the traffic to be matched by IPS.
Threat ID	Select the signature ID from the drop-down list. A whitelist can be configured with a maximum of one threat ID. When the threat ID is not set, the traffic can be filtered based on the source and destination IP address. When user have configured threat ID, the source address, destination address and threat ID must be all matched successfully before the packets can be released.

3. Click **OK**.

Sandbox

A sandbox executes a suspicious file in a virtual environment, collects the actions of this file, analyzes the collected data, and verifies the legality of the file.

The Sandbox function of the system uses the cloud sandbox technology. The suspicious file will be uploaded to the cloud side. The cloud sandbox will collect the actions of this file, analyze the collected data, verify the legality of the file, give the analysis result to the system and deal with the malicious file with the actions set by system.

The Sandbox function contains the following parts:

- Collect and upload the suspicious file: The Sandbox function parses the traffic, and extracts the suspicious file from the traffic.
 - If there are no analyze result about this file in the local database, system will upload this file to the cloud intelligence server, and the cloud server intelligence will upload the suspicious file to the cloud sandbox for analysis.
 - If this file has been identified as an illegal file in the local database of the Sandbox function, system will generate corresponding threat logs and cloudsandbox logs.

Additionally, you can specify the criteria of the suspicious files by configuring a sandbox profile.

- Check the analysis result returned from the cloud sandbox and take actions: The Sandbox function checks the analysis results of the suspicious file returned from the cloud sandbox, verifies the legality of the file, saves the result

to the local database. If this suspicious file is identified as an illegal file, you need to deal with the file according to the actions (reset the connection or report logs) set by system. If it's the first time to find malicious file in local sandbox, system will record threat logs and cloud sandbox logs and cannot stop the malicious link. When malicious file accesses the cached threat information in the local machine, the threat will be effective only by resetting connection.

- Maintain the local database of the Sandbox function: Record the information of the uploaded files, including uploaded time and analysis result. This part is completed by the Sandbox function automatically.



Note: The Sandbox function is controlled by license. To use the Sandbox function, install the Cloud sandbox license.

Related Topics: [Configuring Sandbox](#)

Configuring Sandbox

This chapter includes the following sections:

- [Preparation for configuring the Sandbox function](#)
- [Configuring the Sandbox rules](#)
- [Sandbox global configurations](#)

Preparation

Before enabling the Sandbox function, make the following preparations:

1. Make sure your system version supports the Sandbox function.
2. The current device is registered to the [Cloud View](#) platform.
3. Import the Cloud sandbox license and reboot. The Sandbox function will be enabled after rebooting.



Note: Except M8860/M8260/M7860/M7360/M7260, if the Sandbox function is enabled, the max amount of concurrent sessions will decrease by half.

Configuring Sandbox

System supports the policy-based Sandbox. To create the policy-based Sandbox, take the following steps:

1. Click **Object > Sandbox > Configuration**. Select **Enable** check box to enable the Sandbox function.
2. Click **Object > Sandbox > Profile** to [create a sandbox rule](#) you need.
3. Bind the sandbox rule to a policy. Click **Policy > Security Policy**. Select the policy rule you want to bind or click **New** to [create a new policy](#). In the Policy Configuration dialog box, select the **Protection** tab and then check the **Enable** check box of Sandbox.

Configuring a Sandbox Rule

A sandbox rule contains the files types that device has detected, the protocols types that the device has detected, the white list settings, and the file filter settings.

- File Type: Support to detect PE, APK, JAR, MS-Office, PDF, SWF, RAR and ZIP file.
- Protocol Type: Support to detect HTTP, FTP, POP3, SMTP and IMAP4 protocol.
- White list: A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox.
- File filter: Mark the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analysis result from the cloud sandbox determines whether this suspicious file is legal or not.
- Actions: When the suspicious file accesses the threat items in the local sandbox, system will deal with the malicious file with the set actions.

There are three built-in sandbox rules with the files and protocols type configured, white list enabled and file filter configured. The three default sandbox rules includes `predef_low`, `predef_middle` and `predef_high`.

- **predef_low**: A loose sandbox detection rule, whose file type is PE and protocol types are HTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.
- **predef_middle**: A middle-level sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF and protocol types are HTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.
- **predef_high**: A strict sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF/SWF/RAR/ZIP and protocol types are HTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.

To create a new sandbox rule, take the following steps:

1. Select **Object > Sandbox**.
2. Click **New** to create a new sandbox rule. To edit an existing one, select the check box of this rule and then click **Edit**.

The screenshot shows the 'Sandbox' configuration window. It includes a 'Name' field, 'White list' and 'Certificate verify' checkboxes (both enabled), and a 'File filter' section. The 'File filter' section contains a 'File type' dropdown and a 'Protocol' section with checkboxes for HTTP, SMTP, POP3, IMAP4, and FTP, each paired with an action dropdown (Upload or Download). The window has 'OK' and 'Cancel' buttons at the bottom.

In the Sandbox Configuration dialog box, configure the following settings.

Option	Description
Name	Enter the name of the sandbox rule.
White List	<p>Select Enable to enable the white list function.</p> <p>A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox.</p> <p>You can update the white list in System > Upgrade Management > Signature Database Update > Sandbox Whitelist Database Update.</p>
Certificate verify	Select Enable to enable the verification for the trusted certification. After enabling, system will not detect the PE file whose certification is trusted.
Actions	<p>When the suspicious file accesses the threat items in the local sandbox, system will deal with the malicious file with the set actions. Actions:</p> <ul style="list-style-type: none"> Record logs only - When detecting malicious files, system will pass traffic and record logs only (threat log and cloud sandbox log). Reset - When detecting malicious files, system will reset connection of malicious link and record threat logs and cloud sandbox logs only.
<p>File Filter: Mark the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analysis result from the cloud sandbox determines whether this suspicious file is legal or not. The logical relation is AND.</p>	
File Type	Mark the file of the specified file type as a suspicious file. The system can mark the PE(.exe), APK, JAR, MS-Office, PDF, SWF, RAR and ZIP file as a suspicious file now. If no file type is specified, the Sandbox function will mark no file as a suspicious one.
Protocol	<p>Specifies the protocol to scan. System can scan the HTTP, FTP, POP3, SMTP and IMAP4 traffic now. If no protocol is specified, the Sandbox function will not scan the network traffic.</p> <p>After specifying the protocol type, you have to specify the direction of the detection:</p> <ul style="list-style-type: none"> Upload - The direction is from client to server. Download - The direction is from server to client. Bothway - The direction includes uploading and downloading directions.
File Size	Mark the file that is smaller than the specified file size as a suspicious file. By default, system will mark the files that are smaller than 6M as suspicious files.

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

Threat List

The threat list means the list of threat items in the local sandbox. There are two sources of the threat items:

- The local sandbox finds suspicious files and reports to cloud. After verifying the file is malicious, the cloud will send the synchronous threat information to other devices, which has connected to the cloud and enabled Sandbox function. After the device receiving the synchronous threat information and matching the threat, the threat item will be listed in the threat list and system will block it with the set actions.
- The local sandbox finds suspicious file and reports to cloud. The cloud then analyzes and returns the result to the device. If the result is malicious, the threat item will be listed in the threat list.

You can filter and check threat items through specifying MD5 or the name of virus on the threat list page, as well as add the selected threat item to trust list. Take the following steps:

1. Click **Object > Sandbox > Threat List**.
2. Select the threat item that needs to be added to the trust list and click **Add to Trust List** button. When threat item is added, once it's matched, the corresponding traffic will be released.

Trust List

You can view all the sandbox threat information which can be detected on the device and add them to the trust list. Once the item in trust list is matched, the corresponding traffic will be released and not controlled by the actions of sandbox rule.

To remove threat items in the trust list, take the following steps:

1. Click **Object > Sandbox > Trust List**.
2. Select the threat item that needs to be removed in the trust list and click **Remove from Trust List** button. The threat item will be removed from the trust list.

Sandbox Global Configurations

To configure the sandbox global configurations, take the following steps:

1. Select **Object > Sandbox > Configuration**.
2. Select **Enable** check box of Sandbox to enable the Sandbox function. Clear the Enable check box to disable the Sandbox function.
3. Specify the file size for the files you need. The file that is smaller than the specified file size will be marked as a suspicious file.
4. If you select **Benign file** check box, system will record cloudsandbox logs of the file when it marks it as a benign file. By default, system will not record logs for the benign files.
5. If you select **Greyware** file check box, system will record cloudsandbox logs of the file when it marks it as a greyware file. A greyware file is the one system cannot judge it is a benign file or a malicious file. By default, system will not record logs for the greyware files.
6. Click **OK** to save the settings.

Critical Assets

Critical assets refer to IT assets owned by a company that are essential to its ability to operate and make profit. Those assets include key servers, networking devices, data storage server etc. Since critical assets are essential for day-to-day business operations, they are grown to targets of cyber-attacks. Therefore, the critical assets in a company need to be secured and protected with even stronger defense mechanisms comparing with other individual host machines.

After configuring the critical asset object, system will automatically enable the advanced threat detection and abnormal behavior detection functions in the select security zone, protect the priority and resource for critical asset monitoring, and display the related threat and traffic of the critical asset in the Critical Assets page in iCenter.

Configuring Critical Asset Object

To configure the critical asset object, take the following steps:

1. Select **Object > Critical Assets**.
2. Click **New**.

The screenshot shows a 'Critical Assets' dialog box with the following fields and options:

- Name:** A text input field with a character count '(1 - 31) chars'.
- Zone:** A dropdown menu currently showing 'mgt'.
- IP:** A text input field.
- Description:** A text input field with a character count '(0 - 255) chars'.
- Web Server Advanced Protection:** An unchecked checkbox.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

In Critical Assets dialog box, configure the settings.

Option	Description
Name	Specify the name of the critical asset object.
Zone	Specify the security zone where this object is located. Enable Abnormal Behavior Detection and Advanced Threat Detection function on the selected zone.
IP	Specify the IP address of the critical asset.
Web Server Advanced Protection	<p>Select the Web Server Advanced Protection check box if the critical asset is a Web server. Selecting this check box can detect the following types of attacks and behavior:</p> <ul style="list-style-type: none"> • Web Vulnerability Scan: A web vulnerability scanner is a program which communicates with a web application through the web front-end in order to identify potential security vulnerabilities in the web application and architectural weaknesses. • Http-based DoS Attack: Denial of service (DoS) usually refers to an attack that attempts to make a computer resource unavailable to its intended users by flooding a network or server with requests and data. As the name suggests, Http-Based DoS Attack is based on http protocol. • Web Spider : A Web spider is an internet bot that systematically browses the World Wide Web, typically for the purpose of Web indexing. Web search engines and some other sites use a web spider to update their web content or indexes others' sites' web content. Web spider can copy all of the pages they visit for later processing by a search engine that indexes the downloaded pages so that users can search them much more quickly.
Description	Enter the description for this object.

Attack-Defense

There are various inevitable attacks in networks, such as compromise or sabotage of servers, sensitive data theft, service intervention, or even direct network device sabotage that causes service anomaly or interruption. Security gates, belonging to a category of network security devices, must be designed with attack defense functions to detect various types of network attacks, and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.

Devices provide attack defense functions based on security zones, and can take appropriate actions against network attacks to assure the security of your network systems.

ICMP Flood and UDP Flood

An ICMP Flood/UDP Flood attack sends huge amounts of ICMP messages (such as ping)/UDP packets to a target within a short period and requests for a response. Due to the heavy load, the attacked target cannot complete its normal transmission task.

ARP Spoofing

LAN transmits network traffic based on MAC addresses. ARP spoofing attacks occur by filling in the wrong MAC address and IP address to make a wrong corresponding relationship of the target host's ARP cache table. This will lead to the wrong destination host IP packets, and the packet network's target resources will be stolen.

SYN Flood

Due to resource limitations, a server will only permit a certain number of TCP connections. SYN Flood just makes use of this weakness. During the attack an attacker will craft a SYN packet, set its source address to a forged or non-existing address, and initiate a connection to a server. Typically the server should reply the SYN packet with SYN-ACK, while for such a carefully crafted SYN packet, the client will not send any ACK for the SYN-ACK packet, leading to a half-open connection. The attacker can send large amount of such packets to the attacked host and establish an equally large number of half-open connections until timeout. As a result, resources will be exhausted and normal accesses will be blocked. In the environment of unlimited connections, SYN Flood will exhaust all the available memory and other resources of the system.

WinNuke Attack

A WinNuke attack sends OOB (out-of-band) packets to the NetBIOS port (139) of a Windows system, leading to NetBIOS fragment overlap and host crash. Another attacking vector is IGMP fragment. Generally an ICMP packet will not be fragmented; so many systems cannot properly process IGMP fragments. If your system receives any IGMP fragment, it's almost certain that the system is under attack.

IP Address Spoofing

IP address spoofing is a technology used to gain unauthorized access to computers. An attacker sends packets with a forged IP address to a computer, and the packets are disguised as if they were from a real host. For applications that implement validation based on IP addresses, such an attack allows unauthorized users to gain access to the attacked system. The attacked system might be compromised even if the response packets cannot reach the attacker.

IP Address Sweep and Port Scan

This kind of attack makes a reconnaissance of the destination address and port via scanners, and determines the existence from the response. By IP address sweeping or port scanning, an attacker can determine which systems are alive and connected to the target network, and which ports are used by the hosts to provide services.

Ping of Death Attack

Ping of Death is designed to attack systems by some over-sized ICMP packets. The field length of an IP packet is 16 bits, which means the max length of an IP packet is 65535 bytes. For an ICMP response packet, if the data length is larger than 65507 bytes, the total length of ICMP data, IP header (20 bytes) and ICMP header (8 bytes) will be larger than 65535 bytes. Some routers or systems cannot properly process such a packet, and might result in crash, system down or reboot.

Teardrop Attack

Teardrop attack is a denial of service attack. It is a attack method based on morbid fragmented UDP packets, which works by sending multiple fragmented IP packets to the attacker (IP fragmented packets include the fragmented packets of which packet, the packet location, and other information). Some operating systems contain overlapping offset that will crash, reboot, and so on when receiving fragmented packets.

Smurf Attack

Smurf attacks consist of two types: basic attack and advanced attack. A basic Smurf attack is used to attack a network by setting the destination address of ICMP ECHO packets to the broadcast address of the attacked network. In such a condition all the hosts within the network will send their own response to the ICMP request, leading to network congestion. An advanced Smurf attack is mainly used to attack a target host by setting the source address of ICMP ECHO packets to the address of the attacked host, eventually leading to host crash. Theoretically, the more hosts in a network, the better the attacking effect will be.

Fraggle Attack

A fraggle attack is basically the same with a smurf attack. The only difference is the attacking vector of fraggle is UDP packets.

Land Attack

During a Land attack, an attacker will carefully craft a packet and set its source and destination address to the address of the server that will be attacked. In such a condition the attacked server will send a message to its own address, and this address will also return a response and establish a Null connection. Each of such connections will be maintained until timeout. Many servers will crash under Land attacks.

IP Fragment Attack

An attacker sends the victim an IP datagram with an offset smaller than 5 but greater than 0, which causes the victim to malfunction or crash.

IP Option Attack

An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets.

Huge ICMP Packet Attack

An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack.

TCP Flag Attack

An attacker sends packets with defective TCP flags to probe the operating system of the target host. Different operating systems process unconventional TCP flags differently. The target system will break down if it processes this type of packets incorrectly.

DNS Query Flood Attack

The DNS server processes and replies to all DNS queries that it receives. A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries.

TCP Split Handshake Attack

When a client establishes TCP connection with a malicious TCP server, the TCP server will respond to a fake SYN packet and use this fake one to initialize the TCP connection with the client. After establishing the TCP connection, the malicious TCP server switches its role and becomes the client side of the TCP connection. Thus, the malicious traffic might enter into the intranet.

Configuring Attack Defense

To configure the Attack Defense based on security zones, take the following steps:

1. Create a zone. For more information, refer to ["Security Zone" on Page 44](#).
2. In the Zone Configuration dialog box, select Threat Protection tab.
3. To enable the Attack Defense functions, select the Enable all check box, and click **Configure**.

Attack Defense

Whitelist

Configure

Select All

☐ Enable All

Action: Drop

Flood Attack Defense

☒ ICMP Flood

Threshold: 1500 (1-50,000) Action: Drop

☒ UDP Flood

Src Threshold: 1500 (0-300,000) Action: Drop

Dst Threshold: 1500 (0-300,000)

☐ ARP Spoofing

Max IP Number Per MAC: 0 (0-1,024) Action: Drop

ARP Send Rate: 0 (0-10) ☐ Reverse Query

☒ SYN Flood

Src Threshold: 1500 (0-50,000) Action: Drop

Dst Threshold:

☒ IP-based 1500 (0-50,000)
☐ Port-based 1500 (0-50,000)

MS-Windows Defense

☒ Win Nuke Attack

Scan/Spoof Defense

☒ IP Address Spoof

☒ IP Address Sweep

Threshold: 1 (1-5,000) Action: Drop

☒ Port Scan

Threshold: 1 (1-5,000) Action: Drop

Denial of Service Defense

☒ Ping of Death Attack

☒ Teardrop Attack

☒ IP Fragment

Action: Drop

☒ IP Option

Action: Drop

☒ Smurf or Fragile Attack

Action: Drop

☒ Land Attack

Action: Drop

☐ Large ICMP Packet

Threshold: 1024 (1-50,000) Action: Drop

Proxy

☐ SYN Proxy

Proxy trigger rate: 1000 (0-50,000) ☐ cookie

Max SYN packet rate: 3000 (1-1,500,000) Timeout: 30 (1-180 seconds)

Protocol Anomaly Report

☐ TCP anomalies

Action: Drop

DNS query flood

☐ DNS query flood

Src Threshold: 1500 (0-300,000) Action: Drop

Dst Threshold: 1500 (0-300,000)

☐ Recursive DNS query flood

Src Threshold: 1000 (0-300,000) Action: Drop

Dst Threshold: 1000 (0-300,000)

Restore Default

OK

Cancel

In the <Attack Defense> dialog box, enter the Attack Defense configurations.

Option	Description
Whitelist	IP address or IP range in the whitelist is exempt from attack defense check. click Configure .

Option	Description
	<ul style="list-style-type: none"> IP/Netmask - Specifies the IP address and netmask and click Add to add to the whitelist. Address entry - Specifies the address entry and click Add to add to the whitelist.
Select all	<p>Enable all: Select this check box to enable all the Attack Defense functions for the security zone.</p> <p>Action: Specifies an action for all the Attack Defense functions, i.e., the defense measure system will be taken if any attack has been detected.</p> <ul style="list-style-type: none"> Drop - Drops packets. This is the default action. Alarm - Gives an alarm but still permits packets to pass through. --- - Do not specify global actions.
Flood Attack Defense	<p>ICMP flood: Select this check box to enable ICMP flood defense for the security zone.</p> <ul style="list-style-type: none"> Threshold - Specifies a threshold for inbound ICMP packets. If the number of inbound ICMP packets matched to one single IP address per second exceeds the threshold, system will identify the traffic as an ICMP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. Action - Specifies an action for ICMP flood attacks. If the default action Drop is selected, system will only permit the specified number (threshold) of ICMP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. <p>UDP flood: Select this check box to enable UDP flood defense for the security zone.</p> <ul style="list-style-type: none"> Src threshold - Specifies a threshold for outbound UDP packets. If the number of outbound UDP packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. Dst threshold - Specifies a threshold for inbound UDP packets. If the number of inbound UDP packets destined to one single port of one single destination IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. Action - Specifies an action for UDP flood attacks. If the default action Drop is selected, system will only permit the specified number (threshold) of UDP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. <p>ARP spoofing: Select this check box to enable ARP spoofing defense for the security zone.</p> <ul style="list-style-type: none"> Max IP number per MAC - Specifies whether system will check the IP number per MAC in the ARP table. If the parameter is set to 0, system will not check the IP number; if it is set to a value other than 0, system will check the IP number, and if the IP number per MAC is larger than the parameter value, system will take the spe-

Option	Description
	<p>cified action. The value range is 0 to 1024.</p> <ul style="list-style-type: none"> • Gratuitous ARP send rate - Specifies if StoneOS will send gratuitous ARP packet(s). If the parameter is set to 0 (the default value), StoneOS will not send any gratuitous ARP packet; if it is set to a value other than 0, StoneOS will send gratuitous ARP packet(s), and the number sent per second is the specified parameter value. The value range is 0 to 10. • Reverse query - Select this check box to enable Reverse query. When StoneOS receives an ARP request, it will log the IP address and reply with another ARP request; and then StoneOS will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ARP request packet. <p>SYN flood: Select this check box to enable SYN flood defense for the security zone.</p> <ul style="list-style-type: none"> • Src threshold - Specifies a threshold for outbound SYN packets (ignoring the destination IP address and port number). If the number of outbound SYN packets originating from one single source IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Src threshold is void. • Dst threshold - Specifies a threshold for inbound SYN packets destined to one single destination IP address per second. <ul style="list-style-type: none"> • IP-based - Click IP-based and then type a threshold value into the box behind. If the number of inbound SYN packets matched to one single destination IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Dst threshold is void. • Port-based - Click Port-based and then type a threshold value into the box behind. If the number of inbound SYN packets matched to one single destination port of the destination IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Dst threshold is void. After clicking Port-based, you also need to type an address into or select an IP Address or Address entry from the Dst address combo box to enable port-based SYN flood defense for the specified segment. The SYN flood attack defense for other segments will be IP based. The value range for the mask of the Dst address is 24 to 32. • Action - Specifies an action for SYN flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of SYN packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. Besides if Src threshold and Dst threshold are also configured, StoneOS will first detect if the traffic is a destination SYN flood attack: if so, StoneOS will drop the packets and give an alarm, if not, StoneOS will continue to detect if the traffic is a source SYN attack.
MS-Windows defense	WinNuke attack: Select this check box to enable WinNuke attack defense for the security zone. If any WinNuke attack has been detected, StoneOS

Option	Description
Scan/spoof defense	will drop the packets and give an alarm.
	<p>IP address spoof: Select this check box to enable IP address spoof defense for the security zone. If any IP address spoof attack has been detected, StoneOS will drop the packets and give an alarm.</p> <p>IP address sweep: Select this check box to enable IP address sweep defense for the security zone.</p> <ul style="list-style-type: none"> Threshold - Specifies a time threshold for IP address sweep. If over 10 ICMP packets from one single source IP address are sent to different hosts within the period specified by the threshold, StoneOS will identify them as an IP address sweep attack. The value range is 1 to 5000 milliseconds. The default value is 1. Action - Specifies an action for IP address sweep attacks. If the default action Drop is selected, StoneOS will only permit 10 ICMP packets originating from one single source IP address while matched to different hosts to pass through during the specified period (threshold), and also give an alarm. All the excessive packets of the same type will be dropped during this period. <p>Port scan: Select this check box to enable port scan defense for the security zone.</p> <ul style="list-style-type: none"> Threshold - Specifies a time threshold for port scan. If over 10 TCP SYN packets are sent to different ports of one single destination address within the period specified by the threshold, StoneOS will identify them as a port scan attack. The value range is 1 to 5000 milliseconds. The default value is 1. Action - Specifies an action for port scan attacks. If the default action Drop is selected, StoneOS will only permit 10 TCP SYN packets destined to different ports of one single destination address to pass through, and also give an alarm. All the excessive packets of the same type will be dropped during this period.
Denial of service defense	<p>Ping of Death attack: Select this check box to enable Ping of Death attack defense for the security zone. If any Ping of Death attack has been attacked, StoneOS will drop the attacking packets, and also give an alarm.</p> <p>Teardrop attack: Select this check box to enable Teardrop attack defense for the security zone. If any Teardrop attack has been attacked, StoneOS will drop the attacking packets, and also give an alarm.</p> <p>IP fragment: Select this check box to enable IP fragment defense for the security zone.</p> <ul style="list-style-type: none"> Action - Specifies an action for IP fragment attacks. The default action is Drop. <p>IP option: Select this check box to enable IP option attack defense for the security zone. StoneOS will defend against the following types of IP options: Security, Loose Source Route, Record Route, Stream ID, Strict Source Route and Timestamp.</p> <ul style="list-style-type: none"> Action - Specifies an action for IP option attacks. The default action is Drop. <p>Smurf or fraggle attack: Select this check box to enable Smurf or fraggle attack defense for the security zone.</p>

Option	Description
	<ul style="list-style-type: none"> Action - Specifies an action for Smurf or fraggle attacks. The default action is Drop. <p>Land attack: Select this check box to enable Land attack defense for the security zone.</p> <ul style="list-style-type: none"> Action - Specifies an action for Land attacks. The default action is Drop. <p>Large ICMP packet: Select this check box to enable large ICMP packet defense for the security zone.</p> <ul style="list-style-type: none"> Threshold - Specifies a size threshold for ICMP packets. If the size of any inbound ICMP packet is larger than the threshold, StoneOS will identify it as a large ICMP packet and take the specified action. The value range is 1 to 50000 bytes. The default value is 1024. Action - Specifies an action for large ICMP packet attacks. The default action is Drop.
Proxy	<p>SYN proxy: Select this check box to enable SYN proxy for the security zone. SYN proxy is designed to defend against SYN flood attacks in combination with SYN flood defense. When both SYN flood defense and SYN proxy are enabled, SYN proxy will act on the packets that have already passed detections for SYN flood attacks.</p> <ul style="list-style-type: none"> Proxy trigger rate - Specifies a min number for SYN packets that will trigger SYN proxy or SYN-Cookie (if the Cookie check box is selected). If the number of inbound SYN packets matched to one single port of one single destination IP address per second exceeds the specified value, StoneOS will trigger SYN proxy or SYN-Cookie. The value range is 1 to 50000. The default value is 1000. Cookie - Select this check box to enable SYN-Cookie. SYN-Cookie is a stateless SYN proxy mechanism that enables StoneOS to enhance its capacity of processing multiple SYN packets. Therefore, you are advised to expand the range between "Proxy trigger rate" and "Max SYN packet rate" appropriately. Max SYN packet rate - Specifies a max number for SYN packets that are permitted to pass through per second by SYN proxy or SYN-Cookie (if the Cookie check box is selected). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, StoneOS will only permit the specified number of SYN packets to pass through during the current and the next second. All the excessive packets of the same type will be dropped during this period. The value range is 1 to 1500000. The default value is 3000. Timeout - Specifies a timeout for half-open connections. The half-open connections will be dropped after timeout. The value range is 1 to 180 seconds. The default value is 30.
Protocol abnormally report	<p>TCP option anomaly: Select this check box to enable TCP option anomaly defense for the security zone.</p> <ul style="list-style-type: none"> Action - Specifies an action for TCP option anomaly attacks. The default action is Drop. <p>TCP split handshake: Select this check box to enable TCP split handshake defense for the security zone.</p>

Option	Description
	<ul style="list-style-type: none"> Action - Specifies an action for TCP split handshake attacks. The default action is Drop.
DNS query flood	<p>DNS query flood: Select this check box to enable DNS query flood defense for the security zone.</p> <ul style="list-style-type: none"> Src threshold - Specifies a threshold for outbound DNS query packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. Dst threshold - Specifies a threshold for inbound DNS query packets. If the number of inbound DNS query packets matched to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. Action - Specifies an action for DNS query flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the DNS query packets to pass through. <p>Recursive DNS query flood: Select this check box to enable recursive DNS query flood defense for the security zone.</p> <ul style="list-style-type: none"> Src threshold - Specifies a threshold for outbound recursive DNS query packets packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. Dst threshold - Specifies a threshold for inbound recursive DNS query packets packets. If the number of inbound DNS query packets destined to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. Action - Specifies an action for recursive DNS query flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of recursive DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the recursive DNS query packets to pass through.

4. To restore the system default settings, click **Restore Default**.

5. Click **OK**.

Perimeter Traffic Filtering

Perimeter Traffic Filtering can filter the perimeter traffic based on known IP of black/white list, and take block action on the malicious traffic that hits the blacklist.

Black/White list includes the following three types:

- Predefined black list: Retrieve the IP of black/white list from the Perimeter Traffic Filtering signature database.
- User-defined black/white list : According to the actual needs of users, the specified IP address is added to a user-defined black/white list.
- Third-party black list: Make a linkage with trend of TDA, to get blacklisted from the trend TDA devices regularly.



Note:

- You need to update the IP reputation database before enabling the function for the first time. By default, system will update the database at the certain time everyday, and you can modify the updating settings according to your own requirements, see "[Upgrading System](#)" on Page 494.
- Perimeter Traffic Filtering is controlled by license. To use Threat protection, apply and install the PTF license.

Enabling Perimeter Traffic Filtering

To realize the zone-based Perimeter Traffic Filtering, take the following steps:

1. Create a zone. For more information , refer to "[Security Zone](#)" on Page 44;
2. In the Zone Configuration dialog box, select Threat Protection tab.
3. Select the **Enable** check box after the **Perimeter Traffic Filtering**.
4. Specifies an action for the malicious traffic that hits the blacklist. Select the **User-defined** , **Pre-defined** or **TDA** check box , and select the action from drop-down list:
 - Log Only: Only generates logs if the malicious traffic hits the blacklist. This is the default option.
 - Drop: Drop packets if the malicious traffic hits the blacklist.

Configuring User-defined Black/White List

To configure the user-defined black/white list , take the following steps:

1. Select **Object > Perimeter Traffic Filtering**.
2. Click **New**.

The image shows a dialog box titled "Perimeter Traffic Filtering Configuration". It has a close button (X) in the top right corner. Inside the dialog, there are two input fields: "IP:" and "mask:". Below these fields, there are two radio buttons: "Black list" (which is selected) and "White list". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

In Perimeter Traffic Filtering Configuration dialog box, enter the user-defined black/white list

configuration.

Option	Description
IP	Specify the IP address for the user-defined black/white list.
mask	Specify the netmask of the IP address.
Black/White List	Select the radio button to add the IP address to the blacklist or whitelist .

3. Click **OK**.

Configuring Third-party Black List

To configure the third-party linkage, take the following steps:

1. Select **Object > Perimeter Traffic Filtering**.
2. Click **The Third Party linkage**.

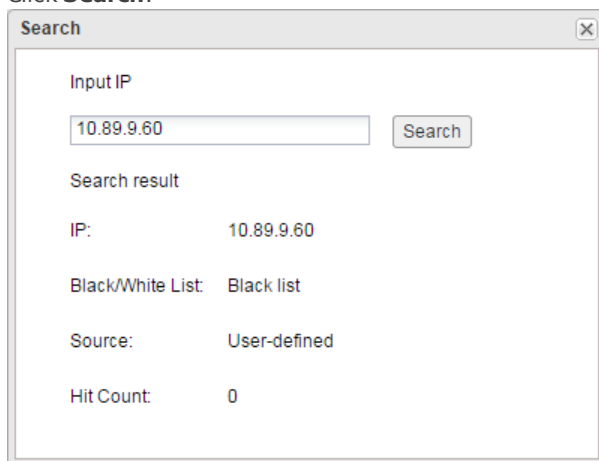
In The Third Party linkage dialog box, enter the linkage configuration.

Option	Description
Enable linkage with trend of TDA	Select the check box to enabling linkage with trend of TDA.
The TDA device address	Specify the address for the TDA device.
The TDA device port	Specify the port number for the TDA device. The value range is 1 to 65535.
Linkage request cycle	Specify the Linkage request period for getting the blacklisted from the TDA devices.
Enable Linkage with sandbox	Select the check box to get the blacklist of the TDA device sandbox.

Searching Black/White List

To search the black/white list, take the following steps:

1. Select **Object > Perimeter Traffic Filtering**.
2. Click **Search**.



The screenshot shows a 'Search' dialog box with a title bar containing a close button. Inside the dialog, there is a section labeled 'Input IP' with a text input field containing '10.89.9.60' and a 'Search' button to its right. Below this is a 'Search result' section containing four lines of text: 'IP: 10.89.9.60', 'Black/White List: Black list', 'Source: User-defined', and 'Hit Count: 0'.

Search result	
IP:	10.89.9.60
Black/White List:	Black list
Source:	User-defined
Hit Count:	0

3. Enter the IP address and click **Search**. The results will be displayed in this dialog box.

Abnormal Behavior Detection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

There are various threat attacks in networks, such as Web server attacks ,DoS Flood attacks, application layer attacks , Port/Server scan attacks , Amplification attacks, SSL attacks etc. These threats have demonstrated a wide variety of abnormal behaviors. System provide an abnormal behavior detection function based on security zones. This function inspects the sessions of the detected object in multiple factors. When one detected object has multiple abnormal parameters, system will analyze the relationship among the abnormal parameters to see whether an abnormal behavior formed. If there is an abnormal behavior, system will send the alarm message and generate the threat log(s).

The followings are the concept description of the Abnormal Behavior Detection:

- Detected object: The protected objects configured in the Host Defender in this chapter and the protected objects configured in ["Configuring Critical Asset Object" on Page 380](#).
- Parameter: The basic statistical factor of a session, like the received bytes of inbound sessions per second. The statistical values of the parameters are used by the system to judge whether the detected object is abnormal or not.
- Baseline: The baseline is the benchmark for the parameters. Value of the baseline is calculated by the system according to the historical data. When the baseline value is higher than the upper limit or lower than the lower limit, the baseline value is considered to be abnormal. If several baseline values of the detected object are abnormal, system will analyze the association of these abnormal baselines, and use discretion in deciding whether this detected object has abnormal behavior. If it has abnormal behavior, system will generate threat logs.
- Abnormal behavior mode database: The abnormal behavior mode database includes the abnormal information of the traffic, which are detecting rules, description of the abnormalities, the reason for the abnormalities, and the suggestions. The information in the database helps you analyze and resolve the abnormal problems. By default, system will update the database at the certain time everyday, and you can modify the updating settings according to your own requirements. System supports automatically update and manual update, see ["Upgrading System" on Page 494](#).



Note: Abnormal Behavior Detection is controlled by license. To use Abnormal Behavior Detection, apply and install the StoneShield license.

Host Defender

You can enable the Host Defender function for the specific zone. Enabling this function can achieve the following targets:

- Establish a data model for each host whose host name can be identified
- Analyze the network behavior of host
- Define the corresponding signature dimension for different network behaviors.
- Detect the abnormal behavior of the host based on the signature dimension and find the more hidden threat attack.

The results are displayed in the iCenter page. For more information, see [Viewing the Abnormal Behavior Detection Information](#).

To enable Host Defender, take the following steps:

1. Create a zone. For more information, refer to ["Security Zone" on Page 44](#);
2. In the Zone Configuration dialog box, select Threat Protection tab.

3. Select the **Enable** check box after the **Abnormal Behavior Detection**.
4. Select the **Host Defender** check box. To enable the abnormal behavior detection of the HTTP factor, select the **Advanced Protection** check box. To enable the DDoS protection for the host, select the **DDoS Protection** check box. To capture and save the corresponding evidence that leads to the alarm of abnormal behavior, select **Forensic**.

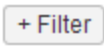
DNS Defender

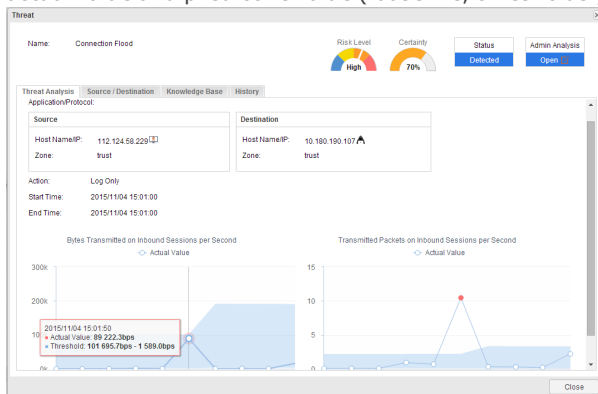
DNS, as the domain name resolution protocol, is designed to resolve fixed domain names to IP addresses. Due to the use of convenient and widely used domain names, the attacker will take different means to use the domain name to generate an attack. For example, an IP address can correspond to multiple domain name. The server, according to the Host field of the HTTP packet, can find the Goal URL, which the malware will use by modifying the Host field to disguise the domain name and generate the abnormal behavior. DGA, domain generation algorithm, will generate a large number of pseudo random domain names that will be used by the malware. ISP DNS hijack adds some of the malicious domain names used by the malicious software to its blacklist.

To solve these problems, the DNS domain name analysis can be used as an important basis to determine the malicious behavior. System will monitor the DNS response packets after the host defender function is enabled and establish the DNS mapping list. The DNS mapping list is used to store domain names and IP addresses, the pseudo random domain name generated by DGA algorithm, and the black and white domain names updated from the cloud. The device can detect malware and abnormal behavior attacks according to the DNS mapping, generate the threat logs, and display the results in the iCenter page. For more information, see [Viewing the Abnormal Behavior Detection Information](#).

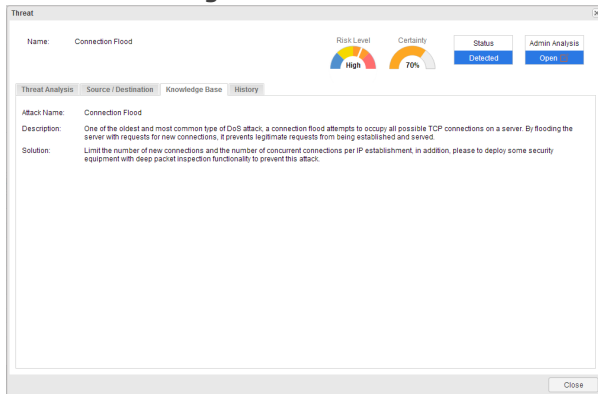
Viewing the Abnormal Behavior Detection Information

To view the Abnormal Behavior Detection information, take the following steps:

1. Select **iCenter**.
2. In Threats tab, click , select **Detected By** and **Abnormal Behavior Detection** in the drop-down list, and then click the threat entry name in the list.
3. Click the **Threat Analysis** tab and view the Abnormal Behavior Detection information and the trend chart of the actual value and predictive value (baseline, thresholds) of the detected object.



4. Click the **Knowledge Base** tab to view the threat attack description information.



Mitigation

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The system can identify the potential risks and network attacks dynamically, and take action on the risk that hits the mitigation rules.

Mitigation Rule

Mitigation rules includes the following two types:

- Predefined rule: This rule is retrieved from the Mitigation rule database. The predefined rules may vary by different mitigation signature databases. For more information about updating the signature database, see "Upgrading System" on Page 494
- User-defined rule: According to the user's needs, specify the trigger condition and action. For more information, see [Configuring a User-defined Mitigation Rules](#).



- Note:**
- Mitigation rules only for the threat types of Scan, Dos and Spam.
 - Predefined rule can not be edited or deleted.

Configuring a User-defined Mitigation Rule

To configure a user-defined mitigation rule, take the following steps:

1. Click **iCenter > Mitigation > Mitigation Rule**.
2. Click **New**.

In Mitigation Configuration dialog box, enter the user-defined mitigation rule configurations.

Description	
Description	Specify the description of user-defined mitigation rule.
Trigger Condition	
Log Type	Specify the log type of first level and second level for the trigger condition.
Severity	Specify the severity for the trigger condition.
Value	Specify the number of threat occurrences for the trigger condition.

Role	The role that this mitigation rule will affect. When selecting the User defined mitigation method, you can select the role.
Action	
Mitigation Method	<p>There are two mitigation methods:</p> <ul style="list-style-type: none"> • Auto-mitigation: For the risks that meet the trigger conditions, system will automatically adopt actions to mitigate risks and prevent threats. • Use defined: Customize your mitigation actions to the threats that meet the trigger conditions: <ul style="list-style-type: none"> • Session Control: By limiting the number of new sessions or concurrent sessions for the attacker, the consumption of resources is reduced, slowing the attack on the victim. • Bandwidth Control: By limiting the threat of an attacker's traffic, the threat of occupied bandwidth, CPU resources, etc. are reduced. • IP Block: By blocking the connection with the attacker, the victims are cut off from the threats.
Session Control	
Session Type	Specify the session type, which includes new session and concurrent session.
Total Number	Specify the limit of the total number of sessions. System will take action when the risk of attacker traffic is in a condition that triggers the system and when the number of sessions exceeds the total number. The value range is 1 to 1000000000.
Per Number	Specify the limit threshold for number of IPs connect with the victim's session. System will take action when the risk of the victim traffic is in a condition that triggers system and when the total number of IP exceeds the inputted number. The value range is 1 to 1000000.
Drop Percent	Specify the proportion for dropping the session packets .The range is 1 to 100%.
Timeouts	Specify the timeout value for dropping the session packets. The value range is 10 to 600 seconds.
Bandwidth Control	
Total Number	Specify the limit of the total number of bandwidth. System will take action when the risk of attacker traffic is in a condition that triggers system and the number of bandwidth exceeds the total number. The value range is 1 to 1000000000.
Per Number	Specify the limit threshold for the number of IP connected with the victim's bandwidth. System will take action when the risk of the victim traffic is in a condition that triggers system and the number of IP exceeds the inputted number. The value range is 1 to 1000000.
Drop Percent	Specify the proportion for dropping the bandwidth packets .The range is 1 to 100%.
Timeouts	Specify the timeout value for dropping the bandwidth packets. The value range is 10 to 600 seconds.
IP Block	
Timeouts	Specify the timeout value for block action. The value range is 10 to 600 seconds.

Auto-learning

Timeouts

Specify the timeout value for auto-learning action. The value range is 10 to 600 seconds.

3. Click **OK**.

Enabling Mitigation

After enabling mitigation, mitigation rules (user-defined rule and predefined rule) will take effect.

To enable the mitigation, take the following steps:

1. Click **iCenter > Mitigation>Mitigation Rule**.
2. Select the **Enable Mitigation** check box.

Viewing Mitigation Action

To view the mitigation action results details of mitigation rules, take the following steps:

1. Click **iCenter > Mitigation>Mitigation Action**.

Mitigation Action		Mitigation Rule					
Filter							
Source Address	Destination Address	Start Time	End Time	Mitigation Method	Status	Hit Count	Action Details
1 192.168.1.10	0.0.0.0	2015/11/20 17.5	2015/11/20 17.5	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
2 0.0.0.0	192.168.4.10	2015/11/20 14.3	2015/11/20 14.3	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
3 0.0.0.0	192.168.4.10	2015/11/20 13.5	2015/11/20 14.0	Auto-learning	Expired	1	Deny source IP: 192.168.1.100;
4 192.168.1.10	0.0.0.0	2015/11/20 13.5	2015/11/20 13.5	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
5 0.0.0.0	192.168.4.10	2015/11/20 13.5	2015/11/20 13.5	Auto-learning	Expired	10193	Deny source IP: 192.168.1.100;
6 192.168.1.10	0.0.0.0	2015/11/20 13.5	2015/11/20 13.5	Auto-learning	Expired	44711	Deny source IP: 192.168.1.100;
7 0.0.0.0	192.168.4.10	2015/11/20 10.3	2015/11/20 10.4	Auto-learning	Expired	575	Enable SYN cookie;Drop SYN packets based on the characteristics extracted from the IP/TCP protocols;
8 0.0.0.0	192.168.4.10	2015/11/20 10.3	2015/11/20 10.4	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
9 0.0.0.0	192.168.4.10	2015/11/27 18.0	2015/11/27 18.2	Auto-learning	Expired	3655	Enable SYN cookie;Drop SYN packets based on the characteristics extracted from the IP/TCP protocols;
10 0.0.0.0	192.168.4.10	2015/11/27 18.0	2015/11/27 18.0	Auto-learning	Expired	3	Deny source IP: 192.168.1.100;
11 192.168.1.10	0.0.0.0	2015/11/27 14.1	2015/11/27 14.1	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
12 192.168.1.10	0.0.0.0	2015/11/27 11.3	2015/11/27 11.3	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
13 0.0.0.0	192.168.4.10	2015/11/25 18.0	2015/11/25 18.0	Auto-learning	Expired	0	Drop no session TCP FIN packet;Drop FIN packets based on the characteristics extracted from the IP/TCP protocols;
14 0.0.0.0	192.168.4.10	2015/11/25 18.0	2015/11/25 18.1	Auto-learning	Expired	12	Deny source IP: 192.168.1.100;
15 192.168.1.10	0.0.0.0	2015/11/25 18.0	2015/11/25 18.0	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
16 0.0.0.0	192.168.4.10	2015/11/24 16.0	2015/11/24 16.5	Auto-learning	Expired	12258	Enable SYN cookie;Drop SYN packets based on the characteristics extracted from the IP/TCP protocols;
17 0.0.0.0	192.168.4.10	2015/11/24 16.0	2015/11/24 16.0	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
18 0.0.0.0	192.168.4.10	2015/11/24 14.2	2015/11/24 14.2	Auto-learning	Expired	0	Drop no session TCP FIN packet;Drop FIN packets based on the characteristics extracted from the IP/TCP protocols;
19 0.0.0.0	192.168.4.10	2015/11/24 14.2	2015/11/24 14.2	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
20 0.0.0.0	192.168.4.10	2015/11/24 14.1	2015/11/24 14.1	Auto-learning	Expired	0	Drop no session TCP FIN packet;Drop FIN packets based on the characteristics extracted from the IP/TCP protocols;

2. As necessary, you can click Filter to view the mitigation action details of specified conditions.



Note: Support for fuzzy search, but does not support IP address search in accordance with the IP address containing mask.

Advanced Threat Detection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

Advanced Threat Detection learns advanced threat detection signatures to analyze the suspicious traffic of hosts, as well as detect malicious behavior and identify APT (Advanced Persistent Threat) attacks, and generates threat logs.



Note:

- You need to update the Malware behavior model database before enabling the function for the first time. By default, System will update the database at the certain time everyday, and you can modify the updating settings according to your own requirements. For more information, see ["Upgrading System" on Page 494](#).
- Advanced Threat Detection is controlled by license. To use Advanced Threat Detection, apply and install the StoneShield license.


Configuring Advanced Threat Detection

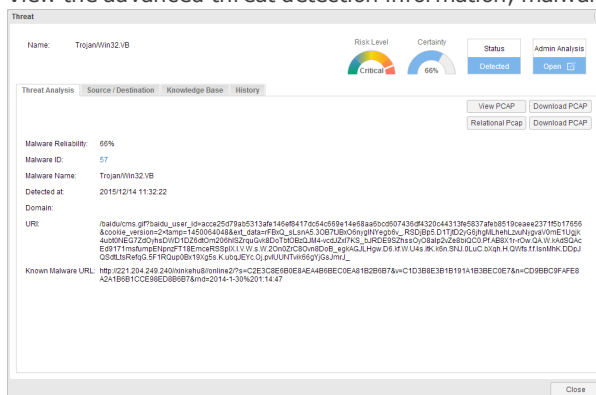
To realize the zone-based Advanced Threat Detection, take the following steps:

- Create a zone. For more information, refer to ["Security Zone" on Page 44](#);
- In the Zone Configuration dialog box, select Threat Protection tab.
- Select the **Enable** check box after the **Advanced Threat Detection**.
- If you need to capture packets, select the **Capture Packets** check box. System will save the evidence messages and have support to download it.

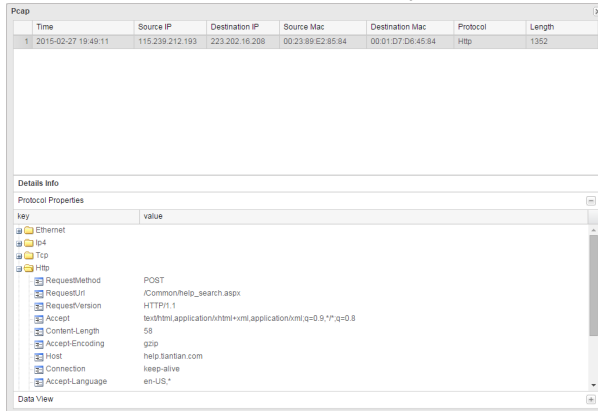
Viewing Advanced Threat Detection Information

To view the Advanced Threat Detection information, take the following steps:


- Select **iCenter**.
- In Threats tab, click , select **Detected By** and **Advanced Threat Detection** in the drop-down list, and then click threat entry name in the list.
- View the advanced threat detection information, malware reliability information and so on.

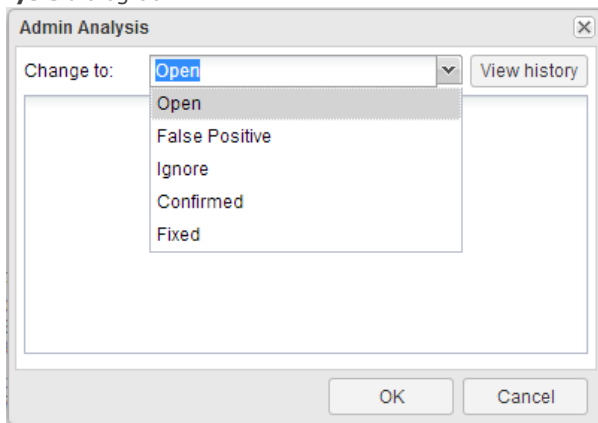


4. Click **View PCAP** to view the detail of packets.



5. Click **Download PCAP** to download the data packets.

6. Click  in **Admin Analysis**, and select the threat status from the **Change to** drop-down list in **Admin Analysis** dialog box.



- Open: When the threat entry status is 'Open', system will display it again next time.
- False Positive: When the threat entry status is ' False Positive ', system will upload it to the cloud and display it again next time.
- Ignore: When the threat entry status is 'Ignore ' , it will not participate in the 'Risk Index' score.
- Confirmed: When the threat entry status is 'Confirmed ' , system will display it again next time.
- Fixed: When the threat entry status is ' Fixed ' , it will not participate in the 'Network Risk Index' score.

Anti-Spam

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The system is designed with an Anti-Spam function, which enables user to identify and filter mails transmitted by SMTP and POP3 protocol through the cloud server, timely discover the mail threats, such as spam, phishing and worm mail, and then process the found spam according to the configuration, so as to protect the user's mail client or mail server.



Note: The Anti-Spam function will not work unless an Anti-Spam license has been installed on a StoneOS that supports Anti-spam.

Related Topics:

- ["Configuring Anti-Spam" on Page 403](#)
- ["Anti-Spam Global Configuration" on Page 406](#)

Configuring Anti-Spam

This chapter includes the following sections:

- Preparation for configuring Anti-Spam function
- Configuring Anti-Spam function

Preparing

Before enabling Anti-Spam, make the following preparations:

1. Make sure your system version supports Anti-Spam.
2. Import an Anti-Spam license and reboot. The Anti-Spam will be enabled after the rebooting.



Note: To assure a proper connection to the cloud server, you need to configure a DNS server for StoneOS before configuring the anti-spam.

Configuring Anti-Spam Function

The Anti-Spam configurations are based on security zones or policies.

- If a security zone is configured with the Anti-Spam function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based Anti-Spam, take the following steps:

1. Create a zone. For more information, refer to "[Security Zone](#)" on Page 44.
2. In the Zone Configuration dialog, select Threat Protection tab.
3. Enable the threat protection you need and select an Anti-Spam rule from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list. To create an Anti-Spam rule, see [Configuring an Anti-Spam Rule](#).
4. Click **OK** to save the settings.

To realize the zone-based Anti-Spam, take the following steps:

1. Create a security policy rule. For more information, refer to "[Security Policy](#)" on Page 296.
2. In the Policy Configuration dialog box, select the Protection tab.
3. Select the **Enable** check box of **Antispam**. Then select an Anti-Spam rule from the Profile drop-down list, or you can click **Add Profile** from the Profile drop-down list to create an Anti-Spam rule. For more information, see [Configuring an Anti-spam Rule](#).
4. Click **OK** to save the settings.

Configuring an Anti-Spam Rule

To configure an Anti-Spam rule, take the following steps:

1. Select **Object > Antispam > Profile**.
2. Click **New**

In the Anti-Spam Configuration dialog box, enter the Anti-Spam rule configurations

Option	Description
Basic Config	
Name	Specifies the rule name.
Type of Mail Protocol	Specifies the mail protocol (SMTP, POP3), spam category and action. spam category: <ul style="list-style-type: none"> Confirmed Spam: The mail from spam source. Bulk Spam: The malicious mass mail from uncertain spam sources. Suspected Spam: The mail from suspicious spam sources. Valid Bulk: Mass mail from legitimate senders. Action: <ul style="list-style-type: none"> Log Only - Only generates log. This is the default action. Reset Connection - If spams has been detected, system will reset connections. Note: The spams transferred over POP3 only supports generate logs action.
Exempt Domain of Sender	
Exempt Domain of Sender	The exempt domain of sender is used to specify the mail domains that will not be filtered by Anti-Spam. Each Anti-Spam profile can specify up to 16 exempt domains of sender. <ul style="list-style-type: none"> Click + to add exempt domain item. Type in the exempt domain name in the text box under the Mail Domain. The length is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters. Select the exempt domain of sender item, click -button to

Option	Description
	delete the exempt domain of sender.

3. Click **OK**.

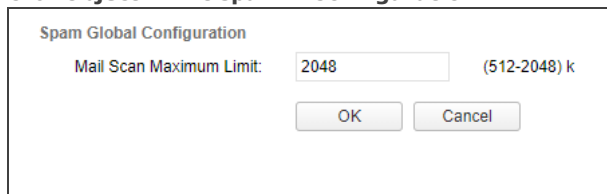


Note: By default, system comes with one default spams filtering rules: `predef_default`. The default rule is not allowed to edit or delete.

Anti-Spam Global Configuration

To configure the Anti-Spam global settings, take the following steps:

1. Click **Object > Antispam > Configuration**.



The screenshot shows a dialog box titled "Spam Global Configuration". Inside the dialog, there is a label "Mail Scan Maximum Limit:" followed by a text input field containing the value "2048". To the right of the input field, the range "(512-2048) k" is displayed. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

2. Type in the mail scan maximum limit in the **Mail Scan Maximum Limit** text box. The range is 512 Kb to 2048 Kb, the default value is 1024 Kb.
3. Click **OK** to save the settings.

Chapter 12 Monitor

The monitor section includes the following functions:

- **Monitor:** The Monitor function statistically analyzes the devices and displays the statistics in a bar chart, line chart, tables, and so on, which helps the users have information about the devices.
- **Alarm:** The warning function can analyze the warning information, and show the analysis results by combining the distribution chart and timeline.
- **Report:** Through gathering and analyzing the device traffic data, traffic management data, threat data, monitor data and device resource utilization data, the function provides the all-around and multi-dimensional staticstcs.
- **Log:** Records various system logs, including system logs, threat logs, session logs, NAT logs and configuration logs.

Monitor

System can monitor the following objects.

- **User:** Displays the application statistics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 week, latest 1 month , customized period) The statistics include the number of applications for the specific interface/zone,application traffic , new sessions and applications' concurrent sessions.
- **Application:** Displays the statistics of applications, application categories, application subcategories, application risk levels, application technologies, application characteristics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 week, latest 1 month , customized period). The statistics include the number of users for the specific interface/zone,application traffic and applications' concurrent sessions.
- **Cloud Application:** Displays statistics of cloud based applications, including their traffic, trend, new sessions and concurrent sessions.
- **Share Access Detect:** Displays the access terminal statistics of specified filter condition(Virtual router, IP, host number), including operation system , online time, login time and last online time of users.
- **Host:** Displays all of the risky hosts of the whole network.
- **QoS:** Displays the pipe traffic statistics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 week, latest 1 month , customized period).
- **Service/Network NodeMonitor:** Displays the statistics of packet loss rate and latency of service/network nodes.
- **Device:** Displays the device statistics within the specified period (Realtime,latest 5 minutes, latest 15 minutes, latest 1 hour, latest 1 day, latest 1 week, latest 1 month , customized period), including the total traffic, CPU/memory status, sessions and hardware status.
- **URL Hit:** If system is configured with "URL Filter" on Page 270, the predefined stat-set of URL Hit can gather statistics on user/IPs, URLs and URL categories.
- **Link State Monitor:** Displays the traffic statistics of the interfaces that have been bound within the specified period .
- **Authentication User:** If system is configured with "Web Authentication" on Page 124, "Single Sign-On" on Page 131, "SSL VPN" on Page 172 , "L2TP VPN" on Page 228 the auth user can gather statistics on the authenticated users.
- **Monitor Configuration:** Enable or disable some monitor items as needed.



Note: If IPv6 is enabled, system will count the total traffic/sessions/AD/URLs/applications of IPv4 and IPv6 address. Only User Monitor/Application Monitor/Cloud Application Monitor/Device Monitor/URL Hit/Application Block/User-defined Monitor support IPv6 address.

Host Monitor

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

Host monitor displays the statistics of the all of the risky hosts of the whole network.

Host Details

Host details displays the statistics of the all of the risky hosts of the whole network.

+ Filter

						Threats Detected			
HostName/IP		Zone	Active	Operating Sy...	Browser	Critical	High	Medium	Low
1	10.200.2.8	tapp				0	0	0	0
2	10.200.3.8	tapp				0	0	0	0
3	10.200.2.7	tapp				0	0	0	0
4	90.10.1.10	mgt				0	0	0	0
5	10.200.5.20	tapp				0	0	0	0
6	10.192.5.7	tapp				0	0	0	0
7	10.180.144.8	tapp				0	0	0	0
8	10.180.146.6	tapp				0	0	0	0
9	10.88.13.10	tapp				0	0	0	0
10	172.16.0.10	tapp				0	0	0	2
11	10.230.0.112	tapp				0	0	0	0
12	10.180.122.9	internal-zone				0	0	0	0
13	172.21.225.221	tapp				0	0	0	0
14	10.230.0.82	tapp				0	0	0	0
15	10.190.197.8	tapp				0	0	0	0
16	169.254.254.253	internal-zone				0	0	0	0
17	172.16.3.17	tapp				0	0	0	0
18	192.168.1.163	tapp				0	0	0	0
19	192.168.31.180	tapp				0	0	0	0
20	172.16.38.159	tapp				0	0	0	0

Page 1 / 124 | Displaying 1 - 20 of 2475 | 20 Per Page

- Click , and click to select the condition in the drop-down list to search for the risky hosts.

Share Access Detect

To detect the users' private behavior of shared access to the Internet, system supports to analyze the User-agent filed of HTTP packet, a share access detect method which is based on the application characteristic. The share access detect page can display the share access detect information with specified filter condition. The aging time of share access detect information is 2 hours.

Click **Monitor> Share Access Detect**.

Virtual Router: <div>trust-vr</div> <div>+ Filter</div>		
IP	Host Number	Login Time
10.89.10.31	1	2016/12/01 00:54:55

- From **Virtual Router** drop-down menu, select the virtual router the IP belongs to. By default ,it is trust-vr.
- Click the **Filter** button and select **IP**. In the drop-down menu, select the source IP's IP information you want to view. You can select 1 IP address.
- Click the **Filter** button and select **Host Number>=**. In the drop-down menu, select the minimum host number of IP information you want to view.
- After configuring filter condition, the upside list will display the information of IP, host number and IP login time, which is matched with the configured filter condition. Click an entry of IP information and the downside list will display the share access detect of this IP, which includes operation system, online time, login time and last online time of users.

IQoS Monitor

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

QoS monitor can be generated under the conditions that configuring pipes and enabling IQoS feature.

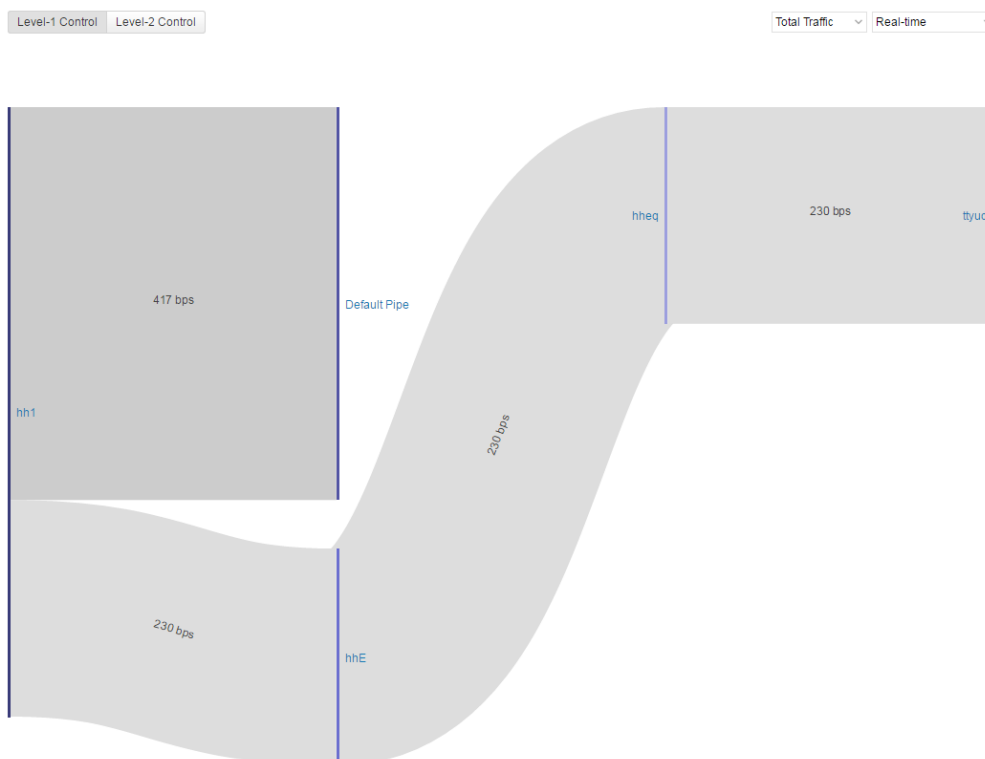
After the IQoS policy is configured and the IQoS function is enabled, QoS monitor can display the real-time and historical traffic information of the first layer flow control and the second layer flow control.



Note: The IQoS monitor function is controlled by license, To use the function, install the IQoS license .For more information on license, please refer to the [License](#) .

IQoS Summary

The summary page displays the statistics for pipe traffic for the specified time period in the form of a pipe chart. Click **Monitor > IQoS > IQoS Summary**



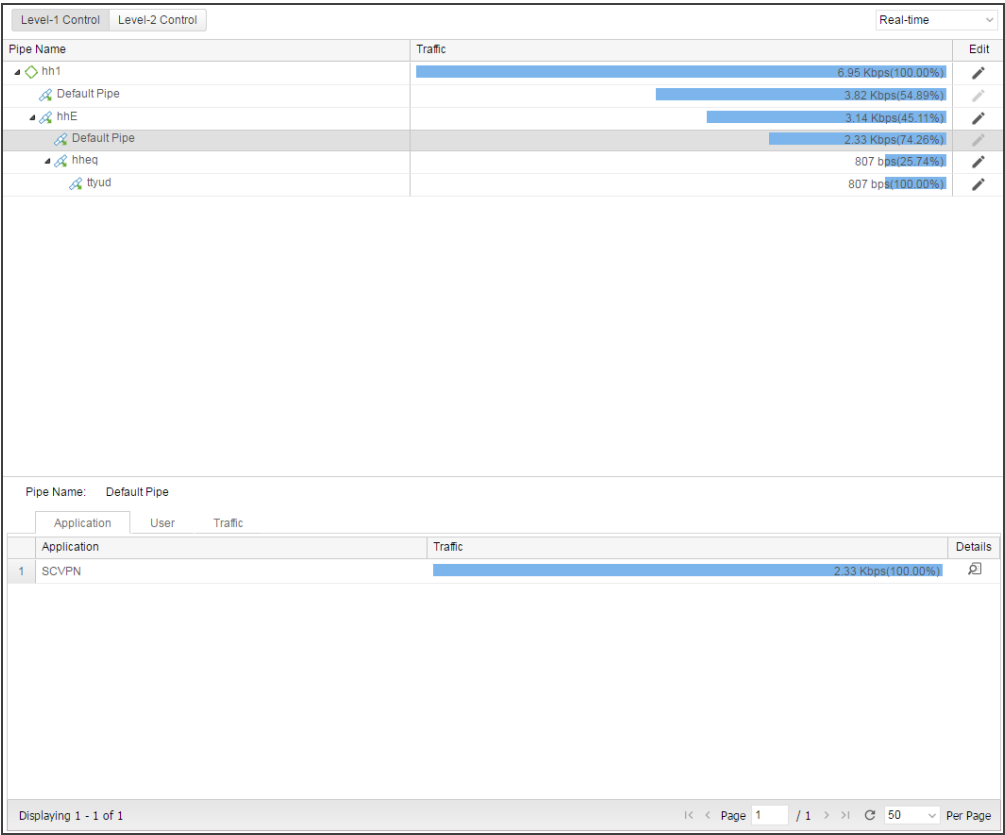
- Click **Level-1 Control** or **Level-2 Control** to display the pipe information of the selected level.
- In the **Total Traff** drop-down menu, select the **Total Traffic**, **Forward** or **Backward** radio button to display the pipe traffic information of the specified direction.
- In the **Realtime** drop-down menu, select Real-time, Last 60 Minutes, Last 24 Hours, Last 7 Days, Last 30 Days, or Customize to display the pipe traffic information in the specified period of time. When

selecting Customize, the Time Customization dialog appears. You can specify the time cycle accordingly. The maximum time cycle is 30 days.

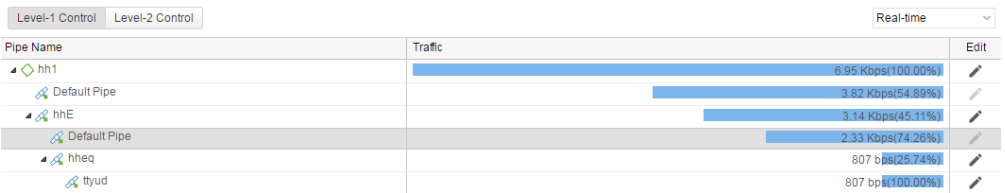
- Hover your mouse over the colored edge at the end of the pipe, showing the name of the pipe and the flow information.
- Click on the pipe name and the page will jump to the pipe details page.


IQoS Details

Click **Monitor > IQoS > IQoS Details** or the pipe name on IQoS Summary page:



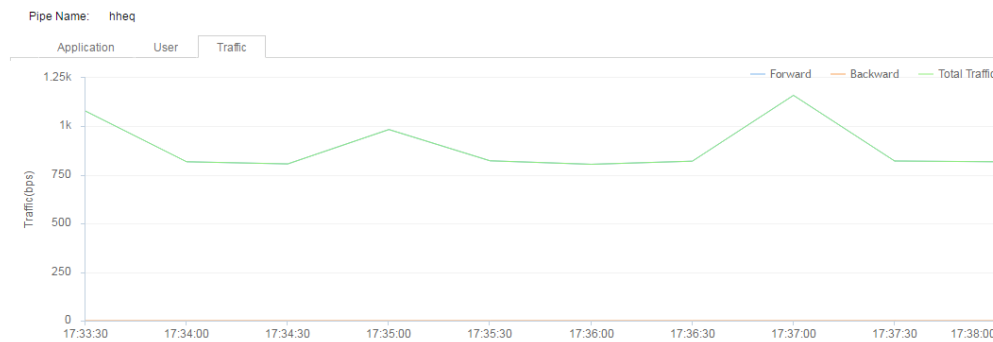
Above the page list the name of the pipe, traffic (forward, backward).







- Click **Level-1 Control** or **Level-2 Control** to display the pipe information of the selected level.
- In the **Realtime** drop-down menu, select Real-time, Last 60 Minutes, Last 24 Hours, Last 7 Days, Last 30 Days, or Customize to display the pipe traffic information in the specified period of time. When selecting Customize, the Time Customization dialog appears. You can specify the time cycle accordingly. The maximum time cycle is 30 days.
- Click the  icon to expand the root pipe and display its sub pipes.

- Click the "Edit" button to edit the selected pipe.
- Mouse over the bar of the Traffic columns to see the forward and backward traffic of the pipe.

Below the page, the traffic details of the selected pipe are displayed, and the details of the traffic are displayed in three ways: application, user and traffic.

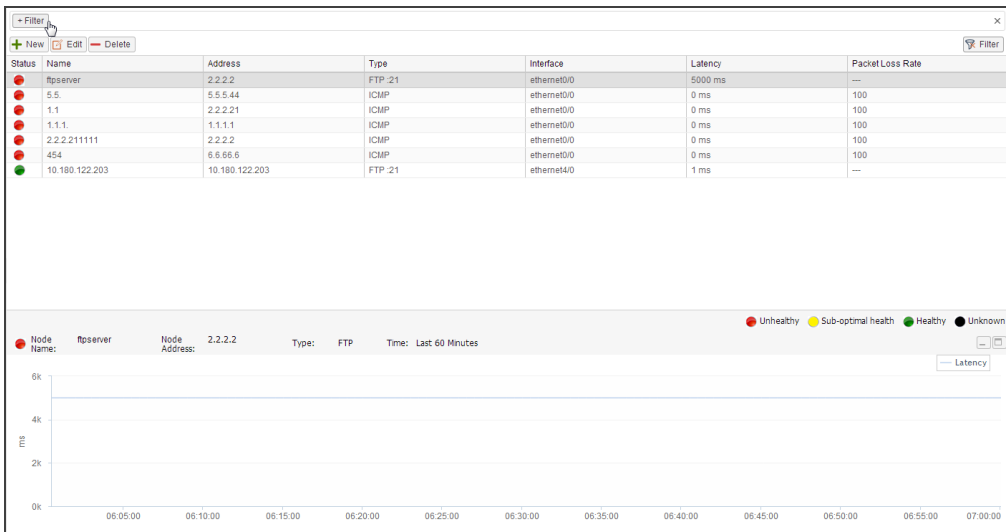


- **Application:** The system displays the traffic for each application as a list. Click the details button , Pops up the application's details window, the trend graph that contains the traffic, and the corresponding traffic for each user-. Click the details button  for a user, View historical trend graphs.
- **User:** The system displays the traffic for each user as a list. Click the details button , Pops up the user's details window, the trend graph that contains the traffic and, and the corresponding traffic for each application, Click the details button  for a app, view historical trend graphs.
- **Traffic:** This page shows the historical trend of the pipe's forward, backward, and total traffic. Hover your mouse over the line chart to view the information of total/forward/backward traffic at a specific moment; Click on the top right corner of the "Forward ", "Backward", "Total Traffic" text, the text will be gray at the same time trend will hide the corresponding traffic polyline, click again to re-display.

Service/Network Node Monitor

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The Service/Network Node page displays the latency of the service node that connects to the current Hillstone device and the latency and packet loss rate of the network node. Click **Monitor > Service/Network Node**.



- Use the table to view the name, detection type, interface, latency, packet loss rate (of network nodes), and health status of the nodes. Click **New**.

Node Configuration

Name:

(1 - 31) chars

Address:

(IP/Domain)

Interface:

ethernet0/0

Interval:

30

s (15 - 120)

Type:

ICMP



Test

OKCancel

In Node Configuration dialog box, enter the service/network node configurations.

Option	Description
Name	Specify the name of the service/network node to be created.
Address	Specify the address of the service/network node.
Interface	Specify the interface that connects to the new node.
Interval	Specify the detection frequency. The range is from 15s to 120s. The default value is 30s.
Type	<div>Specify the detection type. You can choose one type from the following options:</div> <div><div><div>• Customize. When selecting Customize, proceed to select TCP or UDP and then specify the corresponding port.</div><div>• ICMP.</div></div></div>

Option	Description
	<ul style="list-style-type: none"> • DNS. When selecting DNS, proceed to enter the port and the domain name. • FTP. When selecting FTP, proceed to enter the port. To configure the advanced settings, select the Advanced checkbox to provide the username and password for logging into the FTP server and enter the path or file name in the FTP server. • IMAP4. When selecting IMAP4, proceed to enter the port. • POP3. When selecting POP3, proceed to enter the port. • SMTP. When selecting SMTP, proceed to enter the port. • LDAP. When selecting LDAP, proceed to enter the port. To configure the advanced settings, select the Advanced checkbox to provide the username and password for logging into the LDAP server. • HTTP. When selecting HTTP, proceed to enter the port and the URL.
Test	Click Test to test whether the node is reachable or the service is available.

- Click , and click  to select the condition in the drop-down list. The nodes that meet the searching conditions will be displayed in the table or the topology diagram.
- [Viewing_Service/Network_Node_Monitor_information](#) below the list.

- **Health status of the network nodes descriptions.**

Health status color	Description
Red	Unhealthy. The network is unavailable. Latency>600ms or packet loss rate>20%.
Yellow	Subhealthy. 150ms<=Latency<=600ms or 5%<=packet loss rate<=20%.
Green	Healthy. Latency<150ms and packet loss rate<5%.
Black	Unknown. e.g, When the nodes' configuring is finished and no probe data is returned, that is black.

- **Health status of the service nodes descriptions.**


Health status color	Description
Red	Unhealthy. Latency>4000ms.
Yellow	Subhealthy. 2000ms<=Latency<=4000ms.
Green	Healthy. Latency<2000ms.
Black	Unknown. e.g, When the nodes' configuring is finished and no probe data is returned , that is black.



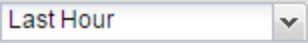
Note: System supports up to 100 nodes.

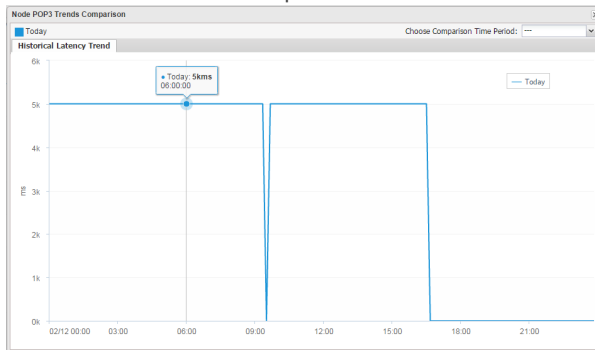
Viewing Service/Network Node Monitor Information

In the Service/Network Node page, you can view the monitoring results using following methods:

- Select a node to view the latency/packet loss rate history trend during the latest 1 hour at the bottom of the page.
- Select a node and click  at the top-right corner of the history trend chart to expand this chart.

After expanding the chart, you can perform the following actions in the expanded chart:

- In the  drop-down menu, select **Last Hour**, **Last Day**, **Last Week**, **Last Month**, and **Customize** to display the statistics during the selected period of time. When selecting Customize, you can specify the time cycle accordingly in the newly appeared window. The maximum time cycle is 30 days.
- Click **Trend Comparison**. The Trend Comparison window appears. Choose comparison items from the Choose Comparison Items drop-down menu. System will display today's history trend and the history trend of the selected items in the trend comparison chart.



Device Monitor

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

The Device page displays the device statistics within the specified period, including the total traffic, sessions, CPU/memory status and hardware status.

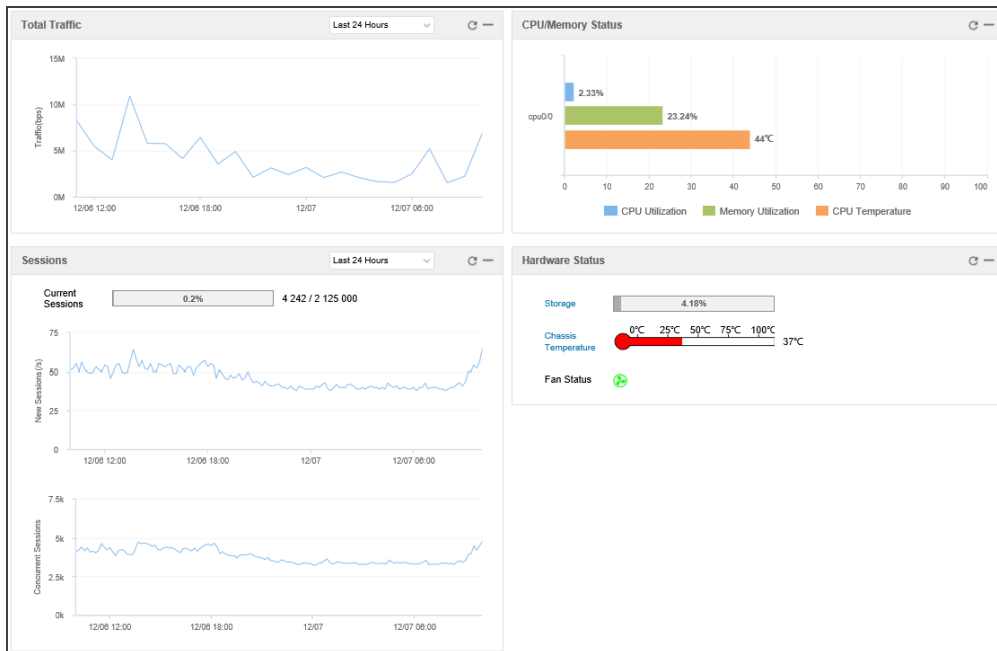
If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.



Note: The non-root VSYS does not have hardware status.

Summary

The summary displays the device statistics within last 24 hours. Click **Monitor>Device>Summary**.




- Total traffic: Displays the total traffic within the specified statistical period.
 - Hover your mouse over the chart to view the total traffic statistics at a specific point in time.
 - Select a different [Statistical Period](#) to view the statistical information in that period of time.
- Hardware status: Displays the real-time hardware status, including storage, chassis temperature and fan status.
 - Storage: Displays the percentage of disk space utilization.
 - Click **Storage** for system to display the disk space utilization trend.
 - Hover your mouse over the chart to view the disk space utilization statistics at a specific point in time.
 - Select a different [Statistical Period](#) to view the statistical information in that period of time.

- Chassis temperature: Displays the current CPU/chassis temperature.
 - Click **Chassis Temperature** for system to display the CPU/chassis temperature trend.
 - Hover your mouse over the chart to view the CPU/chassis temperature statistics at a specific point in time.
 - Select a different [Statistical Period](#) to view the statistical information in that period of time.
- Fan status: Displays the operation status of the fan. Green indicates normal, and red indicates error or a power supply module is not used.
- Sessions: Displays the current sessions utilization, new sessions trend and concurrent sessions trend.
 - Hover your mouse over the chart to view the new sessions and concurrent sessions statistics at a specific point in time.
 - Select different [Statistical Period](#) to view the statistical information in different period of time.
- CPU/memory status: Displays current CPU utilization, memory utilization and CPU temperature statistics.
 - Click legends of **CPU Utilization**, **Memory Utilization** or **CPU Temperature** to specify the histogram statistical objects. By default, it displays statistics of all objects.
 - Hover your mouse over the histogram to view the detailed information, and the link **Details** is displayed.
 - Click **Details** to view the trend of specified histogram.
 - Hover your mouse over the chart to view CPU utilization, memory utilization or CPU temperature statistics at a specific point in time.
 - Select different [Statistical Period](#) to view the statistical information in different period of time.

Statistical Period

System supports the predefined time cycle. The statistical period may vary slightly on different monitored objects. If there is conflict between this guide and the actual page, the latter shall prevail. Select statistical period from the drop-

down menu  at the top right corner of some statistics page to set the time cycle.

- Last 5 Minutes: Displays the statistical information within the latest 5 Minutes.
- Last 15 Minutes: Displays the statistical information within the latest 15 Minutes.
- Custom: Displays the statistical information within the custom period. Click **Custom** to configure the start time and end time.
- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

URL Hit

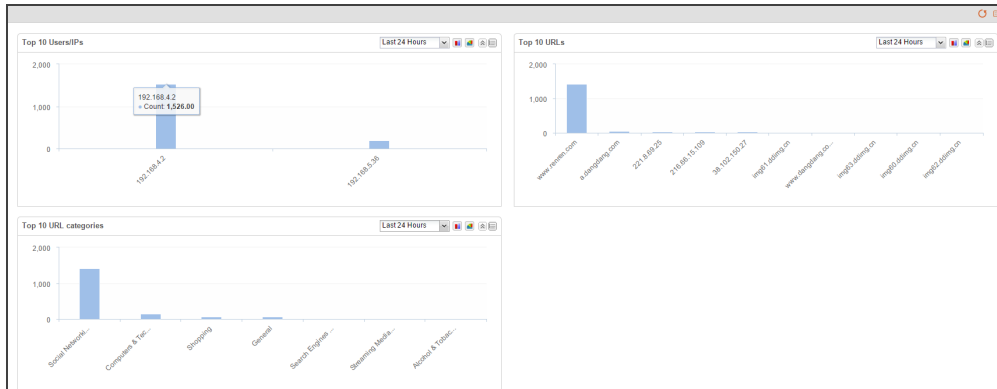
This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.



If the "URL Filter" on Page 270 function is enabled in the security policy rule, the predefined stat-set of URL filter can gather statistics on user/IPs, URLs and URL categories.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

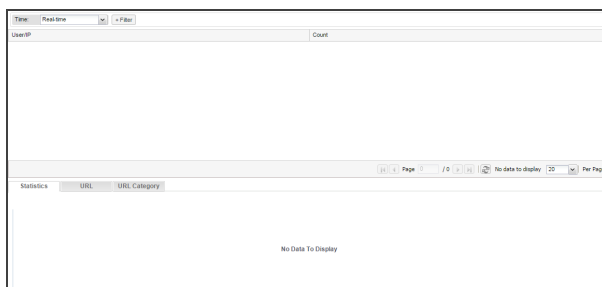
Click **Monitor> URL Hit>Summary**.



- Select a different [Statistical_Period](#) to view the statistical information in that period of time.
- Hover your mouse over a bar, to view the hit count of user/IP, URL or URL Category .
- Click  at top-right corner of every table and enter the corresponding details.
- Click  to switch between the bar chart and the pie chart.

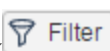
User/IP

Click **Monitor> URL Hit>User/IP**.



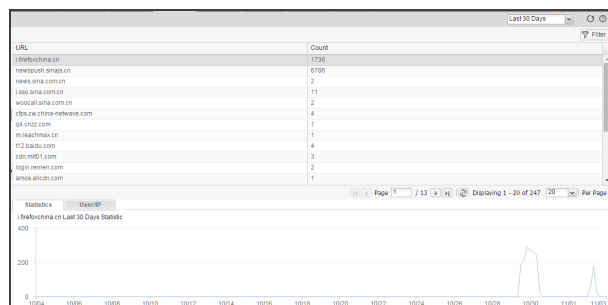
- The user/IPs and detailed hit count are displayed in the list below.
- Click a user/IP in the list to display the corresponding URL hit statistics in the curve chart below.
 - **Statistics:** Displays the hit statistics of the selected User/IP, including the real-time statistics and statistics for the latest 1 hour, 24 hours, 1 week, 30 days and custom period.
 - **URL:** Displays the URLs' real-time hit count of selected User/IP. Click URL link, you can view the corresponding URLs detailed statistics page. Click **Detail** link, you can view the URL hit trend of the selected User-/IP in the **URL Filter Details** dialog .

- URL category: Displays the URL categories' read-time hit count of selected user/IP. Click URL category link , you can view the corresponding URL categories' detailed statistics page. Click **Detail** link, you can view the URL category hit trend of the selected user/IP in the pop-up dialog .

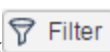
- Click  at top-right corner and then click the **Filter** button at top-left corner. Select **User/IP** and you can search the user/IP hit count information by entering the keyword of the username or IP.


URL

Click **Monitor > URL Hit > URL**.



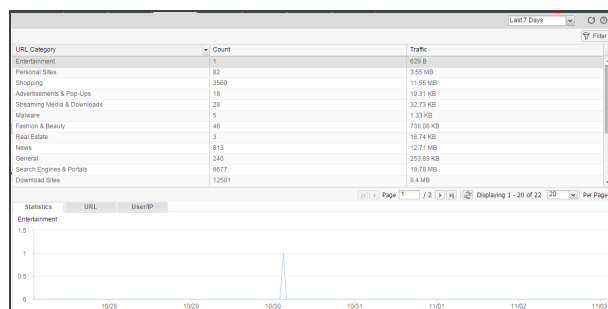
- The URL, URL category and detailed hit count are displayed in the list below.
- Click a URL in the list to view its detailed statistics.
 - Statistics: Displays the hit statistics of the selected URL, including the real-time statistics and statistics for the latest 1 hour, 24 hours , 1 week , 30 days and custom period.
 - User/IP: Displays the User/IP's real-time hit count of selected URL. Click the User/IP link and you can view the corresponding user/IPs detailed statistics page. Click the **Detail** link and you can view the URL hit trend of the selected user/IP in the **URL Filter Details** dialog box.

- Click  at the top-right corner and then click the **Filter** button at the top-left corner. Select **URL** and you can search the URL hit count information by entering the keyword of the URL.

- Click  to refresh the real-time data in the list.

URL Category

Click **Monitor> URL Hit > URL Category**.



- The URL category, count, traffic are displayed in the list.
- Click a URL category in the list to view its detailed statistics displayed in the Statistics, URL(real-time), User/IP (real-time) tabs.

- **Statistics:** Displays the trend of the URL category visits, including the real-time trend and the trend in the last 60 minutes, 24 hours , 1 week, 30 days and custom period.
- **URL:** Displays the visit information of the URLs, contained in the URL category, that are being visited.
- **User/IP:** Displays the visit information of the users or IPs that are visiting the URL category.



- Click  to refresh the real-time data in the list.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click the time button on the top right corner of each tab to set the time cycle.

- **Real-time:** Displays the current statistical information.
- **Last 60 Minutes:** Displays the statistical information within the latest 1 hour.
- **Last 24 Hours:** Displays the statistical information within the latest 1 day.
- **Last 7 Days:** Displays the statistical information within the latest 1 week.
- **Last 30 Days:** Displays the statistical information within the latest 1 month.
- **Custom:** Customize the time cycle. Select **Custom**. The **Custom Date and Time** dialog box appears. Select the start time and the end time according to your requirements.

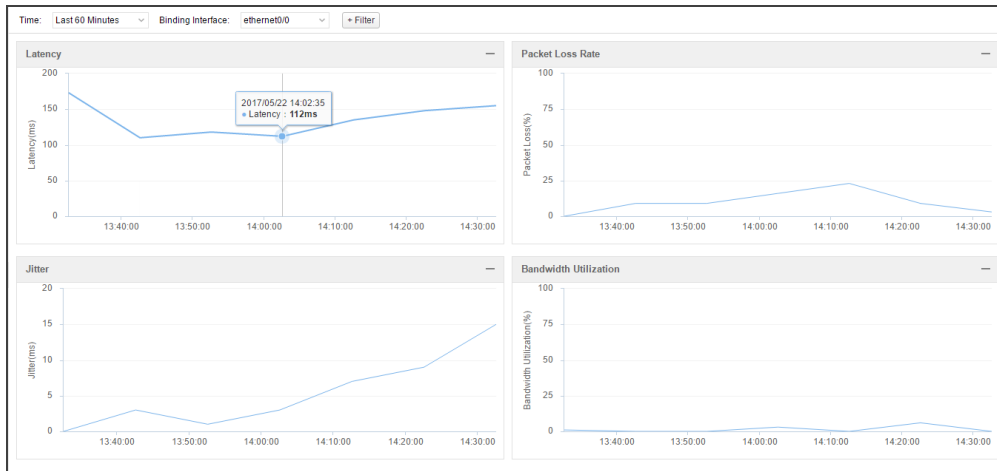
Link State Monitor

Link state monitoring can calculate the sampling traffic information of the specific interface in the link, including latency, packet loss rate, jitter, and bandwidth utilization, to monitor and display the overall status of the link.

Link state monitor page displays the traffic statistics of the interfaces that have been bound within a specified period (Realtime, latest 1 hour, latest 1 day, latest 1 week, latest 1 month , customized period) .

Link State

The link state page displays traffic statistics for all binding interfaces. Click **Monitor > Link State Monitor**. For more information about configuration of binding interfaces, refer to [Link Configuration](#).



- Select a different [Statistical_Period](#) to view the statistical information in that periods of time.
- Select the binding interface **Binding Interface** drop-down list, Click the **Binding Interface** drop-down menu and select the interface name to view the link status monitoring statistics for this interface.
- Click **+ Filter** button and select **Nat-Pool** in the drop-down menu. You can select the NAT address pool name to view the link status monitoring statistics according to the specified NAT address pool.
- Click **+ Filter** button and select **Application** in the drop-down menu. You can select the TOP 10 or Application / Application group name to view the link status monitoring statistics according to the specified application.



Note:

- "Time" and "Binding Interface" are required in the filter condition.
- If the application switch of the specified interface is not enabled in the link configuration, the **Application** filter condition cannot be added.

Link Configuration

In the link configuration page, you can configure the binding interface to monitor the link state and can enable the application switch to specify the NAT address pool as needed.

To configure the link, take the following steps:

1. Click **Monitor > Link State Monitor > Link Configuration**.
2. Click **New**.

In the Link Configuration dialog box, configure these values

Option	Description
Binding Interface	Select the interface in the drop down menu.
Application Switch	Select Enable check box. After enabling, you can see details of the specific application in this interface.
Nat-Pool	<p>After adding the NAT pool, system will classify statistics according to the NAT pool IP address for link interface traffic.</p> <ul style="list-style-type: none"> • Click + button to add a NAT pool. • Type in the NAT pool name in the text box under the Name. • In the Address drop down menu, select the address book to add to the NAT address pool. By default, system uses the address entry of any, which means the NAT pool will be executed on all traffic. <p>Select the NAT pool item, click -button to delete the NAT pool.</p>

3. Click **OK**.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click **Real-time** on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 7 Days: Displays the statistical information within the latest 1 week.
- Last 30 Days: Displays the statistical information within the latest 1 month.

- Custom: Customize the time cycle. Select **Custom**. The **Custom Date and Time** dialog box appears. Select the start time and the end time according to your requirements. You can specify the time period of 30 days before the current time at most.

Authentication User

If system is configured with "Web Authentication" on Page 124, "Single Sign-On" on Page 131, "SSL VPN" on Page 172, "L2TP VPN" on Page 228 the authentication user can gather statistics on the authenticated users.

Click **Monitor>Authentication User**.

Authentication User

+ Filter

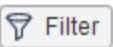


Filter

	Username	AAA Server	User Group	Role	IP/MAC	Interface/Virtual Router	Online Time	Authentication Type	Operation
	eeeeeeee	local			3.2.2.2	trust-vr	0 day 5 hour 25 minute ...	Static Binding	
	qqqqqw	local			0012.0123.1230	trust-vr	0 day 5 hour 26 minute ...	Static Binding	
	qqqqqw	local			1.1.1.1	trust-vr	0 day 5 hour 26 minute ...	Static Binding	

Page 1 / 1

Displaying 1 - 3 of 3

20 Per Page

- Click , and click  to select the condition in the drop-down list to filter the users.
- Click **Kick Out** under the Operation column to kick the user out.
- Click  to refresh the real-time data in the list.

Alarm

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

The alarm feature can actively detect protected networks to locate suspicious issues and send out alarming messages. The rule that defines what behavior should be alerted is called the alarm rule.

System can analyze alarm messages and display the analysis results in the form of a chart and time line. In addition, alarm messages can also be sent to system administrators by sending emails or sms text. In this way, the administrator can receive alerts in the first place and respond to the alarms.

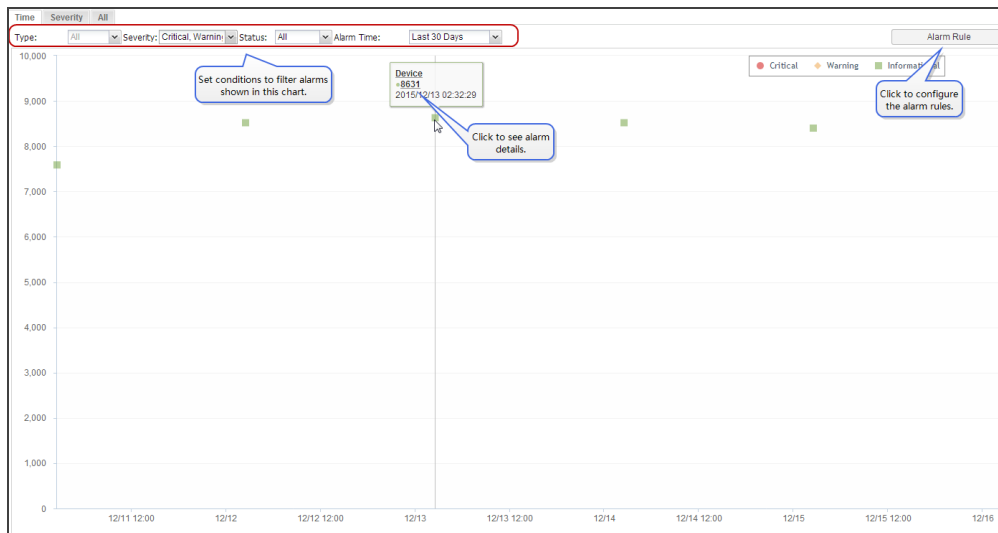
Alarm as a Monitor

The alarms are show under the monitor module. When an occurrence defined in the alarm rule happens, the alarm message is generated and shown in the alarm page. For more information on alarm rules, refer to ["Alarm Rule" on Page 429](#).

In the alarm page, alarms are shown by three categories: alarms arranged by time, alarms arranged by severity levels and alarms details .

Alarms by Time

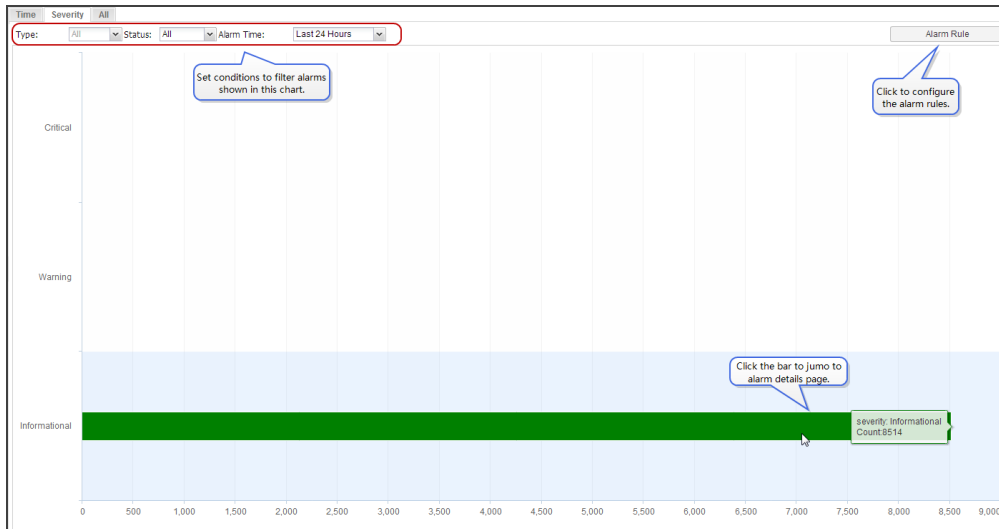
In the Time tab, alarm messages are on a two-dimensional coordinate axis. To see the alarm by time page, select **Monitor > Alarm**, and select the Time tab.



- Configuring filters: The left vertical axis shows the number of alarms. You may define the conditions to filter alarms.
 - **Type:** Select one or more types from the drop-down menu and click **Add** to add them to the right.
 - **Severity:** Select one or more severity levels. There are three severity hierarchy: critical, warning, and informational.
 - **Status:** Select a message status from the drop-down menu: all, unread and read.
 - **Time:** Select the time range when alarms are generated. You may select to view the last one hour, one day, one week, one month or other user-defined time.
- Hover over a dot (red, yellow or green) and click the link, and then you will be redirected to the detail page of that alarm.
- Click [Alarm Rule](#) to jump to the alarm rules configure page.

Alarm by Severity

Alarms in the Severity tab shows the number bar of alarm messages of different severity levels. Select **Monitor > Alarm**, and select the Severity tab.



- Configuring filters:
 - Type:** Select one or more types from the drop-down menu and click **Add** to add them to the right.
 - Status:** Select a message status from the drop-down menu: all, unread and read.
 - Time:** Select the time range when alarms are generated. You may select to view the last one hour, one day, one week, one month or other user-defined time.
- Click a bar, you will be redirected to the alarm details page.
- Click **Alarm Rule** to jump to the alarm rules configure page.


Alarm Details

Select **Monitor > Alarm**, and click the All tab. You will be able to see all alarm messages and their detailed information.

The table displays a list of alarm messages. The first two rows show 'cpu utilization lower ...' messages with counts of 210 and 32. The table includes various interactive elements like checkboxes, filters, and buttons for adding comments or configuring rules.

Last Alarm	Time	Severity	Type	Rule Name	Count	Message	Status	Read by	Read at	Comment
2015/12/11 11:21		Informational	Device : CPU Utilizat...	fd0d	210	cpu utilization lower ...	Unread			
2015/12/11 11:21		Informational	Device : CPU Utilizat...	fd0d(invalid)	32	cpu utilization lower ...	Unread			

- Configuring filters.
 - **Last Alarm Time:** Select the time range when alarms are generated. You may select to view the last one hour, one day, one week, one month or other user-defined time.
 - **Type:** Select one or more types from the drop-down menu and click **Add** to add them to the right.
 - **Severity:** Select one or more severity levels. There are three severity hierarchy: critical, warning, and informational.
 - **Status:** Select a message status from drop-down menu: all status, unread messages or/and read messages.
 - **Read at:** Select what time the message is being read.
 - **Read by:** Select which person has read the message.
 - **Comment:** Select if you want to see messages with or without a comment.
 - **Reason:** Type keywords you want to search in the reasons that trigger an alarm.
- To read and comment alarms, take the following steps:
 - **Batch reading:** Select all the check boxes of alarm messages you want to read, and click **Read Alarm**. In the prompt, enter your comment, and click **OK**.
 - **Single reading:** Hover your cursor over the Status column and click **Read**. In the prompt, enter your comment, and click **OK**.
- To add or modify a comment, take the following steps:
 - **Batch adding/modifying:** Select all the check boxes of alarm messages you want to comment, and click **Add/Modify Comment**. In the prompt, enter your comment, and click **OK**.
 - **Single adding/modifying:** Select the check boxes of alarm message you want to comment, and click **Add/Modify Comment**. In the prompt, enter your comment, and click **OK**.
- To view every messages in an alarm, take the following steps:

Click the number in the Count column, and you will see every occurrence time of this alarm incident.
- Click  to jump to the alarm rules configure page.

Alarm Rule

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

An alarm rule defines the condition which triggers an alarm. When an incident that complies with the alarm rule happens, system will detect that incident and generate an alarm message.

There are three alarm categories: device alarms, application alarms and network service alarms.

Configuring Interface Bandwidth

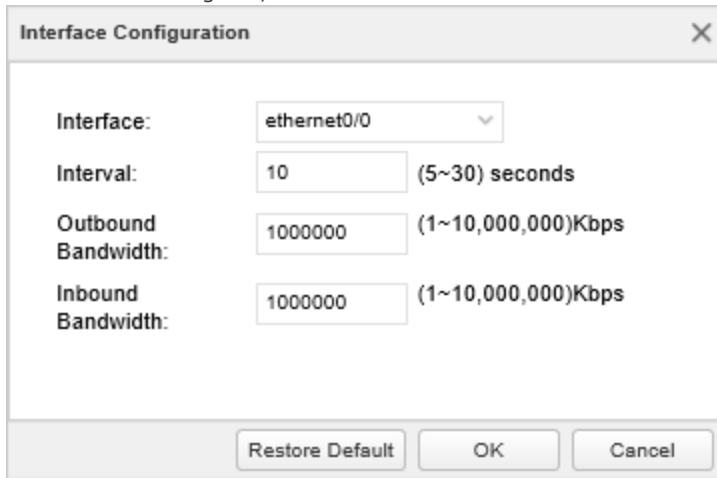
If you intend to use the interrace alarm rule, make sure that you have configured the interface bandwidth. Both are indispensable, otherwise you will not receive the alarms.

To configure the detection rule, take the following steps:

1. Click **Monitor> Device**.
2. Click **Interface Bandwidth Configuration** at the top-right corner.

Interface				
<div>+ Add ✎ Edit ✓ Enable ✗ Disable - Delete</div>				
<input type="checkbox"/>	Interface Name	Outbound Bandwi...	Inbound Bandwidt...	Detection Status
Interval (seconds)				
No data to display				
◀ < Page 0 / 0 > ▶ ↺ 50 ▼ Per Page				
Close				

3. In **Interface** dialog box, click **Add**.



The **Interface Configuration** dialog box contains the following fields and controls:

- Interface:** A dropdown menu showing **ethernet0/0**.
- Interval:** A text box with **10** and a label **(5~30) seconds**.
- Outbound Bandwidth:** A text box with **1000000** and a label **(1~10,000,000)Kbps**.
- Inbound Bandwidth:** A text box with **1000000** and a label **(1~10,000,000)Kbps**.
- Buttons at the bottom: **Restore Default**, **OK**, and **Cancel**.

In the **Interface Configuration** dialog box, configure the corresponding options.

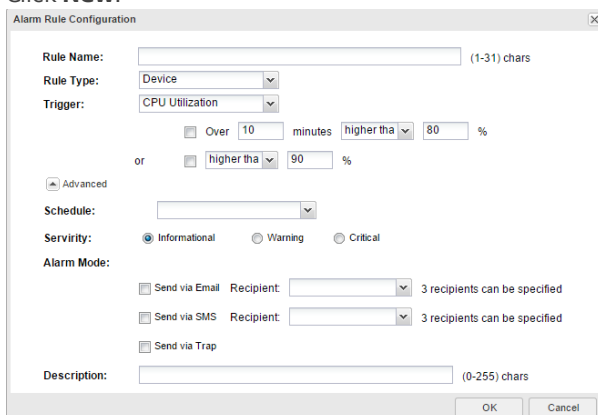
Option	Description
Interface	From the Interface drop-down list, select the interface that you want to enable the monitor function.
Interval	In the Detect Interval text box, specify the detect interval. The range is from 5s to 30s. The default value is 10s.
Outbound Band-width	Specify the maximum outbound bandwidth. The range is from 1Kbps to 10,000,000Kbps. The default value is 1,000,000Kbps.
Inbound Band-width	Specify the maximum inbound bandwidth. The range is from 1Kbps to 10,000,000Kbps. The default value is 1,000,000Kbps.
Restore Default	Click Restore Default to restore the value to the default one.

4. Click **OK**.

Creating an Alarm Rule

To create an alarm rule, take the following steps:

1. Select **System > Alarm Rule**.
2. Click **New**.



The **Alarm Rule Configuration** dialog box contains the following fields and controls:

- Rule Name:** A text box with a label **(1-31) chars**.
- Rule Type:** A dropdown menu showing **Device**.
- Trigger:** A dropdown menu showing **CPU Utilization**.
- Trigger Conditions:**
 - ☐ **Over** **10** minutes **higher tha** **80** %
 - or** ☐ **higher tha** **90** %
- Advanced:** A button to expand advanced options.
- Schedule:** A dropdown menu.
- Servirity:** Radio buttons for **Informational** (selected), **Warning**, and **Critical**.
- Alarm Mode:**
 - ☐ **Send via Email** **Recipient:** [text box] **3 recipients can be specified**
 - ☐ **Send via SMS** **Recipient:** [text box] **3 recipients can be specified**
 - ☐ **Send via Trap**
- Description:** A text box with a label **(0-255) chars**.
- Buttons at the bottom: **OK** and **Cancel**.

In the **Alarm Rule Configuration** dialog box, configure these values.

Option	Description
Rule Name	Specify the rule name. You can input 31 characters at most.
Rule Type	Specify the description of the warning rule. You can input 255 characters at most.
Trigger	<p>Specify the trigger of the warning, including the monitored object and the threshold.</p> <p>Select the monitored objects from the drop-down menu and then select the threshold. Generally, there are two types of thresholds: the threshold within a period, and the threshold at a specific point of time. Administrators can use both of them or one of them. If administrators use both of them, the logical relation between them is "or", which means system will generate the warning information when one threshold meets the settings.</p> <p>Note: If the monitored object is New Sessions, Concurrent Sessions, or Interface Bandwidth, the threshold is percentage.</p>
Advanced	
Schedule	Specify the schedule of the warning rule from the drop-down list. The warning rule will take effect during the specified period of time, which is decided by the schedule. You can also click New Schedule in the drop-down list to create a new schedule.
Severity	Specify the severity of the incident.
Alarm mode	<p>Specify the alarming method .</p> <ul style="list-style-type: none"> Send via Email: Select the checkbox and then specify a recipient or create a new recipient from the Recipient drop-down menu. System will report the events to the recipient by sending a warning email. To create or edit a recipient, go to Object > Send Object (refer to "Send Object" on Page 269). Send via SMS: Select the checkbox and then specify a recipient or create a new recipient from the Recipient drop-down menu. System will report the events to the recipient by sending a mobile phone text message. To create or edit a recipient, go to Object > Send Object (refer to "Send Object" on Page 269). Send via Trap: Select the checkbox, and system will send messages to the Trap host when an event occurs. To configure a Trap host, go to System > SNMP (refer to "SNMP" on Page 489). <p>Note: If you use "Send via Trap", you must designate a SNMP host and Trap host at the same time.</p>
Description	Specify the description of the rule. You can input 255 characters at most.

3. Click **OK**.

Reporting

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The reporting feature gathers and analyzes data for the following report categories, providing all-around and multi-dimensional statistics to you.

Report Categories	Description
Security Report	Helps users quickly understand the overall risk situation of the servers and users.
Flow Report	Analysis and display of the user, application, interface, zone's traffic and concurrency.
Content Report	Detailed description of the URL hit, including the hit times, trends, categories.
System Report	Lists system resources situation, such as CPU, memory, disk.

You can configure report task in ["User-defined Task" on Page 434](#) and ["Predefined Task" on Page 437](#), and view generated report files in ["Report File" on Page 433](#).

Report File

Go to **Monitor > Reports > Report File** and the report file page shows all of the generated report files.

group by Time

Last 24 Hours

Last 7 Days

Last 30 Days

Last 3 Months

Last 6 Months

Last 12 Months

More than a year ...

Delete

Export

Mark as Read

<input type="checkbox"/>	Created at	Name	File Type
<input type="checkbox"/>	2016/06/06 18:19:02	hh	
<input type="checkbox"/>	2016/05/27 17:05:51	System Report_2016.05.27_17:00:40	

- Sort report files by different conditions: Select **Group by Time**, **Group by Task** or **Group by Status** from the drop-down list, and then select a time, task or status from the selective table, and the related report files will be shown in the report file table.
- Click **Delete** to delete the selected report files.
- Click **Export** to download the selected report files.
- Click **Mark as Read** to modify the status of the selected report files.
- Click **Filter** , and click **+ Filter** to select the condition in the drop-down list. In the text box, enter the keyword to search for the report files.
- In the File Type column, click the icon of the report file to preview the report file. Not all platforms support this function.



Note: If your browser has enabled "Blocking pop-up windows", you will not see the generated file. Make sure to set your browser "Always allow pop-up windows", or you can go to your blocked window history to find the report file.

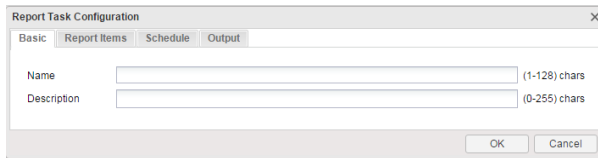
User-defined Task

A user-defined task is a customized report task which can be tailored to meet your requirements.

Creating a User-defined Task


To create a user-defined task, take the following steps:

1. Select **Monitor > Reports > User-defined**.
2. Click **New**.



The image shows a 'Report Task Configuration' dialog box with a close button (X) in the top right corner. It has four tabs: 'Basic', 'Report Items', 'Schedule', and 'Output'. The 'Basic' tab is selected. Inside the 'Basic' tab, there are two text input fields. The first is labeled 'Name' and has a character limit of '(1-128) chars'. The second is labeled 'Description' and has a character limit of '(0-255) chars'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

In the Report Task Configuration dialog box, configure these values.

Option	Description
Basic	
Name	Specifies the name of the report task.
Description	Specifies the description of the report task.
Report Items	
Report Items	<p>Specifies the content for the report file.</p> <p>To add report items to the report task, take the following steps:</p> <ol style="list-style-type: none"> 1. Expand the categories from the left list. 2. Select the category item you want, and click Add to add it to the right column. <p>On the right side of the selected report items, you can click  to set filter conditions so that only specific statistical data can be showed in the report file. The filter conditions are different for different report items. By default, all statistical data of selected report items will be showed in the report file. Filter conditions are described as follows:</p> <ul style="list-style-type: none"> • Critical Assets: Add statistics of critical assets in the report file. By default, there is the top 10 traffic statistics of critical assets in the report file. If more than one to be selected, please hold down the Ctrl key. • Application: Filter the statistics shown in the report file by applications. Only the statistics of the selected application will be shown in the report file. You can also perform other operations: <ul style="list-style-type: none"> • To add a new application group, click New AppGroup. • To add a new application filter, click New AppFilter. • Pipe: Filter the statistics shown in the report file by pipe. Only the statistics of the selected pipes will be shown in the report file. • Zone: Filter the statistics shown in the report file by zones. Only the statistics of the selected zones will be shown in the report file. If more than one to be selected, please hold down the Ctrl key. • Interface: Filter the statistics shown in the report file by interfaces. Only the statistics of the selected interfaces will be shown in the report file. If more than one to be selected, please hold down the Ctrl key.
Schedule	
<p>The schedule specifies the running time of the report task. The report task can be run periodically or run immediately.</p> <p>Periodic: Generates report files as planned.</p> <ul style="list-style-type: none"> • Schedule: Specifies the statistical period. • At: Specifies the running time. <p>Generate Now: Generates report files immediately.</p> <ul style="list-style-type: none"> • Specifies the start time and end time of absolute statistical period in the time text box. 	

Option	Description
Output	
File Format	The output format of the report file is a PDF.
Recipient	Sends report file via email. To add recipients, enter the email addresses in to the recipient text box (use ";" to separate multiple email addresses).
Send via FTP	<p>Check the Send via FTP check box to send the report file to a specified FTP server.</p> <ul style="list-style-type: none"> • Server Name/IP: Specifies the FTP server name or the IP address. • Virtual Router: Specifies the virtual router of the FTP server. • Username: Specifies the username used to log on to the FTP server. • Password: Enter the password of the FTP username. • Anonymous: Check the check box to log on to the FTP server anonymously. • Path: Specifies the location where the report file will be saved.

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

Enabling/Disabling the User-defined Task

To enable or disable the user-defined task, take the following steps:

1. Select **Monitor > Reports > User-defined**.
2. Select the task you want, and click the **Enable** or **Disable** button on the top.
By default, the user-defined task is enabled.

Viewing Report Files

To view the generated report files, select **Monitor > Reports > Report File**.





Predefined Task


The predefined tasks are the system report task template. Each report task is named according to the name of the report item, the configured date and time.

The predefined tasks include the following types:

- Security Report
- Flow Report
- Content Report
- System Report

Generating Report Tasks

Name	Description	Action
Security Report	Help users quickly understand the overall risk situation of the servers, users.	
Flow Report	Analysis and display of the user, application, interface, zone's traffic and concurrency.	
Content Report	Detailed description of the device URL access, including the number of times, trends, categories, etc.	
System Report	List system resources situation, such as cpu, memory, disk etc.	

1. Select **Monitor > Reports > Predefined**.
2. In the **Action** column, click the  icon.

In the Report Task Configuration dialog box, configure these values.

Option	Description
Basic	
Name	Specifies the name of the report task.
Description	Specifies the description of the report task. You can modify according to your requirements.
Schedule	
The schedule specifies the running time of report task. The report task can be run periodically or run immediately.	
Periodic: Generates report files as planned.	
<ul style="list-style-type: none"> • Schedule: Specifies the statistical period. • At: Specifies the running time. 	
Generate Now: Generates report file immediately.	
<ul style="list-style-type: none"> • Specifies the start time and end time of an absolute statistical period in the time text box. 	
Output	
File Format	The report file is outputted in PDF format.
Recipient	Sends report file via email. To add recipients, enter the email addresses in to the recipient text box (use ";" to separate multiple email addresses).
Send via FTP	<p>Check the Send via FTP check box to send the report file to a specified FTP server.</p> <ul style="list-style-type: none"> • Server Name/IP: Specifies the FTP server name or the IP address. • Virtual Router: Specifies the virtual router of the FTP server. • Username: Specifies the username used to log on to the FTP server. • Password: Enter the password of the FTP username. • Anonymous: Check the check box to log on to the FTP server anonymously. • Path: Specifies the location where the report file will be saved.

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

Viewing Report Files

To view the generated report files, select **Monitor > Reports > Report File**.

Logging

Logging is a feature that records various kinds of system logs, including device log, threat log, session log, NAT log, File filter log, Network Behavior Record log and URL logs.

- Device log
 - Event - includes 8 severity levels: debugging, information, notification, warning, error, critical, alert, emergency.
 - Network - logs about network services, like PPPoE and DDNS.
 - Configuration - logs about configuration on command line interface, e.g. interface IP address setting.
- Threat - logs related to behaviors threatening the protected system, e.g. attack defense and application security.
- Session - Session logs, e.g. session protocols, source and destination IP addresses and ports.
- NAT - NAT logs, including NAT type, source and destination IP addresses and ports.
- File Filter - logs related with file filter function.
- Network behavior record logs – Logs related with network behavior record function, e.g. IM behavior ,etc.
- URL - logs about network surfing, e.g. Internet visiting time, web pages visiting history, an URL filtering logs.
- PBR - logs about policy-based route.
- CloudSandBox - logs about sandbox.

The system logs the running status of the device, thus providing information for analysis and evidence.

Log Severity

Event logs are categorized into eight severity levels.

Severity	Level	Description	Log Definition
Emergencies	0	Identifies illegitimate system events.	LOG_EMERG
Alerts	1	Identifies problems which need immediate attention such as device is being attacked.	LOG_ALERT
Critical	2	Identifies urgent problems, such as hardware failure.	LOG_CRIT
Errors	3	Generates messages for system errors.	LOG_ERR
Warnings	4	Generates messages for warning.	LOG_WARNING
Notifications	5	Generates messages for notice and special attention.	LOG_NOTICE
Informational	6	Generates informational messages.	LOG_INFO
Debugging	7	Generates all debugging messages, including daily operation messages.	LOG_DEBUG

Destination of Exported Logs

Log messages can be sent to the following destinations:

- Console - The default output destination. You can close this destination via CLI.
- Remote - Includes Telnet and SSH.
- Buffer - Memory buffer.

- File - By default, the logs are sent to the specified USB destination in form of a file.
- Syslog Server - Sends logs to UNIX or Windows Syslog Server.
- Email - Sends logs to a specified email account.
- Local database - Sends logs to the local database of the device.

Log Format

To facilitate the access and analysis of the system logs, StoneOS logs follow a fixed pattern of information layout, i.e.

date/time, severity level@module: descriptions. See the example below:

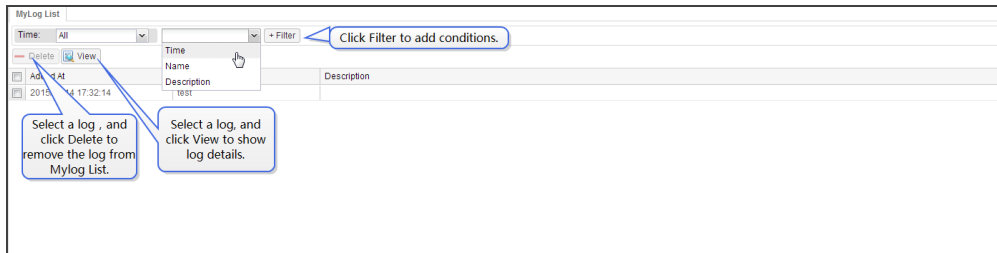
`2000-02-05 01:51:21, WARNING@LOGIN: Admin user "admin" logged in through console from localhost.`

My Logs

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

You can save your favorite filtered log messages to your MyLog List.

To view your saved MyLog list, select **Monitor > Logs > MyLog**.



Event Logs

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view event logs, select **Monitor > Log > Event**.

In this page, you can perform the following actions:



- Configuration: Click to jump to the configuration page.
- Add to My Log: Click to add the current filtered results to MyLog list.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click Filter to add conditions to show logs that march your filter.

Network Logs

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view network logs, select **Monitor > Log > Network**.

In this page, you can perform the following actions:



- Configuration: Click to jump to the configuration page.
- Add to My Log: Click to add the current filtered results to MyLog list.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click  **Filter**, and then click  to add conditions to show logs that march your filter.

Configuration Logs

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view configuration logs, select **Monitor > Log > Configuration**.

In this page, you can perform the following actions:

- Configuration: Click to jump to the configuration page.
- Add to My Log: Click to add the current filtered results to MyLog list.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click  **Filter**, and then click  to add conditions to show logs that march your filter.

Threat Logs



This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

Threat logs can be generated under the conditions that:

- Threat logging in the Logging feature is enabled. Refer to ["Log Configuration" on Page 451](#).
- You have enabled one or more of the following features: ["Anti Virus" on Page 351](#), [" Intrusion Prevention System" on Page 356](#), ["Attack-Defense" on Page 382](#) or ["Perimeter Traffic Filtering" on Page 391](#) .

To view threat logs, select **Monitor > Log > Threat**.

In this page, you can perform the following actions:

- Add to My Log: Click to add the current filtered results to MyLog list.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click  **Filter** , and then click  to add conditions to show logs that march your filter.
- View the details of selected log in the Log Details tab. In the Log Details tab, you can click "View Pcap" "Download" ["Add Whitelist"](#) ["Disable Signatures"](#) to quickly link to the relevant page.

Session Logs

Session logs can be generated under the conditions that:

- Session logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 451.

To view session logs, select **Monitor > Log > Session**.

Click Filter to add conditions to show logs that match your filter.

Click to jump to the configuration page.

Click to delete all the displayed logs.

Click to export the displayed logs as a TXT or CSV file.

Time	Source ID	Source port	Destination IP	Destination port	Protocol	Action	Sent Traffic(bytes)	Received Traffic...	Close Reason
2015-12-15 14:35:06	1	10.0.0.198	110.75.8.9	80	TCP	Session End	752	851	TCP FIN
2015-12-15 14:35:06	1	10.0.0.200	110.75.8.9	80	TCP	Session End	723	776	TCP FIN
2015-12-15 14:35:06	1	10.0.0.200	140.207.54.116	80	TCP	Session End	0	0	Ageout
2015-12-15 14:35:06	1	10.0.0.200	140.207.54.47	80	TCP	Session End	0	0	Ageout
2015-12-15 14:35:06	1	10.0.0.198	43.250.14.49	80	TCP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	10.188.7.10	53	UDP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	42.120.219.31	80	TCP	Session End	936	500	TCP FIN
2015-12-15 14:35:06	1	10.0.0.198	42.120.219.31	80	TCP	Session End	937	500	TCP FIN
2015-12-15 14:35:06	1	10.0.0.198	203.208.49.185	80	TCP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	10.188.7.10	53	UDP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	61.135.185.179	80	TCP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	10.188.7.10	53	UDP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	110.75.8.9	80	TCP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	140.205.174.1	80	TCP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	10.188.7.10	53	UDP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	110.75.8.9	80	TCP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	10.188.7.10	53	UDP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	117.121.28.4	80	TCP	Session Start	0	0	
2015-12-15 14:35:06	1	10.0.0.198	140.206.160.213	80	TCP	Session End	921	1299	TCP RST
2015-12-15 14:35:06	1	10.0.0.198	140.206.160.213	80	TCP	Session End	845	496	TCP RST

Page 1 / 94 Displaying 1 - 20 of 1875 20 Per Page



Note:

- For ICMP session logs, the system will only record the ICMP type value and its code value. As ICMP 3, 4, 5, 11 and 12 are generated by other communications, not a complete ICMP session, system will not record such kind of packets.
- For TCP and UDP session logs, system will check the packet length first. If the packet length is 20 bytes (i.e., with IP header, but no loads), it will be defined as a malformed packet and be dropped; if a packet is over 20 bytes, but it has errors, system will drop it either. So, such abnormal TCP and UDP packets will not be recorded.

PBR Logs

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

PBR logs can be generated under the conditions that:

- PBR logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 451.
- You have enabled logging function in PBR rules. Refer to "Creating a Policy-based Route Rule" on Page 112 .

To view PBR logs, select **Monitor > Log > PBR**.

Time	PBR nam...	Source IP	AAA user ...	Source port	Destinatio...	Destinatio...	Protocol	Application	Next Hop	Egress Int...	Virtual Ro...	Session r...
------	------------	-----------	--------------	-------------	---------------	---------------	----------	-------------	----------	---------------	---------------	--------------

NAT Logs

NAT logs are generated under the conditions that:

- NAT logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 451.
- NAT logging of the NAT rule configuration is enabled. Refer to"Configuring SNAT" on Page 319 and "Configuring SNAT" on Page 319"Configuring DNAT" on Page 324.

To view NAT logs, select **Monitor > Log> NAT**.

NAT type: Both

Filter

Click Filter to add conditions to show logs that march your filter.

Configuration

Clear

Export

Filter

Click to jump to the configuration page.

Click to delete all the displayed logs.

Click to export the displayed logs as a TXT or CSV file.

Time	Type	Source IP	AAA user @ host	Source port	Destination IP	Destination port	Translated IP	Translated port	Protocol
2015-12-15 10:49:38	SNAT	10.0.0.198	UNKNOWN-	50512	110.173.196.36	80	10.160.37.71	50512	TCP
2015-12-15 10:49:37	SNAT	10.0.0.198	UNKNOWN-	59415	10.188.7.10	53	10.160.37.71	59415	UDP
2015-12-15 10:49:33	SNAT	10.0.0.198	UNKNOWN-	50511	124.251.44.12	8099	10.160.37.71	50511	TCP
2015-12-15 10:49:33	SNAT	10.0.0.195	UNKNOWN-	50510	124.251.46.35	80	10.160.37.71	50510	TCP
2015-12-15 10:49:24	SNAT	10.0.0.198	UNKNOWN-	50509	124.251.46.138	80	10.160.37.71	50509	TCP
2015-12-15 10:49:23	SNAT	10.0.0.199	UNKNOWN-	50477	159.106.121.75	443	10.160.37.71	50477	TCP
2015-12-15 10:49:23	SNAT	10.0.0.195	UNKNOWN-	50980	54.231.14.107	443	10.160.37.71	50980	TCP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	57100	10.188.7.10	53	10.160.37.71	57100	UDP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	50508	17.167.194.205	443	10.160.37.71	50508	TCP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	50507	17.167.194.208	443	10.160.37.71	50507	TCP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	50506	17.167.195.12	443	10.160.37.71	50506	TCP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	50505	61.135.186.152	80	10.160.37.71	50505	TCP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	50504	17.167.192.126	443	10.160.37.71	50504	TCP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	54546	10.188.7.10	53	10.160.37.71	54546	UDP
2015-12-15 10:49:23	SNAT	10.0.0.198	UNKNOWN-	50503	17.167.192.244	443	10.160.37.71	50503	TCP
2015-12-15 10:49:02	SNAT	10.0.0.195	UNKNOWN-	50979	139.214.193.61	80	10.160.37.71	50979	TCP
2015-12-15 10:49:02	SNAT	10.0.0.199	UNKNOWN-	50477	159.106.121.75	443	10.160.37.71	50477	TCP
2015-12-15 10:49:02	SNAT	10.0.0.199	UNKNOWN-	58170	10.188.7.10	53	10.160.37.71	58170	UDP
2015-12-15 10:48:52	SNAT	10.0.0.195	UNKNOWN-	50978	140.207.54.116	80	10.160.37.71	50978	TCP
2015-12-15 10:48:39	SNAT	10.0.0.199	UNKNOWN-	50476	159.106.121.75	443	10.160.37.71	50476	TCP

Page 1 / 21 Displaying 1 - 20 of 401 Per Page

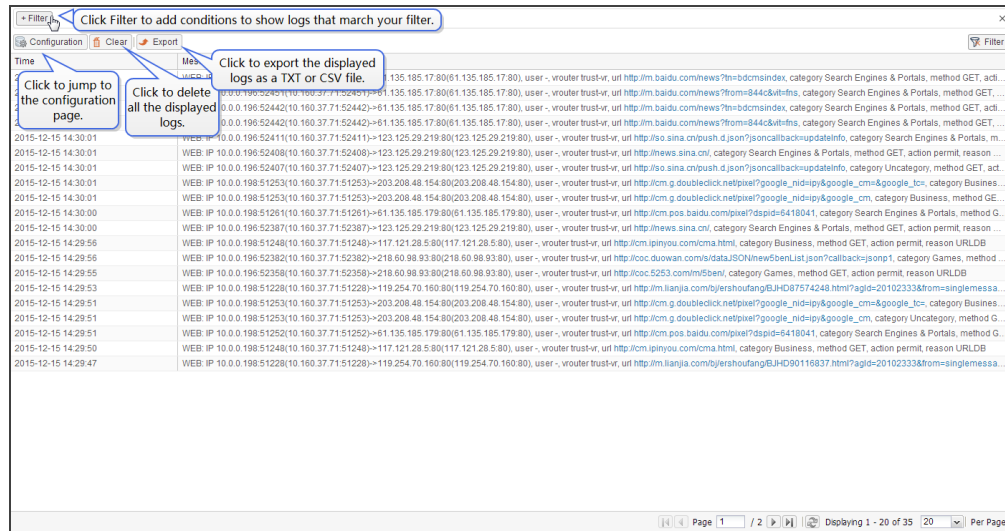
URL Logs

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

URL logs can be generated under the conditions that:

- URL logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 451.
- You have enabled logging function in URL rules. Refer to "URL Filter" on Page 270

To view threat logs, select **Monitor > Log > URL**.



File Filter Logs

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

File Filter logs can be generated under the conditions that:

- File Filter logging in the Logging feature is enabled. Refer to "[Log Configuration](#)" on [Page 451](#).
- You have enabled the function of "[File Filter](#)" on [Page 290](#).

To view File Filter logs, select **Monitor > Log > File Filter**.

- Filter: Click Filter to add conditions to show logs that match your filter
- Configuration: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.
- Export: Click to export the displayed logs as a TXT or CSV file.

Network Behavior Record Logs

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Network Behavior Record logs can be generated under the conditions that:

- Network Behavior Record logging in the Logging feature is enabled. Refer to "[Log Configuration](#)" on Page 451.
- You have enabled the function of "[Network Behavior Record](#)" on Page 292.

To view Network Behavior Record logs, select **Monitor > Log > Network Behavior Record**.



- Filter: Click Filter to add conditions to show logs that march your filter
- Configuration: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.
- Export: Click to export the displayed logs as a TXT or CSV file.

CloudSandBox Logs

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view sandbox logs, select **Monitor > Log > CloudSandBox**.

In this page, you can perform the following actions:

- Configuration: Click to jump to the CloudSandBox page.
- Add to My Log: Click to add the current filtered results to MyLog list.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click  Filter , and then click  to add conditions to show logs that march your filter.

Log Configuration

You can create log server, set up log email address, and add UNIX servers.

Creating a Log Server

To create a log server, take the following steps:

1. Select **Monitor > Log > Configuration**.
2. Click **Log Server** tab.
3. Click **New**.

In the Log Server dialog box, configure these values.

Option	Description
Host name	Enter the name or IP of the log server.
Binding	<p>Specifies the source IP address to receive logs.</p> <ul style="list-style-type: none">• Virtual Router: Select Virtual Router and then select a virtual router from the drop-down list. If a virtual router is selected, the device will determine the source IP address by searching the reachable routes in the virtual router.• Source Interface: Select Source Interface and then select a source interface from the drop-down list. The device will use the IP address of the interface as the source IP to send logs to the syslog server. If management IP address is configured on the interface, the management IP address will be preferred.
Protocol	Specifies the protocol type of the syslog server. If "Secure-TCP" is selected, you can select Do not validate the server certificate option, and system can transfer logs normally and do not need any certifications.
Port	Specifies the port number of the syslog server.
Log Type	Specifies the log types the syslog server will receive.

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



Note: You can add at most 3 log servers.

Cconfiguring Log Encoding

The default encoding format for the log information that is output to the log server is utf-8, and the user can start GBK encoding as needed. After the GBK encoding format is opened, the log encoding format that is output to the log server will be GBK encoding. To enable the GBK encoding :

1. Select **Monitor > Log > Configuration**.
2. Click **Log Server** tab.
3. Click the **Log Encoding Config** button in the upper right corner to open the Log Encoding Config dialog box.
4. Select the check box to enable the GBK encoding.
5. Click **OK** to save the settings.

Adding Email Address to Receive Logs

An email in the log management setting is an email address for receiving log messages.

To add an email address, take the following steps:

1. Select **Monitor > Log > Log Management**.
2. Click **Web Mail** tab.

Email Address: <input type="text"/> + Add (1-63) chars	
Email Address	Operation

3. Enter an email address and click **Add**.
4. If you want to delete an existing email, click **Delete**.



Note: You can add at most 3 email addresses.

Specifying a Unix Server

To specify a Unix server to receive logs, take the following steps:

1. Select **Monitor > Log > Log Management**.
2. Click the **Facility Configuration** tab.

Please select a facility			
<input type="radio"/> Local0	<input type="radio"/> Local1	<input type="radio"/> Local2	<input type="radio"/> Local3
<input type="radio"/> Local4	<input type="radio"/> Local5	<input type="radio"/> Local6	<input checked="" type="radio"/> Local7
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

3. Select the device you want and the logs will be exported to that Unix server.
4. Click **OK**.

Specifying a Mobile Phone

To specify a mobile phone to receive logs, take the following steps:

1. Select **Monitor > Log > Log Management**.
2. Click **SMS** tab.
3. Enter a mobile phone number and click **Add**.
4. If you want to delete an existing mobile phone number, click **Delete**.



Note: You can add at most 3 mobile phone numbers.

Managing Logs

You can configure system to enable the logging function, including enabling various logs.

Configuring Logs

To configure parameters of various log types, take the following steps:

1. Select **Monitor > Log > Log Management**.
2. Click on the tab of the log type you want, and you will enter the corresponding log settings.
3. Click **OK**.

Option Descriptions of Various Log Types

This section describes the options when you set the properties of each log types.

Event Log

Option	Description
Enable	Select the check box to enable the event logging function.
Console	Select the check box to send a syslog to the Console. <ul style="list-style-type: none">• Lowest severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Terminal	Select the check box to send a syslog to the terminal. <ul style="list-style-type: none">• Lowest severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Cache	Select the check box to send a syslog to the cache. <ul style="list-style-type: none">• Lowest severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.• Max buffer size - The maximum size of the cached logs. The default value may vary for different hardware platforms.
File	Select the check box to send a syslog to a file. <ul style="list-style-type: none">• Lowest severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.• Max file size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes.• Redirect log to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the Name box.
Log server	Select the check box to export event logs to the syslog server. <ul style="list-style-type: none">• View Log Server - Click to see all existing syslog servers or to add new server.• Lowest severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Email address	Select the check box to send event logs to the email. <ul style="list-style-type: none">• View Email Address: Click to see all existing email addresses or add a new address.• Lowest severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

Option	Description
Database	<p>Select the checkbox to save logs in the local device. Only several platforms support this parameter.</p> <ul style="list-style-type: none"> • Disk Space - Enter a number as the percentage of storage the logs will take. For example, if you enter 30, the event logs will take at most 30% of the total disk size. • Disk Space Limit - If Auto Overwrite is selected, the logs which exceed the disk space will overwrite the old logs automatically. If Stop Storing is selected, system will stop storing new logs when the logs exceed the disk space.

Network Log

Option	Description
Enable	Select the check box to enable the network logging function.
Cache	<p>Select the check box to export network logs to the cache.</p> <ul style="list-style-type: none"> • Max buffer size - The maximum size of the cached network logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
Log server	<p>Select the check box to export network logs to the syslog server.</p> <ul style="list-style-type: none"> • View Log Server - Click to see all existing syslog servers or to add a new server.
Database	<p>Select the checkbox to save logs in the local device. Only several platforms support this parameter.</p> <ul style="list-style-type: none"> • Disk Space - Enter a number as the percentage of storage the logs will take. For example, if you enter 30, the network logs will take at most 30% of the total disk size. • Disk Space Limit - If Auto Overwrite is selected, the logs which exceed the disk space will overwrite the old logs automatically. If Stop Storing is selected, the system will stop storing new logs when the logs exceed the disk space.

Configuration Log

Option	Description
Enable	Select the check box to enable the configuration logging function.
Cache	<p>Select the check box to export configuration logs to the cache.</p> <ul style="list-style-type: none"> • Max buffer size - The maximum size of the cached configuration logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
Log Server	<p>Select the check box to export network logs to the syslog server.</p> <ul style="list-style-type: none"> • View Log Server - Click to see all existing syslog servers or to add new server.
Database	<p>Select the checkbox to save logs in the local device. Only several platforms support this parameter.</p> <ul style="list-style-type: none"> • Disk Space - Enter a number as the percentage of storage the logs will take. For example, if you enter 30, the configuration logs will take at most 30% of the total disk size. • Disk Space Limit - If Auto Overwrite is selected, the logs which exceed

Option	Description
	the disk space will overwrite the old logs automatically. If Stop Storing is selected, the system will stop storing new logs when the logs exceed the disk space.
Log Generating Limitation	Select the check box to define the maximum efficiency of generating logs. <ul style="list-style-type: none"> Maximum Speed - Specified the speed (messages per second).

Session Log

Option	Description
Enable	Select the check box to enable the session logging function. <ul style="list-style-type: none"> Record User Name: Select to show the user's name in the session log messages. Record Host Name: Select to show the host's name in the session log messages.
Cache	Select the check box to export session logs to cache. <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached session logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Log Server	Select the check box to export session logs to the syslog server. <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server. Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

PBR Log

Option	Description
Enable	Select the check box to enable a PBR logging function. <ul style="list-style-type: none"> Record User Name: Select to show the user's name in the PBR log messages. Record Host Name: Select to show the host's name in the PBR log messages.
Cache	Select the check box to export PBR logs to the cache. <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached PBR logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Log Server	Select the check box to export PBR logs to the syslog server. <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server. Syslog Distribution Methods - The distributed logs can be in the format of plain text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

NAT Log

Option	Description
Enable	<p>Select the check box to enable the NAT logging function.</p> <ul style="list-style-type: none"> Record Host Name: Select to show the host's name in the NAT log messages.
Cache	<p>Select the check box to export NAT logs to cache.</p> <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached NAT logs. The default value may vary for different hardware platforms.
Log Server	<p>Select the check box to export NAT logs to log servers.</p> <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server. Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

URL Log

Option	Description
Enable	<p>Select the check box to enable the URL logging function.</p> <ul style="list-style-type: none"> Record Host Name: Select to show the host's name in the URL log messages.
Cache	<p>Select the check box to export URL logs to the cache.</p> <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached URL logs. The default value may vary for different hardware platforms.
Log Server	<p>Select the check box to export URL logs to a log server.</p> <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server. Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

File Filter Log

Option	Description
Enable	<p>Select this check box to enable the File Filter logging function.</p>
Cache	<p>Select the check box to export File Filter logs to cache.</p> <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached File Filter logs. The default value may vary for different hardware platforms.
Log Server	<p>Select the check box to export File Filter logs to log server.</p> <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server. Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

Network Behavior Record Log

Option	Description
Enable	Select this check box to enable the Network Behavior Record logging function.
Cache	Select the check box to export Network Behavior Record logs to cache. <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached Network Behavior Record logs. The default value may vary from different hardware platforms.
Log Server	Select the check box to export Network Behavior Record logs to log server. <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server. Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

CloudSandBox Log

Option	Description
Enable	Select this check box to enable the CloudSandBox logging function.
Cache	Select the check box to export CloudSandBox logs to the cache. <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached CloudSandBox logs.
File	Select to export CloudSandBox logs as a file.
Log Server	Select the check box to export CloudSandBox logs to log server. <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server.

Threat Log

Option	Description
Enable	Select this check box to enable the threat logging function.
Cache	Select the check box to export threat logs to the cache. <ul style="list-style-type: none"> Max buffer size - The maximum size of the cached threat logs. The default value may vary from different hardware platforms.
File	Select to export threat logs as a file to USB. <ul style="list-style-type: none"> Max File Size - Exported log file maximum size. Save logs to USB - Select a USB device and enter a name as the log file name.
Terminal	Select to send logs to terminals.
Log Server	Select the check box to export threat logs to log server. <ul style="list-style-type: none"> View Log Server - Click to see all existing syslog servers or to add a new server. Syslog Distribution Methods - the distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.
Email address	Select the check box to export logs to the specified email address.

Option	Description
	<ul style="list-style-type: none"> • Viewing Email Address: Click to see or add email address.
Database	<p>Select the checkbox to save logs in the local device. Only several platforms support this parameters.</p> <ul style="list-style-type: none"> • Disk Space - Enter a number as the percentage of a storage the logs will take. For example, if you enter 30, the threat logs will take at most 30% of the total disk size. • Disk Space Limit - If Auto Overwrite is selected, the logs which exceed the disk space will overwrite the old logs automatically. If Stop Storing is selected, system will stop storing new logs when the logs exceed the disk space.

Chapter 13 Diagnostic Tool

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

System supports the following diagnostic methods:

- **Global Fault Detection:** Displays all information that matches the search conditions, which facilitates the viewing of the related information. When there are network issues, you can use the faults such as certain users/groups, certain IPs, or certain applications as the conditions to search all information that relates to the faults. Then you can locate the cause of the faults fast.
- **Packet Path Detection:** Detects the packets and shows the detection processes and results to the users with charts and descriptions.
- **Packet Capture Tool:** Captures packets in the system. After capturing the packets, you can export them to your local disk and then analyze them using third-party tools.
- **Test Tools:** DNS Query, Ping and Traceroute can be used when troubleshooting the network.

Global Fault Detection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The global fault detection function displays all information that matches the search conditions, which facilitates the viewing of the related information. When there are network issues, you can use the faults such as certain user-s/groups, certain IPs, or certain applications as the conditions to search all information that relates to the faults. Then you can locate the cause of the faults fast.

To configure the global fault detection settings:

1. Configure search conditions, including the user/user group, IP address, interface, application, and zone.
2. Click **Search** to start the search. The search results will be listed in the Configuration tab and Network Service Detection tab.

Configuring Search Conditions

To configure search conditions, take the following steps:

1. Select **System > Diagnostic Tool > Global Fault Detection**.
2. **Configure search conditions as follows.**

Option	Description
AAA Server	Select a server from the drop-down list. If the selected AAA server is a local server, select the corresponding user/group from the User/Group drop-down list; if the selected AAA server is not a local server, enter the corresponding username/group name in the blank text box, and then click Add . You can at most configure 3 users/groups.
IP	Enter the IP address, IP address/netmask, or IP address range in the text box, and then click Add . You can at most configure 3 entries. For different IP address, IP address/netmask, or IP address range, separate them with a comma.
Interface	Select the interface from the drop-down list. You can at most configure 3 interfaces.
Application	Select the application from the drop-down list. You can at most configure 3 applications or application groups.
Zone	Select the zone from the drop-down list. You can at most configure 3 zones.
Time	Select the start time and/or the end time. By default, the system will search the conditions for 1 hour at least. The system can search the information 1 month at most.



Note:

- You can set at most 3 search conditions for each condition type.
- For the same condition type, the logical relation between the conditions is OR; for the different condition type, the logical relation between the conditions is AND. If you configure two conditions of the same condition types, for example, IP A and IP B, the search results will list any entry that matches the condition IP A or the condition IP B. If you configure two conditions of different types, IP A and application B, the search results will list the entries that match the condition IP A and the condition application B.

Viewing Search Results

In the Configuration tab, the search results will be listed in the table by category, including the policy, PBR rule, SNAT, DNAT, zone, interface, user/user group, address book, and others. Click the category name, and system jumps to that corresponding module. Users can then view the detailed configurations of each module and configure the settings according to their requirements. If you have filtered time, the results will show you logs in the specified time. If not, system will show you all logs.

In Network Service Detection tab, you can view network nodes, service nodes, historical trend graph of packet loss rate and latency of service/network nodes which satisfy your search requirements.

Packet Path Detection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

Based on the packet process flow, the packet path detection function detects the packets and shows the detection processes and results to the users with charts an descriptions. This function can detect the following packet sources: emulation packet, online packet, and imported packet (system provides the Packet Capture Tool for you that can help you capture the packets).

The detectable packets from different packet sources have different detection measures. System supports the following measures:

- Emulation packet detection: Emulate a packet and detect the process flow in the system of this packet.
- Online packet detection: Perform a real-time detection of the process flow of the packets in system.
- Imported packet detection: Import the existing packets and detect the process flow in system of the packets.

Configuring Packet Path Detection

You can configure the packet path detection configurations and view the detection results in the report.

Emulation Detection

To perform the emulation detection, take the following steps:

1. Select **System > Diagnostic Tool > Packet Path Detection**.
2. Click **Choose Detected Source**.
3. In the Choose Detected Source dialog box, select **Emulation Packet** tab.

The screenshot shows a dialog box titled "Choose Detected Source". On the left, there are four tabs: "Emulation Pac...", "Online Packet", "Imported Packet", and "Detected Sour...". The "Emulation Pac..." tab is currently selected. The main area of the dialog contains several input fields:

- Name:** A text box with a placeholder "(1-31) chars".
- Ingress Interface:** A dropdown menu currently showing "aggregate1".
- Source Addr:** A text box.
- Destination Addr:** A text box.
- Protocol:** A dropdown menu currently showing "TCP".
- Source Port:** A text box with a placeholder "1-65535".
- Destination Port:** A text box with a placeholder "1-65535".
- Description:** A text box with a placeholder "(1-255) chars".




 At the bottom of the dialog, there are three buttons: "Capture screenshot", "OK", and "Cancel".

Configure options as follows.




Option	Description
Name	Specifies the name of the emulation packet.
Ingress Interface	Select the ingress interface of the emulation packet from the drop-down list.
Source Addr	Specifies the source IP address of the emulation packet in the text box.
Destination Addr	Specifies the destination IP address of the emulation packet in the text box.
Protocol	Select the protocol of the emulation packet from the drop-down list. When selecting TCP or UDP, specify the source and destination ports in

Option	Description
	the Source Port and Destination Port text boxes; when selecting ICMP, enter the ICMP type and code in the Type and Value text boxes.
Description	Specifies the description for this emulation packet.

- Click **Start** to start the detection. The system displays the detection flow in the flow chart and describes the detection process. The flow chart contains all modules the packets passes in the system. After the detection for a particular module is completed, the status indicator above the module indicates the detection results.

- Green indicator() - Indicates the detection for this module has been passed. System will proceed with the detection. Hover your mouse over this step to view its introduction.
- Yellow indicator() - Indicates the detection for this module has been passed, but there are potential security risks. System will proceed with the detection. Hover your mouse over this step to view its introduction and the detection results. You can click the **View Results** link to view the detailed detection report.
- Red indicator() - Indicates the detection for this module fails to pass. System has stopped the detection. Hover your mouse over this step to view its introduction and the detection results. You can click the **View Results** link to view the detailed detection report. If the failure is caused by the policy rule configurations, you can click the link in the Policy Rule step to jump to the policy rule configuration page.

- After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicator and detection result summary. You can click the **View Details** link to view the detailed detection report. The meanings of status indicators are as follows:

- Green indicator() - Indicates the detected source has passed all detection.
- Yellow indicator() - Indicates the detected source has passed all detection, but there are potential security risks in one or more steps. You can click the **View Details** link to view the potential risks and advice.
- Red indicator() - Indicates not all detection is passed by the detected source. You can click the **View Details** link to view the failure reasons and advice.

Online Detection

To perform the online detection, take the following steps:


- Select **System > Diagnostic Tool > Packet Path Detection**.
- Click **Choose Detected Source**.
- In the Choose Detected Source dialog box, select **Online Packet** tab.

Configure options as follows.

Option	Description
Name	Specifies the name of the online packet.
Ingress Interface	Select the ingress interface of the online packet from the drop-down list.
Source	Specifies the source IP address or the user/user group of the online packet. <ul style="list-style-type: none"> Address: Select the Address radio button and enter the IP address in the text box. User/User Group: Select the User/User Group radio button and select the user/user group from the drop-down list.
Destination	Specifies the destination IP address of the online packet. <ul style="list-style-type: none"> Address: Select the radio button and enter the IP address in the text box. URL: Select the radio button and enter the URL in the text box.
Protocol	Specifies the protocol type or the protocol number of the packet.
Source Port	Specifies the source port of the online packet.
Destination Port	Specifies the destination port of the online packet.
Application	Specifies the application type of the online packet.
Description	Enter the description of the online packet in the text box.

- Click **OK**.
- If needed, specify the detecting duration in the Detecting Duration section. After reaching the specified duration, system will automatically stop the detection. The default value is 30 minutes.
- If needed, select **Capture Packets** check box to enable the capture packets function. You can download the captured packets to a specified directory. Before selecting this check box, make sure the Packets Capture Tools function is disabled. For more information, see "[Packet Capture Tool](#)" on [Page 467](#).
- Click **Start** to start the detection. The system displays the detection process. If errors occur during the detection, a flow thumbnail in the area of the flow chart pops up to display the corresponding errors. After the detection is completed, you can click the flow thumbnail to view the details. During each detection process, the system can pop up at most six thumbnails.
- After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicator and detection result summary. You can click the **View Details** link to view the

detailed detection report. About the meanings of status indicators, view step 3 in Emulation Detection.



Note: If one of the following situations happens during the detection, the system will stop the detection.

- Click the **Stop** button.
- Reach the upper limit of the detecting duration. If you do not set the detecting duration, the detecting duration keeps the default value (30 minutes).
- The total number of errors of the same type reaches 10. For example, the flow is blocked by the same policy.
- The total number of errors of different types reaches 5. Errors of different types mean the errors occurred in different modules or errors occurred in one module but are different types.
- After selecting the **Capture Packets** option, the size of the captured packet file reaches 10M and errors occurred during the detection.

Imported Detection

To perform the imported detection, take the following steps:

- 1. Select **System > Diagnostic Tool > Packet Path Detection**.
- 2. Click **Choose Detected Source**.
- 3. In the Choose Detected Source dialog box, select **Imported Packet** tab.

Emulation Pac...

Online Packet

Imported Packet

Detected Sour...

Packet: Browse

Name: (1-31) chars

Ingress Interface:

aggregate1

Description: (1-255) chars

<<< Advanced

Source Addr:

Destination Addr:

Protocol:

TCP,UDP,ICMP or Protocol number (1-255)

Source Port: 1-65535

Destination Port: 1-65535

Application:

OK

Cancel

Configure options as follows.

Option	Description
Packet	Click the Browse button and select the packet file to import it. The maximum size of the imported packet file can be 20M.
Name	Specifies the name of the imported packet.
Ingress Interface	Select the ingress interface of the imported packet from the drop-down list.

Option	Description
Description	Enter the description of the online packet in the text box.
Advanced	
Source Addr	Specifies the source IP address of the imported packet.
Destination Addr	Specifies the destination IP address of the imported packet.
Protocol	Specifies the protocol type or the protocol number of the imported packet.
Source Port	Specifies the source port of the imported packet.
Destination Port	Specifies the destination port of the imported packet.
Application	Specifies the application type of the imported packet.

4. Click **OK**.
5. Click **Start** to start the detection. The system displays the detection process in the Detection Process tab. If errors occur during the detection, a flow thumbnail in the area of the flow chart pops up to display the corresponding errors. After the detection is completed, you can click the flow thumbnail to view the details. During each detection process, the system can pop up at most six thumbnails.
6. After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicators and detection result summary. You can click the **View Details** link to view the detailed detection report. For the meanings of the status indicators, view step 3 in Emulation Detection.



Note: If one of following situations happens during the detection, the system will stop the detection.

- Click the **Stop** button.
- The total number of errors of the same type reaches 10. For example the flow is blocked by the same policy.
- The total number of errors of different types reaches 5. Errors of different types mean the errors occurred in different modules or errors occurred in one module but are different types.
- The imported packets have been all detected.

Detected Sources

The detected sources dialog box lists all detected sources in the system, including the emulation packet, online packet, and imported packet.

Click **Choose Detected Source**. In the Choose Detected Source dialog box, select the **Detected Sources** tab. You can then perform the following actions:

- Click **Details** in the Result column to view the detection report of the detected source.
- Click **Export** in the Export Packet column to export the detected packet to the desired directory.
- Click **Edit** in the Option column to edit the configurations of the detected source.
- Click **Delete** in the Option column to delete the detected source.

Packet Capture Tool

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Users can capture packets in the system by Packets Capture Tools. After capturing the packets, you can export them to your local disk and then analyze them by third-party tools.

Configuring Packet Capture Tools

To capture packets, take the following steps:

- 1. Select **System > Diagnostic Tool > Packet Capture Tool**.
- 2. Click **New**.

Packet Capture Configuration

Name:

1-31 chars

Source:

☒ Address

☐ User/User Group

User/User Group

Destination:

☒ Address

☐ URL

1-63 chars

Application:

Protocol:

TCP, UDP, ICMP or Protocol number 1-255

Source Port:

1-65535

Destination Port:

1-65535

File Size:

2MB-20MB

Description:

1-255 chars

OK

Cancel

In the Packet Capture Configuration dialogs, configure as follows.

Option	Description
Name	Enter the name of the packets capture entry.
Source	Specifies the source IP address or the user/user group of the packet. <ul style="list-style-type: none">• Address: Select the Address radio button and enter the IP address in the text box.• User/User Group: Select the User/User Group radio button and select the user/user group from the drop-down list.
Destination	Specifies the destination IP address o of the packet. <ul style="list-style-type: none">• Address: Select the radio button and enter the IP address in the text box.• URL: Select the radio button and enter the URL in the text box.
Application	Specifies the application type of the packet
Protocol	Specifies the protocol type or the protocol number of the packet.
Source Port	Specifies the source port of the packet.
Destination Port	Specifies the destination port of the packet.
File Size	Specifies the maximum size of the captured packet file. When the file size reaches the maximum size, the system stops the capturing. The range of the value is from 2M to 20M. The default value is 10M.
Description	Enter the entry description in the text box.

3. Click **OK**.
4. For each entry, click **Start** button in the Capture Packets column to start capturing packets. The system displays the progress under the table. Hover your mouse over the progress, and the system displays the size of the completed capture packets.
5. To stop capturing packets, click **Stop** button next to the progress bar or the **Stop** button in the Capture Packets column.
6. After you stop capturing packets or the capturing is completed, click **Download** to save the captured packets to a specified location.



Note:

- The system allows you to create at most 5 packets capture entries.
- For each entry, system only saves the latest results of packets capture. When you start an entry again, the system will ask you whether to cover or export the results generated in the last time. Click **Cover** to cover the results generated in the last time; click **Export** to export the results generated in the last time; click **Cancel** to cancel the packets capture.

Test Tools

DNS Query, Ping and Traceroute can be used when troubleshooting the network.

DNS Query

To check the DNS working status of the device, take the following steps:

1. Select **System > Diagnostic Tool > Test Tools**.
2. Type a domain name into the **DNS Query** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Ping

To check the network connecting status, take the following steps:

1. Select **System > Diagnostic Tool > Test Tools**.
2. Type an IP address into the **Ping** box.
3. Click **Test**, and the testing result will be displayed in the list below.
4. The testing result contains two parts:
 - The Ping packet response. If there is no response from the target after timeout, it will print Destination Host Not Response, etc. Otherwise, the response contains sequence of packet, TTL and the response time.
 - Overall statistics, including number of packet sent, number of packet received, percentage of no response, the minimum, average and maximum response time.

Traceroute

Traceroute is used to test and record gateways the packet has traversed from the originating host to the destination. It is mainly used to check whether the network connection is reachable, and analyze the broken point of the network. The common Traceroute function is performed as follows: first, send a packet with TTL 1, so the first hop sends back an ICMP error message to indicate that this packet can not be sent (because of the TTL timeout); then this packet is re-sent, with TTL 2, TTL timeout is sent back again; repeat this process till the packet reaches the destination. In this way, each ICMP TTL timeout source address is recorded. As the result, the path from the originating host to the destination is identified.

To test and record gateways the packet has traversed by Traceroute, take the following steps:

1. Select **System > Diagnostic Tool > Test Tools**.
2. Type an IP address into the **Traceroute** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Chapter 14 High Availability

HA, the abbreviation for High Availability, provides a fail-over solution for communications lines or device failure to ensure the smooth communication and effectively improve the reliability of the network. To implement the HA function, you need to configure the two devices as HA clusters, using the identical hardware platform and firmware version, both enabling Virtual Router and AV functions, with anti-virus license installed. When one device is not available or can not handle the request from the client properly, the request will be promptly directed to the other device that works normally, thus ensuring uninterrupted network communication and greatly improving the reliability of communications.

System supports three HA modes: Active-Passive (A/P), Active-Active (A/A), and Peer.

- **Active-Passive (A/P) mode:** In the HA cluster, configure two devices to form a HA group, with one device acting as a primary device and the other acting as its backup device. The primary device is active, forwarding packets, and meanwhile synchronizes all of its network and configuration information and current session information to the backup device. When the primary device fails, the backup device will be promoted to primary and takes over its work to forward packets. This A/P mode is redundant, and features a simple network structure for you to maintain and manage.
- **Active-Active (A/A) mode:** When the security device is in NAT mode, routing mode or a combination of both, you can configure two Hillstone devices in the HA cluster as active, so that the two devices are running their own tasks simultaneously, and monitoring the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously to ensure uninterrupted work. This mode is known as the Active-Active mode. The A/A mode has the advantage of high-performance, as well as load-balancing.
- **Peer mode:** the Peer mode is a special HA Active-Active mode. In the Peer mode, two devices are both active, perform their own tasks simultaneously, and monitor the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously. In the Peer mode, only the device at the active status can send/receive packets. The device at the disabled status can make two devices have the same configuration information but its interfaces do not send/receive any packets. The Peer mode is more flexible and is suitable for the deployment in the asymmetric routing environment.

HA Active-Active (A/A) and Peer mode may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Basic Concepts

HA Cluster

For the external network devices, a HA cluster is a single device which handles network traffic and provides security services. The HA cluster is identified by its cluster ID. After specifying a HA cluster ID for the device, the device will be in the HA state to implement HA function.

HA Group

System will select the primary and backup device of the same HA group ID in a HA cluster according to the HCMP protocol and the HA configuration. The primary device is in the active state and processes network traffic. When the primary device fails, the backup device will take over its work.

When assigning a cluster ID to the device, the HA group with ID 0 will be automatically created. In Active-Passive (A/P) mode, the device only has HA group 0. In Active-Active (A/A) mode, the latest Hillstone version supports two HA groups, i.e., Group 0 and Group 1.

HA Node

To distinguish the HA devices in a HA group, you can use the value of HA Node to mark the devices. StoneOS support the values of 0 and 1.

In the HA Peer mode, the system can decide which device is the master according to the HA Node value. In the HA group 0, the device whose HA Node value is 0 will be active and the device whose HA Node value is 1 is at the disabled status. In the HA group 1, this does not make sense because both times is HA Node value of 0

Virtual Forward Interface and MAC

In the HA environment, each HA group has an interface to forward traffic, which is known as the Virtual Forward Interface. The primary device of each HA group manages a virtual MAC (VMAC) address which is corresponding with its interface, and the traffic is forwarded on the interface. Different HA groups in a HA cluster cannot forward data among each other. VMAC address is defined by HA base MAC, HA cluster ID, HA group ID and the physical interface index.

HA Selection

In a HA cluster, if the group ID of the HA devices is the same, the one with higher priority will be selected as the primary device.

HA Synchronization

To ensure the backup device can take over the work of the primary device when it fails, the primary device will synchronize its information with the backup device. There are three types of information that can be synchronized: configuration information, files and RDO (Runtime Dynamic Object). The specific content of RDO includes:

- Session information (The following types of session information will not be synchronized: the session to the device itself, tunnel session, deny session, ICMP session, and the tentative session)
- IPsec VPN information
- SCVPN information
- DNS cache mappings
- ARP table
- PKI information
- DHCP information
- MAC table
- WebAuth information

System supports two methods to synchronize: real-time synchronization and batch synchronization. When the primary device has just been selected successfully, the batch synchronization will be used to synchronize all information of the primary device to the backup device. When the configurations change, the real-time synchronization will be used to synchronize the changed information to the backup device. Except for the HA related configurations and local configurations (for example, the host name), all the other configurations will be synchronized.

Configuring HA

To configure the HA function, take the following steps:

1. Configure a HA Virtual Forward Interface. For more information on configuring the interface, see ["Configuring an Interface" on Page 47](#).
2. Configure a HA link interface which is used for the device synchronization and HA packets transmission.
3. Configure a HA cluster. Specify the ID of HA cluster to enable the HA function.
4. Configure a HA group. Specify the priority for devices and HA messages parameters.

You need to configure the HA data link interface when configuring the HA function, and make sure the HA group interface 0 and interface 1 can be configured as a HA control link interface, but not a HA data link interface.

To configure HA, take the following steps:

1. Go to **System > HA**.

The screenshot shows the HA configuration page. At the top, there are dropdown menus for 'Control link interface 1' (set to 'ethernet0/4'), 'Control link interface 2', and 'Data link interface'. Below these are input fields for 'IP Address' and 'HA cluster ID'. There are two tabs: 'HA Synchronize Configuration' and 'HA Synchronize Session'. The main area is divided into two sections: 'Group 0' and 'Group 1'. Each group has a 'New' or 'Delete' button and a set of parameters: Priority (100), Preempt (0), Hello interval (1000), Hello threshold (3), Gratuitous ARP packet number (15), Track Object, and Description. Each parameter has a dropdown menu and a range in parentheses.

Option	Description
Control link interface 1	Specifies the name of the HA control link interface. The control link interface is used to synchronize all data between two devices.
Control link interface 2	Specifies the name of HA control link interface (Backup device).
Data link interface	Specifies the name of the HA data link interface. The data link interface is used to synchronize the data packet information. After specifying this data link, the session information will be synchronized over this data link. You can configure the physical interface or aggregate interface as the interface of the data link and you can specify at most 1 HA data link interface.
IP address	Specifies the IP address and netmask of the HA link interface.
HA cluster ID	Specifies an ID for HA cluster. The value ranges from 1~8. None indicates to disable the HA function.
Node ID	After enabling the HA function, specify the Node ID (HA Node) for the device. The IDs for two devices must be different. The range is 0 to 1. If you do not specify this value, the devices will obtain the Node ID by automatic negotiation.
Peer-mode	Selects the Enable checkbox to enable the HA Peer mode and specifies the role of this device in the HA cluster. The range is 0 to 1. By default, the group 0 in the device whose HA Node ID is 0 will be active and the group 0 in the device whose HA Node ID is will be in the disabled status.
Symmetric-routing	Select Symmetric-routing to make the device work in the symmetrical routing environment.

Option	Description
HA Synchronize Configuration	In some exceptional circumstances, the master and backup configurations may not be synchronized. In such a case you need to manually synchronize the configuration information of the master and backup device. Click HA Synchronize Configuration to synchronize the configuration information of the master and backup device.
HA Synchronize Session	By default the system will synchronize sessions between HA devices automatically. Session synchronization will generate some traffic, and will possibly impact device performance when the device is overloaded. You can enable automatic HA session synchronization according to the device workload to assure stability. Click HA Synchronize Session to enable automatic HA session synchronization.
New	After specifying the HA cluster ID, the system will create the HA group 0 automatically. Click New to create the HA group 1.
Delete	Click Delete to remove HA group 1 if needed.
Priority	Specifies the priority for the device. The device with higher priority (smaller number) will be selected as the primary device.
Preempt	Configure the preempt mode. When the preempt mode is enabled, once the backup device finds that its own priority is higher than the primary device, it will upgrade itself to become the primary device and the original primary device will become the backup device. The value of 0 indicates to disable the preempt mode. When the preempt mode is disabled, even if the device's priority is higher than the primary device, it will not take over the primary device unless the primary device fails.
Hello interval	Specifies the Hello interval value. The Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical.
Hello threshold	Specifies the threshold value of the Hello message. If the device does not receive the specified number of Hello messages from the other device, it will suppose the other device's heartbeat stops.
Gratuitous ARP packet number	Specifies the number of gratuitous ARP packets. When the backup device is selected as the primary device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table.
Track object	Specifies the track object you have configured. The track object is used to monitor the working status of the device. Once finding the device stop working normally, system will take the corresponding action.
Description	Type the descriptions of HA group into the box.

2. Click **OK**.

Chapter 15 System Management

The device's maintenance and management include:

- "System Information" on Page 475
- "Device Management" on Page 477
- "Configuration File Management" on Page 487
- "SNMP" on Page 489
- "Upgrading System" on Page 494
- "License" on Page 496
- "Mail Server" on Page 500
- "SMS Parameters" on Page 501
- "Connecting to HSM" on Page 502
- "Connecting to Hillstone CloudView" on Page 503
- "Test Tools" on Page 469
- "VSYS (Virtual System)" on Page 505

System Information

Users can view the general information of the system in the System Information page, including Serial Number, Hostname, Platform, System Time, System Uptime, Firmware, Signature Database and so on.

Viewing System Information

To view system information, select **System > System Information**.

Option	Description
Serial Number	Show the serial number of device.
Hostname	Show the name of device.
Platform	Show the platform model of device.
System Time	Show the system date and time of device.
System Uptime	Show the system uptime of device.
HA State	Show the HA status of device. <ul style="list-style-type: none">• Standalone: Non-HA mode that represents HA is disabled.• Init: Initial state.• Hello: Negotiation state that represents the device is consulting the relationship between the master and backup.• Master: Master state that represents the current device is the master.• Backup: Backup state that represents the current device is the backup.• Failed: Fault state that represents the device has failed.
Firmware	Show the current firmware version of the device and the date of the last firmware upgrade.
Application Signature	Show the current version of the application signature database and the date of the last update.
Advanced Threat Detection Signature	Show the current version of the advanced threat detection signature database and the date of the last update.
Abnormal Behavior Detection Signature	Show the current version of the abnormal behavior detection signature database and the date of the last update.
URL Signature	Show the current version of the URL signature database and the date of the last update.
Perimeter Traffic Filtering Signature	Show the current version of the perimeter traffic filtering signature database and the date of the last update.
Antivirus Signature	Show the current version of the antivirus signature database and the date of the last update.
IPS Signature	Show the current version of the IPS signature database and the date of the last update.
Mitigation Signature	Show the current version of the mitigation signature database and the date of the last update.



Note: The signature is all license controlled, so you need to make sure that your system has installed that license. Refer to ["License" on Page 496](#).

Device Management

Introduces how to configure the Administrator, Trust Host, MGT Interface, System Time, NTP Key and system options.

Administrators

Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles. By default, the system supports the following administrators, which cannot be deleted or edited:

- **admin**: Permission for reading, executing and writing. This role has the authority over all features. You can view the current or historical configuration information.
- **admin-read-only**: Permission for reading and executing. You can view the current or historical configuration information.
- **operator**: Permission for reading, executing and writing. You have the authority over all features except modify the Administrator's configuration, view the current or historical configuration information, but no permission to check the log information.
- **auditor**: You can only operate on the log information, including view, export and clear.

The following table shows the permissions to different types of administrators.

Operation	Administrator	Administrator (read-only)	Auditor	Operator
Configure (including saving configuration)	√	X	X	√
Configure administrator	√	X	X	X
Restore factory default	√	X	X	X
Delete configuration file	√	X	X	√
Roll back configuration	√	X	X	√
Reboot	√	X	X	X
View configuration information	√	√	X	√
View log information	√	√	√	X
Modify current admin password	√	√	X	√
ping/traceroute	√	√	X	√



Note:

- The device ships with a default administrator named hillstone. You can modify the setting of hillstone. However, this account cannot be deleted.
- Other administrator roles (except default administrator) cannot configure the admin settings, except modifying its own password.
- The system auditor can manage one or more logs, but only the system administrator can manage the log types.

VSYS Administrator

Administrators in different VSYSs are independent from each other. Administrators in the root VSYS are known as root administrators and administrators in the non-root VSYS are known as non-root administrators. The system supports four types of administrator, including Administrators, Administrator(read-only), Operator, and Auditor.

When creating VSYS administrators, you must follow the rules listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root administrators or root operators after logging into the non-root VSYS.
- After logging into the root VSYS, the root administrators can switch to the non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after a successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify the VSYS the administrator belongs to in form of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

The following table shows the permissions to different types of VSYS administrators.

Operation	Root VSYS Administrator	Root VSYS Administrator (read-only)	Root VSYS Auditor	Root VSYS Operator	Non-root VSYS Administrator	Non-root VSYS Administrator (read-only)	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including saving configuration)	√	×	×	√	√	×	√	×
Configure administrator	√	×	×	×	√	×	×	×
Restore factory default	√	×	×	×	×	×	×	×
Delete configuration file	√	×	×	√	√	×	√	×
Roll back configuration	√	×	×	√	√	×	√	×
Reboot	√	×	×	√	×	×	×	×
View configuration information	√	√	×	√	View information in current VSYS	View information in current VSYS	View information in current VSYS	×
View log information	√	√	√	×	√	√	×	√
Modify current admin password	√	√	×	√	√	√	√	√
ping/traceroute	√	√	×	√	√	√	√	×

Creating an Administrator Account

To create an administrator account, take the following steps:

1. Select **System > Device Management > Administrators**.
2. Click **New**.

3. In the Configuration dialog box, configure the following.

The Configuration dialog box includes the following fields and options:

- Name:** Text input field (4-31 chars)
- Role:** Dropdown menu (currently set to 'admin')
- Password:** Text input field (4-31 chars)
- Confirm Password:** Text input field
- Login Type:**
 - ☐ Console
 - ☐ Telnet
 - ☐ SSH
 - ☐ HTTP
 - ☐ HTTPS
 - ☐ Select All
- Description:** Text input field (0-127 chars)

Buttons: OK, Cancel

Configure the following options.

Option	Description
Name	Type a name for the system administrator account.
Role	<p>From the Role drop-down list, select a role for the administrator account. Different roles have different privileges.</p> <ul style="list-style-type: none"> • Admin: Permission for reading, executing and writing. This role has the authority over all features. • Operator: YThis role has the authority over all features except modifying the Administrator's configurations, and has no permission to check the log information • Auditor: You can only operate on the log information, including the view, export and clear. • Admin-read-only: Permission for reading and executing. You can view the current or historical configuration information.
Password	Type a login password for the admin into the Password box. The password should meet the requirements of Password Strategy.
Confirm Password	Re-type the password into the Confirm Password box.
Login Type	Select the access method(s) for the admin, including Console, Telnet, SSH, HTTP and HTTPS. If you need all access methods, select Select All .
Description	Enter descriptions for the administrator account.

4. Click **OK**.

Admin Roles

Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles. The pre-defined administrator role cannot be deleted or edited. You can customize administrator roles according to your requirements:

To create a new administrator role, take the following steps:

1. Select **System > Device Management > Admin Roles**.
2. Click **New**.

The Configuration dialog box contains the following fields and options:

- Role:** Text input field with a character count of (4-95) chars.
- CLI:** Dropdown menu currently set to 'All'.
- webUI:** A list of modules with checkboxes: iCenter, Monitor, Policy, Object, Network, and System. All are currently checked.
- Permissions:** Three radio buttons: Read-Write (selected), Read, and None.
- Description:** Text input field with a character count of (0-255) chars.
- Buttons:** OK and Cancel at the bottom right.

3. In the Configuration dialog box, configure the following:

Option	Description
Role	Enter the role name.
CLI	Specify the administrator role's privileges of CLI.
WebUI	Click module name to set the administrator role's privilege. represents the administrator role does not have privilege of the specified module, and cannot read and edit the configurations of the specified module. represents the administrator role has the read privilege of the specified module, and cannot edit the configurations. represents the administrator role can read and edit the configurations of the specified module.
Description	Specify the description for this administrator role.

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

Trust Host

The device only allows the trust host to manage the system to enhance the security. Administrator can specify an IP range, and hosts in the specified IP range are trust hosts. Only trust hosts could access the management interface to manage the device.



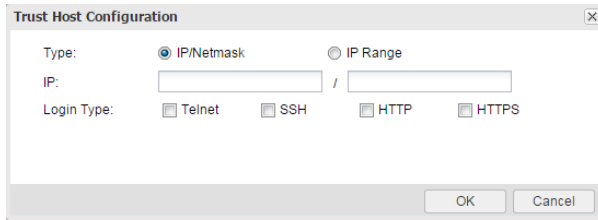
Note: If the system cannot be managed remotely, check the trust host configuration.

Creating a Trust Host

To create a trust host, take the following steps:

1. Select **System > Device Management > Trust Host**.
2. Click **New**.

3. In the Trust Host Configuration dialog box, configure these values.

The image shows a 'Trust Host Configuration' dialog box. It has a title bar with a close button. Inside, there are two radio buttons for 'Type': 'IP/Netmask' (selected) and 'IP Range'. Below this is an 'IP:' field with a slash separator. At the bottom, there are four checkboxes for 'Login Type': 'Telnet', 'SSH', 'HTTP', and 'HTTPS'. At the very bottom are 'OK' and 'Cancel' buttons.

Configure the following options.

Option	Description
Type	<p>Specifies the type of host. You can select IP/Netmask or IP Range.</p> <ul style="list-style-type: none">• IP/Netmask: Type the IP address and netmask into the IP box respectively.• IP Range: Type the start IP and end IP into the IP box respectively.
Login Type	<p>Select the access methods for the trust host, including Telnet, SSH, HTTP and HTTPS.</p>

4. Click **OK**.

Management Interface

The device supports the following access methods: Console, Telnet, SSH and WebUI. You can configure the timeout value, port number, PKI trust domain of HTTPS, and PKI trust domain of certificate authentication. When accessing the device through Telnet, SSH, HTTP or HTTPS, if login fails three times in one minute, the IP address that attempts the login will be blocked for 2 minutes during which the IP address cannot connect to the device.

To configure the access methods:

1. Select **System > Device Management > Management Interface**.
2. In the Management Interface tab, configure these values.

Configure the following options.

Option	Description
Console	<p>Configure the Console access method parameters.</p> <ul style="list-style-type: none">• Timeout: Type the Console timeout value into the Timeout box. The value range is 0 to 60. The default value is 10. The value of 0 indicates never timeout. If there is no activity until the timeout, system will drop the console connection.
Telnet	<p>Configure the Telnet access method parameters.</p> <ul style="list-style-type: none">• Timeout: Specifies the Telnet timeout value. The value range is 1 to 60. The default value is 10.• Port: Specifies the Telnet port number. The value range is 1 to 65535. The default value is 23.
SSH	<p>Configure the SSH access method parameters.</p> <ul style="list-style-type: none">• Timeout: Specifies the SSH timeout value. The value range is 1 to 60. The default value is 10.• Port: Specifies the SSH port number. The value range is 1 to 65535. The default value is 22.

Option	Description
Web	<p>Configure the WebUI access method parameters.</p> <ul style="list-style-type: none"> • Timeout: Specifies the WebUI timeout value. The value range is 1 to 1440. The default value is 10. • HTTP Port: Specifies the HTTP port number. The value range is 1 to 65535. The default value is 80. • HTTPS Port: Specifies the HTTPS port number. The value range is 1 to 65535. The default value is 443. • HTTPS Trust Domain: Select the trust domain existing in the system from the drop-down list. When HTTPS starts, HTTPS server will use the certificate with the specified trusted domain. By default, the trust domain trust_domain_default will be used. • Certificate Authentication: With this checkbox selected, system will start the certificate authentication. The certificate includes the digital certificate of users and secondary CA certificate signed by the root CA. Certificate authentication is one of two-factor authentication. The two-factor authentication does not only need the user's name and password authentication, but also needs other authentication methods, like a certificate or fingerprint. • Binding Trust Domain: After enabling the certificate authentication and logging into the device over HTTPS, HTTPS server will use the certificate with the specified trusted domain. Make sure that root CA certificate is imported into it. • CN Check: After the CN check is enabled, the name of the root CA certificate is checked and verified when the user logs in. Only the certificate and the user can be consistent, and the login succeeds.

3. Click **OK**.



Note: When changing HTTP port, HTTPS port or HTTPS Trust Domain, the web server will restart. You may need to log in again if you are using the Web interface.

System Time

You can configure the current system time manually, or synchronize the system time with the NTP server time via NTP protocol.

Configuring the System Time Manually

To configure the system time manually, take the following steps:

1. Select **System > Device Management > System Time**.
2. Under System Time Configuration in the System Time tab, configure the following.

Option	Description
Sync with Local PC	<p>Specifies the method of synchronize with local PC. You can select Sync Time or Sync Zone&Time.</p> <ul style="list-style-type: none"> • Sync Time: Synchronize the system time with local PC.

Option	Description
Specified the system time.	<ul style="list-style-type: none"> • Sync Zone&Time: Synchronize the system zone&time with local PC. Configure parameter of system time. <ul style="list-style-type: none"> • Time Zone: Select the time zone from the drop-down list. • Date: Specifies the date. • Time: Specifies the time.

3. Click **OK**.

Configuring NTP

The system time may affect the establishment time of VPN tunnel and the schedule, so the accuracy of the system time is very important. To ensure the system is able to maintain an accurate time, the device allows you to synchronize the system time with a NTP server on the network via NTP protocol.

To configure NTP:

1. Select **System > Device Management > System Time**.
2. Under NTP Configuration in the System Time tab, configure the following.

Option	Description
Enable	Select the Enable check box to enable the NTP function. By default, the NTP function is disabled.
Authentication	Select the Authentication check box to enable the NTP Authentication function.
Server	<p>Specifies the NTP server that device need to synchronize with. You can specify at most 3 servers.</p> <ul style="list-style-type: none"> • IP: Type IP address of the server . • Key: Select a key from the Key drop-down list. If you enable the NTP Authentication function, you must specify a key. • Virtual Router: Select the Virtual Router of interface for NTP communication from the drop-down list. • Source interface: Select an interface for sending and receiving NTP packets. • Specify as a preferred server: Click Specify as a preferred server to set the server as the first preferred server. The system will synchronize with the first preferred server.
Sync Interval	Type the interval value. The device will synchronize the system time with the NTP server at the interval you specified to ensure the system time is accurate.
Maximum Adjustment	Type the time value. If the time difference between the system time and the NTP server's time is within the max adjustment value you specified, the synchronization will succeed, otherwise it will fail.

3. Click **OK**.

NTP Key

After enabling NTP Authentication function, you need to configure MD5 key ID and keys. The device will only synchronize with the authorized servers.

Creating a NTP Key

To create an NTP key:

- 1. Select **System > Device Management > NTP Key**.
- 2. Click **NEW**.
- 3. In the NTP Key Configuration dialog box, configure these values.

NTP Key Configuration

Key ID:

(1-65535)

Password:

(1-31)chars

Confirm Password:

OK

Cancel

Configure the following options.

Option	Description
Key ID	Type the ID number into the Key ID box. The value range is 1 to 65535.
Password	Type a MD5 key into the Password box. The value range is 1 to 31.
Confirm Pass-word	Re-type the same MD5 key you have entered into the Confirm box.

- 4. Click **OK**.

Option

Specifies system options, including system language, administrator authentication server, host name, password strategy, reboot and exporting the system debugging information.

To change system option, take the following steps:

- 1. Select **System > Device Management > Option**
- 2. Configure the following.

The screenshot shows a 'System Maintenance' configuration window. It includes sections for 'System Language' (Chinese/English), 'Administrator Authentication Server' (local), 'Host Configuration' (Hostname: SG-6000, Domain:), 'Password Strategy' (Minimum Password Length: 4, Password Complexity: None), and 'System Debug' (Failure Feedback: Enable, System Debug Information: Export). Buttons for 'OK', 'Cancel', 'Reboot', and 'Export' are visible.

Option	Description
System Main-tenance	<p>Configure the system language and administrator authentication server.</p> <ul style="list-style-type: none"> System Language: You can select Chinese or English according to your own requirements. Administrator Authentication Server: Select a server to authenticate the administrator from the drop-down list.
Host Con-figuration	<p>In some situation, more than one devices are installed within a network. To distinguish among these devices, different names should be assigned to different devices. The default host name is assigned according to the model.</p> <ul style="list-style-type: none"> Hostname: Type a host name you want to change into the Host-name box. Domain: Type a domain name you want to specify into the Domain box.
Password Strategy	<p>Configure password complexity for admin user.</p> <ul style="list-style-type: none"> Minimum Password Length: Specifies the minimum length of password. The value range is 4 to 16 characters. The default value is 4. Password Complexity: Unlimited means no restriction on the selection of password characters. You can select Set Password Complexity to enable password complexity checking and configure password complexity. <ul style="list-style-type: none"> Capital letters length: The default value is 2 and the range is 0 to 16. Small letters length: The default value is 2 and the range is 0 to 16. Number letters length: The default value is 2 and the range is 0 to 16. Special letters Length: The default value is 2 and the range is 0 to 16. Validity Period: The unit is day. The range is 0 to 365. The default value is 0, which indicates that there is no restriction on validity period of the password.

3. Click **OK**.

Rebooting the System

Some operations like license installation or image upgrading will require the system to reboot before it can take effect.

To reboot a system, take the following steps:

1. Go to **System > Device Management > Option** .
2. Click **Reboot**, and select **Yes** in the prompt.
3. The system will reboot. You need to wait a while before it can start again.

System Debug

System debug is supported for you to check and analyze the problems.

Failure Feedback

To enable the failure feedback function, take the following steps:

1. Select **System > Device Management> Option**.
2. In the System Tools dialog box, select the **Enable** check box for Failure feedback, and then system will automatically send the technical support file to the manufacturer.

System Debug Information

System debugging helps you to diagnose and identify system errors by the exported file.

To export the system debugging information, take the following steps:

1. Select **System > Device Management> Option**.
2. Click **Export**, system will pack the file in /etc/local/core and prompt to save tech-support file. After selecting the saved location and click **OK**, you can export the file successfully.

Configuration File Management

System configuration information is stored in the configuration file, and it is stored and displayed in the format of command line. The information that is used to initialize the Hillstone device in the configuration file is known as the initial configuration information. If the initial configuration information is not found, the Hillstone device will use the default parameters for the initialization. The information being taking effect is known as the current configuration information.

System initial configuration information includes current initial configuration information (used when the system starts) and backup initial configuration information. System records the latest ten saved configuration information, and the most recently saved configuration information for the system will be recorded as the current initial configuration information. The current configuration information is marked as Startup; the previous nine configuration information is marked with number from 0 to 8, in the order of save time.

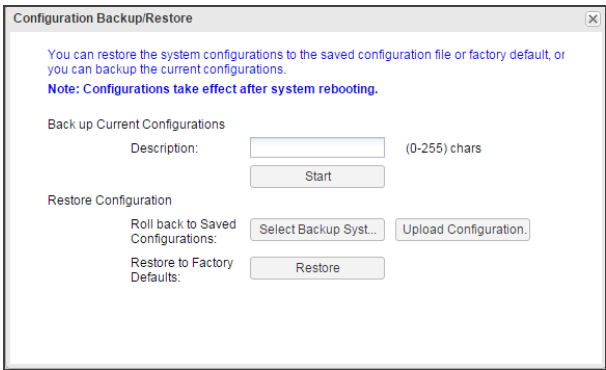
You can not only export or delete the saved configuration files, but also export the current system configurations.

Managing Configuration File

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

To manage the system configuration files, take the following steps:

1. Select **System > Configuration File Management > Configuration File List**.
2. In the Configuration File List page, configure the following.
 - Export: Select the configuration file you want to export, and click **Export**.
 - Delete: Select the configuration file you want to delete, and click **Delete**.
 - Backup Restore: You can restore the system configurations to the saved configuration file or factory default, or you can backup the current configurations.



Option	Description
Back up Current Configurations	Type descriptions for the configuration file into Description box. Click Start to backup.
Restore Con-figuration	<div>Roll back to Saved Configurations:</div> <ul style="list-style-type: none">• Select Backup System Configuration File: Click this button, then select Backup Configuration File from the list. Click OK.• Upload Configuration File: Click this button. In the Importing Configuration File dialog box, click Browse and choose a local configuration file you need in your PC. If you need to make the configuration file take effect, select the check box. Click OK. <div>Restore to Factory Defaults:</div>

Option	Description
	<ul style="list-style-type: none"> Click Restore, in the Restore to Factory Defaults dialog box, click OK. If needed, select Clear History check box. The system will clear the history information automatically.



Note: Device will be restored to factory defaults. Meanwhile, all the system configurations will be cleared, including backup system configuration files.

Viewing the Current Configuration

To view the current configuration file:

1. Select **System > Configuration File Management > Current Configuration**.
2. Click **Export** to export the current configuration file.

SNMP

The device is designed with a SNMP Agent, which can receive the operation request from the Network Management System and give the corresponding information of the network and the device.

The device supports SNMPv1 protocol, SNMPv2 protocol and SNMPv3 protocol. SNMPv1 protocol and SNMPv2 protocol use community-based authentication to limit the Network Management System to get device information. SNMPv3 protocol introduces an user-based security module for information security and a view-based access control module for access control.

The device supports all relevant Management Information Base II (MIB II) groups defined in RFC-1213 and the Interfaces Group MIB (IF-MIB) using SMIV2 defined in RFC-2233. Besides, the system offers a private MIB, which contains the system information, IPSec VPN information and statistics information of the device. You can use the private MIB by loading it into an SNMP MIB browser on the management host.

SNMP Agent

The device is designed with a SNMP Agent, which provides network management and monitors the running status of the network and devices by viewing statistics and receiving notification of important system events.

To configure an SNMP Agent, take the following steps:

1. Select **System > SNMP > SNMP Agent**.
2. In the SNMP Agent page, configure these values.

Agent Configuration

SNMP Agent:

☒ Enabled

ObjectID:

.1.3.6.1.4.1.28557.1.58

System Contact:

(0-255) charaters

Location:

(0-255) charaters

Port/EngineID

Host Port:

(1-65535)

Virtual Router:

trust-vr

Local EngineID:

(1-23) charaters

Apply

Cancel

Option	Description
SNMP Agent	Select the Enable check box for Service to enable the SNMP Agent func-tion.
ObjectID	The Object ID displays the SNMP object ID of the system. The object ID is specific to an individual system and cannot be modified.
System Contact	Type the SNMP system contact information of the device into the System Contact box. System contact is a management variable of the group sys-tem in MIB II and it contains the ID and contact of relevant administrator of the managed device. By configuring this parameter, you can save the important information to the device for the possible use in case of emer-gency.
Location	Type the location of the device into the Location box.
Host Port	Type the port number of the managed device into the Host Port box.
Virtual Router	Select the VRouter from the Virtual Router drop-down list.
Local EngineID	Type the SNMP engine ID into the Local EngineID box.

3. Click **Apply**.



Note: SNMP Engine ID identifies an engine uniquely. SNMP Engine is an important component of the SNMP entity (Network Management System or managed network device) which implements the functions like the reception/sending and verification of SNMP messages, PDU abstraction, encapsulation, and communications with SNMP applications.

SNMP Host

To create an SNMP host, take the following steps:

1. Select **System > SNMP > SNMP Host**.
2. Click **New**.
3. In the SNMP Agent dialog box, configure these values.

The image shows a 'SNMP Host Configuration' dialog box. It has the following fields and options:

- Type:** A drop-down menu currently showing 'IP Address'.
- Hostname:** A text input field with the placeholder text 'Enter IP address'.
- SNMP Version:** A drop-down menu currently showing 'V2C'.
- Community:** A text input field with a label '(1-31) chars' to its right.
- Permission:** A drop-down menu currently showing 'RO'.
- At the bottom right, there are two buttons: 'OK' and 'Cancel'.

Option	Description
Type	Select the SNMP host type from the Type drop-down list. You can select IP Address , IP Range or IP/Netmask . <ul style="list-style-type: none">• IP Address: Type the IP address for SNMP host into Hostname box.• IP Range: Type the start IP and end IP into the Hostname box respectively.• IP/Netmask: Type the start IP address and Netmask for SNMP host into the Hostname box respectively.
SNMP Version	Select the SNMP version from the SNMP Version drop-down list.
Community	Type the community for the SNMP host into the Community box. Community is a password sent in clear text between the manager and the agent. This option is only effective if the SNMP version is V1 or V2C.
Permission	Select the read and write permission for the community from the Permission drop-down list. This option is only effective if the SNMP version is V1 or V2C. <ul style="list-style-type: none">• RO: Stand for read-only, the read-only community is only allowed to read the MIB information.• RW: Stand for read-write, the read-write community is allowed to

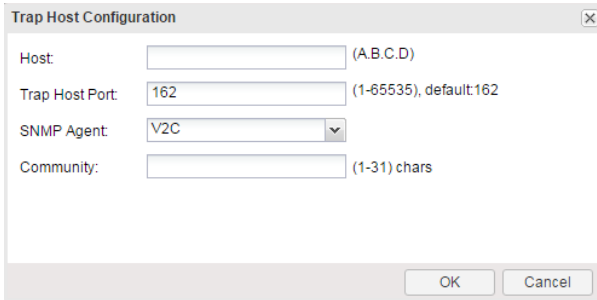
Option	Description
	read and modify the MIB information.

4. Click **OK**.

Trap Host

To create a Trap host, take the following steps:

1. Select **System > SNMP > Trap Host**.
2. Click **New**.
3. In the Trap Host Configuration dialog box, configure these values.



The image shows a 'Trap Host Configuration' dialog box with the following fields and values:

- Host:** A text box with '(A.B.C.D)' as a placeholder.
- Trap Host Port:** A text box containing '162' with '(1-65535), default:162' as a hint.
- SNMP Agent:** A dropdown menu showing 'V2C'.
- Community:** A text box with '(1-31) chars' as a hint.

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

Option	Description
Host	Type the domain name or IP address of the Trap host into the Host box.
Trap Host Port	Type the port number for the Trap host into the Trap Host Port box.
SNMP Agent	Select the SNMP version from the SNMP Agent drop-down list. <ul style="list-style-type: none"> • V1 or V2C: Type the community for the Trap host into the Community box. • V3: Select the V3 user from the V3 User drop-down list. Type the Engine ID for the trap host into the Engine ID box.

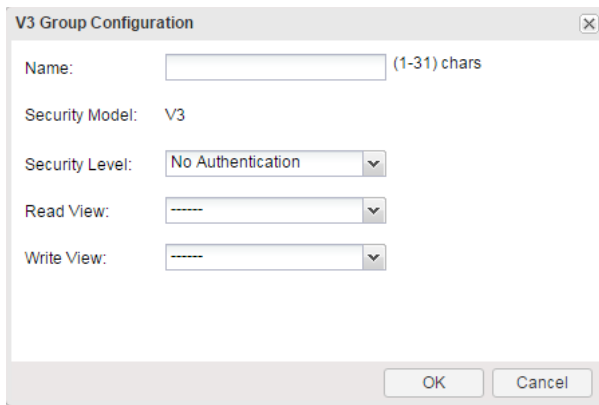
4. Click **OK**.

V3 User Group

SNMPv3 protocol introduces a user-based security module. You need to create an SNMP V3 user group for the SNMP host if the SNMP version is V3.

To create a V3 user group:

1. Select **System > SNMP > V3 User Group**.
2. Click **New**.
3. In the V3 Group Configuration dialog box, enter values.



The image shows a 'V3 Group Configuration' dialog box. It contains the following fields and controls:

- Name:** A text input field with a placeholder '(1-31) chars'.
- Security Model:** A dropdown menu currently set to 'V3'.
- Security Level:** A dropdown menu currently set to 'No Authentication'.
- Read View:** A dropdown menu currently set to '-----'.
- Write View:** A dropdown menu currently set to '-----'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Option	Description
Name	Type the SNMP V3 user group name into the Name box.
Security Model	The Security model option displays the security model for the SNMP V3 user group.
Security Level	<p>Select the security level for the user group from the Security Level drop-down list.</p> <p>Security level determines the security mechanism used in processing an SNMP packet. Security levels for V3 user groups include No Authentication (no authentication and encryption), Authentication (authentication algorithm based on MD5 or SHA) and Authentication and Encryption (authentication algorithm based on MD5 or SHA and message encryption based on AES and DES).</p>
Read View	Select the read-only MIB view name for the user group from the Read View drop-down list. If this parameter is not specified, all MIB views will be none.
Write View	Select the write MIB view name for the user group from the Write View drop-down list. If this parameter is not specified, all MIB views will be none.

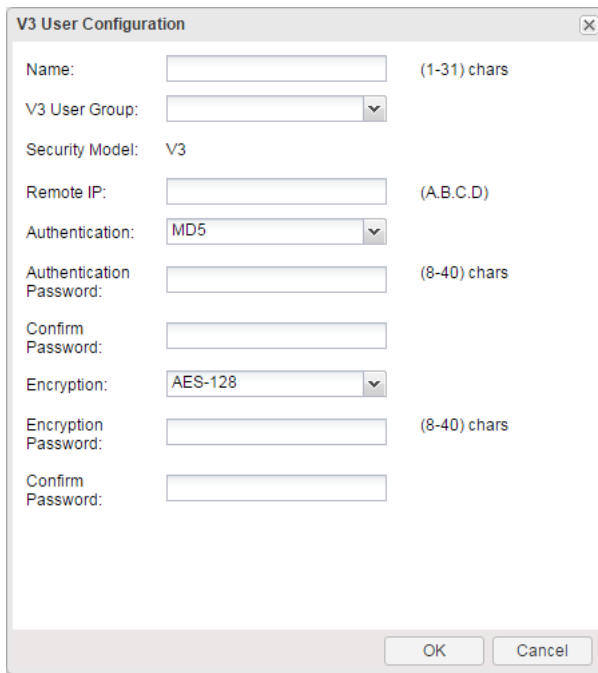
4. Click **OK**.

V3 User

If the selected SNMP version is V3, you need to create an SNMP V3 user group for the SNMP host and then add users to the user group.

To create a user for an existing V3 user group, take the following steps:

1. Select **System > SNMP > V3 User**.
2. Click **New**.
3. In the V3 User Configuration dialog box, configure these values.



The image shows a 'V3 User Configuration' dialog box with the following fields and options:

- Name:** Text input field, (1-31) chars
- V3 User Group:** Drop-down menu
- Security Model:** V3
- Remote IP:** Text input field, (A.B.C.D)
- Authentication:** Drop-down menu, currently set to MD5
- Authentication Password:** Text input field, (8-40) chars
- Confirm Password:** Text input field
- Encryption:** Drop-down menu, currently set to AES-128
- Encryption Password:** Text input field, (8-40) chars
- Confirm Password:** Text input field

At the bottom are 'OK' and 'Cancel' buttons.

Option	Description
Name	Type the SNMP V3 user name into the Name box.
V3 User Group	Select an existing user group for the user from the Group drop-down list.
Security Model	The Security model option displays the security model for the SNMP V3 user.
Remote IP	Type the IP address of the remote management host into the Remote IP box.
Authentication	Select the authentication protocol from the Authentication drop-down list. By default, this parameter is None, i.e., no authentication.
Authentication Password	Type the authentication password into the Authentication password box.
Confirm Password	Re-type the authentication password into the Confirm Password box to confirm.
Encryption	Select the encryption protocol from the Encryption drop-down list.
Encryption Password	Type the encryption password into the Encryption Password box.
Confirm Password	Re-type the encryption password into the Confirm Password box to confirm.

4. Click **OK**.

Upgrading System

The firmware upgrade wizard helps you:

- Upgrade system to a new version or roll back system to a previous version.
- Update the Signature Database.

Upgrading Firmware

To upgrade firmware, take the following steps:

1. Select **System > Upgrade Management > Upgrade Firmware**.
2. In the Upgrade Firmware tab box, configure the following.

Upgrade Firmware

Signature Database Update

Upgrade Firmware

Make sure you have backed up the configuration file before upgrading. [Backup Configuration File](#)

Please clear browser cache after upgrading and then access UI.

Current Version:

S06000-MX_MAIN-TF-01221 bin

Upload Firmware:

Browse

Backup Image:

S06000-MX_MAIN-TF-01220

☐ Reboot to make the new firmware take effect

Apply

Choose a Firmware for the next startup

Firmware downgrading may cause system malfunction. Please clear your system configuration before downgrading, and set up the system again after rebooting.

Please clear browser cache after firmware switch and then access UI.

Choose a Firmware for the next startup:

S06000-MX_MAIN-TF-01221

☐ Reboot to make the new firmware take effect

Apply

Upgrade Firmware	
Backup Con-figuration File	Make sure you have backed up the configuration file before upgrading. Click Backup Configuration File to backup the current fireware file and the system will automatically redirect the Configuration File Management page after the backup.
Current Version	The current firmware version.
Upload Firmware	Click Browse to select a firmware file from your local disk.
Backup Version	The backup firmware version.
Reboot	Select the Reboot to make the new firmware take effect check box and click Apply to reboot system and make the firmware take effect. If you click Apply without selecting the check box, the firmware will take effect after the next startup.
Choose a Firmware for the next startup	
Select the firm-ware that will take effect for the next startup.	Select the firmware that will take effect for the next startup.
Reboot	Select the Reboot to make the new firmware take effect check box and click Apply to reboot system and make the firmware take effect. If you click Apply without selecting the check box, the firmware will take effect after the next startup.

Updating Signature Database

To update signature database, take the following steps:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the Signature Database Update tab box, configure the following.

Chapter 15 System Management

494

Option	Description
Current Version	Show the current version number.
Remote Update	<p>Application signature database, URL signature database, Sandbox Whitelist Database, Antivirus signature database, IPS signature database or IP reputation database.</p> <ul style="list-style-type: none"> • Update Now: Click Update to update the signature database right now. • Auto Update: Select Enable Auto Update and specify the auto update time. Click Save to save your changes. • Configure Update Server: By default the system updates the signature database everyday automatically. You can change the update configuration as needed. Hillstone devices provide two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can customize the servers according to your need. In the pop-up Auto Update Settings dialog box, specify the server IP or domain name and Virtual Router. • Configure Proxy Server: When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update normally. Click Configure Proxy Server, then enter the IP addresses and ports of the main proxy server and the backup proxy server. <p>Mitigation rule database, Abnormal behavior mode database or Malware behavior mode database.</p> <ul style="list-style-type: none"> • Update Now: Click Update to update the signature database right now. • Auto Update: Select Enable Auto Update and specify the auto update time. Click Save to save your changes. • Server: By default the system updates the signature database everyday automatically. You can change the update configuration as needed. Devices provide two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can customize the servers according to your need. In the pop-up Auto Update Settings dialog box, specify the server IP or domain name and Virtual Router. • Server: Devices provide a default update servers: sec-cloud.hillstonenet.com.
Local Update	Click Browse and select the signature file in your local PC, and then click Upload .

License

Licenses are used to authorize the users' features, authorize the users' services, or extend the performance. If you do not buy and install the corresponding license, the features, services, and performance which is based on the license will not be used or cannot be achieved.

License classes and rules.

Platform License	Description	Valid Time
Platform Trial	Platform license is the basis of the other licenses operation. If the platform license is invalid, the other licenses are not effective. The device have been pre-installed platform trial license for 15 days in the factory.	You cannot modify the existing configuration when License expires. The system will restore to factory defaults when the device reboot.
Platform Base	You can install the platform base license after the device formal sale. The license provide basic firewall and VPN function.	System cannot upgrade the OS version when the license expires, but the system could still work normally.
Function License	Description	Valid Time
VSYS	Authorizing the available number of VSYS.	Permanent
SSL VPN	Authorizing the maximum number of SSL VPN access. Through installing multiple SSL VPN licenses, you can add the maximum number of SSL VPN access.	Permanent
iQoS	Enable QoS function.	System cannot upgrade the iQoS function and cannot provide the maintenance service when License expired.
WAP Traffic Distribution	Providing WAP traffic distribution.	Permanent
Sandbox License	Providing sandbox function and white list update, authorizing the number of suspicious files uploaded per day. Including 3 licenses: <ul style="list-style-type: none">Sandbox-300 license: 300 suspicious files are allowed to upload every day.Sandbox-500 license: 500 suspicious files are allowed to upload every day.Sandbox-1000 license: 1000 suspicious files are allowed to upload every day.	The valid time including 1 year, 2 years and 3 years. System cannot analyze the collected data and cannot update the white list when the license expires. The sandbox protection function can only be used according to the local database cache results. If you restart the device, the function cannot be used.
Service License	Description	Valid Time
AntiVirus	Providing antivirus function and antivirus signature database update.	System cannot update the antivirus signature database when the license expires, but the antivirus function could still be used normally
URL	Providing URL database and URL signature database update.	System cannot provide the search URL database online function when the license expires, but the user-

		defined URL and URL filtering function can be used normally.
IPS	Providing IPS function and IPS signature database update.	System cannot update the IPS signature database when the license expires, but the IPS function could still be used normally.
APP signature	APP signature license is issued with platform license, you do not need to apply alone. The valid time of license is same as platform license.	System cannot update the APP signature database when the license expires, but the included functions and rules could still be used normally.
Threat Prevention	A package of features, including AntiVirus, IPS, and corresponding signature database update.	System cannot update all signature databases when the license expires, but the included functions and rules could still be used normally.
PTF	Providing Perimeter Traffic Filtering function of predefined black list and IP reputation database update.	System cannot update the IP reputation database when the license expires.
StoneShield	A package of features, including Abnormal Behavior Detection, Advanced Threat Detection, and corresponding signature database update.	System cannot update all signature databases when the license expires, but the included functions and rules could still be used normally.
Antispam	Providing Anti-Spam function.	The Anti-Spam function cannot be used when the license expires.
Expansion and Enhancement License	Description	Valid Time
AEL	Advance the maximum value of concurrent sessions and performance.	Permanent

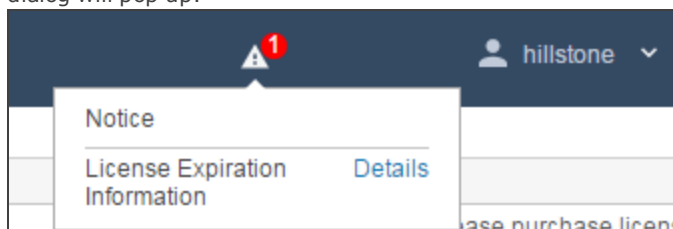
Viewing License List

Select **System > License** to enter the License List page. All licenses the system supports will be displayed in this page, including the authorized licenses and unauthorized licenses.

If there is license that is about to expire (the remaining valid period is within 30 days) or has expired:

- When you log into the device, the **License Expiration Information** dialog box will pop up, which prompts for licenses that are about to expire or have expired. Check the **Don't remind me again** checkbox so that the dialog box will never prompt again when you login. Click the **Update Now** button to jump to the License List page.
- The notification icon with the number of notifications is displayed in the upper-right corner. Hover your mouse over the icon, and click **Details** after the License Expiration Information, the **License Expiration Information**

dialog will pop up.



Applying for a License

Before you apply for a license, you have to generate a license request first.

1. Under License Request, input user information. All fields are required.

License Request	
Customer:	<input type="text"/> (1-127)chars
Address:	<input type="text"/> (1-256)chars
Zip Code:	<input type="text"/> (4-10)chars
Contact:	<input type="text"/> (1-31)chars
Telephone:	<input type="text"/> (3-20)chars
Email:	<input type="text"/> (1-256)chars
<input type="button" value="Generate"/> <input type="button" value="Clear"/>	

2. Click **Generate**, and then appears a bunch of code.
3. Send the code to your sales contact. The sales person will issue the license and send the code back to you.

Installing a License

After obtaining the license, you must install it to the device.

To install a license, take the following steps:

1. Select **System > License**.
2. Under License installation in the License page, configure options below.

Option	Description
Upload License File	Select Upload License File . Click Browse to select the license file, using the TXT format, and then click OK to upload it.
Manual Input	Select Manual Input . Type the license string into the box.
Online Install	Select the Online Install radio button and click the Online Install button, your purchased licenses will be automatically installed. It should be noted that the licenses must be in activated status in the Hillstone Online Registration Platform(http://onlinelic.hillstonenet.com/reqlicense). (To activate the license, you need to log into the platform using your user-name and password of the platform. The username is the same as your mailbox which was provided when placing an order. Hillstone will send the password by e-mail. Then activate the licenses that need to be installed. If you purchased the device from the Hillstone agent, please contact the agent to activate the licenses.)

3. Click **OK**.
4. Go to **System > Device Management**, and click the **Option** tab.
5. Click **Reboot**, and select **Yes** in the prompt.
6. System will reboot. When it starts again, installed license(s) will take effect.

Mail Server

By configuring the SMTP server in the Mail Server page, the system can send the log messages to the specified email address.

Creating a Mail Server

To create a mail server, take the following steps:

- 1. Select **System > Mail Server**.
- 2. In the SMTP Server Configuration page, configure these values.

Name:

(1-31) chars

Server:

Domain or IP

Virtual Router:

trust-vr

▼

Verification:

☒ Enable

Email:

(1-63) chars

Apply

Delete

Option	Description
Name	Type a name for the SMTP server into the box.
Server	Type Domain name or IP address for the SMTP server into the box.
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the SMTP server.
Verification	Select the Enable check box for SMTP verification to enable it if needed. Type the username and its password into the corresponding boxes.
Email	Type the email address that sends log messages.

- 3. Click **Apply**.

SMS Parameters

SMS Modem Devices

An external GSM modem device is required for sending SMS messages. First, you need to prepare a mobile phone SIM card and a GSM SMS Modem. Insert the SIM card into your modem and then, connect the modem and the firewall using a USB cable.

System will show the modem connection status: correctly connected, not exist or no signal.

Configuring SMS Parameters

You can define the maximum SMS message number in one hour or in one day. If the messages exceed the maximum number, system will not make the modem to send messages, but it will keep a log for this behavior.

Option	Description
Maximum messages per hour	Defines the maximum message number the modem can send in one hour.
Maximum messages per day	Defines the maximum messages number the modem can send in one day.

Testing SMS

To test if the message sending works, you can send a test text to a mobile.

To send a text message to a specified mobile number, take the following steps:

1. Select **System > SMS Parameters**.
2. Enter a mobile phone number in the text box.
3. Click **Send**. If the SMS modem is correctly configured and connected, the phone using that number will receive a text message; if it fails, an error message will indicate where the error is.

Connecting to HSM

Hillstone Security Management (HSM) is a centralized management platform to manage and control multiple Hillstone devices. Using WEB2.0 and RIA (Rich Internet Application) technology, HSM supports visualized interface to centrally manage policies, monitor devices, and generates reports.

Each firewall system has an HSM module inside it. When the firewall is configured with correct HSM parameters, it can connect to HSM and be managed by HSM.

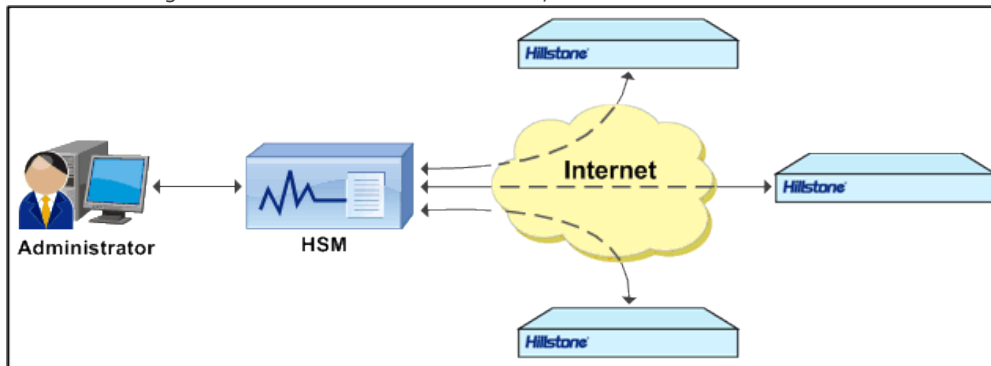


Note: For more information about HSM, please refer to HSM User Guide.

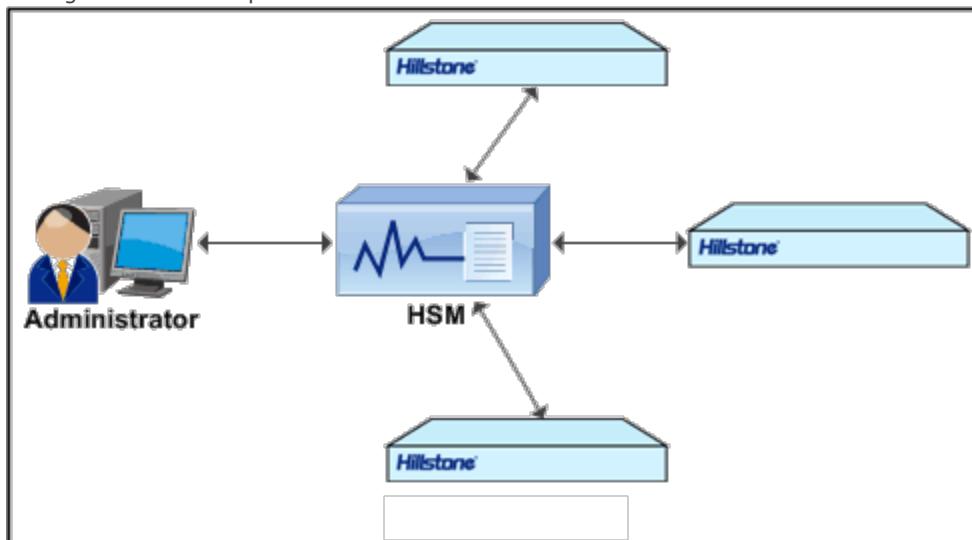
HSM Deployment Scenarios

HSM normally is deployed in one of the two scenarios: installed in public network or in private network:

- Installed in public network: HSM is remotely deployed and connected to managed devices via Internet. When the HSM and managed devices have a accessible route, the HSM can control the devices.



- Installed in private network: In this scenario, HSM and the managed devices are in the same subnet. HSM can manage devices in the private network.



Connecting to HSM

To configure HSM parameters in the firewall, take the following steps:

1. Select **System > HSM Agent**.
2. Select **Enable** of HSM Agent field to enable this feature.

HSM Agent Configuration

HSM Parameters

HSM Agent: ☒ Enable

Status: Disabled

Server IP/Domain:

Server Port: (1~65535), default:9091

Syslog Server

IP Address:

Port:

3. Input HSM server's IP address in the Sever IP/Domain text box. The address cannot be 0.0.0.0 or 255.255.255.255, or mutlicast address.
4. Enter the port number of HSM server.
5. Click **OK**.



Note: The Syslog Server part shows the HSM server's syslog server and its port.

Connecting to Hillstone CloudView

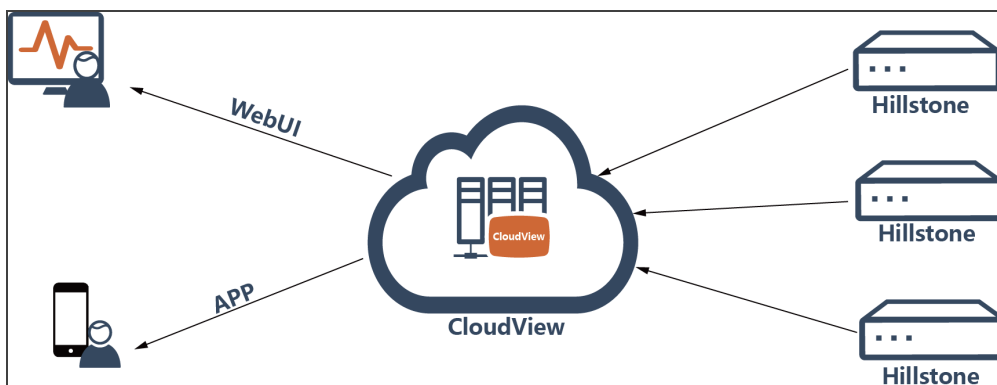
CloudView is a SaaS products of security area and a cloud security services platform in the mobile Internet era. CloudView deployed in the public cloud to provide users with online on-demand services. Users can get convenient, high quality and low cost value-added security services through the Internet and APP, and get a better security experience.

After the Hillstone device is properly configured to connect the CloudView , you can achieve the Hillstone device registration to the public cloud and the connection with the Cloud ·View, and then to achieve the Cloud ·View remote monitoring device.

CloudView Deployment Scenarios

The main deployment scenarios of CloudView are described as follows:

When Hillstone devices register to the public cloud, the device information, traffic data, threat event, and system logs are uploaded to the cloud, which provides a visual display. Users can through the Web or mobile phone APP monitor the device status information, reports, threat analysis, etc.





Note: About CloudView, see CloudView FAQs page.

Connecting to Hillstone CloudView

When using the CloudView, the device needs to connect to the CloudView server.

1. Select **System > Hillstone CloudView**.

The screenshot shows a configuration window titled "Hillstone CloudView". At the top, there is a checkbox labeled "Hillstone CloudView:" which is checked and labeled "Enable". Below this is a "Server" section containing three input fields: "Address:" with the value "cloud1.hillstonenet.com.cn" and a character count "(1-255) chars"; "User:" with the value "defaultuser" and a character count "(1-31) chars"; and "Password:" with masked characters "*****" and a character count "(4-31) chars". Below the input fields, it says "Server Status: Online". Underneath the "Server" section is an "Items" section with five checkboxes, all of which are checked: "Traffic Data", "Threat Event", "System Log", "URL Data", and "Session Data". At the bottom of the window, there is a checkbox labeled "Join The Hillstone cloud security program" which is unchecked. Below this checkbox are two buttons: "OK" and "Cancel".

2. Select the **Enable** check box of Hillstone CloudView.
3. Enter the URL of the CloudView server. The default configuration is cloud.hillstonenet.com.cn.
4. Enter the username of CloudView. Register the device to this user.
5. Enter the password of the user.
6. **Server Status** displays the CloudView status.
7. Select **Traffic Data** to upload the monitor data.
8. Select **Threat Event** to upload the threat events detected by the Hillstone device.
9. Select **System Log** to upload the event logs.
10. Select **URL Data** to upload the URL data.
11. Select **Session Data** to upload the session data.
12. Select whether to join the Hillstone cloud security program. This program will upload the threat prevention data to cloud intelligence server. The uploaded data will be used for internal research to reduce false positives and to achieve better protection of the equipment.
13. Click **OK**.

VSYS (Virtual System)

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

VSYS (Virtual System) is logically divides the physical firewall into several virtual firewalls. Each virtual firewall can work independently as a physical device with its own system resources, and it provides most firewall features. A VSYS is separated from other VSYS, and by default, they cannot directly communicate with each other.

VSYS has the following characteristics:

- Each VSYS has its own administrator;
- Each VSYS has an its own virtual router, zone, address book and service book;
- Each VSYS can have its own physical or logical interfaces;
- Each VSYS has its own security policies.



Note: The maximum VSYS number is determined by the platform capacity and license. You can expand VSYS maximum number by purchasing addition licenses.

VSYS Objects

This section describes VSYS objects, including root VSYS, non-root VSYS, administrator, VRouter, VSwitch, zone, and interface.

Root VSYS and Non-root VSYS

System contains only one root VSYS which cannot be deleted. You can create or delete non-root VSYSs after installing a VSYS license and rebooting the device. When creating or deleting non-root VSYSs, you must follow the rules listed below:

- When creating or deleting non-root VSYSs through CLI, you must be under the root VSYS configuration mode.
- Only the root VSYS administrators and root VSYS operators can create or delete non-root VSYS. For more information about administrator permissions, see ["Device Management" on Page 477](#).
- When creating a non-root VSYS, the following corresponding objects will be created simultaneously:
 - A non-root VSYS administrator named admin. The password is vsys_name-admin.
 - A VRouter named vsys_name-vr.
 - A L3 zone named vsys_name-trust.

For example, when creating the non-root VSYS named vsys1, the following objects will be created:

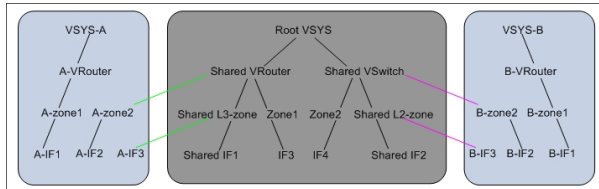
- The RXW administrator named admin with the password vsys1-admin.
- The default VRouter named vsys1-vr.
- The L3 zone named vsys1-trust and it is bound to vsys1-vr automatically.
- When deleting a non-root VSYS, all the objects and logs in the VSYS will be deleted simultaneously.
- The root VSYS contains a default VSwitch named VSwitch1, but there is no default VSwitch in a newly created non-root VSYS. Therefore, before creating I2 zones in a non-root VSYS, a VSwitch must be created. The first VSwitch created in a non-root VSYS will be considered as the default VSwitch, and the I2 zone created in the non-root VSYS will be bound to the default VSwitch automatically.

VRouter, VSwitch, Zone and Interface

VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared object. The dedicated object and shared object have the following characters:

- **Dedicated object:** A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- **Shared object:** A shared object can be shared by multiple VSYSs. A shared object can only belong to the root VSYS and can only be configured in the root VSYS. A non-root VSYS can reference the shared object, but cannot configure them. The name of the shared object must be unique in the whole system.

The figure below shows the reference relationship among dedicated and shared VRouter, VSwitch, zone, and interface.



As shown in the figure above, there are three VSYSs in StoneOS: Root VSYS, VSYS-A, and VSYS B.

Root VSYS contains shared objects (including Shared VRouter, Shared VSwitch, Shared L3-zone, Shared L2-zone, Shared IF1, and Shared IF2) and dedicated objects.

VSYS-A and VSYS-B only contain dedicated objects. The dedicated objects VSYS-A and VSYS-B can reference the shared objects in Root VSYS. For example, A-zone2 in VSYS-A is bound to the shared object Shared VRouter in Root VSYS, and B-IF3 in VSYS-B is bound to the shared object Shared L2-zone in Root VSYS.

Shared VRouter

A shared VRouter contains the shared and dedicated L3 zones of the root VSYS. Bind a L3 zone to a shared VRouter and configure this L3 zone to have the shared property. Then this zone becomes a shared zone.

Shared VSwitch

A shared VSwitch contains the shared and dedicated L2 zones of the root VSYS. Bind a L2 zone to a shared VSwitch and configure this L2 zone to have the shared property. Then this zone becomes a shared zone.

Shared Zone

The shared zones consist of L2 shared zones and L3 shared zones. After binding the L2 zone with the shared property to a shared VSwitch, it becomes a shared L2 zone; after binding the L3 zone with shared property to a shared VRouter, it becomes a shared L3 zone. A shared zone can contain interfaces in both root VSYS and non-root VSYS. All function zones cannot be shared.

Shared Interface

After binding an interface in the root VSYS to a shared zone, it becomes a shared interface automatically.

Interface Configuration

Only RXW administrator in the root VSYS can create or delete interfaces. Configurations to an interface and its sub-interfaces must be performed in the same VSYS.



Note: Only administrator has the authority to delete or create interfaces. If you are about to delete an interface and its-subinterfaces, you have to do it under the same VSYS.

Creating Non-root VSYS

To create a new non-root VSYS, take the following steps:

1. Select **System > VSYS > VSYS**.
2. Click **New** to add a non-root VSYS.
3. In the prompt, configure these values.

Option	Description
Name	Enter a name for the non-root VSYS.
Interface Binding	<p>Select a physical or a logical interface. In VSYS, a physical interface can have its sub-interfaces, but logical interfaces cannot.</p> <ul style="list-style-type: none"> • Physically Import: Select the interface you want, and click Physically Import to add it to the right pane. • Logically Allocate: Select the interface you want, and click Logically Allocate to add it to the right pane. • Release: Select the added interface(s), and click Release to delete it.
Quota	Select an existing quota.

4. Click **OK** to save configuration. The new VSYS will be seen in the VSYS list.

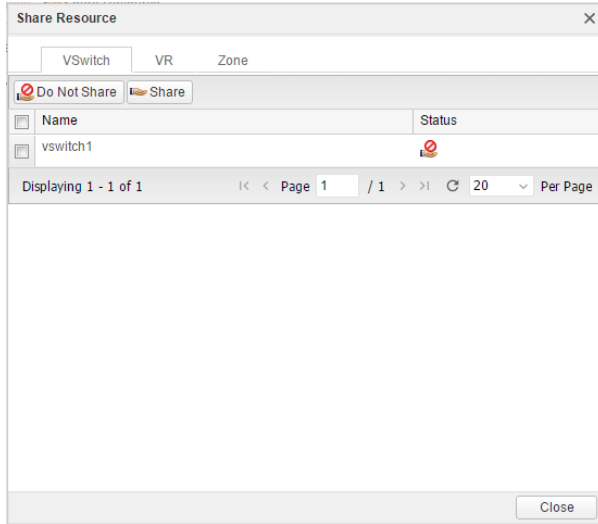
Configuring Dedicated and Shared Objects for Non-root VSYS

VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared object. The dedicated object and shared object have the following characters:

- **Dedicated object:** A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- **Shared object:** A shared object can be shared by multiple VSYSs. A shared object can only belong to the root VSYS and can only be configured in the root VSYS. A non-root VSYS can reference the shared object, but cannot configure them. The name of the shared object must be unique in the whole system.

To configure VSYS shared object, take the following steps:

1. Select **System > VSYS > VSYS**.
2. Click **Share Resource**.
3. **In the prompt, configure these values for VSwitch, VRouter and Zone.**



Option	Description
VSwitch	In the VSwitch tab, select a Vswitch and click Share to set it as a shared object; to make a VSwitch as a dedicated object, click Do Not Share .
VRouter	In the VRouter tab, select a Vswitch and click Share to set it as a shared object; to make a VRouter as a dedicated object, click Do Not Share .
Zone	In the Zone tab, select a Zone and click Share to set it as a shared object; to make a Zone as a dedicated object, click Do Not Share .

4. Click **Close** to exit.

Configuring VSYS Quota

VSYSs work independently in functions but share system resources including concurrent sessions, zone number, policy rule number, SNAT rule number, DNAT rule number, session limit rules number, memory buffer, URL resources and IPS resources. You can specify the reserved quota and maximum quota for each type of system resource in a VSYS by creating a VSYS profile. Reserved quota refers to the resource number reserved for the VSYS; maximum quota refers to the maximum resource number available to the VSYS. The root administrator have the permission to create VSYS quota. The total for each resource of all VSYSs cannot exceed the system capacity.

To define a quota for VSYS, take the following steps:

1. Select **System > VSYS > Quota**.
2. Click **New**.
3. **In the prompt, configure these values.**

Quota

Basic Configuration | System Resources | Protection | Log Configuration

Name: (1-31)chars

CPU

Limit: 550 (10-550)HSCS
*HSCS: Refers to the processing ability consumed on 1Mbps small packets

Reserve: 56 (56-550)

Alarm Threshold: When reaching 0 % of the limit, the alarm logs will be recorded. (Integers between 50 and 99. 0 means no alarm)

OK Cancel

Option	Description
Basic Configuration	
Name	Enter a name for the new quota.
CPU	<p>Specify values for parameters of CPU.</p> <ul style="list-style-type: none"> Limit: Specifies the maximum performance limit for processing 1 Mbps packets. Reserve: A dedicated reserved value for CPU in this VSYS. Alarm Threshold: Specifies a percentage value for alarms. When the CPU usage reaches this value, the system will generate alarm logs.
System Resources	
System Resources	<p>Specify the maximum quota and reserved quota of system resources.</p> <ul style="list-style-type: none"> Session number: Specifies the maximum and reserved number for sessions in the VSYS. Zones: Specifies the maximum and reserved number for zones in the VSYS. Policy rules: Specifies the maximum and reserved number for policy rules in the VSYS. SNAT rules: Specifies the maximum and reserved number for SNAT rules in the VSYS. DNAT rule: Specifies the maximum and reserved number for SNAT rules in the VSYS. Stat-set (session): Specifies the maximum and reserved number for sessions of a static set in the VSYS. Stat-set (other): Specifies the maximum and reserved number for other items than sessions of a static set in the VSYS. IPsec: Specifies the maximum and reserved number for IPsec tunnels in the VSYS. Session Limit Rules Number: Specifies the maximum and reserved number for session limit rules in the VSYS. Key Categories: Specifies the maximum and reserved number for keyword categories in the VSYS. Regular Keys: Specifies the maximum and reserved number for regular expression keywords in a URL category in the VSYS. Keys: Specifies the maximum and reserved number for simple

Option	Description
Basic Configuration	
	keywords in a URL category in the VSYS.
Protection	
URL Resources	<p>Specify the maximum quota and reserved quota of URL resources.</p> <ul style="list-style-type: none"> • URL: Select the Enable check box to enable the URL filter function. • URL Profiles: Specifies the maximum and reserved number for URL filter profiles in a VSYS. • URL Categories: Specifies the maximum and reserved number for user-defined URL categories in a VSYS. • URLs: Specifies the maximum and reserved number for URLs in a VSYS.
IPS Resources	<p>Specify the maximum quota and reserved quota of IPS resources.</p> <ul style="list-style-type: none"> • IPS: Select the Enable check box to enable the IPS function. • IPS Profiles: Specifies the maximum and reserved number for IPS profiles in a VSYS. You can create one IPS Profile at most in non-root VSYS, i.e., the range of maximum quota varies from 0 to 1. The default value of maximum quota and reserved quota is 0, which means only predefined IPS Profiles can be used in non-root VSYS.
Log Configuration	
Log Configuration	<p>Specify the maximum quota and reserved quota of memory buffer for each type of log in a VSYS. The reserved quota should not exceed the maximum quota. If the logs' capacity in a VSYS exceeds its maximum quota, the new logs will override the earliest logs in the buffer.</p> <ul style="list-style-type: none"> • Config Logs: Specify the maximum and reserved value of buffer for configuration logs in a VSYS. • Event Logs: Specify the maximum and reserved value of buffer for event logs in a VSYS. • Network Logs: Specify the maximum and reserved value of buffer for network logs in a VSYS. • Threat Logs: Specify the maximum and reserved value of buffer for threat logs in a VSYS. • Session Logs: Specify the maximum and reserved value of buffer for session logs in a VSYS. • NAT Logs: Specify the maximum and reserved value of buffer for NAT logs in a VSYS. • Websurf Logs: Specify the maximum and reserved value of buffer for websurf logs in a VSYS.

4. Click **OK** to save settings. The new VSYS quota will be shown in the list.

**Note:**

- Up to 128 VSYS quotas are supported.
- The default VSYS profile of the root VSYS named root-vsys-profile and the default VSYS profile of non-root VSYS named default-vsys-profile cannot be edited or deleted.
- Before deleting a VSYS profile, you must delete all the VSYSs referencing the VSYS profile.
- The maximum quota varies from one platform to another. The reserved quota cannot exceed maximum quota.


Entering the VSYS

After typing the management IP in a browser, you should type the username and password in the login page. For example, the management IP of root VSYS is 10.90.89.1, after typing the username (hillstone) and password (hillstone), you can enter the root VSYS. After creating the non-root VSYS (vsys1), you should type the name management IP 10.90.89.1, type the non-root administrator username (vsys1\admin) and password (vsys1-admin), and then you can enter the non-root VSYS directly. For the detailed information of administrator configuration, see "[Device Management](#)" on [Page 477](#).

Besides, the root VSYS administrator can enter the non-root VSYS from root VSYS. The administrator in the root VSYS can configure the functions of the non-root VSYS after entering it. To enter a non-root VSYS, take the following steps:

1. Select **System > VSYS > VSYS** to enter the VSYS page.
2. In the VSYS list, click the name of non-root VSYS, and enter the non-root VSYS.

+ New Edit Delete Share Resource									
	Name	Interface	Quota	CPU(HSCS)			Concurrent sessions		
				Current value	Limit	Reserve	Current value	Limit	Reserve
<input type="checkbox"/>	2		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	4		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	5		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	6		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	7		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	8		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	9		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	11		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	12		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	13		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	14		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	15		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	16		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	17		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	18		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	19		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	20		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	root	twinm_link_vif...	root-vsys-profile	0	250	0	20	637500	0
<input type="checkbox"/>	test		default-vsys-pr...	0	250	0	0	637500	0
<input type="checkbox"/>	vsys1	ethernet0/1	default-vsys-pr...	0	250	0	0	637500	0

3. Return to the root VSYS, click  in the right top corner of the page, and click **Return root Vsys** in the pop-up dialog box.

Note: If you enter the non-root VSYS directly, you cannot back to the root VSYS.