HIRSCHMANN IT

A BELDEN BRAND

User Manual

Web UI

RAVEN5000 Firewall User Manual

Web UI
Release 1.0 04/2020

Technical Support
https://www.belden.com.cn

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Belden. According to the best of the company's knowledge. Belden reserves the right to change the contents of this document without prior notice. Belden can give no guarantee in respect of the correctness or accuracy of the information in this document.

Belden can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.
You can get the latest version of this manual on the Internet at the Hirschmann IT product site (https://hirschmann-it.support.belden.com).

Safety agreement

Safety location

By default, device should be placed in certain location that is safe, stable and reliable; all physical operators should be authorized; the operation CLI scripts should be properly kept, updated and reviewed.

Safety channel

Hirschmann IT devices support multiple managing methods, including Telnet, SSH, HTTP, HTTPS and so forth. All un-encrypted management protocols are not recommended. We highly recommend that our user only use SSH and HTTPs as the way to operate the devices, in order to ensure all management traffic is encrypted.

Safety storage

The login credentials, device configuration and status data should be kept in an appropriate place and be updated regularly and this information can only be accessed and managed by authorized people.

About This Document

This document describes the functions and features of RAVEN5000 firewalls, and provides guidance on how to configure and use the firewalls. This document is divided into 11 parts.

Part 1 Management Method

Part 1 includes chapter 1 and describes how to manage RAVEN5000 firewalls using a web browser.

Part 2 System Information

Part 2 includes chapters 2 to 11 and describes how to use the functions of RAVEN5000 firewalls, such as system status monitoring, historical statistics, and traffic monitoring.

Part 3 Network Configuration

Part 31 includes chapters 12 to 31 and describes how to configure the network-related functions of RAVEN5000 firewalls. It describes virtual local area network (VLAN), link aggregation, IP address, static route, policy-based routing (PBR), dynamic routing, static Address Resolution Protocol (ARP), network address translation (NAT), protocol management, and network debugging.

Part 4 Security Features

Part 4 includes chapters 32 to 52 and describes how to configure the security-related policies of RAVEN5000 firewalls, including the security policy, anti-ARP and anti-denial of service (DoS) policy, traffic control policy, application policy, and session control policy.

Part 5 Template and Object

Part 5 includes chapters 53 to 62. Templates and objects are used to simplify firewall configuration. After an object is created, it can be used by multiple functions. Part 5 describes address object, time object, service object, Internet service provider (ISP) address object, and health check module.

Part 6 System Management

Part 31 includes chapters 63 to 71 and describes how to configure the security-related system features of RAVEN5000 firewalls. It describes basic firewall configuration, time configuration, configuration file management, operating system upgrade management, administrators, license authorization, high reliability, Virtual Router Redundancy Protocol (VRRP), log management, and Simple Network Management Protocol (SNMP).

Contents

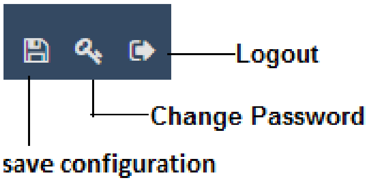
1 Web-based Management

1.1 Overview

You can configure and manage RAVEN5000 firewalls using a PC's web browser over HTTP or HTTPS. Before performing web-based management, configure RAVEN5000 firewalls to enable HTTP or HTTPS management from a specified interface.

The recommended browsers include Internet Explorer 10.0 or later, Mozilla 50.0 or later, and Chrome 54.0. The optimal resolution is 1600x900.

1.2 Toolbar

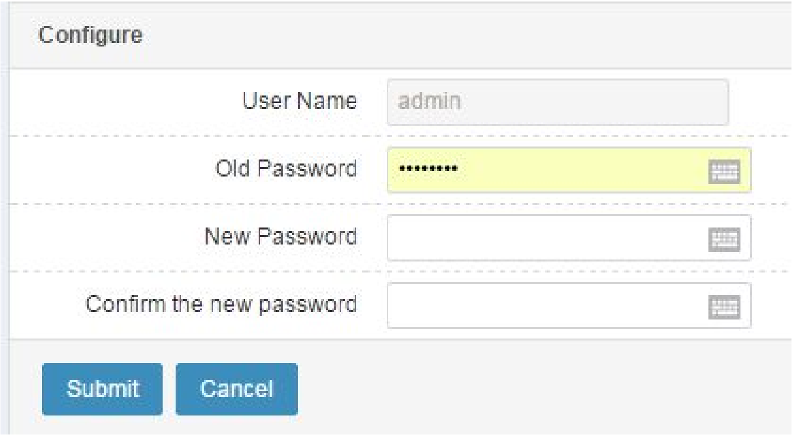


1.2.1 Saving Configuration

Click **Save** to save configuration changes permanently. By default, configuration changes are not saved permanently. If you do not click the **Save** button after you change configurations, the firewall will lose its last configurations upon the next startup.

1.2.2 Changing Password

Click the **Change Password** button to change your password on a new page.



Configure

User Name	admin
Old Password	••••••••
New Password	
Confirm the new password	

Parameter description:

User name: Enter your administrator name.

Old password: Enter your old administrator password.

New password: Enter a new password.

Confirm new password: Enter the new password again.

1.2.3 Logout

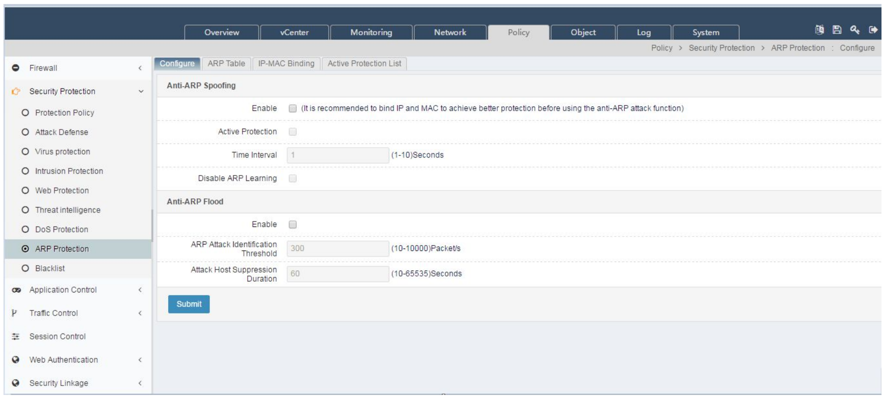
Click the **Logout** button to log out. The **Login** page appears.

1.3 Web-based Management

The web-based management page consists of the top level-1 menus, toolbar, left level-2 and level 3 menus, level-4 menus, and main content area.

Except the **Home** menu, each level-1 menu contains one or more submenus and may have level-4 submenus at most.

For example, after you click level-1 menu **Policy**, its level-2 submenus are displayed on the left, including **Firewall**, **Security**, **Application control**, **Traffic control**, **Session control**, and **Web authentication**. By default, the first level-2 menu **Firewall** expands with its first level-3 submenu **Policy** selected. If a level-3 menu (for example, **Security** > **ARP protection**) has level-4 submenus, the level-4 submenus are displayed as tabs above the main content area on the right. The first level-4 submenu **Configuration** is selected and its content is displayed in the main content area.



Anti-ARP Spoofing

Enable □ (It is recommended to bind IP and MAC to achieve better protection before using the anti-ARP attack function)

Active Protection □

Time Interval 1 (1-10)Seconds

Disable ARP Learning □

Anti-ARP Flood

Enable □

ARP Attack Identification Threshold 300 (10-10000)Packet/s

Attack Host Suppression Duration 60 (10-65535)Seconds

1.3.1 Menu

The menus provide the main configuration options of RAVEN5000 firewalls.

Home: Shows the common service information trend charts, current system running status, high-level log information, system information, and main function configuration overview.

vCenter: Short for visual center, which shows the network usage trends of the system and functions, and the detected attack events flagged as threats.

Monitor: Monitors the firewall's running status, traffic, real-time session status, and historical trend in a comprehensive manner. The monitored items include the system, interfaces, threats, users, applications, URLs, and sessions.

Network: Provides network configuration, including interfaces, security zones, ARP, Dynamic Host Configuration Protocol (DHCP), routing, NAT, virtual private networks (VPNs), system parameters, domain name server (DNS) proxy, DNS service, and network debugging.

Policy: Provides policy configuration, including firewalls, security, application control, traffic control, session control, and web authentication.

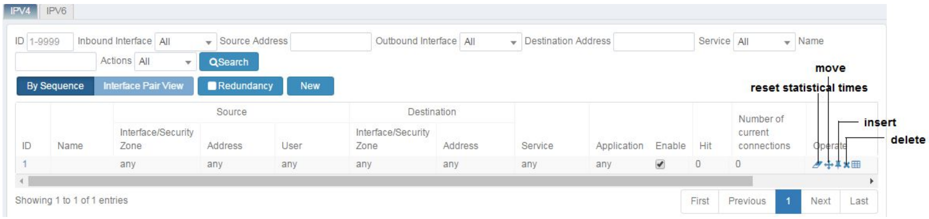
Object: Provides general system configuration items which can be referenced by other modules, including object management, health check, and certificates issued by certificate agencies (CAs).

Log: Shows function logs and provides log configuration, including system logs, audit logs, security logs, VPN logs, and log management.

System: Provides system configuration, including settings, administrators, version management, license management, high availability, VRRP, and SNMP.

1.3.2 List

Many management configuration pages are in the form of lists, such as the administrator list, interface list, and firewall policy list. The following figure shows a list of RAVEN5000 firewalls.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name
Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
1		any	any	any	any	any	any	any	☑	0	0	

Showing 1 to 1 of 1 entries

A list shows the information about each entry. Typically, the right-most column of a list contains the icons and buttons used to perform operations such as **reset statistical times**, **move**, **insert**, and **delete**. Click the name or ID column to edit the entry. Such columns are typically in blue. For example, the **#** column is the ID column.

Click **New** above the list to add an entry. The **New** and **Edit** pages are basically the same.

1.3.3 Icon

The icons on web pages help you with configuration and management. When the cursor hovers over an icon, a message appears to display the meaning of the icon. The common icons are listed as follows:

Icon	Name	Description
⊞ ▷	Expand	Expands the current entry.
⇅	Move	Moves the current entry to a specified position.
▤	Insert	Inserts a new entry in front of the current entry.
✎	Rename	Renames the current entry.
☒ ✖	Delete	Deletes an entry.

1.4 Default Configurations

RAVEN5000 firewalls provide default configurations to allow you to manage and configure the firewalls using a web browser without performing additional configuration.

1.4.1 Management Interface Default Configurations

The default address of the management (MGT) interface is 192.168.1.250/24. You can perform ping and HTTPS-based operations through this interface. Note: For a firewall without the management interface, the default address is configured for the first service interface, which is ge0/0 typically.

1.4.2 Default Administrator

The default administrator is **admin**, and the password is **Raven.private**. This account allows you to log in to the firewall from any address and implement all the functions of the firewall.

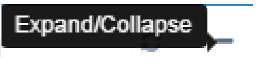
The default auditor is **audit**, and the password is **Raven.audit**. This account allows you to audit the log system.

The default user administrator is **useradmin**, and the password is **Raven.public**. This account allows you to configure system administrators.

2 Home Page

2.1 Home Page

After you log in to a firewall from a web browser, the home page appears by default to display the firewall's overall running status at the current moment, including the top 10 user traffic ranking, top 10 application traffic ranking, uplink and downlink traffic trend, network connections trend, high-level logs, physical interface information table, basic firewall information, and common configuration overview.

The and  icons in the upper-right corner of each pane are used to refresh and show/hide the pane.

You can check the interface information, version, CPU usage, and memory usage on the home page to determine whether the firewall is properly loaded.

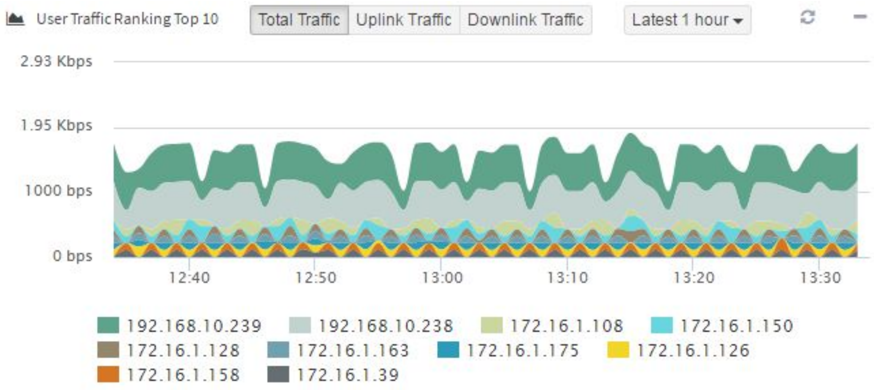
1. Check that the interface information is consistent with the number and types of physical interfaces. If not, check the serial number or hardware.

2. Check that the version is consistent with the released version or the provided interim version. If not, check the upgrade package.

3. Check that the CPU usage and memory usage are displayed properly.

4. Check that the hardware information is correct. If **N/A** is displayed, no disks are configured for the firewall. If disks are configured but not properly loaded, contact the manufacturer.

2.1.1 Top 10 User Traffic Ranking



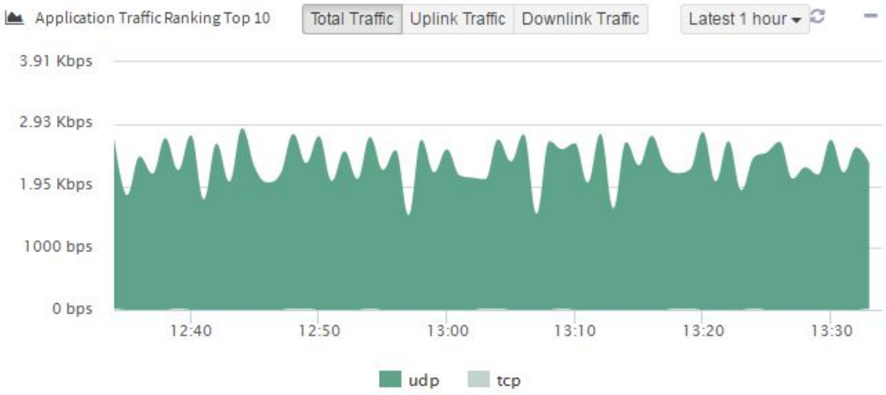
This pane shows the statistics on changes in the traffic rates of the top 10 users (IP addresses) ranked by traffic within a specified time range.

By default, the statistical period is the past 1 hour, and users are ranked by total traffic.

Users can also be ranked by uplink and downlink traffic.

Other statistical periods include past 1 day, past 7 days, and past 30 days.

2.1.2 Top 10 Application Traffic Ranking



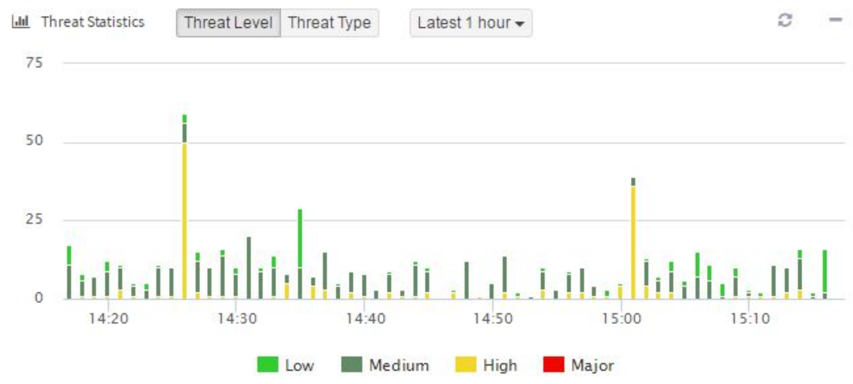
This pane shows the statistics on changes in the traffic rates of the top 10 applications ranked by traffic within a specified time range.

By default, the statistical period is the past 1 hour, and applications are ranked by total traffic.

Applications can also be ranked by uplink and downlink traffic.

Other statistical periods include past 1 day, past 7 days, and past 30 days.

2.1.3 Threat Statistics

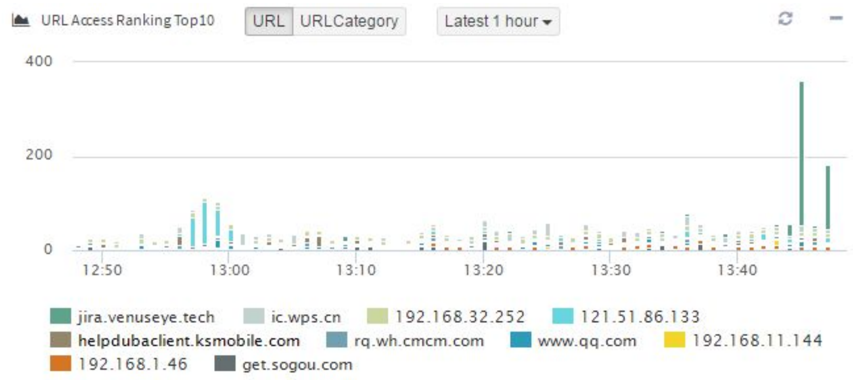


This pane shows the statistics on changes in the threat severity and threat type within a specified time range.

By default, the statistical period is the past 1 hour.

Other statistical periods include past 1 day, past 7 days, and past 30 days.

2.1.4 Top 10 Accessed URL Ranking

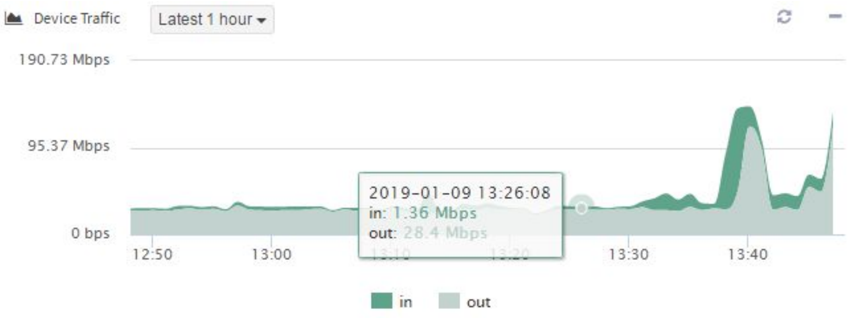


This pane shows the statistics on changes in access traffic, which are sorted by URL or URL category.

By default, the statistical period is the past 1 hour.

Other statistical periods include past 1 day, past 7 days, and past 30 days.

2.1.5 Firewall Traffic

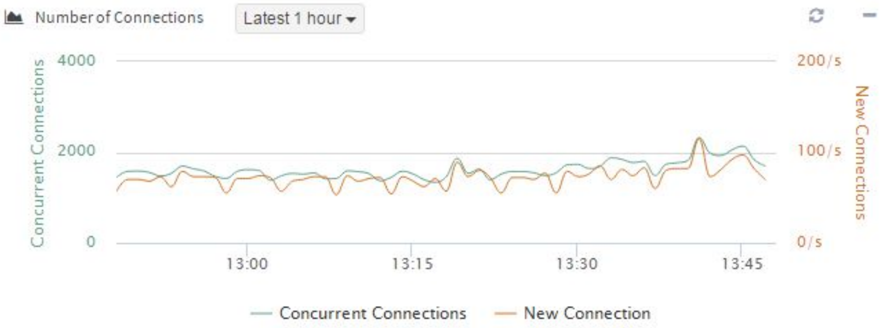


This pane shows the statistics on changes in the incoming and outgoing traffic rates of the firewall within a specified time range.

By default, the statistical period is the past 1 hour.

Other statistical periods include past 1 day, past 7 days, and past 30 days.

2.1.6 Connections

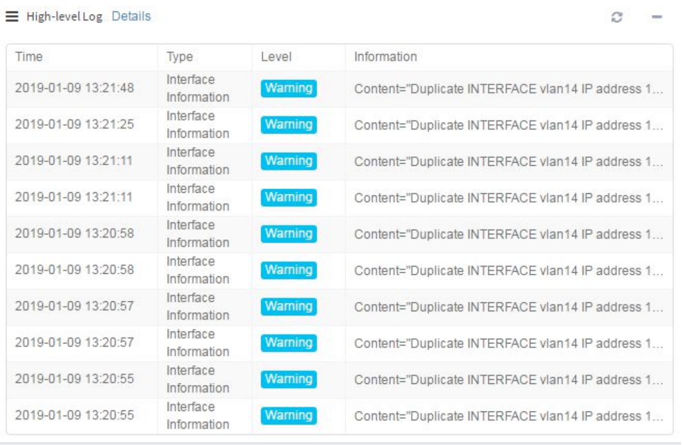


This pane shows the statistics on changes in the average numbers of concurrent connections and new connections within a specified time range.

By default, the statistical period is the past 1 hour.

Other statistical periods include past 1 day, past 7 days, and past 30 days.

2.1.7 High-level Logs



High-level Log Details

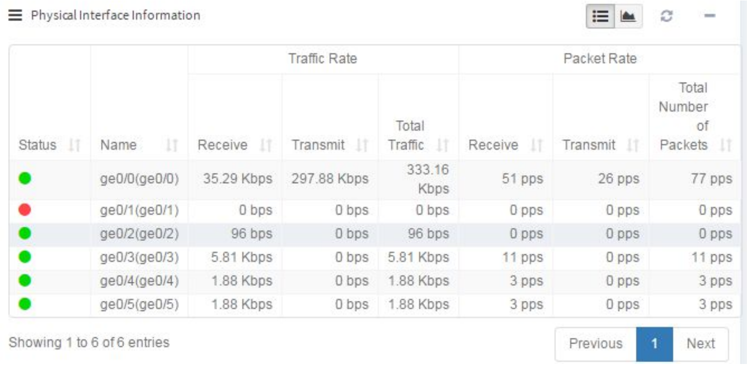
Time	Type	Level	Information
2019-01-09 13:21:48	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:21:25	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:21:11	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:21:11	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:20:58	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:20:58	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:20:57	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:20:57	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:20:55	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...
2019-01-09 13:20:55	Interface Information	Warning	Content="Duplicate INTERFACE vlan14 IP address 1...

You can view the latest high-level logs.

The home page lists the high-level logs of all types.

Click **Details** to go to the **Log** menu, which shows the details about logs of all types.

2.1.8 Physical Interface Information

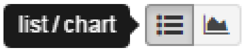


Physical Interface Information

		Traffic Rate			Packet Rate		
Status	Name	Receive	Transmit	Total Traffic	Receive	Transmit	Total Number of Packets
🟢	ge0/0(ge0/0)	35.29 Kbps	297.88 Kbps	333.16 Kbps	51 pps	26 pps	77 pps
🔴	ge0/1(ge0/1)	0 bps	0 bps	0 bps	0 pps	0 pps	0 pps
🟢	ge0/2(ge0/2)	96 bps	0 bps	96 bps	0 pps	0 pps	0 pps
🟢	ge0/3(ge0/3)	5.81 Kbps	0 bps	5.81 Kbps	11 pps	0 pps	11 pps
🟢	ge0/4(ge0/4)	1.88 Kbps	0 bps	1.88 Kbps	3 pps	0 pps	3 pps
🟢	ge0/5(ge0/5)	1.88 Kbps	0 bps	1.88 Kbps	3 pps	0 pps	3 pps

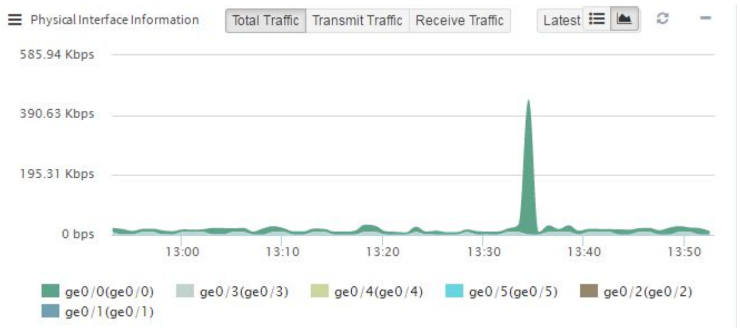
Showing 1 to 6 of 6 entries

You can view the real-time information and historical trend of the firewall's physical interfaces. By default, the real-time information is displayed.



Click the **Table** and **Chart** buttons in the upper-right corner to change the display form, as shown in the following figure.

Then the physical interface information table changes to a line chart.



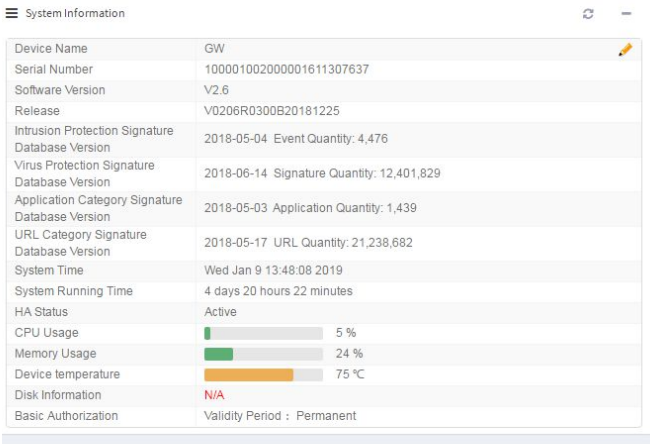
This pane shows the statistics on changes in the traffic rates of physical interfaces within a specified time range.

By default, the statistical period is the past 1 hour, and physical interfaces are ranked by total traffic.

Physical interfaces can also be ranked by sent and received traffic.

Other statistical periods include past 1 day, past 7 days, and past 30 days.

2.1.9 System Information



Device Name	GW
Serial Number	100001002000001611307637
Software Version	V2.6
Release	V0206R0300B20181225
Intrusion Protection Signature Database Version	2018-05-04 Event Quantity: 4,476
Virus Protection Signature Database Version	2018-06-14 Signature Quantity: 12,401,829
Application Category Signature Database Version	2018-05-03 Application Quantity: 1,439
URL Category Signature Database Version	2018-05-17 URL Quantity: 21,238,682
System Time	Wed Jan 9 13:48:08 2019
System Running Time	4 days 20 hours 22 minutes
HA Status	Active
CPU Usage	5 %
Memory Usage	24 %
Device temperature	75 ℃
Disk Information	N/A
Basic Authorization	Validity Period： Permanent

You can view the basic firewall information.

Host name: Configured by the administrator to distinguish firewalls.

Serial number: Default and unique identifier of a firewall.

Software version: Version of the system software running on the firewall.

Release: Code used for the after-sales service.

Intrusion prevention feature database version: Last update time of the intrusion prevention feature database and the number of features in the database.

Antivirus database version: Last update time of the antivirus database and the number of features in the database.

Application category feature database version: Last update time of the application category feature database and the number of features in the database.

URL category feature database version: Last update time of the URL category feature database and the number of features in the database.

System time: Current system time.

System runtime: Duration for which the system has been running since last startup.

HA status: HA status of the firewall, including the standalone state, active state, standby state, active A state, and active N state.

CPU usage: Usage of processing resources by the firewall.

Memory usage: Usage of memory resources by the firewall.

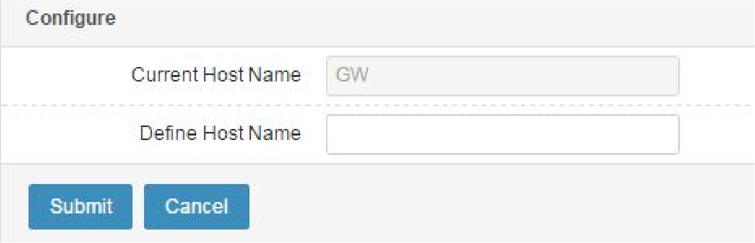
Disk information: Disk capacity of the firewall.

Basic authorization: Basic authorization period of the firewall.

Changing the Host Name

Change the host name to distinguish firewalls.

Choose **Home** > **System information**, and click ✎ next to **Host name**.



Configure

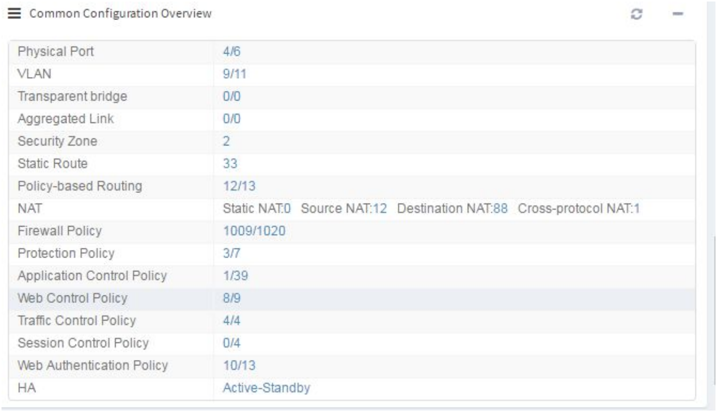
Current Host Name	GW
Define Host Name	

Current host name: Current host name of the firewall.

Define host name: New host name of the firewall.

Enter a new host name in **Define host name**, and click **Submit**.

2.1.10 Common Configuration Overview



Common Configuration Overview

Physical Port	4/6
VLAN	9/11
Transparent bridge	0/0
Aggregated Link	0/0
Security Zone	2
Static Route	33
Policy-based Routing	12/13
NAT	Static NAT:0 Source NAT:12 Destination NAT:88 Cross-protocol NAT:1
Firewall Policy	1009/1020
Protection Policy	3/7
Application Control Policy	1/39
Web Control Policy	8/9
Traffic Control Policy	4/4
Session Control Policy	0/4
Web Authentication Policy	10/13
HA	Active-Standby

You can view the basic configurations of common functions, including:

Physical interface, VLAN, link aggregation, security zone, static route, PBR, NAT, firewall policy, anti-attack policy, application control policy, web control policy, traffic control policy, session control policy, web authentication policy, and HA.

Click the numbers next to a configuration item to go to the corresponding configuration page.

3 vCenter

3.1 Overview

vCenter allows you to monitor a firewall's traffic and captured threats. You can set the monitoring period to past 1 hour, past 1 day, past 7 days, and past 30 days.

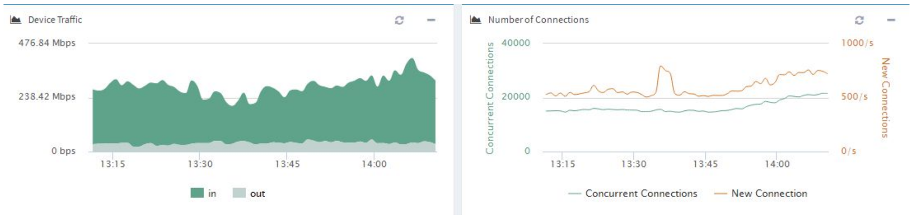
3.2 Traffic

Procedure:

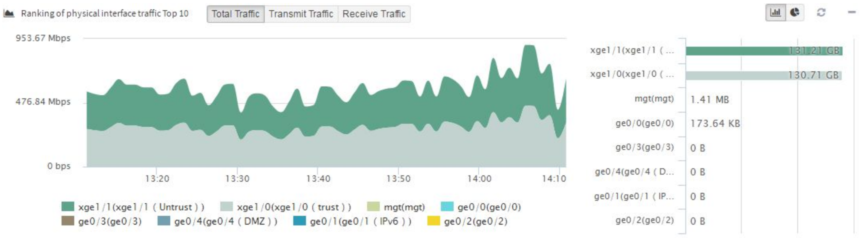
Choose **vCenter** > **Traffic** to display the traffic statistics during the past 1 hour, past 1 day, past 7 days, and past 30 days.

The statistical items include the firewall traffic, connections, top 10 physical interfaces ranked by traffic, top 10 users ranked by traffic, top 10 application categories ranked by traffic, top 10 applications ranked by traffic, top 10 URL categories ranked by access volume, and top 10 URLs ranked by access volume.

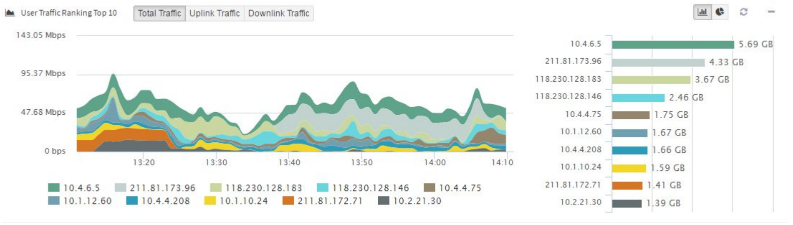
Statistics on the firewall traffic and connections:



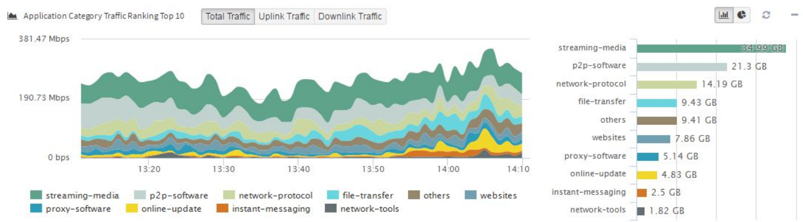
Top 10 physical interfaces ranked by traffic:



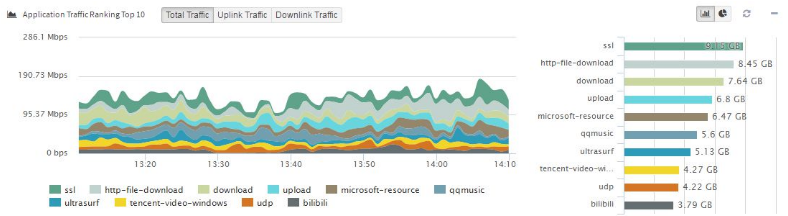
Top 10 users ranked by traffic:



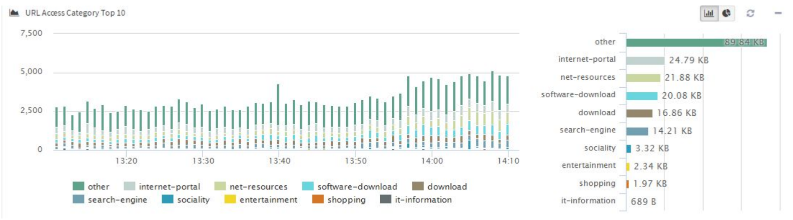
Top 10 application categories ranked by traffic:



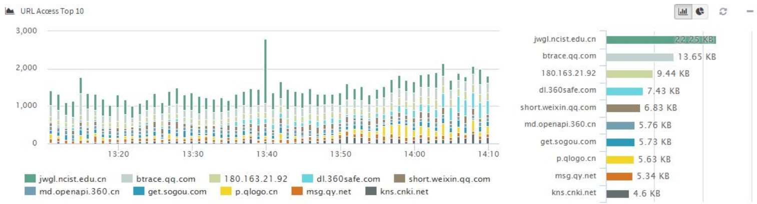
Top 10 applications ranked by traffic:



Top 10 URL categories ranked by access volume:



Top 10 URLs ranked by access volume:



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Export this page to PDF** to export the content of the entire page to a PDF file. The file contains all the statistics displayed on the page. If a statistical item is hidden on the page, it is also hidden in the file.

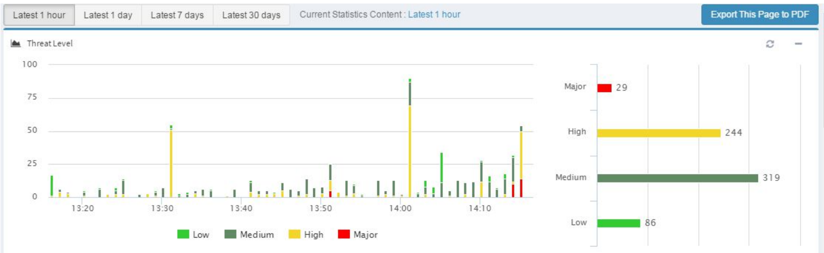
3.3 Threat

Procedure:

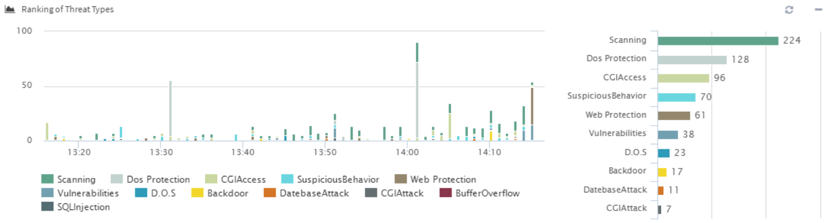
Choose **vCenter** > **Threat** to display the threat statistics during the past 1 hour, past 1 day, past 7 days, and past 30 days.

The statistical items include the threat severity, threat type, threat map, top 10 threat events, top 10 threat source hosts, and top 10 threat-targeted hosts. The last two statistical items can be displayed in the forms of a table and a bar graph.

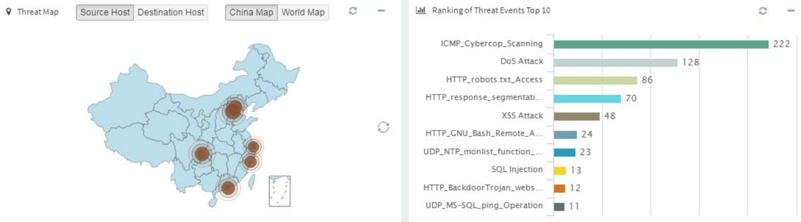
Threat statistics sorted by severity:



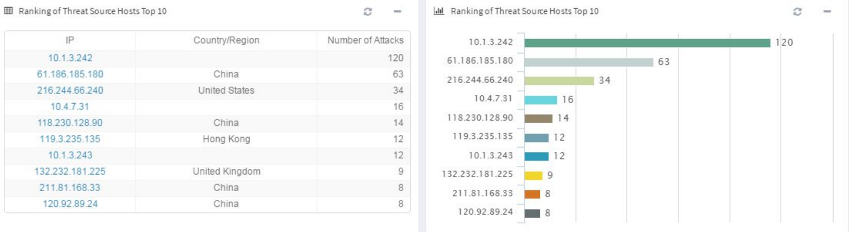
Threat statistics sorted by type:



Threat map and top 10 threat events:


Threat Map
Source Host
Destination Host
China Map
World Map
Ranking of Threat Events Top 10
ICMP_Cybercop_Scanning 222
DoS Attack 128
HTTP_robots.txt_Access 86
HTTP_response_segmentati... 70
XSS Attack 48
HTTP_GNU_Bash_Remote_A... 24
UDP_NTP_monlist_function_... 23
SQL Injection 13
HTTP_BackdoorTrojan_webs... 12
UDP_MS-SQL_ping_Operation 11

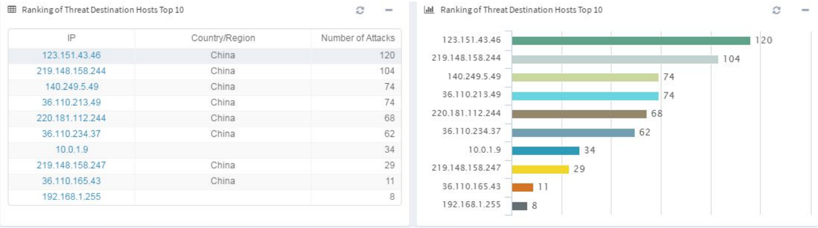
Top 10 threat source hosts displayed in the forms of a table and a bar graph:



Ranking of Threat Source Hosts Top 10

IP	Country/Region	Number of Attacks
10.1.3.242		120
61.186.185.180	China	63
216.244.66.240	United States	34
10.4.7.31		16
118.230.128.90	China	14
119.3.235.135	Hong Kong	12
10.1.3.243		12
132.232.181.225	United Kingdom	9
211.81.168.33	China	8
120.92.89.24	China	8

Top 10 threat-targeted hosts displayed in the forms of a table and a bar graph:



Ranking of Threat Destination Hosts Top 10

IP	Country/Region	Number of Attacks
123.151.43.46	China	120
219.148.158.244	China	104
140.249.5.49	China	74
36.110.213.49	China	74
220.181.112.244	China	68
36.110.234.37	China	62
10.0.1.9		34
219.148.158.247	China	29
36.110.165.43	China	11
192.168.1.255		8

Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Export this page to PDF** to export the content of the entire page to a PDF file. The file contains all the statistics displayed on the page. If a statistical item is hidden on the page, it is also hidden in the file.

4 System Monitoring

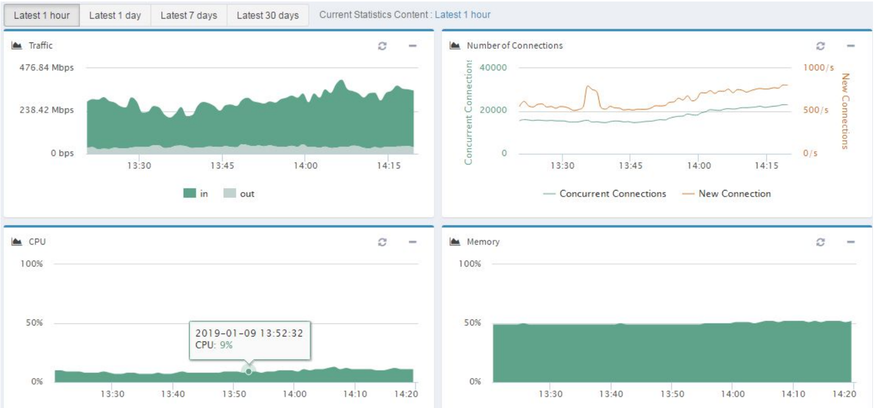
4.1 Overview

The system monitoring function allows you to monitor a firewall's traffic rate, concurrent connections, new connections, CPU usage, and memory usage. Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

4.2 System Monitoring

Procedure:

4.2.1 Choose **Monitor** > **System** to display the statistics on the firewall's traffic rate, connections, CPU usage, and memory usage during the past 1 hour, past 1 day, past 7 days, and past 30 days.



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

5 Interface Monitoring

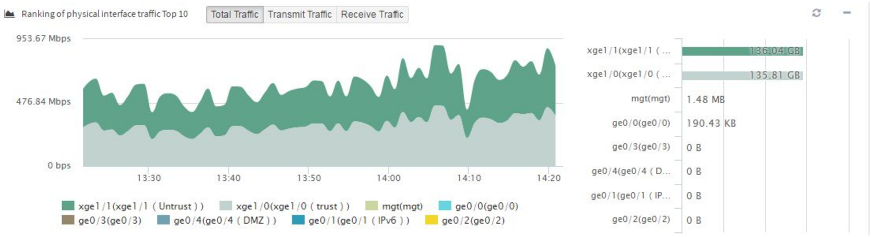
5.1 Overview

The interface monitoring function allows you to monitor and collect statistics on the interface traffic changes of a firewall. Interfaces are classified into physical interfaces, VLAN interfaces, and link aggregation interfaces. You can view the traffic changes sorted by interface type during different historical periods, and view the real-time traffic rates of interfaces on the **Interface details** page.

5.2 Interface Overview

Procedure:

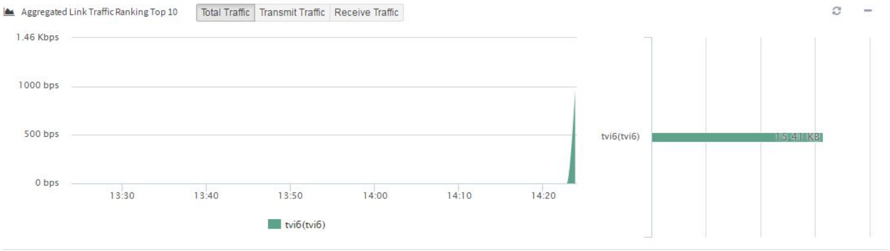
1. Choose **Monitor** > **Interface** > **Overview** to display the traffic statistics on the top 10 interfaces ranked by total traffic during a statistical period. The line chart shows the changes in the interface traffic rate during the statistical period, whereas the bar graph shows the ranking of interfaces by total traffic during the statistical period. You can view the statistics sorted by total traffic, sent traffic, and received traffic, respectively.
2. Display the statistics on the top 10 physical interfaces ranked by traffic.



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Total traffic**, **Sent traffic**, and **Received traffic** to display statistics in different traffic directions.

3. Display the statistics on the top 10 link aggregation interfaces ranked by traffic.



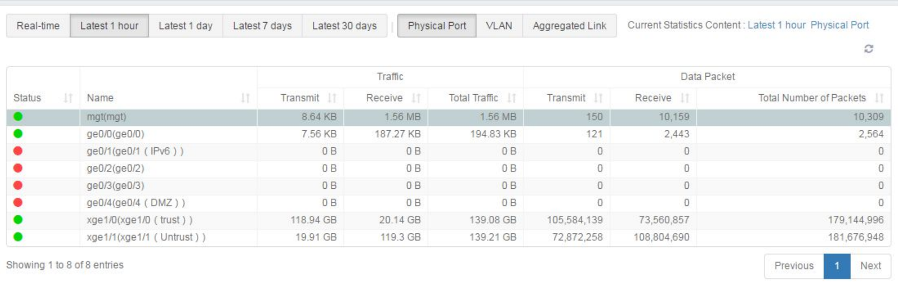
Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Total traffic**, **Sent traffic**, and **Received traffic** to display statistics in different traffic directions.

5.3 Interface Details

Procedure:

1. Choose **Monitor** > **Interface** > **Interface details** to display the traffic statistics on physical interfaces, VLAN interfaces, and link aggregation interfaces in real time or during the past 1 hour, past 1 day, past 7 days, and past 30 days.
2. Display the real-time traffic rates of interfaces.



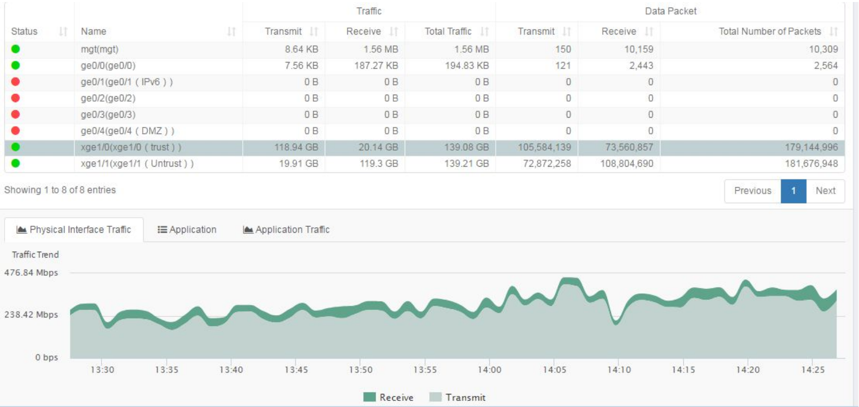
Current Statistics Content : Latest 1 hour Physical Port

		Traffic			Data Packet		
Status	Name	Transmit	Receive	Total Traffic	Transmit	Receive	Total Number of Packets
●	mgt(mgt)	8.64 KB	1.56 MB	1.56 MB	150	10,159	10,309
●	ge0/0(ge0/0)	7.56 KB	187.27 KB	194.83 KB	121	2,443	2,564
●	ge0/1(ge0/1 (IPv6))	0 B	0 B	0 B	0	0	0
●	ge0/2(ge0/2)	0 B	0 B	0 B	0	0	0
●	ge0/3(ge0/3)	0 B	0 B	0 B	0	0	0
●	ge0/4(ge0/4 (DMZ))	0 B	0 B	0 B	0	0	0
●	xge1/0(xge1/0 (trust))	118.94 GB	20.14 GB	139.08 GB	105,584,139	73,560,857	179,144,996
●	xge1/1(xge1/1 (Untrust))	19.91 GB	119.3 GB	139.21 GB	72,872,258	108,804,690	181,676,948

Showing 1 to 8 of 8 entries

Click **Physical interface** , **VLAN**, and **Link aggregation** to display the real-time traffic rate by interface type.

3. Display the historical interface traffic.



		Traffic			Data Packet		
Status	Name	Transmit	Receive	Total Traffic	Transmit	Receive	Total Number of Packets
🟢	mgt(mgt)	8.64 KB	1.56 MB	1.56 MB	150	10,159	10,309
🟢	ge0/0(ge0/0)	7.56 KB	187.27 KB	194.83 KB	121	2,443	2,564
🔴	ge0/1(ge0/1 (IPv6))	0 B	0 B	0 B	0	0	0
🔴	ge0/2(ge0/2)	0 B	0 B	0 B	0	0	0
🔴	ge0/3(ge0/3)	0 B	0 B	0 B	0	0	0
🔴	ge0/4(ge0/4 (DMZ))	0 B	0 B	0 B	0	0	0
🟢	xge1/0(xge1/0 (trust))	118.94 GB	20.14 GB	139.08 GB	105,584,139	73,560,857	179,144,996
🟢	xge1/1(xge1/1 (Untrust))	19.91 GB	119.3 GB	139.21 GB	72,872,258	108,804,690	181,676,948

Showing 1 to 8 of 8 entries

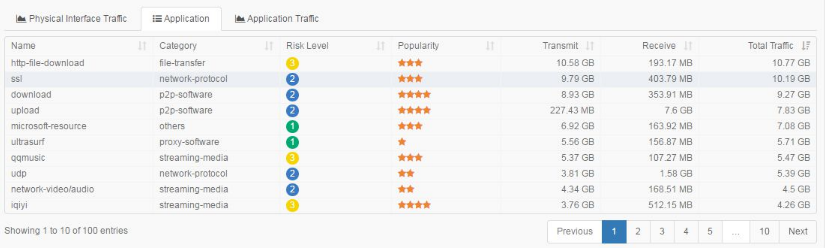
Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Physical interface** , **VLAN**, and **Link aggregation** to change the interface type.

Click a specific interface to display its traffic rate curve and application traffic statistics during a statistical period.

4. After you click an interface, the page shows the distribution of application traffic over the interface.

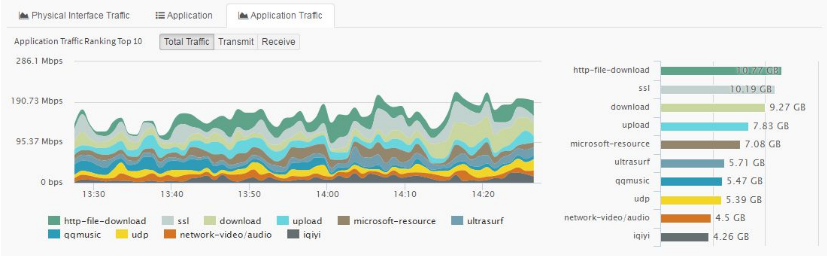
Application traffic list:



Name	Category	Risk Level	Popularity	Transmit	Receive	Total Traffic
http-file-download	file-transfer	3	★★★	10.58 GB	193.17 MB	10.77 GB
ssl	network-protocol	2	★★★	9.79 GB	403.79 MB	10.19 GB
download	p2p-software	2	★★★★	8.93 GB	353.91 MB	9.27 GB
upload	p2p-software	2	★★★★	227.43 MB	7.6 GB	7.83 GB
microsoft-resource	others	1	★★★	6.92 GB	163.92 MB	7.08 GB
ultrasurf	proxy-software	1	★	5.56 GB	156.87 MB	5.71 GB
qqmusic	streaming-media	3	★★★	5.37 GB	107.27 MB	5.47 GB
udp	network-protocol	2	★★	3.81 GB	1.58 GB	5.39 GB
network-video/audio	streaming-media	2	★★	4.34 GB	168.51 MB	4.5 GB
iqiyi	streaming-media	3	★★★★	3.76 GB	512.15 MB	4.26 GB

Showing 1 to 10 of 100 entries

Top 10 application traffic ranking shown in a line chart and a bar graph:



6 Threat Monitoring

6.1 Overview

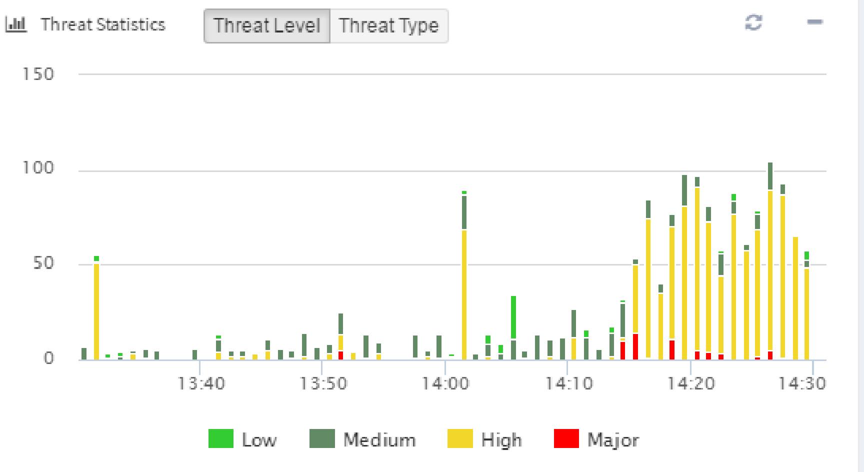
The threat monitoring function allows you to monitor threats. You can monitor threats during the past 1 hour, past 1 day, past 7 days, and past 30 days, and analyze the severity, types, events, and geographic distribution of attacks in a comprehensive manner. You can also determine threat sources by analyzing the provided chart, table, and distribution diagram.

6.2 Threat Overview

Procedure:

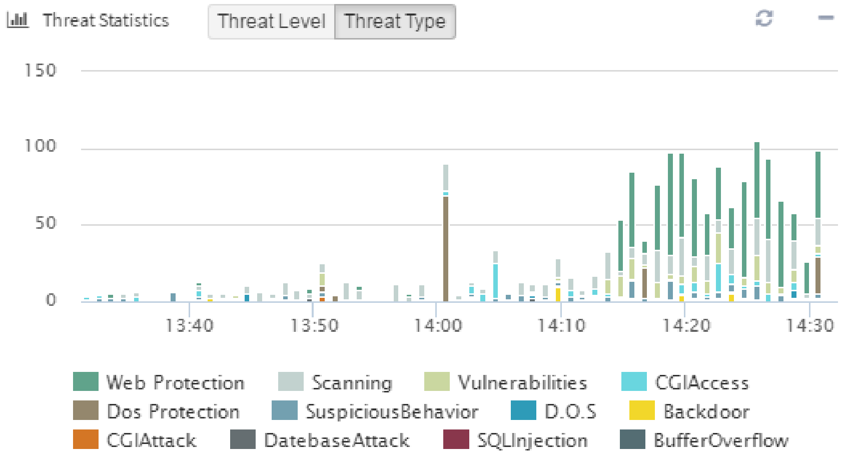
1. Choose **Monitor** > **Threat** > **Overview** to display the threat statistics, threat map, top 10 threat-related hosts, and top 10 threats during the past 1 hour, past 1 day, past 7 days, and past 30 days. The statistical items include the threat severity, threat type, threat event, and threat distribution, which is shown on a map of China or a map of the world.

2. Display the threat statistics sorted by severity.



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

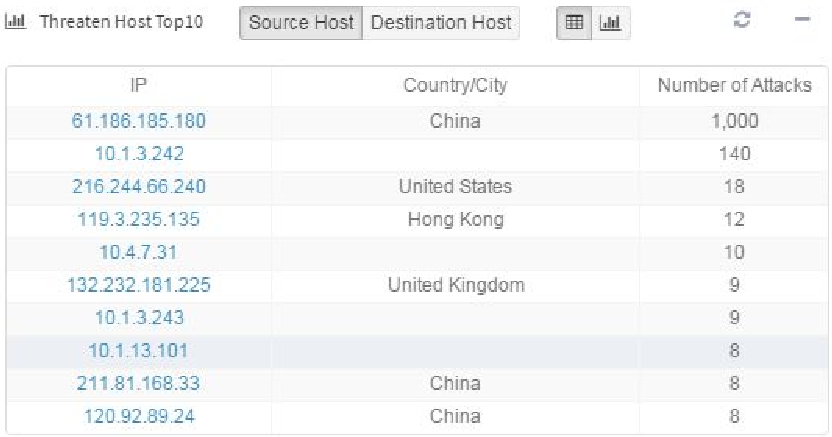
3. Display the threat statistics sorted by type.



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Threat severity** and **Threat type** to display different statistics.

4. Display the top 10 threat-related hosts in the form of a table.



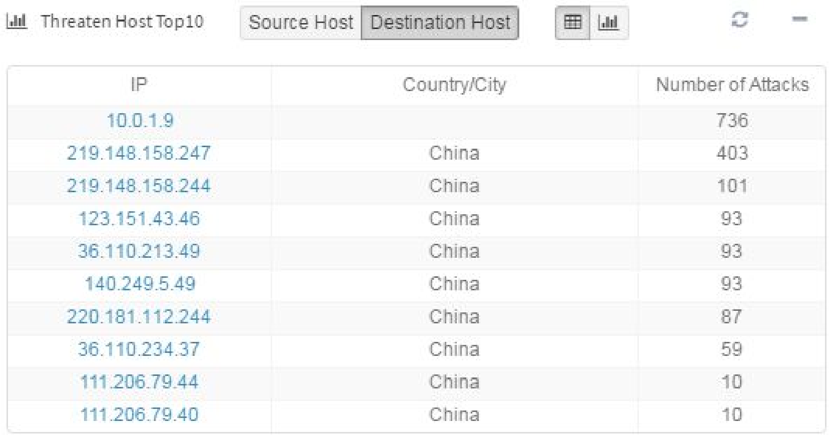
IP	Country/City	Number of Attacks
61.186.185.180	China	1,000
10.1.3.242		140
216.244.66.240	United States	18
119.3.235.135	Hong Kong	12
10.4.7.31		10
132.232.181.225	United Kingdom	9
10.1.3.243		9
10.1.13.101		8
211.81.168.33	China	8
120.92.89.24	China	8

Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Source host** and **Target host** to display the statistics on attacking hosts and attacked hosts.

Click the **Table** and **Chart** buttons to display statistics in the form of a table or a chart.

5. Display the top 10 threat-related hosts in the form of a bar graph.



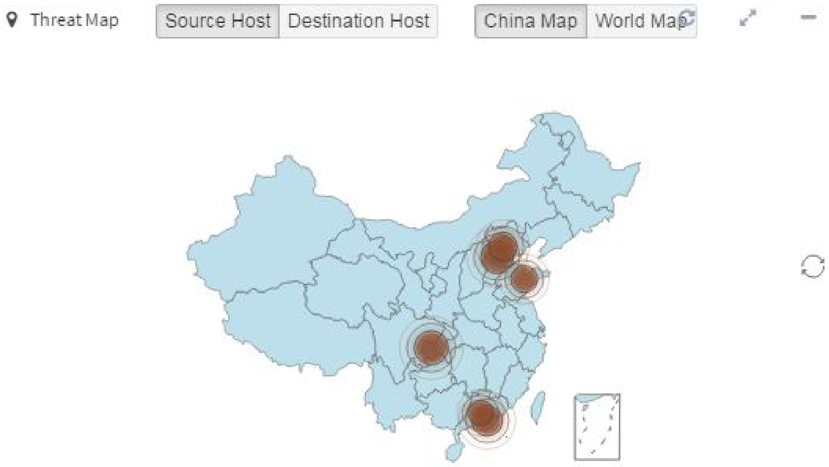
IP	Country/City	Number of Attacks
10.0.1.9		736
219.148.158.247	China	403
219.148.158.244	China	101
123.151.43.46	China	93
36.110.213.49	China	93
140.249.5.49	China	93
220.181.112.244	China	87
36.110.234.37	China	59
111.206.79.44	China	10
111.206.79.40	China	10

Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Source host** and **Target host** to display the statistics on attacking hosts and attacked hosts.

Click the **Table** and **Chart** buttons to display statistics in the form of a table or a chart.

6. Display the distribution of threat-targeted hosts on a map of China.

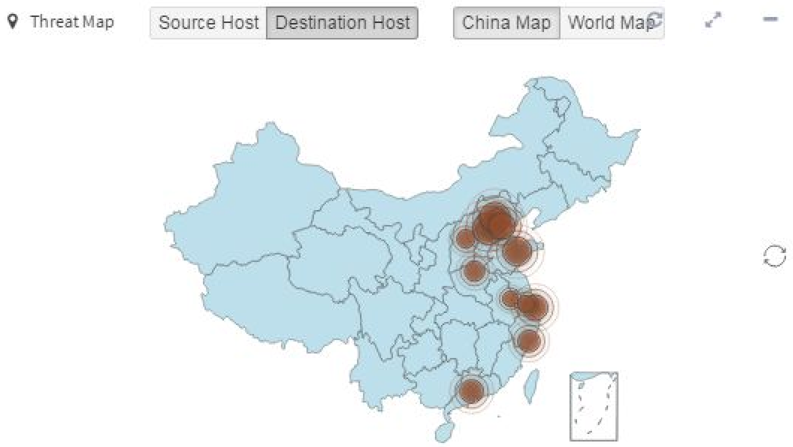


Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Source host** and **Target host** to display the statistics on attacking hosts and attacked hosts.

Click **China** and **World** to display the distribution of attacks on a map of China or a map of the world.

7. Display the distribution of threat-targeted hosts on a map of the world.

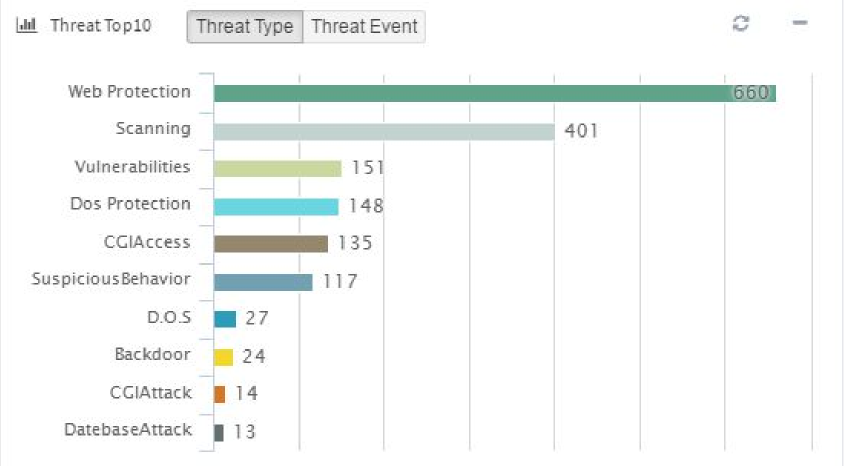


Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Source host** and **Target host** to display the statistics on attacking hosts and attacked hosts.

Click **China** and **World** to display the distribution of attacks on a map of China or a map of the world.

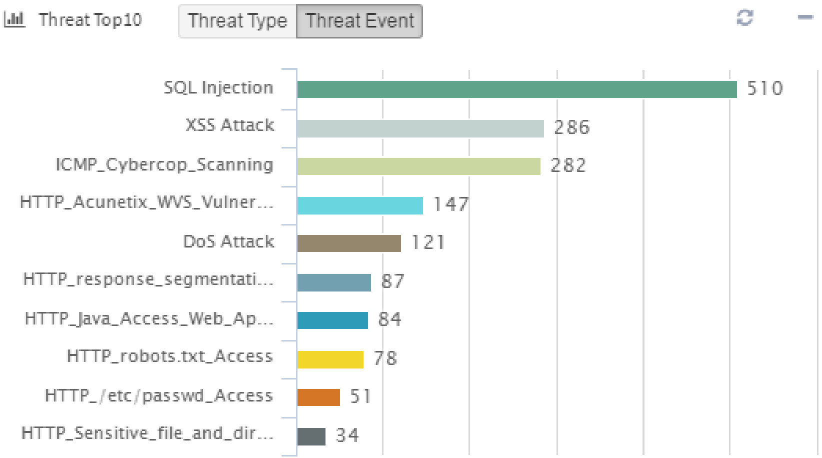
8. Display the top 10 threat types.



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Threat type** and **Threat event** to display different statistics.

9. Display the top 10 threat events.



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

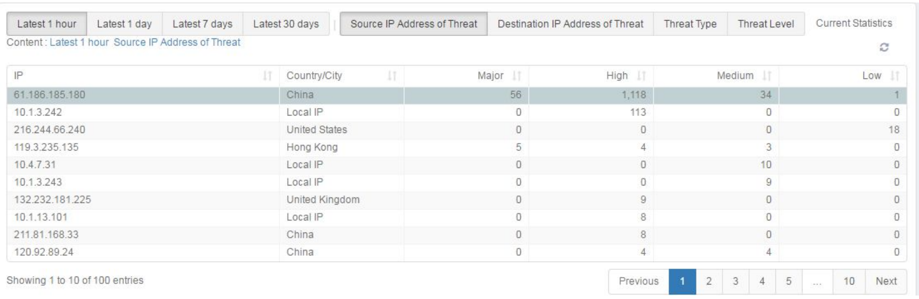
Click **Threat type** and **Threat event** to display different statistics.

6.3 Threat Details

Procedure:

1. Choose **Monitor** > **Threat** > **Threat details**.

2. Display the threat details.

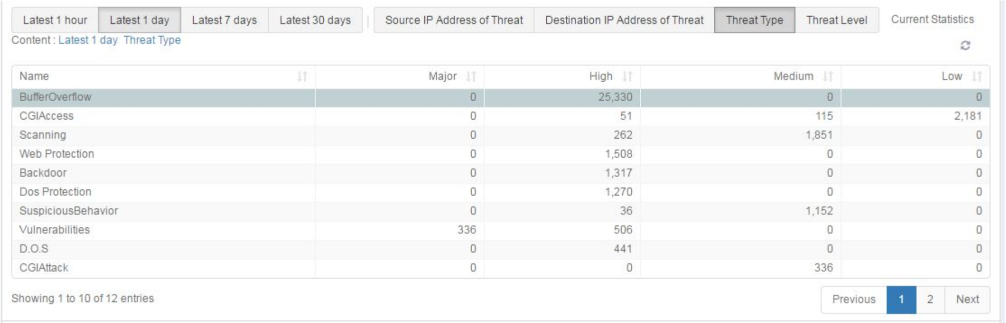


Content : Latest 1 hour Source IP Address of Threat

IP	Country/City	Major	High	Medium	Low
61.186.185.180	China	56	1,118	34	1
10.1.3.242	Local IP	0	113	0	0
216.244.66.240	United States	0	0	0	18
119.3.235.135	Hong Kong	5	4	3	0
10.4.7.31	Local IP	0	0	10	0
10.1.3.243	Local IP	0	0	9	0
132.232.181.225	United Kingdom	0	9	0	0
10.1.13.101	Local IP	0	8	0	0
211.81.168.33	China	0	8	0	0
120.92.89.24	China	0	4	4	0

Showing 1 to 10 of 100 entries

The preceding figure shows statistics on the IP addresses flagged as threats, including their geographic locations and threat severities.

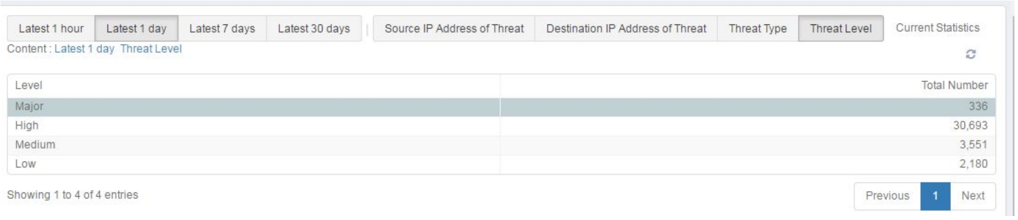


Content : Latest 1 day Threat Type

Name	Major	High	Medium	Low
BufferOverflow	0	25,330	0	0
CGIAccess	0	51	115	2,181
Scanning	0	262	1,851	0
Web Protection	0	1,508	0	0
Backdoor	0	1,317	0	0
Dos Protection	0	1,270	0	0
SuspiciousBehavior	0	36	1,152	0
Vulnerabilities	336	506	0	0
D.O.S	0	441	0	0
CGIAttack	0	0	336	0

Showing 1 to 10 of 12 entries

The preceding figure shows the statistics sorted by threat type, including the severity distribution under each threat type.



Content : Latest 1 day Threat Level

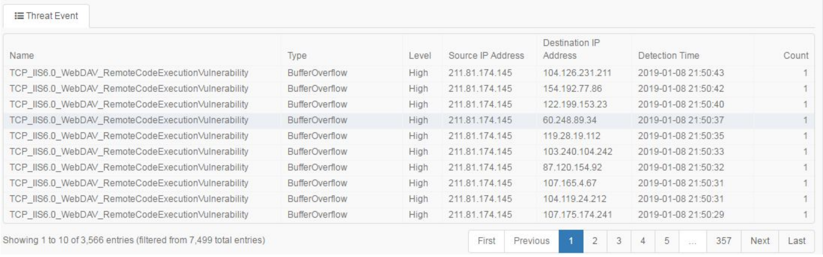
Level	Total Number
Major	336
High	30,693
Medium	3,551
Low	2,180

Showing 1 to 4 of 4 entries

The preceding figure shows the statistics sorted by threat severity, including the total threats of each severity.

3. Click a statistical item to display the related threat events.

Threat event details:



Name	Type	Level	Source IP Address	Destination IP Address	Detection Time	Count
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	104.126.231.211	2019-01-08 21:50:43	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	154.192.77.86	2019-01-08 21:50:42	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	122.199.153.23	2019-01-08 21:50:40	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	60.248.89.34	2019-01-08 21:50:37	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	119.28.19.112	2019-01-08 21:50:35	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	103.240.104.242	2019-01-08 21:50:33	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	87.120.154.92	2019-01-08 21:50:32	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	107.165.4.67	2019-01-08 21:50:31	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	104.119.24.212	2019-01-08 21:50:31	1
TCP_IIS6.0_WebDAV_RemoteCodeExecutionVulnerability	BufferOverflow	High	211.81.174.145	107.175.174.241	2019-01-08 21:50:29	1

Showing 1 to 10 of 3,566 entries (filtered from 7,499 total entries)

The preceding statistics show the following details about each threat event: type, severity, source IP address, target IP address, detected time, times of detecting the same event.

Notice	The data of threat events is stored in a disk, and the stored data volume depends on the disk capacity. If many threats have been detected, the earliest data is deleted and cannot be queried.

7 User Monitoring

7.1 Overview

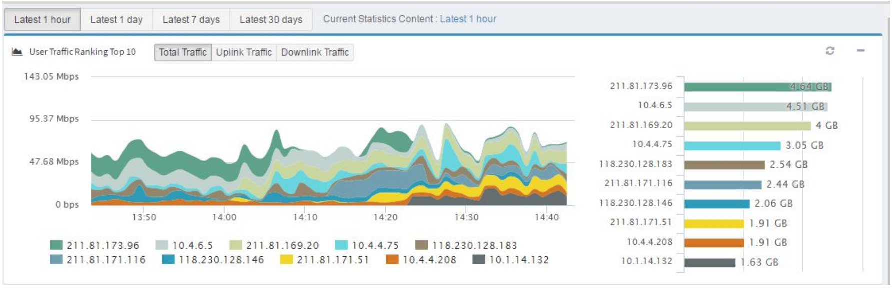
The user monitoring function allows you to monitor users' traffic and sessions. You can view the top 10 users ranked by total traffic, uplink traffic, downlink traffic, and concurrent connections during the past 1 hour, past 1 day, past 7 days, and past 30 days. On the **User details** page, you can view the details about the top 100 IP addresses ranked by traffic.

7.2 User Overview

Procedure:

1. Choose **Monitor** > **User** > **Overview** to display the top 10 IP addresses ranked by traffic passing the firewall during the past 1 hour, past 1 day, past 7 days, and past 30 days. The line chart shows the rate of the total traffic, sent traffic, or received traffic of the top 10 IP addresses. The bar graph ranks IP addresses by total traffic, sent traffic, or received traffic.

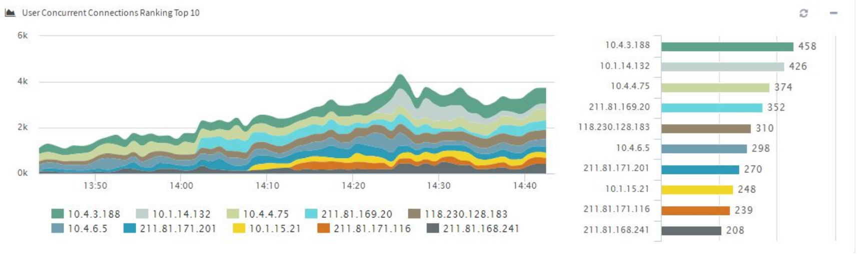
2. Display the top 10 users ranked by traffic.



Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

Click **Total traffic**, **Uplink traffic**, and **Downlink traffic** to display statistics in different traffic directions.

3. Display the top 10 users ranked by concurrent connections.

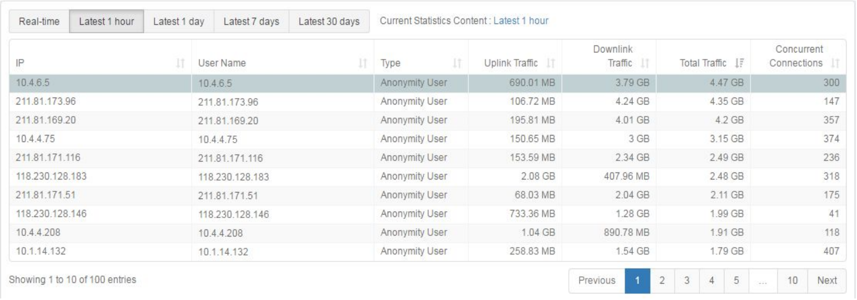


Click **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

7.3 User Details

Procedure:

1. Choose **Monitor** > **User** > **User details** to display the real-time traffic rates of user IP addresses and the details about the top 10 IP addresses ranked by total traffic during the past 1 hour, past 1 day, past 7 days, and past 30 days.



Current Statistics Content : Latest 1 hour

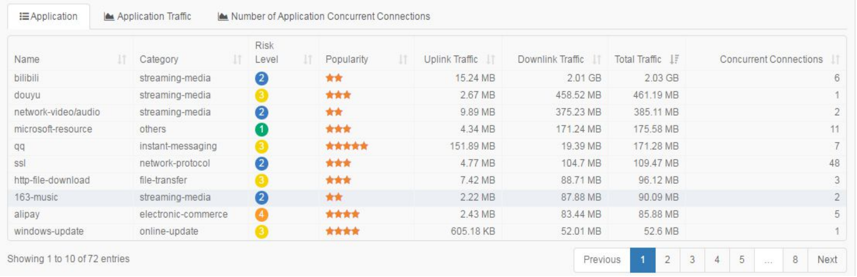
IP	User Name	Type	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
10.4.6.5	10.4.6.5	Anonymity User	690.01 MB	3.79 GB	4.47 GB	300
211.81.173.96	211.81.173.96	Anonymity User	106.72 MB	4.24 GB	4.35 GB	147
211.81.169.20	211.81.169.20	Anonymity User	195.81 MB	4.01 GB	4.2 GB	357
10.4.4.75	10.4.4.75	Anonymity User	150.65 MB	3 GB	3.15 GB	374
211.81.171.116	211.81.171.116	Anonymity User	153.59 MB	2.34 GB	2.49 GB	236
118.230.128.183	118.230.128.183	Anonymity User	2.08 GB	407.96 MB	2.48 GB	318
211.81.171.51	211.81.171.51	Anonymity User	68.03 MB	2.04 GB	2.11 GB	175
118.230.128.146	118.230.128.146	Anonymity User	733.36 MB	1.28 GB	1.99 GB	41
10.4.4.208	10.4.4.208	Anonymity User	1.04 GB	890.78 MB	1.91 GB	118
10.1.14.132	10.1.14.132	Anonymity User	258.83 MB	1.54 GB	1.79 GB	407

Showing 1 to 10 of 100 entries

Click **Real-time**, **Past 1 hour**, **Past 1 day**, **Past 7 days**, and **Past 30 days** to change the monitoring period.

2. Click a user in the traffic ranklist to display the distribution of the user's traffic among all the applications.

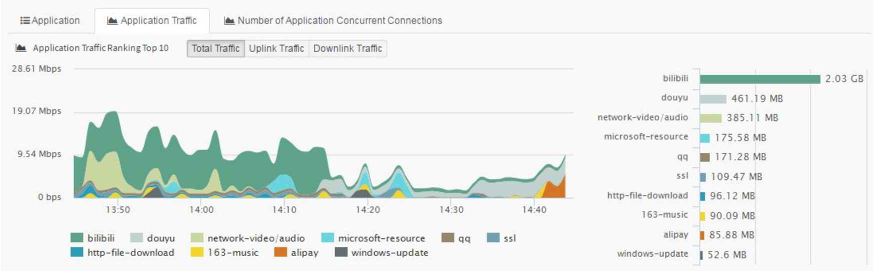
   Application traffic list:



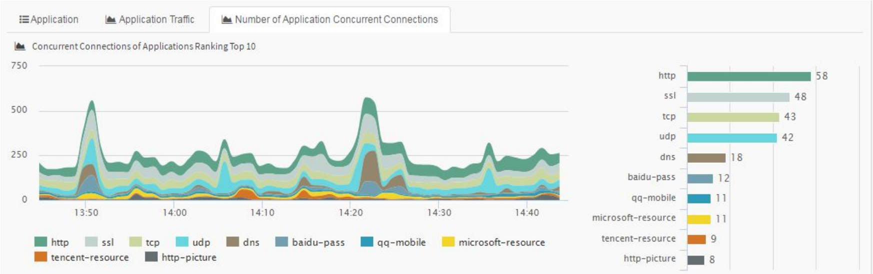
Name	Category	Risk Level	Popularity	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
bilibili	streaming-media	2	★★	15.24 MB	2.01 GB	2.03 GB	6
douyu	streaming-media	3	★★★	2.67 MB	458.52 MB	461.19 MB	1
network-video/audio	streaming-media	2	★★	9.89 MB	375.23 MB	385.11 MB	2
microsoft-resource	others	1	★★★	4.34 MB	171.24 MB	175.58 MB	11
qq	instant-messaging	3	★★★★★	151.89 MB	19.39 MB	171.28 MB	7
ssl	network-protocol	2	★★★	4.77 MB	104.7 MB	109.47 MB	48
http-file-download	file-transfer	3	★★★	7.42 MB	88.71 MB	96.12 MB	3
163-music	streaming-media	2	★★	2.22 MB	87.88 MB	90.09 MB	2
alipay	electronic-commerce	4	★★★★	2.43 MB	83.44 MB	85.88 MB	5
windows-update	online-update	3	★★★★	605.18 KB	52.01 MB	52.6 MB	1

Showing 1 to 10 of 72 entries

Line chart and bar graph showing application traffic:



Line chart and bar graph showing application-initiated concurrent connections:



8 Application Monitoring

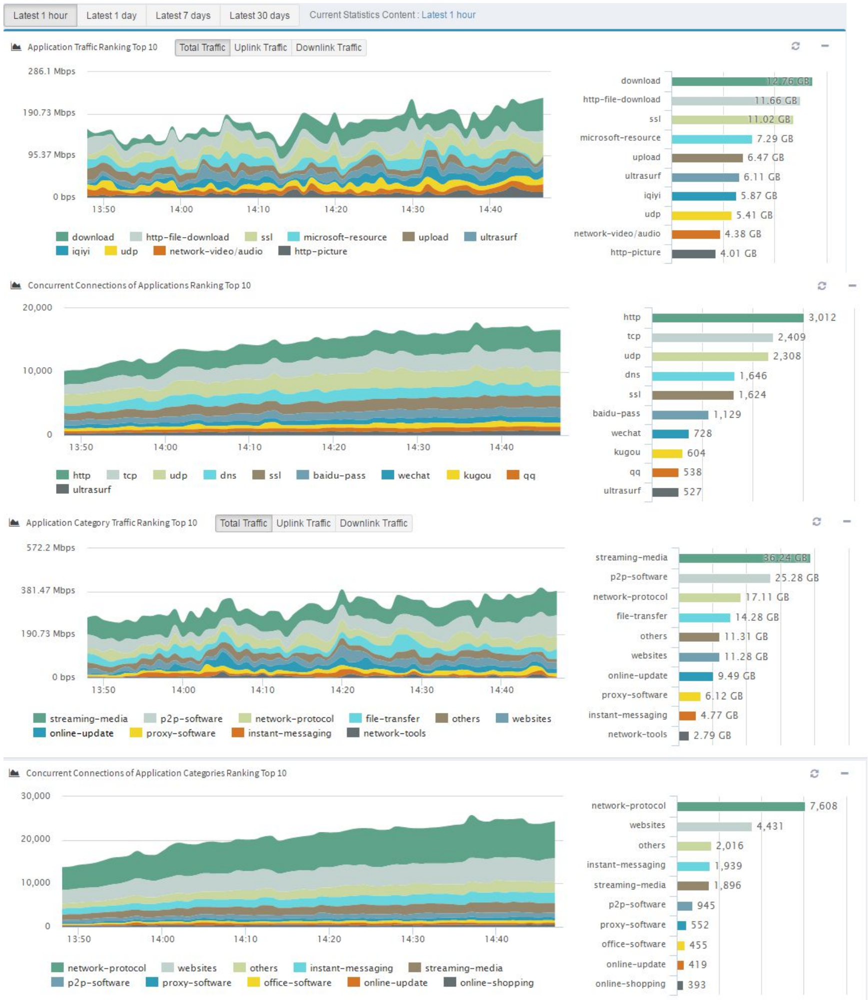
8.1 Overview

The application monitoring function allows you to monitor and collect statistics on the application traffic passing a firewall. You can view the top 10 applications ranked by total traffic, uplink traffic, downlink traffic, and concurrent connections during the past 1 hour, past 1 day, past 7 days, and past 30 days. You can also view the details about the top 100 applications ranked by traffic.

8.2 Application Monitoring Overview

Procedure:

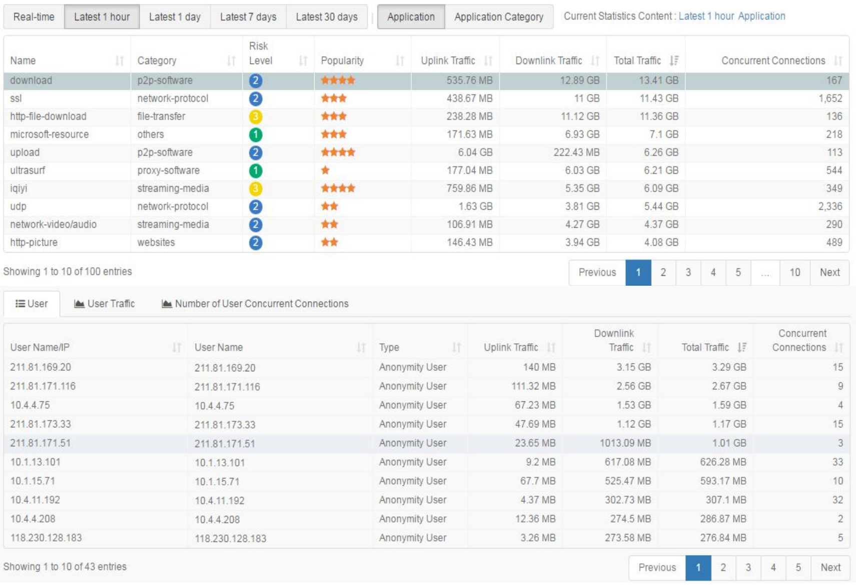
1. Choose **Monitor** > **Application** > **Overview** to display the statistics on traffic and concurrent connections sorted by traffic and traffic category during the past 1 hour, past 1 day, past 7 days, and past 30 days. The line chart shows the rates of total traffic, sent traffic, and received traffic of applications, whereas the bar graph ranks applications by total traffic, sent traffic, and received traffic.



8.3 Application Statistics Details

Procedure:

1. Choose **Monitor** > **Application** > **Application details** to display the statistics sorted by application and application category during the past 1 hour, past 1 day, past 7 days, and past 30 days, and the real-time statistics on traffic and concurrent connections. A maximum of 100 records can be displayed.



Current Statistics Content : Latest 1 hour Application

Name	Category	Risk Level	Popularity	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
download	p2p-software	2	★★★★	535.76 MB	12.89 GB	13.41 GB	167
ssl	network-protocol	2	★★★	438.67 MB	11 GB	11.43 GB	1,652
http-file-download	file-transfer	3	★★★	238.28 MB	11.12 GB	11.36 GB	136
microsoft-resource	others	1	★★★	171.63 MB	6.93 GB	7.1 GB	218
upload	p2p-software	2	★★★★	6.04 GB	222.43 MB	6.26 GB	113
ultrasurf	proxy-software	1	★	177.04 MB	6.03 GB	6.21 GB	544
iqiyi	streaming-media	3	★★★★	759.86 MB	5.35 GB	6.09 GB	349
udp	network-protocol	2	★★	1.63 GB	3.81 GB	5.44 GB	2,336
network-video/audio	streaming-media	2	★★	106.91 MB	4.27 GB	4.37 GB	290
http-picture	websites	2	★★	146.43 MB	3.94 GB	4.08 GB	489

Showing 1 to 10 of 100 entries

User Name/IP	User Name	Type	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
211.81.169.20	211.81.169.20	Anonymity User	140 MB	3.15 GB	3.29 GB	15
211.81.171.116	211.81.171.116	Anonymity User	111.32 MB	2.56 GB	2.67 GB	9
10.4.4.75	10.4.4.75	Anonymity User	67.23 MB	1.53 GB	1.59 GB	4
211.81.173.33	211.81.173.33	Anonymity User	47.69 MB	1.12 GB	1.17 GB	15
211.81.171.51	211.81.171.51	Anonymity User	23.65 MB	1013.09 MB	1.01 GB	3
10.1.13.101	10.1.13.101	Anonymity User	9.2 MB	617.08 MB	626.28 MB	33
10.1.15.71	10.1.15.71	Anonymity User	67.7 MB	525.47 MB	593.17 MB	10
10.4.11.192	10.4.11.192	Anonymity User	4.37 MB	302.73 MB	307.1 MB	32
10.4.4.208	10.4.4.208	Anonymity User	12.36 MB	274.5 MB	286.87 MB	2
118.230.128.183	118.230.128.183	Anonymity User	3.26 MB	273.58 MB	276.84 MB	5

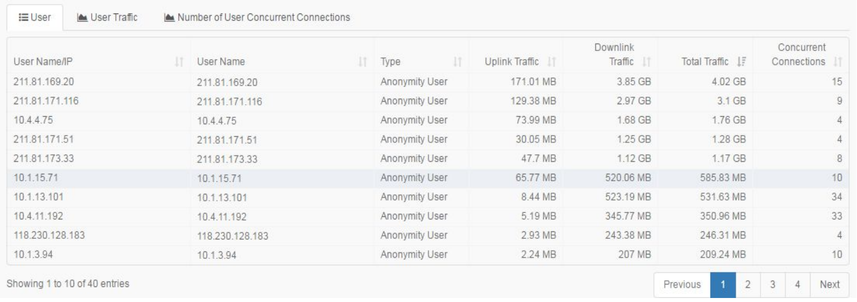
Showing 1 to 10 of 43 entries

2. Select **Application** or **Application category** to display the statistics sorted by application or application category.

3. Select **Past 1 hour**, **Past 1 day**, **Past 7 days**, or **Past 30 days** to display the statistics collected during the corresponding period.

4. Click an application in the application or application category ranklist to display the distribution of the application's traffic among all the user IP addresses.

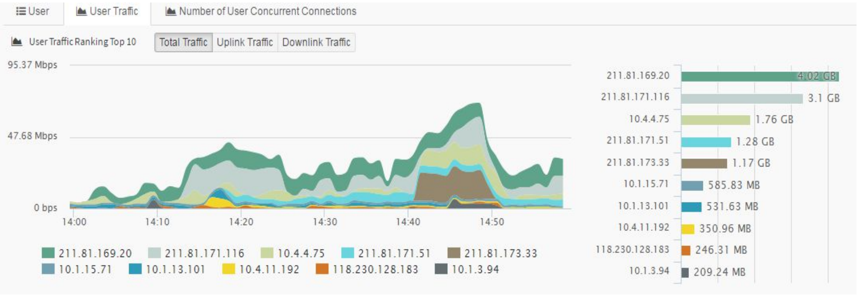
   User traffic list:



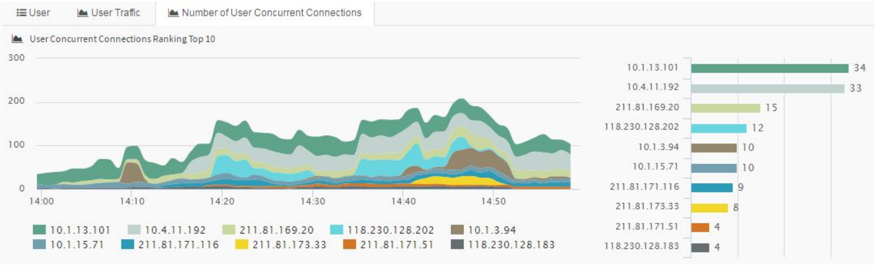
User Name/IP	User Name	Type	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
211.81.169.20	211.81.169.20	Anonymity User	171.01 MB	3.85 GB	4.02 GB	15
211.81.171.116	211.81.171.116	Anonymity User	129.38 MB	2.97 GB	3.1 GB	9
10.4.4.75	10.4.4.75	Anonymity User	73.99 MB	1.68 GB	1.76 GB	4
211.81.171.51	211.81.171.51	Anonymity User	30.05 MB	1.25 GB	1.28 GB	4
211.81.173.33	211.81.173.33	Anonymity User	47.7 MB	1.12 GB	1.17 GB	8
10.1.15.71	10.1.15.71	Anonymity User	65.77 MB	520.06 MB	585.83 MB	10
10.1.13.101	10.1.13.101	Anonymity User	8.44 MB	523.19 MB	531.63 MB	34
10.4.11.192	10.4.11.192	Anonymity User	5.19 MB	345.77 MB	350.96 MB	33
118.230.128.183	118.230.128.183	Anonymity User	2.93 MB	243.38 MB	246.31 MB	4
10.1.3.94	10.1.3.94	Anonymity User	2.24 MB	207 MB	209.24 MB	10

Showing 1 to 10 of 40 entries

   Line chart and bar graph showing user traffic:

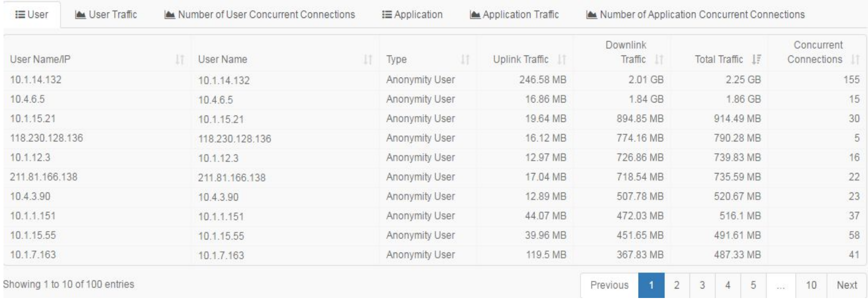


   Line chart and bar graph showing user-initiated concurrent connections:



4. Click an application category in the application category ranklist to display the distribution of traffic and concurrent connections among all the user IP addresses and applications under that category.

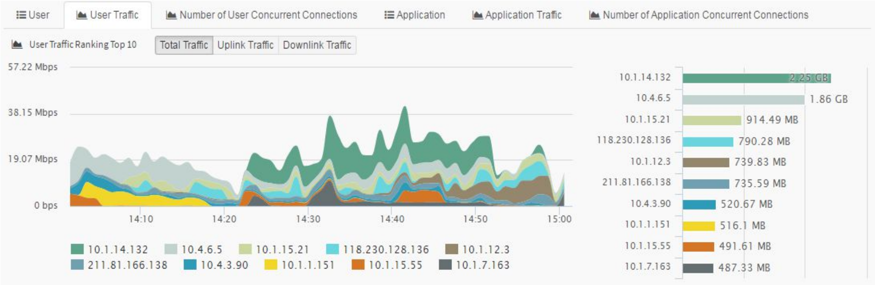
   User traffic list:


User
User Traffic
Number of User Concurrent Connections
Application
Application Traffic
Number of Application Concurrent Connections

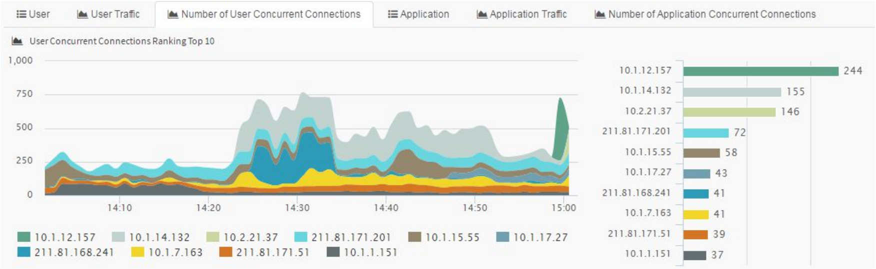
User Name/IP	User Name	Type	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
10.1.14.132	10.1.14.132	Anonymity User	246.58 MB	2.01 GB	2.25 GB	155
10.4.6.5	10.4.6.5	Anonymity User	16.86 MB	1.84 GB	1.86 GB	15
10.1.15.21	10.1.15.21	Anonymity User	19.64 MB	894.85 MB	914.49 MB	30
118.230.128.136	118.230.128.136	Anonymity User	16.12 MB	774.16 MB	790.28 MB	5
10.1.12.3	10.1.12.3	Anonymity User	12.97 MB	726.86 MB	739.83 MB	16
211.81.166.138	211.81.166.138	Anonymity User	17.04 MB	718.54 MB	735.59 MB	22
10.4.3.90	10.4.3.90	Anonymity User	12.89 MB	507.78 MB	520.67 MB	23
10.1.1.151	10.1.1.151	Anonymity User	44.07 MB	472.03 MB	516.1 MB	37
10.1.15.55	10.1.15.55	Anonymity User	39.96 MB	451.65 MB	491.61 MB	58
10.1.7.163	10.1.7.163	Anonymity User	119.5 MB	367.83 MB	487.33 MB	41

Showing 1 to 10 of 100 entries

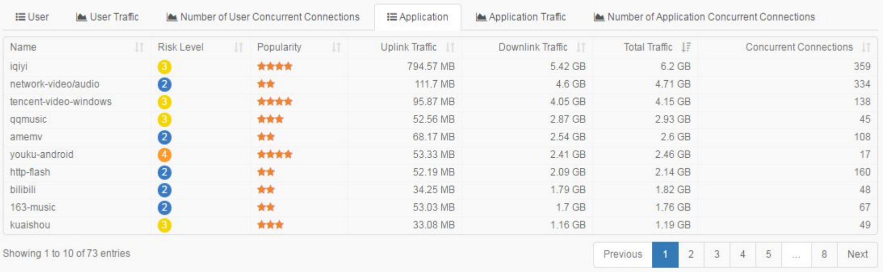
Line chart and bar graph showing user traffic:



Line chart and bar graph showing user-initiated concurrent connections:



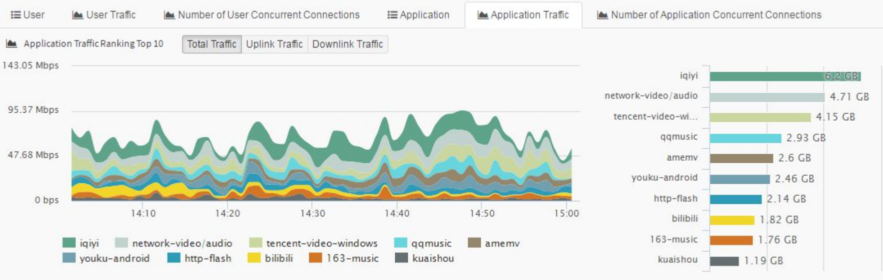
Application traffic list:


User
User Traffic
Number of User Concurrent Connections
Application
Application Traffic
Number of Application Concurrent Connections

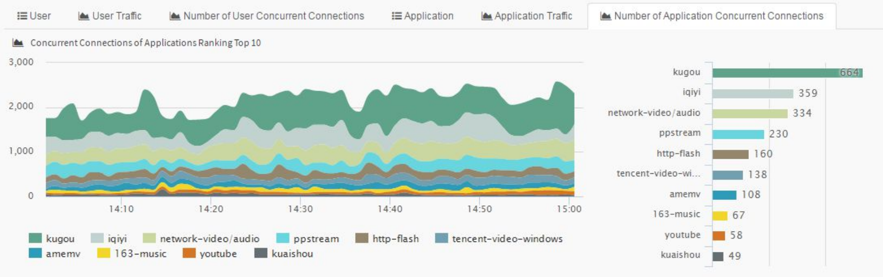
Name	Risk Level	Popularity	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
iqiyi	3	★★★★	794.57 MB	5.42 GB	6.2 GB	359
network-video/audio	2	★★	111.7 MB	4.6 GB	4.71 GB	334
tencent-video-windows	3	★★★★	95.87 MB	4.05 GB	4.15 GB	138
qqmusic	3	★★★	52.56 MB	2.87 GB	2.93 GB	45
amemv	2	★★	68.17 MB	2.54 GB	2.6 GB	108
youku-android	4	★★★★	53.33 MB	2.41 GB	2.46 GB	17
http-flash	2	★★	52.19 MB	2.09 GB	2.14 GB	160
bilibili	2	★★	34.25 MB	1.79 GB	1.82 GB	48
163-music	2	★★	53.03 MB	1.7 GB	1.76 GB	67
kuaishou	3	★★★	33.08 MB	1.16 GB	1.19 GB	49

Showing 1 to 10 of 73 entries

Line chart and bar graph showing application traffic:

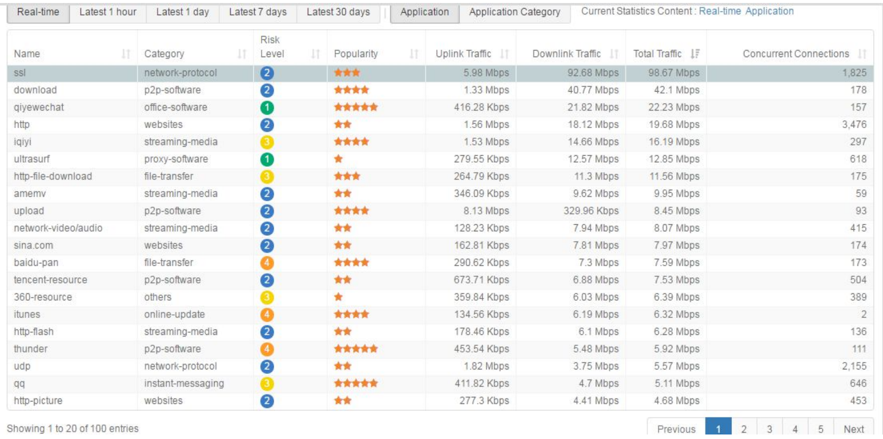


Line chart and bar graph showing application-initiated concurrent connections:



5. Display the real-time information about application traffic.

Select **Real-time** on the **Application details** page to display the real-time traffic and concurrent connections of applications or application categories.



Current Statistics Content : Real-time Application

Name	Category	Risk Level	Popularity	Uplink Traffic	Downlink Traffic	Total Traffic	Concurrent Connections
ssl	network-protocol	2	★★★	5.98 Mbps	92.68 Mbps	98.67 Mbps	1,825
download	p2p-software	2	★★★★	1.33 Mbps	40.77 Mbps	42.1 Mbps	178
qiyewechat	office-software	1	★★★★★	416.28 Kbps	21.82 Mbps	22.23 Mbps	157
http	websites	2	★★	1.56 Mbps	18.12 Mbps	19.68 Mbps	3,476
iqiyi	streaming-media	3	★★★★	1.53 Mbps	14.66 Mbps	16.19 Mbps	297
ultrasurf	proxy-software	1	★	279.55 Kbps	12.57 Mbps	12.85 Mbps	618
http-file-download	file-transfer	3	★★★	264.79 Kbps	11.3 Mbps	11.56 Mbps	175
amemv	streaming-media	2	★★	346.09 Kbps	9.62 Mbps	9.95 Mbps	59
upload	p2p-software	2	★★★★	8.13 Mbps	329.96 Kbps	8.45 Mbps	93
network-video/audio	streaming-media	2	★★	128.23 Kbps	7.94 Mbps	8.07 Mbps	415
sina.com	websites	2	★★	162.81 Kbps	7.81 Mbps	7.97 Mbps	174
baidu-pan	file-transfer	4	★★★★	290.62 Kbps	7.3 Mbps	7.59 Mbps	173
tencent-resource	p2p-software	2	★★	673.71 Kbps	6.88 Mbps	7.53 Mbps	504
360-resource	others	3	★	359.84 Kbps	6.03 Mbps	6.39 Mbps	389
itunes	online-update	4	★★★★	134.56 Kbps	6.19 Mbps	6.32 Mbps	2
http-flash	streaming-media	2	★★	178.46 Kbps	6.1 Mbps	6.28 Mbps	136
thunder	p2p-software	4	★★★★★	453.54 Kbps	5.48 Mbps	5.92 Mbps	111
udp	network-protocol	2	★★	1.82 Mbps	3.75 Mbps	5.57 Mbps	2,155
qq	instant-messaging	3	★★★★★	411.82 Kbps	4.7 Mbps	5.11 Mbps	646
http-picture	websites	2	★★	277.3 Kbps	4.41 Mbps	4.68 Mbps	453

Showing 1 to 20 of 100 entries

9 Traffic Monitoring

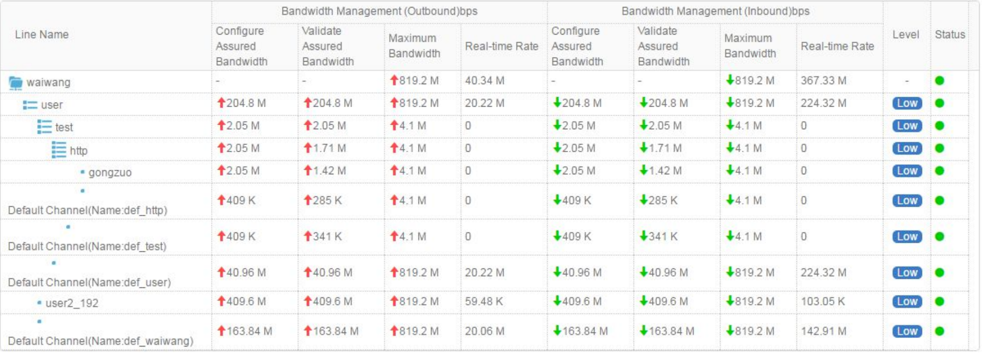
9.1 Overview

The traffic monitoring function allows you to monitor the effectiveness of a traffic control policy.

9.2 Details

Procedure:

1. Choose **Monitor** > **Traffic control** to display the real-time rate and allocated bandwidth of each line regulated by a traffic control policy.



Line Name	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Level	Status
	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Real-time Rate	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Real-time Rate		
waiwang	-	-	↑819.2 M	40.34 M	-	-	↓819.2 M	367.33 M	-	●
user	↑204.8 M	↑204.8 M	↑819.2 M	20.22 M	↓204.8 M	↓204.8 M	↓819.2 M	224.32 M	Low	●
test	↑2.05 M	↑2.05 M	↑4.1 M	0	↓2.05 M	↓2.05 M	↓4.1 M	0	Low	●
http	↑2.05 M	↑1.71 M	↑4.1 M	0	↓2.05 M	↓1.71 M	↓4.1 M	0	Low	●
gongzuo	↑2.05 M	↑1.42 M	↑4.1 M	0	↓2.05 M	↓1.42 M	↓4.1 M	0	Low	●
Default Channel(Name:def_http)	↑409 K	↑285 K	↑4.1 M	0	↓409 K	↓285 K	↓4.1 M	0	Low	●
Default Channel(Name:def_test)	↑409 K	↑341 K	↑4.1 M	0	↓409 K	↓341 K	↓4.1 M	0	Low	●
Default Channel(Name:def_user)	↑40.96 M	↑40.96 M	↑819.2 M	20.22 M	↓40.96 M	↓40.96 M	↓819.2 M	224.32 M	Low	●
user2_192	↑409.6 M	↑409.6 M	↑819.2 M	59.48 K	↓409.6 M	↓409.6 M	↓819.2 M	103.05 K	Low	●
Default Channel(Name:def_waiwang)	↑163.84 M	↑163.84 M	↑819.2 M	20.06 M	↓163.84 M	↓163.84 M	↓819.2 M	142.91 M	Low	●

10 URL Monitoring

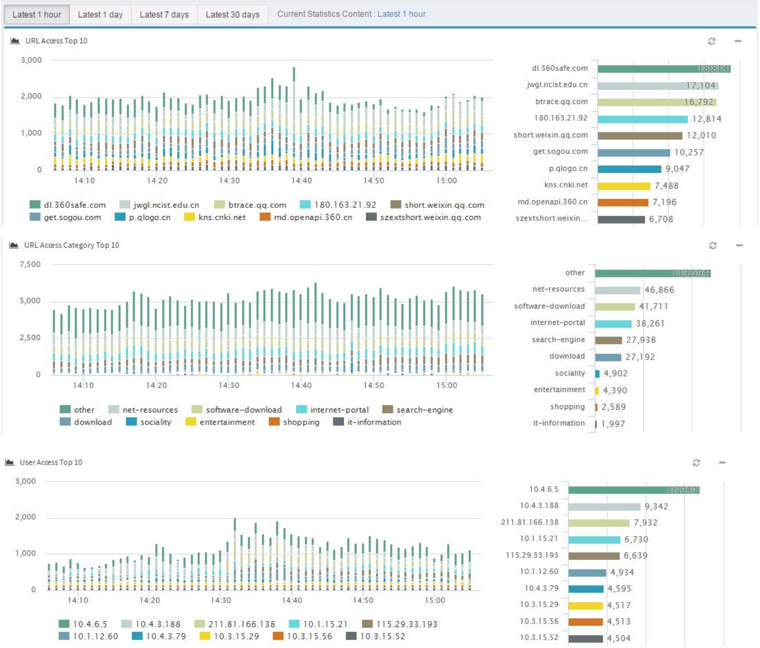
10.1 Overview

The URL monitoring function allows you to monitor and collect statistics on the URLs accessed through the firewall. You can view the top 10 URLs and URL categories and the top 100 user IP addresses ranked by total access volume during the past 1 hour, past 1 day, past 7 days, and past 30 days.

10.2 URL Monitoring Overview

Procedure:

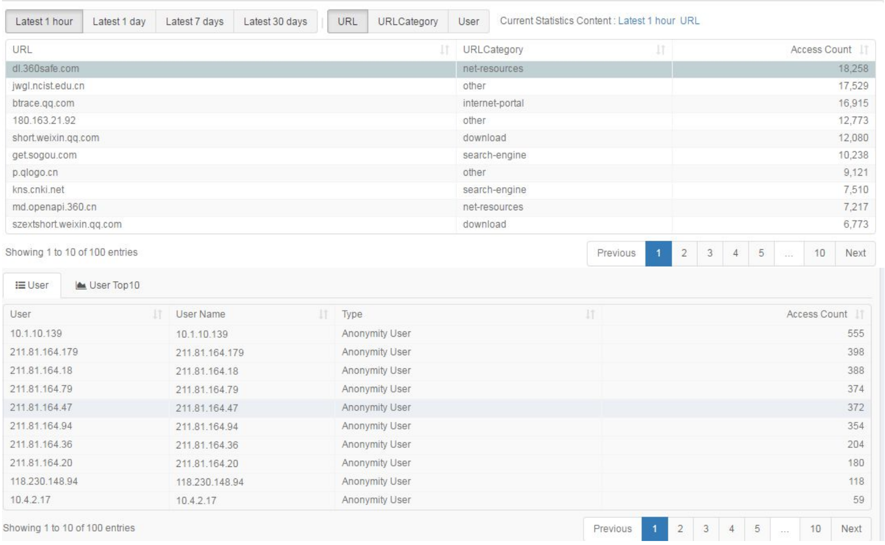
1. Choose **Monitor** > **URL** > **Overview** to display the top 10 URLs, URL categories, and user IP addresses ranked by total access volume during the past 1 hour, past 1 day, past 7 days, and past 30 days. The histogram shows the access status of the top 10 URLs during a specified statistical period, whereas the bar graph shows the access volumes of the top 10 URLs.



10.3 URL Statistics Details

Procedure:

1. Choose **Monitor** > **URL** > **URL details** to display the URL access statistics sorted by URL, URL category, and IP address during the past 1 hour, past 1 day, past 7 days, and past 30 days. A maximum of 100 records can be displayed.



URL	URLCategory	Access Count
dl.360safe.com	net-resources	18,258
jwgl.ncist.edu.cn	other	17,529
btrace.qq.com	internet-portal	16,915
180.163.21.92	other	12,773
short.weixin.qq.com	download	12,080
get.sogou.com	search-engine	10,238
p.qlogo.cn	other	9,121
kns.cnki.net	search-engine	7,510
md.openapi.360.cn	net-resources	7,217
szextshort.weixin.qq.com	download	6,773

Showing 1 to 10 of 100 entries

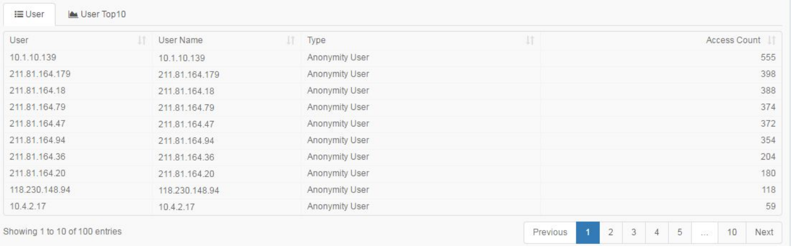
User	User Name	Type	Access Count
10.1.10.139	10.1.10.139	Anonymity User	555
211.81.164.179	211.81.164.179	Anonymity User	398
211.81.164.18	211.81.164.18	Anonymity User	388
211.81.164.79	211.81.164.79	Anonymity User	374
211.81.164.47	211.81.164.47	Anonymity User	372
211.81.164.94	211.81.164.94	Anonymity User	354
211.81.164.36	211.81.164.36	Anonymity User	204
211.81.164.20	211.81.164.20	Anonymity User	180
118.230.148.94	118.230.148.94	Anonymity User	118
10.4.2.17	10.4.2.17	Anonymity User	59

Showing 1 to 10 of 100 entries

2. Click **URL**, **URL category**, and **User** sort statistics by different criteria.

3. Select **Past 1 hour**, **Past 1 day**, **Past 7 days**, or **Past 30 days** to display the statistics collected during the corresponding period.

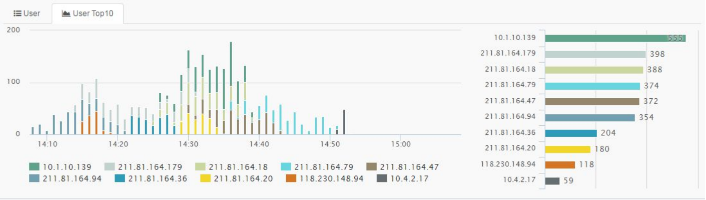
4. Click a URL in the URL ranklist to display the distribution of the URL's access traffic among all the user IP addresses.
   User access volume list:



User	User Name	Type	Access Count
10.1.10.139	10.1.10.139	Anonymity User	555
211.81.164.179	211.81.164.179	Anonymity User	398
211.81.164.18	211.81.164.18	Anonymity User	388
211.81.164.79	211.81.164.79	Anonymity User	374
211.81.164.47	211.81.164.47	Anonymity User	372
211.81.164.94	211.81.164.94	Anonymity User	354
211.81.164.36	211.81.164.36	Anonymity User	204
211.81.164.20	211.81.164.20	Anonymity User	180
118.230.148.94	118.230.148.94	Anonymity User	118
10.4.2.17	10.4.2.17	Anonymity User	59

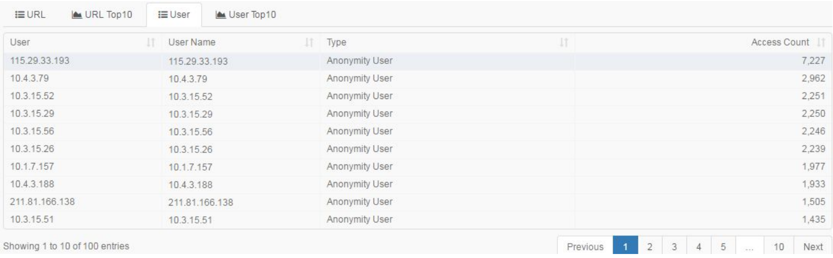
Showing 1 to 10 of 100 entries

User access volume displayed in the forms of a histogram and a bar graph:



5. Click a URL category in the URL category rank list to display the distribution of access traffic among all the user IP addresses and URLs under that category.

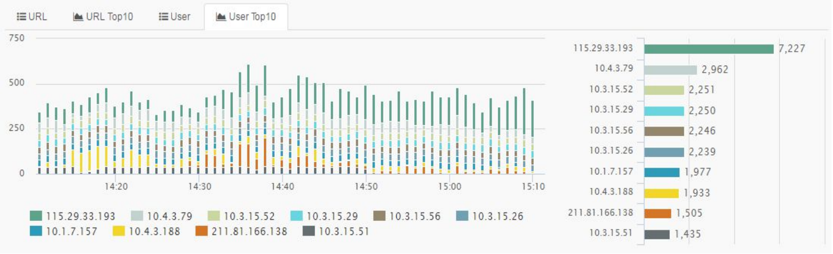
User access volume list:



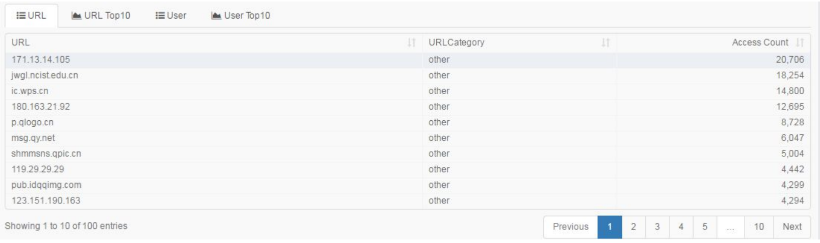
User	User Name	Type	Access Count
115.29.33.193	115.29.33.193	Anonymity User	7,227
10.4.3.79	10.4.3.79	Anonymity User	2,962
10.3.15.52	10.3.15.52	Anonymity User	2,251
10.3.15.29	10.3.15.29	Anonymity User	2,250
10.3.15.56	10.3.15.56	Anonymity User	2,246
10.3.15.26	10.3.15.26	Anonymity User	2,239
10.1.7.157	10.1.7.157	Anonymity User	1,977
10.4.3.188	10.4.3.188	Anonymity User	1,933
211.81.166.138	211.81.166.138	Anonymity User	1,505
10.3.15.51	10.3.15.51	Anonymity User	1,435

Showing 1 to 10 of 100 entries

User access volume displayed in the forms of a histogram and a bar graph:



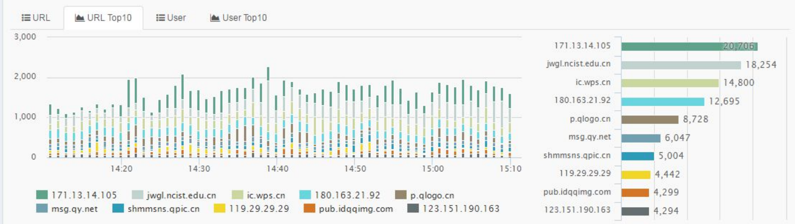
URL access volume list:



URL	URLCategory	Access Count
171.13.14.105	other	20,706
jwgl.ncist.edu.cn	other	18,254
ic.wps.cn	other	14,800
180.163.21.92	other	12,695
p.qlogo.cn	other	8,728
msg.qy.net	other	6,047
shmmsns.qpic.cn	other	5,004
119.29.29.29	other	4,442
pub.idqqimg.com	other	4,299
123.151.190.163	other	4,294

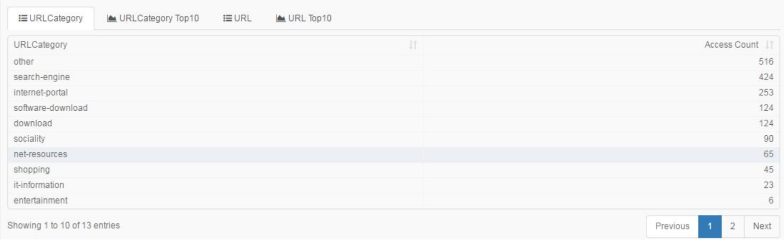
Showing 1 to 10 of 100 entries

URL access volume displayed in the forms of a histogram and a bar graph:



6. Click a user in the user ranklist to display the distribution of the user's access traffic among URLs and URL categories.

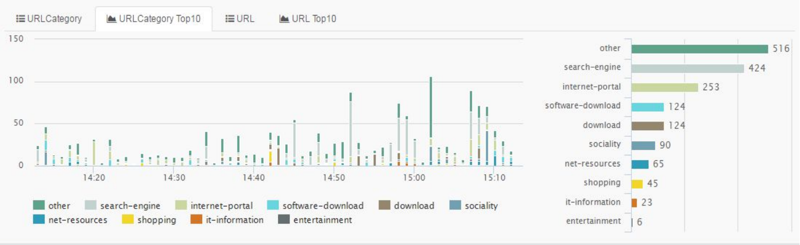
URL category access volume list:



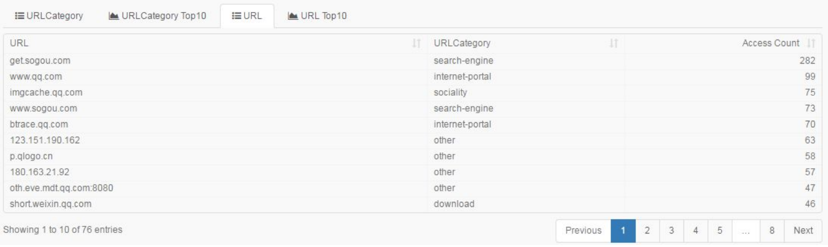
URLCategory	Access Count
other	516
search-engine	424
internet-portal	253
software-download	124
download	124
sociality	90
net-resources	65
shopping	45
it-information	23
entertainment	6

Showing 1 to 10 of 13 entries

URL category access volume displayed in the forms of a histogram and a bar graph:



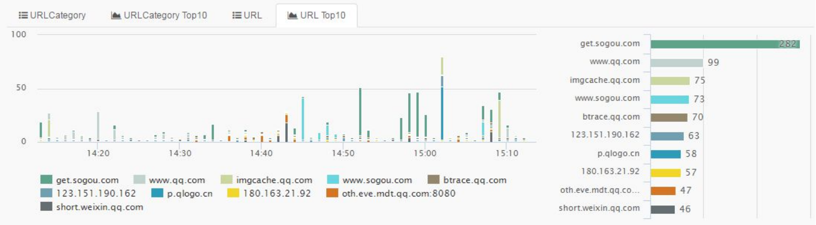
URL access volume list:



URL	URLCategory	Access Count
get.sogou.com	search-engine	282
www.qq.com	internet-portal	99
imgcache.qq.com	sociality	75
www.sogou.com	search-engine	73
btrace.qq.com	internet-portal	70
123.151.190.162	other	63
p.qlogo.cn	other	58
180.163.21.92	other	57
oth.eve.mdt.qq.com:8080	other	47
short.weixin.qq.com	download	46

Showing 1 to 10 of 76 entries

URL access volume displayed in the forms of a histogram and a bar graph:



11 Session Monitoring

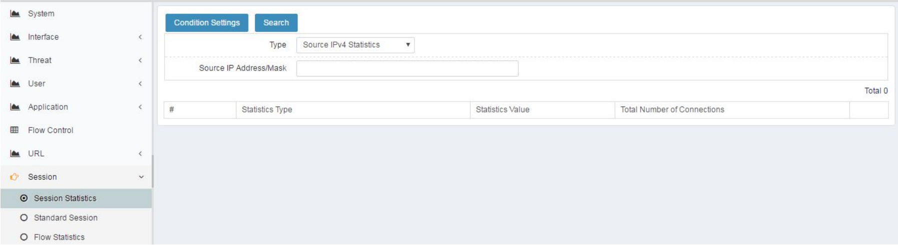
11.1 Overview

The session monitoring function allows you to monitor and collect statistics on a firewall's connections. You can query the statistics based on custom parameters. The session monitoring function divides connections into full connections and half-open connections. When a new connection receives no response for a long time, it will remain in a half-open connection state until it is answered correctly.

11.2 Session Statistics

Procedure:

1. Choose **Monitor** > **Session** > **Session statistics** to display the current number of connections in the system. The connections can be sorted by **Source IPv4 address**, **Source IPv6 address**, **Destination IPv4 address**, **Destination IPv6 address**, **Destination port**, or other criteria. The number of connections is sorted in descending order. A maximum of the first 50 connections are displayed.



Type: Source IPv4 Statistics

Source IP Address/Mask:

Total 0

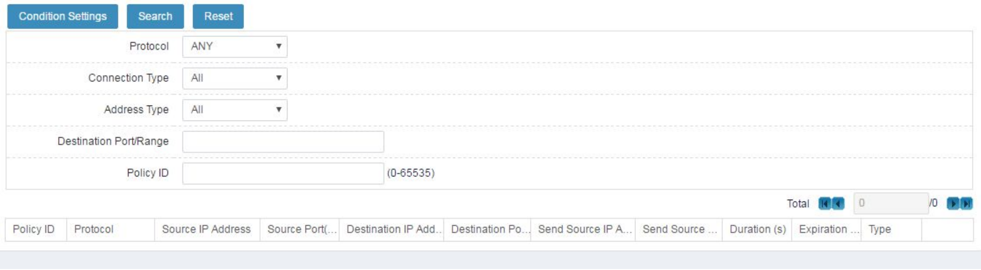
#	Statistics Type	Statistics Value	Total Number of Connections	

2. In **Type**, select **Source IPv4 address**, **Source IPv6 address**, **Destination IPv4 address**, **Destination IPv6 address**, or **Destination port**. By default, **Source IPv4 address** is selected.
3. In **Source IP address/Mask**, enter an IP address/range/mask or a port number/range. You can also leave this parameter empty.
4. Click Search to collect statistics.
5. After the results are displayed, you can click to display connection details on the **Standard session** page.

11.3 Standard Session

Procedure:

1. Choose **Monitoring** > **Session** > **Standard session**.



Protocol	ANY
Connection Type	All
Address Type	All
Destination Port/Range	
Policy ID	(0-65535)

Total 0 /0

Policy ID	Protocol	Source IP Address	Source Port(...	Destination IP Add...	Destination Po...	Send Source IP A...	Send Source ...	Duration (s)	Expiration ...	Type

2. Select a protocol, a connection type, and an address type from the drop-down lists. Enter the source IP address, destination IP address, and service port. The default value is **ANY**.

3. Click Search to search for connections that meet the

conditions. Note: The Tx IP address/mask is the address converted by

NAT.

11.4 Configuration Examples

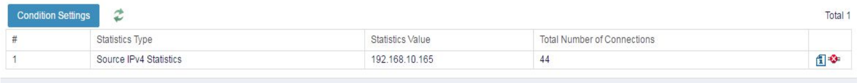
Example 1: Source host connections

Description:

Display the number of connections of the source IP address.

Procedure:

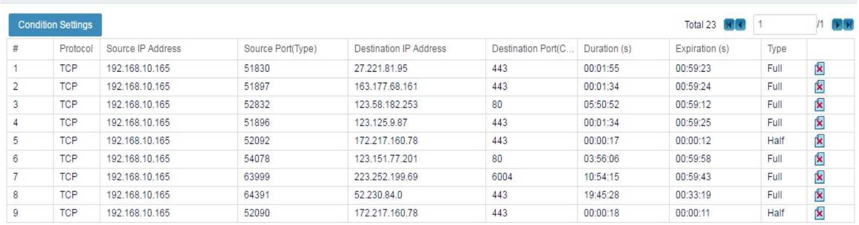
1. Select **Source IPv4 address** for **Type**.
2. Enter an IP address.
3. Click Search.



Condition Settings | Total 1

#	Statistics Type	Statistics Value	Total Number of Connections	
1	Source IPv4 Statistics	192.168.10.165	44	☒

Click to show details.



Condition Settings | Total 23 | 1 /1

#	Protocol	Source IP Address	Source Port(Type)	Destination IP Address	Destination Port(C...	Duration (s)	Expiration (s)	Type	
1	TCP	192.168.10.165	51830	27.221.81.95	443	00:01:55	00:59:23	Full	☒
2	TCP	192.168.10.165	51897	163.177.68.161	443	00:01:34	00:59:24	Full	☒
3	TCP	192.168.10.165	52832	123.58.182.253	80	05:50:52	00:59:12	Full	☒
4	TCP	192.168.10.165	51896	123.125.9.87	443	00:01:34	00:59:25	Full	☒
5	TCP	192.168.10.165	52092	172.217.160.78	443	00:00:17	00:00:12	Half	☒
6	TCP	192.168.10.165	54078	123.151.77.201	80	03:56:06	00:59:58	Full	☒
7	TCP	192.168.10.165	63999	223.252.199.69	6004	10:54:15	00:59:43	Full	☒
8	TCP	192.168.10.165	64391	52.230.84.0	443	19:45:28	00:33:19	Full	☒
9	TCP	192.168.10.165	52090	172.217.160.78	443	00:00:18	00:00:11	Half	☒

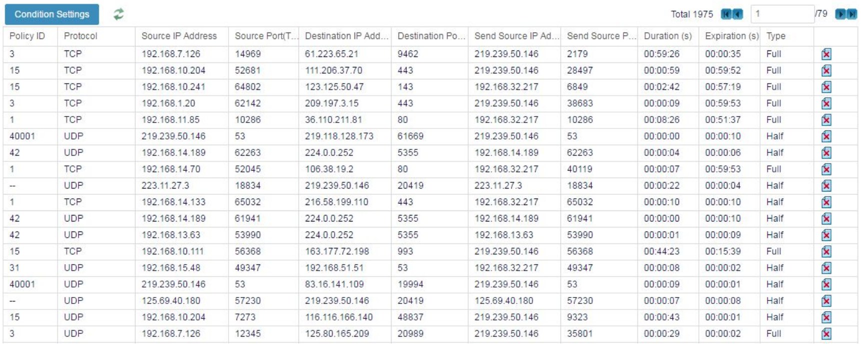
Example 2: Standard session connections

Description:

Display the number of standard session connections after NAT.

Procedure:

1. Select **ANY** for **Protocol**.
2. Select **ANY** for **Connection type**.
3. Select **IPv4** for **Address type**.
4. Keep the default source IP address/mask.
5. Set the Tx IP address/mask to the address converted by NAT.
6. Keep the default destination IP address/mask.
7. Keep the default destination port number/range.
8. Click Search.



Condition Settings | Total 1975 | 1 /79

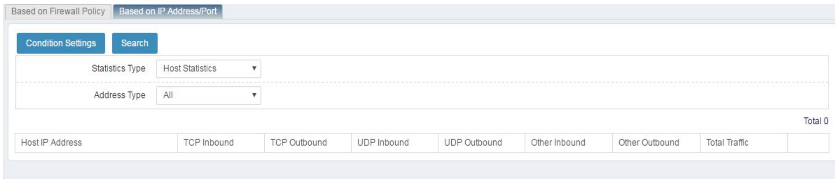
Policy ID	Protocol	Source IP Address	Source Port(T...	Destination IP Add...	Destination Po...	Send Source IP Ad...	Send Source P...	Duration (s)	Expiration (s)	Type	
3	TCP	192.168.7.126	14969	61.223.65.21	9462	219.239.50.146	2179	00:59:26	00:00:35	Full	☒
15	TCP	192.168.10.204	52681	111.206.37.70	443	219.239.50.146	28497	00:00:59	00:59:52	Full	☒
15	TCP	192.168.10.241	64802	123.125.50.47	143	192.168.32.217	6849	00:02:42	00:57:19	Full	☒
3	TCP	192.168.1.20	62142	209.197.3.15	443	219.239.50.146	38683	00:00:09	00:59:53	Full	☒
1	TCP	192.168.11.85	10286	36.110.211.81	80	192.168.32.217	10286	00:08:26	00:51:37	Full	☒
40001	UDP	219.239.50.146	53	219.118.128.173	61669	219.239.50.146	53	00:00:00	00:00:10	Half	☒
42	UDP	192.168.14.189	62263	224.0.0.252	5355	192.168.14.189	62263	00:00:04	00:00:06	Half	☒
1	TCP	192.168.14.70	52045	106.38.19.2	80	192.168.32.217	40119	00:00:07	00:59:53	Full	☒
--	UDP	223.11.27.3	18834	219.239.50.146	20419	223.11.27.3	18834	00:00:22	00:00:04	Half	☒
1	TCP	192.168.14.133	65032	216.58.199.110	443	192.168.32.217	65032	00:00:10	00:00:10	Half	☒
42	UDP	192.168.14.189	61941	224.0.0.252	5355	192.168.14.189	61941	00:00:00	00:00:10	Half	☒
42	UDP	192.168.13.63	53990	224.0.0.252	5355	192.168.13.63	53990	00:00:01	00:00:09	Half	☒
15	TCP	192.168.10.111	56368	163.177.72.198	993	219.239.50.146	56368	00:44:23	00:15:39	Full	☒
31	UDP	192.168.15.48	49347	192.168.51.51	53	192.168.32.217	49347	00:00:08	00:00:02	Half	☒
40001	UDP	219.239.50.146	53	83.16.141.109	19994	219.239.50.146	53	00:00:09	00:00:01	Half	☒
--	UDP	125.69.40.180	57230	219.239.50.146	20419	125.69.40.180	57230	00:00:07	00:00:08	Half	☒
15	UDP	192.168.10.204	7273	116.116.166.140	48837	219.239.50.146	9323	00:00:43	00:00:01	Half	☒
3	UDP	192.168.7.126	12345	125.80.165.209	20989	219.239.50.146	35801	00:00:29	00:00:02	Full	☒

12 Traffic Statistics

12.1 Traffic Statistics by IP Address and Port

You can query traffic statistics sorted by IP address and port.

Choose **Monitor** > **Session** > **Traffic statistics** > **IP address/Port**. The following page appears. Set search criteria to query traffic statistics.



Statistics Type: Host Statistics

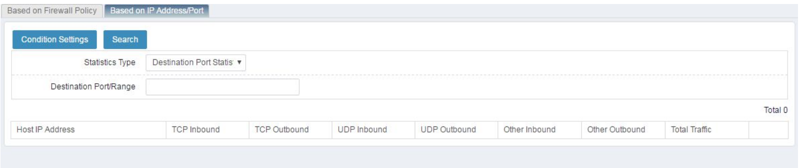
Address Type: All

Total 0

Host IP Address	TCP Inbound	TCP Outbound	UDP Inbound	UDP Outbound	Other Inbound	Other Outbound	Total Traffic	

Statistical type: The options are **Host** and **Destination port**.

Address type: The options are **IPv4** and **IPv6**.



Statistics Type: Destination Port Statis

Destination Port/Range:

Total 0

Host IP Address	TCP Inbound	TCP Outbound	UDP Inbound	UDP Outbound	Other Inbound	Other Outbound	Total Traffic	

Destination port/range: Enter the destination port or port range, for example, 100-2410.

Key fields in the list:

Host IP address: Statistical host address

TCP in: TCP traffic in the reverse direction

TCP out: TCP traffic in the forward direction

UDP in: UDP traffic in the reverse direction

UDP out: UDP traffic in the forward direction

Others in: Traffic of other protocol types in the reverse direction

Others out: Traffic of other protocol types in the forward direction

Total traffic: Total traffic of all protocol types in the forward and reverse directions

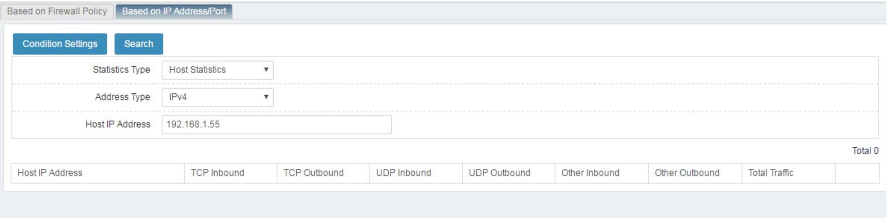
12.2 Configuration Example

Description:

Configure filter criteria to query traffic statistics.

Procedure:

1. Choose **Monitor** > **Session** > **Traffic statistics** > **IP address/Port**. Set filter criteria.



Statistics Type: Host Statistics

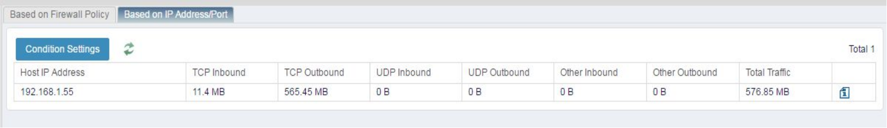
Address Type: IPv4

Host IP Address: 192.168.1.55

Total 0

Host IP Address	TCP Inbound	TCP Outbound	UDP Inbound	UDP Outbound	Other Inbound	Other Outbound	Total Traffic

2. Click **Search** to query the host traffic statistics.



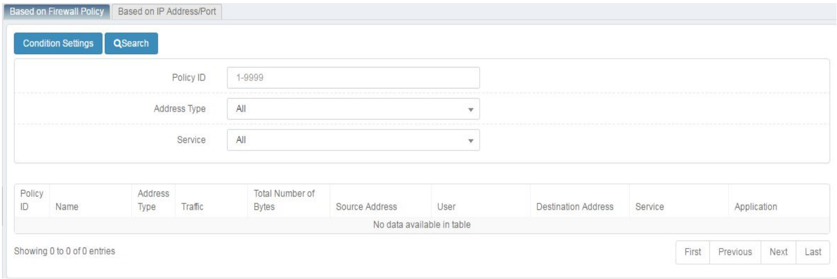
Total 1

Host IP Address	TCP Inbound	TCP Outbound	UDP Inbound	UDP Outbound	Other Inbound	Other Outbound	Total Traffic	
192.168.1.55	11.4 MB	565.45 MB	0 B	0 B	0 B	0 B	576.85 MB	

12.3 Traffic Statistics by Policy

You can collect traffic statistics on the firewall policies enabled with this function.

Choose **Monitor** > **Session** > **Traffic statistics** > **Firewall policy**. The following page appears. Set search criteria to query traffic statistics.



Policy ID: 1-9999

Address Type: All

Service: All

Policy ID	Name	Address Type	Traffic	Total Number of Bytes	Source Address	User	Destination Address	Service	Application
No data available in table									

Showing 0 to 0 of 0 entries

Policy ID: Enter the ID of the statistical policy.

Address type: Select **IPv4** or **IPv6**.

Source address: Enter the source address or the name keyword of the source address object.

Destination address: Enter the destination address or the name keyword of the destination address object.

Service: Select the policy service type.

Key fields in the list:

Policy ID: ID of the statistical policy

Name: Name of the statistical policy

Address type: Address type of the policy

Traffic: Real-time rate of the traffic filtered by the policy

Total bytes: Total traffic filtered by the policy, in bytes

Source address: Source address object of the policy

User: User object of the policy

Destination address: Destination address object of the policy

Service: Service object of the policy

Application: Application object of the policy

⚠ Notice

1. You must enable traffic statistics for the target policy and
2. Ensure that the entered search criteria are the same as the policy settings.

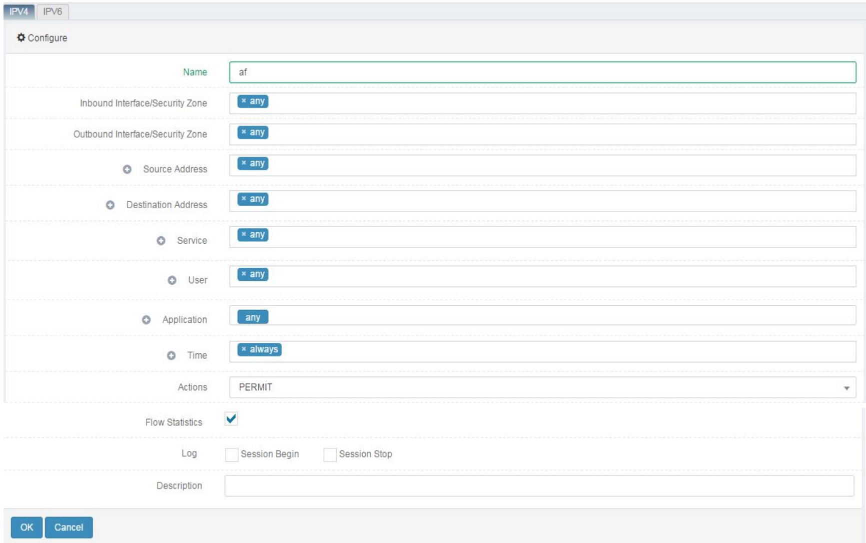
12.4 Configuration Example

Description:

Configure traffic statistics for firewall policies and display statistic results.

Procedure:

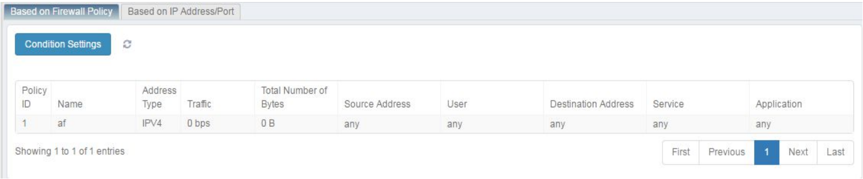
1. Choose **Policy** > **Firewall** > **Policy** and enable policy-based traffic statistics.



Name	af
Inbound Interface/Security Zone	× any
Outbound Interface/Security Zone	× any
Source Address	× any
Destination Address	× any
Service	× any
User	× any
Application	any
Time	× always
Actions	PERMIT
Flow Statistics	☑
Log	□ Session Begin □ Session Stop
Description	

Note: Only firewall policies of the permit type support traffic statistics.

2. Choose **Monitor** > **Session** > **Traffic statistics** > **Firewall policy**. Set filter criteria to query the policy-based traffic statistics.



Policy ID	Name	Address Type	Traffic	Total Number of Bytes	Source Address	User	Destination Address	Service	Application
1	af	IPV4	0 bps	0 B	any	any	any	any	any

Showing 1 to 1 of 1 entries

13 Interface

13.1 Overview

RAVEN 5000 firewalls support the following network interface management: physical interface configuration and management, VLAN configuration and management, and link aggregation configuration and management.

Physical interface configuration and management mainly involves the configuration of Ethernet interface attributes.

VLAN configuration involves creating a VLAN and adding member interfaces to the VLAN. Two VLAN join modes are supported: tag and untag. The tag mode enables 802.1Q and supports handling of protocol packets, whereas the untag mode only supports handling of untagged Ethernet packets. VLANs support the Spanning Tree Protocol (STP) and can form a spanning tree based on this protocol.

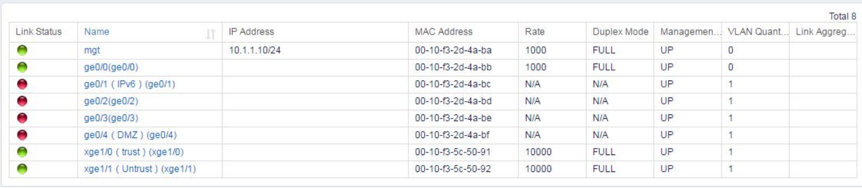
Link aggregation is a method for bundling a group of physical ports into a logical port to increase the bandwidth by balancing outgoing and incoming traffic among the member ports. Dynamic link aggregation can be formed between the local and peer devices based on the Link Aggregation Control Protocol (LACP).

13.2 Physical Interface Configuration

You can query the status of a firewall's physical interfaces and configure the interface management status, negotiation mode, rate, and duplex mode.

Procedure:

1. Choose **Network** > **Interface** > **Physical interface**. A physical interface list appears, as shown in the following figure.



Total 8

Link Status	Name	IP Address	MAC Address	Rate	Duplex Mode	Managemen...	VLAN Quant...	Link Aggreg...
🟢	mgt	10.1.1.10/24	00-10-f3-2d-4a-ba	1000	FULL	UP	0	
🟢	ge0/0(ge0/0)		00-10-f3-2d-4a-bb	1000	FULL	UP	0	
🔴	ge0/1 (IPv6) (ge0/1)		00-10-f3-2d-4a-bc	N/A	N/A	UP	1	
🔴	ge0/2(ge0/2)		00-10-f3-2d-4a-bd	N/A	N/A	UP	1	
🔴	ge0/3(ge0/3)		00-10-f3-2d-4a-be	N/A	N/A	UP	1	
🔴	ge0/4 (DMZ) (ge0/4)		00-10-f3-2d-4a-bf	N/A	N/A	UP	1	
🟢	xge1/0 (trust) (xge1/0)		00-10-f3-5c-50-91	10000	FULL	UP	1	
🟢	xge1/1 (Untrust) (xge1/1)		00-10-f3-5c-50-92	10000	FULL	UP	1	

Link status: Link status of a physical interface. The green color indicates that the interface is up, and red indicates it is down.

Name: Name of the physical interface. **mgt** is the management interface, **ge X/X** is a gigabit interface, and **xge X/X** is a 10-GB interface.

IP address: IP address or mask of the physical interface.

MAC address: MAC address of the physical interface.

Rate: Actual rate of the physical interface, in Mbps.

Duplex mode: A physical interface may be full-duplex or half-duplex.

Management status: Manual management status of the physical interface, which may be **UP** or **DOWN**.

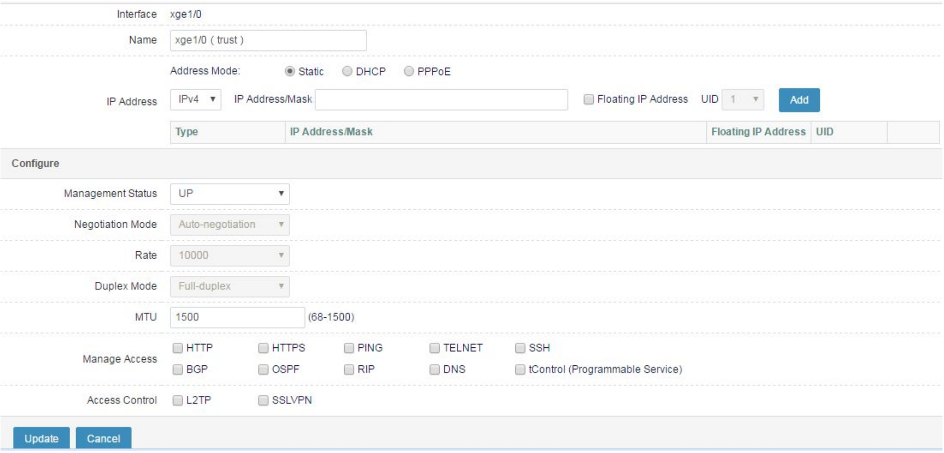
VLANs: Number of VLANs to which the physical interface belongs.

Link aggregation: Link aggregation group (LAG) to which the physical interface belongs, which is identified as tvi X by the firewall.

Note

A physical interface can join multiple VLANs in tag mode.

2. Click an interface in the **Name** column to configure the interface, as shown in the following figure.



Interface xge1/0

Name xge1/0 (trust)

IP Address
Address Mode: ● Static ○ DHCP ○ PPPoE
IPv4 ▾ IP Address/Mask □ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID	

Configure

Management Status UP ▾

Negotiation Mode Auto-negotiation ▾

Rate 10000 ▾

Duplex Mode Full-duplex ▾

MTU 1500 (68-1500)

Manage Access □ HTTP □ HTTPS □ PING □ TELNET □ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)

Access Control □ L2TP □ SSLVPN

Update Cancel

Basic attributes

Interface: Name of the physical interface. **mgt** is the management interface, **ge X/X** is a gigabit interface, and **xge X/X** is a 10-GB interface.

Name: Alias of the physical interface.

Manually specify IP address: Set the IP address of the physical interface manually.

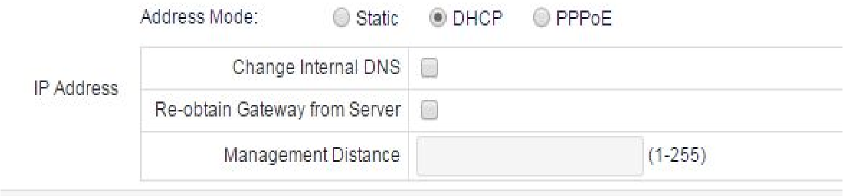
IP address/Mask: IP address of the physical interface. You can select **IPv4** or

IPv6, and enter an IP address and click **Add**.

Floating IP address: Whether the IP address of the physical interface is a floating IP address.

UID: ID of the HA unit.

DHCP (automatically obtain IP address): Obtain the IP address of the physical interface over DHCP.



Address Mode: ○ Static ● DHCP ○ PPPoE

IP Address		
	Change Internal DNS	□
	Re-obtain Gateway from Server	□
	Management Distance	(1-255)

Change internal DNS: Use the DNS obtained from the DHCP server as the local DNS.

Re-obtain gateway from server: Add a default DHCP route and obtain a gateway from the DHCP server.

Management distance: Management distance of the default route obtained over DHCP.

Configuration

Management status: The options are **UP** and **DOWN**, which indicate enabling and disabling the physical interface.

Negotiation mode: The options are **Auto negotiation** and **Non-auto negotiation**.

Rate: Negotiated rate of the physical interface, in Mbps. The options are **1000**, **100**, and **10**.

Duplex mode: A physical interface may be full-duplex or half-duplex.

MTU: Maximum transmission unit (MTU) of the physical interface. The value ranges from 68 to 1500.

Management access: Type of service accessible from the interface address.

> **HTTP**: Allow you to access and manage the firewall from the interface address over HTTP.
>
> **HTTPS**: Allow you to access and manage the firewall from the interface address over HTTPS.
>
> **PING**: Allow the interface address to respond to ping requests.
>
> **TELNET**: Allow you to access and manage the firewall from the interface address over Telnet.
>
> **SSH**: Allow you to access and manage the firewall from the interface address over SSH.

BGP: Allow access to the Border Gateway Protocol (BGP) service provided by the firewall from the interface address.

OSPF: Allow access to the Open Shortest Path First (OSPF) service provided by the firewall from the interface address.

RIP: Allow access to the Routing Information Protocol (RIP) service provided by the firewall from the interface address.

DNS: Allow access to the DNS service provided by the firewall from the interface address.

tControl: Allow access to the programmable service provided by the firewall from the interface address.

Access control: Check this box to apply the Layer 2 Tunneling Protocol (L2TP) to the physical interface.

Note

Rate and **Duplex mode** are configurable only when **Negotiation mode** is set to **Non-auto negotiation**. When the physical interface is an optical interface, **Negotiation mode** is grayed out.

Click **Update** to apply the settings to the physical interface.

13.3 VLAN Configuration

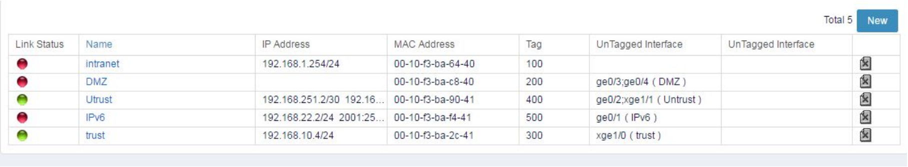
The devices in a LAN can be allocated to independent groups based on ports. The devices in the same group can communicate with each other freely, whereas the devices in different groups need to implement Layer-3 routing for communication. Those groups in the LAN are called VLANs. Two VLAN join modes are supported: tag and untag. The tag mode enables 802.1Q and supports handling of protocol packets, whereas the untag mode only supports handling of untagged Ethernet packets.

VLANs support STP, which applies to a loop network to block some undesirable redundant paths through certain algorithms and prune a loop network into a loop-free tree network to prevent the generation and infinite loop of packets.

VLAN interfaces support the transparent bridge function, whereby VLAN tags are transparently transmitted through commands.

13.3.1 Adding a VLAN

1. Choose **Network** > **Interface** > **VLAN**. The following page appears.



Total 5 New

Link Status	Name	IP Address	MAC Address	Tag	UnTagged Interface	UnTagged Interface	
🔴	intranet	192.168.1.254/24	00-10-f3-ba-64-40	100			☒
🔴	DMZ		00-10-f3-ba-c8-40	200	ge0/3;ge0/4 (DMZ)		☒
🟢	Utrust	192.168.251.2/30 192.16...	00-10-f3-ba-90-41	400	ge0/2;xge1/1 (Untrust)		☒
🔴	IPv6	192.168.22.2/24 2001:25...	00-10-f3-ba-f4-41	500	ge0/1 (IPv6)		☒
🟢	trust	192.168.10.4/24	00-10-f3-ba-2c-41	300	xge1/0 (trust)		☒

Link status: Status of a VLAN. **Name**: Name of the VLAN.

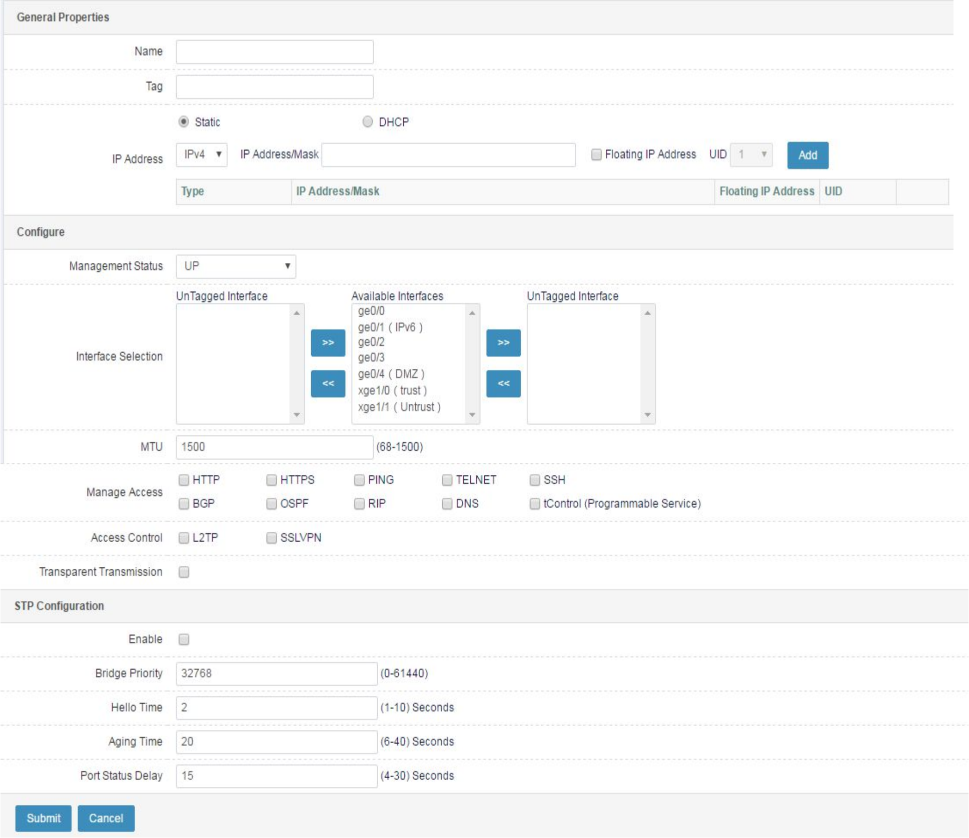
IP address: IP address or mask of the VLAN.

Tag: ID of the VLAN.

Untagged interfaces: Untagged physical interfaces in the VLAN.

Tagged interfaces: Tagged physical interfaces in the VLAN, with 802.1Q enabled.

2. Click **New** to create a VLAN. The following page appears.



General Properties

Name

Tag

IP Address: ● Static ○ DHCP

IPv4 ▾ IP Address/Mask ☐ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID	

Configure

Management Status: UP ▾

Interface Selection

UnTagged Interface >> << Available Interfaces: ge0/0, ge0/1 (IPv6), ge0/2, ge0/3, ge0/4 (DMZ), xge1/0 (trust), xge1/1 (Untrust) >> << UnTagged Interface

MTU: 1500 (68-1500)

Manage Access: ☐ HTTP ☐ HTTPS ☐ PING ☐ TELNET ☐ SSH ☐ BGP ☐ OSPF ☐ RIP ☐ DNS ☐ tControl (Programmable Service)

Access Control: ☐ L2TP ☐ SSLVPN

Transparent Transmission ☐

STP Configuration

Enable ☐

Bridge Priority: 32768 (0-61440)

Hello Time: 2 (1-10) Seconds

Aging Time: 20 (6-40) Seconds

Port Status Delay: 15 (4-30) Seconds

Submit Cancel

Basic attributes

Name: Name of the VLAN.

Tag: ID of the VLAN.

Manually specify IP address: Set the IP address of the VLAN interface manually.

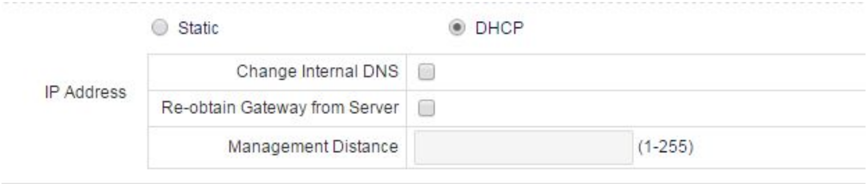
IP address/Mask: IP address of the physical interface. You can select **IPv4** or

IPv6, and enter an IP address and click **Add**.

Floating IP address: Whether the IP address is a floating IP address.

UID: ID of the HA unit.

DHCP (automatically obtain IP address): Obtain the IP address of the interface over DHCP.



IP Address

○ Static ● DHCP

Change Internal DNS □

Re-obtain Gateway from Server □

Management Distance (1-255)

Change internal DNS: Use the DNS obtained from the DHCP server as the local

DNS.

Re-obtain gateway from server: Add a default DHCP route and

obtain a gateway from the DHCP server.

Management distance: Management distance of the default route obtained over DHCP.

Access control: Check this box to apply L2TP to the interface.

Transparent transmission: Enable the VLAN to transparently transmit all tags. Before you enable this function, add all the related interfaces to the VLAN in untag mode.

Configuration

Management status: The options are **UP** and **DOWN**, which indicate enabling and disabling the VLAN.

Available interfaces: Physical interfaces of the firewall that can be added to the VLAN.

UnTagged interfaces: Physical interfaces to be added to the VLAN in untag mode.

Tagged interfaces: Physical interfaces to be added to the VLAN in tag mode, with 802.1Q enabled.

MTU: MTU of the VLAN. The value ranges from 68 to 1500.

Management access: Type of service accessible from the interface address.

HTTP: Allow you to access and manage the firewall from the interface address over HTTP.

HTTPS: Allow you to access and manage the firewall from the interface address over HTTPS.

PING: Allow the interface address to respond to ping requests.

TELNET: Allow you to access and manage the firewall from the interface address over Telnet.

SSH: Allow you to access and manage the firewall from the interface address over SSH.

BGP: Allow access to the BGP service provided by the firewall from the interface address.

OSPF: Allow access to the OSPF service provided by the firewall from the interface address.

RIP: Allow access to the RIP service provided by the firewall from the interface address.**DNS**: Allow access to the DNS service provided by the firewall from the interface address.

tControl: Allow access to the programmable service provided by the firewall from the interface address.

3. Complete the STP configuration for the VLAN.

Enable: Check this box to enable STP in the VLAN.

Bridge priority: Bridge priority of the VLAN in the STP tree. The value ranges from 0 to 61440.

Hello time: Interval at which the VLAN sends STP bridge protocol data unit (BPDU) packets. The value ranges from 1 to 10, in seconds.

Aging time: The topology is deemed to change if the STP status remains nonupdated for the aging time. The value ranges from 6 to 40, in seconds.

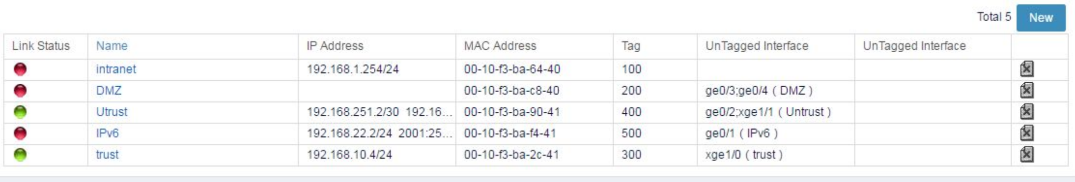
Port status delay: Delay before the port status changes. The value ranges from 4 to 30, in seconds.

Note

Specifically, the delay is the interval at which the port status changes from Listening to Learning to Forwarding after STP is enabled.

13.3.2 Modifying a VLAN

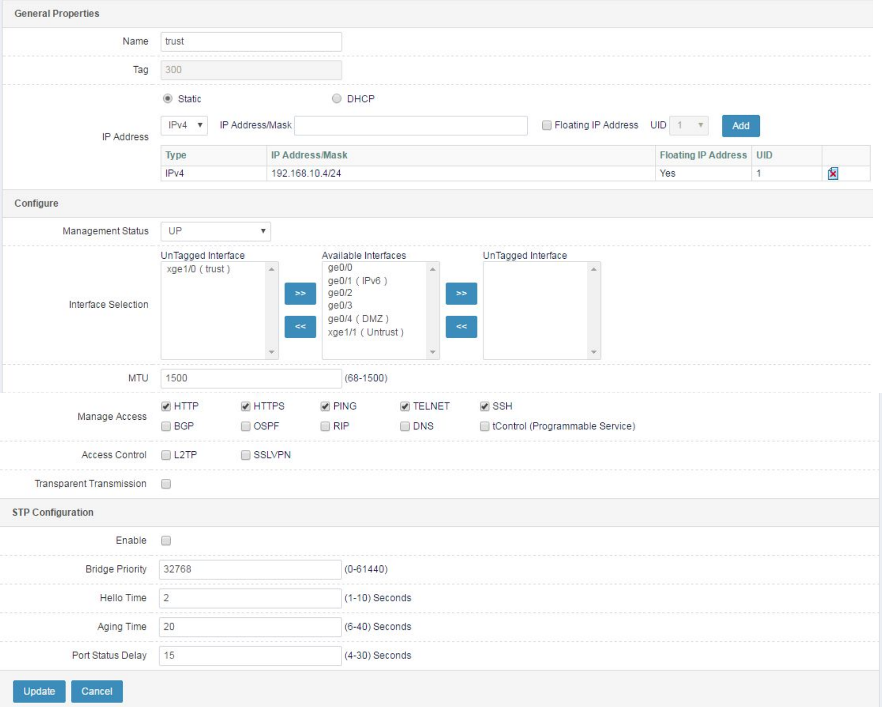
1. Choose **Network** > **Interface** > **VLAN**. The following page appears.



Total 5 New

Link Status	Name	IP Address	MAC Address	Tag	UnTagged Interface	UnTagged Interface	
●	intranet	192.168.1.254/24	00-10-f3-ba-64-40	100			☒
●	DMZ		00-10-f3-ba-c8-40	200	ge0/3;ge0/4 (DMZ)		☒
●	Utrust	192.168.251.2/30 192.16...	00-10-f3-ba-90-41	400	ge0/2;xge1/1 (Untrust)		☒
●	IPv6	192.168.22.2/24 2001:25...	00-10-f3-ba-f4-41	500	ge0/1 (IPv6)		☒
●	trust	192.168.10.4/24	00-10-f3-ba-2c-41	300	xge1/0 (trust)		☒

2. Click a VLAN in the **Name** column. The following page appears.



General Properties

Name	trust
Tag	300
IP Address	● Static ○ DHCP IPv4 ▾ IP Address/Mask □ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID	
IPv4	192.168.10.4/24	Yes	1	☒

Configure

Management Status	UP ▾
Interface Selection	UnTagged Interface: xge1/0 (trust) Available Interfaces: ge0/0, ge0/1 (IPv6), ge0/2, ge0/3, ge0/4 (DMZ), xge1/1 (Untrust) UnTagged Interface:
MTU	1500 (68-1500)
Manage Access	☑ HTTP ☑ HTTPS ☑ PING ☑ TELNET ☑ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)
Access Control	□ L2TP □ SSLVPN
Transparent Transmission	□

STP Configuration

Enable	□
Bridge Priority	32768 (0-61440)
Hello Time	2 (1-10) Seconds
Aging Time	20 (6-40) Seconds
Port Status Delay	15 (4-30) Seconds

You can modify the IP address, management status, untagged interfaces, tagged interfaces, MTU, STP configuration, and other information of the VLAN.

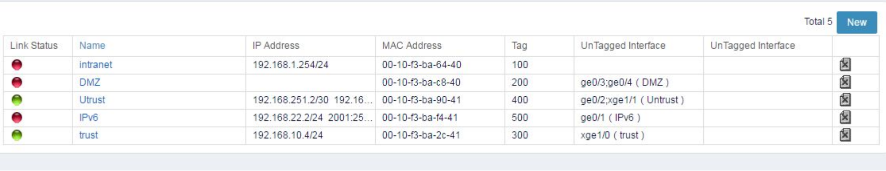
3. Click **Update** to apply the modification.

Note

The name and tag value of the VLAN cannot be modified.

13.3.3 Deleting a VLAN

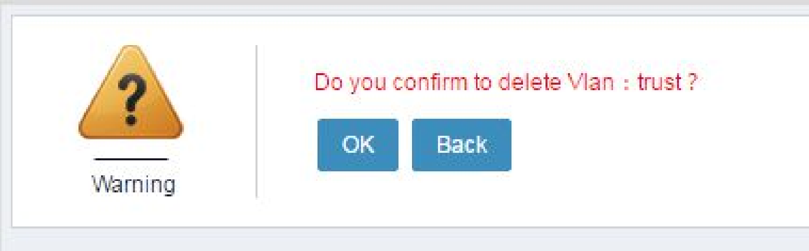
1. Choose **Network** > **Interface** > **VLAN**. The following page appears.



Total 5

Link Status	Name	IP Address	MAC Address	Tag	UnTagged Interface	UnTagged Interface	
🔴	intranet	192.168.1.254/24	00-10-f3-ba-64-40	100			☒
🔴	DMZ		00-10-f3-ba-c8-40	200	ge0/3;ge0/4 (DMZ)		☒
🟢	Utrust	192.168.251.2/30 192.16...	00-10-f3-ba-90-41	400	ge0/2;xge1/1 (Untrust)		☒
🔴	IPv6	192.168.22.2/24 2001:25...	00-10-f3-ba-f4-41	500	ge0/1 (IPv6)		☒
🟢	trust	192.168.10.4/24	00-10-f3-ba-2c-41	300	xge1/0 (trust)		☒

2. Click ☒ next to a VLAN you want to delete.



Do you confirm to delete Vlan : trust ?

3. Click **OK**.

Note

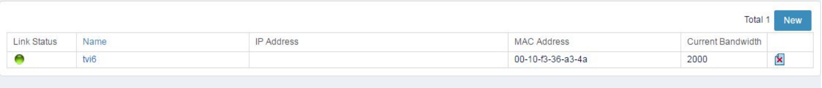
A VLAN referenced by other functions cannot be deleted.

13.4 Link Aggregation Configuration

Link aggregation is a process of aggregating multiple links into a logical network link to increase the capacity and reliability of the communication channels between devices. Link aggregation balances the communication load among links to prevent overload. In many applications, link aggregation offers benefits such as higher reliability, increased bandwidth, and lower costs without the need to update existing devices.

13.4.1 Adding a LAG

1. Choose **Network** > **Interface** > **Link aggregation**. The following page appears.



Link Status	Name	IP Address	MAC Address	Current Bandwidth	
●	tvi6		00-10-f3-36-a3-4a	2000	☒

Link status: Status of a LAG.

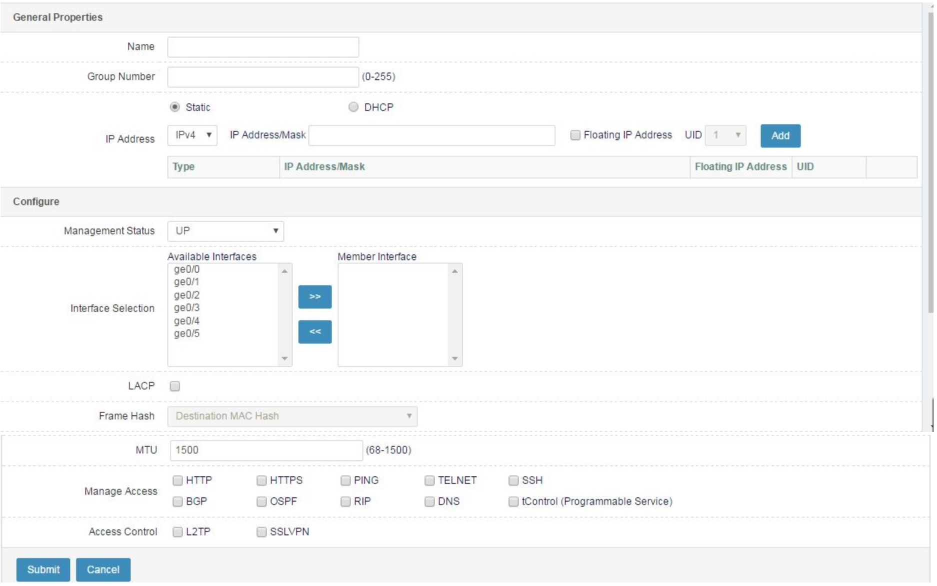
Name: Name of the LAG.

IP address: IP address of the LAG.

MAC address: MAC address of the LAG.

Current bandwidth: Total bandwidth from link aggregation, in M.

2. Click **New** to create a LAG. The following page appears.



General Properties

Name

Group Number (0-255)

IP Address ● Static ○ DHCP

IPv4 ▾ IP Address/Mask □ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID

Configure

Management Status: UP ▾

Interface Selection: Available Interfaces: ge0/0, ge0/1, ge0/2, ge0/3, ge0/4, ge0/5 >> << Member Interface

LACP □

Frame Hash: Destination MAC Hash ▾

MTU: 1500 (68-1500)

Manage Access: □ HTTP □ HTTPS □ PING □ TELNET □ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)

Access Control: □ L2TP □ SSLVPN

Submit Cancel

Basic attributes

Name: Name of the new LAG.

Group ID: ID of the LAG.

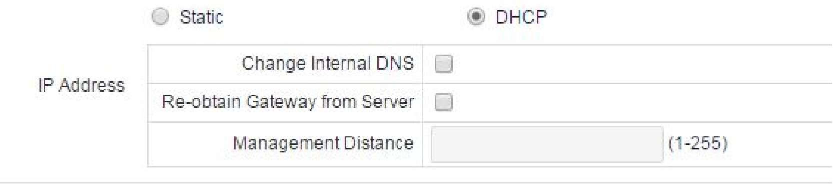
Manually specify IP address: Set the IP address of the interface manually.

IP address/Mask: IP address of the physical interface. You can select **IPv4** or **IPv6**, and enter an IP address and click **Add.**

Floating IP address: Whether the IP address is a floating IP address.

UID: ID of the HA unit.

DHCP (automatically obtain IP address): Obtain the IP address of the interface over DHCP.



IP Address ○ Static ● DHCP

Change Internal DNS □

Re-obtain Gateway from Server □

Management Distance (1-255)

Change internal DNS: Use the DNS obtained from the DHCP server as the local DNS.

Re-obtain gateway from server: Add a default DHCP route and obtain a gateway from the DHCP server.

Management distance: Management distance of the default route obtained over DHCP.

Management status: The options are **UP** and **DOWN**, which indicate enabling and disabling the LAG.

Available interfaces: Physical interfaces of the firewall that can be added to the LAG.

Member interfaces: Physical interfaces added to the LAG.

LACP: Check this box to enable LACP.

Frame hash: Sent data hash method. The options are **Destination MAC address** and **Source/Destination IP address and port**.

MTU: MTU of the LAG. The value ranges from 68 to 1500.

Management access: Type of service provided by the firewall that can be accessed from the LAG address.

> **HTTP**: Allow access to the HTTP service provided by the firewall from the LAG address.
>
> **HTTPS**: Allow access to the HTTPS service provided by the firewall from the LAG address.
>
> **PING**: Allow the LAG address to respond to ping requests.
>
> **TELNET**: Allow telnet to the firewall from the LAG address.
>
> **SSH**: Allow SSH connection to the firewall from the LAG address.
>
> **BGP**: Allow access to the BGP service provided by the firewall from the LAG address.
>
> **OSPF**: Allow access to the OSPF service provided by the firewall from the LAG address.
>
> **RIP**: Allow access to the RIP service provided by the firewall from the LAG address.
>
> **DNS**: Allow access to the DNS service provided by the firewall from the LAG address.
>
> **tControl**: Allow access to the programmable service provided by the firewall from the LAG address.

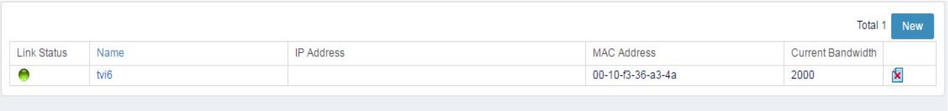
Access control: Check this box to apply L2TP to the interface.

⚠ Notice

When LACP is disabled, sent and received packets are subjected to static round robin. After LACP is enabled, the firewall supports dynamic link aggregation and backup.

13.4.2 Modifying a LAG

1. Choose **Network** > **Interface** > **Link aggregation**. The following page appears.



Link Status	Name	IP Address	MAC Address	Current Bandwidth	
●	tvi6		00-10-f3-36-a3-4a	2000	☒

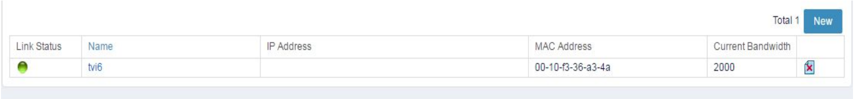
2. Click a LAG.

Modify the IP address, management status, member interfaces, LACP, frame hash, and other information of the LAG.

3. Click **Update** to apply the modification.

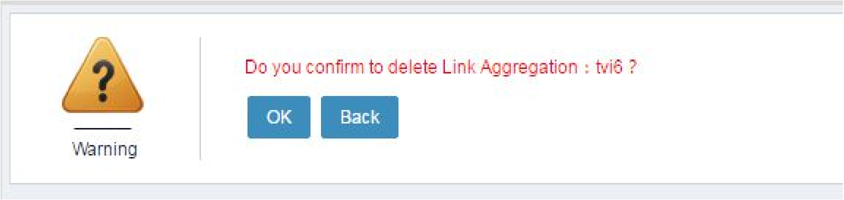
13.4.3 Deleting a LAG

1. Choose **Network** > **Interface** > **Link aggregation**. The following page appears.



Link Status	Name	IP Address	MAC Address	Current Bandwidth	
●	tvi6		00-10-f3-36-a3-4a	2000	☒

2. Click ☒ next to a LAG you want to delete.



Do you confirm to delete Link Aggregation：tvi6 ?

3. Click **OK**.

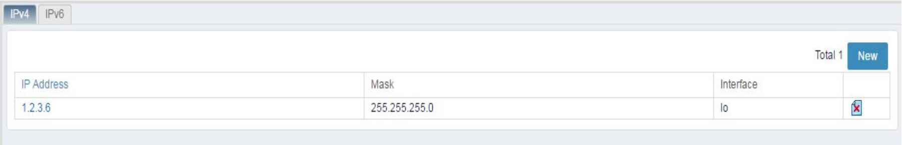
Note

An LAG added to a VLAN cannot be deleted.

13.5 Loopback Interface Configuration

13.5.1 Adding a Loopback Interface

1. Choose **Network** > **Interface** > **Loopback interface**. The following page



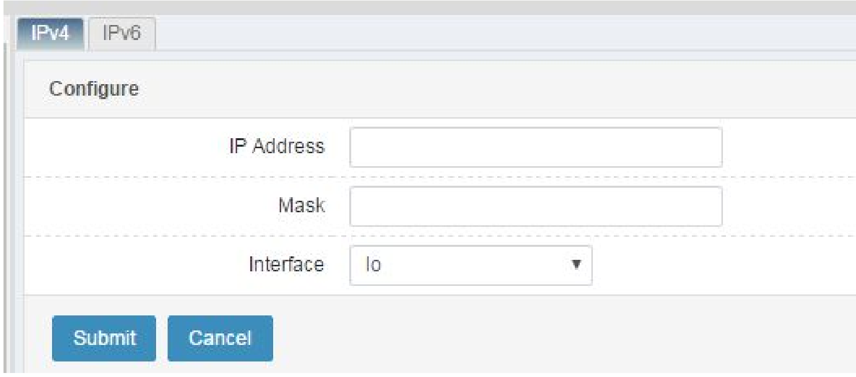
IP Address	Mask	Interface	
1.2.3.6	255.255.255.0	lo	☒

IP address: IP address of a loopback interface.

Mask: Mask of the loopback interface.

Interface: Interface description. **lo** indicates a loopback interface.

2. Click **New** to create a loopback interface in the IPv4 or IPv6 address format.

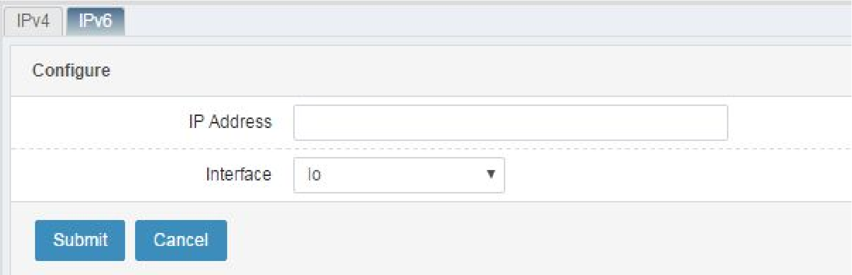


Interface: lo

IP address: IPv4 address of the new loopback interface.

Mask: Mask of the loopback interface.

Interface: Interface description. **lo** indicates a loopback interface.



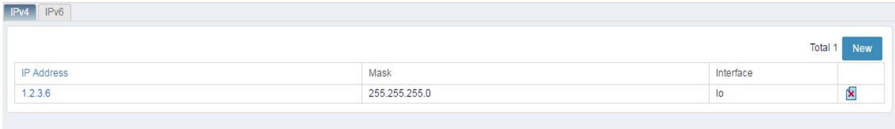
Interface: lo

IP address: IPv6 address of the loopback interface.

Interface: Interface description. **lo** indicates a loopback interface.

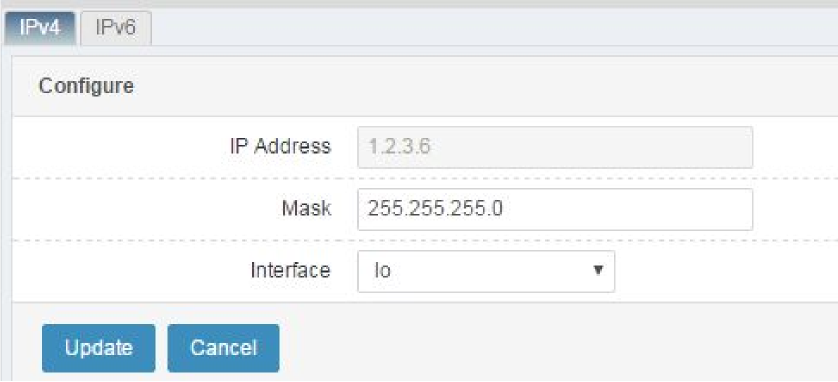
13.5.2 Modifying a Loopback Interface

1. Choose **Network** > **Interface** > **Loopback interface**. The following page appears.



IP Address	Mask	Interface	
1.2.3.6	255.255.255.0	lo	☒

2. a loopback interface.



IP Address: 1.2.3.6

Mask: 255.255.255.0

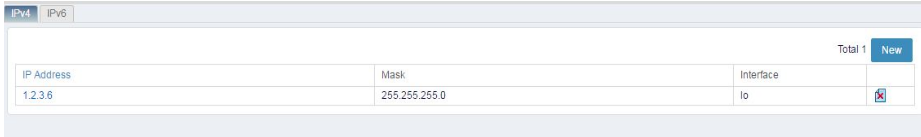
Interface: lo

Modify the mask of the loopback interface.

3.Click **Update** to apply the modification.

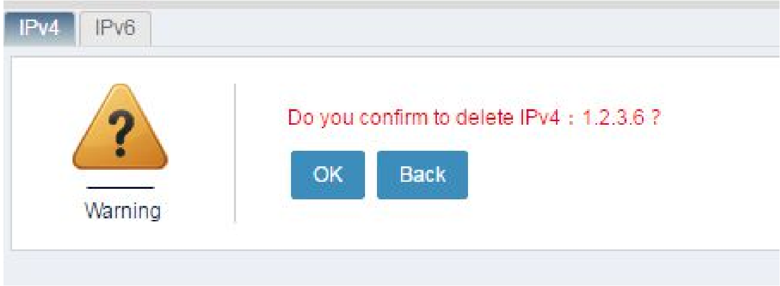
13.5.3 Deleting a Loopback Interface

1. Choose **Network** > **Interface** > **Loopback interface**. The following page appears.



IP Address	Mask	Interface	
1.2.3.6	255.255.255.0	lo	☒

2. Click ☒ next to a loopback interface you want to delete.



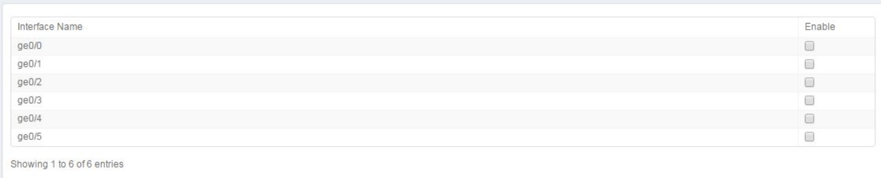
Do you confirm to delete IPv4：1.2.3.6 ?

3. Click **OK**.

13.6 Out-of-path Deployment

Procedure:

Choose **Network** > **Interface** > **Out-of-path**. Check the **Enable** box next to the interface for which you want to enable the out-of-path mode.



Interface Name	Enable
ge0/0	□
ge0/1	□
ge0/2	□
ge0/3	□
ge0/4	□
ge0/5	□

Showing 1 to 6 of 6 entries

13.7 Interface Association

13.7.1 Overview

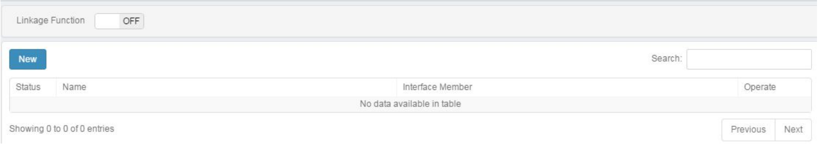
Multiple physical interfaces can be bound by configuring an interface association group to achieve consistent link status among those interfaces.

13.7.2 Configuring an Interface Association Group

An interface association group contains only physical interfaces. A physical interface in an interface association group cannot be added to other association groups. Before adding a physical interface to an interface association group, remove the interface from the original association group.

Procedure:

1. Choose **Network** > **Interface** > **Interface association**. The following page appears.



Linkage Function OFF

Status	Name	Interface Member	Operate
No data available in table			

Showing 0 to 0 of 0 entries

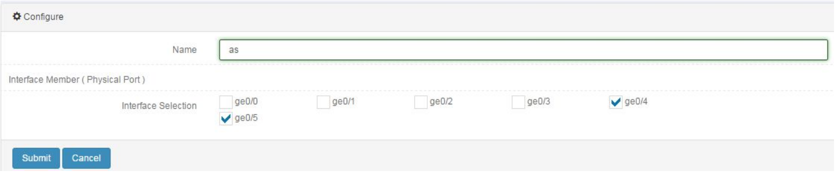
Association: The options are **ON** and **OFF**, which indicate enabling and disable interface association.

Status: Link status of the interfaces in the association group. ● indicates unknown, ● indicates down, and ● indicates up.

Name: Name of an interface association group.

Member interface: Interfaces in the interface association group.

2. Click **New** to create an interface association group, as shown in the following figure.



Configure

Name: as

Interface Member (Physical Port)

Interface Selection: ☐ ge0/0 ☐ ge0/1 ☐ ge0/2 ☐ ge0/3 ☑ ge0/4 ☑ ge0/5

Parameter description:

Name: Enter a name for the new interface association group.

Member interface: Select the interfaces to be added to the interface association group.

2 Click **Submit** after you complete the settings.

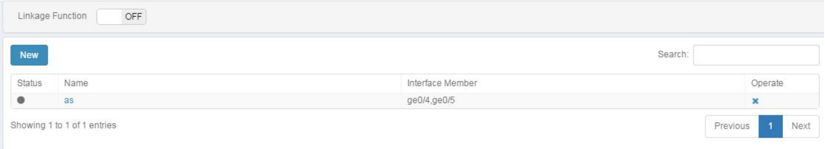
Note

Interfaces referenced by other association groups cannot be selected.

13.7.3 Modifying an Interface Association Group

Procedure:

1. Choose **Network** > **Interface** > **Interface association** and click an interface association group.

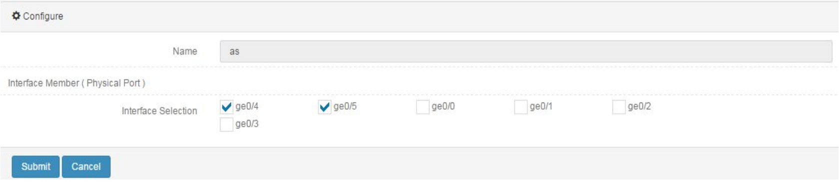


Linkage Function: OFF

Status	Name	Interface Member	Operate
●	as	ge0/4,ge0/5	✖

Showing 1 to 1 of 1 entries

2. Modify the information about the interface association group. Click **Submit** to apply the modification.



Configure

Name: as

Interface Member (Physical Port)

Interface Selection: ☑ ge0/4 ☑ ge0/5 ☐ ge0/0 ☐ ge0/1 ☐ ge0/2 ☐ ge0/3

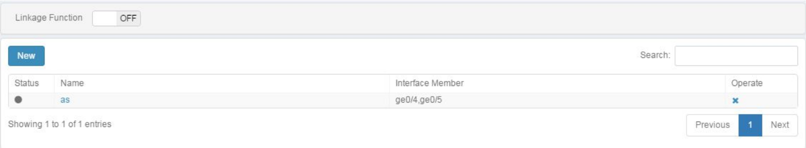
Notice

The group name cannot be modified.

13.7.4 Deleting an Interface Association Group

Procedure:

1. Choose **Network** > **Interface** > **Interface association**. The following page appears.



Linkage Function OFF

New

Search:

Status	Name	Interface Member	Operate
●	as	ge0/4,ge0/5	✖

Showing 1 to 1 of 1 entries

Previous 1 Next

2. Click ✖ next to an interface association group.

13.8 Configuration Examples

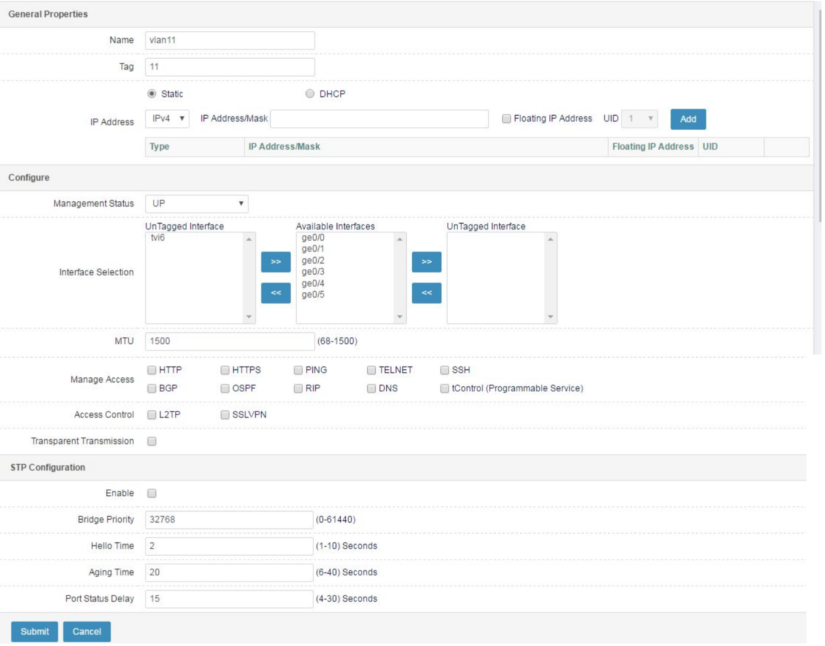
13.8.1 Example 1: Adding a VLAN

Description:

Create a VLAN and add physical interfaces to it.

Procedure:

1. Choose **Network** > **Interface** > **VLAN** and click **New**. The following page appears.



General Properties

Name: vlan11

Tag: 11

IP Address: ◉ Static ○ DHCP

IPv4 ▾ IP Address/Mask □ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID

Configure

Management Status: UP ▾

Interface Selection: UnTagged Interface: tvi6 | Available Interfaces: ge0/0, ge0/1, ge0/2, ge0/3, ge0/4, ge0/5 | UnTagged Interface

MTU: 1500 (68-1500)

Manage Access: □ HTTP □ HTTPS □ PING □ TELNET □ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)

Access Control: □ L2TP □ SSLVPN

Transparent Transmission: □

STP Configuration

Enable: □

Bridge Priority: 32768 (0-61440)

Hello Time: 2 (1-10) Seconds

Aging Time: 20 (6-40) Seconds

Port Status Delay: 15 (4-30) Seconds

Submit Cancel

2. Set **Name** to **vlan1**, **Tag** to **1**, **Management status** to **UP**, and **MTU** to 1500.

3. Select **ge0/1** in **Available interfaces** and click << to add it to **UnTagged interfaces**. Select **ge0/2** in **Available interfaces** and click >> to add it to **Tagged interfaces**.
4. In **STP configuration**, check the **Enable** box, and set **Bridge priority** to **32768**, **Hello time** to **2**, **Aging time** to **20**, and **Port status delay** to **15**.
5. Click **Submit** after you complete the settings.

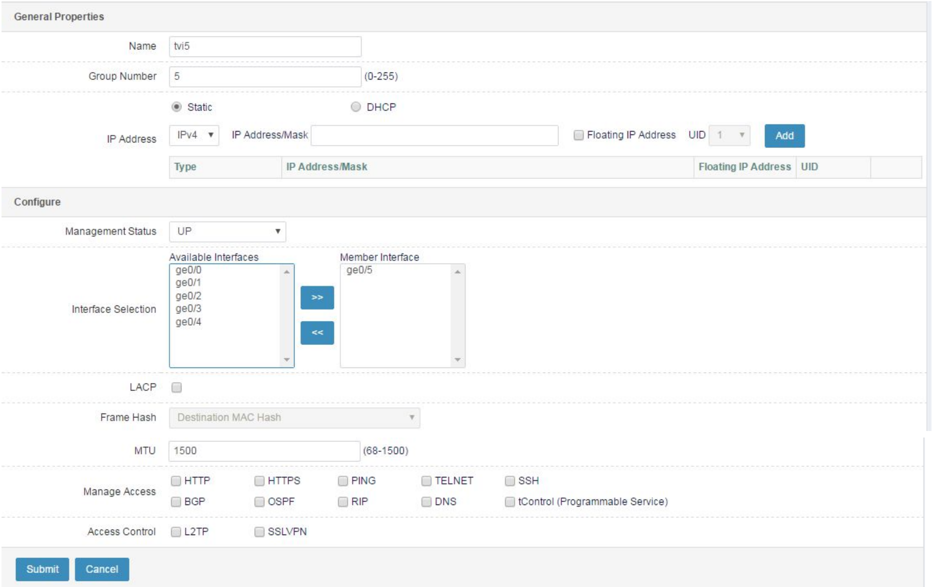
13.8.2 Example 2: Adding a LAG

Description:

Create a LAG and add physical interfaces to it.

Procedure:

1. Choose **Network** > **Interface** > **Link aggregation** and click **New**. The following page appears.



General Properties

Name: tvi5

Group Number: 5 (0-255)

IP Address: ● Static ○ DHCP
IPv4 ▾ IP Address/Mask □ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID

Configure

Management Status: UP ▾

Interface Selection:
Available Interfaces: ge0/0, ge0/1, ge0/2, ge0/3, ge0/4
>> <<
Member Interface: ge0/5

LACP □

Frame Hash: Destination MAC Hash ▾

MTU: 1500 (68-1500)

Manage Access: □ HTTP □ HTTPS □ PING □ TELNET □ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)

Access Control: □ L2TP □ SSLVPN

Submit Cancel

Set **Name** to **tvi1**, **Group ID** to **1**, and **Management status** to **UP**.

2. Select **ge0/3** and **ge0/4** in **Available interfaces** and click >> to add them to the LAG.
3. Check the **LACP** box, and select **Source/Destination IP address and Port** for **Frame hash**.
4. Click **Submit** after you complete the settings.

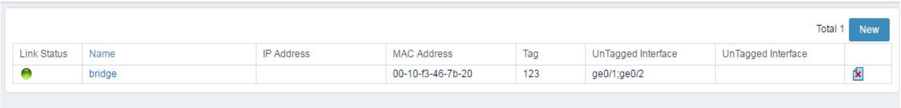
13.8.3 Example 3: Configuring a Bridge Mode

Description:

Configure a transparent bridge mode.

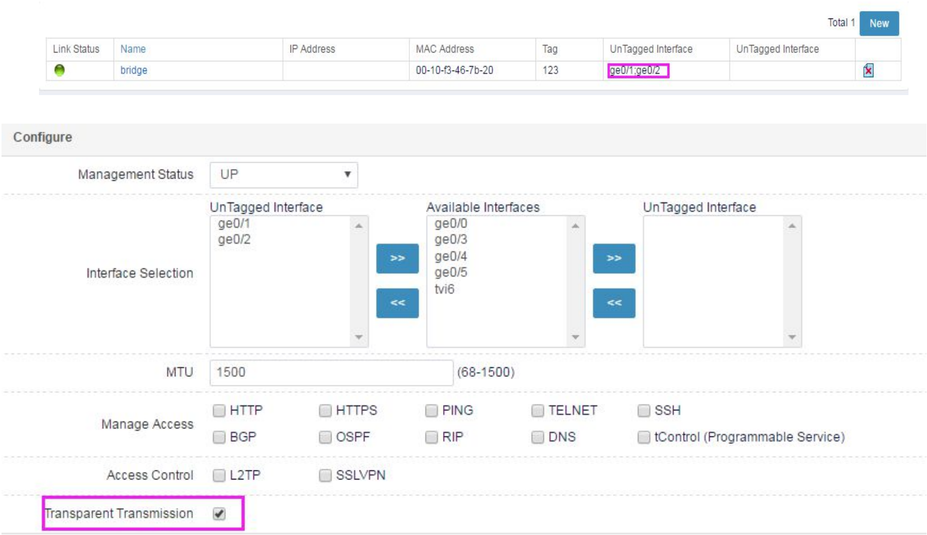
Procedure:

1. Choose **Network** > **Interface** > **VLAN** and click **New** to create a VLAN interface.



Link Status	Name	IP Address	MAC Address	Tag	UnTagged Interface	UnTagged Interface	
●	bridge		00-10-f3-46-7b-20	123	ge0/1;ge0/2		☒

2. Add the two physical interfaces to be bridged to the VLAN in untag mode. Enable VLAN transparent transmission.



Link Status	Name	IP Address	MAC Address	Tag	UnTagged Interface	UnTagged Interface	
●	bridge		00-10-f3-46-7b-20	123	ge0/1;ge0/2		☒

Configure

Management Status: UP

Interface Selection:
UnTagged Interface: ge0/1, ge0/2
Available Interfaces: ge0/0, ge0/3, ge0/4, ge0/5, tvi6
UnTagged Interface:

MTU: 1500 (68-1500)

Manage Access: □ HTTP □ HTTPS □ PING □ TELNET □ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)

Access Control: □ L2TP □ SSLVPN

Transparent Transmission ☑

3. Direct the traffic to be bridged to the physical interfaces of the bridge.

13.9 Troubleshooting

13.9.1 Link Aggregation Interfaces Do Not Work

Symptom	Link aggregation interfaces do not receive and send packets.
Analysis	The link aggregation interfaces are not activated due to failed LACP negotiation.

Solution	Check the peer device's LACP configuration to ensure successful negotiation.

13.9.2 Tagged Interfaces in a VLAN Do Not Work

Symptom	The tagged interfaces in a VLAN do not receive and send packets.
Analysis	The packets sent by the peer device are not 802.1Q packets, or the packet's VLAN ID is different from its tag.
Solution	Check that the peer device sends 802.1Q packets with the VLAN ID the same as the tag.

14 Security Zone

14.1 Overview

The policy configuration of a firewall is typically applied to the interfaces that receive and send packets, especially for dual homed firewalls. Some firewalls are designed to provide densely deployed ports, apart from the traditional role of connecting external and internal networks. A high-end firewall can provide a dozen more physical interfaces and connect to multiple logical network segments. In such a network environment, a common practice is to configure a security policy for every interface, which is a great burden on the network administrator. Besides, it doubles the workload of security policy maintenance and increases the probability of configuration-related security risks.

To solve these issues, mainstream firewalls are developed to support security policy configuration based on security zones. Security zone is an abstract concept. A security zone may contain physical and logical interfaces, or contain Layer-2 physical trunk interfaces and VLANs. The interfaces allocated to the same security zone have consistent security requirements in security policy control. The security zone feature allows the security administrator to allocate interfaces with same security requirements to different zones for hierarchical policy management. When the network changes, the security administrator only needs to adjust the interfaces in related zones without modifying security policies.

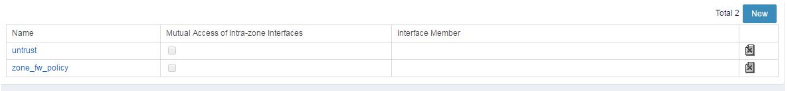
14.2 Configuration

14.2.1 Configuring a Security Zone

A security zone may contain physical and logical interfaces, or contain Layer-2 physical trunk interfaces and VLANs. A security zone can be referenced by a security policy in the outbound and inbound interface configuration to filter interfaces. With policy match enabled on a firewall, if no security policy is hit, the interfaces in the same security zone can be configured to communicate with each other.

Procedure:

1. Choose **Network** > **Security zone**. The following page appears.



Total 2 New

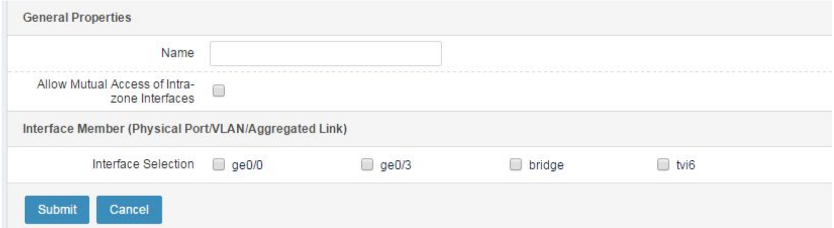
Name	Mutual Access of Intra-zone Interfaces	Interface Member	
untrust	□		☒
zone_fw_policy	□		☒

Name: Name of a security zone.

Intra-zone interface access: Whether intra-zone interface access is enabled for the security zone.

Member interface: Interfaces in the security zone.

2. Click **New** to create a security zone. The following page appears.



General Properties

Name

Allow Mutual Access of Intra-zone Interfaces □

Interface Member (Physical Port/VLAN/Aggregated Link)

Interface Selection □ ge0/0 □ ge0/3 □ bridge □ tvi6

Parameter description:

Name: Name of the new security zone.

Allow inter-interface access: With this option selected and policy match enabled on the firewall, if no security policy is hit, the interfaces in the security zone can still communicate with each other.

Select interfaces: Select the interfaces you want to add to the security zone.

3. Click **Submit** after you complete the settings.

Note

The name of a security zone cannot be the same as the name of any interface or any other security zone.

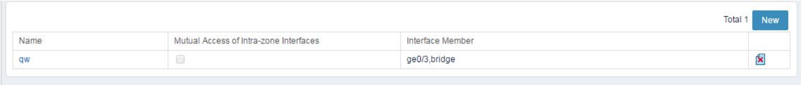
Note

A security zone cannot reference the interfaces that are currently referenced by other security zones, VLANs, trunks, or firewall policies.

14.2.2 Modifying a Security Zone

Procedure:

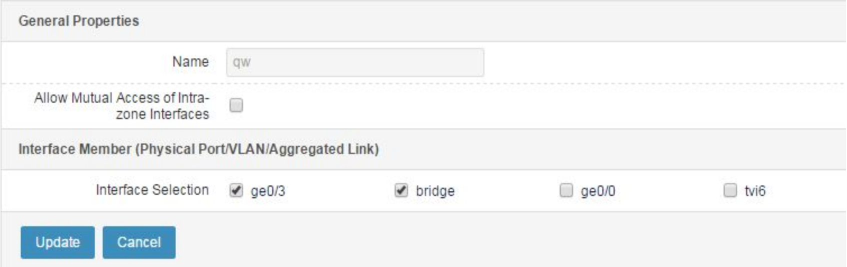
1. Choose **Network** > **Security zone** and click a security zone.



Total 1 New

Name	Mutual Access of Intra-zone Interfaces	Interface Member	
qw	☐	ge0/3,bridge	☒

2. Modify the information about the security zone. Click **Update** to apply the modification.



General Properties

Name: qw

Allow Mutual Access of Intra-zone Interfaces: ☐

Interface Member (Physical Port/VLAN/Aggregated Link)

Interface Selection: ☑ ge0/3 ☑ bridge ☐ ge0/0 ☐ tvi6

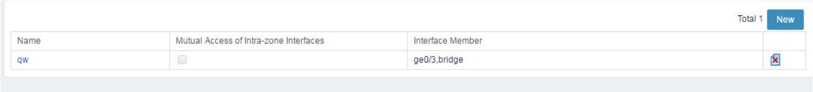
Notice

The name of the security zone cannot be modified.

14.2.3 Deleting a Security Zone

Procedure:

1. Choose **Network** > **Security zone**. The following page appears.



Total 1 New

Name	Mutual Access of Intra-zone Interfaces	Interface Member	
qw	☐	ge0/3,bridge	☒

2. Click ☒ next to the security zone you want to delete.

14.3 Configuration Example

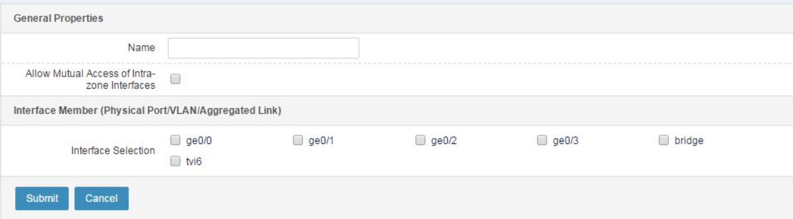
14.3.1 Adding and Referencing a Security Zone in a Firewall Policy

Description:

Configure a security zone containing interfaces ge0/1 and ge0/2 in a firewall policy, and configure the interfaces as the inbound interfaces for the firewall policy.

Procedure:

1. Choose **Network** > **Security zone** and click **New**. The following page appears.



General Properties

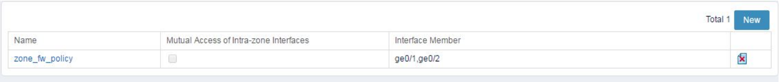
Name	
Allow Mutual Access of Intra-zone Interfaces	□

Interface Member (Physical Port/VLAN/Aggregated Link)

Interface Selection: □ ge0/0 □ ge0/1 □ ge0/2 □ ge0/3 □ bridge □ tvi6

Set **Name** to **zone_fw_policy** and select **ge0/1** and **ge0/2** as member interfaces.

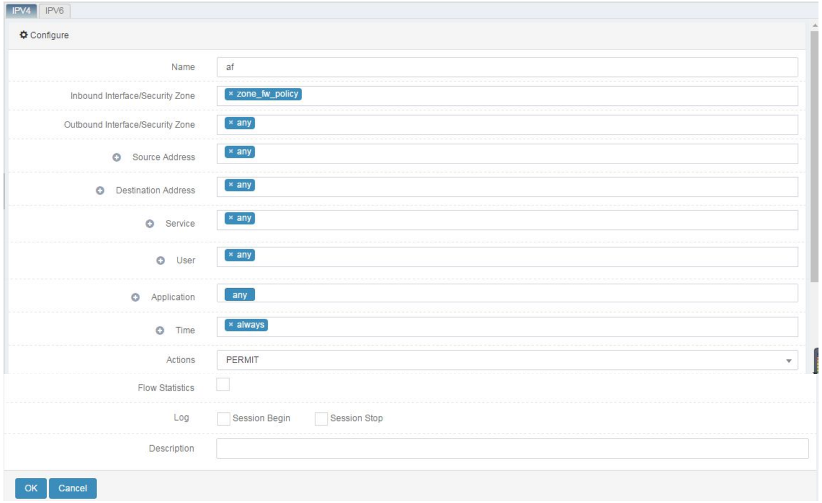
2. Click **Submit** after you complete the settings, as shown in the following figure.



Total 1

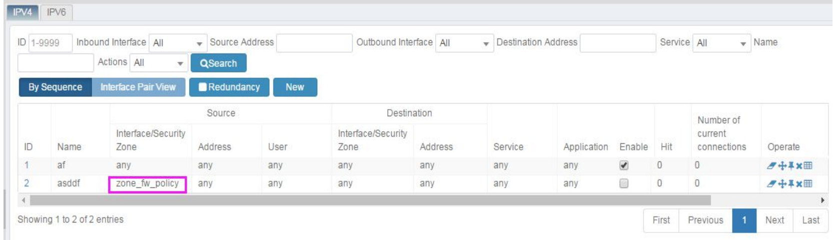
Name	Mutual Access of Intra-zone Interfaces	Interface Member	
zone_fw_policy	□	ge0/1,ge0/2	☒

3. Choose **Policy** > **Firewall** > **Policy** and click **New**. Complete the settings on the following page.



Name	af
Inbound Interface/Security Zone	× zone_fw_policy
Outbound Interface/Security Zone	× any
Source Address	× any
Destination Address	× any
Service	× any
User	× any
Application	any
Time	× always
Actions	PERMIT
Flow Statistics	□
Log	□ Session Begin □ Session Stop
Description	

4. Select **zone_fw_policy** for **Inbound interface/Security Zone**. Click **Submit** after you complete the settings.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
1	af	any	any	any	any	any	any	any	☑	0	0	
2	asddf	zone_fw_policy	any	any	any	any	any	any	□	0	0	

Showing 1 to 2 of 2 entries

14.4 Troubleshooting

14.4.1 An Interface Is Unavailable for Selection When a Security Zone Is Created

Symptom	The desired interface is unavailable for selection when a security zone is created.
Analysis	An interface cannot be added to a security zone due to the following causes: ➢ The interface is referenced by a VLAN, trunk, or another security zone. ➢ The interface is referenced by a firewall policy.
Solution	Select an available interface, or cancel the reference to the desired interface.

15 Static ARP

15.1 Overview

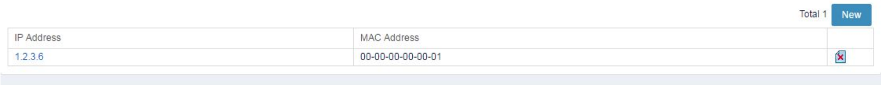
IP packets are usually sent over the Ethernet. Ethernet devices cannot identify 32-bit IP addresses. They transmit Ethernet packets based on 48-bit MAC addresses. Therefore, IP drives are required to convert IP addresses into MAC addresses. A static mapping or algorithm-based mapping exists between IP and MAC addresses, and the conversion between them requires table lookup. The Address Resolution Protocol (ARP) is used to determine the mapping.

Normally, devices acquire ARP tables dynamically from networks. When a device fails to acquire an ARP table, it uses static ARP to send data. Static ARP binds an IP address to a MAC address to implement black hole routing and direct IP data sending.

15.2 Configuration

15.2.1 Adding a Static ARP Entry

1. Choose **Network** > **ARP** > **Static ARP**. The following page appears.

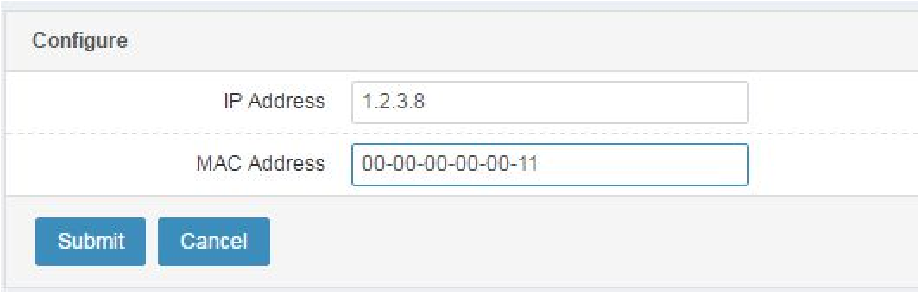


IP Address	MAC Address	
1.2.3.6	00-00-00-00-00-01	☒

IP address: IP address bound by static ARP

MAC address: MAC address bound by static ARP

2. Click **New** to create a static ARP entry. The following page appears.



IP Address: 1.2.3.8

MAC Address: 00-00-00-00-00-11

IP address: IP address bound by static ARP
MAC address: MAC address bound by static ARP

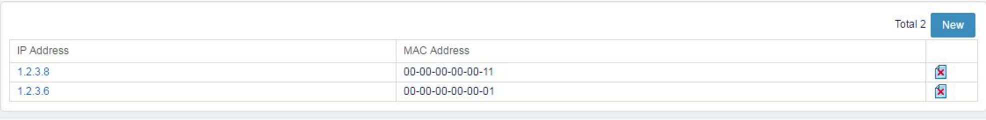
3. Click **Submit** after you complete the settings.

Notice

When configuring a static ARP entry, you can add multiple MAC addresses but can add only one IP address.

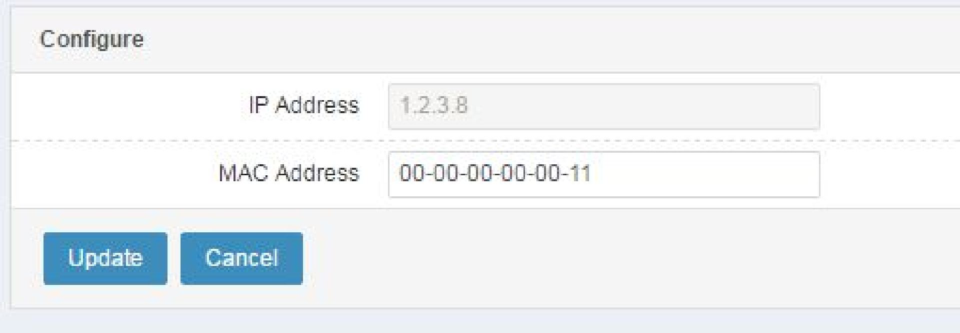
15.2.2 Modifying a Static ARP Entry

1. Choose **Network configuration** > **ARP** > **Static ARP**. The following page appears.



IP Address	MAC Address	
1.2.3.8	00-00-00-00-00-11	☒
1.2.3.6	00-00-00-00-00-01	☒

2. Click an IP address. The following page appears.



IP Address: 1.2.3.8

MAC Address: 00-00-00-00-00-11

Modify the MAC address.

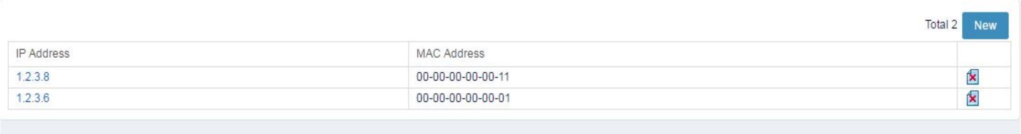
3. Click **Update** to apply the modification.

Notice

When modifying a static ARP entry, you can only change the MAC address but cannot change the IP address.

15.2.3 Deleting a Static ARP Entry

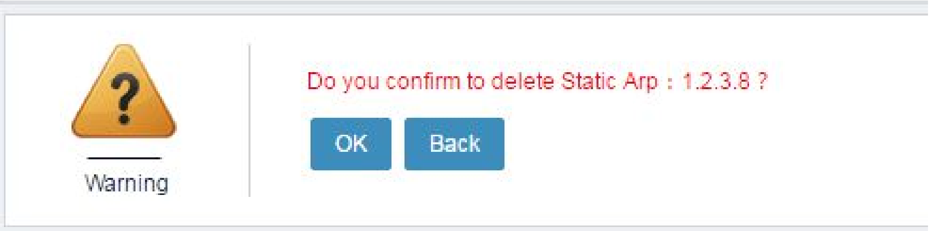
1. Choose **Network configuration** > **ARP** > **Static ARP**. The following page appears.



Total 2 New

IP Address	MAC Address	
1.2.3.8	00-00-00-00-00-11	☒
1.2.3.6	00-00-00-00-00-01	☒

2. Click ☒ next to the static ARP entry you want to delete. A delete confirmation prompt appears, as shown in the following figure.



Do you confirm to delete Static Arp : 1.2.3.8 ?

3. Click **OK**.

15.3 Troubleshooting

15.3.1 Network Is Unavailable After a Static ARP Entry Is Added

Symptom	The peer end is unreachable after a static ARP entry is added.
Analysis	The IP address in the static ARP entry may conflict with the peer IP address.
Solution	Delete the static ARP entry and use the peer IP address.

16 DHCP Server

16.1 Overview

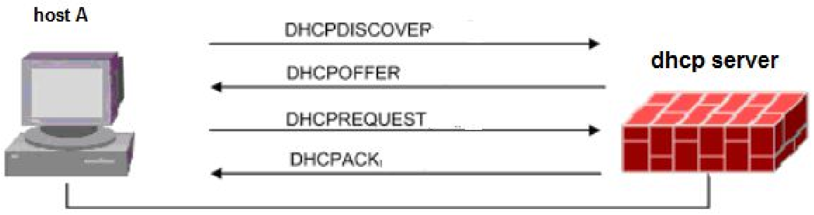
RAVEN 5000 firewalls provide two DHCP functions: DHCP server and DHCP relay.

16.1.1 DHCP Server

DHCP is short for Dynamic Host Configuration Protocol. A RAVEN 5000 firewall can work as a DHCP server to dynamically allocate and centrally manage IP addresses in the network. The IP address that a DHCP client borrows from a DHCP server can be used only for a limited period. Upon expiration of the IP address, the client must release the IP address for use by other workstations. The DHCP server must be configured with an IP address pool whose IP addresses can be allocated dynamically to users.

The following figure shows how a DHCP client applies for an IP address from a DHCP server. Host A (client) sends a DHCPDISCOVER broadcast packet to search for a DHCP server in the network. A DHCP server returns a parameter-carrying DHCPOFFER unicast packet to the client.

Figure 13-1 Flowchart for a DHCP client to apply for an IP address from a DHCP server



- When a client logs in to a network for the first time, it sends a DHCPDISCOVER broadcast packet encapsulated with the source address 0.0.0.0 and destination address 255.255.255.255 because the client does not know the specific network.
- Each DHCP server with valid IP addresses in the network selects an available IP address and returns an offer message to the client.

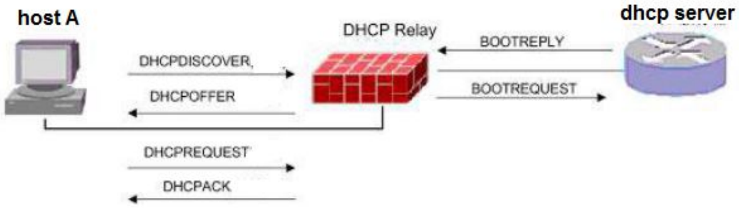
- The client selects the IP address in the first offer message and broadcasts a lease request. The DHCP server which sends the first offer message accepts the request and starts leasing.
- The client uses the IP address after receiving the acceptance message.

⚠ The DHCP client can receive messages from multiple DHCP servers and select a DHCP server, indicating that the client rejects the parameters offered by the other DHCP servers.

16.1.2 DHCP Relay

A DHCP relay forwards DHCP requests to the DHCP servers in another network segment for IP address allocation. When a DHCP client without IP environment setting sends a DHCP request, the DHCP relay forwards the message to DHCP servers and then forwards the response from a DHCP server to the client so that the client can acquire an IP address. The DHCP relay helps eliminate the additional cost and management inconvenience of deploying DHCP servers in every network segment. The following figure shows how the DHCP relay works.

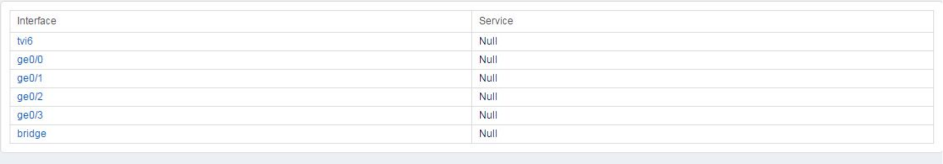
Figure 13-2 Flowchart for a DHCP client to apply for an IP address from a DHCP server through a DHCP relay



16.2 Configuration

16.2.1 Specifying a DHCP Service for an Interface

Choose Network > DHCP > Service.

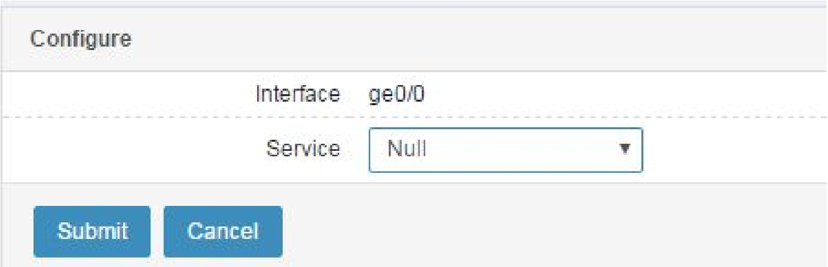


Interface	Service
tvi6	Null
ge0/0	Null
ge0/1	Null
ge0/2	Null
ge0/3	Null
bridge	Null

Interface: Physical interface, VLAN interface, or trunk interface.

Service: DHCP service type enabled on an interface. The options are **Null**, **DHCP server**, and **DHCP relay.**

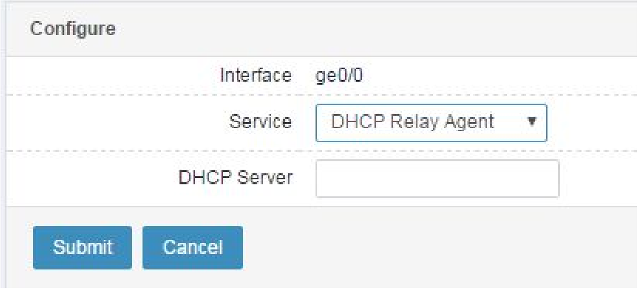
Configure a DHCP service for an interface as follows: Click an interface.



Configure

Interface ge0/0

Service Null

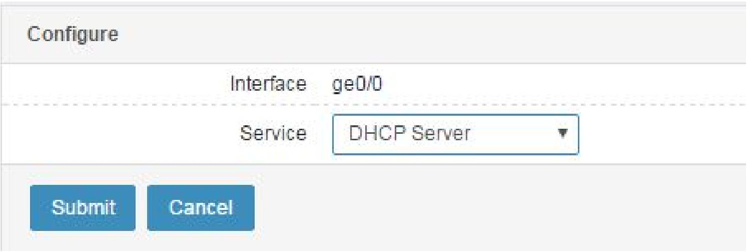


Configure

Interface ge0/0

Service DHCP Relay Agent

DHCP Server



Configure

Interface ge0/0

Service DHCP Server

Interface name: Name of an interface.

Service:

Null: DHCP is not enabled on the interface.

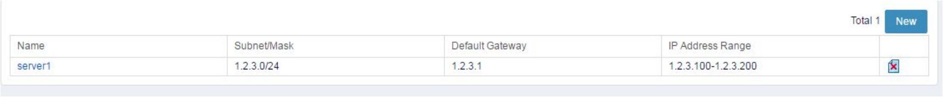
DHCP server: Enable the DHCP server function on the interface.

DHCP relay: Enable the DHCP relay function on the interface.

DHCP server text box: Enter the address of the peer DHCP server if you select **DHCP relay** for **Service**.

16.2.2 Configuring a DHCP Server Address Pool

Choose Network > DHCP > Server.



Total 1 New

Name	Subnet/Mask	Default Gateway	IP Address Range	
server1	1.2.3.0/24	1.2.3.1	1.2.3.100-1.2.3.200	☒

Name: Name of a DHCP server address pool.

Subnet/Mask: Subnet and mask of the address pool.

Default gateway: Default gateway for the address pool.

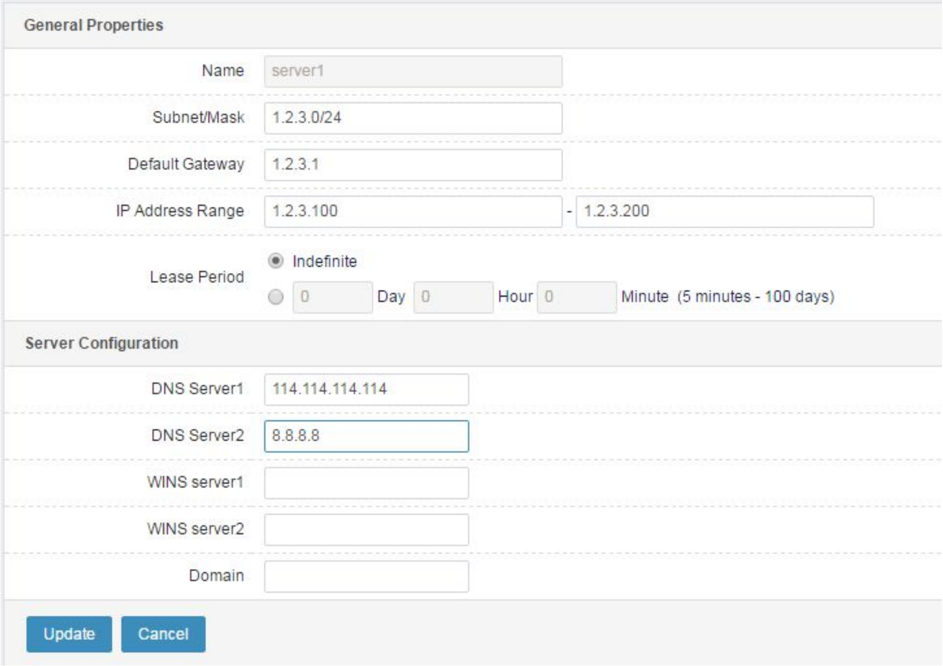
IP address range: Range of the address pool.

New: Click this button to create a DHCP server address pool.

☒: Click this button to delete an address pool.

Configure a DHCP server address pool as follows:

Click **New**.



General Properties

Name	server1
Subnet/Mask	1.2.3.0/24
Default Gateway	1.2.3.1
IP Address Range	1.2.3.100 - 1.2.3.200
Lease Period	● Indefinite ○ 0 Day 0 Hour 0 Minute (5 minutes - 100 days)

Server Configuration

DNS Server1	114.114.114.114
DNS Server2	8.8.8.8
WINS server1	
WINS server2	
Domain	

Name: Name of a DHCP server address pool.

Subnet/Mask: Subnet and mask of the address pool.

Default gateway: Default gateway for the address pool.

IP address range: Range of the address pool.

Lease term: Address lease term. You can select **Permanent** or set a specific lease term.

DNS server 1: Preferred DNS server.

DNS server 2: Alternate DNS server.

WINS server 1: Preferred WINS server.

WINS server 2: Alternate WINS server.

Domain: Domain name.

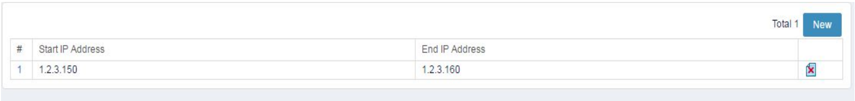
Update: Click this button to create a DHCP server address pool.

Cancel: Click this button to cancel the configuration.

⚠ Notice	Only one address pool can be created for each subnet. If **Lease Term** is not set to **Permanent**, the value ranges from 5 minutes to 100 days.

16.2.3 Configuring DHCP Server Address Exclusion

Choose Network > DHCP > Exclusion range.



#	Start IP Address	End IP Address	
1	1.2.3.150	1.2.3.160	☒

Start IP address: Start IP address of an exclusion range.

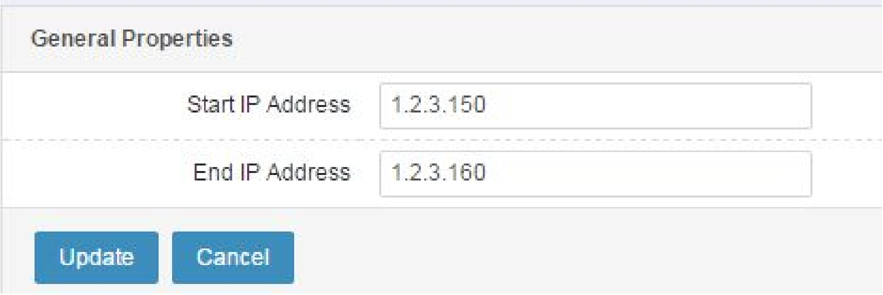
End IP address: End IP address of the exclusion range.

New: Click this button to create an address exclusion range.

☒: Click this button to delete an address exclusion range.

Configure DHCP server address exclusion as follows:

Click **New**.



Start IP Address: 1.2.3.150

End IP Address: 1.2.3.160

Start IP address: Start IP address of an exclusion range.

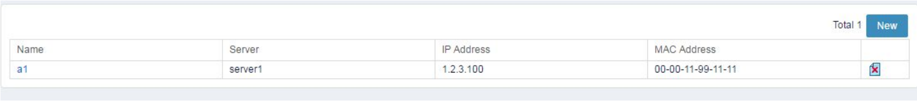
End IP address: End IP address of the exclusion range.

Update: Click this button to create an address exclusion range.

Cancel: Click this button to cancel the configuration.

16.2.4 Configuring Address Binding for a DHCP Server

Choose Network > DHCP > IP-MAC address binding.



Name	Server	IP Address	MAC Address	
a1	server1	1.2.3.100	00-00-11-99-11-11	☒

Name: Name of a DHCP address binding entry.

Server: DHCP server associated with the IP-MAC address binding.

IP address: Bound IP address.

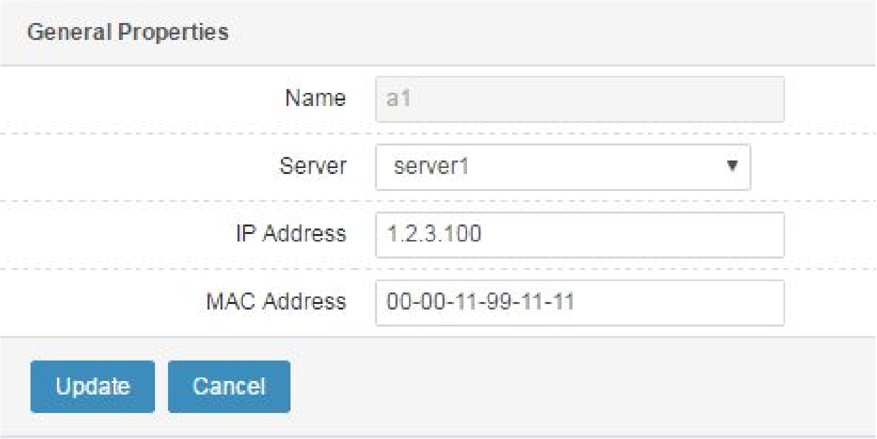
MAC address: Bound MAC address.

New: Click this button to create a DHCP address binding entry.

☒**:** Click this button to delete a DHCP address binding entry.

Configure address binding for a DHCP server as follows:

Click **New**.



Name	a1
Server	server1 ▾
IP Address	1.2.3.100
MAC Address	00-00-11-99-11-11

Name: Name of a DHCP address binding entry.

Server: DHCP server associated with the IP-MAC address binding.

IP address: Bound IP address.

MAC address: Bound MAC address.

Update: Click this button to create a DHCP address binding entry.

Cancel: Click this button to cancel the configuration.

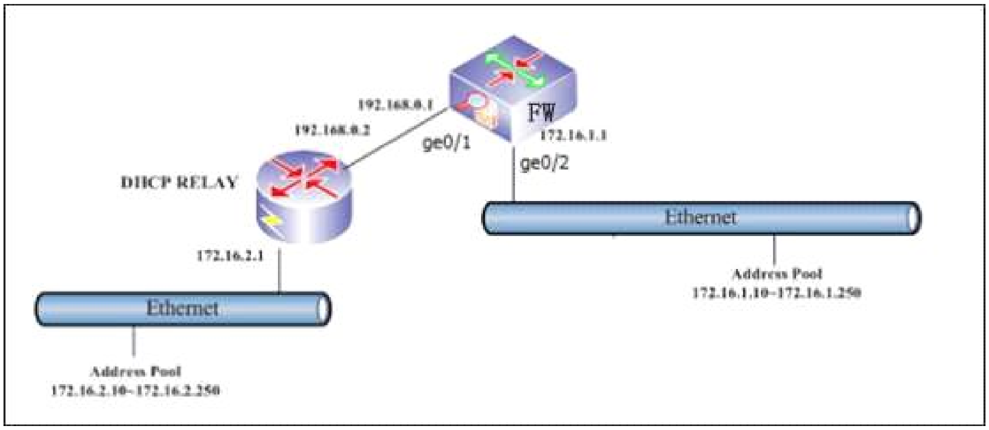
16.3 Configuration Examples

16.3.1 Example 1: Configuring the DHCP Server Function on Interface ge0/2

Description:

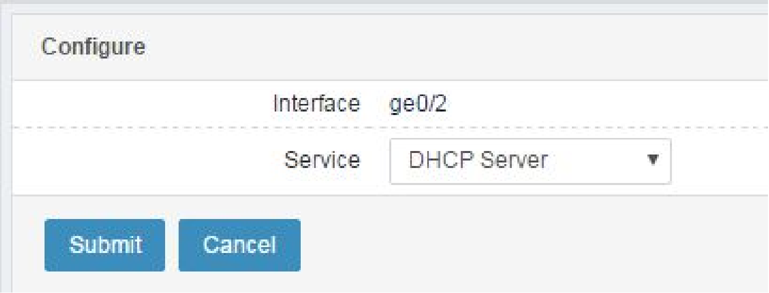
Configure a DHCP server to allocate IP addresses to two subnets: 172.16.1.0/16 which is a directly connected subnet and 172.16.2.0/16 which is connected through a DHCP relay, as shown in the following figure.

Figure 16-1 Network diagram of DHCP server configuration



Procedure:

1. Choose **Network** > **DHCP** > **Service** and click **ge0/2.** The following page appears.



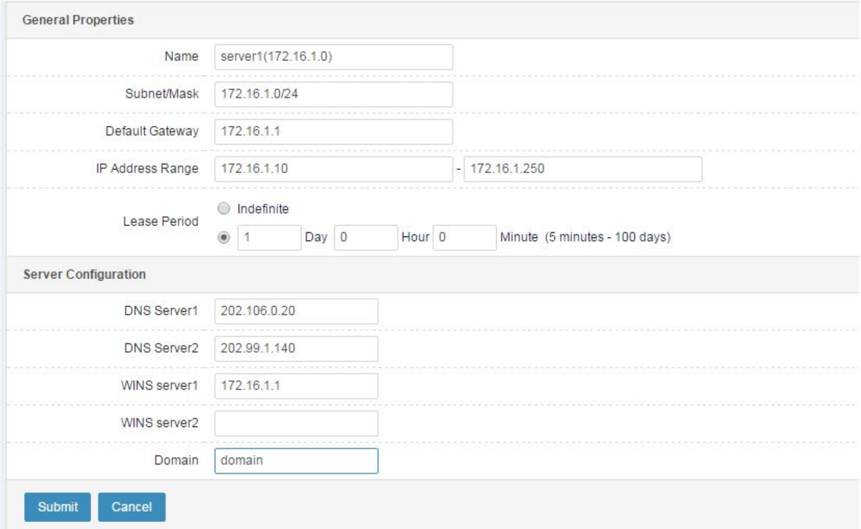
Configure

Interface ge0/2

Service DHCP Server

Select **DHCP server** for **Service**.

2. Click **Submit** after you complete the settings.
3. Choose **Network** > **DHCP** > **Server** and click **New**. Complete the settings on the following page.



General Properties

Name	server1(172.16.1.0)
Subnet/Mask	172.16.1.0/24
Default Gateway	172.16.1.1
IP Address Range	172.16.1.10 - 172.16.1.250
Lease Period	○ Indefinite ● 1 Day 0 Hour 0 Minute (5 minutes - 100 days)

Server Configuration

DNS Server1	202.106.0.20
DNS Server2	202.99.1.140
WINS server1	172.16.1.1
WINS server2	
Domain	domain

Set the following server parameters:

Name: Name of a DHCP server address pool. Set it to **server1(172.16.1.0)**.

Subnet/Mask: Subnet and mask of the address pool. Set it to **172.16.1.0/24**.

Default gateway: Default gateway for the address pool. Set it to **172.16.1.1**.

IP address range: Range of the address pool. Set it to **172.16.1.10-172.16.1.250**.

Lease term: Address lease term. Set it to **1 day**.

DNS server 1: Preferred DNS server. Set it to **202.106.0.20**.

DNS server 2: Alternate DNS server. Set it to **202.99.1.140**.

WINS server 1: Preferred WINS server. Set it to **172.16.1.1**.

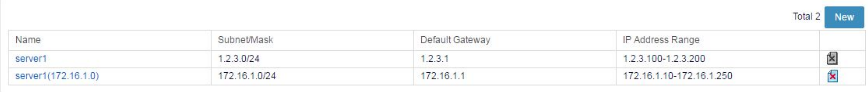
WINS server 2: Alternate WINS server. Leave this parameter empty.

Domain: Domain name. Set it to **domain**.

4. Click **Submit** after you complete the settings.

5. Configure the client PC to automatically acquire an IP address.

6. Check the information displayed by the DHCP monitor on the firewall.



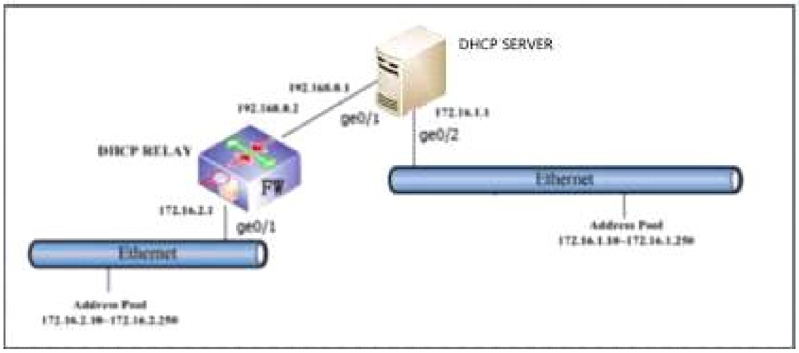
Name	Subnet/Mask	Default Gateway	IP Address Range	
server1	1.2.3.0/24	1.2.3.1	1.2.3.100-1.2.3.200	☒
server1(172.16.1.0)	172.16.1.0/24	172.16.1.1	172.16.1.10-172.16.1.250	☒

16.3.2 Example 2: Configuring the DHCP Relay Function on Interface ge0/1

Description:

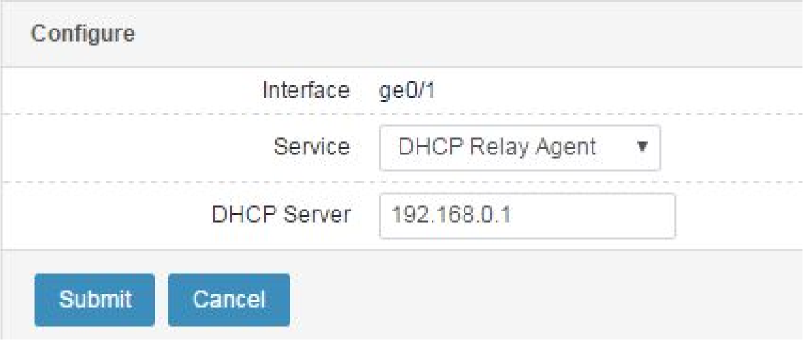
Configure a DHCP relay to allocate IP addresses from a DHCP server (192.168.0.1) to clients, as shown in the following figure.

Figure 16-2 Network diagram of DHCP relay configuration



Procedure:

1. Choose **Network** > **DHCP** > **Service** and click **ge0/1**. Complete the settings on the following page.


Configure

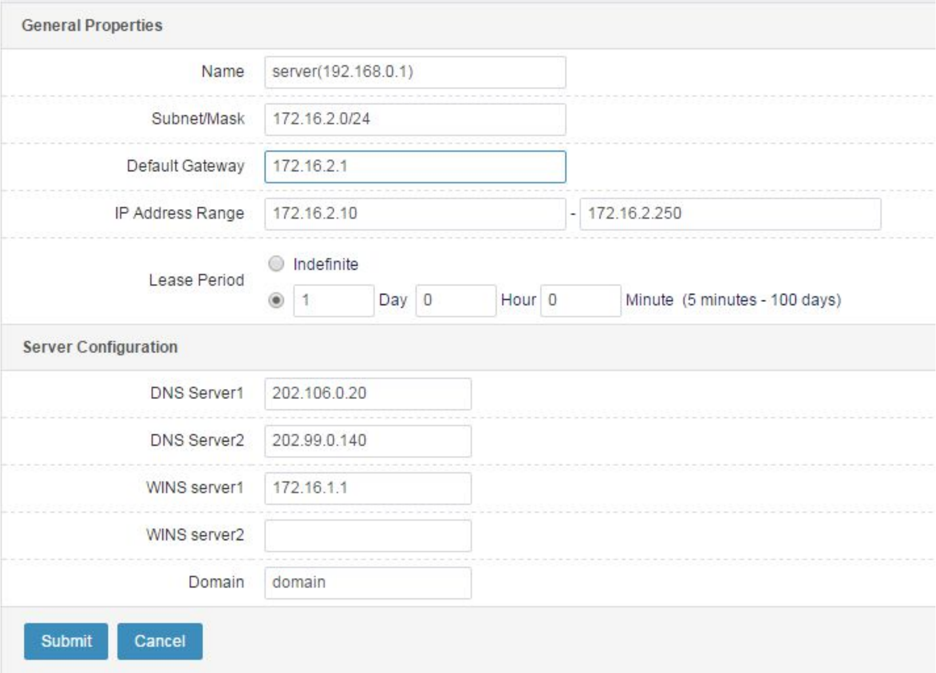
Interface ge0/1

Service DHCP Relay Agent

DHCP Server 192.168.0.1

Select **DHCP relay** for **Service**, and enter the DHCP server address 192.168.0.1 in the **DHCP server** text box.

2. Click **Submit** after you complete the settings.
3. Configure the DHCP server. First ensure that a reachable route exists between the DHCP server and the client network segment 172.16.2.0/24.


General Properties

Name server(192.168.0.1)

Subnet/Mask 172.16.2.0/24

Default Gateway 172.16.2.1

IP Address Range 172.16.2.10 - 172.16.2.250

Lease Period ○ Indefinite ● 1 Day 0 Hour 0 Minute (5 minutes - 100 days)

Server Configuration

DNS Server1 202.106.0.20

DNS Server2 202.99.0.140

WINS server1 172.16.1.1

WINS server2

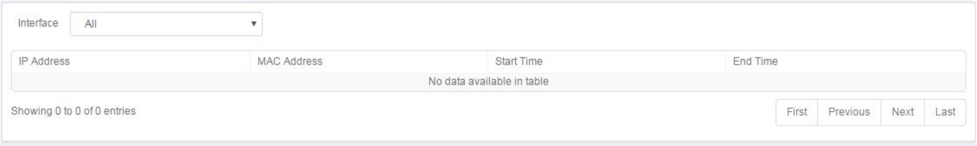
Domain domain

4. Click **Submit** after you complete the settings.

16.4 Monitoring and Maintenance

16.4.1 Checking Address Allocation by a DHCP Server

Choose **Network** > **DHCP** > **Monitor**. The following page appears.



IP Address	MAC Address	Start Time	End Time
No data available in table			

Showing 0 to 0 of 0 entries

IP address: IP address acquired by the client associated with the address lease.

MAC address: MAC address of the client associated with the address lease.

Start time: Application time of the address lease.

End time: End time of the address lease.

Interface: Interface through which addresses are allocated. If you select **ANY**, all the allocated addresses are listed.

16.5 Troubleshooting

16.5.1 DHCP Clients Cannot Acquire IP Addresses from the Interface Enabled with the DHCP Server Function

Symptom	DHCP clients cannot acquire IP addresses from an interface.
Analysis	1. Check whether the interface is configured with an IP address. 2. Check whether the interface is enabled with the DHCP server function. 3. Check whether the DHCP server is configured with an address pool corresponding to the interface IP address.
Solution	1. Configure a correct interface address. 2. Enable the DHCP server function on the interface. 3. Configure the DHCP server with an address pool corresponding to the interface IP address.

16.5.2 DHCP Clients Cannot Acquire IP Addresses from the Interface Enabled with the DHCP Relay Function

Symptom	DHCP clients cannot acquire IP addresses from an interface.
Analysis	1. Check whether the interface address can communicate with the DHCP server at the peer end. 2. Check whether the interface is enabled with the DHCP relay function and configured with the DHCP server address. 3. Check whether the DHCP server is configured with an

	address pool corresponding to the interface IP address.
Solution	1. Configure a correct interface address and route. 2. Enable the DHCP relay function on the interface and configure it with the DHCP server address. 3. Configure an address pool for the DHCP server properly and enable the DHCP service.

17 Static Route

17.1 Overview

A static route is a fixed route entry manually configured on a router. The static route does not change automatically. It must be changed by the network administrator. Because it cannot adapt to network changes, it is typically configured in small-sized and medium-sized networks with a fixed topology. Static routes are simple, efficient, and reliable. They take precedence over all other routes. Static routes prevail when there is a conflict between dynamic and static routes.

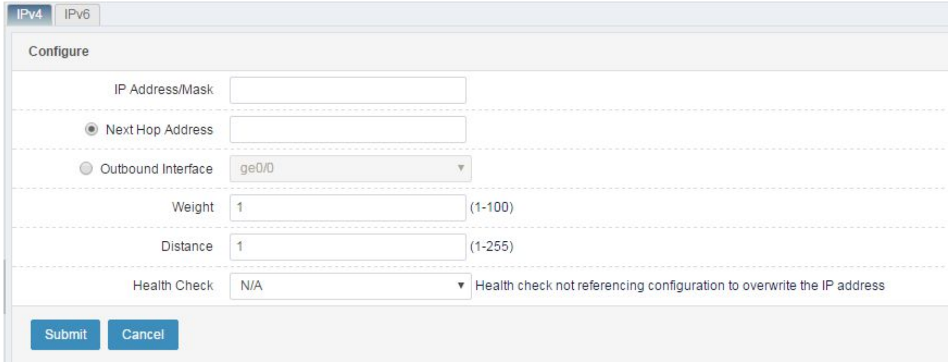
RAVEN 5000 firewalls allow you to configure a health check policy to monitor the static route status. When health check fails, the route status is set to Invalid to prevent data from being forwarded to an unavailable next hop.

17.2 Configuration

17.2.1 Configuring an IPv4 Static Route

Procedure:

Choose **Network** > **Route** > **Static route: IPv4**. The following page appears.



IP Address/Mask		
● Next Hop Address		
○ Outbound Interface	ge0/0 ▾	
Weight	1	(1-100)
Distance	1	(1-255)
Health Check	N/A ▾	Health check not referencing configuration to overwrite the IP address

IP address/Mask: Destination network segment for the static route.

Next hop address: Gateway address for the static route.

Outbound interface: Outbound interface for the static route.

Weight: Weight of the static route. The value ranges from 1 to 100. Weighted round robin is applied to equal-cost routes.

Distance: Priority of the route. The value ranges from 1 to 255.

Health check: Reference a health check template. TCP and ICMP health check modes are supported.

Click **Submit** after you complete the settings.

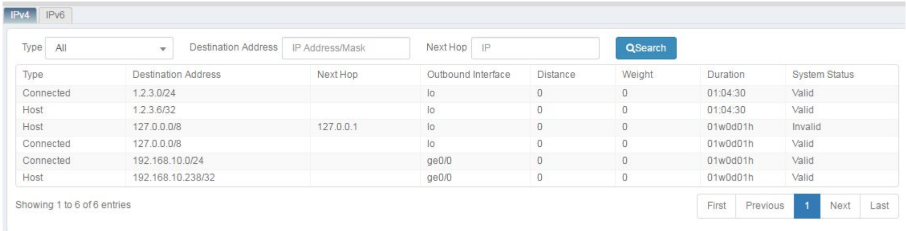
⚠ Notice

The health check object can only be the next hop of a static route.

17.2.2 Displaying an IPv4 Routing Table

Procedure:

Choose **Network** > **Route** > **Routing table: IPv4**. The following page appears.



Type	Destination Address	Next Hop	Outbound Interface	Distance	Weight	Duration	System Status
Connected	1.2.3.0/24		lo	0	0	01:04:30	Valid
Host	1.2.3.6/32		lo	0	0	01:04:30	Valid
Host	127.0.0.0/8	127.0.0.1	lo	0	0	01w0d01h	Invalid
Connected	127.0.0.0/8		lo	0	0	01w0d01h	Valid
Connected	192.168.10.0/24		ge0/0	0	0	01w0d01h	Valid
Host	192.168.10.238/32		ge0/0	0	0	01w0d01h	Valid

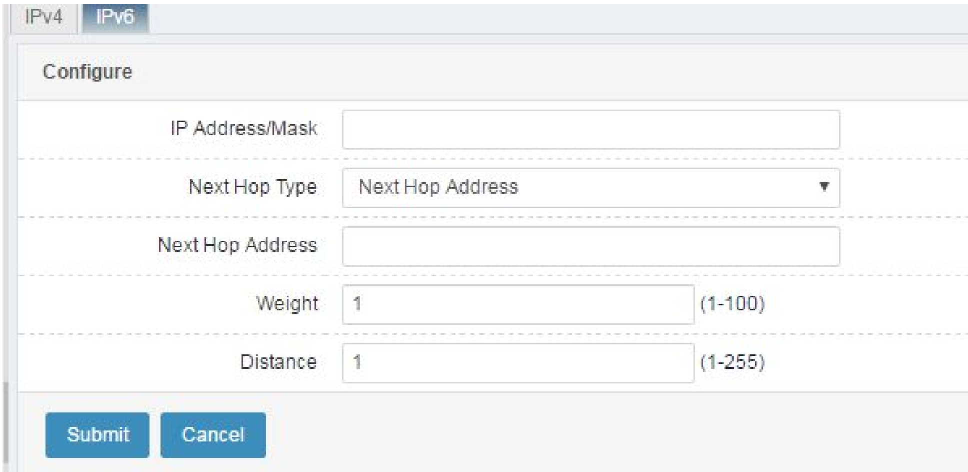
Showing 1 to 6 of 6 entries

The page lists route information. You can filter the routes by specifying the destination address and next hop.

17.2.3 Configuring an IPv6 Static Route

Procedure:

Choose **Network** > **Route** > **Static route: IPv6**. The following page appears.



Configure

IP Address/Mask	
Next Hop Type	Next Hop Address ▾
Next Hop Address	
Weight	1 (1-100)
Distance	1 (1-255)

IP address/Mask: Destination IPv6 address and mask.

Next hop type: The options are **Next hop address**, **Outbound interface**, and **Next hop address & outbound interface**.

Next hop address: Address of the router gateway.

Outbound interface: Interface that forwards data.

Next hop address & outbound interface: Router gateway address and data-forwarding interface.

Weight: Route weight. The value ranges from 1 to 100.

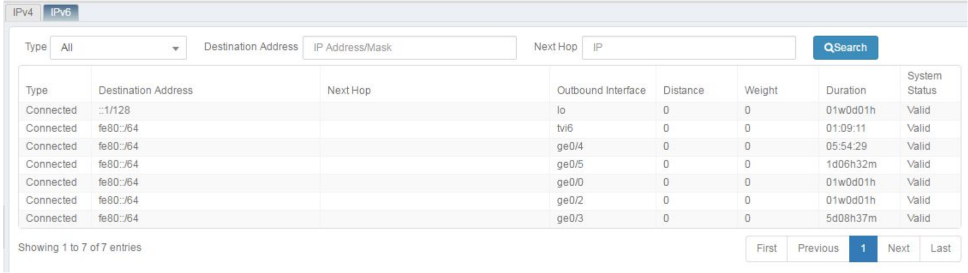
Distance: Priority of the route. The value ranges from 1 to 255.

Click **Submit** after you complete the settings.

17.2.4 Displaying an IPv6 Routing Table

Procedure:

Choose **Network** > **Route** > **Routing table: IPv6**. The following page appears.



Type All ▾ Destination Address IP Address/Mask Next Hop IP

Type	Destination Address	Next Hop	Outbound Interface	Distance	Weight	Duration	System Status
Connected	::1/128		lo	0	0	01w0d01h	Valid
Connected	fe80::/64		tvi6	0	0	01:09:11	Valid
Connected	fe80::/64		ge0/4	0	0	05:54:29	Valid
Connected	fe80::/64		ge0/5	0	0	1d06h32m	Valid
Connected	fe80::/64		ge0/0	0	0	01w0d01h	Valid
Connected	fe80::/64		ge0/2	0	0	01w0d01h	Valid
Connected	fe80::/64		ge0/3	0	0	5d08h37m	Valid

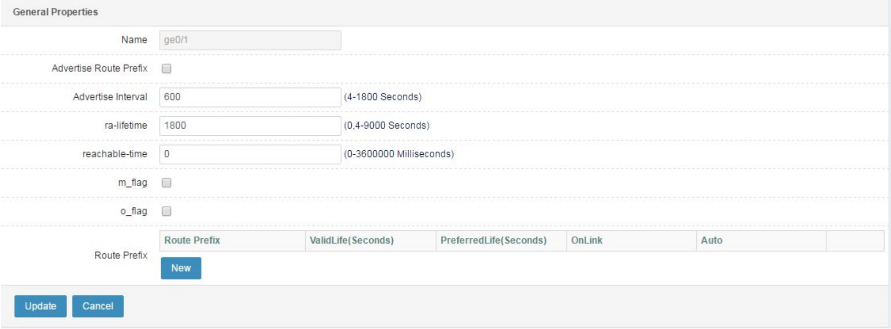
Showing 1 to 7 of 7 entries

The page lists route information. You can filter the routes by specifying the destination address and next hop.

17.2.5 Configuring IPv6 Prefix Advertisement

Procedure:

Choose **Network** > **Route** > **IPv6 prefix advertisement**. The following page appears.



General Properties

Name: ge0/1

Advertise Route Prefix: □

Advertise Interval: 600 (4-1800 Seconds)

ra-lifetime: 1800 (0,4-9000 Seconds)

reachable-time: 0 (0-3600000 Milliseconds)

m_flag: □

o_flag: □

Route Prefix:

Route Prefix	ValidLife(Seconds)	PreferredLife(Seconds)	OnLink	Auto	

Name: Name of the VLAN interface with a route prefix.

Advertise route prefix: Check this box to enable route prefix advertisement.

Advertising interval: Interval of route prefix advertisement.

ra-lifetime: Time to live (TTL) of the route prefix.

reachable-time: Reachable time of the router.

m_flag: Configuration identifier of the management address.

o_flag: Configuration identifier of other status.

Route prefix: Route prefix to be advertised.

ValidLife: Valid TTL of the route prefix.

PreferredLife: Preferred TTL of the route prefix.

Click **Update** to apply the settings.

17.3 Configuration Example

17.3.1 Configuring Multi-route Monitoring

Description:

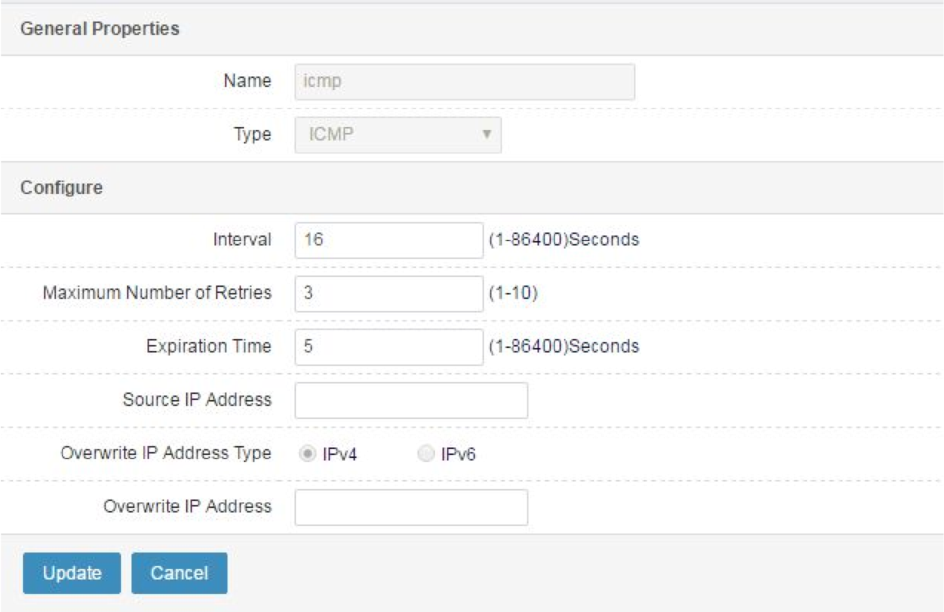
A company has multiple egresses with the next hop addresses 30.1.1.1, 31.1.1.1, and 32.1.1.1.

The customer requirements are as follows:

1. Configure two default routes, and perform health check on the next hops to check their availability. Set the route status to Invalid upon failed health check to ensure that services are forwarded to an available next hop.
2. Perform ICMP-based health check on 30.1.1.1 and 31.1.1.1, and perform TCP-based health check on 32.1.1.1.

Procedure:

1. Choose **Object** > **Health check** to create an ICMP-based health check template. If you do not specify **Included IP address**, health check will be performed on the next hop of the route.



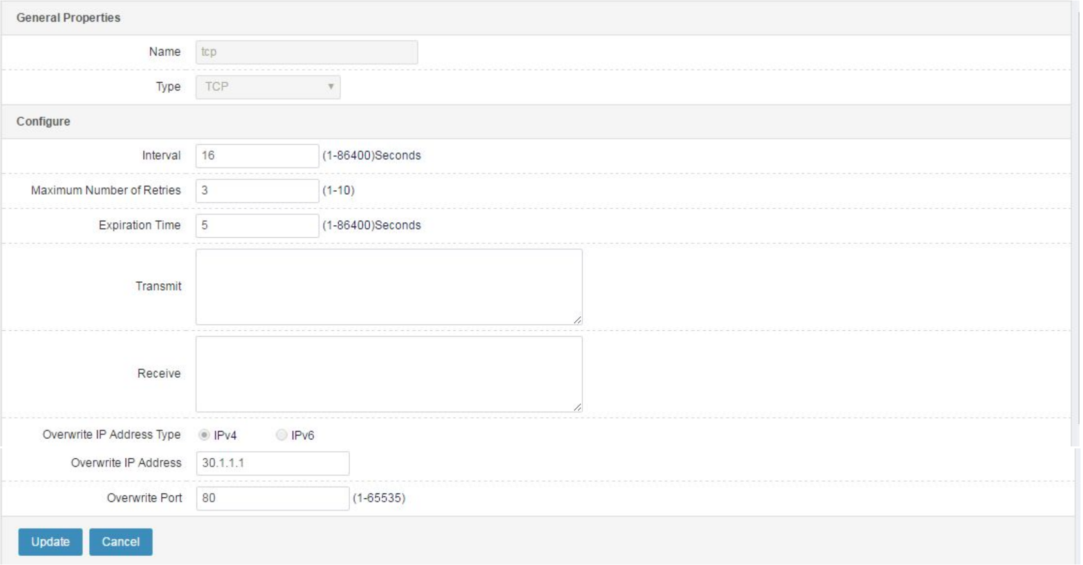
General Properties

Name	icmp
Type	ICMP

Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Source IP Address	
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	

2. Choose **Object** > **Health check** to create a TCP-based health check template. Set **Included IP address** to the next hop address of the route, and set **Included port** to the available port of the next hop.



General Properties

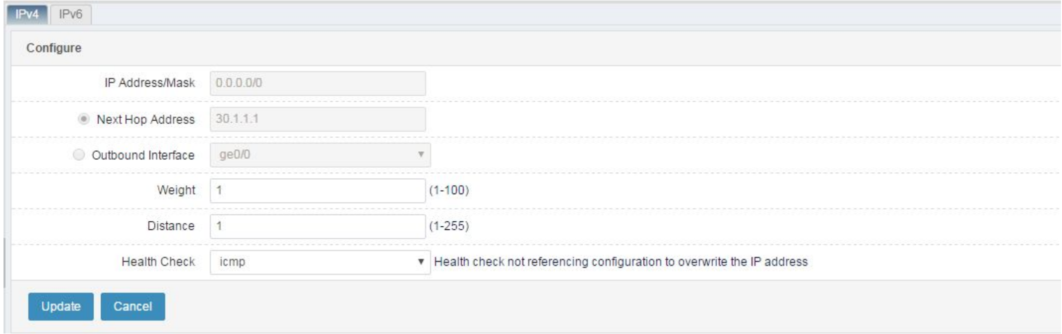
Name	tcp
Type	TCP ▾

Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Transmit	
Receive	
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	30.1.1.1
Overwrite Port	80 (1-65535)

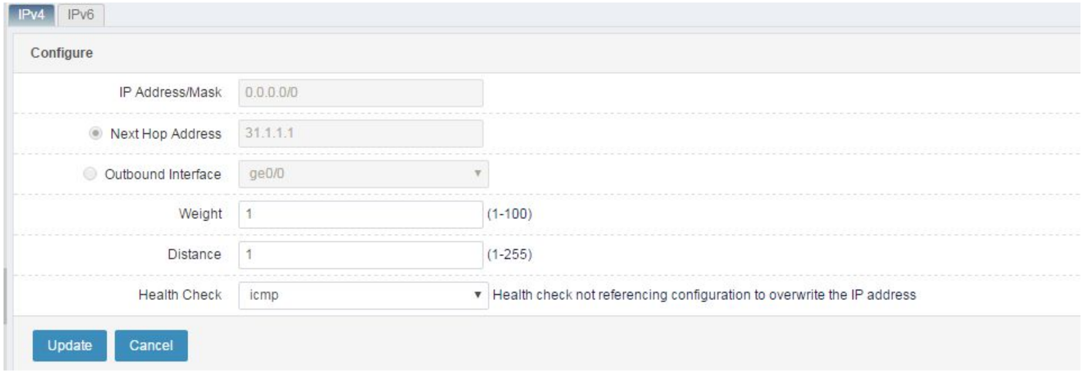
3. Choose **Network** > **Route** > **Static route**. Add three default routes.

   Reference the ICMP-based health check template for 30.1.1.1 and 31.1.1.1, and reference the TCP-based health check template for 32.1.1.1.



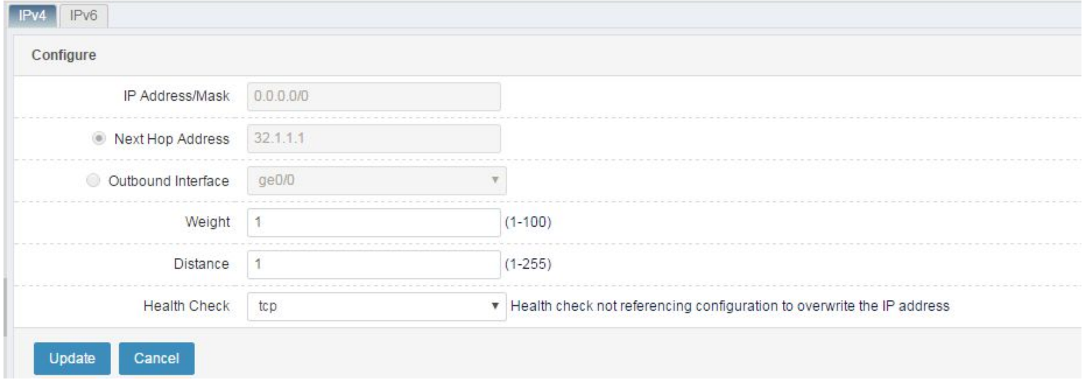
Configure

IP Address/Mask	0.0.0.0/0
● Next Hop Address	30.1.1.1
○ Outbound Interface	ge0/0 ▾
Weight	1 (1-100)
Distance	1 (1-255)
Health Check	icmp ▾ Health check not referencing configuration to overwrite the IP address



Configure

IP Address/Mask	0.0.0.0/0
● Next Hop Address	31.1.1.1
○ Outbound Interface	ge0/0 ▾
Weight	1 (1-100)
Distance	1 (1-255)
Health Check	icmp ▾ Health check not referencing configuration to overwrite the IP address



IPv4 | IPv6

Configure

IP Address/Mask: 0.0.0.0/0

● Next Hop Address: 32.1.1.1

○ Outbound Interface: ge0/0

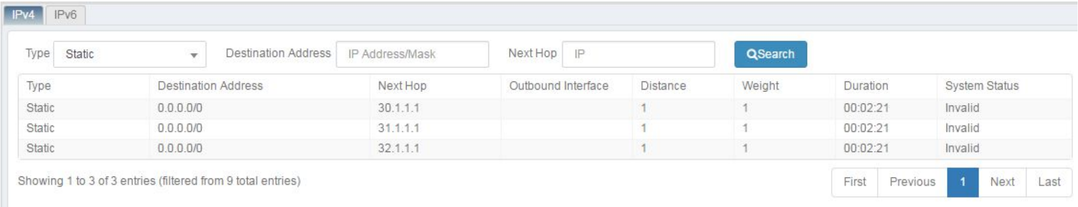
Weight: 1 (1-100)

Distance: 1 (1-255)

Health Check: tcp Health check not referencing configuration to overwrite the IP address

4. Choose **Network** > **Route** > **Routing table** to check the route status.

   If health check is successful, the route status is Valid. If health check fails, the route status is Invalid.



Type: Static Destination Address: IP Address/Mask Next Hop: IP

Type	Destination Address	Next Hop	Outbound Interface	Distance	Weight	Duration	System Status
Static	0.0.0.0/0	30.1.1.1		1	1	00:02:21	Invalid
Static	0.0.0.0/0	31.1.1.1		1	1	00:02:21	Invalid
Static	0.0.0.0/0	32.1.1.1		1	1	00:02:21	Invalid

Showing 1 to 3 of 3 entries (filtered from 9 total entries)

17.4 Troubleshooting

17.4.1 The Route Status is Invalid

Symptom	After a static route is configured, its status is Invalid.
Analysis	If health check is not configured for the static route, check whether: 1. The outbound interface for the next hop of the route is down. 2. No outbound interface is found for the next hop of the

	route. 3. A route with a preferred management distance exists among equal-cost routes. If health check is configured for the static route, also check whether: 1. Health check fails, which can be determined by checking the health check log. 2. The included IP address in the health check template is set to a non-next-hop IP address. 3. The timeout period and retry times of health check are set to small values. In this case, health check is deemed to fail if a health check packet does not get a response within the timeout period.
Solution	Identify the cause through the preceding analysis and solve the problem accordingly.

18 RIP Route

18.1Overview

RIP is an internal dynamic routing protocol based on the D-V algorithm, also called Bellmen-Ford algorithm. RIP is a commonly used Interior Gateway Protocol (IGP) and supports routing information exchange by UDP packets. The D-V algorithm is a vector distance algorithm and used to calculate routes in computer networks in the early stage of the Advanced Research Projects Agency Network (ARPANET). RIP is a standard adopted by routers and hosts to transmit routing information. It is widely used by IP router vendors. RIP is designed to run in small- and medium-sized networks that adopt the same technology. Therefore, it is applicable to many campus networks and continuous regional networks with moderate rate changes. RIP is not used in complex networks.

RIP determines the distance to the destination based on routing metric (hop count), and uses two packet forms: path information request packet and response packet. When a router port starts for the first time, it sends a request packet. A response packet, including the actual routing information, is sent to the neighboring port at a 30-second interval. RIP adopts split horizon and poison reverse to eliminate routing loops, and adopts triggered update and route timeout mechanisms to ensure correct routing.

18.2 Configuration

18.2.1 Default Configurations

RAVEN5000firewalls have the following default RIP configurations:

Default RIP configurations

Parameter	Default Value	Remarks
Enable/Disable RIP	Disabled	The default value can be changed.
Interface authentication type (options: **none**, **text**, and **md5**)	none	The default value can be changed.
Version	2	The default value can be changed.

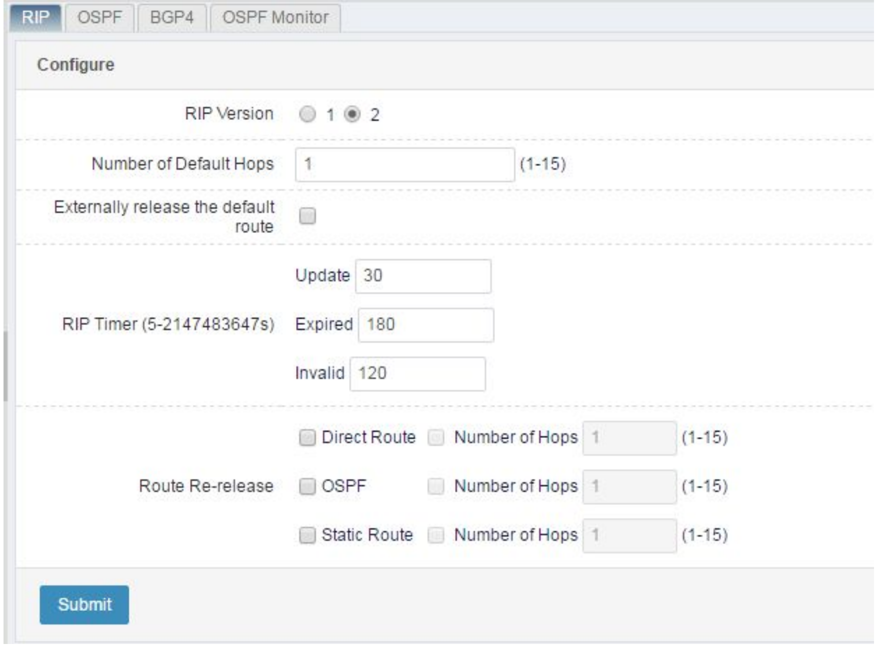
Parameter	Default Value	Remarks
Scheduled update time	30s	The default value is recommended.
Timeout period	180s	The default value is recommended.
Garbage-collection time	120s	The default value is recommended.

18.2.2 Configuring the RIP Version

You can configure the RIP version of received and sent packets when interface-based version configuration is unavailable. If advanced settings are not configured, the default settings apply.

Procedure:

1. Choose **Network** > **Route** > **Dynamic route** > **RIP**. The following page appears.



RIP Version ○ 1 ● 2

Number of Default Hops 1 (1-15)

Externally release the default route □

RIP Timer (5-2147483647s) Update 30 Expired 180 Invalid 120

Route Re-release □ Direct Route □ Number of Hops 1 (1-15)
□ OSPF □ Number of Hops 1 (1-15)
□ Static Route □ Number of Hops 1 (1-15)

Parameter description:

RIP version: Select **1** or **2**.

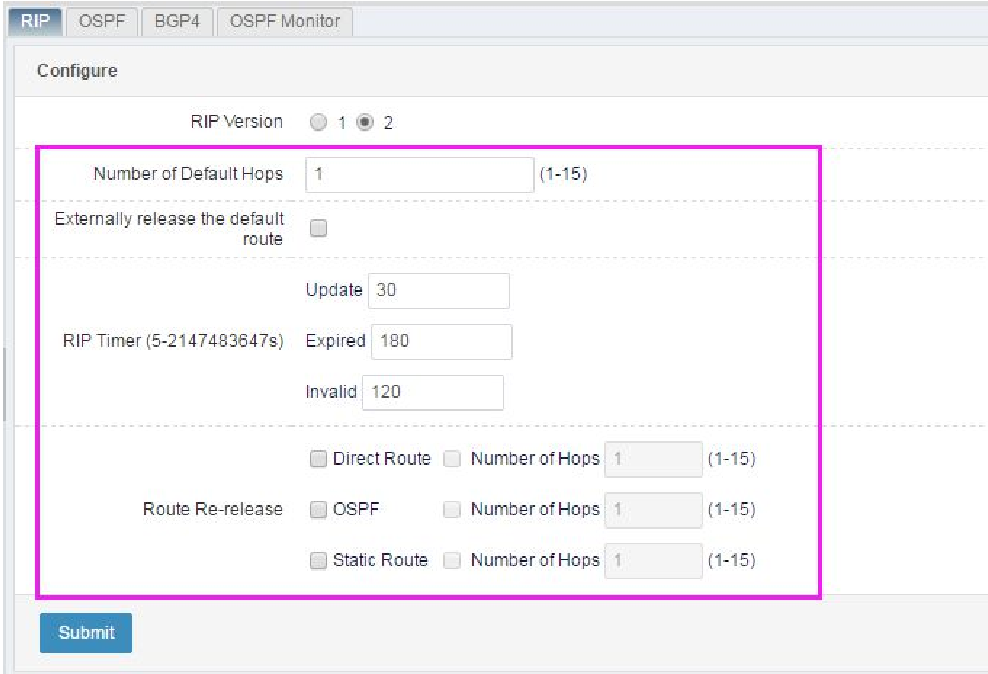
2. Keep the default advanced settings. Click **Submit**.

18.2.3 Configuring the Advanced RIP Settings

The advanced RIP settings include the default route re-advertisement metric, default route re-advertisement setting, trigger time for the scheduled update timer, timeout timer, and garbage-collection timer, and re-advertised route type setting.

Procedure:

1. Choose **Network** > **Route** > **Dynamic route** > **RIP**. The following page appears.



Configure

RIP Version	○ 1 ● 2			
Number of Default Hops	1 (1-15)			
Externally release the default route	□			
RIP Timer (5-2147483647s)	Update 30			
	Expired 180			
	Invalid 120			
Route Re-release	□ Direct Route	□ Number of Hops	1	(1-15)
	□ OSPF	□ Number of Hops	1	(1-15)
	□ Static Route	□ Number of Hops	1	(1-15)

Parameter description:

Default hop count: Default number of hops of the re-advertised route.

Advertise default route externally: Check this box to generate and advertise a default route.

RIP timer – **Update**: Trigger time for the scheduled update timer.

RIP timer – **Timeout**: Trigger time for the timeout timer.

RIP timer – **Invalid**: Trigger time for the garbage-collection timer.

Route re-advertisement – **Direct route**: Check this box to re-advertise direct routes.

Route re-advertisement – **OSPF**: Check this box to re-advertise OSPF routes.

Route re-advertisement – **Static route**: Check this box to re-advertise static routes.

Hop count: Metric for re-advertising direct routes, OSPF routes, and static routes.

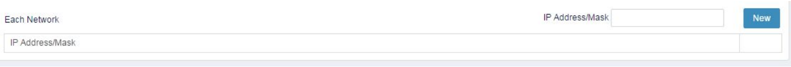
2. Click **Submit** after you complete the settings.

18.2.4 Configuring RIP Advertisement for a Network

You can configure route advertisement for the direct network where the system is located so that other routers can learn the routes destined for the local network.

Procedure:

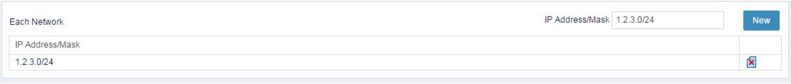
1. Choose **Network** > **Route** > **Dynamic route** > **RIP.** The following page appears.



IP Address/Mask	

IP address/Mask: Address of the local direct network, in the format of *A.B.C.D/M*.

2. Click **Add** to add the network.



IP Address/Mask 1.2.3.0/24

IP Address/Mask	
1.2.3.0/24	☒

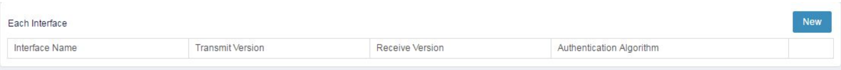
3. To delete an existing network, click ☒.

18.2.5 Configuring an RIP Interface

You can configure the version and authentication type of the packets sent and received by an interface.

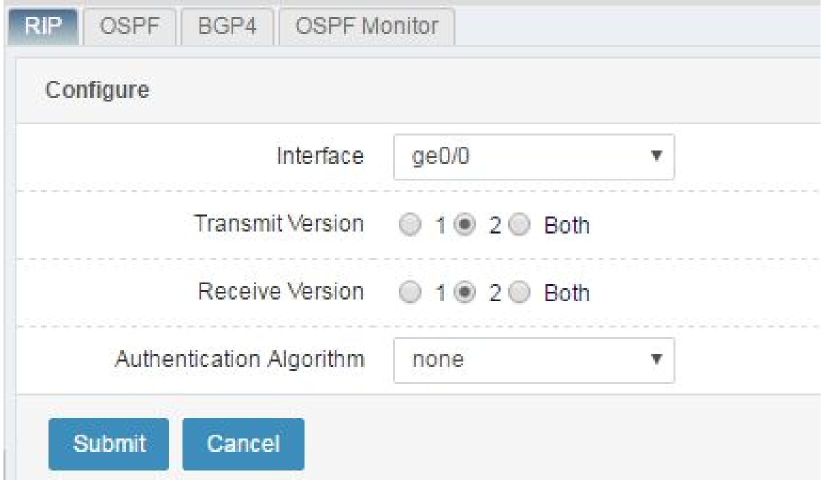
Procedure:

1. Choose **Network** > **Route** > **Dynamic route** > **RIP.** The following page appears.



Interface Name	Transmit Version	Receive Version	Authentication Algorithm	

2. Click **New.** The interface configuration page appears.



Configure

Interface: ge0/0

Transmit Version: ○ 1 ● 2 ○ Both

Receive Version: ○ 1 ● 2 ○ Both

Authentication Algorithm: none

Interface: Name of the interface to be configured.

Tx version: Version of the packets sent by the interface.

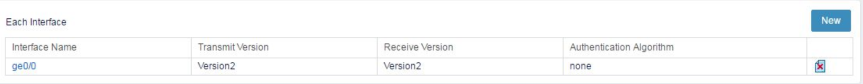
Rx version: Version of the packets received by the interface.

Authentication algorithm: Authentication type of the interface.

Submit: Click this button to submit the settings.

Cancel: Click this button to cancel the configuration.

3. Click **Submit** after you complete the settings.



Each Interface

Interface Name	Transmit Version	Receive Version	Authentication Algorithm	
ge0/0	Version2	Version2	none	☒

Click an interface name to modify its settings.

Click ☒ to delete an interface.

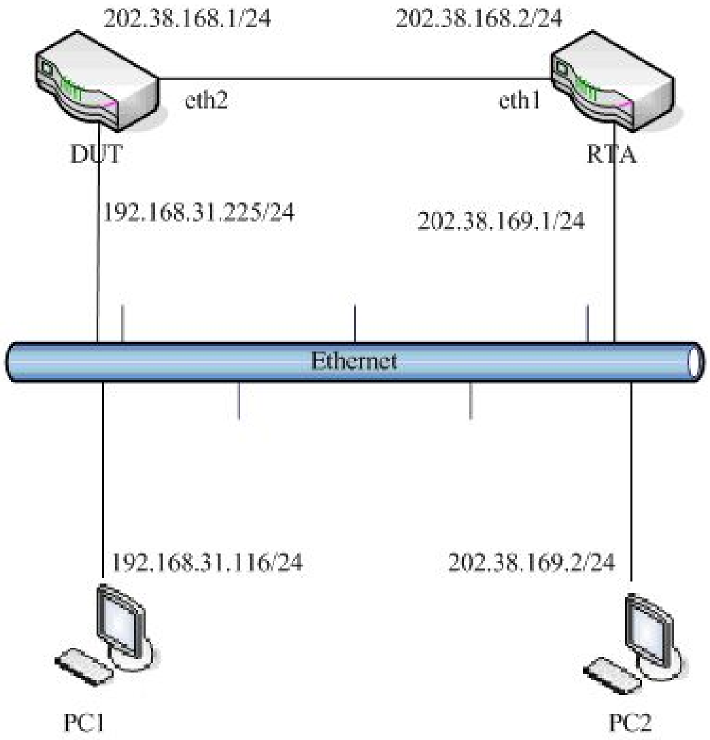
18.3 Configuration Example

18.3.1 Configuring Connection Between Two T-series Firewalls

Description:

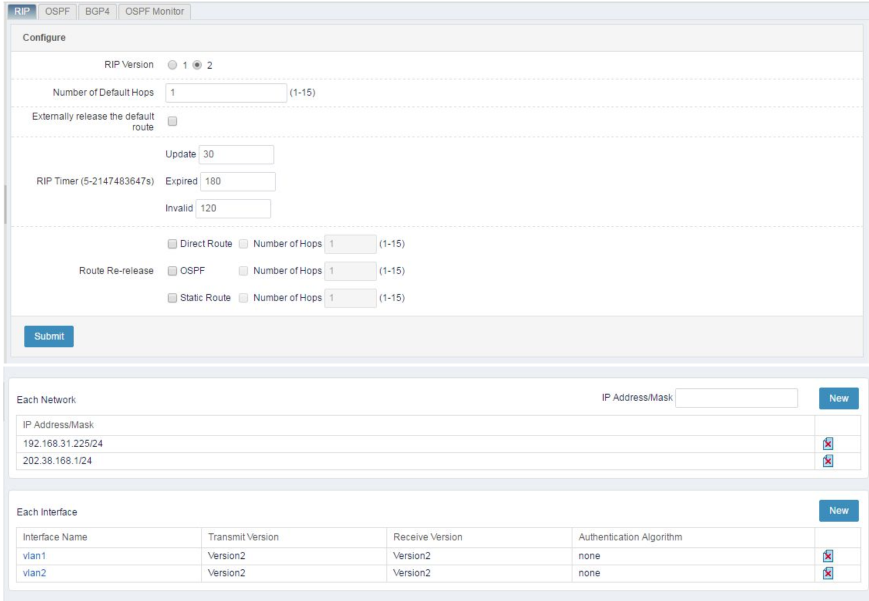
In the following figure, DUT and RTA are T-series firewalls and configured with IP addresses. Enable RIP on DUT's VLAN 1 and VLAN 2 interfaces and on RTA's VLAN 1 and VLAN 2 interfaces. Set the RIP version of the packets exchanged between the interfaces of DUT and RTA to 2.

Network diagram:



Procedure:

1. Configure the basic information about DUT.



Configure

RIP Version	○ 1 ● 2
Number of Default Hops	1 (1-15)
Externally release the default route	□
RIP Timer (5-2147483647s)	Update 30 Expired 180 Invalid 120
Route Re-release	□ Direct Route □ Number of Hops 1 (1-15) □ OSPF □ Number of Hops 1 (1-15) □ Static Route □ Number of Hops 1 (1-15)

Each Network

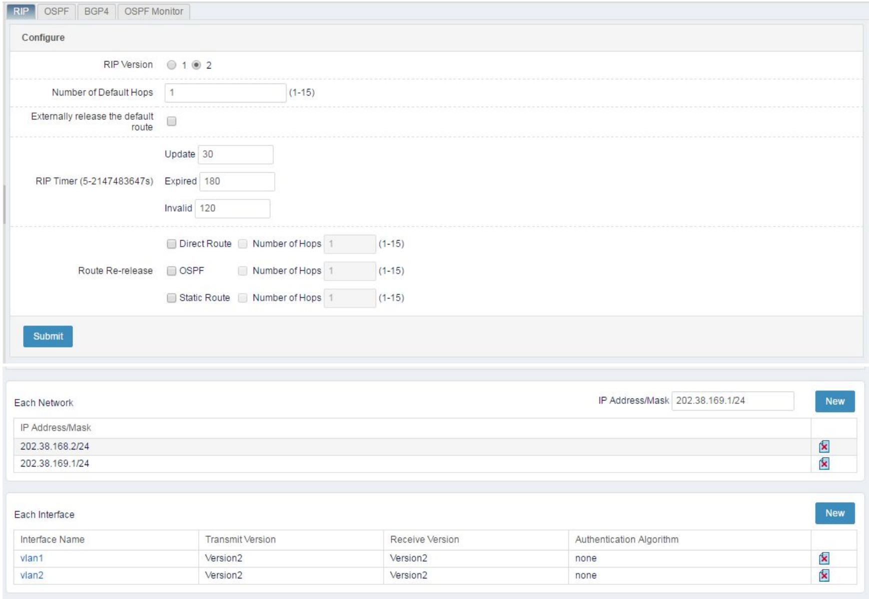
IP Address/Mask

IP Address/Mask	
192.168.31.225/24	☒
202.38.168.1/24	☒

Each Interface

Interface Name	Transmit Version	Receive Version	Authentication Algorithm	
vlan1	Version2	Version2	none	☒
vlan2	Version2	Version2	none	☒

2. Configure the basic information about RTA.



Configure

RIP Version ○ 1 ● 2

Number of Default Hops 1 (1-15)

Externally release the default route □

RIP Timer (5-2147483647s) Update 30 Expired 180 Invalid 120

Route Re-release □ Direct Route □ Number of Hops 1 (1-15)
□ OSPF □ Number of Hops 1 (1-15)
□ Static Route □ Number of Hops 1 (1-15)

Each Network IP Address/Mask 202.38.169.1/24

IP Address/Mask	
202.38.168.2/24	☒
202.38.169.1/24	☒

Each Interface

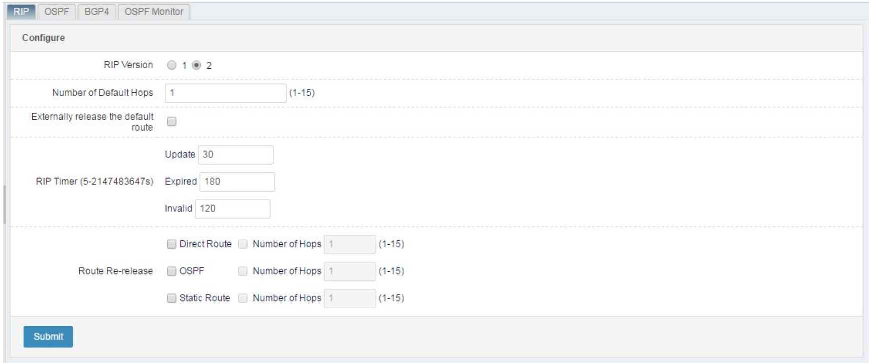
Interface Name	Transmit Version	Receive Version	Authentication Algorithm	
vlan1	Version2	Version2	none	☒
vlan2	Version2	Version2	none	☒

3. Set the gateway address for PC 1 to 192.168.31.225, and set the gateway address for PC 2 to 202.38.169.1. Ping PC 2 from PC 1, and ensure that the ping test is successful.

18.4 Displaying RIP Configurations

18.4.1 Procedure

Choose **Network** > **Route** > **Dynamic route** > **RIP**. A page appears to display the RIP configurations.



Configure

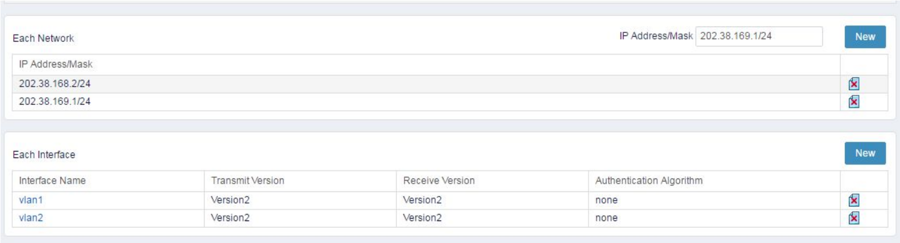
RIP Version ○ 1 ● 2

Number of Default Hops 1 (1-15)

Externally release the default route □

RIP Timer (5-2147483647s) Update 30 Expired 180 Invalid 120

Route Re-release □ Direct Route □ Number of Hops 1 (1-15)
□ OSPF □ Number of Hops 1 (1-15)
□ Static Route □ Number of Hops 1 (1-15)



Each Network

IP Address/Mask 202.38.169.1/24

IP Address/Mask	
202.38.168.2/24	☒
202.38.169.1/24	☒

Each Interface

Interface Name	Transmit Version	Receive Version	Authentication Algorithm	
vlan1	Version2	Version2	none	☒
vlan2	Version2	Version2	none	☒

18.5 Troubleshooting

18.5.1 Communication Between Two Firewalls Is Abnormal

Symptom	The communication between two firewalls is abnormal.
Analysis	The RIP versions or authentication types of the packets exchanged between the firewall interfaces do not match, or the interfaces are improperly configured.
Solution	Check and modify the interface configurations.

19 OSPF Route

19.1 Overview

Open Shortest Path First (OSPF) is a dynamic routing protocol which implements routing between networks.

OSPF is an IGP running in an autonomous system (AS) to determine routing. OSPF is a link-state routing protocol, which is different from RIP, an equidistance vector routing protocol. OSPF can generate routes quickly to adapt to link changes, and manage ASs of a range much larger than the management range of RIP.

OSPF is a link-state routing protocol running in an AS. A link state database is constructed based on the link-state advertisement (LSA) messages exchanged between routers. The shortest path tree is calculated for each node using the OSPF algorithm to determine routing. OSPF works differently from RIP and IGRP. OSPF only sends the information about routing from the current node to the neighboring node, whereas RIP and IGRP sends the entire or part of the routing table of the current node to the neighboring node, which then updates its routing table based on the received information. The information volume sent by OSPF is less than RIP. OSPF supports the IP subnet structure in LSA messages.

OSPF periodically sends a Hello packet to the neighboring router, and receives a Hello packet from the neighboring router. The Hello packet helps the router understand the neighbor's structure and running condition. The local router cannot receive a Hello packet from the neighbor when the neighbor is powered off or the link is unreachable. In this way, the local router can determine which neighboring router fails and quickly adapt to changes of the network topology.

For a network supporting multiple routers, a designated router (DR) and a backup DR (BDR) can be elected among the OSPF routers in the same network segment. When the link state database is synchronized, the DR sends LSA messages across the network to reduce traffic cost.

19.2Configuration

19.2.1 Default Configurations

RAVEN5000firewalls have the following default OSPF configurations:

Default OSPF configurations

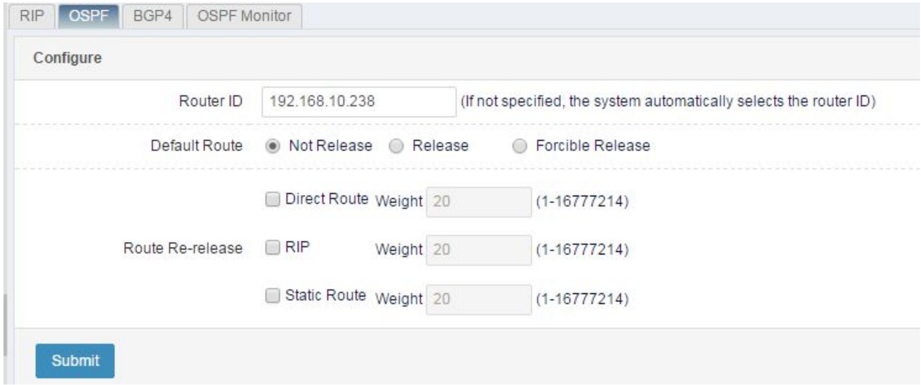
18.5.1.1 Parameter	2. Default Value	3. Remarks
Enable/Disable OSPF	Disabled	The default value can be changed.
OSPF area authentication type (options: **none**, **text**, and **md5**)	none	The default value can be changed.
Interface authentication type (options: **none**, **text**, and **md5**)	none	The default value can be changed.
Advertise default route	No	The default value can be changed.
LSA retransmission time	5s	The default value is recommended.
LSA transmission delay	1s	The default value is recommended.
Hello interval	10s	The default value can be changed.
Dead interval	Four times **Hello interval**	The default value can be changed.
Interface-elected DR priority	1	The default value can be changed.

19.2.2 Configuring OSPF

In OSPF, a router ID uniquely identifies a router in an AS. A router ID is automatically selected after OSPF is enabled. If loopback interfaces exist, the router ID is specified as the greatest loopback address. If no loopback interfaces exist, the router ID is specified as the greatest interface IP address. It is recommended that you specify the router ID manually.

Route re-advertisement is a process where routes of other types are advertised to an OSPF AS.

1. Choose **Network** > **Route** > **Dynamic route** > **OSPF**. The following page appears.



Configure

Router ID	192.168.10.238 (If not specified, the system automatically selects the router ID)
Default Route	● Not Release ○ Release ○ Forcible Release
Route Re-release	□ Direct Route Weight 20 (1-16777214) □ RIP Weight 20 (1-16777214) □ Static Route Weight 20 (1-16777214)

Router ID: Enter a router ID. If you do not set this parameter, a router ID will be automatically selected.

Default route: Check this box to advertise a default route. Select **Advertise forcibly** if the routing table has no default route information but it is required to advertise a default route.

Direct route: Check this box to re-advertise direct routes.

Static route: Check this box to re-advertise static routes.

RIP route: Check this box to re-advertise RIP routes.

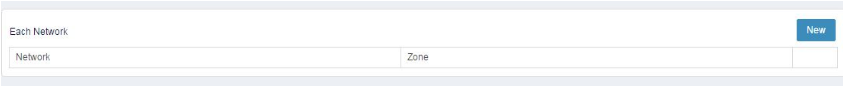
Weight: Weight of the re-advertised route.

2. Click **Submit** after you complete the settings.

19.2.2 Configuring an OSPF Network

You can configure an OSPF-enabled interface and the area it belongs to.

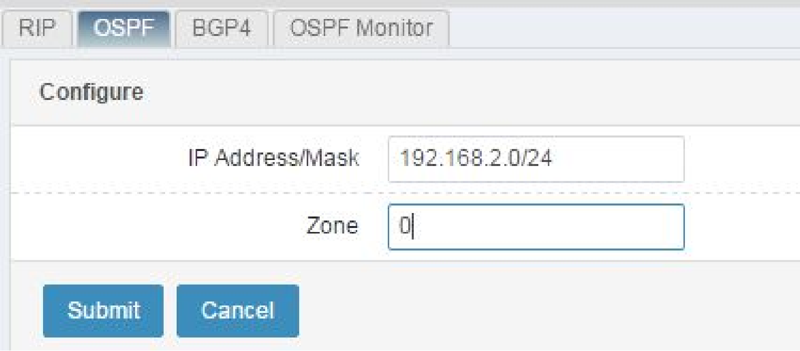
1. Choose **Network** > **Route** > **Dynamic route** > **OSPF**. The following page appears.



Each Network

Network	Zone

2. Click **Add**. The following page appears.



Configure

IP Address/Mask: 192.168.2.0/24

Zone: 0

IP address/Mask: Network address and its mask.

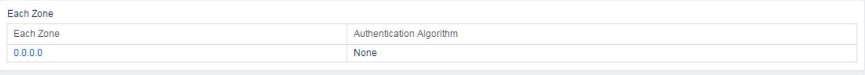
Area: Area ID.

3. Click **Submit** after you complete the settings.

19.2.3 Modifying Area Attributes

Modify the authentication mode of an area as follows:

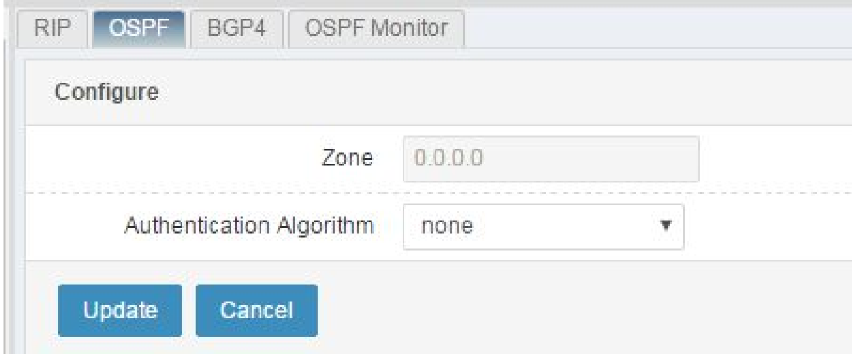
1. Choose **Network** > **Route** > **Dynamic route** > **OSPF**. The following page appears.



Each Zone

Each Zone	Authentication Algorithm
0.0.0.0	None

2. Click an area ID to modify the area attributes.



Configure

Zone: 0.0.0.0

Authentication Algorithm: none

Area: Area ID.

Authentication algorithm: The options are **none** (no authentication), **text** (plaintext authentication), and **md5** (ciphertext authentication).

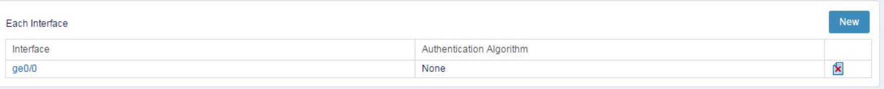
3. Click **Update**.

19.2.4 Configuring an OSPF Interface

You can configure the version and authentication type of the packets sent and received by an interface.

Procedure:

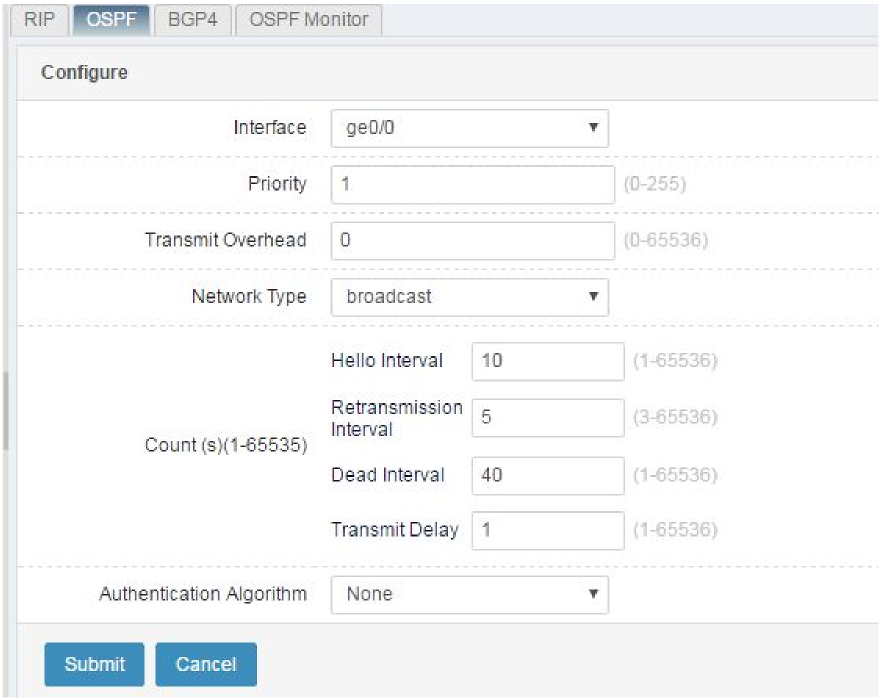
1. Choose **Network** > **Route** > **Dynamic route** > **OSPF**. The following page appears.



Each Interface

Interface	Authentication Algorithm	
ge0/0	None	☒

2. Click **New**. The interface configuration page appears.



Configure

Interface	ge0/0 ▾	
Priority	1	(0-255)
Transmit Overhead	0	(0-65536)
Network Type	broadcast ▾	
Count (s)(1-65535)	Hello Interval: 10	(1-65536)
	Retransmission Interval: 5	(3-65536)
	Dead Interval: 40	(1-65536)
	Transmit Delay: 1	(1-65536)
Authentication Algorithm	None ▾	

Interface: Name of the interface to be configured.

Priority: Priority of the DR and BDR elected on the interface.

Tx cost: Cost of packet sending. **0** indicates calculating the cost based on the interface type and rate.

Network type: OSPF network type of the interface.

Authentication algorithm: Authentication type of the interface. The options are **none** (no authentication), **text** (plaintext authentication), and **md5** (ciphertext authentication).

Password: Key used by plaintext authentication. This parameter is valid when **text** is selected for **Authentication algorithm**.

ID: Key ID. This parameter is valid when the authentication password is MD5.

Key: Key used by ciphertext authentication. This parameter is valid when the authentication password is MD5.

Hello interval: Interval at which Hello packets are sent.

Dead interval: Interval after which the neighboring router is deemed to fail.
Retransmission interval: Interval at which LSA messages are retransmitted.

Transmission delay: Delay after which LSA messages are sent.

Submit: Click this button to submit the settings.

Cancel: Click this button to cancel the configuration.

Notice

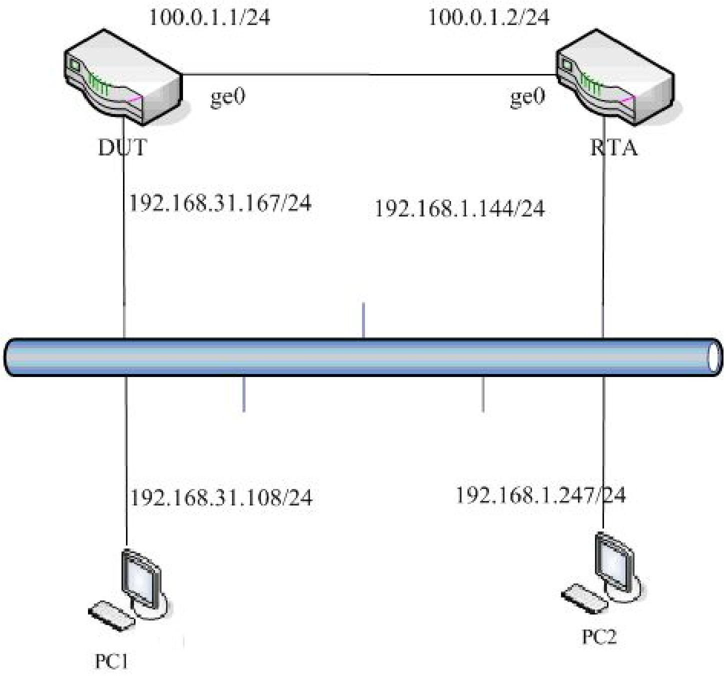
If you choose to keep the default parameter settings of the OSPF interface, the web page does not display the interface information after you click **Submit**. The interface information is displayed only when some default values are changed.

19.3 Configuration Example

Configuring Connection Between Two T-series Firewalls

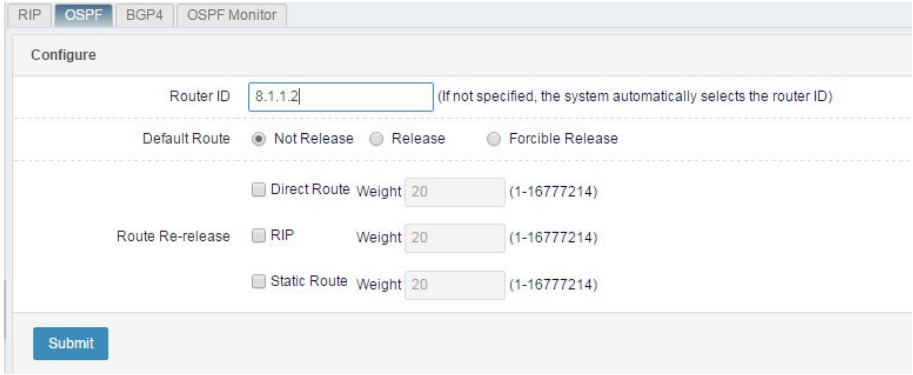
Description:

In the following figure, DUT and RTA are T-series firewalls and configured with IP addresses. Enable OSPF on DUT and RTA so that DUT can learn the route to 192.168.1.0/24 and RTA can learn the route to 192.168.31.0/24.



Procedure:

1. Configure the basic information about DUT.



Router ID: 8.1.1.2 (If not specified, the system automatically selects the router ID)

Default Route: ● Not Release ○ Release ○ Forcible Release

Route Re-release:

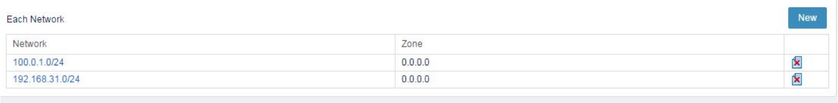
□ Direct Route Weight 20 (1-16777214)

□ RIP Weight 20 (1-16777214)

□ Static Route Weight 20 (1-16777214)

Because the router ID is automatically generated by election, you can leave this parameter unspecified and click **Submit**.

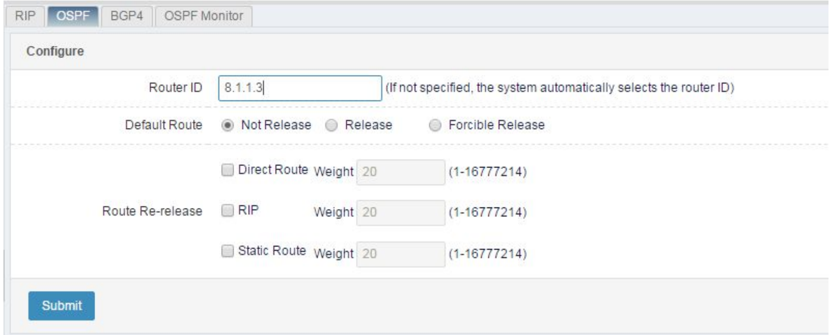
2. Configure the network whose routing information will be advertised by DUT.



Each Network

Network	Zone	
100.0.1.0/24	0.0.0.0	☒
192.168.31.0/24	0.0.0.0	☒

3. Configure the basic information about RTA.



Router ID: 8.1.1.3 (If not specified, the system automatically selects the router ID)

Default Route: ● Not Release ○ Release ○ Forcible Release

Route Re-release:

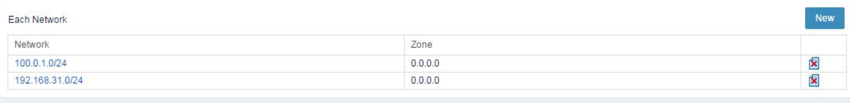
□ Direct Route Weight 20 (1-16777214)

□ RIP Weight 20 (1-16777214)

□ Static Route Weight 20 (1-16777214)

Because the router ID is automatically generated by election, you can leave this parameter unspecified and click **Submit**.

4. Configure the network whose routing information will be advertised by RTA.



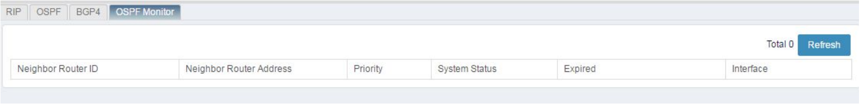
Each Network

Network	Zone	
100.0.1.0/24	0.0.0.0	☒
192.168.31.0/24	0.0.0.0	☒

19.4 Monitoring and Maintenance

Displaying the Neighboring Router Status

Choose **Route** > **Dynamic route** > **OSPF** > **Monitor** to display the neighboring router status.



Neighbor Router ID	Neighbor Router Address	Priority	System Status	Expired	Interface

19.5 Troubleshooting

Two Firewalls Cannot Establish a Neighbor Relationship

Symptom	Two firewalls cannot establish a neighbor relationship.
Analysis	1. Check whether the area IDs match. 2. Check whether the authentication types match. 3. Check whether the keys match. 4. Check whether the subnet masks match. 5. Check whether the **Hello interval** values match. 6. Check whether the **Dead interval** values match. 7. Check whether the two firewalls need to establish a neighbor relationship.
Solution	1. Check the OSPF parameter settings on the interface. 2. Check whether a neighbor relationship needs to be established with the neighboring router. A neighbor relationship will be established if one or more of the following conditions are met: A. The network type is point-to-point. B. The network type is point-to-multipoint. C. The network type is virtual link. D. The local router is a DR in the network where the neighboring router is located. E. The local router is a BDR in the network where the neighboring router is located. F. The neighboring router is a DR. G. The neighboring router is a BDR.

20 BGP Route

20.1 Overview

The Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) for the communication between routers in different ASs. It is used to exchange network reachability information between AS and eliminate routing loops.

BGP adopts TCP for reliable transmission.

A BGP-enabled router is called a BGP speaker. The BGP speakers that set up a BGP session are called BGP peers. BGP peers can be formed in two modes: Internal BGP (IBGP) and External BGP (EBGP). IBGP is used to establish BGP connection within an AS, whereas EBGP is used to establish BGP connection across ASs. Simply put, EBGP exchanges routing information between AS, whereas IBGP transmits routing information within an AS.

RAVEN 5000 firewalls support BGP-4, which has the following features: Manual router ID configuration

Manual BGP peer designation

BGP peer group

Use of loopback interfaces

Multihop EBGP connection

Received routes limit

Private AS number filter

Timer setup

BGP-IGP interaction

BGP route aggregation

BGP route dampening

BGP route reflector

AS federation

Management distance configuration

BGP soft reset

BGP monitoring and maintenance

The following route attributes are supported:

ORIGN

AS_PATH

NEXT_HOP

MULTI_EXIT_DISC LOCAL-

PREFERENCE

ATOMIC_AGGREGATE

AGGREGATOR

COMMUNITY

ORIGINATOR_ID

CLUSTER_LIST

BGP-4 also supports policy-based handling of sent and received routes, AS path list filter, access list filter, prefix list filter, distribution control list filter, and route mapping filter.

20.2 Configuration

20.2.1 Default Configurations

Default BGP configurations

Parameter	Default Value	Remarks
Router ID	If loopback interfaces are configured, the router ID is specified as the greatest loopback address. If no loopback interfaces are configured, the router ID is specified as the greatest physical interface IP address.	The default value can be changed.
20.2.1.1 Generate default route	No	The default value can be changed.
EBGP multihop	Off/255	The default value can be changed.
20.2.1.3 Advertise default route	No	The default value can be changed.

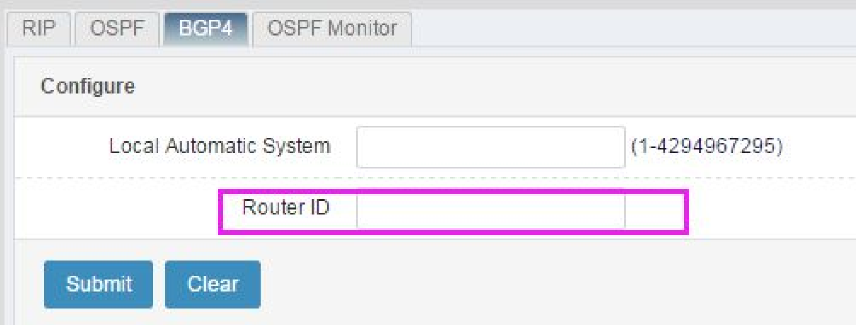
Parameter	Default Value	Remarks
5. TCP MD5 authentication	none	The default value cannot be changed.
6. Keepalive Time	60s	The default value is recommended.
7. Holdtime	180s	The default value can be changed.
8. ConnectRetry time	120s	The default value cannot be changed.
9. AdvIntelval (IBGP)	15s	The default value is recommended.
10. Advintelval (EBGP)	30s	The default value is recommended.
11. Bgp scan time	60s	The default value can be changed.
12. MED	0	The default value can be changed.
13. Local_pref	100	The default value can be changed.
14. Link aggregation	Disabled	The default value can be changed.
15. Link dampening	Disabled	The default value can be changed.
16. Suppress limit	2000	The default value can be changed.
17. Half-life-time	15 minutes	The default value can be changed.
18. Reuse limit	750	The default value can be changed.
19. Max-suppress time	Four times **Half-life-time**	The default value can be changed.
20. Management distance	EBGP 20 IBGP 200 Local 200	
21. IGP route check	No	The default value can be changed.

20.2.2 Configuring a BGP Router ID

In BGP, a router ID uniquely identifies a router in an AS. A router ID is automatically selected after BGP is enabled. The greatest IP address of a loopback address is typically selected as the router ID. If no loopback address exists, the greatest IP address of an up interface is selected as the router ID. The router ID can also be specified manually. If advanced settings are not configured, the default settings apply.

Procedure:

1. Choose **Network** > **Route** > **Dynamic route** > **BGP4**. The following page appears.



Parameter description:

Router ID: Enter a router ID. If you do not set this parameter, a router ID will be automatically selected.

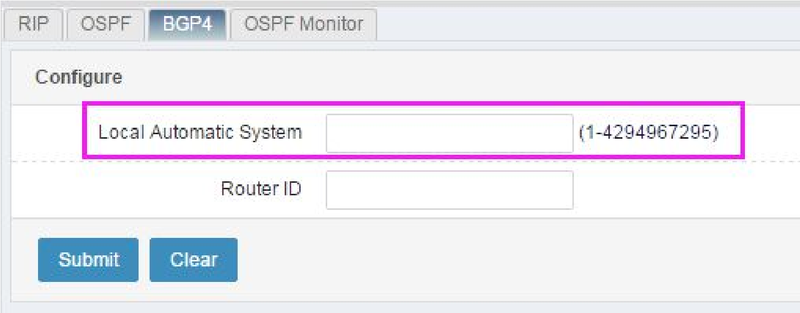
2. Click **Submit** after you complete the settings. The default advanced settings are kept.

20.2.3 Enabling BGP

This section describes how to enable BGP.

Procedure:

1. Choose **Network** > **Route** > **Dynamic route** > **BGP4**. The following page appears.



Parameter description:

Local AS number: The value ranges from 1 to 4294967295.

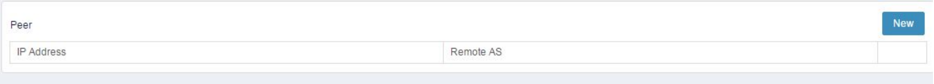
2. Click **Submit** after you complete the settings.

20.2.4 Configuring a BGP Peer

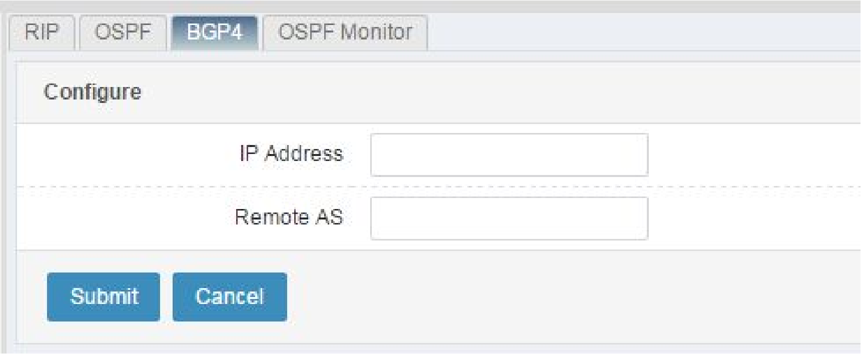
This section describes how to configure a BGP peer.

Procedure:

1. Choose **Network** > **Route** > **Dynamic route** > **BGP4**. The following page appears.



2. Click **Add**.



IP address: IP address of the peer.

Remote AS: Number of the remote AS.

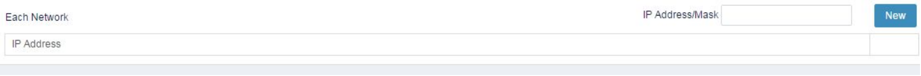
3. Click **Submit** after you complete the settings. To cancel the configuration, click **Cancel**.

20.2.5 Configuring Route Advertisement for a Network

You can configure route advertisement for a network.

Procedure:

1. Choose **Network** > **Route** > **Dynamic route** > **BGP4**. The following page appears.



IP address/Mask: IP address and subnet mask of the network whose routing information will be advertised.

2. Click **Add** to add the network.

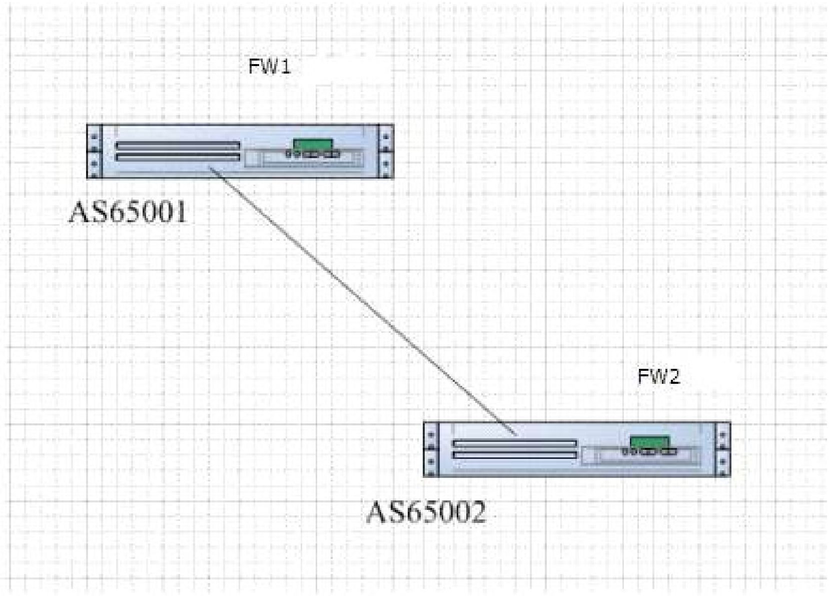
20.3 Configuration Example

20.3.1 Configuring Connection Between Two Firewalls

Description:

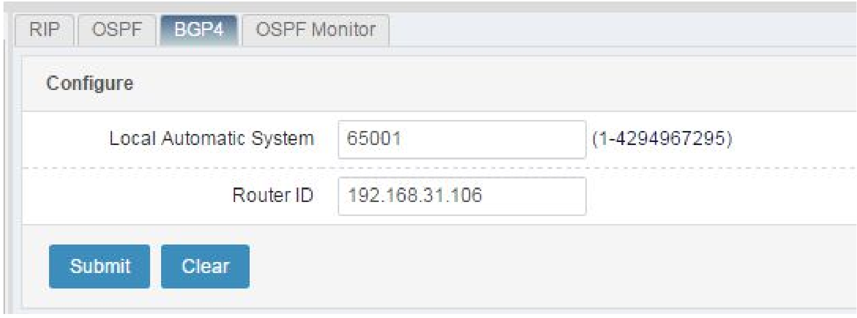
FW1 and FW2 are RAVEN5000 networks. FW1 belongs to AS65001 and its router ID is 192.168.31.106. FW2 belongs to AS65002 and its router ID is 192.168.31.107. Configure FW1 and FW2 as EBGP peers.

Network diagram:



Procedure:

1. Enable BGP on FW1.

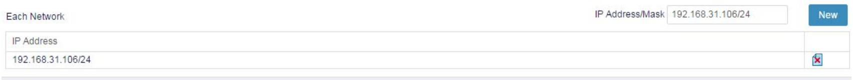


Configure

Local Automatic System: 65001 (1-4294967295)

Router ID: 192.168.31.106

2. Configure route advertisement for the network where FW1 is located.

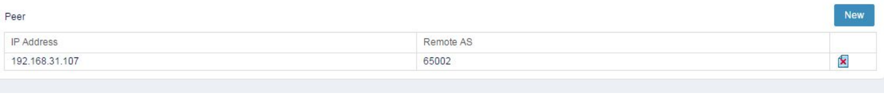


Each Network

IP Address/Mask: 192.168.31.106/24

IP Address	
192.168.31.106/24	☒

3. Configure a peer for FW1.



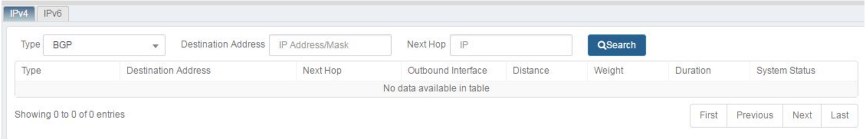
IP Address	Remote AS	
192.168.31.107	65002	☒

4. Repeat the preceding steps on FW2.

20.4 Monitoring and Maintenance

Displaying BGP Routing Information

Choose **Network** > **Route** > **Routing table**. Select **BGP** for **Type** and click **Search** to display BGP routing information.



Type: BGP

Destination Address: IP Address/Mask

Next Hop: IP

Type	Destination Address	Next Hop	Outbound Interface	Distance	Weight	Duration	System Status
No data available in table							

Showing 0 to 0 of 0 entries

20.5 Troubleshooting

20.5.1 Two Firewalls Cannot Establish a Neighbor Relationship

Symptom	Two firewalls cannot establish a neighbor relationship.
Analysis	1. The route between the two peers is unreachable. 2. The IP addresses or AS numbers of the peers are incorrect. 3. Open packet negotiation fails. 4. The route configured with a loopback interface is unreachable. 5. The network between IGP peers is unreachable. 6. The route IDs conflict.
Solution	1. Check the interface configurations. 2. Enable debugging. 3. Perform packet capture analysis.

21 Policy-based Routing

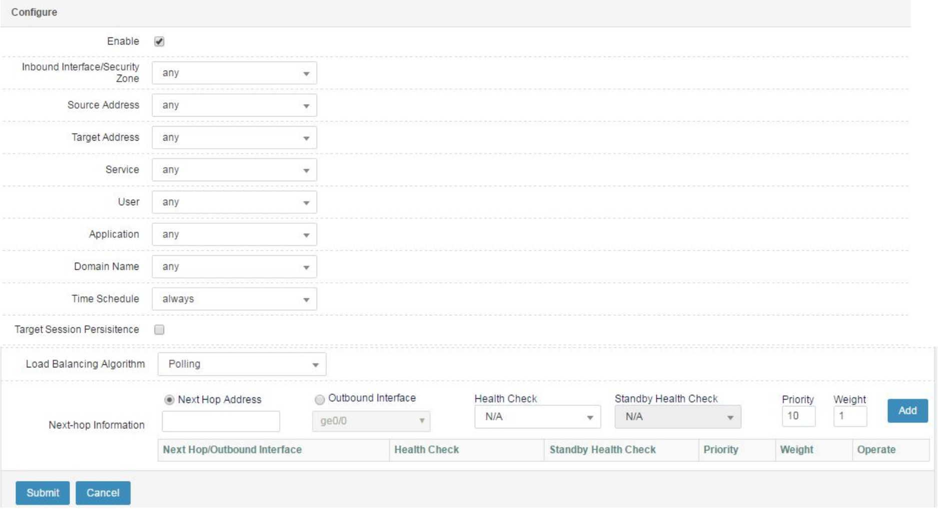
21.1 Overview

Policy-based routing (PBR) is a technique used to determine the next hop for an IP packet based on a range of elements or their combination such as the source address, destination address, inbound interface, service, user, application, domain name, and time table. PBR supports round robin, weighted round robin, source IP address hash, and source IP address and port hash to determine the next hop. It can change the next hop availability status based on the health check result. PBR is a flexible routing technique with a priority higher than route selection.

21.2 Configuration

21.2.1 Creating a PBR Policy

1. Configure an address object, a service object, an application object, a time object, and a health check template before creating a PBR policy.
2. Choose **Network** > **Route** > **PBR** and click **New**.



Configure

Enable ☑

Inbound Interface/Security Zone: any

Source Address: any

Target Address: any

Service: any

User: any

Application: any

Domain Name: any

Time Schedule: always

Target Session Persisitence ☐

Load Balancing Algorithm: Polling

Next-hop Information: ● Next Hop Address ○ Outbound Interface: ge0/0 Health Check: N/A Standby Health Check: N/A Priority: 10 Weight: 1

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate

Parameter description:

Enable: Check this box to enable the new PBR policy. The PBR policy will be matched only after it is enabled.

Inbound interface: Inbound interface of the virtual link. Only the packets passing the inbound interface are matched with PBR policies. The value **Any** indicates all interfaces.

Source address: Source address or network segment of the PBR policy. The value **Any** indicates all source addresses.

Destination address: Destination address or network segment of the PBR policy. The value **Any** indicates all source addresses.

Service: Service object of the PBR policy. The value **Any** indicates all destination services.

User: User object of the PBR policy. The option **any** indicates all users.

Application: Application object of the PBR policy. The option **any** indicates all applications.

Domain name: Domain name object of the PBR policy. The option **any** indicates all domain names.

Time table: Time object of the PBR policy. The option **always** indicates all time points.

Destination session persistence: Check this box to enable session persistence based on the destination address.

Load balancing algorithm: Algorithm used to determine the next hop. Round robin, weighted round robin, source IP address hash, and source IP address and port hash are supported.

Gateway: Address of the next hop.

Health check: Reference a health check template to detect the health status of the next hop.

Backup health check: Reference a health check template to detect the health status of the next hop. The gateway address is considered invalid when the primary health check and backup health check fail.

Priority: Priority of the next hop. The value ranges from 1 to 100.

Weight: Weight of the next hop. The value ranges from 1 to 255.

3. Click **Submit** after you complete the settings.

Notice

1. PBR has a higher priority than route selection.
2. PBR checks for conflicts by interface, source address, and destination address. A configuration error message is displayed if the configurations overlap or conflict.
3. The next hop with a higher priority is preferred. If the health

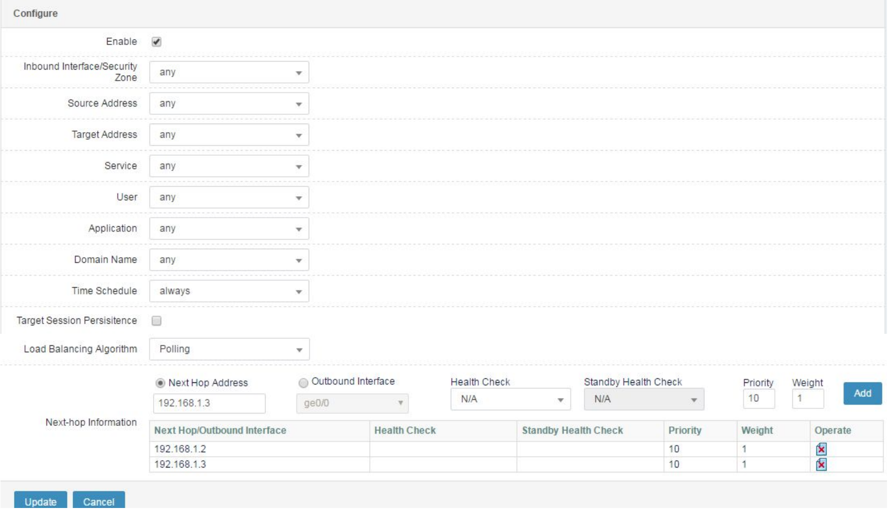
check on a link with a high priority fails, packets are forwarded to the next hop with a lower priority. After the high-priority link recovers, subsequent packets are forwarded to its next hop.

4. If the health check object is a non-next-hop address, ensure that the firewall has a route to the address and the next hop matches the next hop address of the PBR policy.

5. For a directly connected network segment, the firewall searches for a direct route for forwarding packets without PBR matching.

21.2.2 Modifying a PBR Policy

1. Choose **Network** > **Route** > **PBR** and click a PBR policy ID.
2. Modify the parameters of the PBR policy, as shown in the following figure.



Configure

Enable	☑
Inbound Interface/Security Zone	any
Source Address	any
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	always
Target Session Persisitence	□
Load Balancing Algorithm	Polling

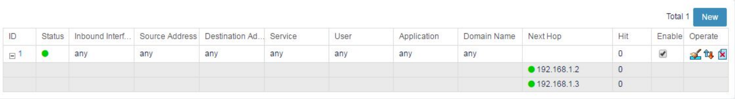
Next-hop Information: ● Next Hop Address 192.168.1.3 ○ Outbound Interface ge0/0 Health Check N/A Standby Health Check N/A Priority 10 Weight 1

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
192.168.1.2			10	1	☒
192.168.1.3			10	1	☒

3. Click **Update** to apply the modification.

21.2.3 Deleting a PBR Policy

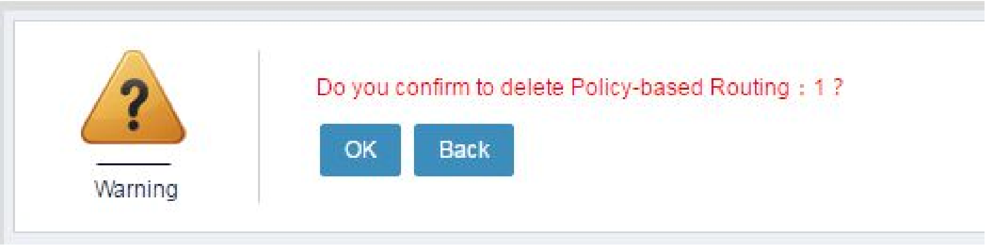
1. Choose **Network** > **Route** > **PBR**. The following page appears.



Total 1

ID	Status	Inbound Interf...	Source Address	Destination Ad...	Service	User	Application	Domain Name	Next Hop	Hit	Enable	Operate
⊟ 1	●	any	any	any	any	any	any	any		0	☑	
									● 192.168.1.2	0		
									● 192.168.1.3	0		

2. Click ☒ next to the PBR policy you want to delete.



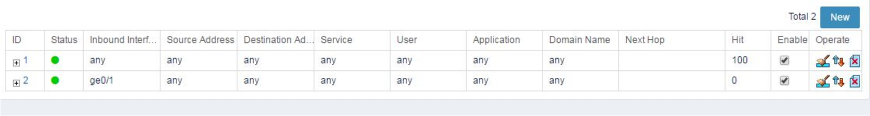
Warning

Do you confirm to delete Policy-based Routing : 1 ?

1. Click **OK**.

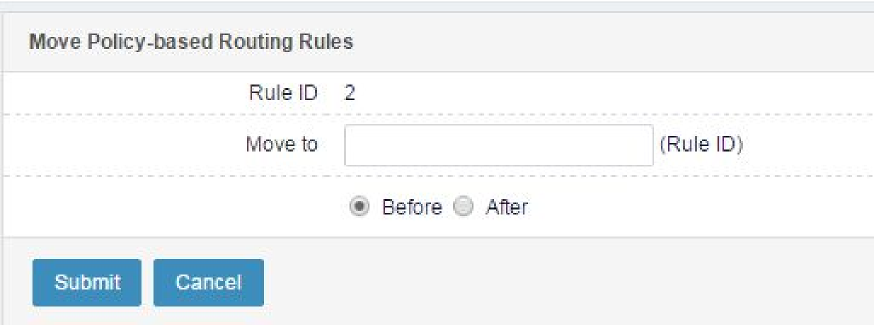
21.2.4 Adjusting the Order of PBR Policies

1. Choose **Network** > **Route** > **PBR**. The following page appears.



ID	Status	Inbound Interf...	Source Address	Destination Ad...	Service	User	Application	Domain Name	Next Hop	Hit	Enable	Operate
⊞ 1	●	any	any	any	any	any	any	any		100	☑	
⊞ 2	●	ge0/1	any	any	any	any	any	any		0	☑	

2. Click ⇅ to adjust the match priority of a PBR policy.



Move Policy-based Routing Rules

Rule ID 2

Move to (Rule ID)

● Before ○ After

Rule ID: ID of the PBR policy to be moved.

Move to: Reference policy ID.

Before: Move the PBR policy before the reference policy ID.

After: Move the PBR policy after the reference policy ID.

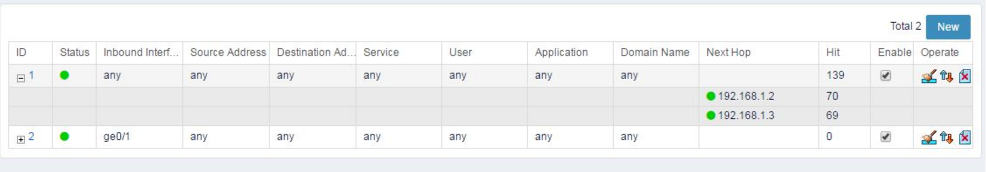
Notice

PBR policies are matched from top down as listed on page. Once a policy is hit, the remaining ones are not matched. When no PBR policy is hit, traffic is matched with routing and forwarding policies.

21.2.5 Enabling or Disabling a PBR Policy

1. Choose **Network** > **Route** > **PBR**, and check the **Enable** check box next to

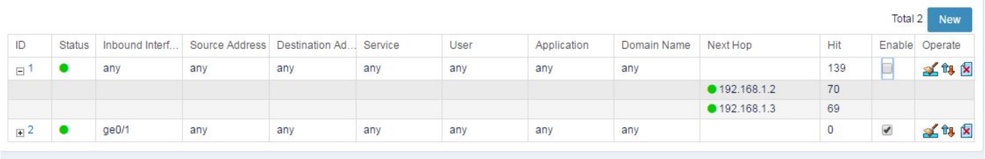
the PBR policy you want to enable.



Total 2 New

ID	Status	Inbound Interf...	Source Address	Destination Ad...	Service	User	Application	Domain Name	Next Hop	Hit	Enable	Operate
⊟ 1	●	any	any	any	any	any	any	any		139	☑	
									● 192.168.1.2	70		
									● 192.168.1.3	69		
⊞ 2	●	ge0/1	any	any	any	any	any	any		0	☑	

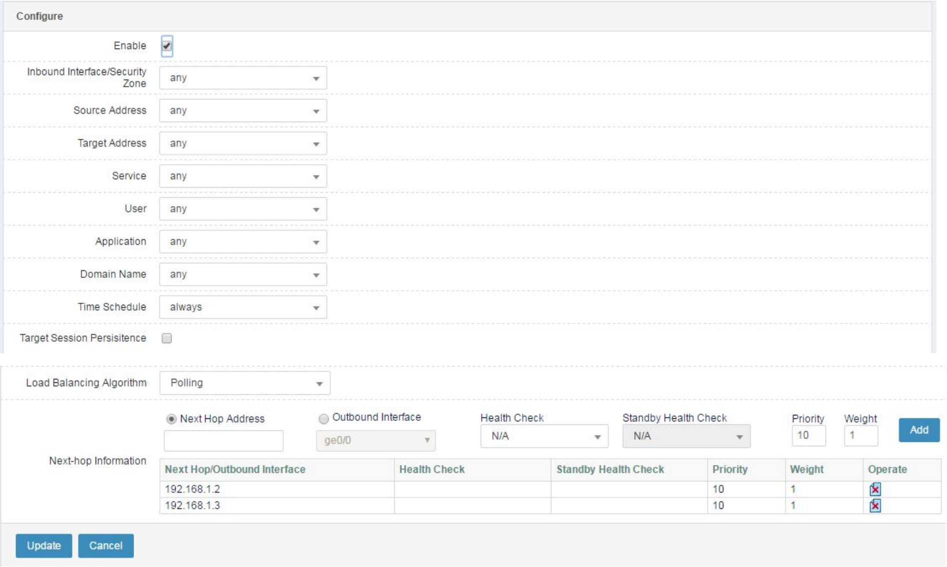
2. Choose **Network** > **Route** > **PBR**, and uncheck the **Enable** check box next to the PBR policy you want to disable.



Total 2 New

ID	Status	Inbound Interf...	Source Address	Destination Ad...	Service	User	Application	Domain Name	Next Hop	Hit	Enable	Operate
⊟ 1	●	any	any	any	any	any	any	any		139	□	
									● 192.168.1.2	70		
									● 192.168.1.3	69		
⊞ 2	●	ge0/1	any	any	any	any	any	any		0	☑	

3. Choose **Network** > **Route** > **PBR**, and click the ID of the PBR policy you want to enable. On the displayed page, check the **Enable** box and click **Submit**. See the following figure.



Configure

Enable	☑
Inbound Interface/Security Zone	any
Source Address	any
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	always
Target Session Persisitence	□
Load Balancing Algorithm	Polling

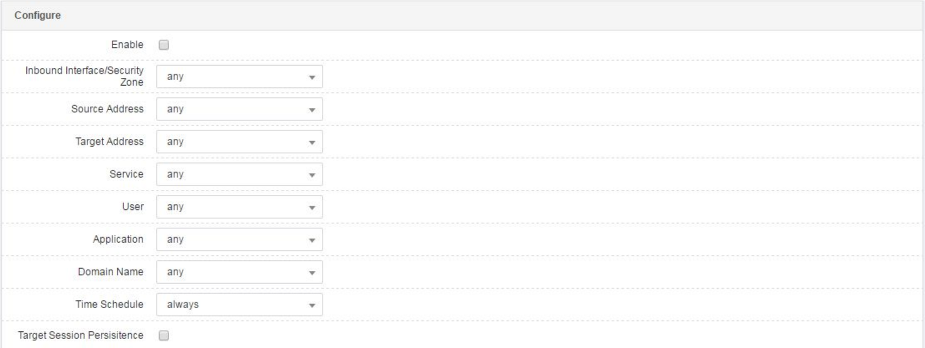
Next-hop Information

◉ Next Hop Address ○ Outbound Interface ge0/0 Health Check N/A Standby Health Check N/A Priority 10 Weight 1 Add

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
192.168.1.2			10	1	☒
192.168.1.3			10	1	☒

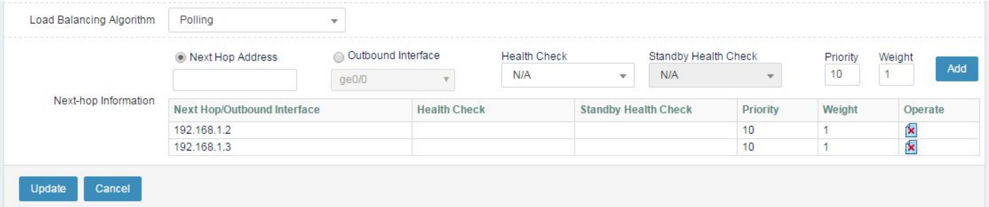
Update Cancel

4. Choose **Network** > **Route** > **PBR**, and click the ID of the PBR policy you want to disable. On the displayed page, uncheck the **Enable** box and click **Update** See the following figure.



Configure

Enable	☐
Inbound Interface/Security Zone	any
Source Address	any
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	always
Target Session Persisitence	☐



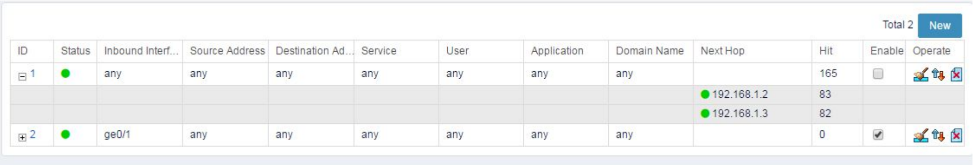
Load Balancing Algorithm: Polling

Next-hop Information: ◉ Next Hop Address ○ Outbound Interface (ge0/0) Health Check: N/A Standby Health Check: N/A Priority: 10 Weight: 1

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
192.168.1.2			10	1	☒
192.168.1.3			10	1	☒

Displaying the PBR Policy List

1. Choose **Network** > **Route** > **PBR**. The following page appears.



Total 2

ID	Status	Inbound Interf...	Source Address	Destination Ad...	Service	User	Application	Domain Name	Next Hop	Hit	Enable	Operate
⊟ 1	●	any	any	any	any	any	any	any		165	☐	
									● 192.168.1.2	83		
									● 192.168.1.3	82		
⊞ 2	●	ge0/1	any	any	any	any	any	any		0	☑	

2. Policy status: 🟢 indicates that the policy is available. 🔴 indicates that no available next hop exists and the policy is unavailable.

4. Next hop status: 🟢 indicates that health check is successful and the next hop is available. 🔴 indicates that health check fails and the next hop is unavailable.

5. Click ⊞ to show or hide next hops.

6. Click 🧹 to reset the hit statistics of a PBR policy.

21.3 Configuration Examples

21.3.1 Example 1

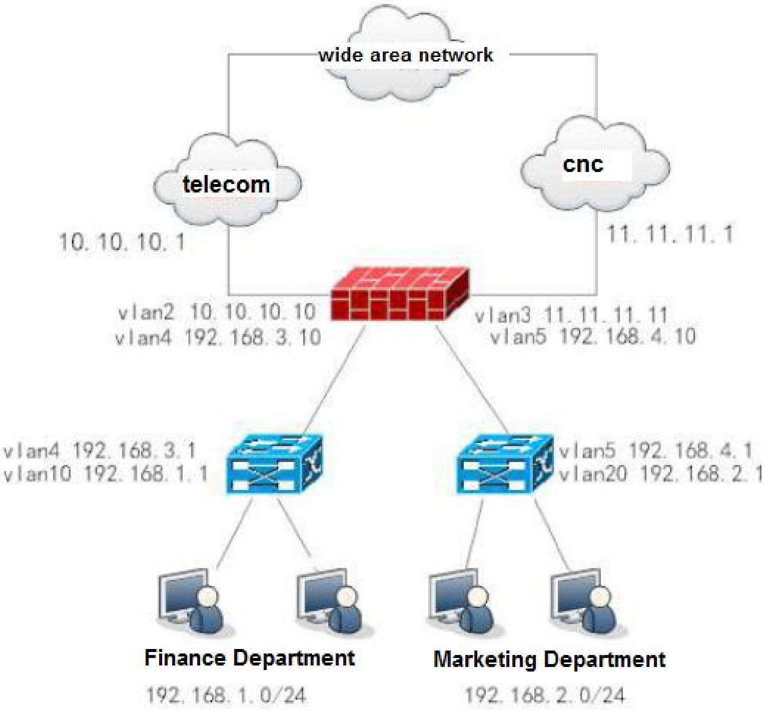
Description:

A company wants to access the Internet through a firewall. The internal address segments are 192.168.1.0/24 and 192.168.2.0/24. There are two egress links which belong to China Telecom and CNC. For the Telecom link, its public address is 10.10.10.10 and gateway address is 10.10.10.1. For the CNC link, its public address is 11.11.11.11 and gateway address is 11.11.11.1.

The customer requirements are as follows:

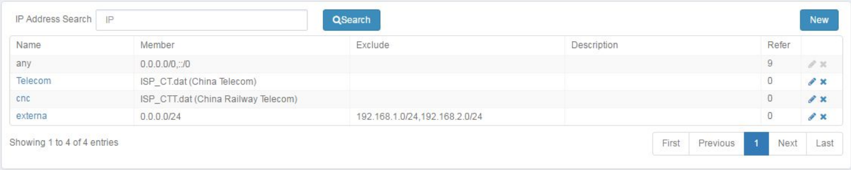
1. If the destination address is a Telecom IP address, select the Telecom link as the egress link. When the Telecom link is faulty, select the CNC link as the egress link.
2. If the destination address is a CNC IP address, select the CNC link as the egress link. When the CNC link is faulty, select the Telecom link as the egress link.
3. If the destination address is neither a Telecom nor a CNC link, either egress link can be selected. Access within the intranet is not controlled by PBR.

Network diagram:



Procedure:

1. Choose **Object** > **Address object** > **Address node**. Create an address object with the Telecom ISP address library, an address object with the CNC ISP address library, and an external address object with 0.0.0.0/0. Add the internal address segments 192.168.1.0/24 and 192.168.2.0/24 to the excluded address list.



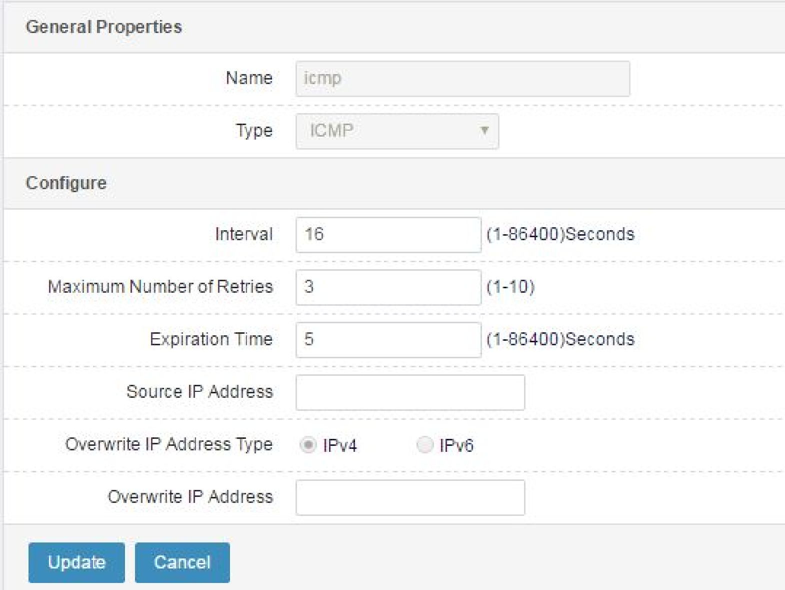
IP Address Search IP Search New

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			9
Telecom	ISP_CT.dat (China Telecom)			0
cnc	ISP_CTT.dat (China Railway Telecom)			0
externa	0.0.0.0/24	192.168.1.0/24,192.168.2.0/24		0

Showing 1 to 4 of 4 entries

2. Choose **Object** > **Health check** to create an ICMP-based health check template.

   If you do not specify **Source IP address** and **Included IP address**, health check will be performed on the next hop in the PBR policy, and the source IP address will be specified as the IP address of the outbound interface.



General Properties

Name	icmp
Type	ICMP

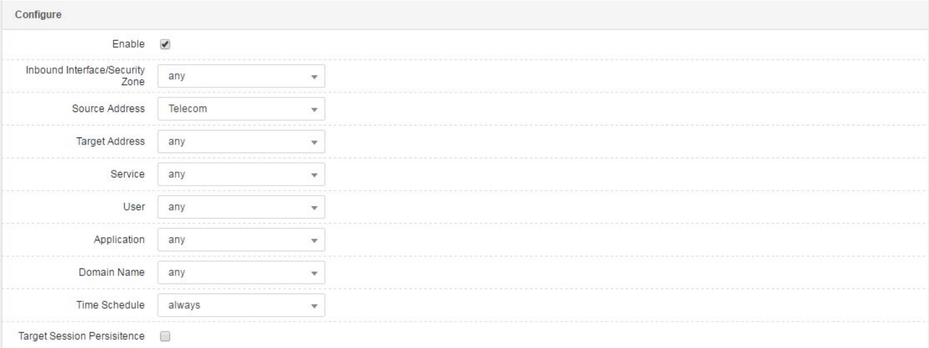
Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Source IP Address	
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	

3. Choose **Network** > **Route** > **PBR**. Create a Telecom PBR policy, a CNC PBR policy, and a default PBR policy.

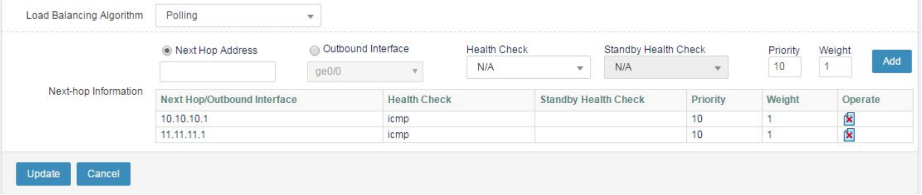
   Telecom PBR policy:

   Select **China Telecom** for **Destination address**, add the Telecom link and CNC link in **Gateway**, set the Telecom link priority higher than the CNC link, and reference the ICMP-based health check template.



Configure

Enable	☑
Inbound Interface/Security Zone	any
Source Address	Telecom
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	always
Target Session Persisitence	☐

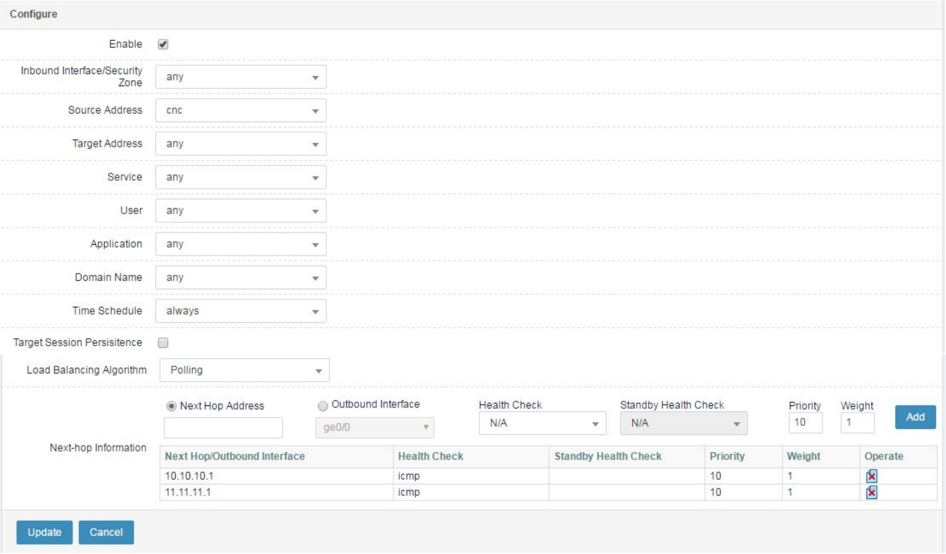


Load Balancing Algorithm	Polling
Next-hop Information	● Next Hop Address ○ Outbound Interface ge0/0 · Health Check N/A · Standby Health Check N/A · Priority 10 · Weight 1 · Add

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
10.10.10.1	icmp		10	1	☒
11.11.11.1	icmp		10	1	☒

CNC PBR policy:

Select **CNC** for **Destination address**, add the Telecom link and CNC link in **Gateway**, set the CNC link priority higher than the Telecom link, and reference the ICMP-based health check template.



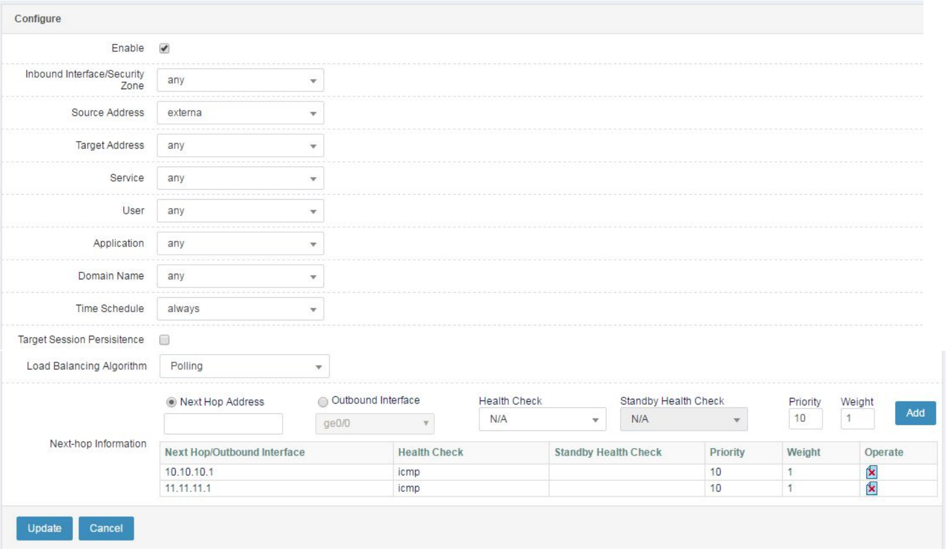
Configure

Enable	☑
Inbound Interface/Security Zone	any
Source Address	cnc
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	always
Target Session Persisitence	□
Load Balancing Algorithm	Polling
Next-hop Information	● Next Hop Address ○ Outbound Interface ge0/0 · Health Check N/A · Standby Health Check N/A · Priority 10 · Weight 1 · Add

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
10.10.10.1	icmp		10	1	☒
11.11.11.1	icmp		10	1	☒

Default PBR policy:

Select **External address** for **Destination address**. Because the internal address segments 192.168.1.0/24 and 192.168.2.0/24 are added to the excluded address list of the external address object, access within the intranet is not controlled by PBR. Add the Telecom link and CNC link in **Gateway**, set the CNC link priority higher than the Telecom link to enable forwarding based on round robin, and reference the ICMP-based health check template.



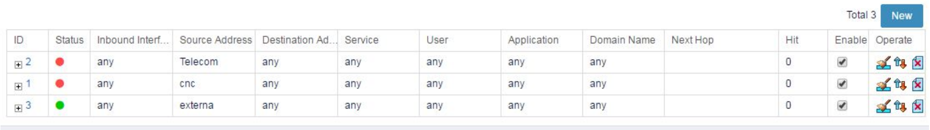
Configure

Enable	☑
Inbound Interface/Security Zone	any
Source Address	externa
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	always
Target Session Persisitence	☐
Load Balancing Algorithm	Polling

Next-hop Information: ◉ Next Hop Address ○ Outbound Interface (ge0/0) Health Check: N/A Standby Health Check: N/A Priority: 10 Weight: 1

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
10.10.10.1	icmp		10	1	☒
11.11.11.1	icmp		10	1	☒

4. Check the policies after the configuration. The number of hits indicates the PBR policy matching results.



Total 3

ID	Status	Inbound Interf...	Source Address	Destination Ad...	Service	User	Application	Domain Name	Next Hop	Hit	Enable	Operate
⊞ 2	●	any	Telecom	any	any	any	any	any		0	☑	
⊞ 1	●	any	cnc	any	any	any	any	any		0	☑	
⊞ 3	●	any	externa	any	any	any	any	any		0	☑	

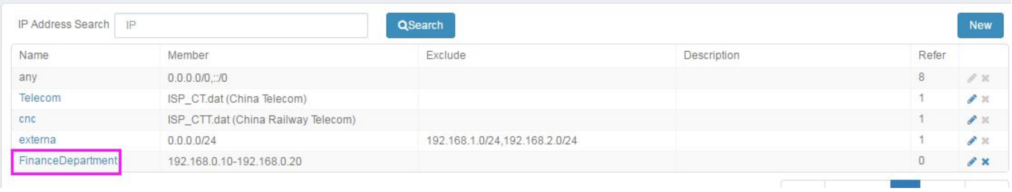
21.3.2 Example 2

Description:

A company's financial department has office applications such as email and office software that need to access the external network through the Telecom leased line. The IP address range of the financial department is 192.168.0.10 to 192.168.0.20.

Procedure:

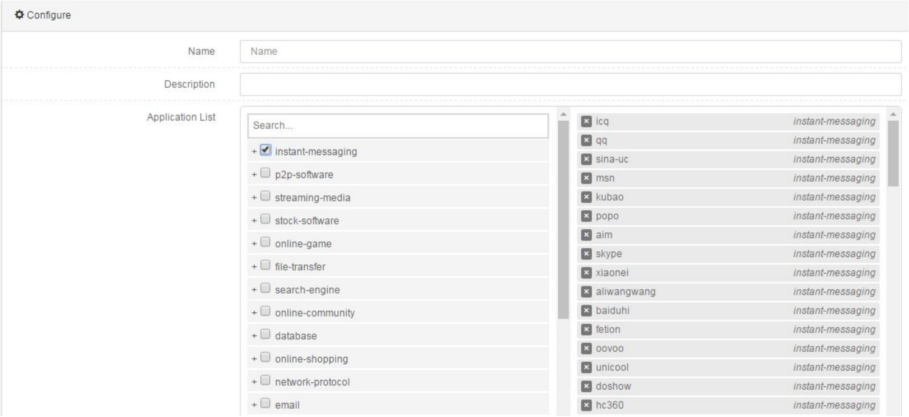
1. Choose **Object** > **Address object** > **Address node** to create an address object for the financial department.



IP Address Search: IP

Name	Member	Exclude	Description	Refer	
any	0.0.0.0/0,::/0			8	
Telecom	ISP_CT.dat (China Telecom)			1	
cnc	ISP_CTT.dat (China Railway Telecom)			1	
externa	0.0.0.0/24	192.168.1.0/24,192.168.2.0/24		1	
FinanceDepartment	192.168.0.10-192.168.0.20			0	

2. Choose **Object** > **Application object** > **Application group** to create an application object.



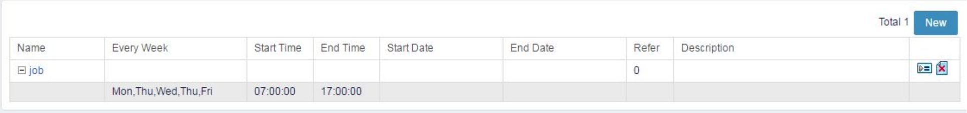
⚙ Configure

Name	Name
Description	
Application List	Search...

- + ☑ instant-messaging
- + □ p2p-software
- + □ streaming-media
- + □ stock-software
- + □ online-game
- + □ file-transfer
- + □ search-engine
- + □ online-community
- + □ database
- + □ online-shopping
- + □ network-protocol
- + □ email

☒ icq	instant-messaging
☒ qq	instant-messaging
☒ sina-uc	instant-messaging
☒ msn	instant-messaging
☒ kubao	instant-messaging
☒ popo	instant-messaging
☒ aim	instant-messaging
☒ skype	instant-messaging
☒ xiaonei	instant-messaging
☒ aliwangwang	instant-messaging
☒ baiduhi	instant-messaging
☒ fetion	instant-messaging
☒ oovoo	instant-messaging
☒ unicool	instant-messaging
☒ doshow	instant-messaging
☒ hc360	instant-messaging

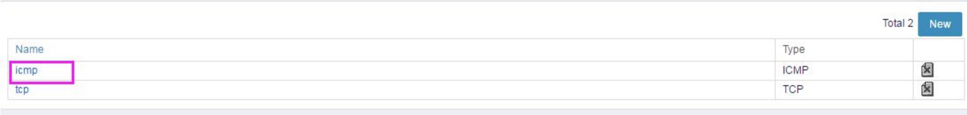
3. Choose **Object** > **Time object** > **Cycle** to create a work time object.



Total 1 New

Name	Every Week	Start Time	End Time	Start Date	End Date	Refer	Description	
⊟ job						0		
	Mon,Thu,Wed,Thu,Fri	07:00:00	17:00:00					

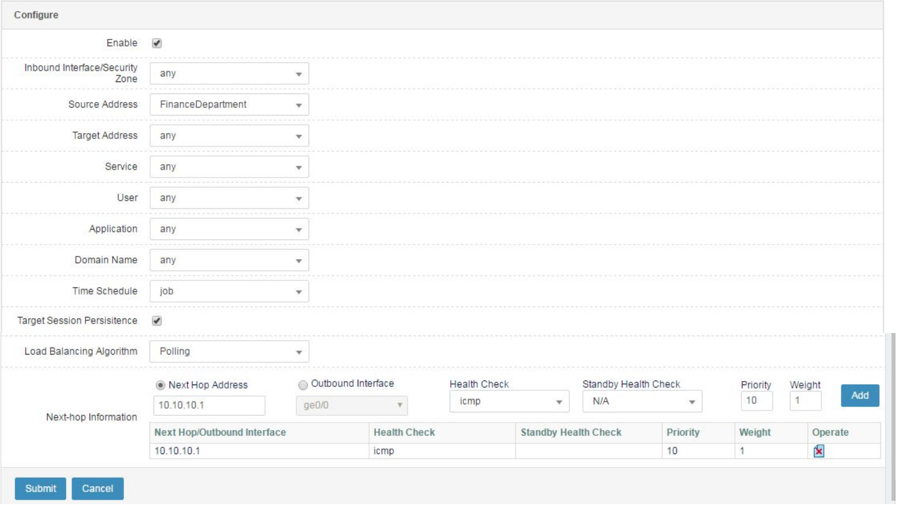
4. Choose **Object** > **Health check** to create an ICMP-based health check template.



Total 2 New

Name	Type	
icmp	ICMP	
tcp	TCP	

5. Choose **Network** > **Route** > **PBR** to create a financial department PBR policy.



Configure

Enable	☑
Inbound Interface/Security Zone	any
Source Address	FinanceDepartment
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	job
Target Session Persistence	☑
Load Balancing Algorithm	Polling

Next-hop Information

● Next Hop Address	○ Outbound Interface	Health Check	Standby Health Check	Priority	Weight	
10.10.10.1	ge0/0	icmp	N/A	10	1	Add

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
10.10.10.1	icmp		10	1	☒

Submit Cancel

Select **Financial dept.** for **Source address**, **Office application** for **Application**, and **Work time** for **Time table**. Enter the next-hop gateway of the Telecom leased line in **Gateway**, select **ICMP** for **Health check**, and click **Add**. Click **Submit** after you complete the settings. Then the financial department can use office applications with access to the external network through the Telecom leased line during the work time.

21.4 Troubleshooting

21.4.1 A PBR Policy Is Ineffective

Symptom	After a PBR policy is configured, traffic is not forwarded to the next hop specified by the PBR policy.
Analysis	1. Check whether the PBR policy is not enabled. 2. Check whether another PBR policy with a higher priority is hit. 3. Check whether the configured next hop is correct and has a direct route. 4. Check whether the health check on the next hop is successful. 5. Check whether the source or destination IP address is added to the excluded address list of the address object. 6. Check whether a direct route to the destination network segment exists on the firewall. 7. Check whether the packets that hit the PBR policy are reverse packets. 8. Check whether the connection is established before the PBR policy is enabled according to session information. 9. Check whether the packets that hit the PBR policy are forwarded by the firewall at Layer 2.

Solution	1. Enable the PBR policy. 2. Modify the PBR policy or adjust the policy order as needed. 3. If no direct route is found for the next hop, traffic is not forwarded to the next hop and is matched with other PBR policies in order. 4. Identify the cause of failed health check, and check whether the next hop is unreachable or the link is faulty. 5. Remove the IP address from the excluded address list. 6. If a direct route exists, traffic is forwarded along the direct route and is not matched with the PBR policy. Therefore, the PBR policy is invalid if a direct route to the destination network segment exists on the firewall. 7. PBR is a flow-based matching technique. Forward packets are matched with PBR policies, whereas reverse packets are not. The latter is forwarded by means of route lookup along the same path as the forward packet. 8. To avoid disconnection, PBR does not affect existing traffic forwarding. You can establish a new connection to check whether the PBR policy is matched properly. 9. Only Layer-3 forwarded packets are matched with PBR policies.

21.4.2 Some Next Hops of a PBR Policy Have No Hit Count

Symptom	Multiple next hops are added to a PBR policy. When traffic exists, some next hops have no hit count.
Analysis	1. Check whether an available next hop has a higher priority than the problematic next hop. 2. Check whether session persistence is enabled and its mask is the same as that of the destination network segment. 3. Check whether session persistence is enabled but the destination network segment is unreachable from the problematic next hop. A session persistence entry is created only when reverse packets exists, which ensures entry reliability. No session persistence entry is created when no reverse packets are returned for the traffic routed

	along a faulty link.
Solution	1. The next hop with a lower priority than an available next hop is not scheduled. If you want to schedule the lower-priority next hop, increase its priority. 2. After session persistence is enabled, packets destined for the same network segment are forwarded to the same next hop. You can adjust the bits of the subnet mask as needed. 3. Check whether the link connected to the next-hop outbound interface is faulty.

22 Session Persistence

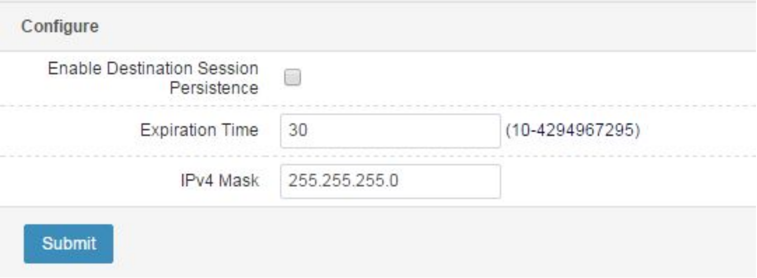
22.1 Overview

In many e-commerce application systems or online systems that require user authentication, a customer can complete a transaction or a task only after multiple interactions with the server. The interactions are closely related and must be handled by the same server. Before proceeding to the next step, the server needs to get the results of one or more previous interactions. Session persistence is a method to send requests to the same server for processing.

22.2 Configuration

22.2.1 Procedure

1. Choose **Network** > **Route** > **Session persistence**. The following page appears.



Configure

Enable Destination Session Persistence ☐

Expiration Time 30 (10-4294967295)

IPv4 Mask 255.255.255.0

Parameter description:

Enable session persistence: Check this box to enable session persistence based on the destination address.

Timeout: Timeout period for a session persistence entry. The value ranges from 10 to 4294967295, in seconds. If a session persistence entry is not hit within the timeout period, it is automatically deleted.

IPv4 mask: AND operation is performed on the mask and destination IP address. If the results are the same, traffic is scheduled to the same next hop.

2. Click **Submit** after you complete the settings.

22.2.2 Important Notes

1. **Enable session persistence** is effective for other equal-cost routes except PBR.
2. **Timeout period** and **IPv4 mask** are globally effective.
3. **Enable session persistence** is ineffective for PBR. To enable session persistence for PBR, go to the PBR configuration page.
4. Session persistence is only based on the destination address.

22.3 Troubleshooting

22.3.1 Session Persistence Is Ineffective for PBR

Symptom	Session persistence is ineffective for PBR.
Analysis	1. Session persistence must be enabled for specific PBR policies.
Solution	Enable session persistence for the desired PBR policy.

22.3.2 Session Persistence Is Ineffective

Symptom	With session persistence enabled, traffic destined for the same network segment is not routed to the same next hop.
Analysis	The possible causes are as follows: 1. Traffic destined for the same network segment hits a PBR policy and is forwarded accordingly. 2. A finer route to the destination network segment exists, and traffic is forwarded along this route according to route selection. 3. The route fails and traffic is not forwarded along this route.
Solution	Identify the cause through the preceding analysis and solve the problem accordingly.

23 NAT

23.1 Overview

Network address translation (NAT) was defined by RFC1631 (replaced by RFC3022) to convert private addresses to public addresses to solve public IP address shortage. With continuous development and deeper application, NAT proves to be useful and versatile. For example, NAT provides unidirectional isolation with robust security; allows public addresses to access servers configured with private addresses through destination address mapping; and supports server load balancing and address multiplexing.

NAT is classified into source NAT (SNAT) and destination NAT (DNAT) SNAT is an address translation technique based on the source address. It is further classified into dynamic NAT, port address translation (PAT), and static NAT. A type of unidirectional source address mapping, dynamic NAT and PAT are used for external service access using an internal address, help reduce public addresses, and hide internal addresses. Dynamic NAT converts and maps a source address to a small address pool dynamically. The same source IP address may be mapped to different addresses in an address pool depending on different connections. PAT maps all source addresses to the same address and differentiates connections by means of port mapping, thus enabling public address sharing. Static NAT is a one-to-one bidirectional address mapping, enabling internal servers to provide services externally. An internal server enabled with static NAT can access external services and also receive access requests from external networks, which is equivalent to establishing a bidirectional channel between internal and external networks.

RAVEN5000 firewalls provide SNAT and static NAT.

23.2 Configuration

NAT configuration is divided into SNAT, DNAT, and static NAT. Bidirectional NAT configuration supports configuring SNAT and DNAT together. Currently, IPv4-to-IPv4 address conversion and IPv6-to-IPv6 address conversion are supported.

Each NAT rule is associated with an interface. Because SNAT is performed when traffic leaves an interface, the SNAT rule must be associated with the outbound interface. Similarly, because DNAT is performed when traffic enters an interface, the DNAT rule must be associated with the inbound interface.

Notice

If two NAT rules have the same source address, destination address, service, and outbound interface (four-tuples), the first NAT rule is matched preferentially.

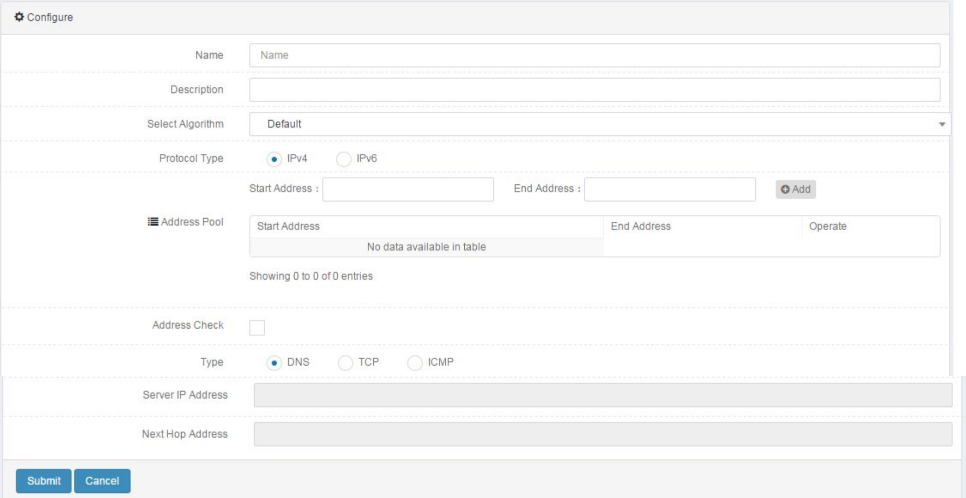
23.2.1 Configuring a NAT Pool

A NAT pool is a set of addresses for use by dynamic NAT. It supports three use modes: round robin, source address holdover, and default. NAT pool segmentation is supported.

NAT converts the real address of a packet to an address in the NAT pool.

Procedure:

1. Choose **Network** > **NAT** > **NAT pool** and click **New**.



Name: Name

Description:

Select Algorithm: Default

Protocol Type: ● IPv4 ○ IPv6

Address Pool: Start Address : End Address :

Start Address	End Address	Operate
No data available in table		

Showing 0 to 0 of 0 entries

Address Check: □

Type: ● DNS ○ TCP ○ ICMP

Server IP Address:

Next Hop Address:

Name: Name of the new NAT pool, no more than 64 characters.

Description: Description about the NAT pool, no more than 128 characters.

Select algorithm: Addresses are selected from the NAT pool based on an algorithm. The options are:

Default: Select a random address in the NAT pool as the address after conversion.

Round robin: Select the addresses in the NAT pool cyclically during address conversion.

Source address holdover: Select a random address in the NAT pool. The same address is selected for packets with the same source address.

Protocol type: The options are **IPv4** and **IPv6**. A NAT pool can only contain either IPv4 or IPv6 addresses.

Start address: Start address of the NAT pool.

End address: End address of the NAT pool. The end address cannot be smaller than the start address. The NAT pool contains all the addresses from the start to the end address.

Address check: Check this box to check the availability of the addresses in the NAT pool. After you check this box, specify the server IP address and next-hop address. By default, address check is disabled.

Type: Protocol type of address check.

Server IP address: The addresses in the NAT pool send packets to the specified server to check whether the addresses are available. Run the **show snat-pool-check list** command to display the address availability status.

Next-hop address: Next-hop address used by address check of the NAT pool.

⚠ Notice

The end address cannot be smaller than the start address. The addresses in the range cannot overlap. The addresses between the start and end address cannot exceed 10,000.

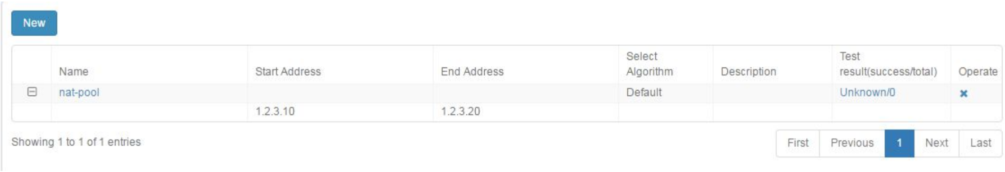
2. Click **Submit** after you complete the settings.

23.2.2 Modifying a NAT Pool

You can modify an existing NAT pool.

Procedure:

1. Choose **Network** > **NAT** > **NAT pool**. The following page appears.

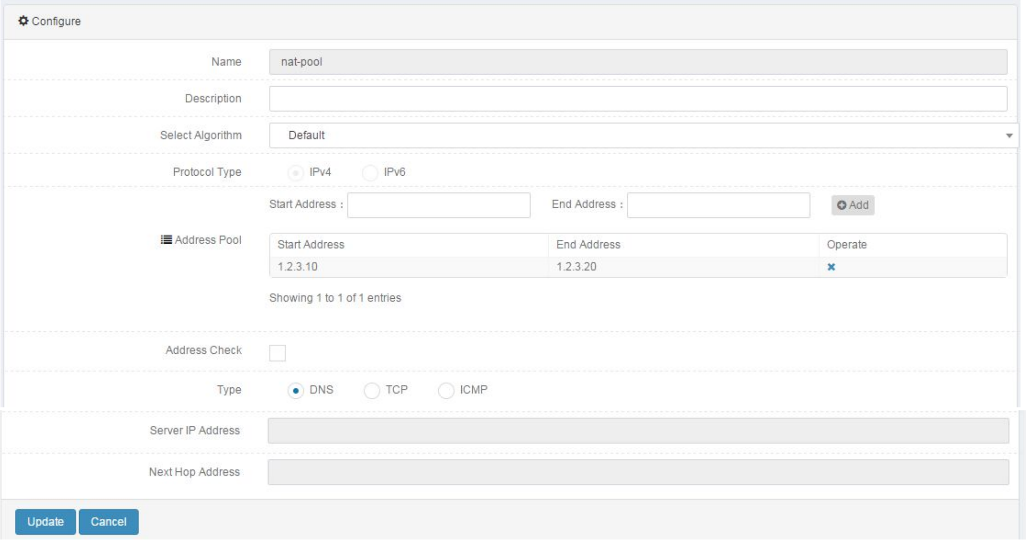


New

	Name	Start Address	End Address	Select Algorithm	Description	Test result(success/total)	Operate
⊟	nat-pool			Default		Unknown/0	✖
		1.2.3.10	1.2.3.20				

Showing 1 to 1 of 1 entries

Click a pool name.



Name	nat-pool
Description	
Select Algorithm	Default
Protocol Type	● IPv4 ○ IPv6
Address Pool	Start Address : End Address : Add

Start Address	End Address	Operate
1.2.3.10	1.2.3.20	×

Showing 1 to 1 of 1 entries

Address Check	□
Type	● DNS ○ TCP ○ ICMP
Server IP Address	
Next Hop Address	

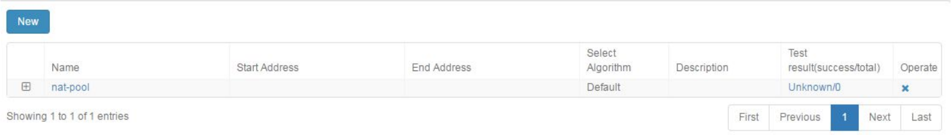
Modify the parameters. **Name** and **Protocol type** cannot be modified.

Click **Update**.

23.2.3 Deleting a NAT Pool

Procedure:

1. Choose **Network** > **NAT** > **NAT pool**. The following page appears.



	Name	Start Address	End Address	Select Algorithm	Description	Test result(success/total)	Operate
⊞	nat-pool			Default		Unknown/0	×

Showing 1 to 1 of 1 entries

2. Click ✖ next to the NAT pool you want to delete.

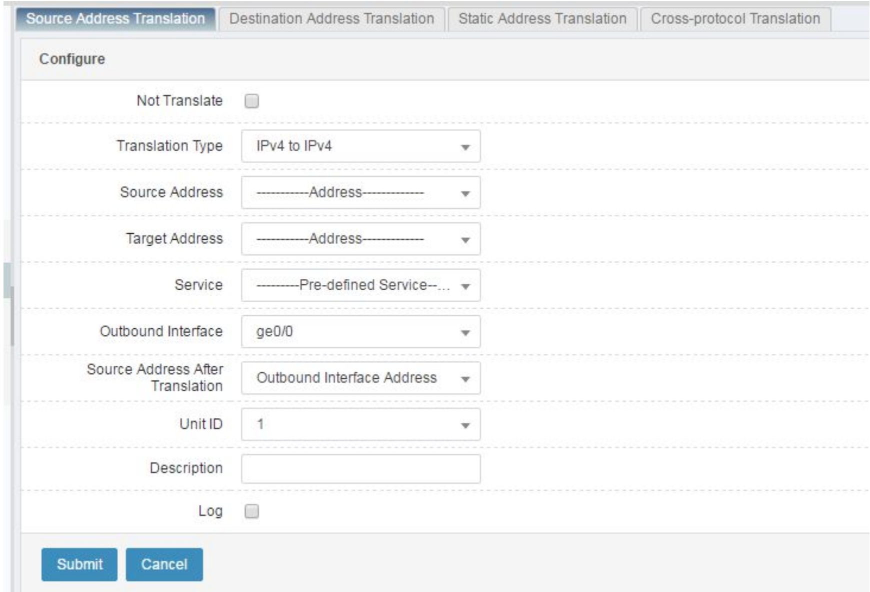
> ⚠ Notice
>
> When the **Delete** button is grayed out, the NAT pool is being referenced and cannot be deleted.

23.2.4 Configuring SNAT

A type of unidirectional source address mapping, SNAT is used for external service access using an internal address, helps reduce public addresses, and hides internal addresses.

Procedure:

Choose **Network** > **NAT** > **NAT rule** > **SNAT** and click **New**.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure
Submit
Cancel

Not Translate	☐
Translation Type	IPv4 to IPv4
Source Address	----------Address------------
Target Address	----------Address------------
Service	---------Pre-defined Service--...
Outbound Interface	ge0/0
Source Address After Translation	Outbound Interface Address
Unit ID	1
Description	
Log	☐

No conversion: If you check this box, address conversion is not performed when the NAT rule is hit.

Conversion type: The options are **IPv4 to IPv4** and **IPv6 to IPv6**.

Source address: Source address matched with the NAT rule, which may be an address object or an address group. The address object type must be consistent with **Conversion type**. For example, if **IPv4 to IPv4** is selected for **Conversion type**, the address object type must be IPv4.

Destination address: Destination address matched with the NAT rule, which may be an address object or an address group. The address object type must be consistent with **Conversion type**.

Service: Name of the service matched with the NAT rule, which may be a service object or a service group.

Outbound interface: Name of the outbound interface matched with the NAT rule.

Source address after conversion: Address after conversion, which may be an outbound interface address, a NAT pool name, or an IP address. The selected pool type must be consistent with **Conversion type**.

Unit ID: Unit ID of the NAT rule, which takes effect when the high availability feature is enabled. For example, when the HA active-active mode is enabled, if the host ID is inconsistent with the NAT rule ID, the NAT rule does not take effect. The default value is **1**.

Description: Description about the NAT rule, which cannot exceed 128 characters.

Log: Check this box to enable logging for the NAT rule.

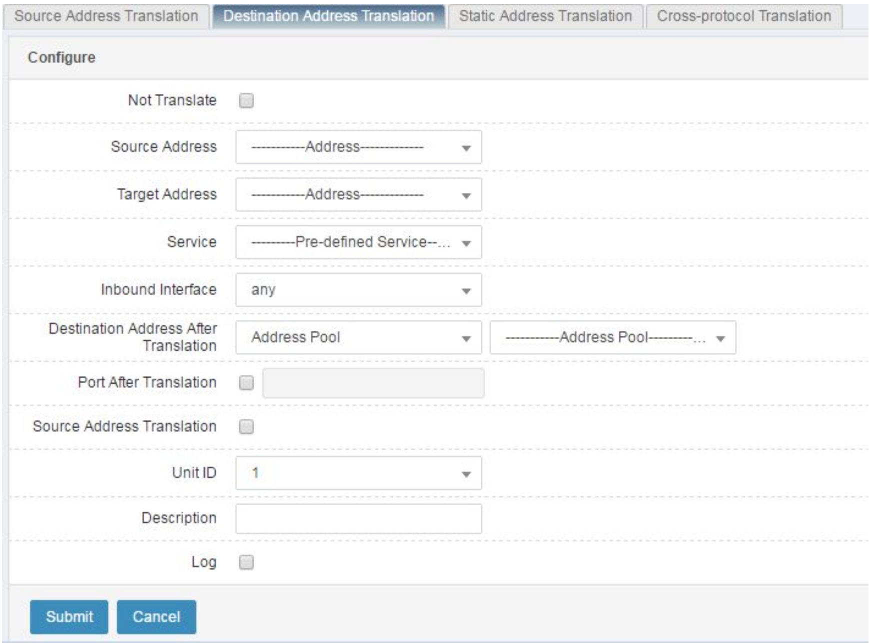
Click **Submit** after you complete the settings.

23.2.5 Configuring DNAT

A type of unidirectional destination address mapping, DNAT is used for internal service access using an external address and allows internal servers to provide services externally. External devices can access the intranet, but internal devices cannot access the external network.

Procedure:

Choose **Network** > **NAT** > **NAT rule** > **DNAT** and click **New**.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure
Submit
Cancel

Not Translate □

Source Address: ----------Address------------

Target Address: ----------Address------------

Service: ---------Pre-defined Service--...

Inbound Interface: any

Destination Address After Translation: Address Pool | ----------Address Pool---------...

Port After Translation □

Source Address Translation □

Unit ID: 1

Description:

Log □

No conversion: If you check this box, address conversion is not performed when the NAT rule is hit.

Source address: Source address matched with the NAT rule, which may be an address object or an address group.

Destination address: Destination address matched with the NAT rule, which may be an address object or an address group.

Service: Name of the service matched with the NAT rule, which may be a service object or a service group.

Inbound interface: Name of the inbound interface matched with the NAT rule.

Destination address after conversion: Address after conversion, which may be a NAT pool name or an IP address.

Port after conversion: Port number after conversion.

Source address conversion: NAT pool or IP address after SNAT in bidirectional NAT. Do not check this box when configuring DNAT.

Unit ID: Unit ID of the NAT rule, which takes effect when the high availability feature is enabled. For example, when the HA active-active mode is enabled, if the host ID is inconsistent with the NAT rule ID, the NAT rule does not take effect. The default value is **1**.

Description: Description about the NAT rule, which cannot exceed 128 characters.

Log: Check this box to enable logging for the NAT rule.

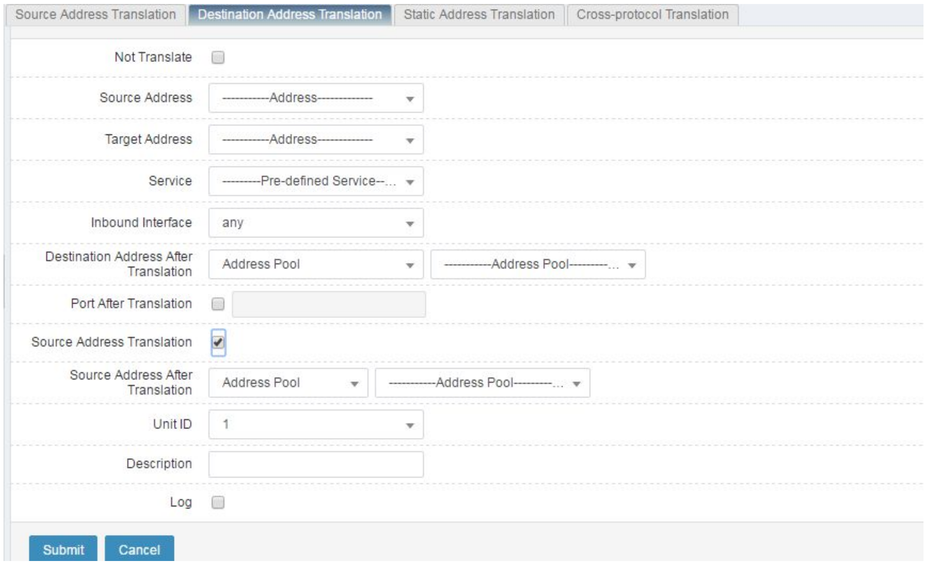
Click **Submit** after you complete the settings.

23.2.6 Configuring Bidirectional NAT

Bidirectional NAT supports SNAT and DNAT. When an internal PC accesses an internal server, the internal server provides a virtual address, which must be subjected to SNAT and DNAT.

Procedure:

Choose **Network** > **NAT** > **NAT rule** > **DNAT** and click **New**.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation

Not Translate	□	
Source Address	-----------Address------------	
Target Address	-----------Address------------	
Service	---------Pre-defined Service--...	
Inbound Interface	any	
Destination Address After Translation	Address Pool	-----------Address Pool---------...
Port After Translation	□	
Source Address Translation	☑	
Source Address After Translation	Address Pool	-----------Address Pool---------...
Unit ID	1	
Description		
Log	□	

Source address: Source address matched with the NAT rule, which may be an address object or an address group.

Destination address: Destination address matched with the NAT rule, which may be an address object or an address group.

Service: Name of the service matched with the NAT rule, which may be a service object or a service group.

Inbound interface: Name of the inbound interface matched with the NAT rule.

Destination address after conversion: Address after conversion, which is a NAT pool name.

Port after conversion: Port number after conversion.

Source address conversion: NAT pool or IP address after SNAT in bidirectional NAT. Check this box when configuring bidirectional NAT.

Unit ID: Unit ID of the NAT rule, which takes effect when the high availability feature is enabled. For example, when the HA active-active mode is enabled, if the host ID is inconsistent with the NAT rule ID, the NAT rule does not take effect. The default value is **1**.

Description: Description about the NAT rule, which cannot exceed 128 characters.

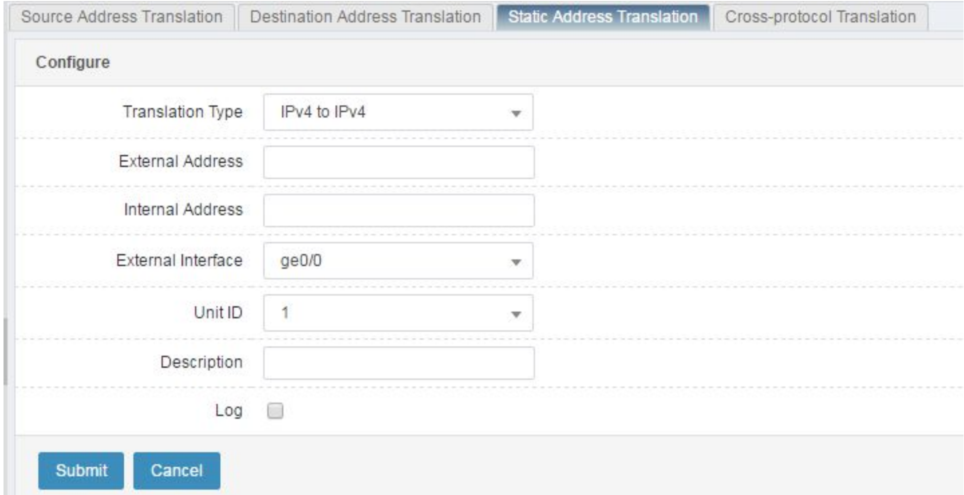
Log: Check this box to enable logging for the NAT rule.

23.2.7 Configuring Static NAT

Static NAT is one-to-one bidirectional address mapping. The mapped internal host can access external services and also receive access requests from external networks, which is equivalent to establishing a bidirectional channel between internal and external networks.

Procedure:

Choose **Network** > **NAT** > **NAT rule** > **Static NAT** and click **New**.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Submit
Cancel

Configure

Translation Type	IPv4 to IPv4
External Address	
Internal Address	
External Interface	ge0/0
Unit ID	1
Description	
Log	□

Conversion type: The options are **IPv4 to IPv4** and **IPv6 to IPv6**.

External address: External address to be converted.

Internal address: Internal address to be converted.

External interface: Name of the interface connected to an external network.

Unit ID: Unit ID of the NAT rule, which takes effect when the high availability feature is enabled. For example, when the HA active-active mode is enabled, if the host ID is inconsistent with the NAT rule ID, the NAT rule does not take effect. The default value is **1**.

Description: Description about the NAT rule, which cannot exceed 128 characters.

Log: Check this box to enable logging for the NAT rule.

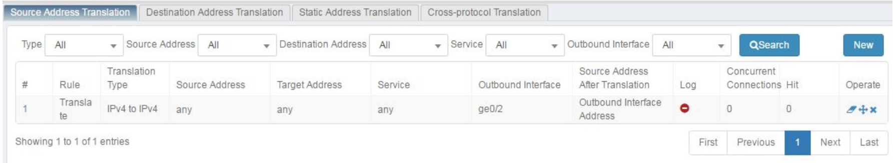
Click **Submit** after you complete the settings.

23.2.8 Modifying a NAT Rule

You can modify an existing NAT rule.

Procedure:

Choose **Network configuration** > **NAT** > **NAT rule** > **SNAT**. The following page appears.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Search
New

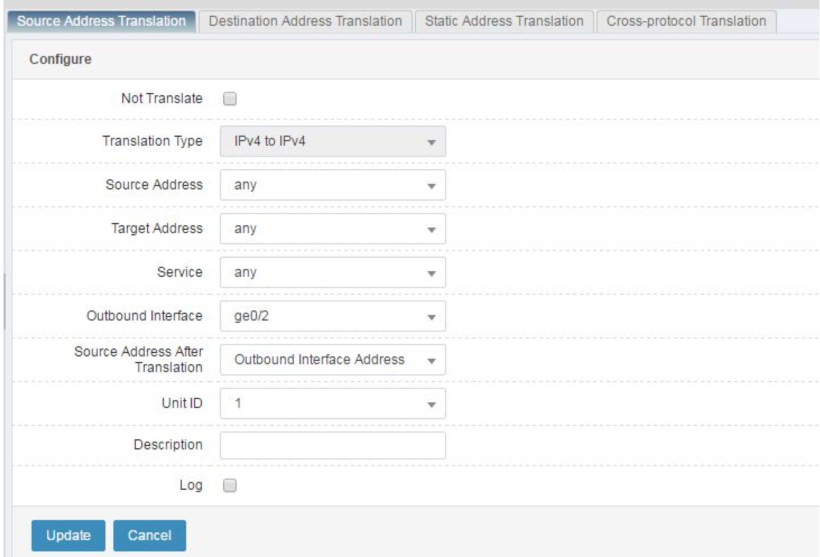
Type All | Source Address All | Destination Address All | Service All | Outbound Interface All

#	Rule	Translation Type	Source Address	Target Address	Service	Outbound Interface	Source Address After Translation	Log	Concurrent Connections	Hit	Operate
1	Translate	IPv4 to IPv4	any	any	any	ge0/2	Outbound Interface Address	⛔	0	0	✎ ✥ ✕

Showing 1 to 1 of 1 entries

First
Previous
1
Next
Last

Click a rule ID.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure
Update
Cancel

Not Translate	□
Translation Type	IPv4 to IPv4
Source Address	any
Target Address	any
Service	any
Outbound Interface	ge0/2
Source Address After Translation	Outbound Interface Address
Unit ID	1
Description	
Log	□

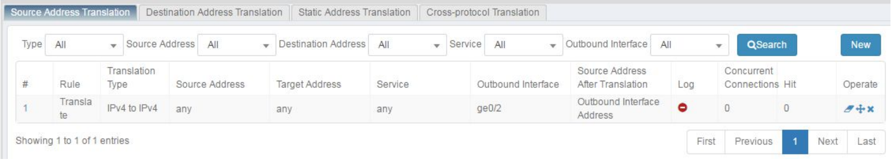
Modify the parameters. **Conversion type** cannot be modified.

Click **Submit** after you complete the settings.

23.2.9 Deleting a NAT Rule

Procedure:

Choose **Network configuration** > **NAT** > **NAT rule** > **SNAT**. The following page appears.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Search
New

Type All | Source Address All | Destination Address All | Service All | Outbound Interface All

#	Rule	Translation Type	Source Address	Target Address	Service	Outbound Interface	Source Address After Translation	Log	Concurrent Connections	Hit	Operate
1	Translate	IPv4 to IPv4	any	any	any	ge0/2	Outbound Interface Address	⛔	0	0	✎ ✥ ✕

Showing 1 to 1 of 1 entries

First
Previous
1
Next
Last

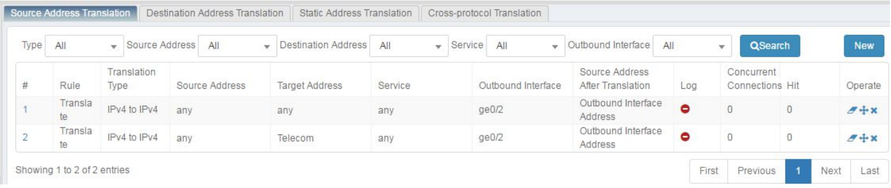
Click ✖ next to the NAT rule you want to delete.

23.2.10 Moving a NAT Rule

You can adjust the match order of NAT rules of the same conversion type.

Procedure:

Choose **Network configuration** > **NAT** > **NAT rule** > **SNAT**. The following page appears.

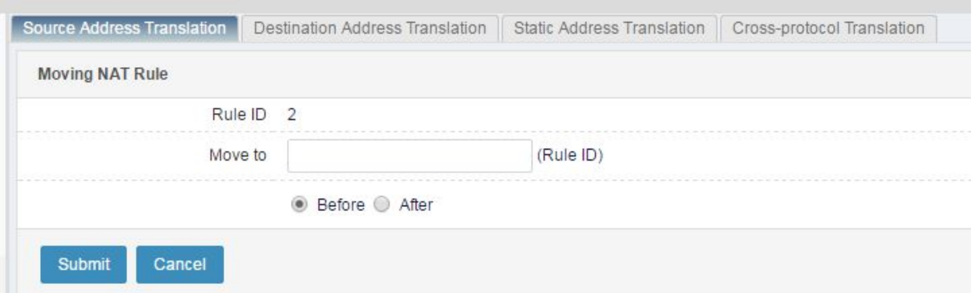


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Type All
Source Address All
Destination Address All
Service All
Outbound Interface All
Search
New

#	Rule	Translation Type	Source Address	Target Address	Service	Outbound Interface	Source Address After Translation	Log	Concurrent Connections	Hit	Operate
1	Translate	IPv4 to IPv4	any	any	any	ge0/2	Outbound Interface Address	⛔	0	0	✎✥✖
2	Translate	IPv4 to IPv4	any	Telecom	any	ge0/2	Outbound Interface Address	⛔	0	0	✎✥✖

Showing 1 to 2 of 2 entries

Click ✥ next to a rule.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation

Moving NAT Rule

Rule ID 2

Move to ________ (Rule ID)

● Before ○ After

Rule ID: ID of the rule to be moved.

Move to: New position of the rule.

> ⚠ Notice
>
> A rule can be moved only among other rules of the same conversion type. For example, an IPv4-to-IPv4 NAT rule can be moved only among other IPv4-to-IPv4 NAT rules. Similarly, an IPv6-to-IPv6 NAT rule can be moved only among other IPv6-to-IPv6 NAT rules.

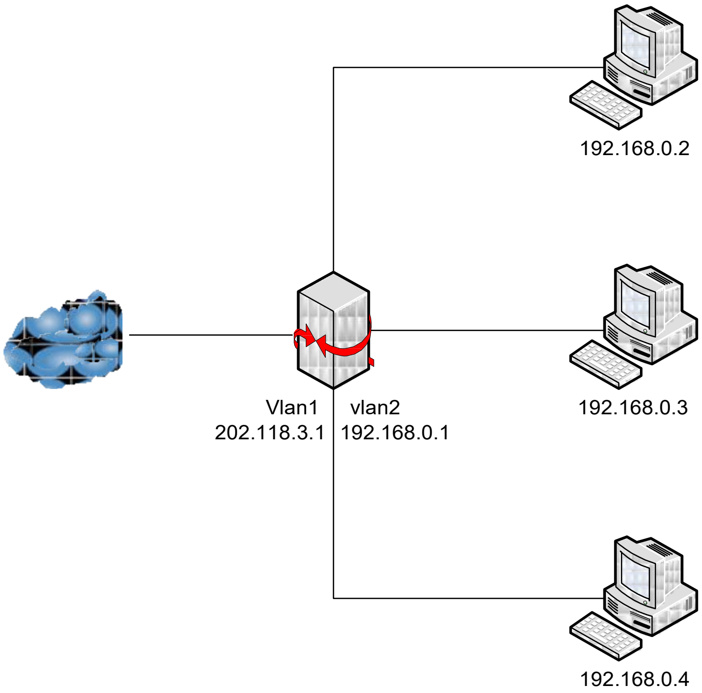
23.3 Configuration Examples

23.3.1 Configuring SNAT

Description:

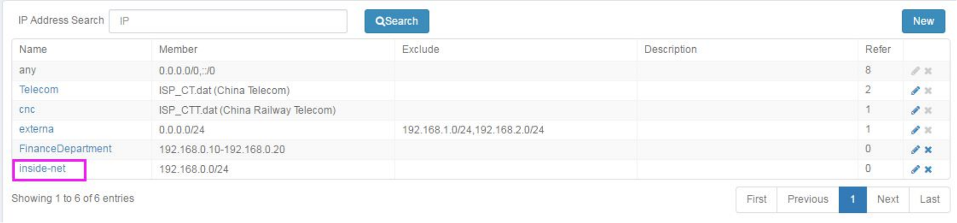
A company's LAN needs to access external networks through an application device. The internal address segment is 192.168.0.0/24, and the public address is 202.118.3.1.

Network diagram:



Procedure:

1. Choose **Object** > **Address object** > **Address node** to create an IPv4 address object named **inside-net**.



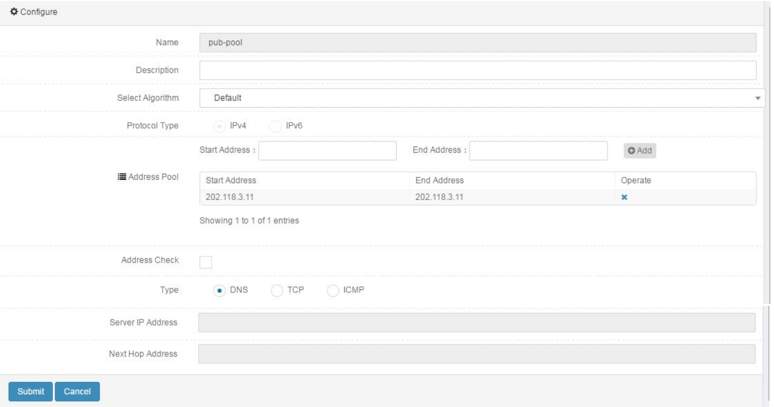
IP Address Search [IP] Search New

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			8
Telecom	ISP_CT.dat (China Telecom)			2
cnc	ISP_CTT.dat (China Railway Telecom)			1
externa	0.0.0.0/24	192.168.1.0/24,192.168.2.0/24		1
FinanceDepartment	192.168.0.10-192.168.0.20			0
inside-net	192.168.0.0/24			0

Showing 1 to 6 of 6 entries

First Previous 1 Next Last

2. Choose **Network** > **NAT** > **NAT pool** to create a NAT pool called **pub-pool**.



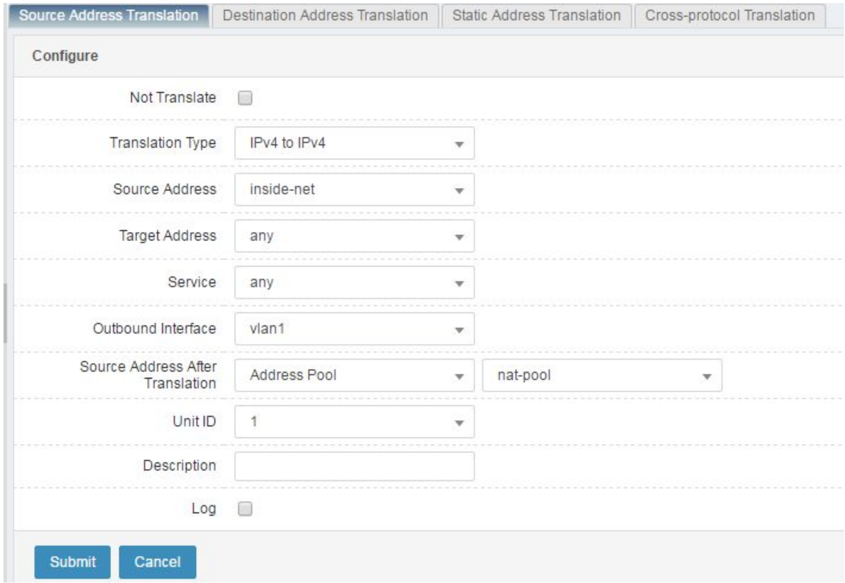
Configure

Name	pub-pool
Description	
Select Algorithm	Default
Protocol Type	● IPv4 ○ IPv6
	Start Address : [ ] End Address : [ ] Add
Address Pool	Start Address: 202.118.3.11, End Address: 202.118.3.11 Showing 1 to 1 of 1 entries
Address Check	□
Type	● DNS ○ TCP ○ ICMP
Server IP Address	
Next Hop Address	

Submit Cancel

Click **Submit** after you complete the settings.

3. Choose **Network** > **NAT** > **NAT rule** > **SNAT** and click **New**.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure

Not Translate	□	
Translation Type	IPv4 to IPv4	
Source Address	inside-net	
Target Address	any	
Service	any	
Outbound Interface	vlan1	
Source Address After Translation	Address Pool	nat-pool
Unit ID	1	
Description		
Log	□	

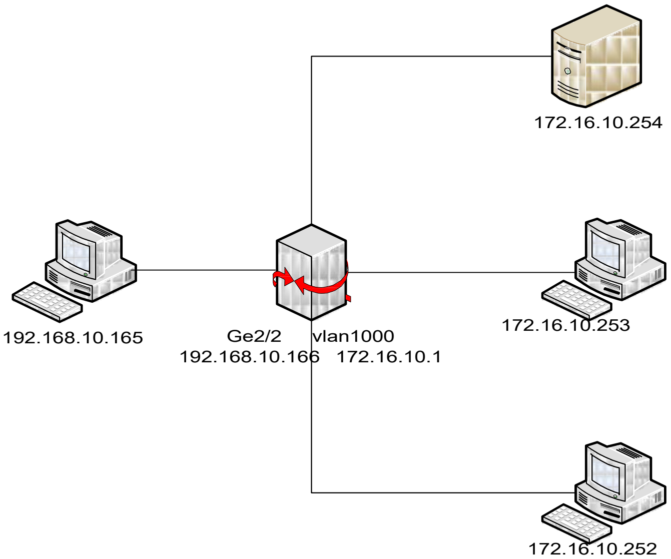
4. Click **Submit** after you complete the settings.

23.3.2 Configuring DNAT

Description:

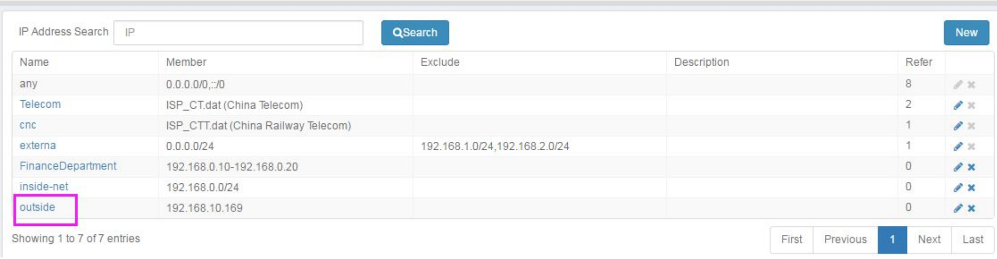
A server on an intranet provides services externally. The server's internal address is 172.16.10.254, which is mapped to the external address 192.168.10.169.

Network diagram:



Procedure:

1. Choose **Object** > **Address object** > **Address node** to create an IPv4 address object named **outside**.

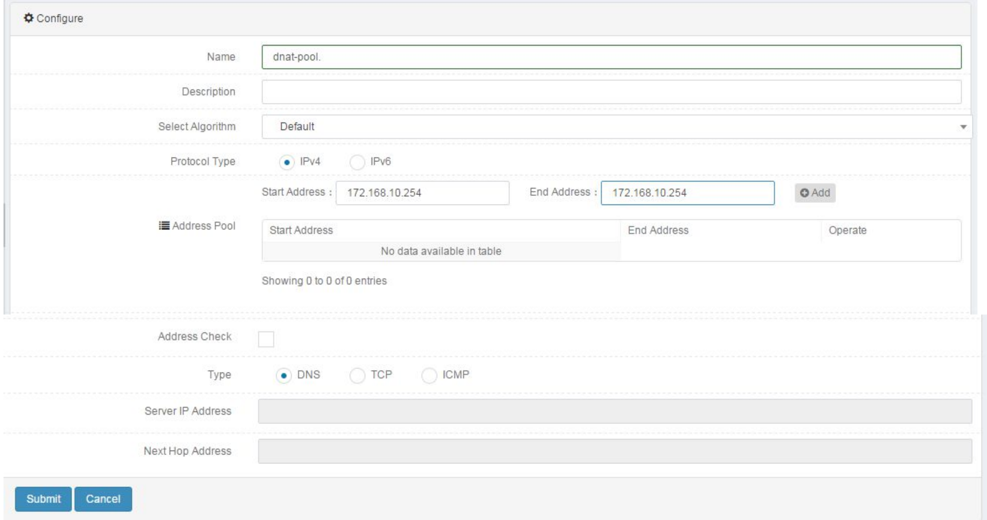


IP Address Search IP

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			8
Telecom	ISP_CT.dat (China Telecom)			2
cnc	ISP_CTT.dat (China Railway Telecom)			1
externa	0.0.0.0/24	192.168.1.0/24,192.168.2.0/24		1
FinanceDepartment	192.168.0.10-192.168.0.20			0
inside-net	192.168.0.0/24			0
outside	192.168.10.169			0

Showing 1 to 7 of 7 entries

2. Choose **Network** > **NAT** > **NAT pool** to create a NAT pool called **dnat-pool**.



Configure

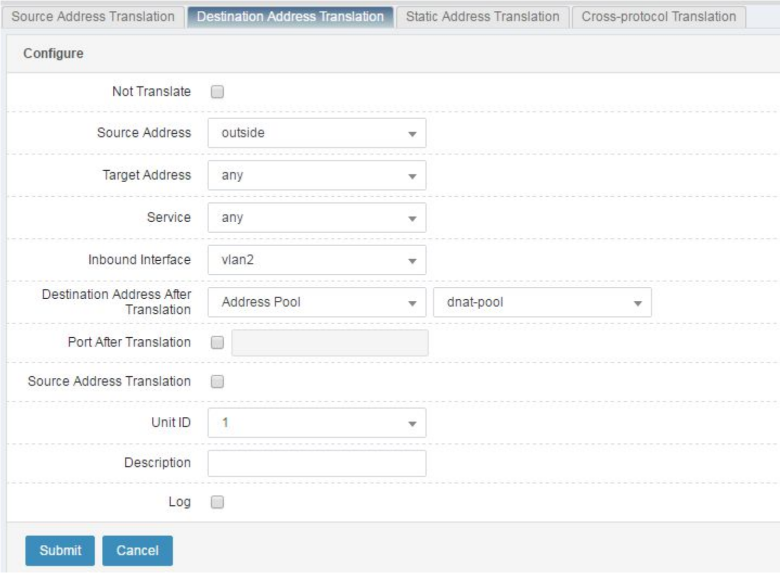
Name	dnat-pool.
Description	
Select Algorithm	Default
Protocol Type	● IPv4 ○ IPv6
Address Pool	Start Address : 172.168.10.254 End Address : 172.168.10.254

Start Address	End Address	Operate
No data available in table		

Showing 0 to 0 of 0 entries

Address Check	□
Type	● DNS ○ TCP ○ ICMP
Server IP Address	
Next Hop Address	

3. Choose **Network** > **NAT** > **NAT rule** > **DNAT** and click **New**.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure
Submit
Cancel

Not Translate	□
Source Address	outside
Target Address	any
Service	any
Inbound Interface	vlan2
Destination Address After Translation	Address Pool / dnat-pool
Port After Translation	□
Source Address Translation	□
Unit ID	1
Description	
Log	□

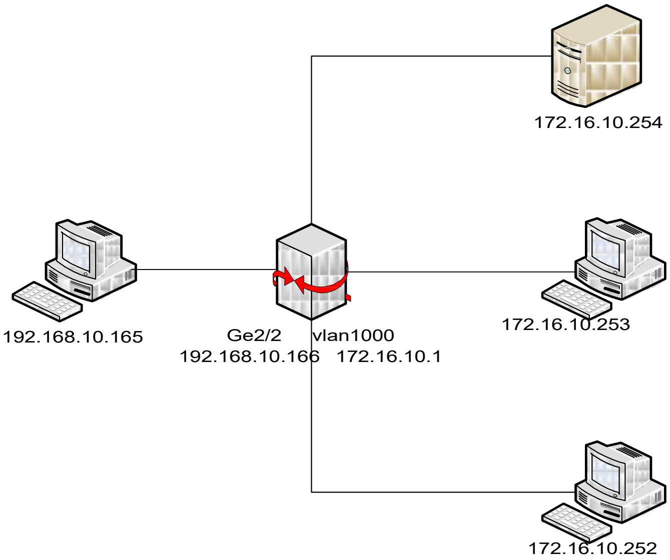
4. Click **Submit** after you complete the settings.

23.3.3 Configuring Bidirectional NAT

Description:

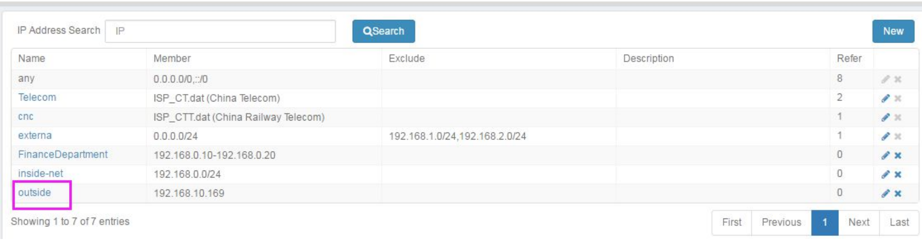
A server on an intranet provides services externally. The server's internal address is 172.16.10.254, which is mapped to the external address 192.168.10.169. An internal address 172.16.10.252 and an external IP address 192.168.10.165 need to access the server.

Network diagram:



Procedure:

1. Choose **Object** > **Address object** > **Address node** to create an IPv4 address object named **outside**.

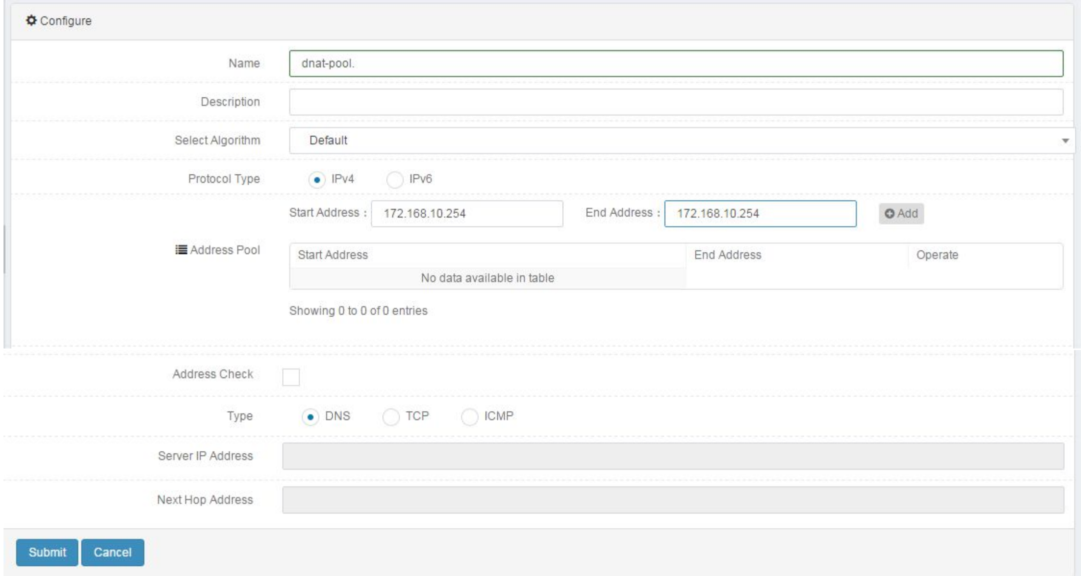


IP Address Search IP

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			8
Telecom	ISP_CT.dat (China Telecom)			2
cnc	ISP_CTT.dat (China Railway Telecom)			1
externa	0.0.0.0/24	192.168.1.0/24,192.168.2.0/24		1
FinanceDepartment	192.168.0.10-192.168.0.20			0
inside-net	192.168.0.0/24			0
outside	192.168.10.169			0

Showing 1 to 7 of 7 entries

2. Choose **Network** > **NAT** > **NAT pool** to create a NAT pool called **dnat-pool**.



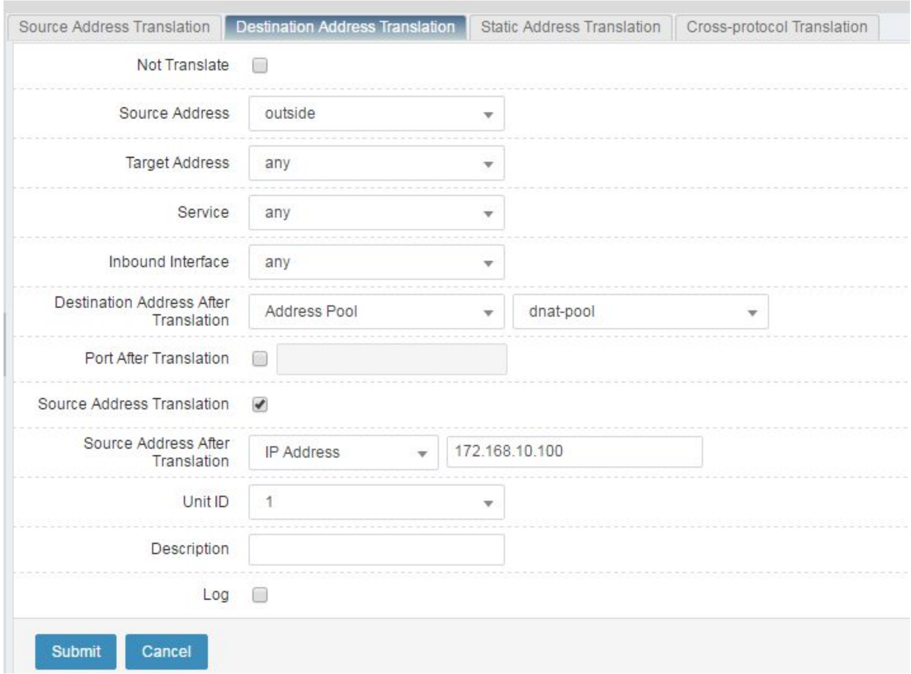
Configure

Name	dnat-pool.
Description	
Select Algorithm	Default
Protocol Type	● IPv4 ○ IPv6
Address Pool	Start Address : 172.168.10.254 End Address : 172.168.10.254
Address Check	□
Type	● DNS ○ TCP ○ ICMP
Server IP Address	
Next Hop Address	

Start Address	End Address	Operate
No data available in table		

Showing 0 to 0 of 0 entries

3. Choose **Network** > **NAT** > **NAT Rule** > **DNAT** and click **New**.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation

Not Translate	□
Source Address	outside
Target Address	any
Service	any
Inbound Interface	any
Destination Address After Translation	Address Pool dnat-pool
Port After Translation	□
Source Address Translation	☑
Source Address After Translation	IP Address 172.168.10.100
Unit ID	1
Description	
Log	□

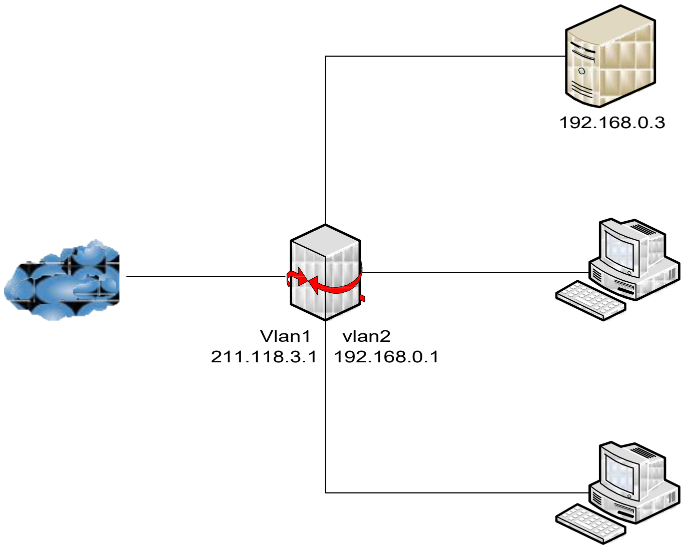
4. Click **Submit** after you complete the settings.

23.3.4 Configuring Static NAT

Description:

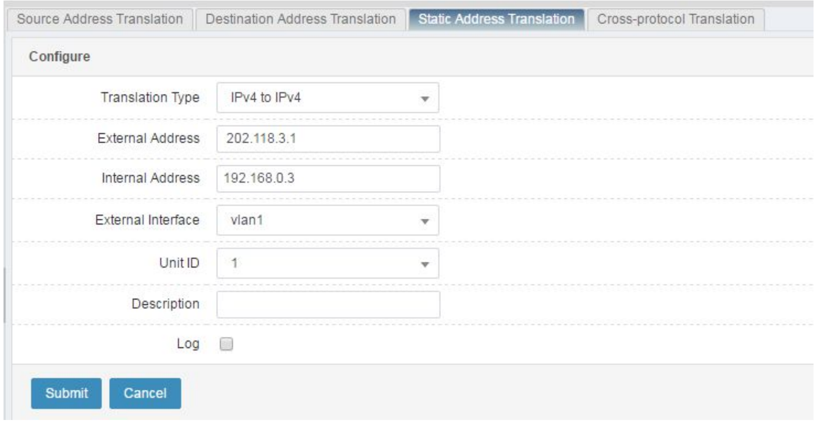
A server on an intranet provides services externally. The server's internal address is 192.168.0.3, which is mapped to the public address 202.118.3.1.

Network diagram:



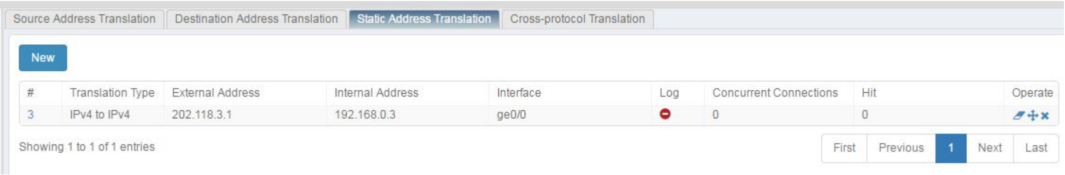
Procedure:

1. Choose **Network configuration** > **NAT** > **NAT rule** > **Static NAT** and click **New.**


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure

Translation Type	IPv4 to IPv4
External Address	202.118.3.1
Internal Address	192.168.0.3
External Interface	vlan1
Unit ID	1
Description	
Log	□

2. Click **Submit** after you complete the settings. The following page appears.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
New

#	Translation Type	External Address	Internal Address	Interface	Log	Concurrent Connections	Hit	Operate
3	IPv4 to IPv4	202.118.3.1	192.168.0.3	ge0/0	⛔	0	0	

Showing 1 to 1 of 1 entries

First
Previous
1
Next
Last

23.4 Monitoring and Maintenance

23.4.1 Displaying NAT Pools and NAT Rules

Choose **Network** > **NAT** to display the configured NAT pools and NAT rules.

23.5 Troubleshooting

23.5.1 Intermittent Disconnection

Symptom	After NAT is performed, a device in another network is pinged. The device is occasionally or always unreachable.
Solution	1. Check whether the address after conversion conflicts with another address or is already in use. Some addresses may not be pingable, while some others may be already in use. In the latter case, check whether ping packets are blocked at the peer end. 2. Check the ARP entry of the pinged device. Check whether the MAC address corresponding to the address after NAT is the device's MAC address. If not, the IP address is used by another device. Use an idle address as the address after NAT.

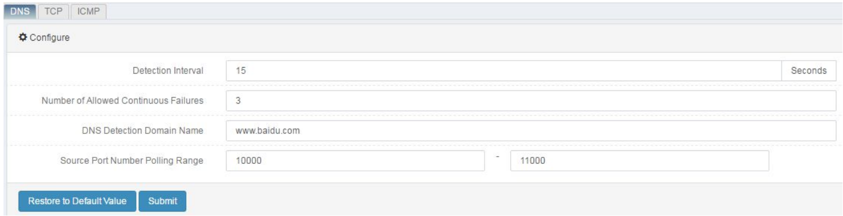
24 NAT PoolChecking

24.1 Configuring NAT Pool Checking

The NAT pool checking function checks the availability of the addresses in a NAT pool. After this function is enabled, the unavailable addresses in the NAT pool can be excluded from SNAT. NAT pool checking supports DNS, TCP, and ICMP modes. You can select a mode to check a NAT pool as needed. Each mode has default parameter settings.

Procedure:

1. Choose **Network** > **NAT** > **NAT pool checking**. The following page appears.

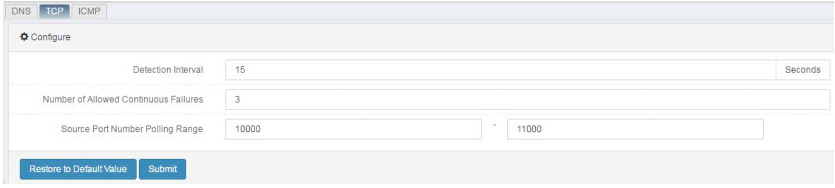


Detection Interval 15 Seconds

Number of Allowed Continuous Failures 3

DNS Detection Domain Name www.baidu.com

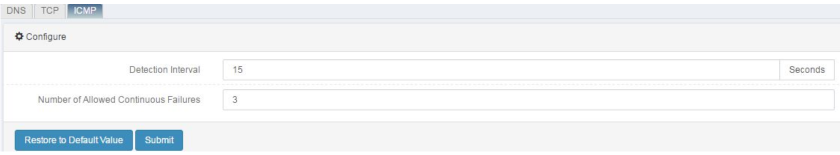
Source Port Number Polling Range 10000 - 11000



Detection Interval 15 Seconds

Number of Allowed Continuous Failures 3

Source Port Number Polling Range 10000 - 11000



Detection Interval 15 Seconds

Number of Allowed Continuous Failures 3

Detection interval: The default value is **15**, in seconds, indicating that availability check is performed on the addresses in the NAT pool every 15s.

Allowed consecutive failure times: The default value is **3**. For example, availability check is performed on the addresses in the NAT pool every 15s. If address A is found to be unavailable once, one failure is recorded. Availability check is performed for the second time after 15s. When address A is found to be unavailable for three consecutive times, A is marked as Unavailable.

DNS detection domain name: The default value is **www.baidu.com**. The domain name cannot exceed 128 characters.

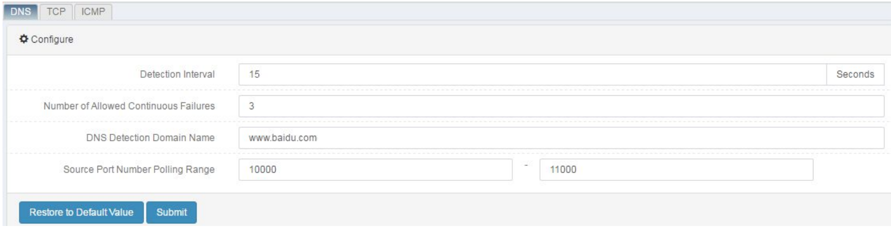
Source port round robin range: The default range is 10000 to 11000. The allowable range is 1024 to 65535.

⚠ Notice

The NAT pool checking function is only applicable to the IPv4 protocol type.

24.2 Modifying the NAT Pool Checking Configurations

Choose **Network** > **NAT** > **NAT pool checking**.



Detection Interval: 15 Seconds

Number of Allowed Continuous Failures: 3

DNS Detection Domain Name: www.baidu.com

Source Port Number Polling Range: 10000 - 11000

Click the **DNS** tab and modify the parameters. Then click **Submit**. To restore the default settings, click **Restore default** and click **Submit**. The modification in TCP and ICMP modes is similar.

Detection interval: Interval at which a NAT pool is checked.

Allowed consecutive failure times: Maximum number of consecutive times an address is found to be unavailable until its status is marked as Unavailable.

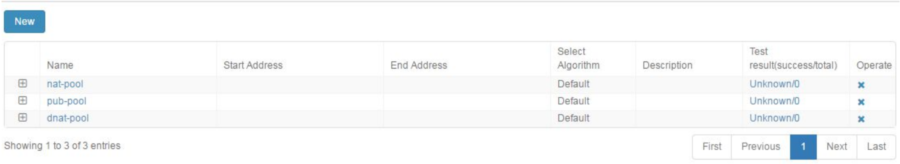
DNS detection domain name: Set this parameter

when NAT pool checking is in DNS mode.

Source port range: Source ports that send packets. The default range is 10000 to 11000.

24.3 Enabling NAT Pool Checking

Choose **Network** > **NAT** > **NAT pool**. The following page appears.

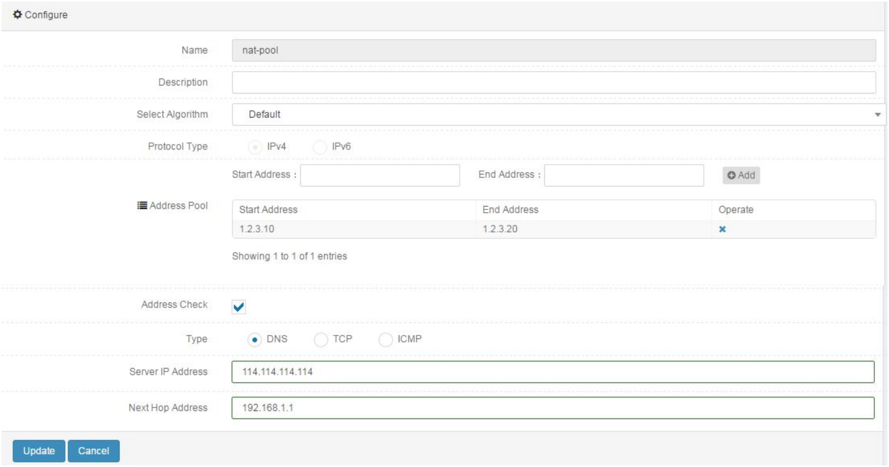


New

	Name	Start Address	End Address	Select Algorithm	Description	Test result(success/total)	Operate
⊞	nat-pool			Default		Unknown/0	✖
⊞	pub-pool			Default		Unknown/0	✖
⊞	dnat-pool			Default		Unknown/0	✖

Showing 1 to 3 of 3 entries

For a NAT pool not enabled with the checking function, its **Check result** column shows **Unknown**. Click a pool name to enable the checking function for the NAT pool.



Configure

Name	nat-pool
Description	
Select Algorithm	Default
Protocol Type	○ IPv4 ○ IPv6
Address Pool	Start Address : End Address : Add
Address Check	☑
Type	● DNS ○ TCP ○ ICMP
Server IP Address	114.114.114.114
Next Hop Address	192.168.1.1

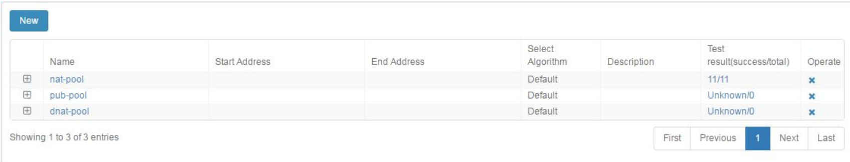
Start Address	End Address	Operate
1.2.3.10	1.2.3.20	✖

Showing 1 to 1 of 1 entries

Check the **Address check** box, and set **Server IP address** and **Next-hop address**. If you select **TCP**, also set the destination port. Click **Update**.

24.4 Disabling NAT Pool Checking

Choose **Network** > **NAT** > **NAT pool**. The following page appears.

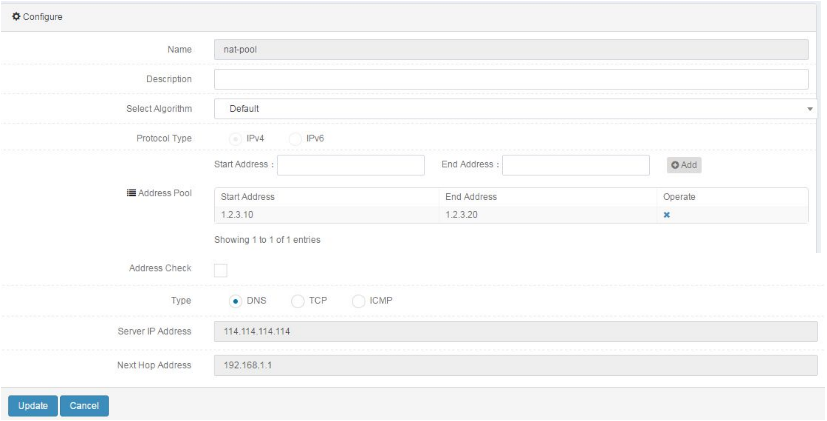


New

	Name	Start Address	End Address	Select Algorithm	Description	Test result(success/total)	Operate
⊞	nat-pool			Default		11/11	✖
⊞	pub-pool			Default		Unknown/0	✖
⊞	dnat-pool			Default		Unknown/0	✖

Showing 1 to 3 of 3 entries

Click the name of the NAT pool for which you want to disable the checking function.



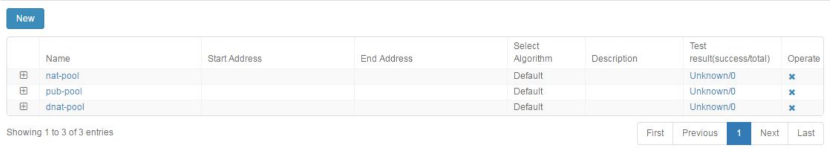
Configure

Name	nat-pool
Description	
Select Algorithm	Default
Protocol Type	○ IPv4 ○ IPv6
Address Pool	Start Address : End Address : Add
Address Check	□
Type	● DNS ○ TCP ○ ICMP
Server IP Address	114.114.114.114
Next Hop Address	192.168.1.1

Start Address	End Address	Operate
1.2.3.10	1.2.3.20	✖

Showing 1 to 1 of 1 entries

Uncheck the **Address check** box and click **Update**.



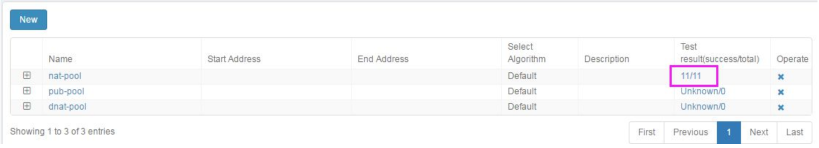
New

	Name	Start Address	End Address	Select Algorithm	Description	Test result(success/total)	Operate
⊞	nat-pool			Default		Unknown/0	✖
⊞	pub-pool			Default		Unknown/0	✖
⊞	dnat-pool			Default		Unknown/0	✖

Showing 1 to 3 of 3 entries

24.5 Displaying the NAT Pool Checking Result

Choose **Network** > **NAT** > **NAT pool**. The following page appears.

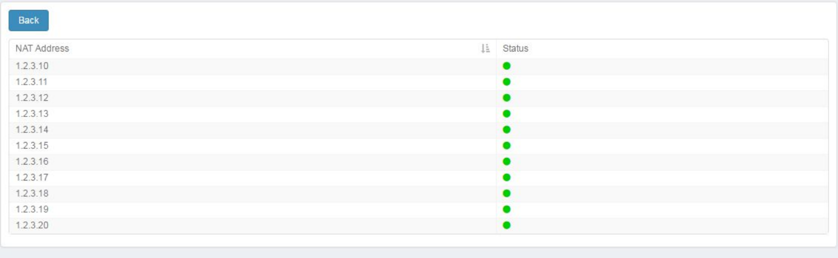


New

	Name	Start Address	End Address	Select Algorithm	Description	Test result(success/total)	Operate
⊞	nat-pool			Default		11/11	✖
⊞	pub-pool			Default		Unknown/0	✖
⊞	dnat-pool			Default		Unknown/0	✖

Showing 1 to 3 of 3 entries

View the **Check result** column. Click the check result to display the detailed results of specific addresses in the NAT pool.



NAT Address	Status
1.2.3.10	●
1.2.3.11	●
1.2.3.12	●
1.2.3.13	●
1.2.3.14	●
1.2.3.15	●
1.2.3.16	●
1.2.3.17	●
1.2.3.18	●
1.2.3.19	●
1.2.3.20	●

25 Cross-protocol Address Translation

25.1 Overview

Cross-protocol address translation is a method to convert between IPv4 and IPv6 addresses for seamless interoperability between the two protocol stacks to support gradual transition from IPv4 to IPv6 network environments.

RAVEN 5000 firewalls support NAT46 and NAT64. In NAT46, the IPv4 address of a request packet is converted to an IPv6 address. In NAT64, the IPv6 address of a request packet is converted to an IPv4 address. Multiple conversion methods are provided. You can select a suitable one according to your network environment to enable access between IPv4 and IPv6 networks.

25.2 Configuration

Cross-protocol address translation supports NAT46 and NAT64 and three conversion methods: IVI conversion, embedded address conversion, and NAT pool conversion.

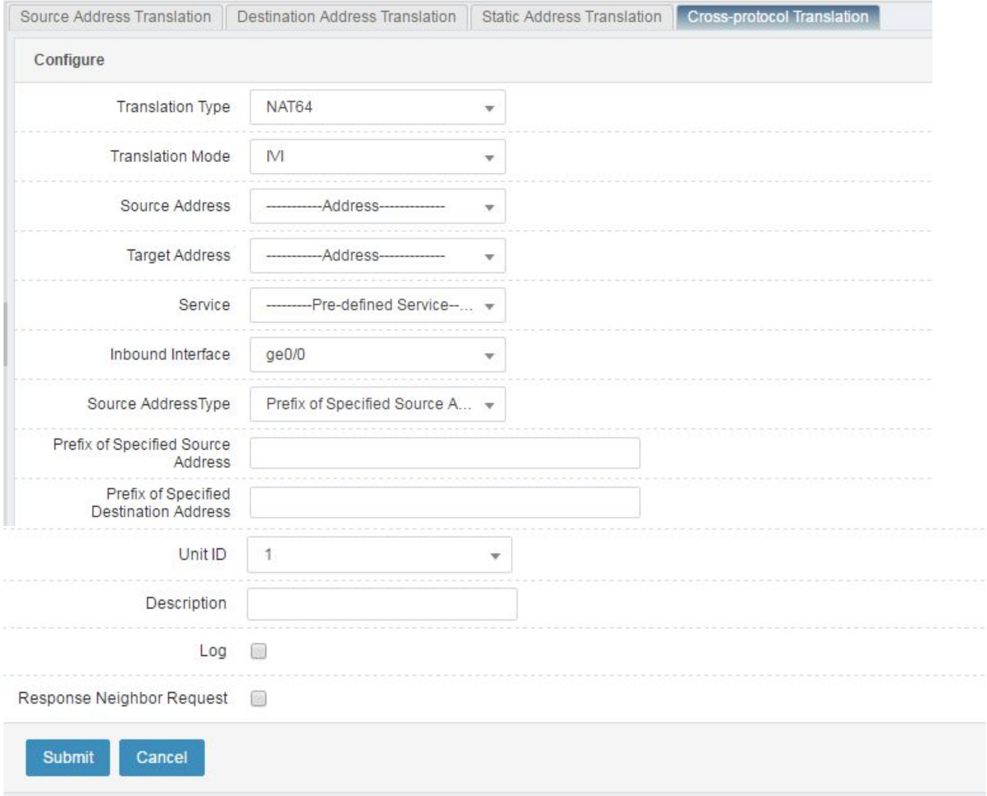
25.2.1 Configuring IVI Conversion

IVI conversion is a stateless address mapping technique proposed by China Education and Research Network (CERNET). It converts between IPv4 and IPv6 addresses using a specified prefix.

IVI conversion is applicable to NAT46 and NAT64.

Procedure:

1. Choose **Network** > **NAT** > **NAT Rule: Cross-protocol address translation** and click **New.** The following page appears.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Submit
Cancel

Configure

Translation Type	NAT64
Translation Mode	IVI
Source Address	-----------Address------------
Target Address	-----------Address------------
Service	---------Pre-defined Service--...
Inbound Interface	ge0/0
Source AddressType	Prefix of Specified Source A...
Prefix of Specified Source Address	
Prefix of Specified Destination Address	
Unit ID	1
Description	
Log	□
Response Neighbor Request	□

Conversion type: The options are **NAT46** and **NAT64**.

Conversion method: The options are **IVI**, **Embedded address**, and **NAT pool**. Select **IVI**.

Source address: Source address object or address group matched with the rule.

Destination address: Destination address object or address group matched with the rule.

Service: Service object matched with the rule.

Inbound interface: Inbound interface matched with the rule.

Source address type: Source address conversion method. The options are:

> **Specify source address prefix**: Convert the source address by IVI based on a specified prefix. It must be a 32-bit mask.
>
> **Source address after conversion**: Select an address in a specified NAT pool as the source address after conversion, or converts the source address to an outbound interface address.

Specify destination address prefix: Convert the destination address by IVI based on a specified prefix. It must be a 32-bit mask.

Unit ID: Unit ID of the rule, which takes effect when the high availability feature is enabled.

Description: Description about the rule, no more than 128 bytes.

Log: Check this box to enable logging.

Respond to ARP or **Respond to neighbor request**: Whether the rule responds to ARP requests or neighbor requests. The range of ARP requests to which the NAT46 rule responds and the range of neighbor requests to which the NAT64 rule responds are determined by the destination address object and inbound interface.

⚠ Notice

When configuring NAT64 in IVI mode, ensure that the matched address object does not conflict with the conversion prefix; otherwise, packets are forwarded as they are.

If the address of an IPv6 packet matched with a NAT64 IVI rule is not a standard IVI-formatted address, the packet will be forwarded as it is.

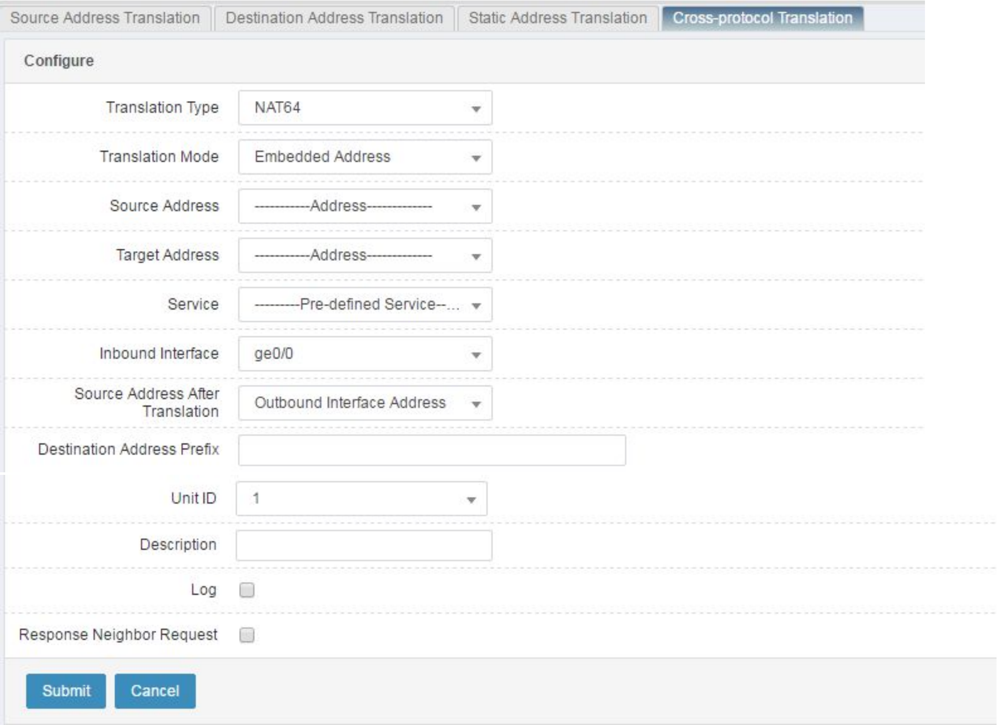
2. Click **Submit** after you complete the settings.

25.2.2 Configuring Embedded Address Conversion

Embedded address conversion is only applicable to NAT64. The destination address after conversion is the 32-bit segment after a specified prefix of the original IPv6 destination address. For source address conversion, you can specify a NAT pool or convert it to an outbound interface address.

Procedure:

Choose **Network** > **NAT** > **NAT Rule: Cross-protocol address translation** and click **New**. On the displayed page, select **NAT64** for **Conversion type** and **Embedded address** for **Conversion method**.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure
Submit
Cancel

Translation Type	NAT64
Translation Mode	Embedded Address
Source Address	-----------Address-------------
Target Address	-----------Address-------------
Service	---------Pre-defined Service--…
Inbound Interface	ge0/0
Source Address After Translation	Outbound Interface Address
Destination Address Prefix	
Unit ID	1
Description	
Log	□
Response Neighbor Request	□

Conversion type: The options are **NAT46** and **NAT64**. Select **NAT64** for embedded address conversion.

Conversion method: The options are **IVI**, **Embedded address**, and **NAT pool**. Select **Embedded address**.

Source address: Source address object or address group matched with the rule.

Destination address: Destination address object or address group matched with the rule.

Service: Service object matched with the rule.

Inbound interface: Inbound interface matched with the rule.

Source address after conversion: Select an address in a specified NAT pool as the source address after conversion, or converts the source address to an outbound interface address.

Destination address prefix: Convert the destination address to the embedded 32-bit IPv4 address after a specified prefix of the IPv6 destination address. The maximum prefix length is 96 bits.

Unit ID: Unit ID of the rule, which takes effect when the high availability feature is enabled.

Description: Description about the rule, no more than 128 bytes.

Log: Check this box to enable logging.

Respond to neighbor request: Whether the rule responds to neighbor requests. The range of neighbor requests to which the NAT64 rule responds to is determined by the matched destination address object and inbound interface.

⚠ Notice

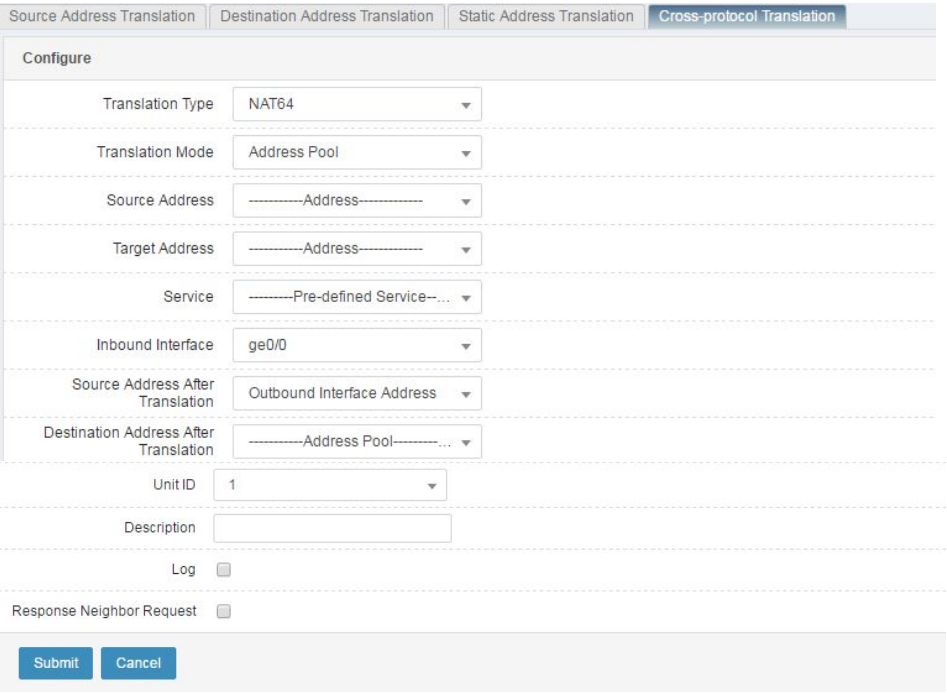
During embedded address conversion, if the configured destination address prefix is inconsistent with the packet's destination address, the packet will be forwarded as it is.

25.2.3 Configuring NAT Pool Conversion

NAT pool conversion is applicable to NAT64 and NAT46. The destination address after conversion is specified as an address in a NAT pool. The source address after conversion is also specified as an address in a NAT pool or an outbound interface address.

Procedure:

Choose **Network** > **NAT** > **NAT rule: Cross-protocol address translation** and click **New**. On the displayed page, select **NAT pool** for **Conversion method**.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Submit
Cancel

Configure

Translation Type	NAT64
Translation Mode	Address Pool
Source Address	-----------Address-------------
Target Address	-----------Address-------------
Service	---------Pre-defined Service--...
Inbound Interface	ge0/0
Source Address After Translation	Outbound Interface Address
Destination Address After Translation	-----------Address Pool---------...
Unit ID	1
Description	
Log	□
Response Neighbor Request	□

Conversion type: The options are **NAT46** and **NAT64**.

Conversion method: The options are **IVI**, **Embedded address**, and **NAT pool**. Select **NAT pool**.

Source address: Source address object or address group matched with the rule.

Destination address: Destination address object or address group matched with the rule.

Service: Service object matched with the rule.

Inbound interface: Inbound interface matched with the rule.

Source address after conversion: Select an address in a specified NAT pool as the source address after conversion, or converts the source address to an outbound interface address.

Destination address after conversion: Select an address in a specified NAT pool as the destination address after conversion.

Unit ID: Unit ID of the rule, which takes effect when the high availability feature is enabled.

Description: Description about the rule, no more than 128 bytes.

Log: Check this box to enable logging.

Respond to ARP or **Respond to neighbor request**: Whether the rule responds to ARP requests or neighbor requests. The range of ARP requests to which the NAT46 rule responds and the range of neighbor requests to which the NAT64 rule responds are determined by the destination address object and inbound interface.

⚠ Notice	The NAT pool corresponding to the destination address after conversion must contain at least one routable address; otherwise, the packet will be forwarded as it is.

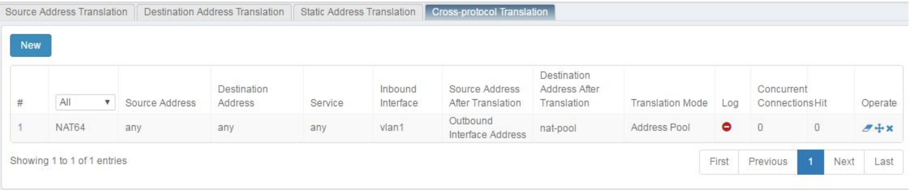
⚠ Notice	The source address and destination address configured for each NAT64 rule must be IPv6 address objects, and the referenced NAT pool must be of the IPv4 type. The source address and destination address configured for each NAT46 rule must be IPv4 address objects, and the referenced NAT pool must be of the IPv6 type.

25.2.4 Modifying a NAT46 or NAT64 Rule

You can modify an existing NAT46 or NAT64 rule.

Procedure:

1. Choose **Network configuration** > **NAT** > **Cross-protocol address translation.** The following page appears.



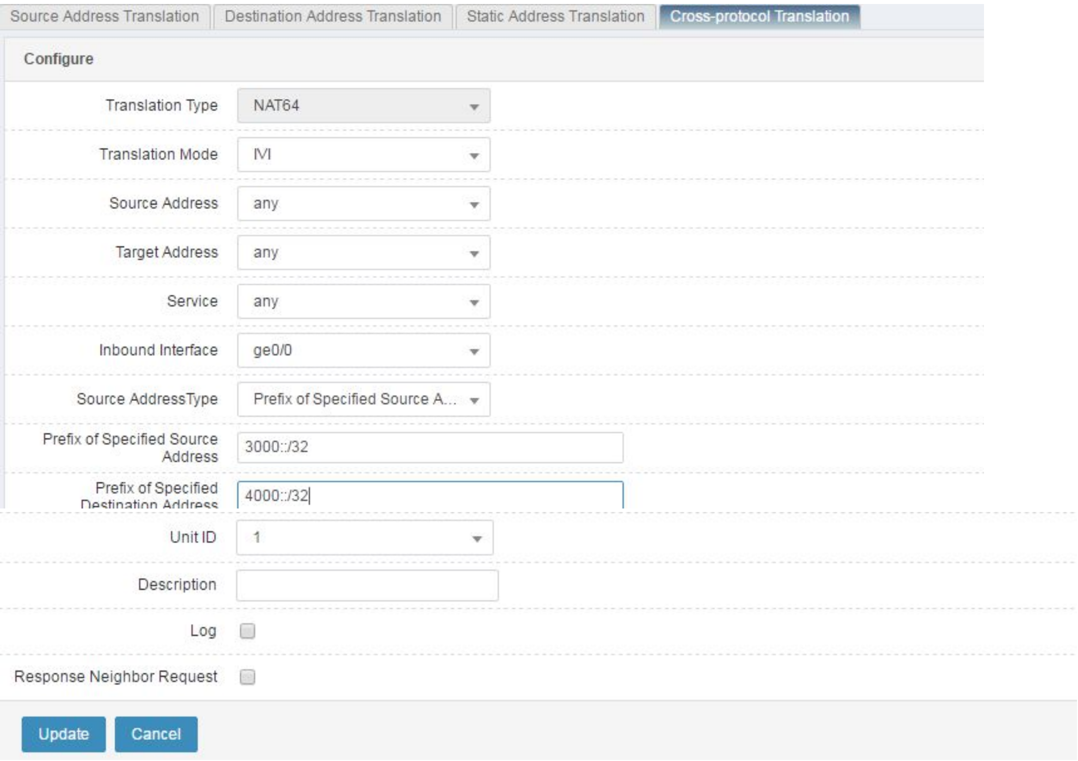
Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
New

#	All ▾	Source Address	Destination Address	Service	Inbound Interface	Source Address After Translation	Destination Address After Translation	Translation Mode	Log	Concurrent Connections	Hit	Operate
1	NAT64	any	any	any	vlan1	Outbound Interface Address	nat-pool	Address Pool	⊖	0	0	✎ ✣ ✕

Showing 1 to 1 of 1 entries

First
Previous
1
Next
Last

2. Click a rule ID.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure

Translation Type	NAT64
Translation Mode	IVI
Source Address	any
Target Address	any
Service	any
Inbound Interface	ge0/0
Source AddressType	Prefix of Specified Source A...
Prefix of Specified Source Address	3000::/32
Prefix of Specified Destination Address	4000::/32
Unit ID	1
Description	
Log	□
Response Neighbor Request	□

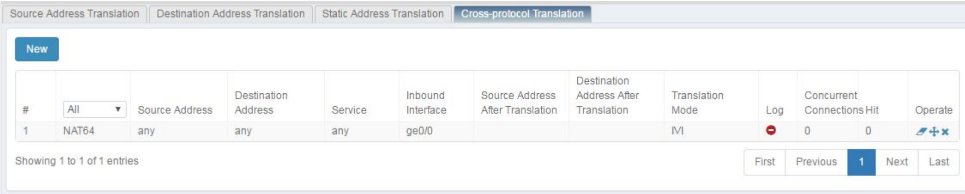
3. Modify the parameters. **Conversion type** cannot be modified.

4. Click **Update**.

25.2.5 Deleting a NAT46 or NAT64 Rule

Procedure:

1. Choose **Network configuration** > **NAT** > **Cross-protocol address translation**. The following page appears.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
New

#	All ▾	Source Address	Destination Address	Service	Inbound Interface	Source Address After Translation	Destination Address After Translation	Translation Mode	Log	Concurrent Connections	Hit	Operate
1	NAT64	any	any	any	ge0/0			IVI	⊖	0	0	✎ ✥ ✖

Showing 1 to 1 of 1 entries

First
Previous
1
Next
Last

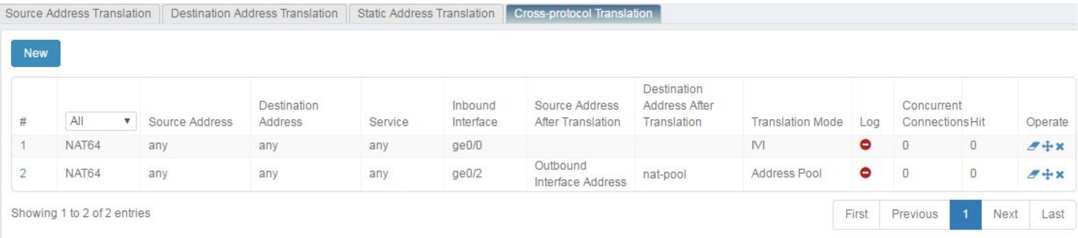
2. Click ✖ next to the rule ID you want to delete.

25.2.6 Moving a NAT46 or NAT64 Rule

You can adjust the match order of NAT46 and NAT64 rules of the same conversion type.

Procedure:

1. Choose **Network configuration** > **NAT** > **Cross-protocol address translation**. The following page appears.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
New

#	All ▾	Source Address	Destination Address	Service	Inbound Interface	Source Address After Translation	Destination Address After Translation	Translation Mode	Log	Concurrent Connections	Hit	Operate
1	NAT64	any	any	any	ge0/0			IVI	⊖	0	0	✎ ✣ ✕
2	NAT64	any	any	any	ge0/2	Outbound Interface Address	nat-pool	Address Pool	⊖	0	0	✎ ✣ ✕

Showing 1 to 2 of 2 entries

First
Previous
1
Next
Last

2. Click ✣ next to the rule ID you want to move.

25.3 Configuration Examples

25.3.1 Configuring NAT46

Description:

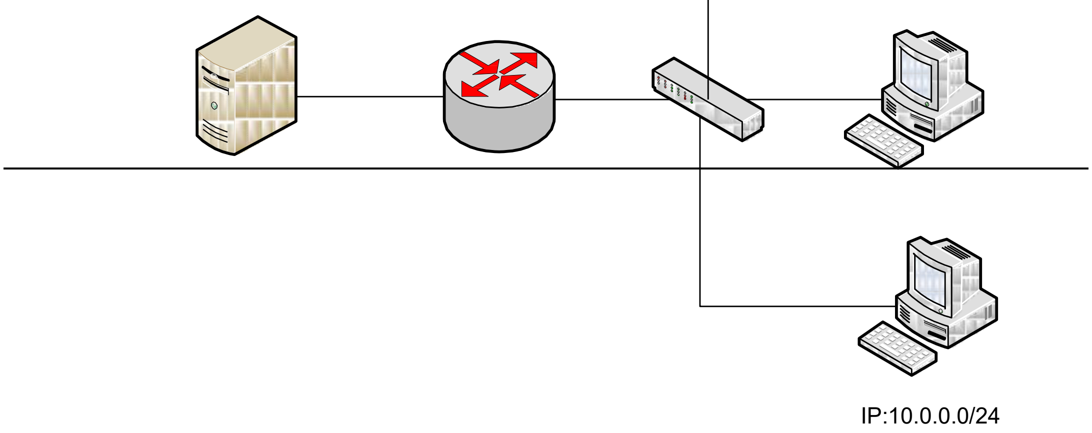
A company's LAN is an IPv4 network. It needs to access an FTP site in an IPv6 LAN through a T-series firewall. The FTP site address is 2010::80, and the company's LAN address segment is 10.0.0.0/24. The T-series firewall works as a core router which is serially connected to the network.

Network diagram:

Server
2010::80

Vlan2
2010::1

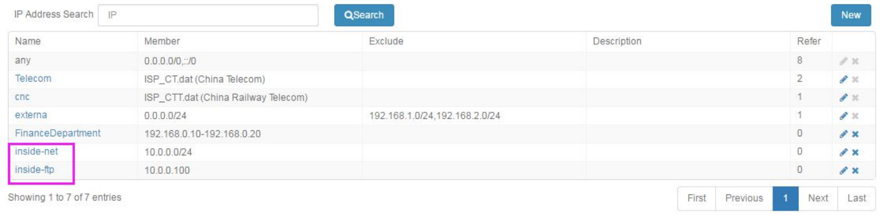
Vlan1
10.0.0.1



Procedure:

1. Choose **Object** > **Address object** > **Address node** to create an IPv4 address object named **inside-net**.

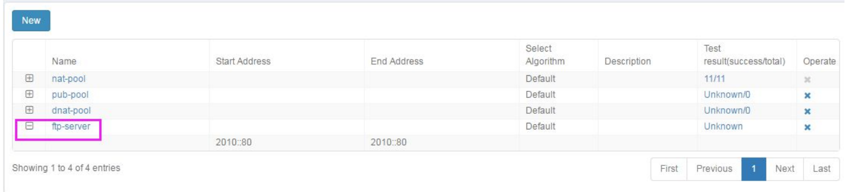
2. address object named **inside-ftp**. The address is the address of the FTP server mapped to the intranet and cannot conflict with the address of any internal PC.


IP Address Search IP Search New

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			8
Telecom	ISP_CT.dat (China Telecom)			2
cnc	ISP_CTT.dat (China Railway Telecom)			1
externa	0.0.0.0/24	192.168.1.0/24,192.168.2.0/24		1
FinanceDepartment	192.168.0.10-192.168.0.20			0
inside-net	10.0.0.0/24			0
inside-ftp	10.0.0.100			0

Showing 1 to 7 of 7 entries

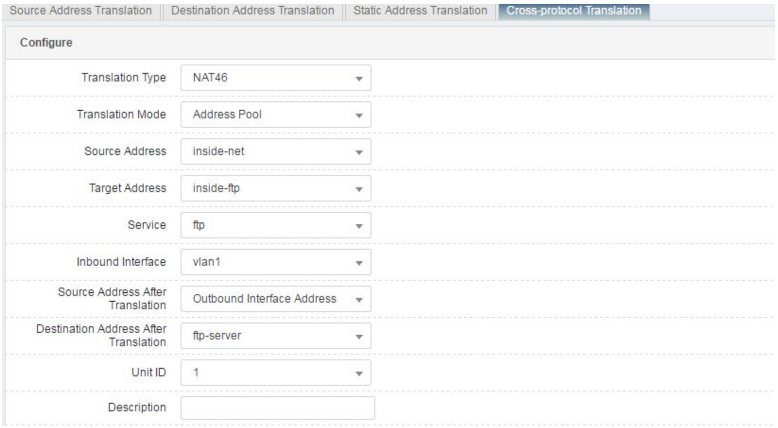
2. Choose **Network** > **NAT** > **NAT pool** to create an IPv6 address pool named **ftp-server**.



	Name	Start Address	End Address	Select Algorithm	Description	Test result(success/total)	Operate
⊞	nat-pool			Default		11/11	✖
⊞	pub-pool			Default		Unknown/0	✖
⊞	dnat-pool			Default		Unknown/0	✖
⊟	ftp-server			Default		Unknown	✖
		2010::80	2010::80				

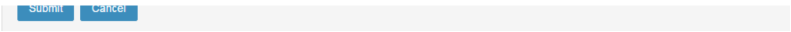
Showing 1 to 4 of 4 entries

3. Choose **Network** > **NAT** > **Cross-protocol address translation** to create a NAT46 rule.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation

Configure

Translation Type	NAT46
Translation Mode	Address Pool
Source Address	inside-net
Target Address	inside-ftp
Service	ftp
Inbound Interface	vlan1
Source Address After Translation	Outbound Interface Address
Destination Address After Translation	ftp-server
Unit ID	1
Description	



Notice

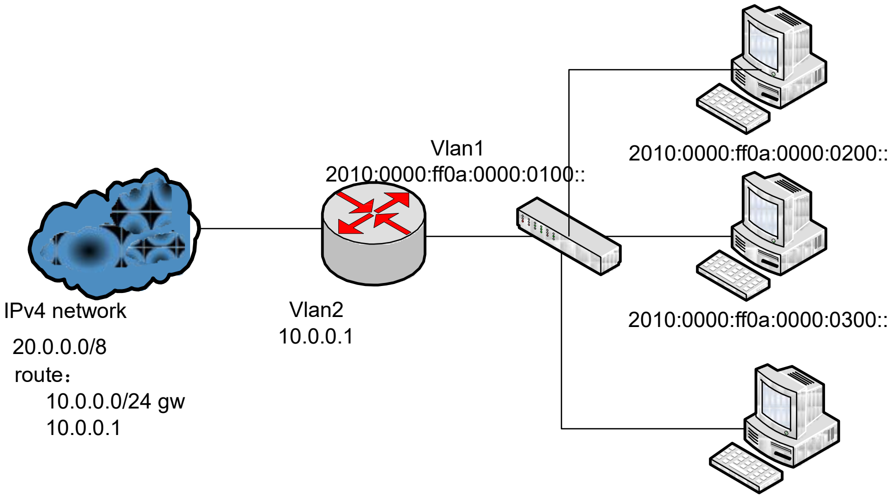
The firewall works as an IPv6 server proxy. **Respond to ARP** must be selected to ensure that the requests sent from the IPv4 intranet to the proxy server address 10.0.0.100 can be forwarded to the firewall.

25.3.2 Configuring NAT64

Description:

An ISP allocates an IVI prefix 2010::/32 to an IPv6 educational LAN, where users need to access the external IPv4 address segment 20.0.0.0/8. The T-series firewall works as a core router which is serially connected to the network.

Network diagram:

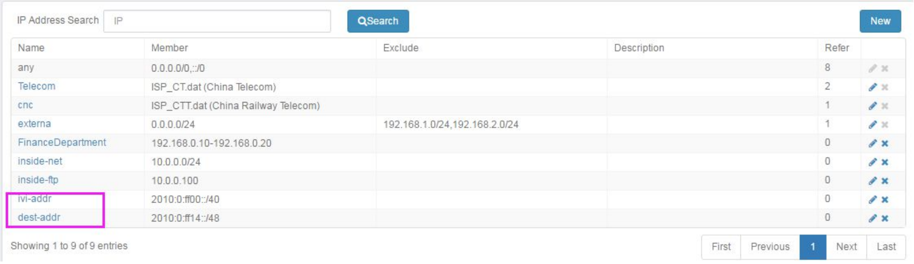

Vlan1
2010:0000:ff0a:0000:0100::
2010:0000:ff0a:0000:0200::
2010:0000:ff0a:0000:0300::
IPv4 network
20.0.0.0/8
route：
10.0.0.0/24 gw
10.0.0.1
Vlan2
10.0.0.1

2010:0000:ff0a:0000:0400::

internal route
2010:0000:ff14::/48 gw
2010:0000:ff0a:0000:0100::

Procedure:

1. Choose **Object** > **Address object** > **Address node** to create IPv6 address objects named **ivi-addr** and **dest-addr**.

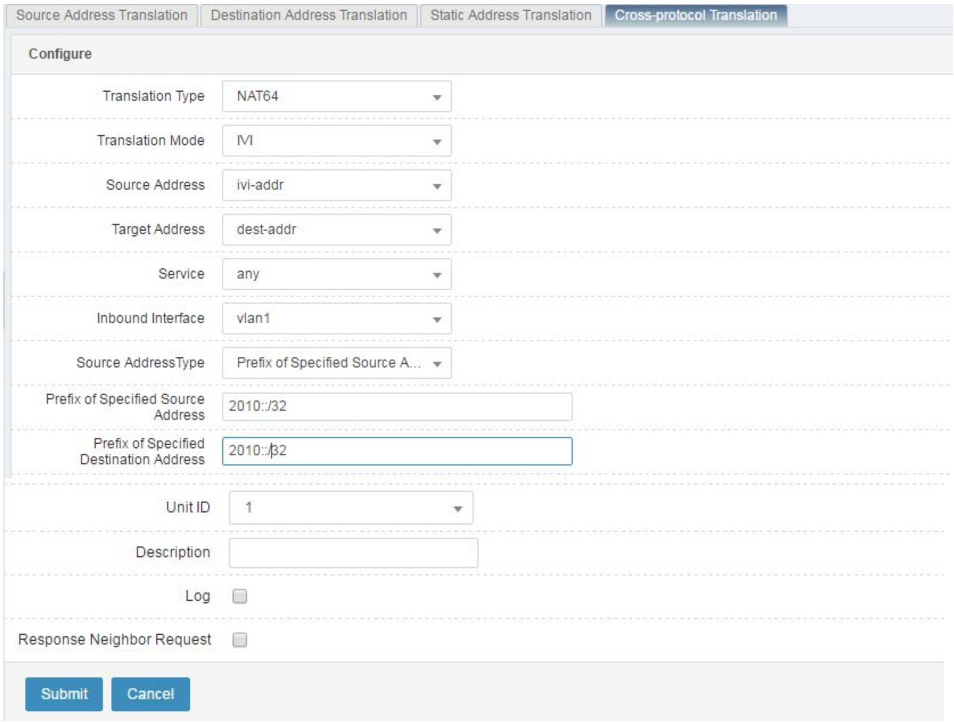


IP Address Search: IP

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			8
Telecom	ISP_CT.dat (China Telecom)			2
cnc	ISP_CTT.dat (China Railway Telecom)			1
externa	0.0.0.0/24	192.168.1.0/24,192.168.2.0/24		1
FinanceDepartment	192.168.0.10-192.168.0.20			0
inside-net	10.0.0.0/24			0
inside-ftp	10.0.0.100			0
ivi-addr	2010:0:ff00::/40			0
dest-addr	2010:0:ff14::/48			0

Showing 1 to 9 of 9 entries

2. Choose **Network** > **NAT** > **Cross-protocol address translation** to create a NAT64 rule.



Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation

Configure

Translation Type	NAT64
Translation Mode	IVI
Source Address	ivi-addr
Target Address	dest-addr
Service	any
Inbound Interface	vlan1
Source AddressType	Prefix of Specified Source A...
Prefix of Specified Source Address	2010::/32
Prefix of Specified Destination Address	2010::/32
Unit ID	1
Description	
Log	□
Response Neighbor Request	□

Notice

1. Do not select **Respond to neighbor request** when configuring a NAT 64 rule because a route must be configured on every internal host.
2. 2. For IVI conversion, the firewall does not respond to ARP or neighbor requests corresponding to the address after

conversion. Therefore, a proper route must be configured.

25.4 Troubleshooting

25.4.1 Address Conflict Persists

Symptom	A user's PC has address conflict.
Solution	Check whether **Respond to ARP** or **Respond to neighbor request** is selected for the NAT64 or NAT46 rule. If yes, the firewall responds to the neighbor or ARP requests with the matched destination address on the inbound interface. It is recommended that you deselect **Respond to ARP** or **Respond to neighbor request** if **Destination address** is set to **Any**.

25.4.2 The Request Packet Sent by a User Cannot Reach the Firewall

Symptom	A user wants to access a network of a different protocol type via NAT64 or NAT46. However, packet capture shows that ARP or NS requests are being sent.
Solution	Check whether **Respond to ARP** or **Respond to neighbor request** is selected for the NAT64 or NAT46 rule. If not, request packets may not be able to learn the MAC address corresponding to the destination address.

25.4.3 Address Translation Fails

Symptom	Packet capture on the firewall's outbound interface shows that addresses are not converted.
Solution	For NAT64, check the following configurations: 1. IVI conversion. If the source or destination address is not in the IVI format, addresses are not converted. 2. IVI conversion. If the address object of the rule conflicts with the prefix, addresses are not converted. 3. Embedded address conversion. If the destination address object of the rule conflicts with the prefix of the destination address, addresses are not converted. If routing based on the destination address after conversion fails, packets are forwarded as they are.

26 Port Management

26.1 Overview

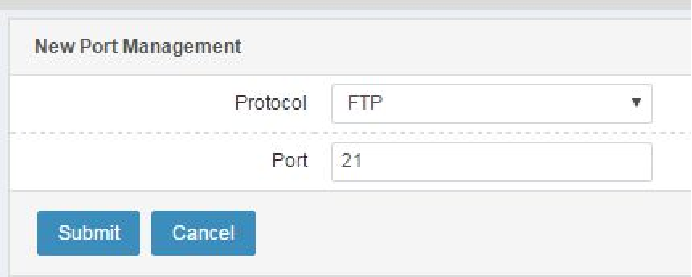
A server may change or add a listening port to a provided service by changing or adding a predefined application level gateway (ALG) port to correctly identify the service type indicated by the port number in a packet.

For example, an FTP server enables port 21 to listen to requests and enables port 1000 to listen to FTP requests. When receiving a packet whose destination port number is 1000, the server identifies the packet to be FTP-related based on the ALG port.

26.2 Configuration

26.2.1 Setting a Port Number

Choose **Network** > **NAT** > **Port management** and click **New**. The following page appears.



New Port Management

Protocol: FTP

Port: 21

Protocol: Protocol type. The options are **FTP** and **TFTP.**

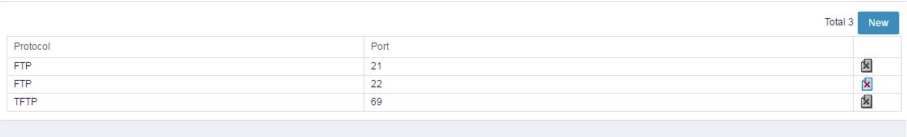
Port: Number of a new listening port of the selected protocol type.

Notice

Apart from the default port, a maximum of seven ports can be added under each protocol type.

26.2.2 Deleting a Port Number

Choose **Configuration** > **NAT** > **Port management.** The following page appears.



Total 3 New

Protocol	Port	
FTP	21	☒
FTP	22	☒
TFTP	69	☒

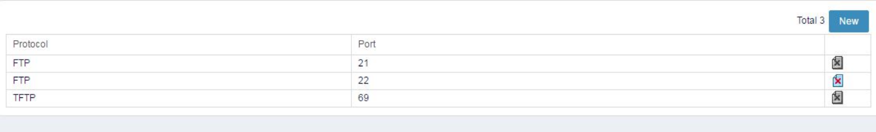
Click ☒ next to the port you want to delete.

Notice

The default port cannot be deleted.

26.2.3 Displaying Port Numbers

Choose **Configuration** > **NAT** > **Port management.** A page appears to display all the configured port numbers.



Total 3 New

Protocol	Port	
FTP	21	☒
FTP	22	☒
TFTP	69	☒

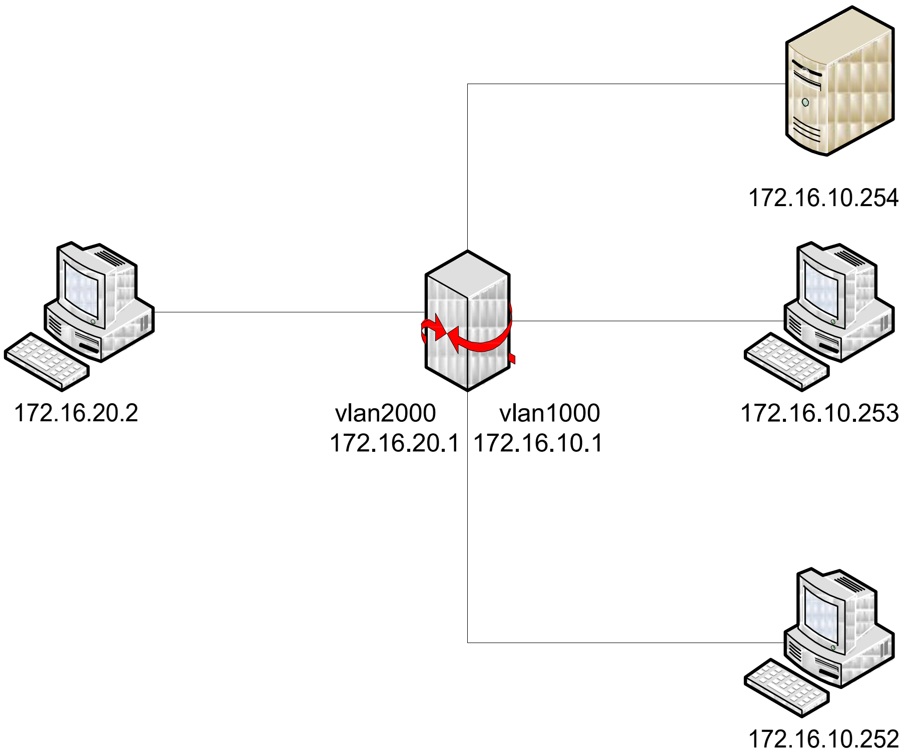
26.3 Configuration Example

Example 1

Description:

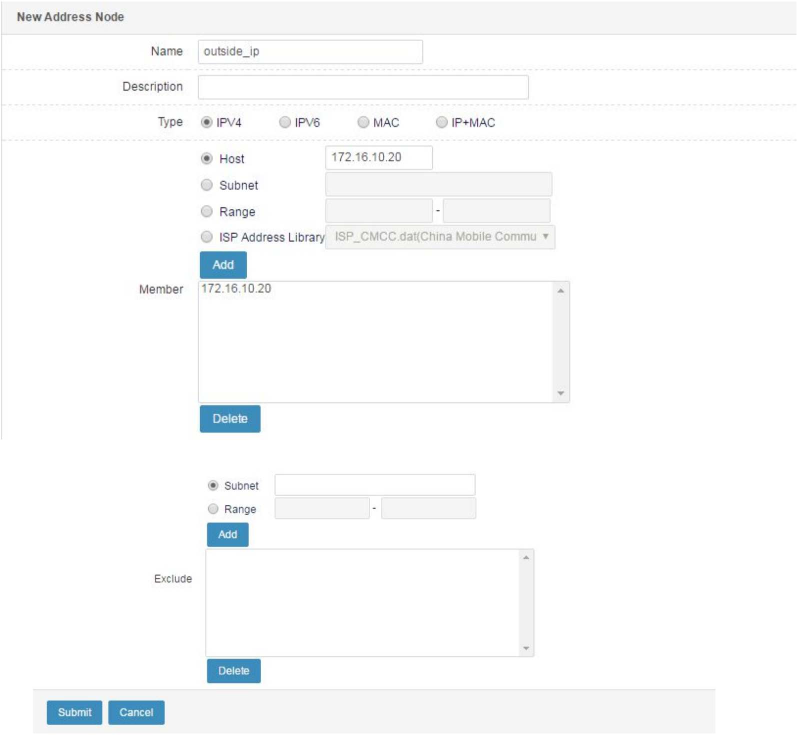
An external client wants to access an internal FTP server, which uses non-default port 2121.

Network diagram:



Procedure:

1. Choose **Object** > **Address object** > **Address node** and click **New** to create an address object.



New Address Node

Name: outside_ip

Description:

Type: ● IPV4 ○ IPV6 ○ MAC ○ IP+MAC

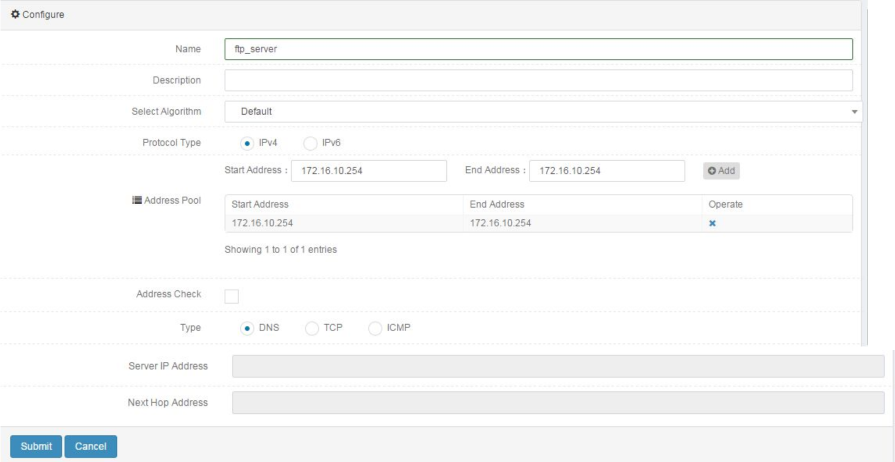
● Host 172.16.10.20
○ Subnet
○ Range -
○ ISP Address Library ISP_CMCC.dat(China Mobile Commu

Member: 172.16.10.20

● Subnet
○ Range -

Exclude:

2. Choose **Network** > **NAT** > **NAT pool** and click **New** to create a NAT pool.



Configure

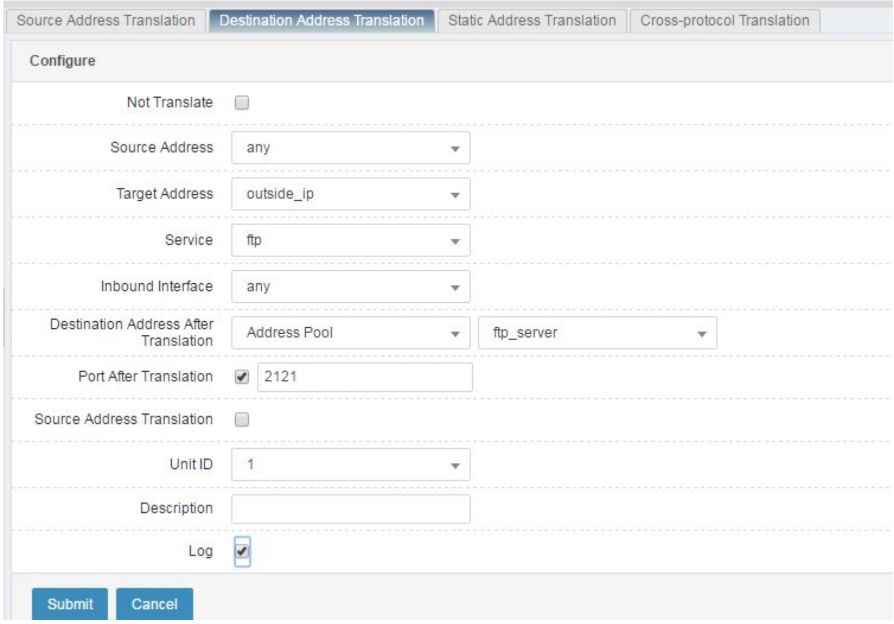
Name	ftp_server
Description	
Select Algorithm	Default
Protocol Type	● IPv4 ○ IPv6
Address Pool	Start Address : 172.16.10.254 End Address : 172.16.10.254 Add

Start Address	End Address	Operate
172.16.10.254	172.16.10.254	×

Showing 1 to 1 of 1 entries

Address Check	□
Type	● DNS ○ TCP ○ ICMP
Server IP Address	
Next Hop Address	

3. Choose **Network** > **NAT** > **NAT rule** > **DNAT** and click **New** to create a DNAT rule.

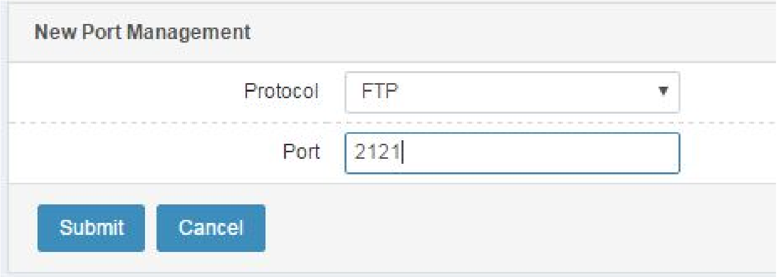


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation

Configure

Not Translate	□
Source Address	any
Target Address	outside_ip
Service	ftp
Inbound Interface	any
Destination Address After Translation	Address Pool ftp_server
Port After Translation	☑ 2121
Source Address Translation	□
Unit ID	1
Description	
Log	☑

4. Choose **Network** > **NAT** > **Port management** and click **New**. The following page appears.



New Port Management

Protocol	FTP
Port	2121

Click **Submit** after you complete the settings.

⚠ Notice

The same port can be added under different protocol types.

27 IPsec VPN

27.1 Overview

IPsec ensures the security of sensitive information transmitted on the Internet. It encrypts and authenticates IP packets at the network layer. IPsec provides optional network security services, which one(s) to use depends on the local security policy.

- Data confidentiality: The IPsec sender encrypts the data sent to the peer.
- Data integrity: The IPsec recipient authenticates the received data to ensure that the data is not tampered with during transmission.
- Data origin authentication: The IPsec recipient authenticates the data origin.
- Anti-replay: The IPsec recipient detects which replayed IP packets are dropped.

IPsec prevents packets from being listened to, tampered with, and spoofed, and allows packets to be transmitted securely in unsecure public networks. A typical application of IPsec is VPN construction. IPsec uses encapsulation security payload (ESP) or authentication header (AH) to authenticate the data origin, ensure data integrity and confidentiality, and prevent endless replay of the same packet. The Internet Security Association and Key Management Protocol (ISAKMP) is used with IPsec based on the security policy database (SPDB) to negotiate security associations (SAs) and manage SA databases dynamically.

Terms:

- AH: A security protocol used to authenticate packets.
- ESP: A security protocol used to encrypt and authenticate packets. It can work independently or with AH.
- Encryption algorithm: Used by ESP.
- Authentication algorithm: Algorithm used by AH or ESP to authenticate the peer.
- Key management: A key management solution. Internet Key Exchange (IKE) is the default protocol for automatic key exchange.

27.2 Configuration

IPsec VPN provides gateway-to-gateway and remote access security functions. It supports two encapsulation modes: tunneling and transmission. It supports two authentication modes: certificate and preshared key.

The basic process of IPsec VPN configuration is as follows:

1. Configure an IKE negotiation policy, including the peer address, authentication mode, and negotiation parameters.

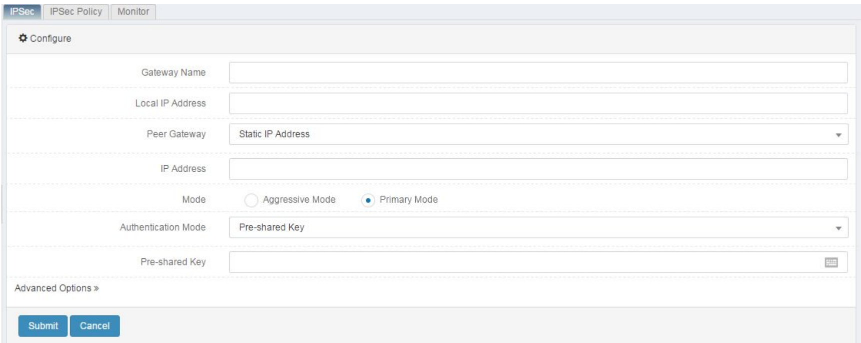
2. Configure an IPsec negotiation policy, including the IPsec encryption algorithm and encapsulation mode.

3. Configure an IPsec policy to specify the network range that requires data encryption.

27.2.1 Configuring an IKE Negotiation Policy

Procedure:

Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec** and click New .



IPSec | IPSec Policy | Monitor

Configure

Gateway Name

Local IP Address

Peer Gateway: Static IP Address

IP Address

Mode: ○ Aggressive Mode ● Primary Mode

Authentication Mode: Pre-shared Key

Pre-shared Key

Advanced Options »

Submit Cancel

1. Set **Local IP address** to the local IP address used by negotiation.

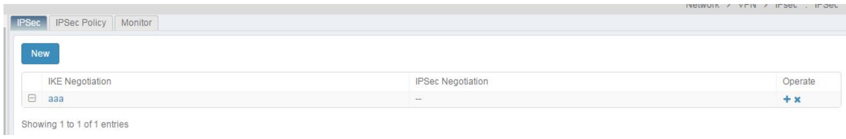
2. Set **Peer gateway**. Select **Static IP address** if the peer address is fixed. Select **Dynamic address** if the peer address is uncertain.

3. Set **Authentication mode**. The options are **Preshared key** and **Certificate**. If you select **Certificate**, ensure that a certificate has been imported. If you select **Preshared key**, the key must be consistent with that at the peer end.

27.2.2 Configuring an IPsec Negotiation Policy

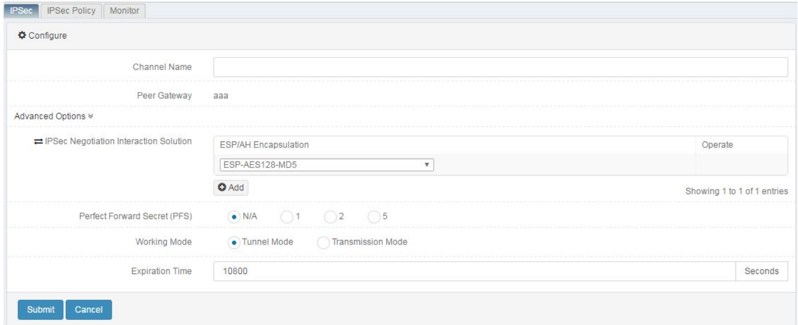
Procedure:

Click + in the **Action** column to create an IPsec negotiation policy.



IKE Negotiation	IPSec Negotiation	Operate
⊟ aaa	--	+ ×

Showing 1 to 1 of 1 entries



Channel Name

Peer Gateway aaa

Advanced Options

IPSec Negotiation Interaction Solution

ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

Add

Showing 1 to 1 of 1 entries

Perfect Forward Secret (PFS) ● N/A ○ 1 ○ 2 ○ 5

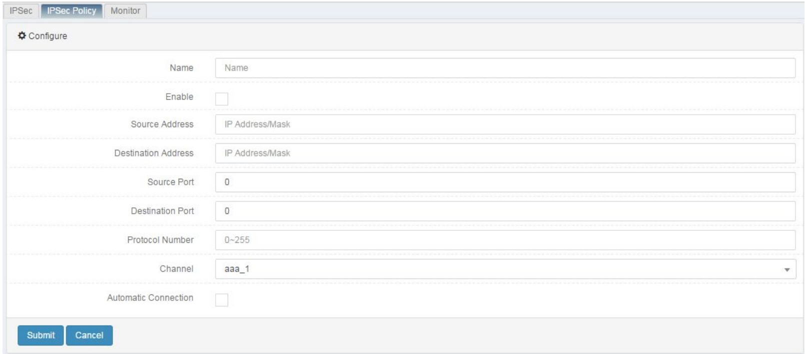
Working Mode ● Tunnel Mode ○ Transmission Mode

Expiration Time 10800 Seconds

1. Set **Channel name**.
2. Set **IPsec negotiation interaction scheme**. You can select the ESP or AH algorithm according to the one used at the peer one. If NAT traversal is enabled, do not use AH.
3. Set **Operation mode**. Select **Tunneling** for IPsec transmission between networks. Select **Transmission** for L2TP remote access. The value must be consistent with that at the peer end.

27.2.3 Configuring an IPsec Policy

Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec Policy** and click **New**.



Name: Name

Enable: □

Source Address: IP Address/Mask

Destination Address: IP Address/Mask

Source Port: 0

Destination Port: 0

Protocol Number: 0~255

Channel: aaa_1

Automatic Connection: □

1. Set **Source address**, **Source port**, **Destination address**, **Destination port**, and **Protocol number**. **Source address** indicates the local private network to be protected. **Destination address** indicates the peer private network to be protected.
2. Set **Channel** to the VPN tunnel that is configured for the IPsec negotiation policy.

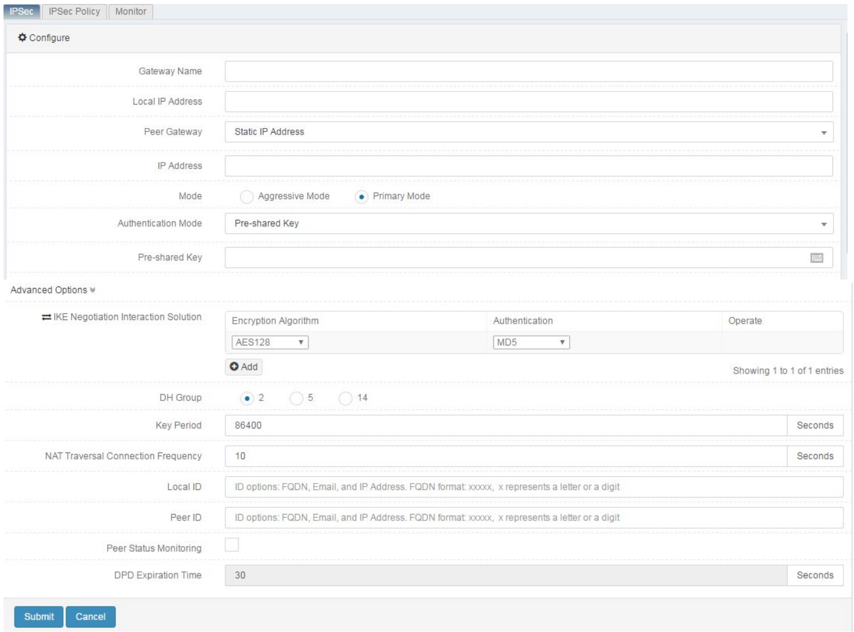
27.3 IPsec VPN Parameter Configuration

27.3.1 IKE Negotiation Parameters

An IKE policy defines a set of IKE negotiation parameters. The local and peer VPN devices establish ISAKMP SA (IPsec phase 1) through IKE negotiation.

Procedure:

Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec** and click New .



IPSec | IPSec Policy | Monitor

Configure

Gateway Name	
Local IP Address	
Peer Gateway	Static IP Address
IP Address	
Mode	○ Aggressive Mode ● Primary Mode
Authentication Mode	Pre-shared Key
Pre-shared Key	

Advanced Options

IKE Negotiation Interaction Solution

Encryption Algorithm	Authentication	Operate
AES128	MD5	

Add

Showing 1 to 1 of 1 entries

DH Group	● 2 ○ 5 ○ 14
Key Period	86400 Seconds
NAT Traversal Connection Frequency	10 Seconds
Local ID	ID options: FQDN, Email, and IP Address. FQDN format: xxxxx, x represents a letter or a digit
Peer ID	ID options: FQDN, Email, and IP Address. FQDN format: xxxxx, x represents a letter or a digit
Peer Status Monitoring	□
DPD Expiration Time	30 Seconds

Gateway name: Name of IKE negotiation.

Local IP address: Local address used to receive or initiate negotiation.

Peer gateway:

- **Static IP address**: If you specify the peer address as a static IP address, enter the peer IP address.
- **Dynamic IP address**: Specify the peer address as a dynamic IP address.

Mode: IKE negotiation mode. The options are **Aggressive** and **Main**.

Authentication mode: Authentication mode adopted by negotiation. The options are **Preshared key** and **Certificate**.

Preshared key: If you select this option, enter the key value.

Certificate: If you select this option, select a local certificate.

IKE negotiation interaction scheme: Includes the encryption algorithm and authentication algorithm adopted by negotiation.

DH group: Group value used by DH exchange during negotiation.

Key period: SA TTL in phase 1.

NAT traversal connection frequency: TTL of NAT traversal.

(Optional) **Local ID**: Applicable to static NAT in NAT traversal.

(Optional) **Peer ID**: Applicable to static NAT in NAT traversal.

Peer status detection: Check this box to enable dead peer detection (DPD).

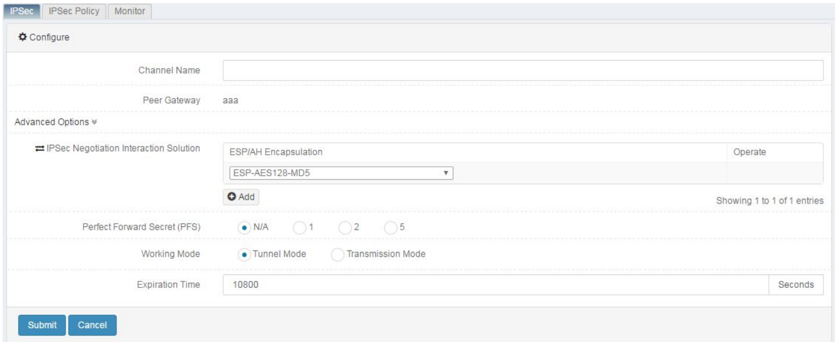
DPD traversal connection frequency: DPD interval.

27.3.2 IPsec Negotiation Parameters

The IPsec negotiation parameters are used to establish IPsec phase 2 SA after the local and peer VPN devices establish ISAKMP SA through IKE negotiation.

Procedure:

Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec**, and click + next to an existing IKE negotiation to create an IPsec negotiation.



Channel Name

Peer Gateway aaa

IPSec Negotiation Interaction Solution

ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

Showing 1 to 1 of 1 entries

Perfect Forward Secret (PFS) ● N/A ○ 1 ○ 2 ○ 5

Working Mode ● Tunnel Mode ○ Transmission Mode

Expiration Time 10800 Seconds

Channel name: Name of the new IPsec negotiation.

Peer gateway: Name of the gateway in IKE negotiation.

IPsec negotiation interaction scheme: Encapsulation mode and algorithm adopted by IPsec negotiation.

Perfect forward secrecy (PFS): Check this box adopt DH exchange during IPsec negotiation.

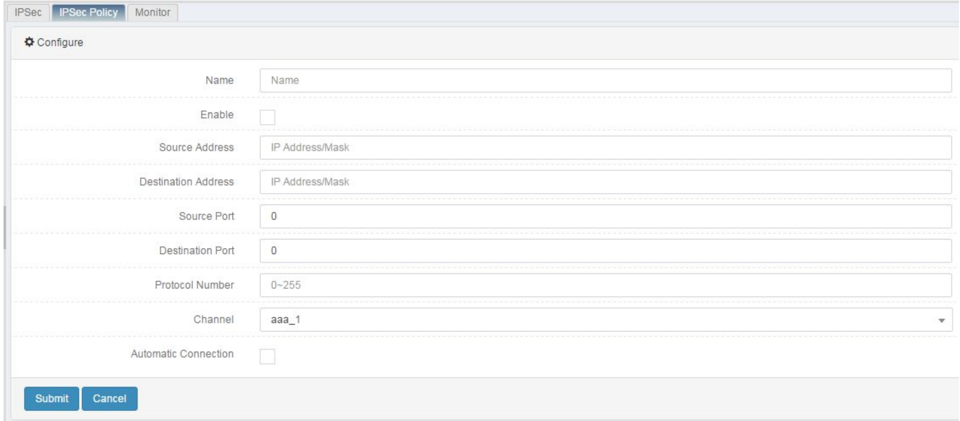
Operation mode: Operation mode during encapsulation of IPsec negotiation.

Timeout: IPsec SA TTL, in seconds or bytes.

27.3.3 IPsec Policy

An IPsec policy defines a set of parameters such as the protected subnet of IPsec negotiation. **Procedure:**

Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec policy**, and click New next to an existing IKE negotiation to create an IPsec policy.



Name	Name
Enable	□
Source Address	IP Address/Mask
Destination Address	IP Address/Mask
Source Port	0
Destination Port	0
Protocol Number	0~255
Channel	aaa_1
Automatic Connection	□

Name: Name of the new IPsec policy.

Enable: Check this box to enable the IPsec policy.

Source address: Address of the protected local subnet.

Destination address: Address of the protected peer subnet.

Source port: Protected source port with local outgoing traffic.

Destination port: Protected destination port with local outgoing traffic.

Protocol number: Protected destination protocol with local outgoing traffic.

Channel: Phase 2 of traffic protection.

Auto-connection: If you select this option, a connection is automatically initiated.

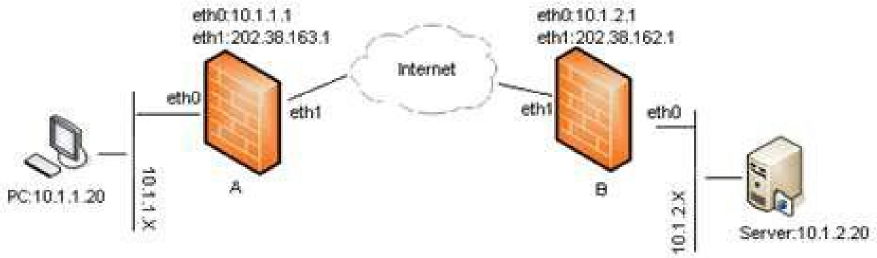
27.4 Configuration Examples

27.4.1 Example 1: Configuring Basic IPsec Networking

Description:

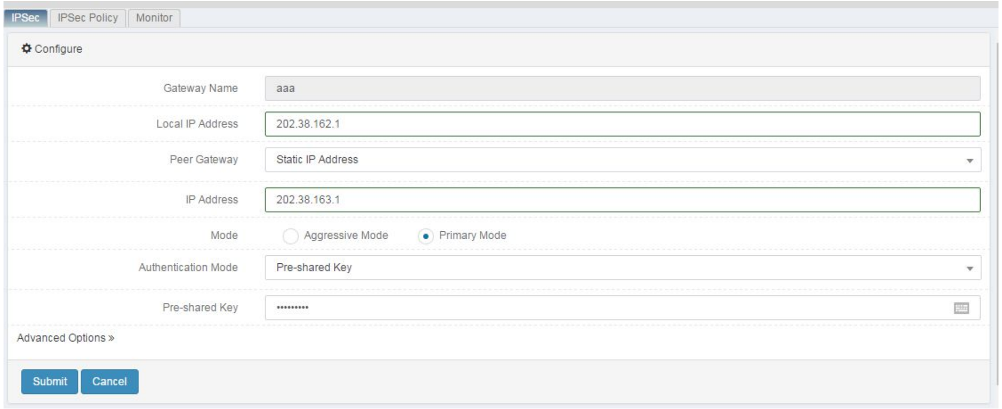
The following figure shows the network environment. Traffic from the PC to server is transmitted over the Internet to which two firewalls are connected. Establish an IPsec VPN tunnel between FW A and FW B to ensure communication security.

Figure 27-1 Network diagram:



Configuration on FW B:

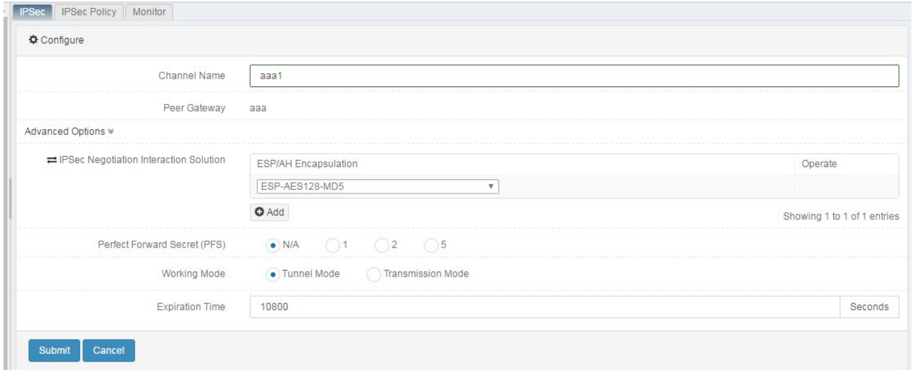
7. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec** and click **New**. On the displayed page, set the parameters.



Gateway Name	aaa
Local IP Address	202.38.162.1
Peer Gateway	Static IP Address
IP Address	202.38.163.1
Mode	○ Aggressive Mode ● Primary Mode
Authentication Mode	Pre-shared Key
Pre-shared Key	••••••••••

Click **Submit**.

8. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec**, and click + to create an IPsec negotiation. On the displayed page, set the parameters.



Channel Name: aaa1

Peer Gateway: aaa

Advanced Options

IPSec Negotiation Interaction Solution:

ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

Add

Showing 1 to 1 of 1 entries

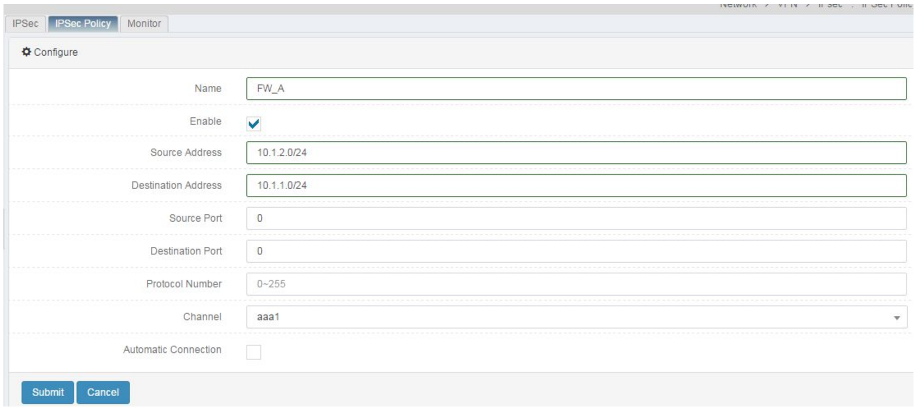
Perfect Forward Secret (PFS): ● N/A ○ 1 ○ 2 ○ 5

Working Mode: ● Tunnel Mode ○ Transmission Mode

Expiration Time: 10800 Seconds

Click **Submit**.

9. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec policy** and click **New**. On the displayed page, set the parameters.



Name: FW_A

Enable: ☑

Source Address: 10.1.2.0/24

Destination Address: 10.1.1.0/24

Source Port: 0

Destination Port: 0

Protocol Number: 0~255

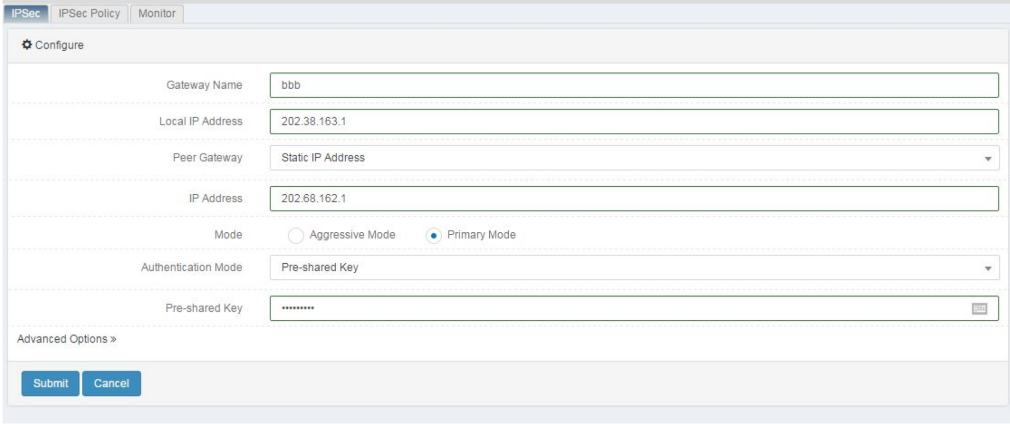
Channel: aaa1

Automatic Connection: □

Click **Submit**.

Configuration on FW A:

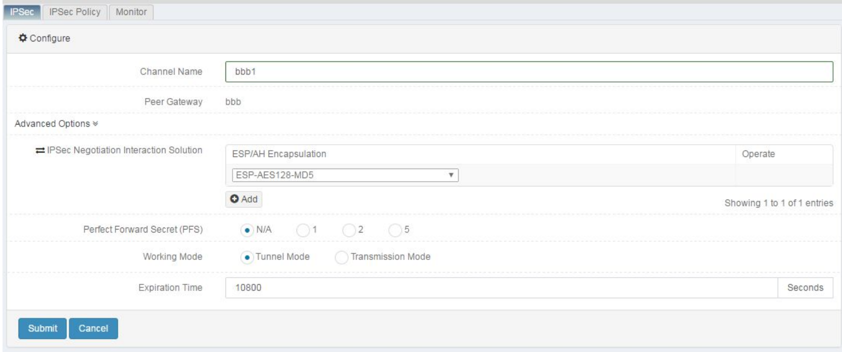
10. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec** and click **New**. On the displayed page, set the parameters.



Gateway Name	bbb
Local IP Address	202.38.163.1
Peer Gateway	Static IP Address
IP Address	202.68.162.1
Mode	○ Aggressive Mode ● Primary Mode
Authentication Mode	Pre-shared Key
Pre-shared Key	•••••••••

Click **Submit**.

11. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec**, and click + to create an IPsec negotiation. On the displayed page, set the parameters



Channel Name	bbb1
Peer Gateway	bbb

IPSec Negotiation Interaction Solution

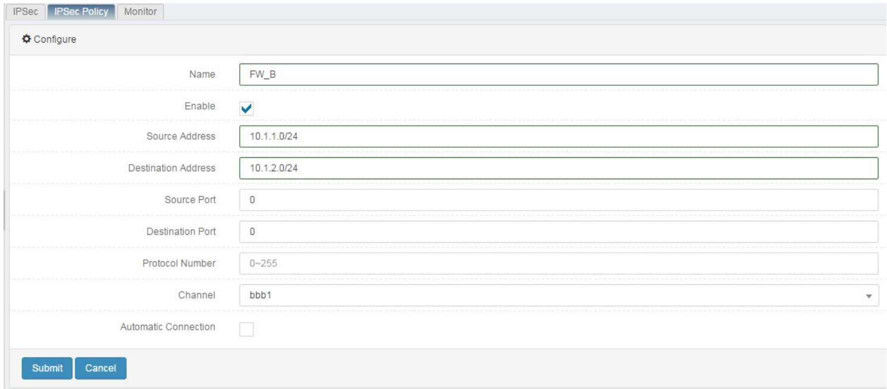
ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

Showing 1 to 1 of 1 entries

Perfect Forward Secret (PFS)	● N/A ○ 1 ○ 2 ○ 5
Working Mode	● Tunnel Mode ○ Transmission Mode
Expiration Time	10800 Seconds

Click **Submit**.

12. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec policy** and click **New**. On the displayed page, set the parameters.



Name	FW_B
Enable	☑
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Source Port	0
Destination Port	0
Protocol Number	0~255
Channel	bbb1
Automatic Connection	□

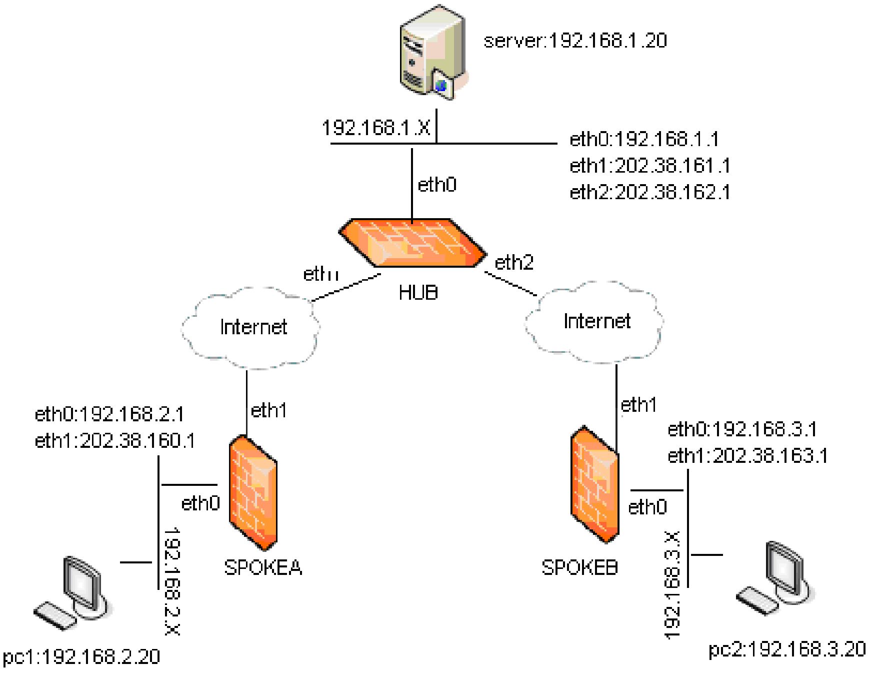
Click **Submit**.

27.4.2 Example 2: Configuring IPsec HUB_SPOKE

Description:

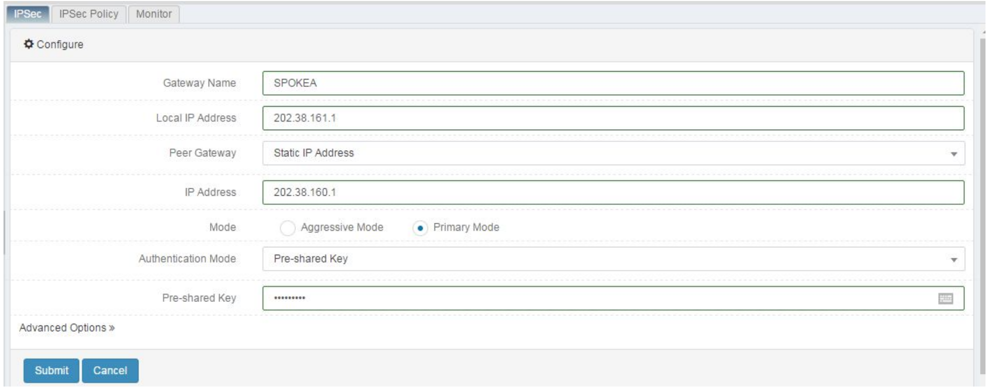
The following figure shows the network environment. No connection exists between Spoke A and Spoke B. Perform configuration to forward the access traffic from Spoke A to Spoke B through a hub.

Figure 27-2 Network diagram:



Hub configuration:

1. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec** and click **New**. On the displayed page, set the parameters.



Gateway Name: SPOKEA

Local IP Address: 202.38.161.1

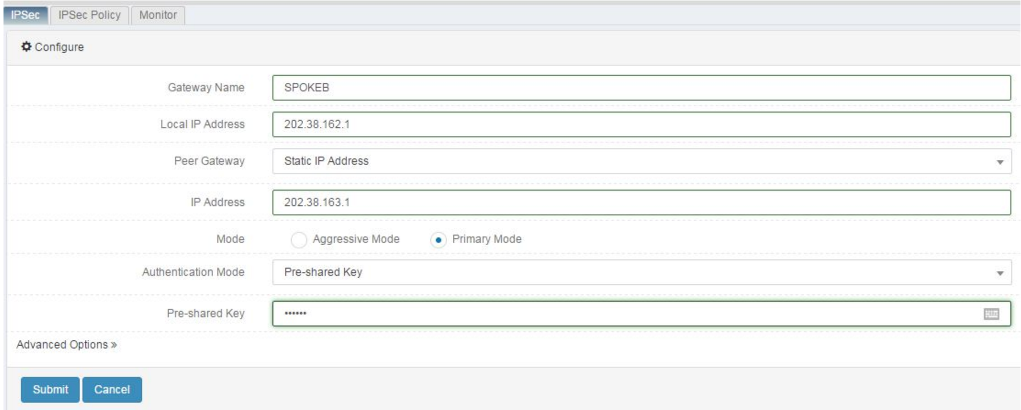
Peer Gateway: Static IP Address

IP Address: 202.38.160.1

Mode: ○ Aggressive Mode ● Primary Mode

Authentication Mode: Pre-shared Key

Pre-shared Key: •••••••••



Gateway Name: SPOKEB

Local IP Address: 202.38.162.1

Peer Gateway: Static IP Address

IP Address: 202.38.163.1

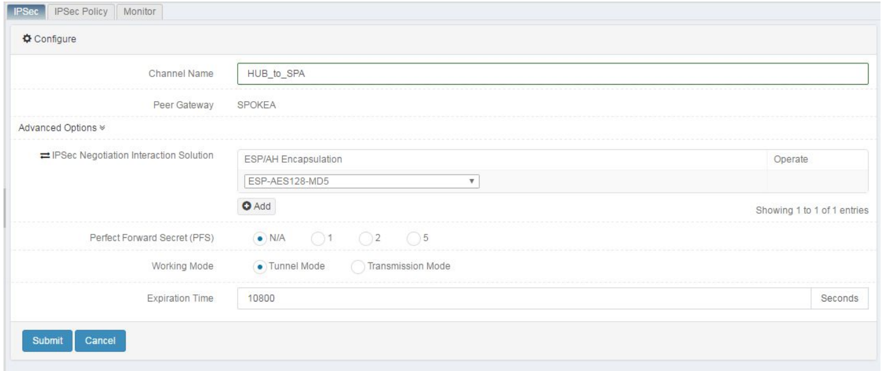
Mode: ○ Aggressive Mode ● Primary Mode

Authentication Mode: Pre-shared Key

Pre-shared Key: ••••••

Click **Submit**.

2. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec**, and click + to create an IPsec negotiation. On the displayed page, set the parameters.



Channel Name: HUB_to_SPA

Peer Gateway: SPOKEA

Advanced Options

IPSec Negotiation Interaction Solution

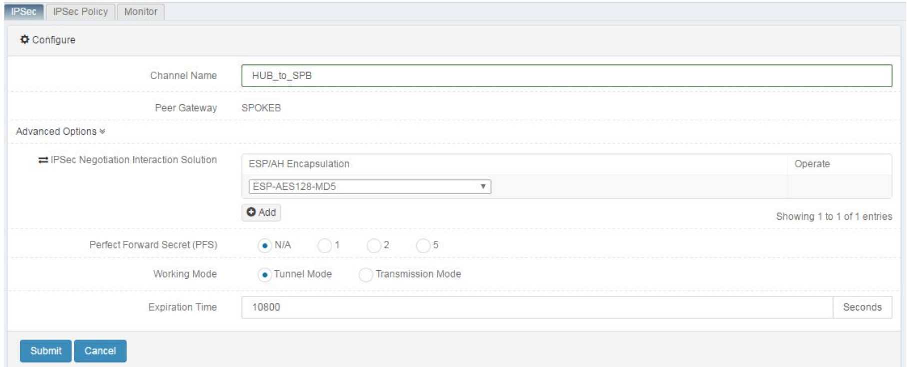
ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

Add — Showing 1 to 1 of 1 entries

Perfect Forward Secret (PFS): ● N/A ○ 1 ○ 2 ○ 5

Working Mode: ● Tunnel Mode ○ Transmission Mode

Expiration Time: 10800 Seconds



Channel Name: HUB_to_SPB

Peer Gateway: SPOKEB

Advanced Options

IPSec Negotiation Interaction Solution

ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

Add — Showing 1 to 1 of 1 entries

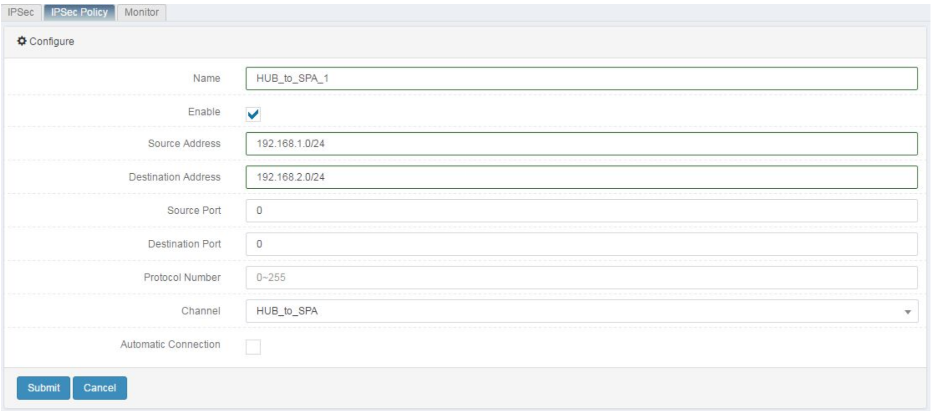
Perfect Forward Secret (PFS): ● N/A ○ 1 ○ 2 ○ 5

Working Mode: ● Tunnel Mode ○ Transmission Mode

Expiration Time: 10800 Seconds

Click **Submit**.

3. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec policy** and click **New**. On the displayed page, set the parameters.



Name: HUB_to_SPA_1

Enable: ☑

Source Address: 192.168.1.0/24

Destination Address: 192.168.2.0/24

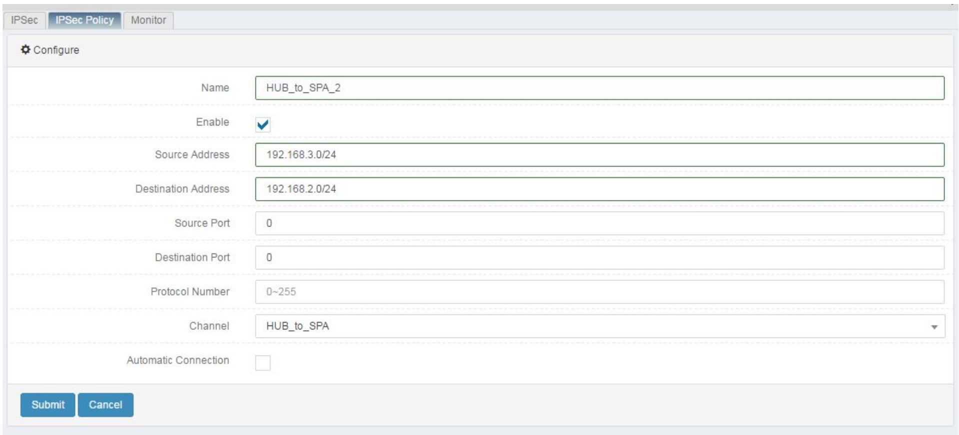
Source Port: 0

Destination Port: 0

Protocol Number: 0~255

Channel: HUB_to_SPA

Automatic Connection: □

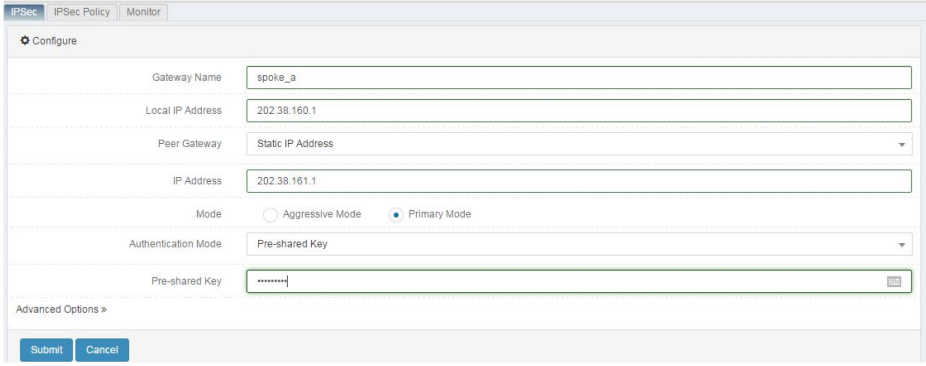


Name	HUB_to_SPA_2
Enable	☑
Source Address	192.168.3.0/24
Destination Address	192.168.2.0/24
Source Port	0
Destination Port	0
Protocol Number	0~255
Channel	HUB_to_SPA
Automatic Connection	□

Click **Submit**.

Configuration on Spoke A:

4. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec** and click **New**. On the displayed page, set the parameters.

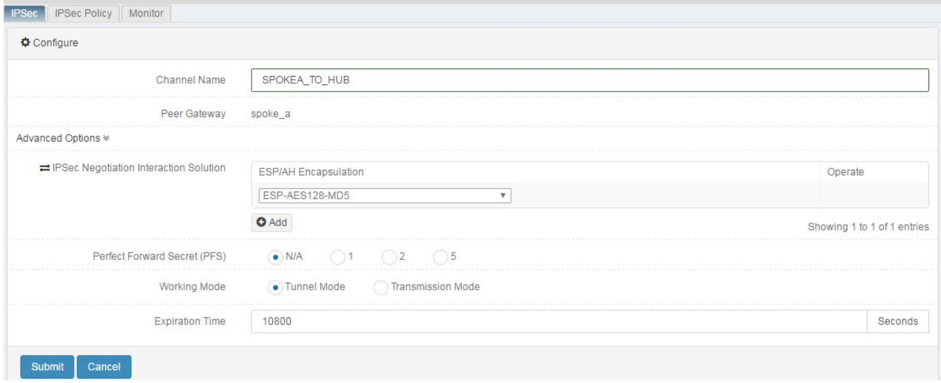


Gateway Name	spoke_a
Local IP Address	202.38.160.1
Peer Gateway	Static IP Address
IP Address	202.38.161.1
Mode	○ Aggressive Mode ● Primary Mode
Authentication Mode	Pre-shared Key
Pre-shared Key	•••••••••

Click **Submit**.

5. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec**, and click + to create an

IPsec negotiation. On the displayed page, set the parameters.



Channel Name: SPOKEA_TO_HUB

Peer Gateway: spoke_a

Advanced Options

IPSec Negotiation Interaction Solution:

ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

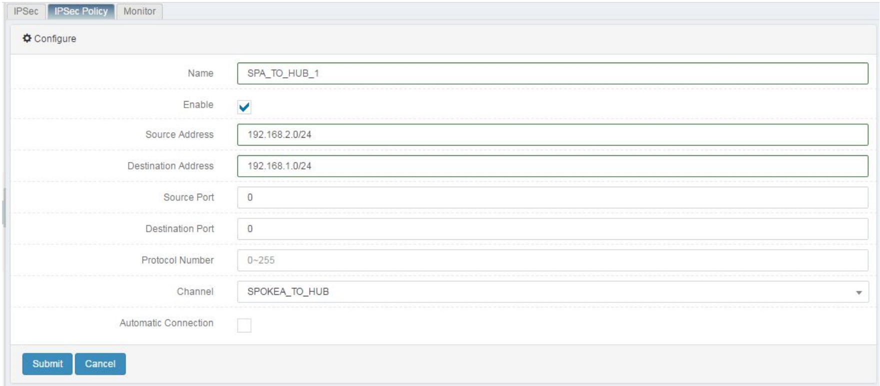
Perfect Forward Secret (PFS): ● N/A ○ 1 ○ 2 ○ 5

Working Mode: ● Tunnel Mode ○ Transmission Mode

Expiration Time: 10800 Seconds

Click **Submit**.

6. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec policy** and click **New**. On the displayed page, set the parameters.



Name: SPA_TO_HUB_1

Enable: ☑

Source Address: 192.168.2.0/24

Destination Address: 192.168.1.0/24

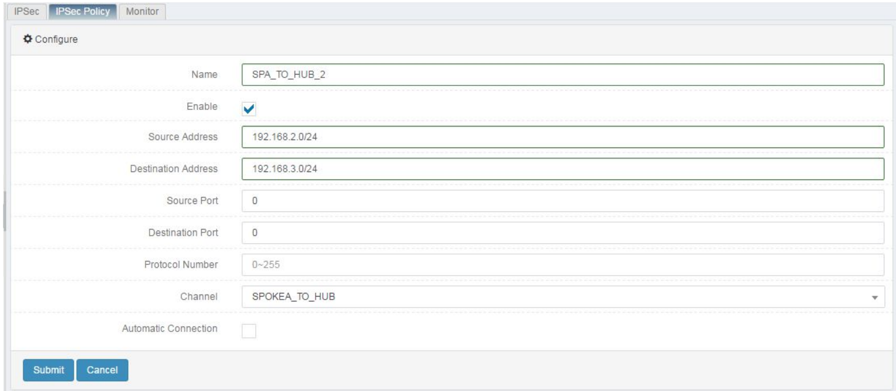
Source Port: 0

Destination Port: 0

Protocol Number: 0~255

Channel: SPOKEA_TO_HUB

Automatic Connection: □



Name: SPA_TO_HUB_2

Enable: ☑

Source Address: 192.168.2.0/24

Destination Address: 192.168.3.0/24

Source Port: 0

Destination Port: 0

Protocol Number: 0~255

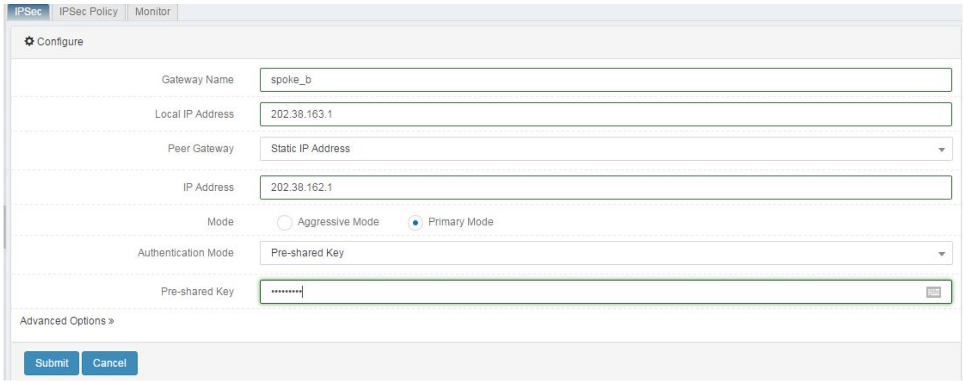
Channel: SPOKEA_TO_HUB

Automatic Connection: □

Click **Submit**.

Configuration on Spoke B:

7. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec** and click **New**. On the displayed page, set the parameters.



Gateway Name: spoke_b

Local IP Address: 202.38.163.1

Peer Gateway: Static IP Address

IP Address: 202.38.162.1

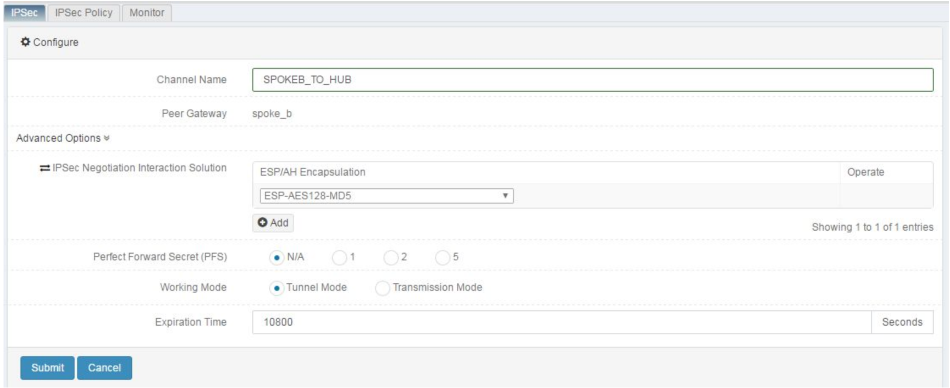
Mode: ○ Aggressive Mode ● Primary Mode

Authentication Mode: Pre-shared Key

Pre-shared Key: •••••••••

Click **Submit**.

8. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec**, and click + to create an IPsec negotiation. On the displayed page, set the parameters.



Channel Name: SPOKEB_TO_HUB

Peer Gateway: spoke_b

IPSec Negotiation Interaction Solution:

ESP/AH Encapsulation	Operate
ESP-AES128-MD5	

Showing 1 to 1 of 1 entries

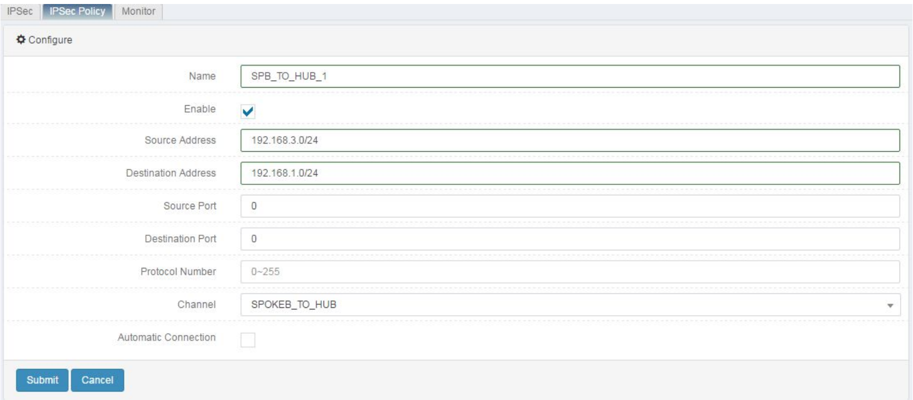
Perfect Forward Secret (PFS): ● N/A ○ 1 ○ 2 ○ 5

Working Mode: ● Tunnel Mode ○ Transmission Mode

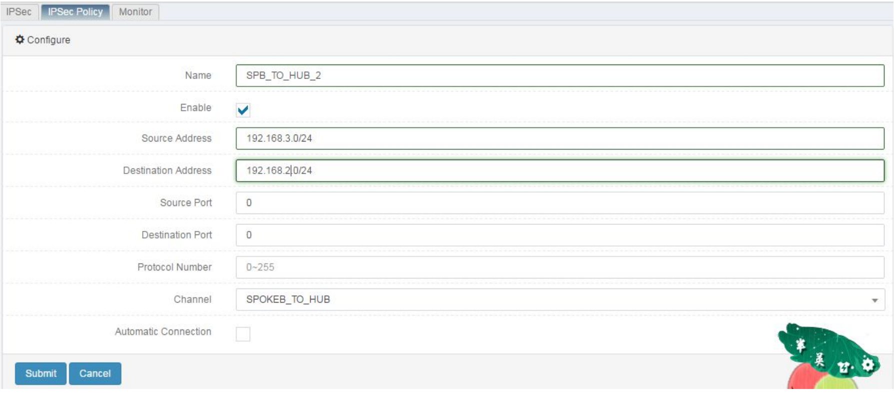
Expiration Time: 10800 Seconds

Click **Submit**.

9. Choose **Network** > **VPN** > **IPsec-VPN** > **IPsec policy** and click **New**. On the displayed page, set the parameters.



Name	SPB_TO_HUB_1
Enable	☑
Source Address	192.168.3.0/24
Destination Address	192.168.1.0/24
Source Port	0
Destination Port	0
Protocol Number	0~255
Channel	SPOKEB_TO_HUB
Automatic Connection	□



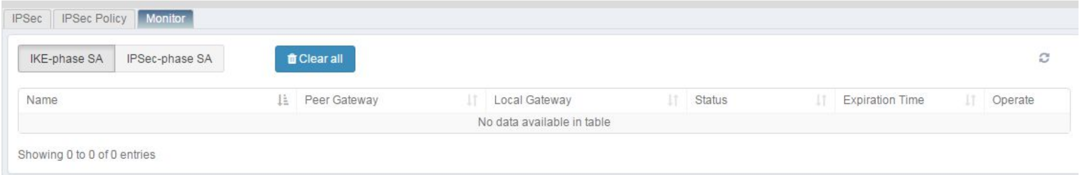
Name	SPB_TO_HUB_2
Enable	☑
Source Address	192.168.3.0/24
Destination Address	192.168.2.0/24
Source Port	0
Destination Port	0
Protocol Number	0~255
Channel	SPOKEB_TO_HUB
Automatic Connection	□

Click **Submit**.

27.5 Monitoring and Maintenance

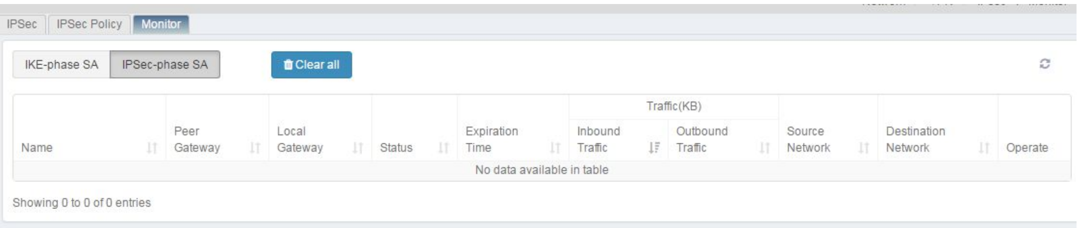
27.5.1 Checking SA Establishment

Choose **Network** > **VPN** > **IPsec-VPN** > **Monitor**. The displayed page shows SA information.



Name	Peer Gateway	Local Gateway	Status	Expiration Time	Operate
No data available in table					

Showing 0 to 0 of 0 entries



					Traffic(KB)				
Name	Peer Gateway	Local Gateway	Status	Expiration Time	Inbound Traffic	Outbound Traffic	Source Network	Destination Network	Operate
No data available in table									

Showing 0 to 0 of 0 entries

27.5.2 Deleting an SA

Click ✖ to delete the SAs of two negotiations.

Click ℹ to show details about the SA in the IPsec phase.

27.6 Troubleshooting

27.6.1 Unable to Establish a Tunnel

Symptom	An SA cannot be established due to failed negotiation. The **show crypto ipsec sa** command output shows no SA information.
Analysis	1. Check whether the security policies at the local and peer ends are consistent. 2. Check whether the IKE negotiation policies and authentication keys at the local and peer ends are consistent. 3. Check whether the IPsec negotiation policies at the local and peer ends are consistent.
Solution	1. If the security policies are inconsistent, modify them. 2. If the IKE or IPsec negotiation policies are inconsistent, modify them.

28 L2TP

28.1 Overview

PPP defines an encapsulation mechanism to transmit packets of different protocol types over Layer-2 point-to-point connection. Typically, a user can establish a Layer-2 connection to a network access server (NAS) by means of ISDN, ADSL dial-up, or other access technique, and initiate a PPP session over the connection. The Layer-2 terminal node and the PPP session's terminal node are both located on the NAS.

The Layer 2 Tunneling Protocol (L2TP) extends the PPP model by extending a PPP session's terminal node to a different device (which is connected to a packet switched network) through a Layer-2 tunnel. L2TP removes the Layer-2 terminal node limitation on PPP sessions and extends the PPP application scope.

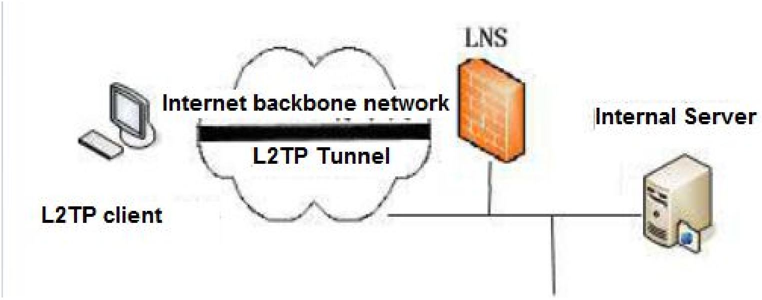
L2TP provides the L2TP access concentrator (LAC) and L2TP network server (LNS) features.

- LAC is an endpoint of an L2TP tunnel and also an LNS peer. A LAC forwards PPP packets between an LNS and a remote system, and maintains the tunnel and session between LAC and LNS.
- LNS is an endpoint of an L2TP tunnel and also a LAC peer. An LNS maintains the PPP connection to a remote system and allows the remote system to access the intranet.

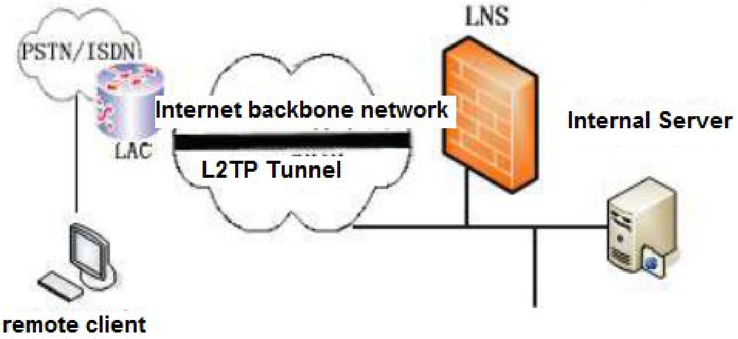
An L2TP tunnel allows a remote dial-up user to connect to a VPN gateway. Dial-up VPN is also called virtual private dial network (VPDN). The VPN gateway works as an LNS. If the dial-up user supports L2TP, the user can directly connect to the LNS in voluntary tunneling mode. If the user does not support L2TP, the user can connect to the LNS in compulsory tunneling mode by using the LAC feature provided by the local ISP.

See the following topologies.

Direct connection from an L2TP client to an LNS

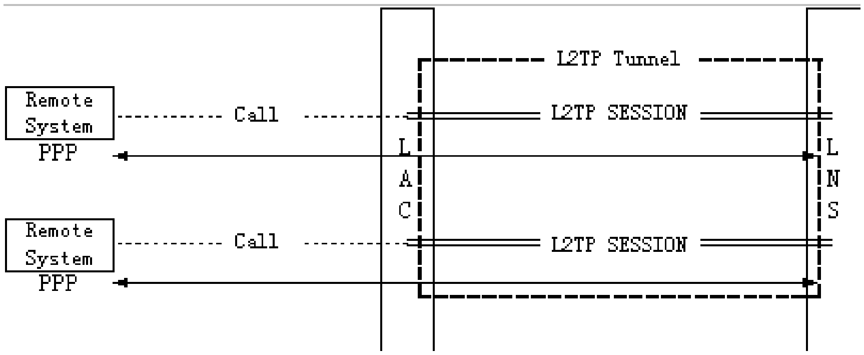


Remote connection from a dial-up user to an LNS through a LAC



Two types of connection exist between LNS and LAC: tunnel and session. A tunnel defines an LNS-LAC pair, whereas a session is multiplexed on the tunnel to represent every PPP session carried by the tunnel.

Transparent transmission of PPP frames through a tunnel



L2TP connection maintenance and PPP data transmission are implemented by L2TP packet exchange. L2TP packets are encapsulated in UDP packets to be carried over TCP/IP.

L2TP packets are classified into control packets and data packets. Control packets are used to establish and maintain tunnels and sessions. Control packets are transmitted reliably using various techniques such as packet number confirmation, sliding window, retransmission after timeout, and tunnel keep-alive detection. Data packets carry users' PPP session packets. Reliable transmission of data packets is ensured by upper-layer protocols based onupper-layer applications.

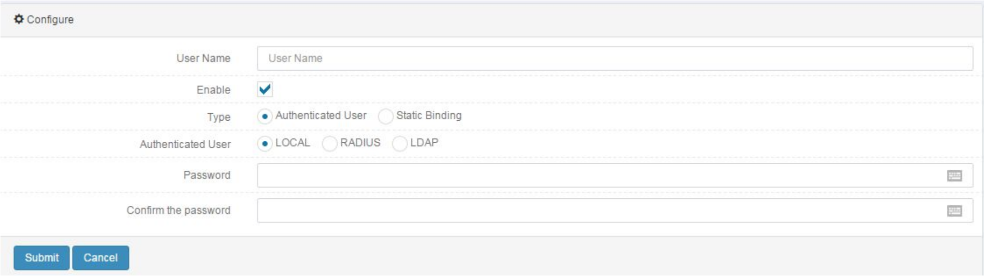
28.2 Configuration

By default, RAVEN5000 firewalls have no L2TP configurations. To configure L2TP, you must configure an address pool, an authentication user group, and other settings.

28.2.1 Configuring an Authentication User

User authentication is performed when a client dials up to a network. The configuration items include the user name and password.

Choose **Object** > **User object** > **User** and click **New**.



Configure

User Name	User Name
Enable	☑
Type	● Authenticated User ○ Static Binding
Authenticated User	● LOCAL ○ RADIUS ○ LDAP
Password	
Confirm the password	

Parameter description:

User name: Name of an account, containing a maximum of 63 characters.

Enable: Check this box to enable the account.

Type: The options are **Authentication user** and **Static binding**.

Authentication user: Type of the authentication user.

Password: Password of the account. No password needs to be set for RADIUS authentication.

Confirm password: Enter the password again.

Procedure:

1. Enter an account name in **User name**.
2. Check the **Enable** box.
3. Select **Authentication user** for **Type**.

4. If authentication is not RADIUS, enter a password twice.

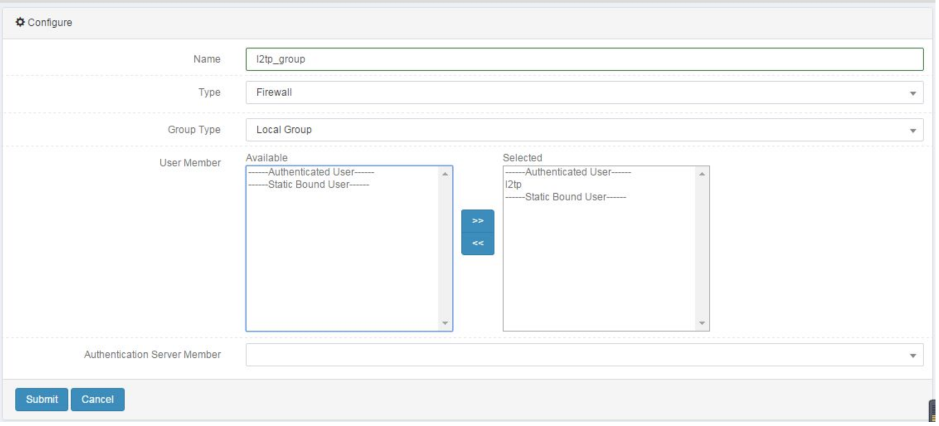
5. If authentication is RADIUS, select existing RADIUS configuration.

6. Click **Submit**.

28.2.2 Configuring a User Group

A user group is required for configuring an L2TP template. The dial-up account of a client must be one included in a user group.

Choose **Object** > **User object** > **User group** and click **New**.



Configure

Name: l2tp_group

Type: Firewall

Group Type: Local Group

User Member:

Available:
------Authenticated User------
------Static Bound User------

Selected:
------Authenticated User------
l2tp
------Static Bound User------

Authentication Server Member:

Name: Name of a user group.

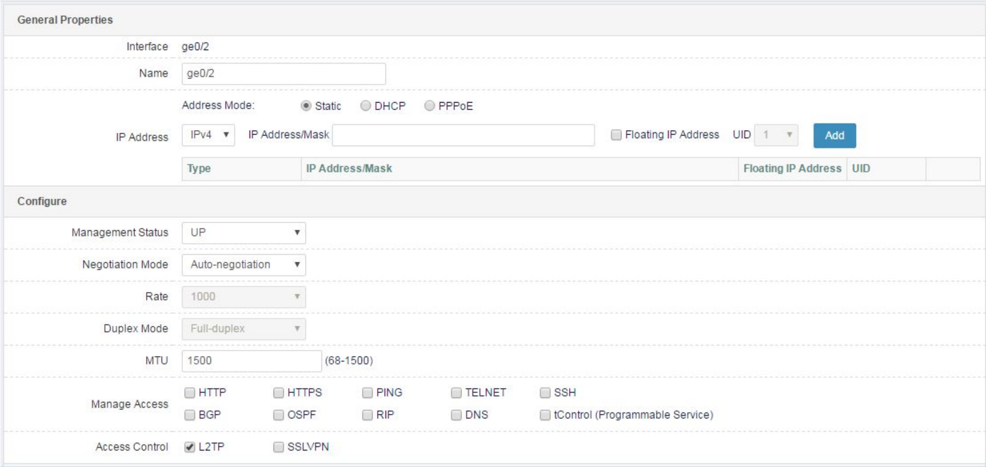
User members: Authentication users to be added to the user group.

Procedure:

1. Enter a user group name.
2. Select available accounts and click >> to add them to the user group.
3. Click **Submit**.

28.2.3 Configuring Interface Access Control

Choose **Network** > **Interface** > **Physical interface**. Click an interface to modify its settings.



General Properties

Interface ge0/2

Name ge0/2

IP Address: Address Mode: ● Static ○ DHCP ○ PPPoE

IPv4 ▾ IP Address/Mask □ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID	

Configure

Management Status UP ▾

Negotiation Mode Auto-negotiation ▾

Rate 1000 ▾

Duplex Mode Full-duplex ▾

MTU 1500 (68-1500)

Manage Access □ HTTP □ HTTPS □ PING □ TELNET □ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)

Access Control ☑ L2TP □ SSLVPN

Parameter description:

Interface: Name of the physical interface.

Name: Alias of the physical interface.

Management status: The options are **UP** and **DOWN**, which indicate enabling and disabling the physical interface.

Negotiation mode: The options are **Autonegotiation** and **Non-autonegotiation**.

Rate: Negotiated rate of the physical interface, in Mbps. The options are **1000**, **100**, and **10**.

Duplex mode: A physical interface may be full-duplex or half-duplex.

MTU: MTU of the physical interface. The value ranges from 68 to 1500.

Management access: Type of service accessible from the interface address.

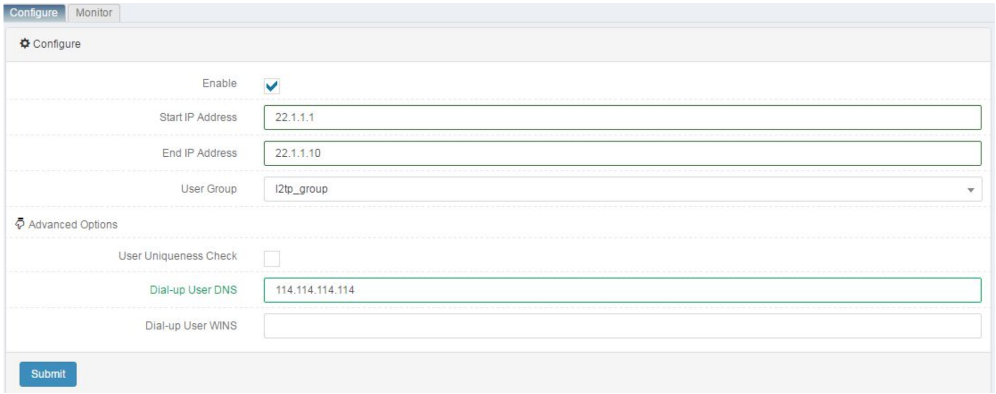
Access control: Access mode of the interface in the network.

Procedure:

1. Select **Static** for **Address mode** and set **IP address/Mask** correctly.
2. Set **Management access**.
3. Select **L2TP** for **Access control**.
4. Click **Submit**.

28.2.4 Configuring L2TP

Choose **Network** > **VPN** > **L2TP** > **Configuration**.



Enable ☑
Start IP Address 22.1.1.1
End IP Address 22.1.1.10
User Group l2tp_group
Advanced Options
User Uniqueness Check □
Dial-up User DNS 114.114.114.114
Dial-up User WINS

Parameter description:

Enable: Check this box to enable L2TP, or uncheck it to disable L2TP.

Start IP address: Start IP address used by address allocation.

End IP address: End IP address used by address allocation.

User group: User group used to authenticate the dial-up client.

Advanced options: **Dial-up user DNS** and **Dial-up user WINS** are optional and used to set the DNS and WINS addresses of the dial-up connection established by the user. **User uniqueness check** is optional and used to determine whether the same account can be logged in to by multiple users during the same period.

Procedure:

1. Check the **Enable** box.
2. Set **Start IP address**.
3. Set **End IP address**.
4. Select a user group.
5. Click **Submit**.

28.3 Configuration Example

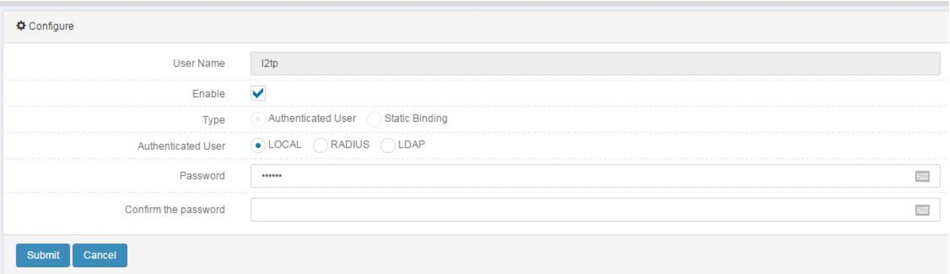
28.3.1 Enabling L2TP on Interface ge0/0

Description:

Configure L2TP on physical interface ge0/0 to allow clients to perform L2TP dial-up.

Procedure:

1. Choose **Object** > **User object** > **User** and click **New**. The following page appears.



Configure

User Name: l2tp

Enable: ☑

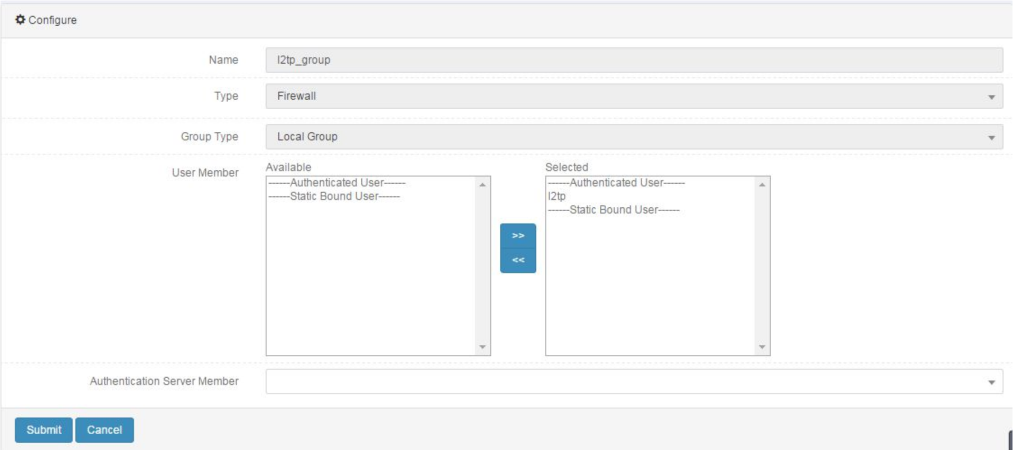
Type: ○ Authenticated User ○ Static Binding

Authenticated User: ● LOCAL ○ RADIUS ○ LDAP

Password: ••••••

Confirm the password:

2. Set parameters.
3. Click **Submit**.
4. Choose **Object** > **User object** > **User group** and click **New**. The following page appears.



Configure

Name: l2tp_group

Type: Firewall

Group Type: Local Group

User Member:

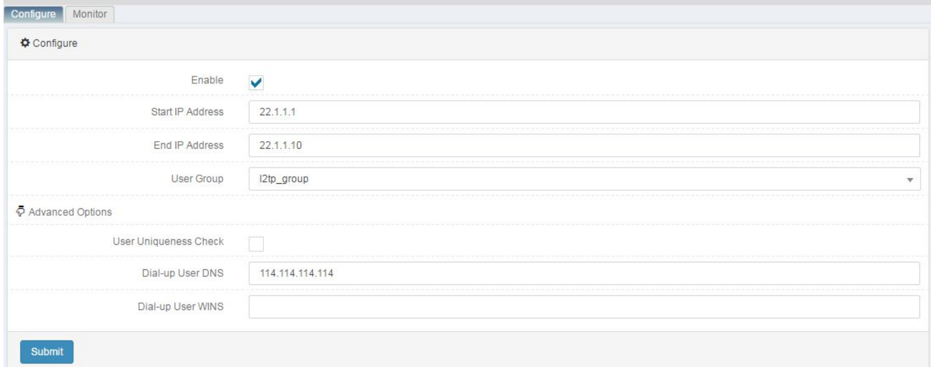
Available:
------Authenticated User------
------Static Bound User------

Selected:
------Authenticated User------
l2tp
------Static Bound User------

Authentication Server Member:

5. Set parameters.
6. Click **Submit**.

7. Choose **Network** > **VPN** > **L2TP** > **Configuration**. The following page appears.

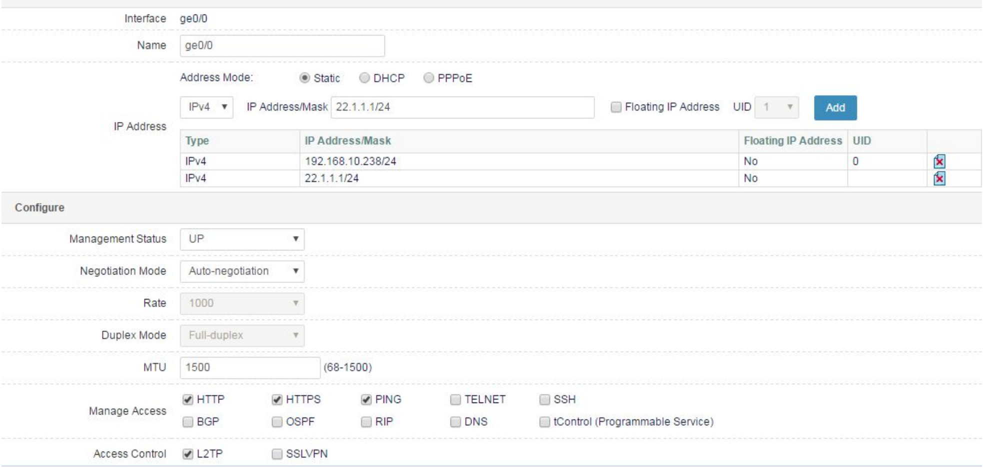


Enable	☑
Start IP Address	22.1.1.1
End IP Address	22.1.1.10
User Group	l2tp_group
User Uniqueness Check	☐
Dial-up User DNS	114.114.114.114
Dial-up User WINS	

8. Set parameters.

9. Click **Submit**.

10. Choose **Network** > **Interface** > **Physical interface**. Click interface ge0/0 to modify it.



Interface	ge0/0
Name	ge0/0
IP Address	Address Mode: ● Static ○ DHCP ○ PPPoE IPv4 IP Address/Mask 22.1.1.1/24 ☐ Floating IP Address UID 1

Type	IP Address/Mask	Floating IP Address	UID	
IPv4	192.168.10.238/24	No	0	☒
IPv4	22.1.1.1/24	No		☒

Management Status	UP
Negotiation Mode	Auto-negotiation
Rate	1000
Duplex Mode	Full-duplex
MTU	1500 (68-1500)
Manage Access	☑ HTTP ☑ HTTPS ☑ PING ☐ TELNET ☐ SSH ☐ BGP ☐ OSPF ☐ RIP ☐ DNS ☐ tControl (Programmable Service)
Access Control	☑ L2TP ☐ SSLVPN

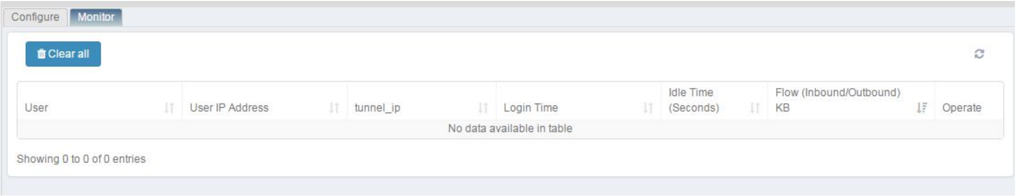
11. Set **IP address** and select **L2TP** for **Access control**.

12. Click **Submit**.

28.4 Monitoring and Maintenance

28.4.1 Displaying L2TP Session Information

Choose **Network** > **VPN** > **L2TP** > **Monitor** to display L2TP session information.



User	User IP Address	tunnel_ip	Login Time	Idle Time (Seconds)	Flow (Inbound/Outbound) KB	Operate
No data available in table						

Showing 0 to 0 of 0 entries

Click ✖ to disconnect a login user. Click Clear all to disconnect all the login users.

28.5 Troubleshooting

28.5.1 An L2TP Client Fails to Establish Connection via Dial-up

Sympto m	An L2TP client dials up to an LNS but fails to establish connection.
Analysis	The possible causes are as follows: ● The user name and password entered by the client are incorrect. Check the user name and password. ● The connection address specified by the client is not the address configured for the LNS dial-up interface. ● Check whether the server's address pool still has available addresses. ● Check whether **L2TP** is selected for **Access control** for the interface to allow client connection.

28.5.2 L2TP Connection Is Interrupted Abnormally

Sympto m	The direct connection from an L2TP client to an LNS is interrupted abnormally.
Analysis	The possible causes are as follows: ● The Hello packet transmitted in an L2TP tunnel gets no

	response due to a network fault, causing disconnection from the tunnel. Check that the network line is normal and the L2TP server interface works properly.

29 DNS Proxy

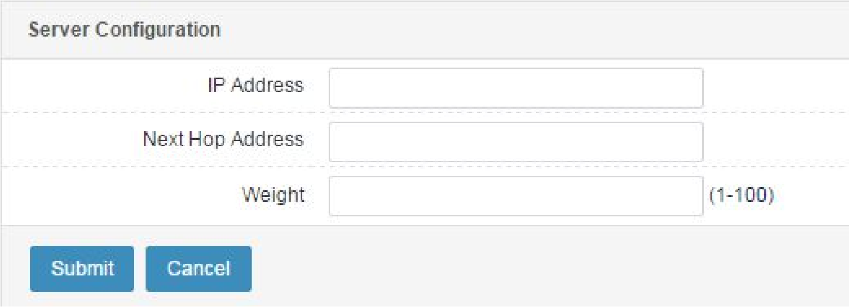
29.1 Overview

Transparent DNS proxy enables proper bandwidth use on multiple links to avoid resource waste. Transparent DNS proxy optimizes DNS resolution when intranet users access external resources. All the DNS requests of intranet users can be forwarded by a DNS proxy device. DNS request detection is initiated to multiple links, and DNS requests are forwarded to different servers based on the detection results and predefined policies, allowing users to get desired DNS responses. This ensures proper use of link bandwidth.

29.2 Configuration

29.2.1 Configuring a Server

1. Choose **Network** > **DNS proxy** > **Server**. The following page appears.



Server Configuration

IP Address		
Next Hop Address		
Weight		(1-100)

IP address: IP address of the DNS server.

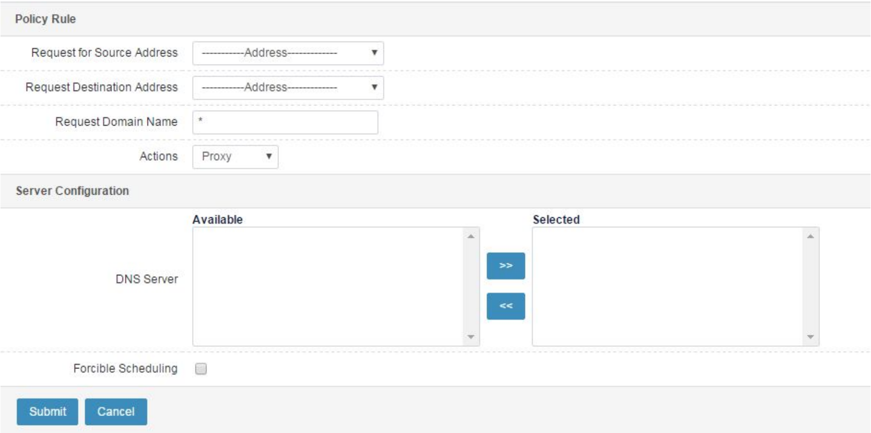
Next-hop address: Next hop destined for the DNS server.

Weight: Weight or priority of the DNS server. The value ranges from 1 to 100.

2. Set parameters.
3. Click **Submit**.

29.2.2 Configuring a Proxy Policy

1. Choose **Network** > **DNS proxy** > **Proxy policy**. The following page appears.



Policy Rule

Request for Source Address: ------------Address-------------

Request Destination Address: ------------Address-------------

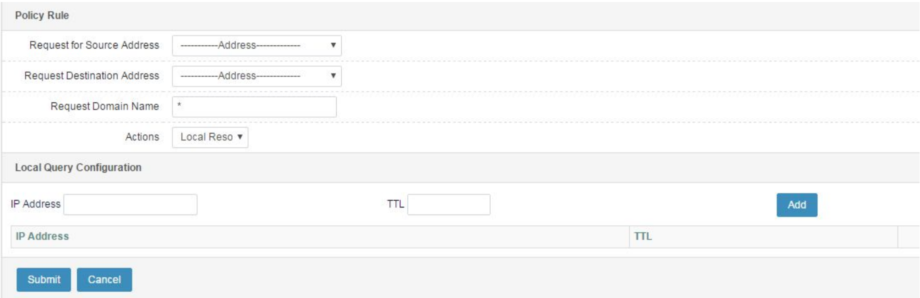
Request Domain Name: *

Actions: Proxy

Server Configuration

DNS Server: Available / Selected

Forcible Scheduling □



Policy Rule

Request for Source Address: ------------Address-------------

Request Destination Address: ------------Address-------------

Request Domain Name: *

Actions: Local Reso

Local Query Configuration

IP Address / TTL

IP Address	TTL

Policy parameter description:

Request source address: Source address of DNS requests. If **Any** is selected, the requests from all source addresses are matched.

Request destination address: Destination address of DNS requests. If **Any** is selected, the requests to all destination addresses are matched.

Request domain name: Domain name of DNS requests.

Action: Action taken after the policy is hit. The options are **Proxy**, **Forward**, and **Local resolution**.

Server parameter description:

DNS server: Select a server if **Proxy** is selected for **Action**.

Local resolution parameter description:

IP address: IP address corresponding to the requested domain name, in dotted decimal notation.

TTL: Cache time for the locally resolved IP address.

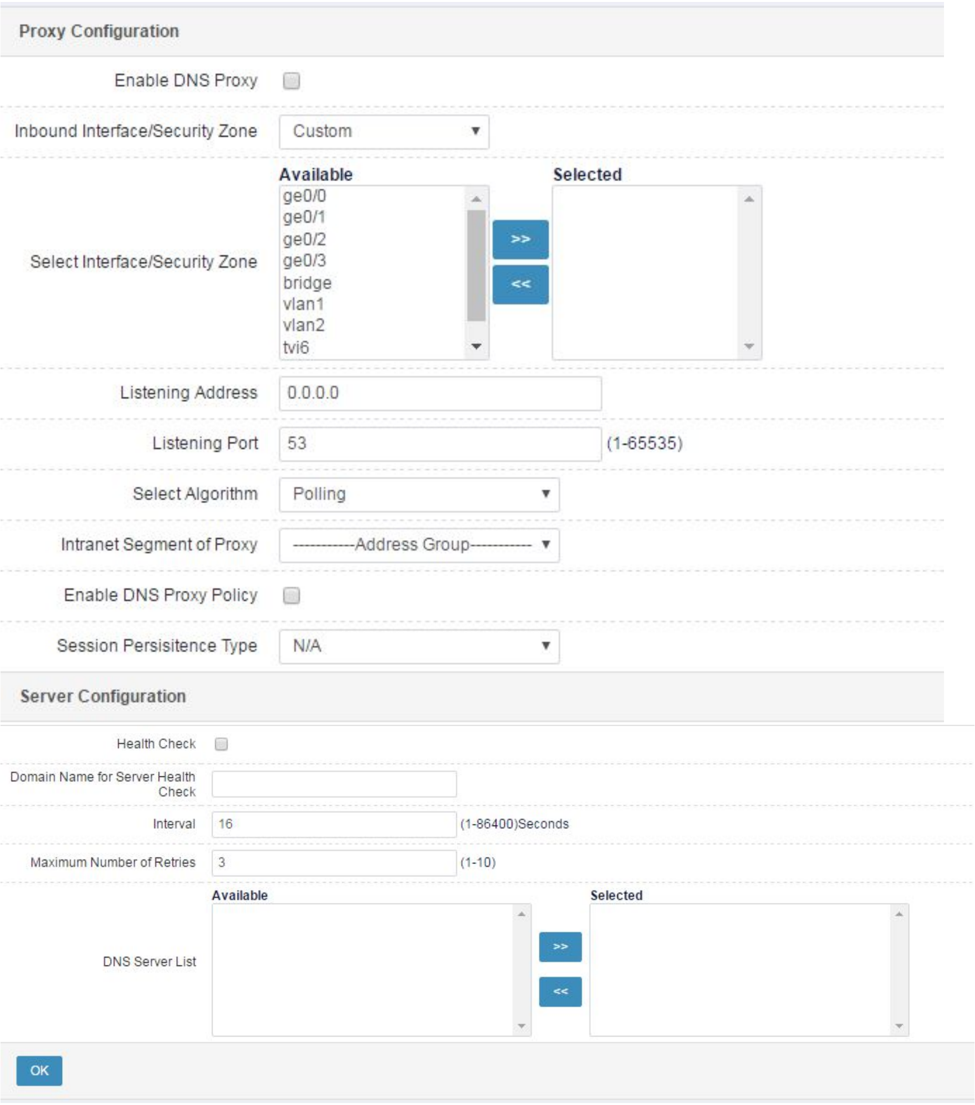
Add: Click this button to add DNS local resolution entries. A maximum of five entries can be added.

2. Set parameters.

3. Click **Submit**.

29.2.3 Configuring Global Settings

1. Choose **Network** > **DNS proxy** > **Global configuration**. The following page appears.



Proxy Configuration

Enable DNS Proxy	□
Inbound Interface/Security Zone	Custom ▼
Select Interface/Security Zone	Available: ge0/0, ge0/1, ge0/2, ge0/3, bridge, vlan1, vlan2, tvi6 Selected:
Listening Address	0.0.0.0
Listening Port	53 (1-65535)
Select Algorithm	Polling ▼
Intranet Segment of Proxy	-----------Address Group----------- ▼
Enable DNS Proxy Policy	□
Session Persisitence Type	N/A ▼

Server Configuration

Health Check	□
Domain Name for Server Health Check	
Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
DNS Server List	Available: Selected:

Proxy parameter description:

Enable DNS proxy: Check this box to enable DNS proxy.

Inbound interface/Security zone: Interface that receives DNS requests.

Listening address: Address of the listening DNS server. It is typically set to the address of the DNS server in the user network. The default value is **Any**.

Listening port: Port of the listening DNS server. The default value is **53**.

Select algorithm: Algorithm used by the server. The options are **Round robin**, **Weighted round robin**, **Weighted minimum traffic**, and **Priority**.

Proxy internal network segment: Source IP address object for proxy.

Enable DNS proxy policy: It is unchecked by default. If it is checked, the settings on the **DNS proxy** > **Proxy policy** page take effect.

Session persistence type: Select an option to enable session persistencebased on the request domain name and source address and enable session persistence based on the request source address for DNS requests. By default, this parameter is unspecified.

Timeout: Timeout period for a session persistence entry. The default value is **30s**.

IPv4 mask: Mask of the source address for session persistence. The default value is **255.255.255.255.**

Server parameter description:

Health check: Check this box to perform health check on the DNS servers in the DNS server list. After health check is enabled, the system sends detection packets to the DNS servers. If a DNS server does not respond to the detection packet, it will not participate in scheduling.

Server health check domain name: DNS domain name to be checked.

Interval: Interval at which health check is performed on the DNS servers in the DNS server list. The default value is **16s**.

Maximum retry times: Retry times allowed after a detection packet gets no response. The default value is **3**, indicating if three consecutive detection packets get no response or health check fails three consecutive times, the heath check status is Failed.

DNS server list: Select available DNS servers.

2. Set parameters.

3. Click **Submit**.

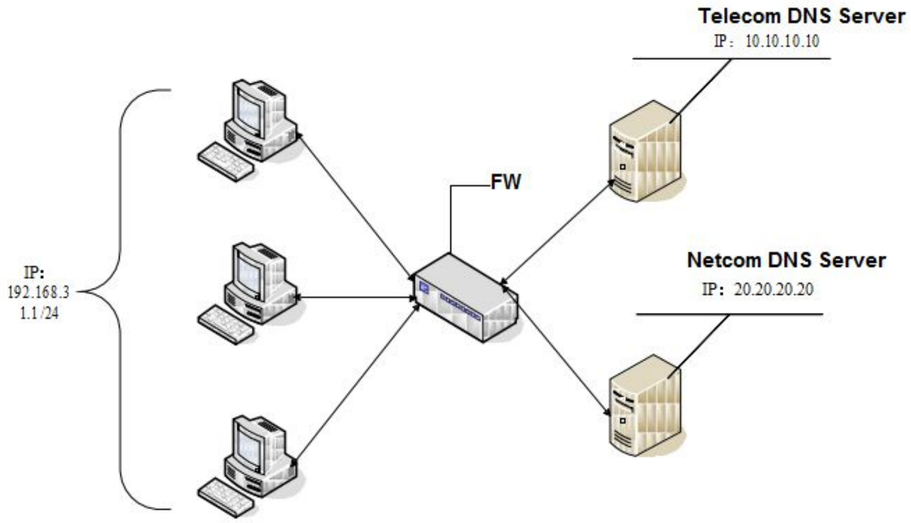
29.3 Configuration Examples

29.3.1 Example 1

A China Telecom link and a CNC link are deployed at the network egress. If many PCs on the intranet use the Telecom DNS address, a large amount of resource access traffic is routed along the Telecom link, while the CNC link handles a small portion of access tasks. In this case, the Telecom link may be

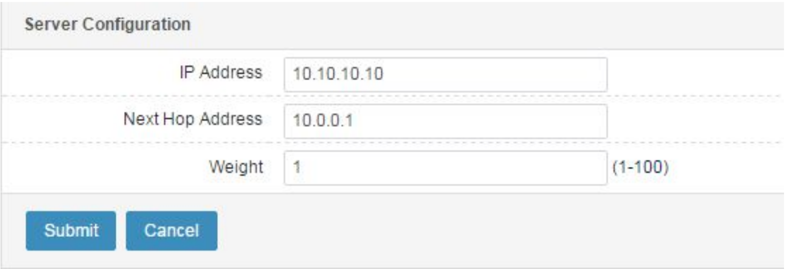
congested whereas the CNC link is idle. After transparent DNS proxy is configured, the DNS requests of intranet users with Telecom and CNC DNS addresses are forwarded by the firewall. The firewall selects a suitable DNS server based on a scheduling policy, and returns the resolved address to the intranet user. This enables proper use of bandwidth resources.

Procedure:



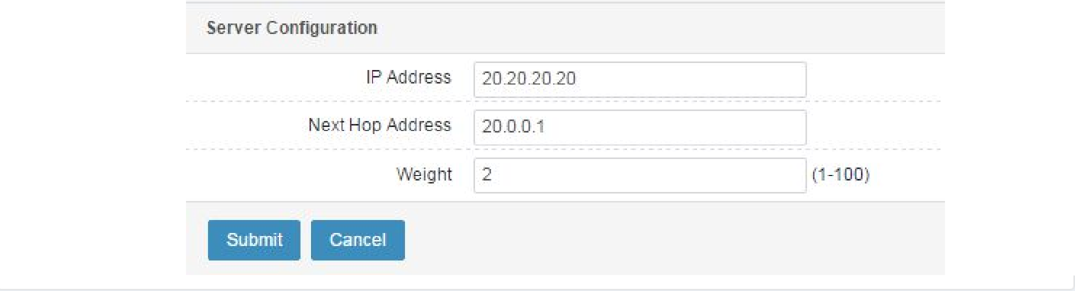
1. Configure a network environment to ensure that internal traffic is properly routed to external networks.
2. Complete the following configuration:

(1) Configure a server.



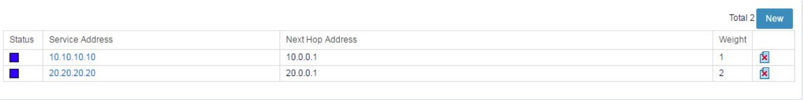
Server Configuration

IP Address	10.10.10.10	
Next Hop Address	10.0.0.1	
Weight	1	(1-100)



Server Configuration

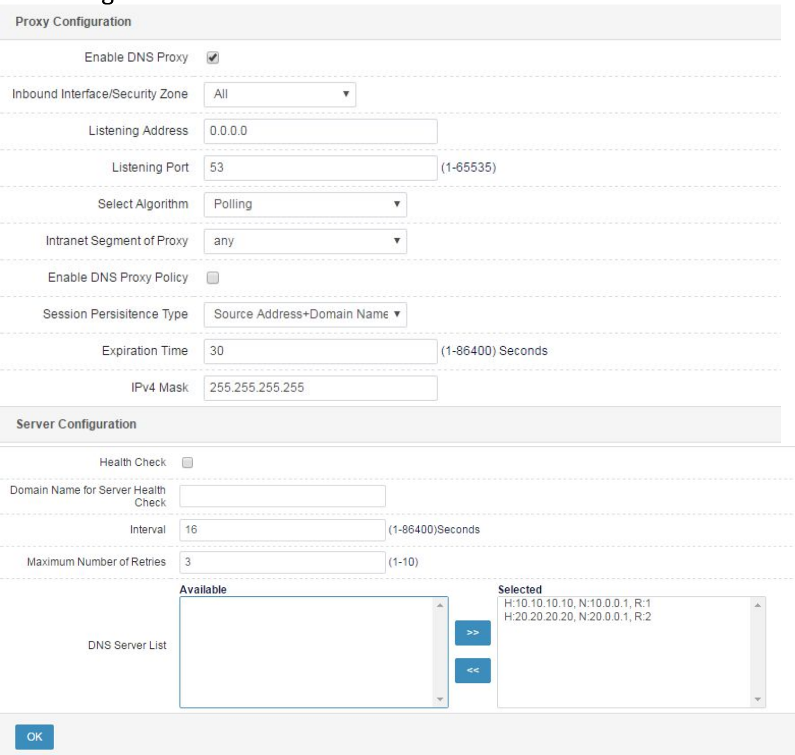
IP Address	20.20.20.20	
Next Hop Address	20.0.0.1	
Weight	2	(1-100)



Total 2

Status	Service Address	Next Hop Address	Weight	
■	10.10.10.10	10.0.0.1	1	☒
■	20.20.20.20	20.0.0.1	2	☒

(2) Configure global settings.



Proxy Configuration

Enable DNS Proxy	☑	
Inbound Interface/Security Zone	All ▼	
Listening Address	0.0.0.0	
Listening Port	53	(1-65535)
Select Algorithm	Polling ▼	
Intranet Segment of Proxy	any ▼	
Enable DNS Proxy Policy	☐	
Session Persisitence Type	Source Address+Domain Name ▼	
Expiration Time	30	(1-86400) Seconds
IPv4 Mask	255.255.255.255	

Server Configuration

Health Check	☐	
Domain Name for Server Health Check		
Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)

DNS Server List

Available

Selected
H:10.10.10.10, N:10.0.0.1, R:1
H:20.20.20.20, N:20.0.0.1, R:2

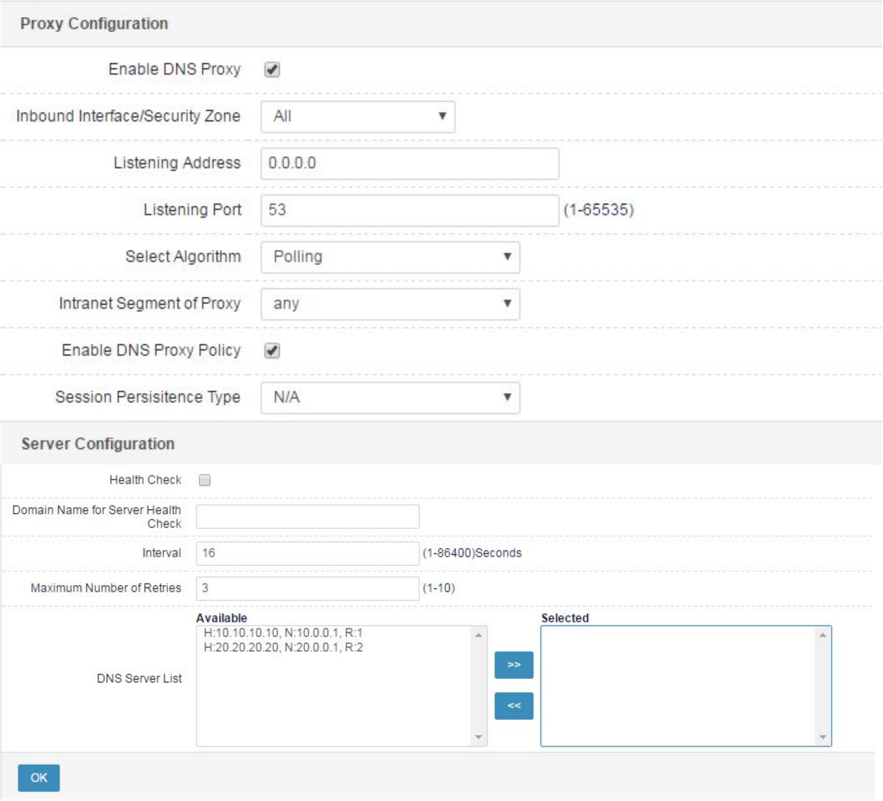
29.3.2 Example 2

If **Enable DNS proxy** is selected in global settings but a DNS policy with local resolution is not configured, DNS requests are forwarded based on the PC's DNS address or based on the matched DNS proxy policy and global settings. The firewall selects a suitable DNS server based on a scheduling policy and returns the resolved address to the user. If DNS local resolution is configured, DNS requests are not sent to the DNS server for resolution, but are resolved using an A record based on the local manual settings. This removes the process of DNS server access.

Procedure:

1. Choose **DNS** > **Proxy**. On the displayed page, check the **Enable DNS proxy** and **Enable DNS proxy policy** boxes.
2. Complete the following configuration:

Configure global settings.



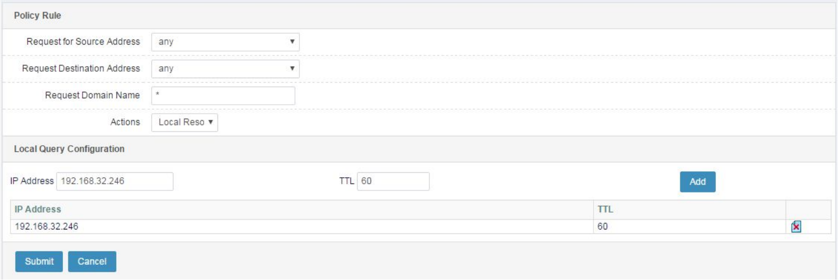
Proxy Configuration

Enable DNS Proxy	☑
Inbound Interface/Security Zone	All ▾
Listening Address	0.0.0.0
Listening Port	53 (1-65535)
Select Algorithm	Polling ▾
Intranet Segment of Proxy	any ▾
Enable DNS Proxy Policy	☑
Session Persisitence Type	N/A ▾

Server Configuration

Health Check	☐
Domain Name for Server Health Check	
Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
DNS Server List	Available: H:10.10.10.10, N:10.0.0.1, R:1 H:20.20.20.20, N:20.0.0.1, R:2 Selected:

(1) Configure a local resolution proxy policy and check the **Enable** box.



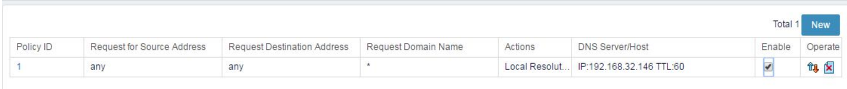
Policy Rule

Request for Source Address	any ▾
Request Destination Address	any ▾
Request Domain Name	*
Actions	Local Reso ▾

Local Query Configuration

IP Address 192.168.32.246 TTL 60

IP Address	TTL	
192.168.32.246	60	☒



Policy ID	Request for Source Address	Request Destination Address	Request Domain Name	Actions	DNS Server/Host	Enable	Operate
1	any	any	*	Local Resolut...	IP:192.168.32.146 TTL:60	☑	⇅ ☒

According to the results of packet capture by Wireshark, the URL www.baidu.com can be accessed when local resolution is disabled. After the local resolution policy with the address 192.168.32.246 is referenced, the domain name request initiated by a PC to the preceding URL is redirected to 192.168.32.246. The DNS server does not resolve the IP address of the URL.

30 DNS Service

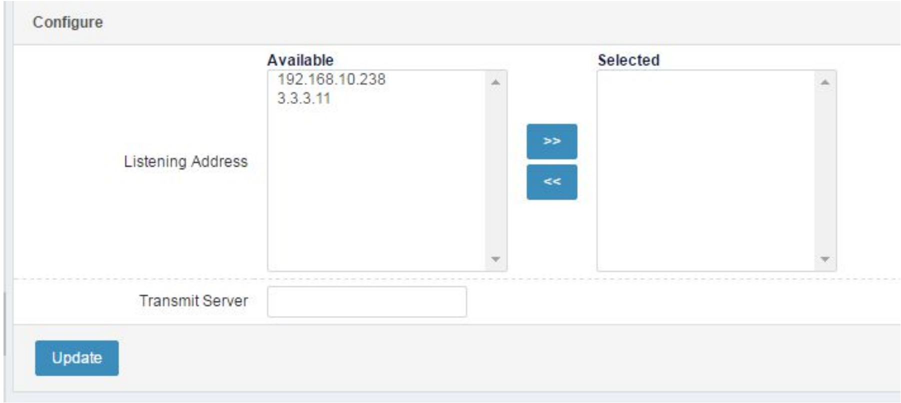
30.1 Overview

A DNS server converts domain names to corresponding IP addresses. RAVEN 5000 firewalls provide the standard DNS service.

30.2 Configuration

30.2.1 Basic Configuration

1. Choose **Network** > **DNS service** > **Basic configuration**. The following page appears.



Parameter description:

Listening address: Address that listens to DNS requests.

Available: Available IP addresses.

Selected: IP addresses selected to listen to DNS requests.

Forwarding server: A DNS request is forwarded to this server for resolution when the local DNS query fails.

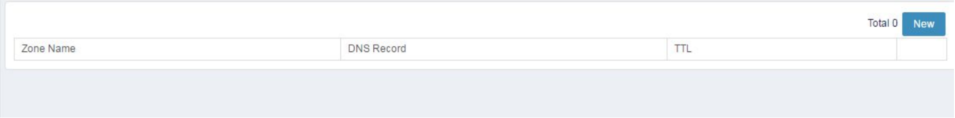
2. Select the left-side IP addresses to listen to DNS requests and click >> to add them to the right-side column.

3. Click **Update**.

30.2.2 Configuring a DNS Record

A DNS record provides multiple types of authoritative local resolution. DNS records are managed in the same way as bind. Multiple DNS records are allocated to a zone for management.

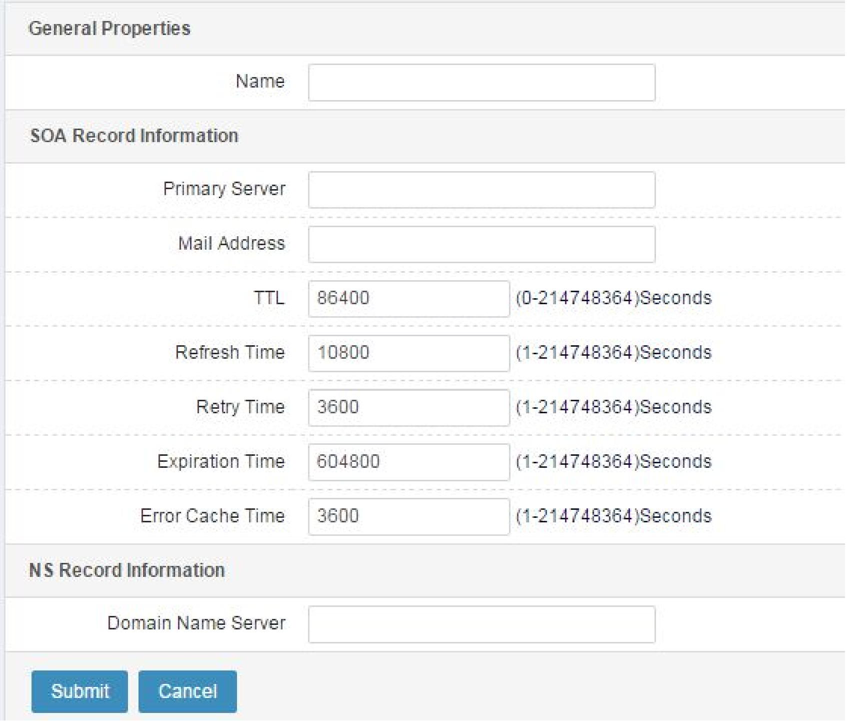
Choose **Network** > **DNS service** > **DNS Zones**. The following page appears.



Total 0

Zone Name	DNS Record	TTL

Click **New** to create a zone.



General Properties

Name		

SOA Record Information

Primary Server		
Mail Address		
TTL	86400	(0-214748364)Seconds
Refresh Time	10800	(1-214748364)Seconds
Retry Time	3600	(1-214748364)Seconds
Expiration Time	604800	(1-214748364)Seconds
Error Cache Time	3600	(1-214748364)Seconds

NS Record Information

Domain Name Server	

Name: Name of a zone.

Master server: Name of the master server in the zone.

Email address: Email address of the zone.

TTL: TTL of the SOA record for the zone, also the default TTL of the records in the zone.

Refresh time: Refresh time of the SOA record, which indicates the interval at which the slave DNS server synchronizes zone files from the master DNS server.

Retry time: Retry time of the SOA record, which indicates the retry interval when the slave DNS server fails to synchronize zone files from the master DNS server.

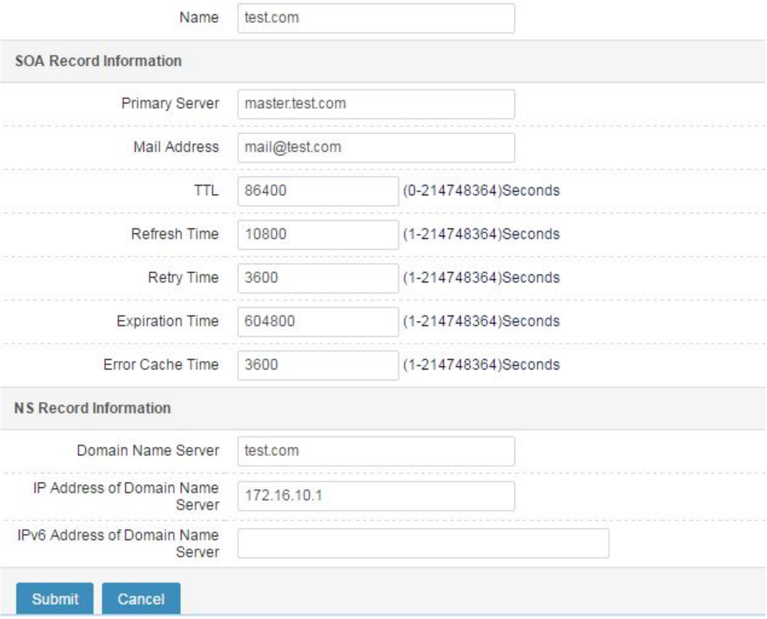
Expiration: Validity period of the SOA record. If the duration of failedcommunication between the slave and master DNS server exceeds the validity period, the zone is considered to fail.

Error cache time: Negative TTL of the SOA record, which indicates the duration for which the zone's error records are cached.

DNS server: At least one NS record must exist when a zone is created. This parameter indicates the content of the NS record named after the zone, that is, the name of the DNS server in the zone. If the domain name belongs to the zone (that is, the zone name ends with the domain name), you must enter the corresponding A record (IPv4 address) or AAAA record (IPv6 address).

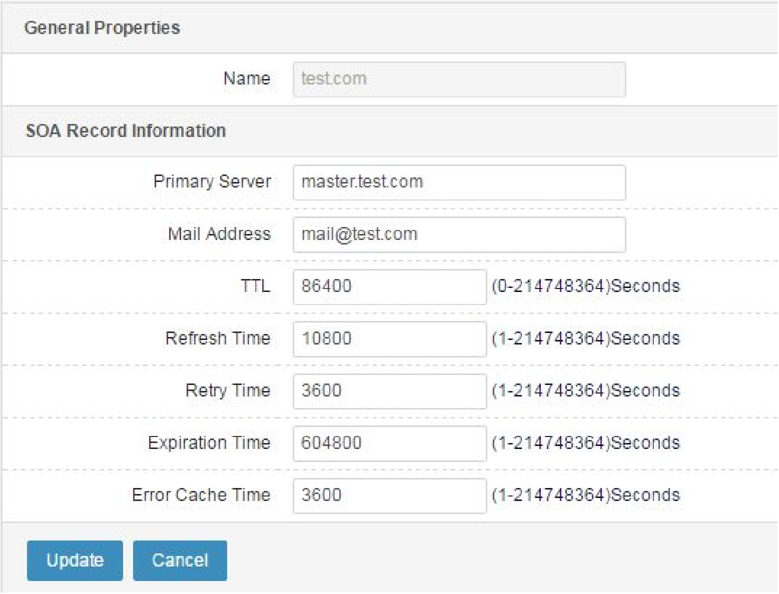
Procedure:

Set the parameters and click **Submit**.



Name	test.com	
SOA Record Information		
Primary Server	master.test.com	
Mail Address	mail@test.com	
TTL	86400	(0-214748364)Seconds
Refresh Time	10800	(1-214748364)Seconds
Retry Time	3600	(1-214748364)Seconds
Expiration Time	604800	(1-214748364)Seconds
Error Cache Time	3600	(1-214748364)Seconds
NS Record Information		
Domain Name Server	test.com	
IP Address of Domain Name Server	172.16.10.1	
IPv6 Address of Domain Name Server		

If you want to modify the parameters (**Name** cannot be modified), click the zone name in the zone list. The following page appears.



General Properties

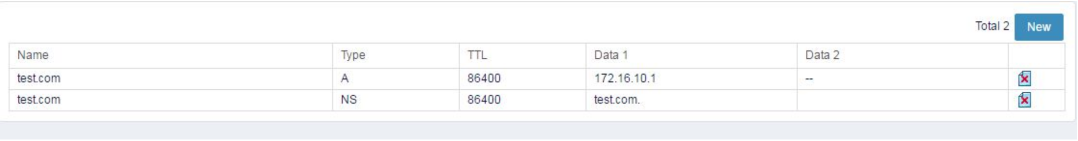
Name	test.com

SOA Record Information

Primary Server	master.test.com	
Mail Address	mail@test.com	
TTL	86400	(0-214748364)Seconds
Refresh Time	10800	(1-214748364)Seconds
Retry Time	3600	(1-214748364)Seconds
Expiration Time	604800	(1-214748364)Seconds
Error Cache Time	3600	(1-214748364)Seconds

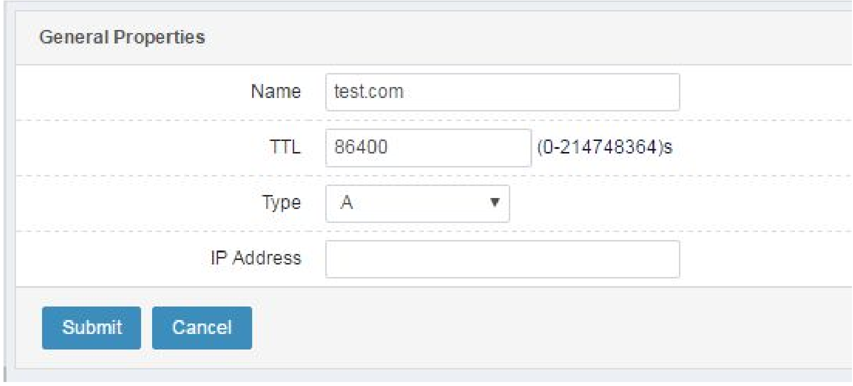
Modify the parameters and click **Update**.

In the zone list, click the DNS record count of a zone to go to the DNS record management page, as shown in the following figure.



Name	Type	TTL	Data 1	Data 2	
test.com	A	86400	172.16.10.1	--	☒
test.com	NS	86400	test.com.		☒

Click **New** to create a DNS record.



General Properties

Name	test.com	
TTL	86400	(0-214748364)s
Type	A ▼	
IP Address		

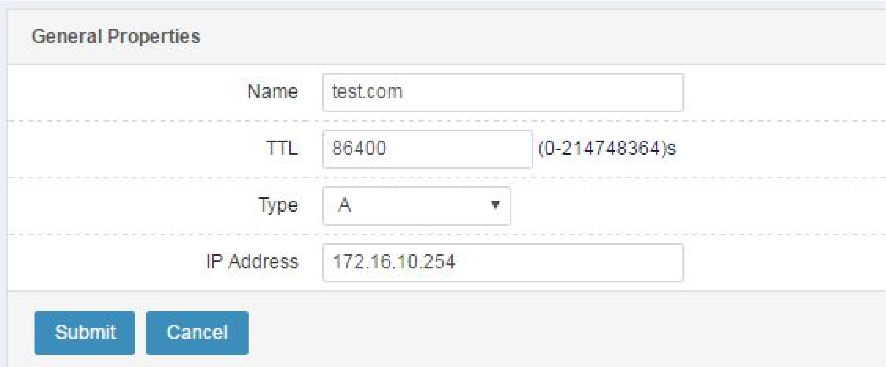
Name: Name of the new record.

TTL: TTL of the record.

Type: Record type. The options are **A**, **AAAA**, **NS**, **CNAME**, **MX**, **TXT**, and **PTR**.

A: IPv4 address record.

IP address: IP address corresponding to the record name.

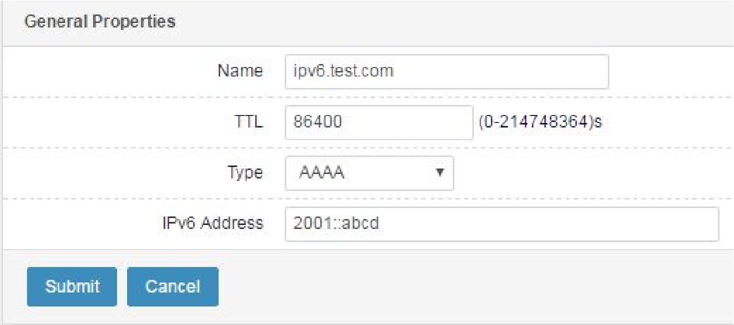


General Properties

Name	test.com
TTL	86400 (0-214748364)s
Type	A
IP Address	172.16.10.254

AAAA: IPv6 address record.

IPv6 address: IPv6 address corresponding to the record name.

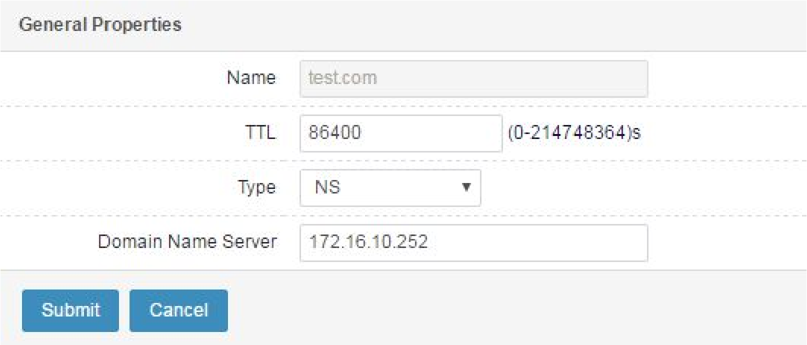


General Properties

Name	ipv6.test.com
TTL	86400 (0-214748364)s
Type	AAAA
IPv6 Address	2001::abcd

NS: DNS server record.

DNS server: Name of the authoritative DNS server corresponding to the zone, which is indicated by the record name.

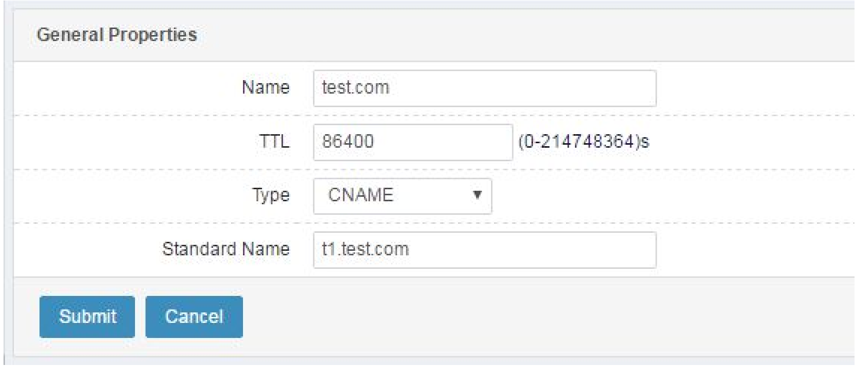


General Properties

Name	test.com
TTL	86400 (0-214748364)s
Type	NS
Domain Name Server	172.16.10.252

CNAME: Standard name record.

Standard name: Standard domain name corresponding to the alias, which is indicated by the record name.



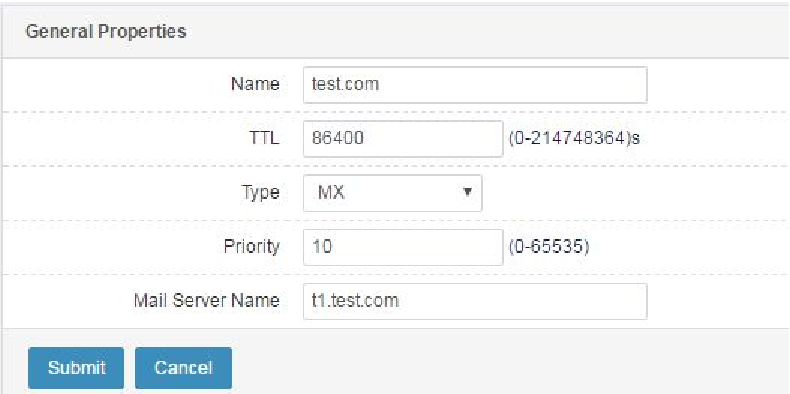
General Properties

Name	test.com
TTL	86400 (0-214748364)s
Type	CNAME
Standard Name	t1.test.com

MX: Email hub record.

Priority: Priority of the MX record. The smaller the value, the higher the priority.

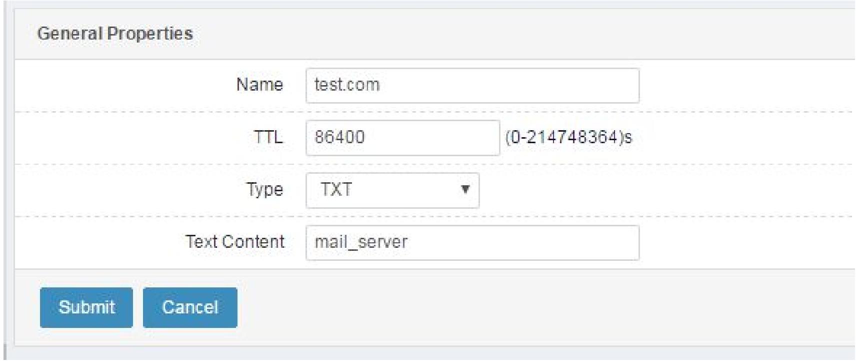
Mail server name: Name of the mail server to which the email domain name (indicated by the domain name in the record name) belongs to (or the name of the forwarding mail server connected to the mail server).



Name	test.com
TTL	86400 (0-214748364)s
Type	MX ▼
Priority	10 (0-65535)
Mail Server Name	t1.test.com

TXT: Text record.

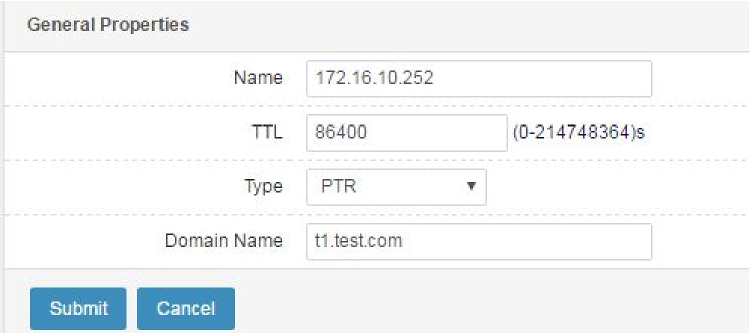
Text content: Text content corresponding to the record name, which can be customized by the zone administrator as needed. The text content can be in Chinese or English.



Name	test.com
TTL	86400 (0-214748364)s
Type	TXT ▼
Text Content	mail_server

PTR: Reverse lookup record.

Domain name: Contrary to A or AAAA. The system searches for the domain name corresponding to an IPv4 or IPv6 address. This parameter is managed in reverse zone (in-addr.arpa. Or ip6.arpa.).



General Properties

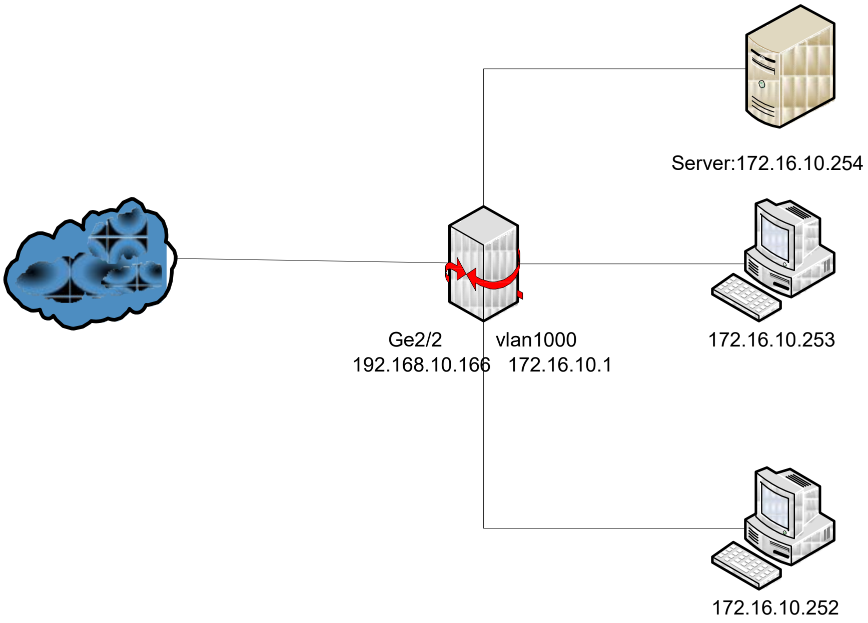
Name	172.16.10.252
TTL	86400 (0-214748364)s
Type	PTR
Domain Name	t1.test.com

30.2.3 Configuration Example

Description:

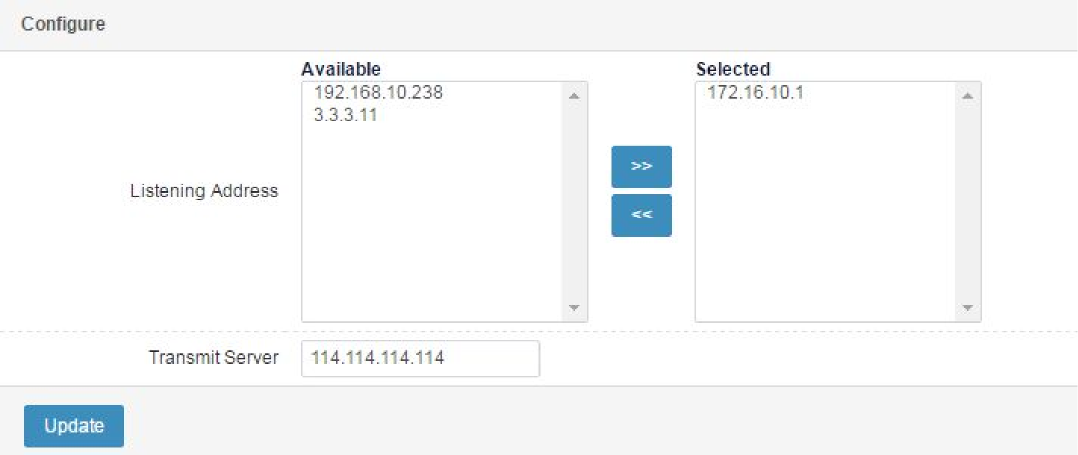
Perform configuration to allow users on an intranet to access internal services using domain names and access the Internet normally. (A route destined for the Internet must be configured in advance.)

Network diagram:



Procedure:

1. Configure a DNS listening address and a DNS forwarding server.



Configure

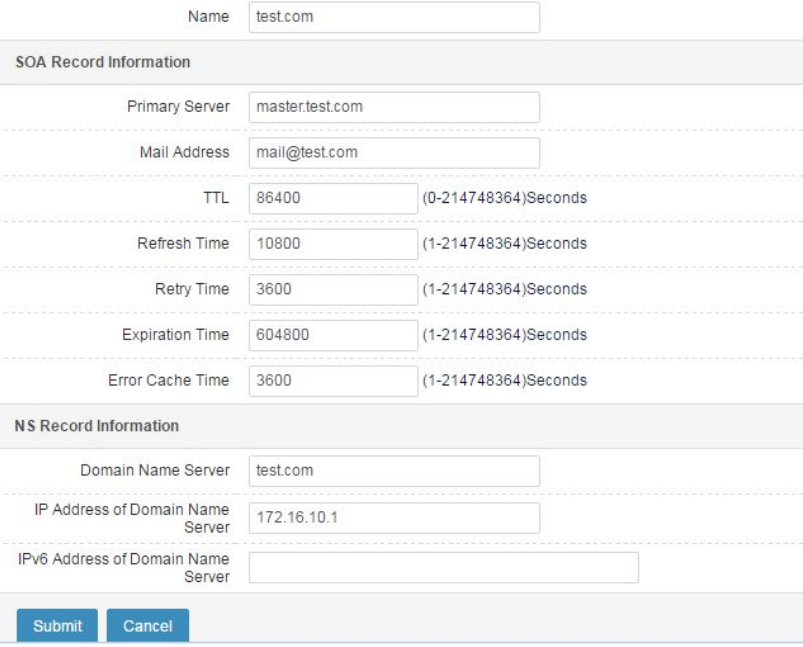
Listening Address

Available: 192.168.10.238, 3.3.3.11

Selected: 172.16.10.1

Transmit Server: 114.114.114.114

2. Configure DNS zones.



Name: test.com

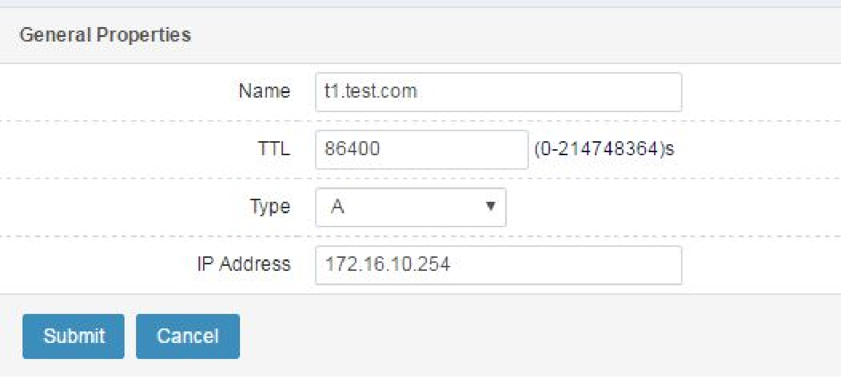
SOA Record Information

Primary Server	master.test.com	
Mail Address	mail@test.com	
TTL	86400	(0-214748364)Seconds
Refresh Time	10800	(1-214748364)Seconds
Retry Time	3600	(1-214748364)Seconds
Expiration Time	604800	(1-214748364)Seconds
Error Cache Time	3600	(1-214748364)Seconds

NS Record Information

Domain Name Server	test.com
IP Address of Domain Name Server	172.16.10.1
IPv6 Address of Domain Name Server	

3. Create a DNS record. Enter the A record corresponding to the server's domain name. Click **Submit**.



General Properties

Name	t1.test.com
TTL	86400 (0-214748364)s
Type	A
IP Address	172.16.10.254

31 System Parameters

31.1 Overview

Protocol management: Network devices delete timeout protocol connections to protect connection resources. On RAVEN5000 firewalls, the default timeout period is 1 hour for TCP and 30 seconds for UDP. In some applications, after a full connection is established, packets are exchanged only based on actual data, without a keep-alive mechanism. As a result, timeout connections are deleted, and the device cannot receive subsequent data. The protocol management function allows you to set the timeout period of a specific service to keep alive long-time idle connections.

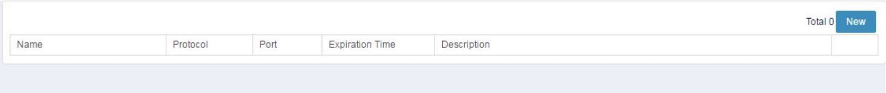
TCP status management: The system determines whether to count a connection based on its TCP status during connection statistics. If **ESTABLISHED connections** is selected, the system only counts established connections; if **All connections** is selected, the system counts all connections.

Parameter management: Parameters are provided to enable and disable module functions.

31.2 Configuring Protocol Management

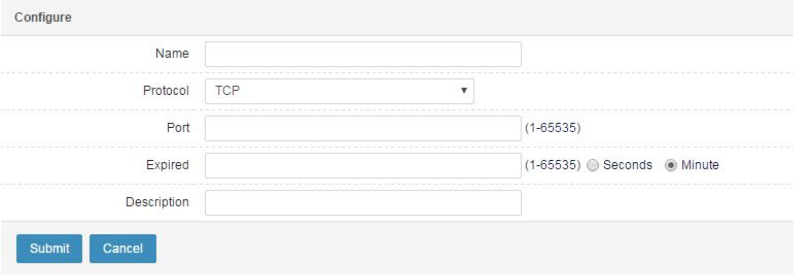
Procedure:

1. Choose **Network** > **System parameters** > **Protocol management**.



Name	Protocol	Port	Expiration Time	Description	

2. Click **New**.



Configure

Name	
Protocol	TCP ▾
Port	(1-65535)
Expired	(1-65535) ○ Seconds ● Minute
Description	

Parameter description:

Name: Name of protocol management.

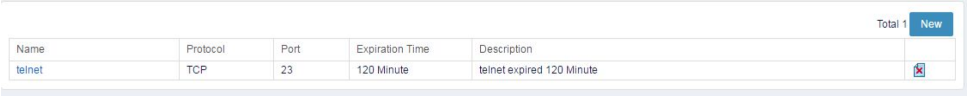
Protocol: Protocol type, TCP or UDP.

Port: Service port for the protocol.

Timeout: 1 to 65535, in minutes or seconds.

Description: Protocol management description.

3. Click **Submit** to apply the settings. The following figure shows an example of configured protocol management.



Total 1

Name	Protocol	Port	Expiration Time	Description	
telnet	TCP	23	120 Minute	telnet expired 120 Minute	☒

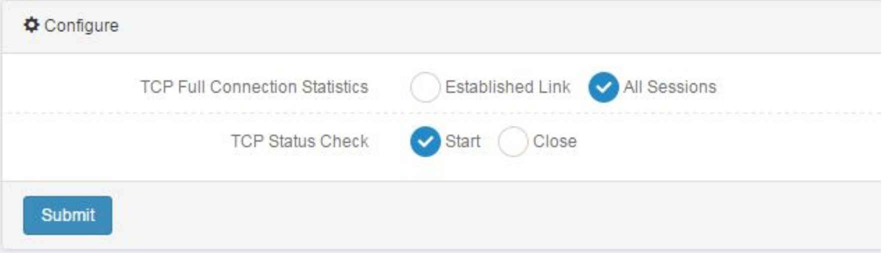
Notice

Protocol management takes effect for new connections only after being configured.

31.3 Configuring TCP Status Management

Procedure:

1. Choose **Network** > **System parameters** > **TCP status management**.



Configure

TCP Full Connection Statistics	○ Established Link ✓ All Sessions
TCP Status Check	✓ Start ○ Close

2. Set **TCP full connection status statistics**.

If you select **ESTABLISHED connections**, the system only counts full connections. If you select **All connections**, the system counts full connections and half-open connections.

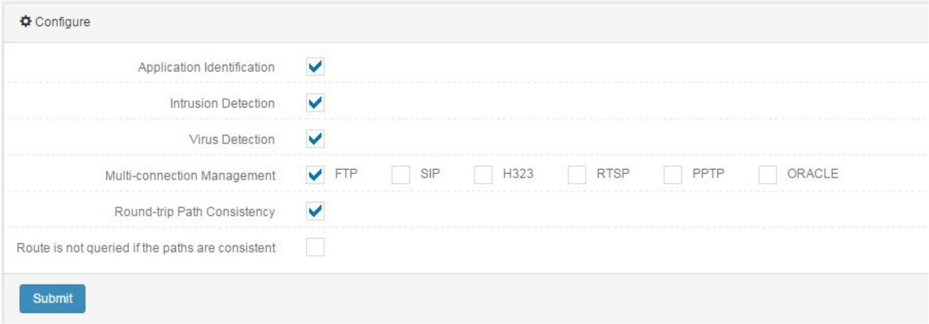
3. Set **TCP status check**.

Select **Enable** or **Disable** to enable or disable loose TCP check.

31.4 Configuring Parameter Management

Procedure:

1. Choose **Network** > **System parameters** > **parameter management**.



Configure

Application Identification	☑
Intrusion Detection	☑
Virus Detection	☑
Multi-connection Management	☑ FTP □ SIP □ H323 □ RTSP □ PPTP □ ORACLE
Round-trip Path Consistency	☑
Route is not queried if the paths are consistent	□

Submit

Application identification: Check this box to enable application identification.

Intrusion detection: Check this box to enable intrusion detection.

Virus detection: Check this box to enable virus detection.

Multi-connection management: Check this box to identify multiple connections of a protocol type.

Round-trip path consistency: Check this box to enable round-trip path consistency check.

Path consistency without route lookup: Check this box to enable path consistency without route lookup.

32 Network Debugging

32.1 Overview

RAVEN5000 firewalls provide web debugging to facilitate configuration troubleshooting. Web debugging allows you to check the key processes of handling forwarded packets that match specified conditions,

including packet flow processing, NAT processing, firewall policy processing, and packet information.

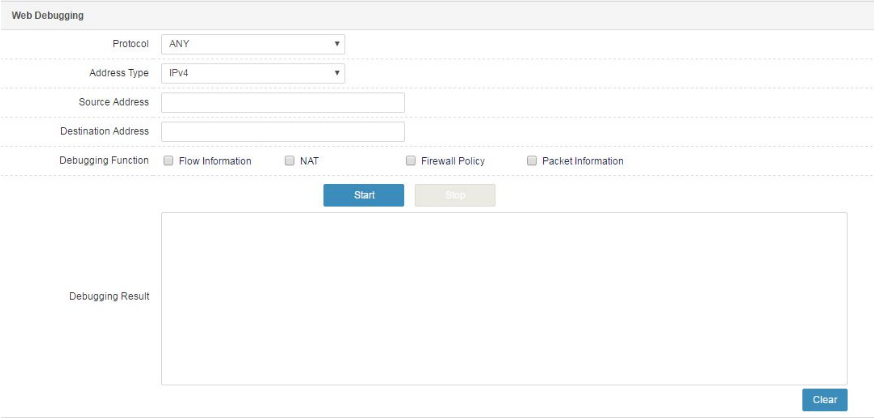
32.2 Configuration

32.2.1 Configuring the Basic Elements of Web Debugging

The basic elements of web debugging are the packet protocol, address type, source address, destination address, and debugging function. You can perform configuration to check how a specified function module processes the forwarded packets that match the basic elements.

Procedure:

1. Choose **Network** > **Network debugging** > **Web debugging**. The following page appears.



Web Debugging

Protocol: ANY

Address Type: IPv4

Source Address:

Destination Address:

Debugging Function: □ Flow Information □ NAT □ Firewall Policy □ Packet Information

Debugging Result:

Parameter description:

Protocol: Protocol type of packets. The options are **ANY**, **TCP**, **UDP**, **ICMP**, and **OTHER.** To check packets of all protocol types, select **ANY**. The parameters vary depending on different protocols.

Address type: IP address type of packets. The options are **IPv4** and **IPv6**.

Source address: Source address of packets.

Destination address: Destination address of packets.

Debugging: Processing results of a function module. The options are **Flow info**, **NAT**, and **Firewall policy**.

Flow info: Packet flow creation and match information.

NAT: Information about packet address conversion.

Firewall policy: Information about packets matched with firewall policies.

Packet info: Packet information.

2. After you complete the settings, click **Start** to start debugging.
3. Click **Clear** to clear the information in the debugging result box.
4. To stop debugging in progress, click **Stop**.

⚠ Notice

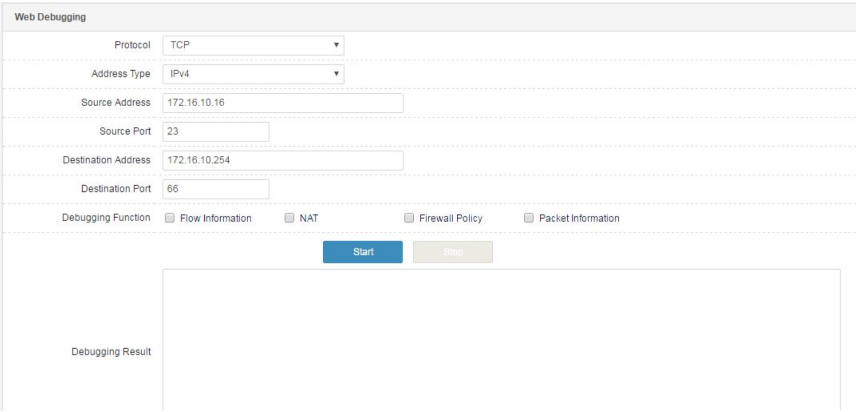
If you want to modify parameters, you need to stop debugging.

32.2.2 Configuring TCP- or UDP-based Web Debugging

When configuring TCP- or UDP-based web debugging, specify **Source port** and **Destination port**.

Procedure:

1. Choose **Network** > **Network debugging** > **Web debugging**. Select **TCP** for **Protocol** and set parameters, as shown in the following figure.



Web Debugging

Protocol: TCP

Address Type: IPv4

Source Address: 172.16.10.16

Source Port: 23

Destination Address: 172.16.10.254

Destination Port: 66

Debugging Function: ☐ Flow Information ☐ NAT ☐ Firewall Policy ☐ Packet Information

Debugging Result

Source port: Source port number of packets.

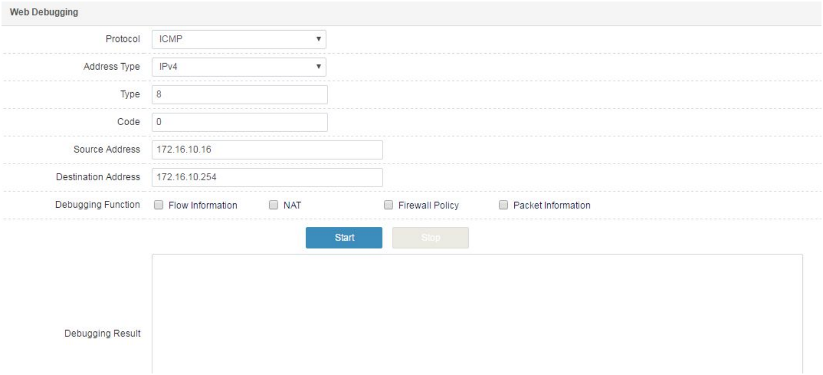
Destination port: Destination port number of packets.

32.2.3 Configuring ICMP-based Web Debugging

When configuring ICMP-based web debugging, specify **Code** and **Type**.

Procedure:

1. Choose **Network** > **Network debugging** > **Web debugging**. Select **ICMP** for **Protocol** and set parameters, as shown in the following figure.



Web Debugging

Protocol: ICMP

Address Type: IPv4

Type: 8

Code: 0

Source Address: 172.16.10.16

Destination Address: 172.16.10.254

Debugging Function: ☐ Flow Information ☐ NAT ☐ Firewall Policy ☐ Packet Information

Debugging Result

Type: ICMP packet type. The value ranges from 0 to 255.

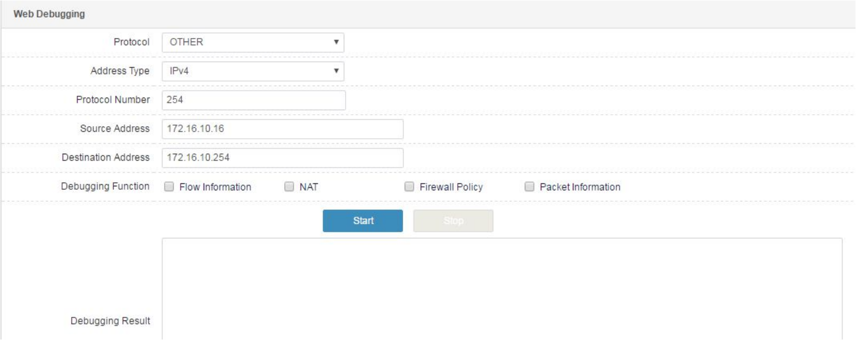
Code: Code carried by ICMP packets. The value ranges from 0 to 255.

32.2.4 Configuring Web Debugging of Other Protocol Type

If you select **OTHER** for **Protocol**, you need to specify the Layer-4 protocol number.

Procedure:

1. Choose **Network** > **Network debugging** > **Web debugging**. Select **OTHER** for **Protocol** and set parameters, as shown in the following figure.



Web Debugging

Protocol	OTHER
Address Type	IPv4
Protocol Number	254
Source Address	172.16.10.16
Destination Address	172.16.10.254
Debugging Function	□ Flow Information □ NAT □ Firewall Policy □ Packet Information
Debugging Result	

Protocol number: Layer-4 protocol number of packets. The value ranges from 1 to 255.

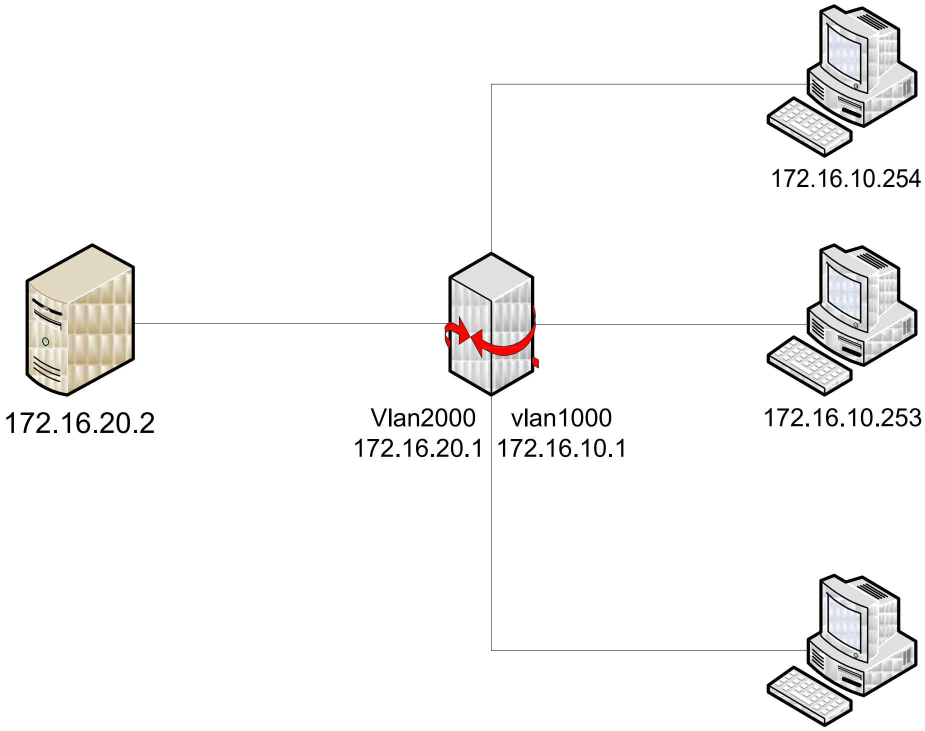
32.3 Configuration Example

32.3.1 Configuring IPv4-based Web Debugging

Description:

Display information about packet exchange for HTTP server access after SNAT is performed on internal addresses.

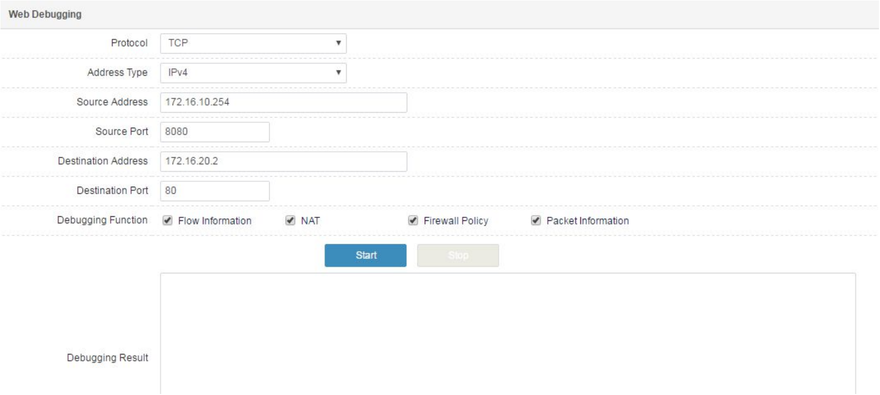
Network diagram:


172.16.10.254
172.16.20.2
Vlan2000
172.16.20.1
vlan1000
172.16.10.1
172.16.10.253

172.16.10.252

Procedure:

1. Choose **Network** > **Network debugging** > **Web debugging**. Select **TCP** for **Protocol** and **IPv4** for **IP address type**. Set **Source address** to the client address, **Destination address** to the HTTP server address, and **Destination port** to **80**. Select **Flow info**, **NAT**, and **Firewall policy** for **Debugging**. See the following figure.



Web Debugging

Protocol	TCP
Address Type	IPv4
Source Address	172.16.10.254
Source Port	8080
Destination Address	172.16.20.2
Destination Port	80
Debugging Function	☑ Flow Information ☑ NAT ☑ Firewall Policy ☑ Packet Information
Debugging Result	

2. Click **Sta**

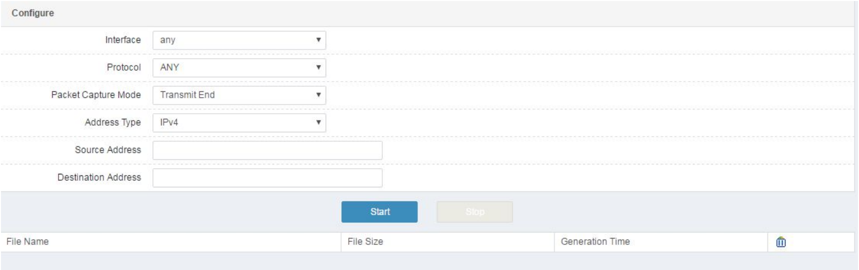
33 Custom Packet Capture

33.1 Overview

The custom packet capture function allows you to capture packets in a real network by specifying filter criteria to analyze the network status and trace problems.

33.2 Configuration

Choose **Network** > **Network Debugging** > **User-defined Packet Capture.** On the displayed page, set filter criteria to capture specified packets.


Configure

Interface: any

Protocol: ANY

Packet Capture Mode: Transmit End

Address Type: IPv4

Source Address:

Destination Address:

Protocol: Transport protocol for packet capture. The default value is **ANY**.

> If you select **TCP** or **UDP**, you can specify the source and destination port. If you do not specify them, packet capture will be performed on all ports.
>
> If you select **ICMP**, you can specify **Type** and **Code**. If you do not specify them, all ICMP packets will be captured.
>
> If you select **OTHER**, you can specify a transport protocol number. If you do not specify it, packets of all protocol types except TCP, UDP, and ICMP will be captured.

Capture mode: At which end packets will be captured.

Tx end: Capture packets sent and received at the transmit end.

Rx end: Capture packets sent and received at the receive end.

ANY: Capture packets at any ends.

Address type: Network layer protocol type of captured packets. The options are **IPv4**, **IPv6**, and **ANY**. (If **ANY** is selected, address setting is disabled.)

Source address: Source address of captured packets, which is of the specified type. The following address formats are supported: host address *A.B.C.D*, address range *A.B.C.D-E.F.G.H*, and network address *A.B.C.D/M*. If you do not set this parameter, all addresses of the specified type will apply.

Destination address: Destination address of captured packets, which is of the specified type. The following address formats are supported: host address *A.B.C.D*, network segment address range *A.B.C.D-E.F.G.H*, and network address *A.B.C.D/M*. If you do not set this parameter, all addresses of the specified type will apply.

Start: Click this button to start capturing packets.

Stop: Click this button to stop capturing packets. Packet capture will automatically stop after 10 packets are captured.

⚠ Notice

1. The maximum size of every packet capture file is 10 MB. When this limit is exceeded, the packet is saved to the next file.
2. A maximum of 10 packet capture files can be saved. When this limit is reached, packet capture stops.
3. If 10 packet capture files are already saved and you want to start capturing again, you must delete and clear the existing files.
4. For multi-connection protocols, such as FTP, after you specify connection filter criteria, the system will capture packets over the corresponding data connections.
5. The source and destination addresses are always the initial source and destination addresses of a connection.

33.3 Configuration Example

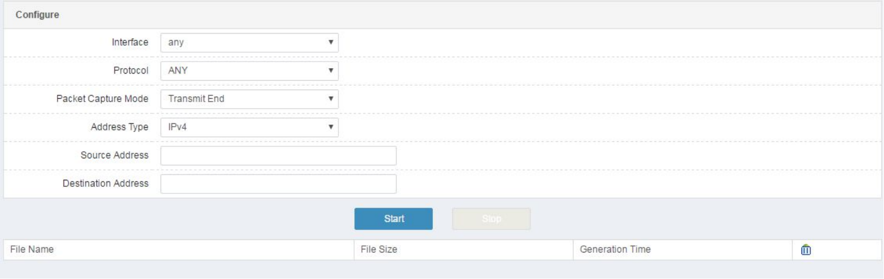
Description:

Capture packets sent by host 6.6.6.6.

Procedure:

1. Choose **Network** > **Network Debugging** > **User-defined Packet Capture**

and set filter
criteria.


Configure

Interface: any

Protocol: ANY

Packet Capture Mode: Transmit End

Address Type: IPv4

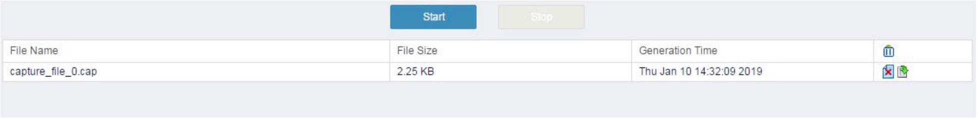
Source Address:

Destination Address:

File Name	File Size	Generation Time

Note: If you do not specify addresses and ports, all the ports and addresses of the specified type will apply.

2. Click **Start** to start capturing packets. Click **Stop** after a time and check the captured packets.



File Name	File Size	Generation Time
capture_file_0.cap	2.25 KB	Thu Jan 10 14:32:09 2019

3. Click 📥 next to a packet to download it for analysis. Open the file in Wireshark.

34 Route Tracking

34.1 Overview

The route tracking function allows you to check packet processing on a firewall to facilitate configuration and management. You can simulate packet processing on a firewall and locate problems based on the results to adjust configurations accordingly and get to know the firewall's processing performance.

The results of route tracking include the function modules that process the simulated packet and the processing outcome.

The supported function modules include security policy match, address pool call, session control policy match, protection policy match, user authentication policy match, traffic or connections limit check result, NAT, and route query result.

The results of route tracking only show the function modules that process the simulated packet.

34.2 Configuration

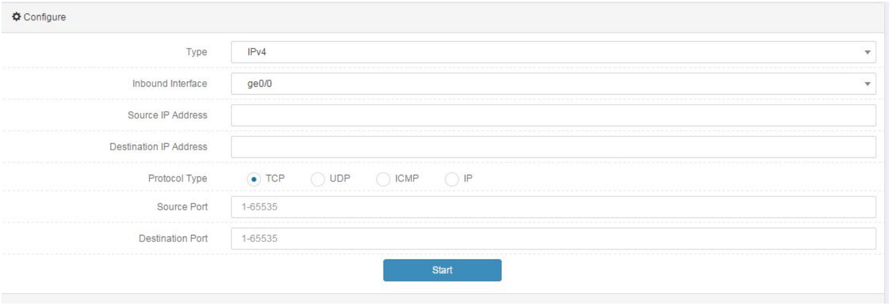
34.2.1 Configuring the Basic Elements of Route Tracking

The basic elements of route tracking are the address type, inbound interface, source address, destination address, and protocol type of data flows. The configuration varies depending on different protocol types.

You must specify all the basic elements to simulate a packet.

Procedure:

1. Choose **Network** > **Network debugging** > **Route tracking**. The following page appears.



Configure

Type: IPv4

Inbound Interface: ge0/0

Source IP Address:

Destination IP Address:

Protocol Type: ● TCP ○ UDP ○ ICMP ○ IP

Source Port: 1-65535

Destination Port: 1-65535

Parameter description:

Type: Protocol type of a packet. The options are **IPv4** and **IPv6.**

Inbound interface: Inbound direction of the packet. You can enter a physical interface, VLAN interface, or trunk interface.

Source address: Source address of the packet.

Destination address: Destination address of the packet.

Protocol type: Layer-4 protocol type of the packet. The options are **TCP**, **UDP**, **ICMP**, and **IP.**

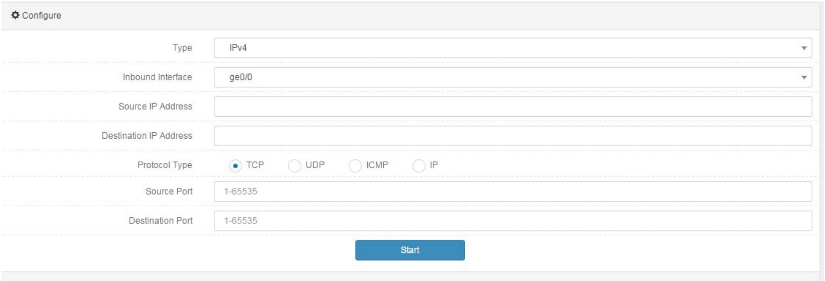
2. Click **Start** after you complete the settings.

34.2.2 Configuring TCP or UDP Route Tracking

When configuring TCP or UDP route tracking, specify **Source port** and **Destination port.**

Procedure:

1. Choose **Network** > **Network debugging** > **Route tracking**, and select **TCP** or **UDP** for **Protocol type**, as shown in the following figure.



Configure

Type: IPv4

Inbound Interface: ge0/0

Source IP Address:

Destination IP Address:

Protocol Type: ● TCP ○ UDP ○ ICMP ○ IP

Source Port: 1-65535

Destination Port: 1-65535

Source port: Source port number of the packet.

Destination port: Destination port number of the packet.

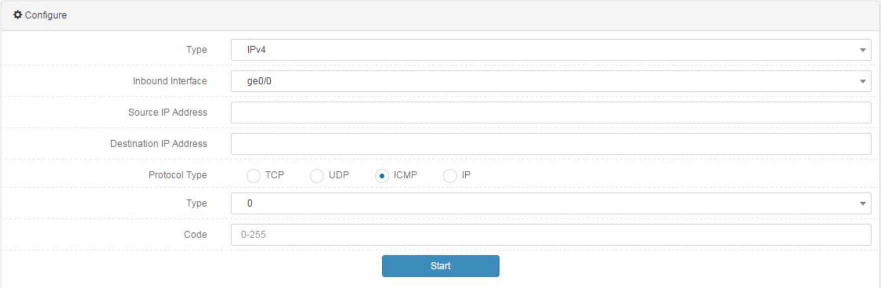
2. Click **Start**.

34.2.3 Configuring ICMP Route Tracking

When configuring ICMP route tracking, specify **Type** and **Code**.

Procedure:

1. Choose **Network** > **Network debugging** > **Route tracking**, and select **ICMP** for **Protocol type**, as shown in the following figure.



Configure

Type	IPv4
Inbound Interface	ge0/0
Source IP Address	
Destination IP Address	
Protocol Type	○ TCP ○ UDP ● ICMP ○ IP
Type	0
Code	0-255

Type: ICMP packet type.

Code: ICMP packet code.

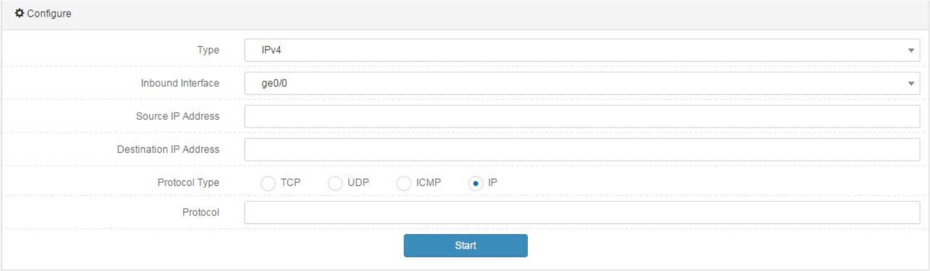
2. Click **Start**.

34.2.4 Configuring IP Route Tracking

When configuring IP route tracking, specify **Protocol**.

Procedure:

1. Choose **Network** > **Network debugging** > **Route tracking**, and select **IP** for **Protocol type**, as shown in the following figure.



Configure

Type	IPv4
Inbound Interface	ge0/0
Source IP Address	
Destination IP Address	
Protocol Type	○ TCP ○ UDP ○ ICMP ● IP
Protocol	

Protocol: Layer-4 protocol number of the data flow. The value ranges from 1 to 255.

2. Click **Start**.

34.3 Configuration Examples

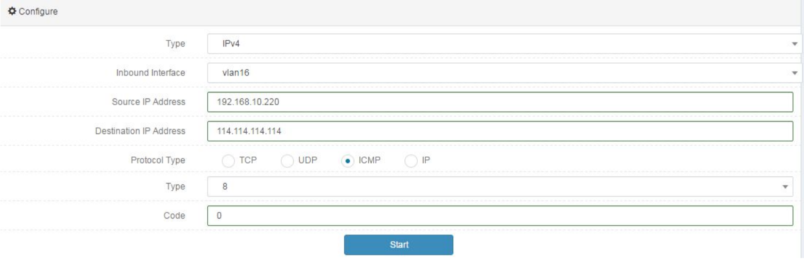
34.3.1 Example 1: Configuring IPv4 Route Tracking

Description:

Configure IPv4 route tracking to simulate a ping packet sent from 192.168.10.220 to 114.114.114.114

Procedure:

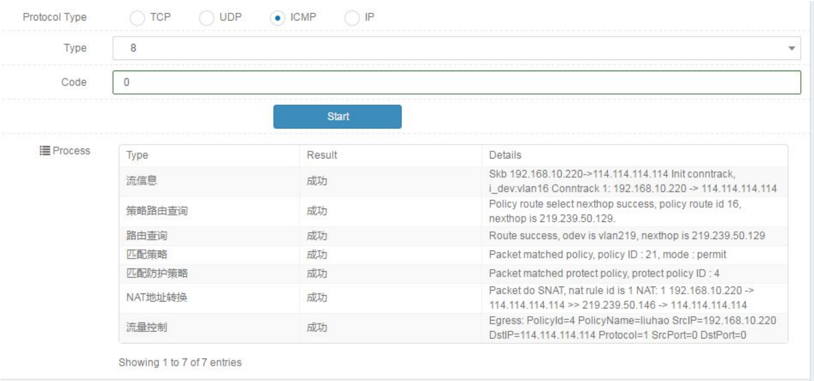
1. Choose **Network** > **Network debugging** > **Route tracking**. Select **ICMP** for **Protocol type** and set other parameters, as shown in the following figure.



Configure

Type	IPv4
Inbound Interface	vlan16
Source IP Address	192.168.10.220
Destination IP Address	114.114.114.114
Protocol Type	○ TCP ○ UDP ● ICMP ○ IP
Type	8
Code	0

2. Click **Start** after you complete the settings, as shown in the following figure.



Protocol Type	○ TCP ○ UDP ● ICMP ○ IP
Type	8
Code	0

Process

Type	Result	Details
流信息	成功	Skb 192.168.10.220->114.114.114.114 Init conntrack, i_dev:vlan16 Conntrack 1: 192.168.10.220 -> 114.114.114.114
策略路由查询	成功	Policy route select nexthop success, policy route id 16, nexthop is 219.239.50.129.
路由查询	成功	Route success, odev is vlan219, nexthop is 219.239.50.129
匹配策略	成功	Packet matched policy, policy ID : 21, mode : permit
匹配防护策略	成功	Packet matched protect policy, protect policy ID : 4
NAT地址转换	成功	Packet do SNAT, nat rule id is 1 NAT: 1 192.168.10.220 -> 114.114.114.114 >> 219.239.50.146 -> 114.114.114.114
流量控制	成功	Egress: PolicyId=4 PolicyName=liuhao SrcIP=192.168.10.220 DstIP=114.114.114.114 Protocol=1 SrcPort=0 DstPort=0

Showing 1 to 7 of 7 entries

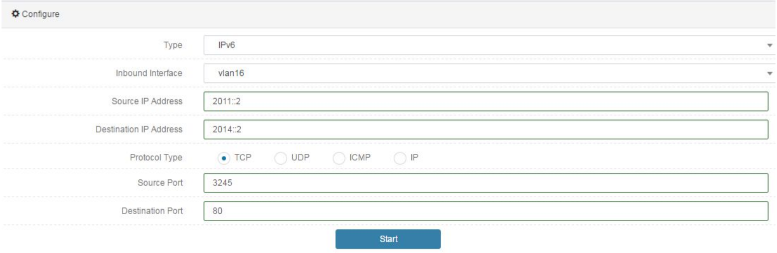
34.3.2 Example 2: Configuring IPv6 Route Tracking

Description:

Configure IPv6 route tracking to simulate a packet sent from 2011::4 to port 80 of 2014::2.

Procedure:

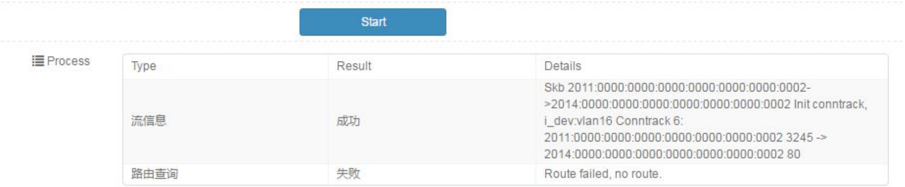
1. Choose **Network** > **Network debugging** > **Route tracking**. Select **TCP** for **Protocol type** and set other parameters, as shown in the following figure.



Configure

Type	IPv6
Inbound Interface	vlan16
Source IP Address	2011::2
Destination IP Address	2014::2
Protocol Type	● TCP ○ UDP ○ ICMP ○ IP
Source Port	3245
Destination Port	80

2. Click **Start** after you complete the settings, as shown in the following figure.



Type	Result	Details
流信息	成功	Skb 2011:0000:0000:0000:0000:0000:0000:0002->2014:0000:0000:0000:0000:0000:0000:0002 Init conntrack, i_dev:vlan16 Conntrack 6: 2011:0000:0000:0000:0000:0000:0000:0002 3245 -> 2014:0000:0000:0000:0000:0000:0000:0002 80
路由查询	失败	Route failed, no route.

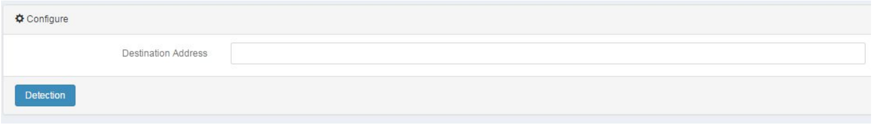
35 PMTU

35.1 Overview

Path maximum transmission unit (PMTU) is a method of discovering the supported MTU on a path to a specified destination IP address.

35.2 Configuration

Choose **Network** > **Network debugging** > **PMTU**. The following page appears.



Destination address: Enter the destination address to be detected based on a specific address type.

Detect: Click this button to start detection.

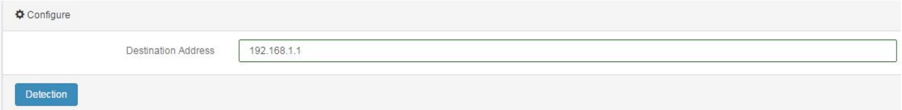
35.3 Configuration Example

Description:

Discover the MTU on the path to 192.168.1.1.

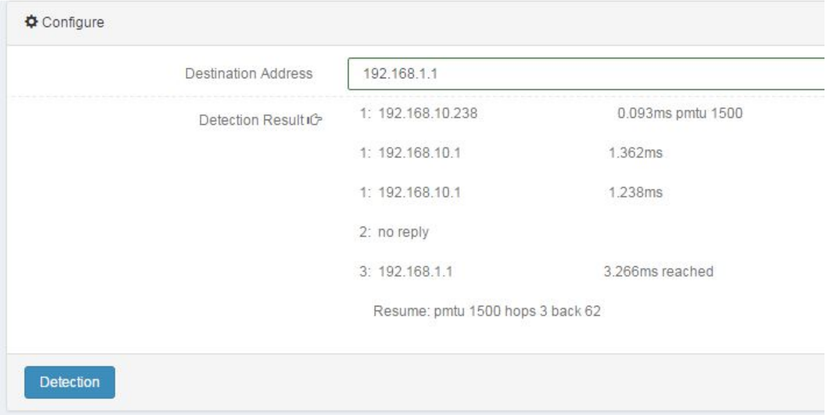
Procedure:

1. Choose **Network** > **Network debugging** > **PMTU**. Set **Destination address**.



Destination Address 192.168.1.1

2. Click **Detect**. The following figure shows the detection results.



192.168.1.1

```
1:  192.168.10.238            0.093ms pmtu 1500
1:  192.168.10.1              1.362ms
1:  192.168.10.1              1.238ms
2:  no reply
3:  192.168.1.1               3.266ms reached
    Resume: pmtu 1500 hops 3 back 62
```

36 Firewall Policy

36.1 Overview

The firewall policy feature is introduced to control data flows centrally and facilitate configuration and management.

You can configure firewall policies to effectively control and manage the data flows passing a firewall. When receiving a packet, the firewall matches the packet's inbound interface, source address, destination address, protocol, service, user, and application information to the configured policies to determine whether to establish a data flow. The firewall associates the data flow with the hit policy to determine whether to allow or drop subsequent packets and what users and data can pass the firewall and the passing time and place.

Firewall policies are matched from top down as listed on page. Only the packets passing the firewall are processed, whereas the packets sent by the firewall are not limited.

To verify that a firewall policy takes effect, you can check its hit count. If traffic hits a policy, the hit count increases by 1.

36.2 Configuration

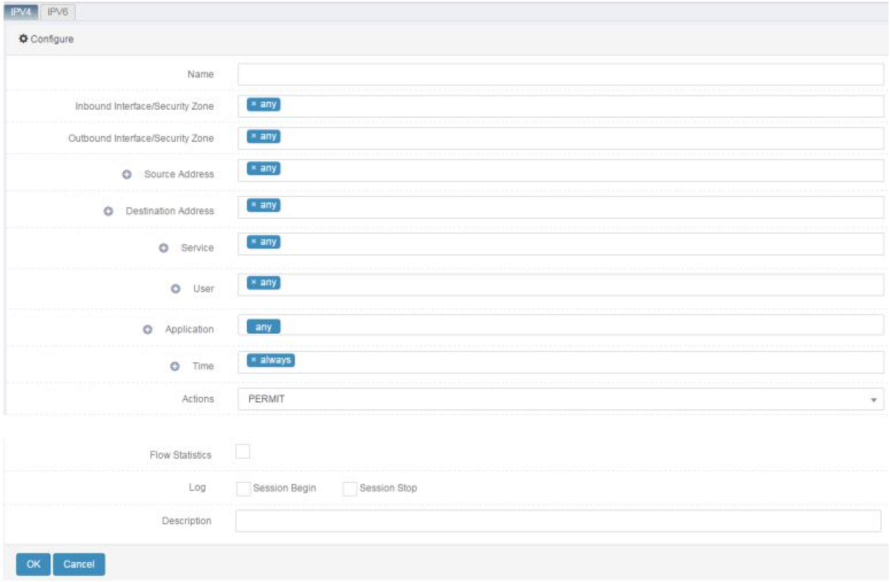
36.2.1 Configuring Basic Policy Elements

The basic elements of a firewall policy are the match conditions and action. Match conditions include the data flow direction, source address, destination address, service, user, application, and policy effective period. The data flow direction is determined by the inbound interface, outbound interface, source address, and destination address. Service, user, application, and policy effective period can reference predefined objects.

Policy actions include Permit and Deny, which have different optional configurations to determine the services applied to the data flow that meet the match conditions.

Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. Select **IPv4** or **IPv6** and click **New** to create a firewall policy.



Name	
Inbound Interface/Security Zone	any
Outbound Interface/Security Zone	any
Source Address	any
Destination Address	any
Service	any
User	any
Application	any
Time	always
Actions	PERMIT
Flow Statistics	□
Log	□ Session Begin □ Session Stop
Description	

Parameter description:

Name: Name of the new firewall policy, which must be unique. If the name is specified, ensure that different policies have different names.

Inbound interface: Inbound direction of a data flow. You can specify an interface. The option **any** indicates all interfaces.

Outbound interface: Outbound direction of the data flow. You can specify an interface. The option **any** indicates all interfaces.

Source address: Source address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates all objects.

Destination address: Destination address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates all objects.

Service: Service attributes of the data flow, including the protocol, source port, and destination port. You can reference a predefined service, a custom service object or service object group. The option **any** indicates all objects.

User: User attribute of the data flow. You can reference a predefined authentication user or user group. The option **any** indicates all user objects. **Application**: Application attribute of the data flow. You can reference a predefined application, a custom application object or application object group. The option **any** indicates all applications.

Time: Policy effective time. You can reference an existing time object. The option **always** indicates all time points.

Action: Action taken for the data flow if it meets the match conditions. The options are **PERMIT** and **DENY**.

Traffic statistics: This parameter is available only when **Action** is set to **PERMIT**. Statistics are collected on the traffic that hits the policy. You can check the statistics on **Monitor** > **Session** > **Traffic statistics** > **Based on firewall policy**.

Log: When **Action** is set to **PERMIT**, this parameter enables logging of session initiation and completion. When **Action** is set to **DENY**, this parameter enables logging of the Deny action.

(Optional) **Description**: Description about the firewall policy, no more than 127 characters.

2. Click **Submit** after you complete the settings.

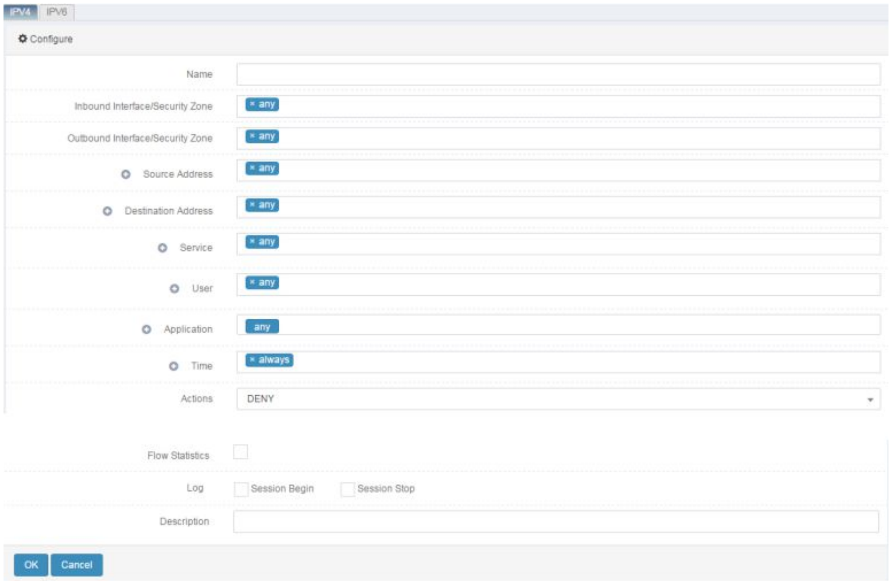
Note

1. When creating a firewall policy, ensure that the referenced address object type is consistent with the policy protocol type.
2. A maximum of 16 objects can be referenced by each match condition of a firewall policy.
3. An ID is automatically generated to uniquely identify the firewall policy. The IDs of firewall policies of different protocol types are independent of each other.

36.2.2 Configuring a Deny Policy

Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. Click **New** and select **DENY** for **Action**.



IPV4 IPV6

Configure

Name

Inbound Interface/Security Zone: any

Outbound Interface/Security Zone: any

Source Address: any

Destination Address: any

Service: any

User: any

Application: any

Time: always

Actions: DENY

Flow Statistics □

Log □ Session Begin □ Session Stop

Description

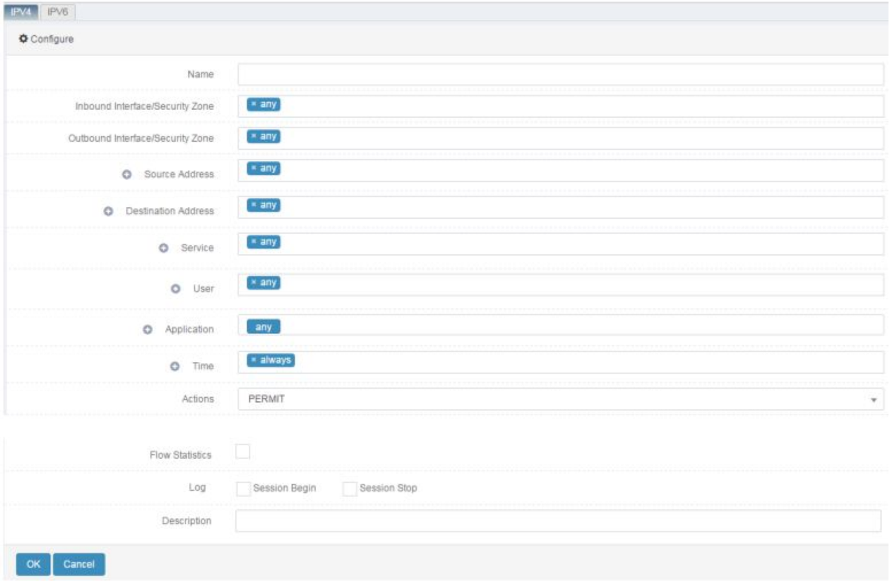
Log: Check this box to enable logging. If the data flow hits the policy, the block information will be sent to a syslog server or a device-level local log will be generated. The log priority is Info.

2. Click **Submit**.

36.2.3 Configuring a Permit Policy

Procedure:

Choose **Policy** > **Firewall** > **Policy**. Click **New** and select **PERMIT** for **Action**.



Name	
Inbound Interface/Security Zone	× any
Outbound Interface/Security Zone	× any
Source Address	× any
Destination Address	× any
Service	× any
User	× any
Application	any
Time	× always
Actions	PERMIT
Flow Statistics	□
Log	□ Session Begin □ Session Stop
Description	

Log: Check this box to enable logging. If the data flow hits the policy, the flow setup and release information will be sent to a syslog server or a device -level local log will be generated. The log priority is Info.

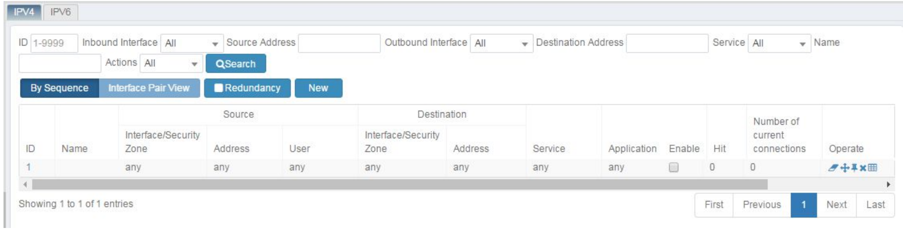
Traffic statistics: Statistics are collected on the traffic that hits the policy. You can check the statistics on **Monitor** > **Session** > **Traffic statistics** > **Based on firewall policy**.

36.2.4 Enabling a Firewall Policy

After configuring a firewall policy, enable it to make it effective.

Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. The following page appears.



		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
1		any	any	any	any	any	any	any	□	0	0	

Showing 1 to 1 of 1 entries

2. Check the **Enable** box next to a firewall policy to enable it.

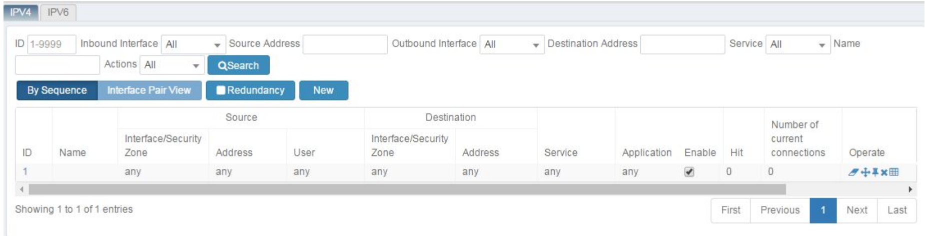
Notice

By default, a firewall policy is in the disabled state after being configured. It must be enabled manually to take effect.

36.2.5 Modifying a Firewall Policy

Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. Click a policy ID.



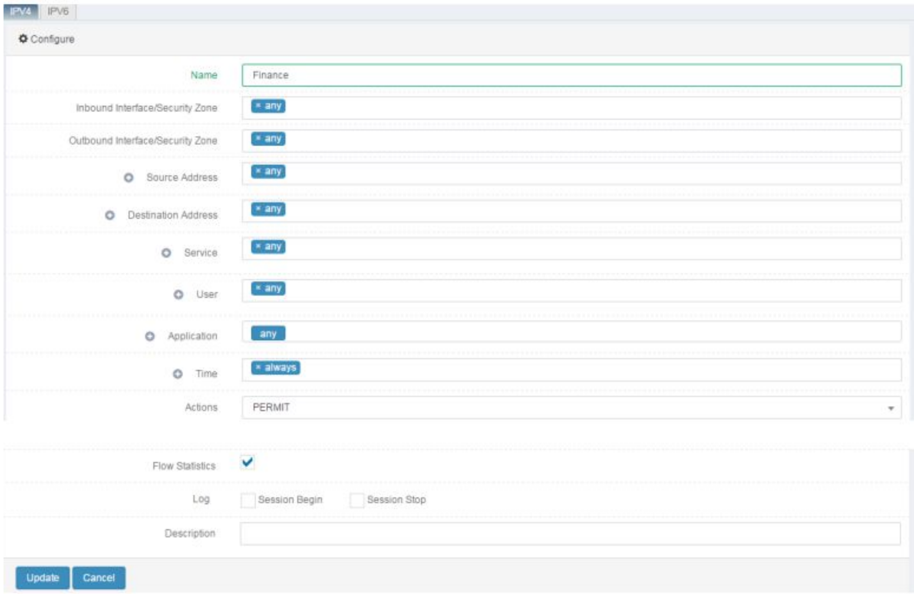
ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name

Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
1		any	any	any	any	any	any	any	☑	0	0	

Showing 1 to 1 of 1 entries

2. Modify the information about the firewall policy. Click **Update** to apply the modification.

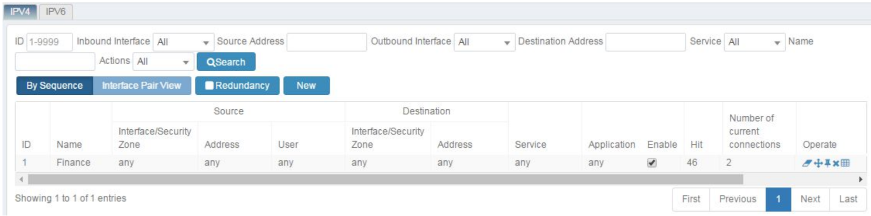


Name	Finance
Inbound Interface/Security Zone	any
Outbound Interface/Security Zone	any
Source Address	any
Destination Address	any
Service	any
User	any
Application	any
Time	always
Actions	PERMIT
Flow Statistics	☑
Log	□ Session Begin □ Session Stop
Description	

36.2.6 Deleting a Firewall Policy

Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. The following page appears.



		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
1	Finance	any	any	any	any	any	any	any	☑	46	2	

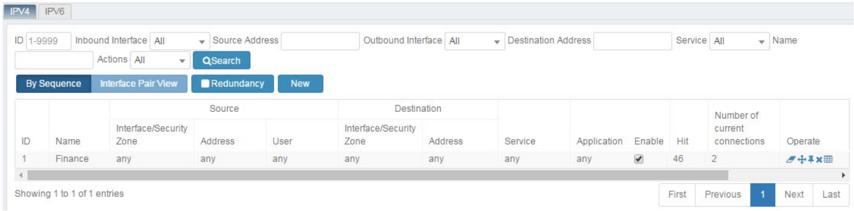
2. Click ✖ next to the firewall policy you want to delete.

36.2.7 Adjusting the Order of Firewall Policies

You can change the match priorities of firewall policies by adjusting their order. Policies are matched from top down as listed on page.

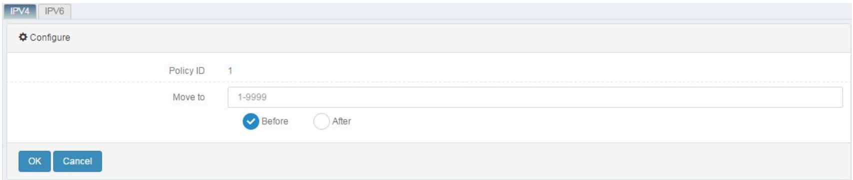
Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. The following page appears.



		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
1	Finance	any	any	any	any	any	any	any	☑	46	2	

2. Click ✥ next to the policy you want to move.



Policy ID 1

Move to 1-9999

● Before ○ After

Policy ID: ID of the policy to be moved.

Move to: ID of the reference policy.

Before: Move the policy before the reference policy.

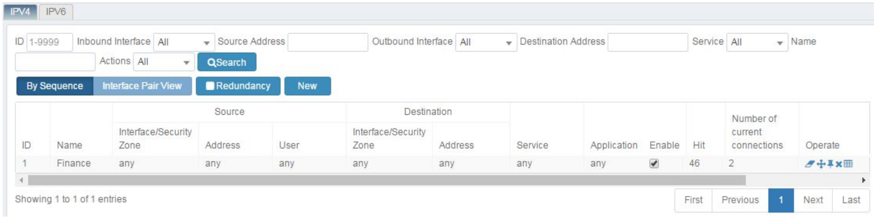
After: Move the policy after the reference policy.

3. Click **Submit**.

36.2.8 Inserting a Firewall Policy

Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. The following page appears.

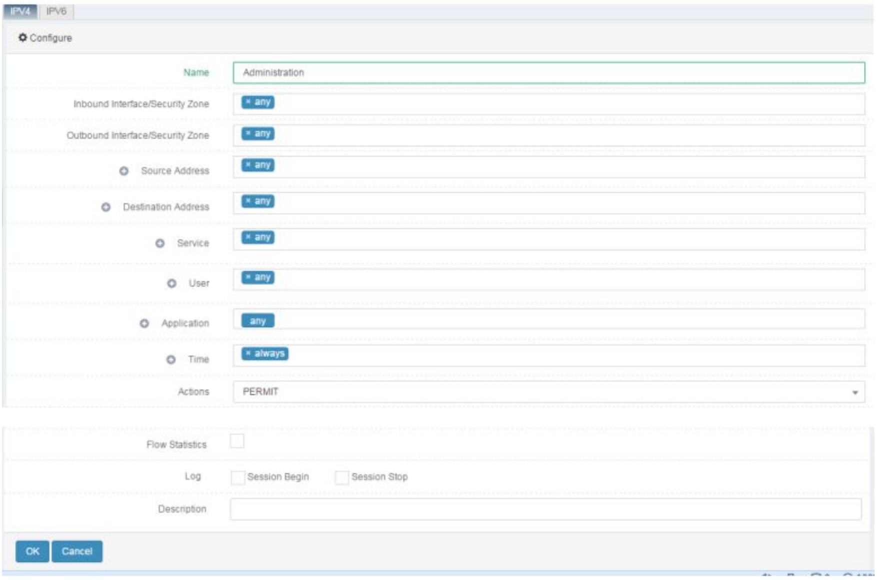


ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name
Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
1	Finance	any	any	any	any	any	any	any	☑	46	2	

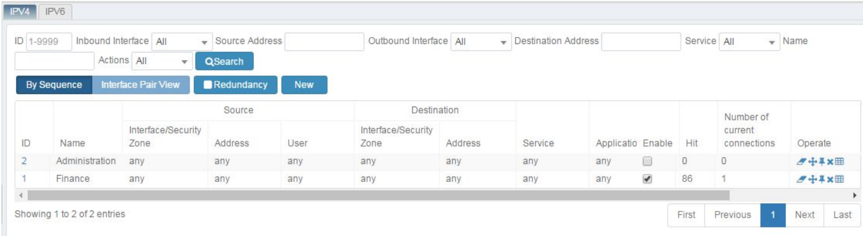
Showing 1 to 1 of 1 entries

2. Click to insert a new firewall policy before the reference policy.



Name	Administration
Inbound Interface/Security Zone	any
Outbound Interface/Security Zone	any
Source Address	any
Destination Address	any
Service	any
User	any
Application	any
Time	always
Actions	PERMIT
Flow Statistics	□
Log	□ Session Begin □ Session Stop
Description	

3. Click **OK**. The following page appears.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name
Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Applicatio	Enable	Hit	Number of current connections	Operate
2	Administration	any	any	any	any	any	any	any	□	0	0	
1	Finance	any	any	any	any	any	any	any	☑	86	1	

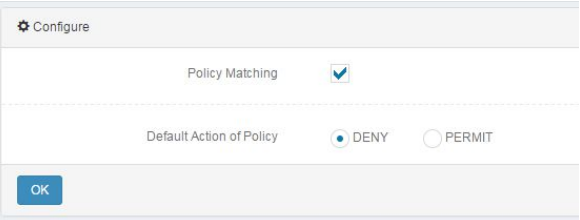
Showing 1 to 2 of 2 entries

36.2.9 Setting the Policy Configuration Module

The policy configuration module allows you to enable or disable the policy match module and set the default action taken when no policy is hit.

Procedure:

1. Choose **Policy** > **Firewall** > **Policy configuration**. The following page appears.

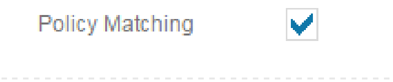


Configure

Policy Matching ☑

Default Action of Policy ● DENY ○ PERMIT

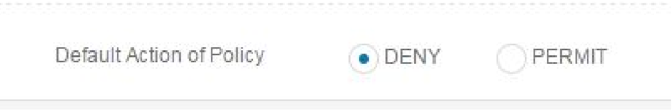
2. Check or uncheck the **Policy match** box to enable or disable the policy match module.



Policy Matching ☑

After the policy match module is enabled, all the packets passing the system are matched with the firewall policies. If the module is disabled, policy match is not performed.

3. Select **PERMIT** or **DENY** for **Policy default action**, which specifies the action to be taken when no firewall policy is hit.



Default Action of Policy ● DENY ○ PERMIT

Notice

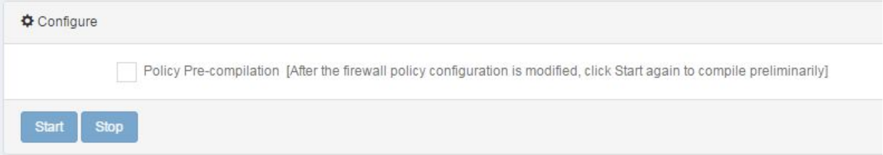
By default, policy match is enabled and the action is Deny.

36.2.10 Setting the Policy Precompiling Module

The policy precompiling module allows you to enable or disable the firewall policy precompiling function. By default, this function is disabled. When many firewall policies exist, the policy precompiling function can improve the policy match performance.

Procedure:

1. Choose **Policy** > **Firewall** > **Policy precompiling**. The following page appears.



Configure

□ Policy Pre-compilation [After the firewall policy configuration is modified, click Start again to compile preliminarily]

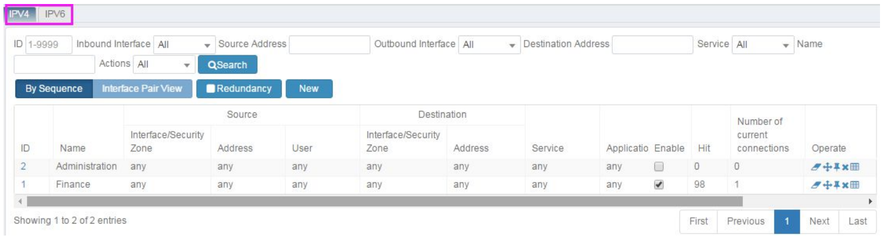
2. Check or uncheck the **Policy precompiling** box to enable or disable the policy precompiling function. You can check this box and click **Start** to precompile the existing firewall policy configurations. Click **Stop** to release the compiled policy configurations, and the default match mode applies.

> ⚠ Notice
>
> After the firewall policy configurations are modified, click **Start** to start precompiling.

36.3 Monitoring and Maintenance

36.3.1 Displaying Firewall Policies by Protocol Type

Choose **Policy** > **Firewall** > **Policy** to display existing firewall policies by protocol type.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name Actions All

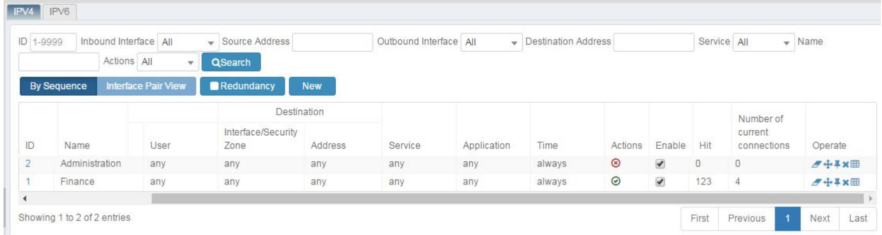
		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Applicatio	Enable	Hit	Number of current connections	Operate
2	Administration	any	any	any	any	any	any	any	□	0	0	✎ ✥ 📌 × ▦
1	Finance	any	any	any	any	any	any	any	☑	98	1	✎ ✥ 📌 × ▦

Showing 1 to 2 of 2 entries

36.3.2 Querying Firewall Policies

Procedure:

1. Choose **Policy** > **Firewall** > **Policy**. The following page appears.

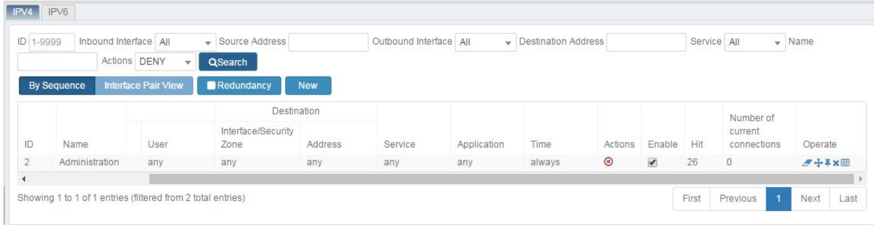


ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name Actions All

				Destination									
ID	Name		User	Interface/Security Zone	Address	Service	Application	Time	Actions	Enable	Hit	Number of current connections	Operate
2	Administration		any	any	any	any	any	always	⊗	☑	0	0	✎ ✥ 📌 × ▦
1	Finance		any	any	any	any	any	always	✓	☑	123	4	✎ ✥ 📌 × ▦

Showing 1 to 2 of 2 entries

2. Select options for **Source address**, **Destination address**, **Service**, and **Action**, and click **Search** to search for the firewall policies that match the criteria.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name

Actions DENY

			Destination									
ID	Name	User	Interface/Security Zone	Address	Service	Application	Time	Actions	Enable	Hit	Number of current connections	Operate
2	Administration	any	any	any	any	any	always	⊗	☑	26	0	

Showing 1 to 1 of 1 entries (filtered from 2 total entries)

Note

a) Fuzzy match is performed based on all the search criteria except the policy ID.

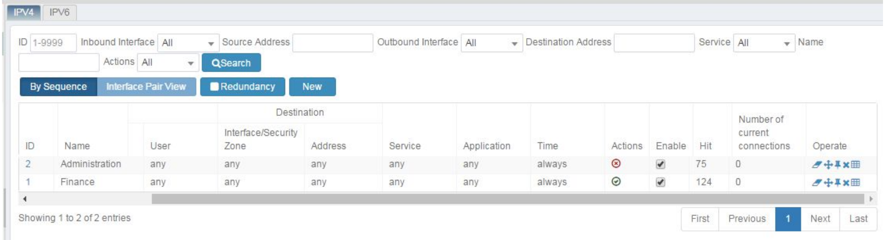
b) You can search address objects by specifying an IP address or an address object name as a search criterion.

36.3.3 Detecting Firewall Policy Redundancy

Firewall policies are matched from top down as listed on page. If a policy is not hit because it is overwritten by a previous one, such a policy is called a redundant policy. You can enable redundancy check to detect redundant firewall policies.

Procedure:

a) Choose **Policy** > **Firewall** > **Policy**. The following page appears.



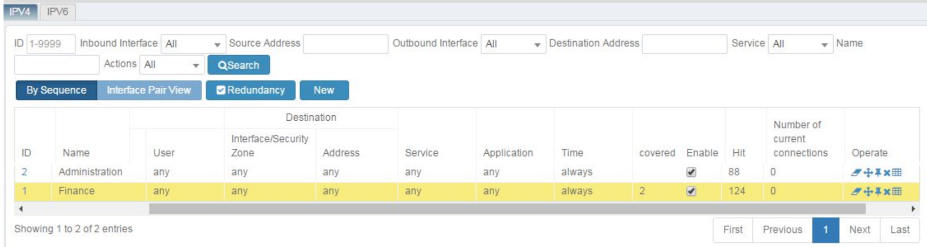
ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name

Actions All

			Destination									
ID	Name	User	Interface/Security Zone	Address	Service	Application	Time	Actions	Enable	Hit	Number of current connections	Operate
2	Administration	any	any	any	any	any	always	⊗	☑	75	0	
1	Finance	any	any	any	any	any	always	✓	☑	124	0	

Showing 1 to 2 of 2 entries

b) **Select Redundancy.**



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name

Actions All

			Destination									
ID	Name	User	Interface/Security Zone	Address	Service	Application	Time	covered	Enable	Hit	Number of current connections	Operate
2	Administration	any	any	any	any	any	always		☑	88	0	
1	Finance	any	any	any	any	any	always	2	☑	124	0	

Showing 1 to 2 of 2 entries

Notice

a) After redundancy check is enabled, a redundant policy is highlighted in yellow. Drag the horizontal scrollbar to the right to show a new column **Overwritten**, which displays the ID of the policy that overwrites the redundant policy.

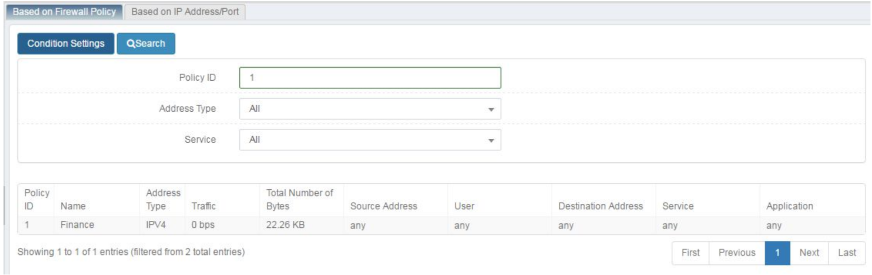
b) Redundancy check is performed on enabled firewall policies.

c) Currently redundancy check does not support union set overwriting check. It checks for redundant content among individual objects instead of treating the objects as whole, even for a policy with multiple objects.

36.3.4 Displaying Traffic Statistics

When the policy action is Permit and traffic statistics is enabled, you can go to the **Traffic statistics** page to view the traffic statistics on firewall policies.

Choose **Monitor** > **Session** > **Traffic statistics** > **Based on firewall policy** to display all the Permit policies. If a policy is enabled with traffic statistics and has a hit count, the page shows the volume and total bytes of the hit traffic, as shown in the following figure.



Policy ID: 1

Address Type: All

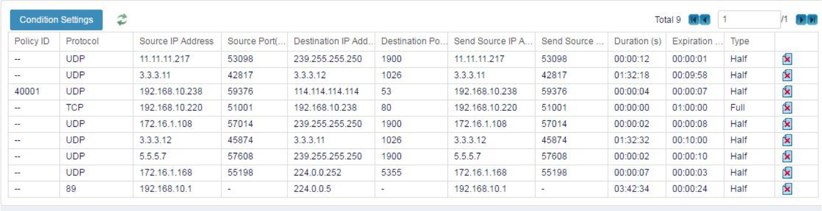
Service: All

Policy ID	Name	Address Type	Traffic	Total Number of Bytes	Source Address	User	Destination Address	Service	Application
1	Finance	IPV4	0 bps	22.26 KB	any	any	any	any	any

Showing 1 to 1 of 1 entries (filtered from 2 total entries)

36.3.5 Displaying Firewall Policies with Session Hit

Choose **Monitor** > **Session** > **Standard session** to display the session information and the policies hit by sessions, as shown in the following figure.



Policy ID	Protocol	Source IP Address	Source Port(...	Destination IP Add...	Destination Po...	Send Source IP A...	Send Source ...	Duration (s)	Expiration ...	Type	
--	UDP	11.11.11.217	53098	239.255.255.250	1900	11.11.11.217	53098	00:00:12	00:00:01	Half	☒
--	UDP	3.3.3.11	42817	3.3.3.12	1026	3.3.3.11	42817	01:32:18	00:09:58	Half	☒
40001	UDP	192.168.10.238	59376	114.114.114.114	53	192.168.10.238	59376	00:00:04	00:00:07	Half	☒
--	TCP	192.168.10.220	51001	192.168.10.238	80	192.168.10.220	51001	00:00:00	01:00:00	Full	☒
--	UDP	172.16.1.108	57014	239.255.255.250	1900	172.16.1.108	57014	00:00:02	00:00:08	Half	☒
--	UDP	3.3.3.12	45874	3.3.3.11	1026	3.3.3.12	45874	01:32:32	00:10:00	Half	☒
--	UDP	5.5.5.7	57608	239.255.255.250	1900	5.5.5.7	57608	00:00:02	00:00:10	Half	☒
--	UDP	172.16.1.168	55198	224.0.0.252	5355	172.16.1.168	55198	00:00:07	00:00:03	Half	☒
--	89	192.168.10.1	-	224.0.0.5	-	192.168.10.1	-	03:42:34	00:00:24	Half	☒

Note

1. When **Policy ID** shows **--**, the session does not hit any firewall policy.
2. When **Policy ID** shows **40000**, the session hits an intra-zone access policy of a security zone.
3. When **Policy ID** shows **40001**, the session hits the default firewall policy.

36.4 Configuration Examples

36.4.1 Example 1: Creating an IPv4 Firewall Policy

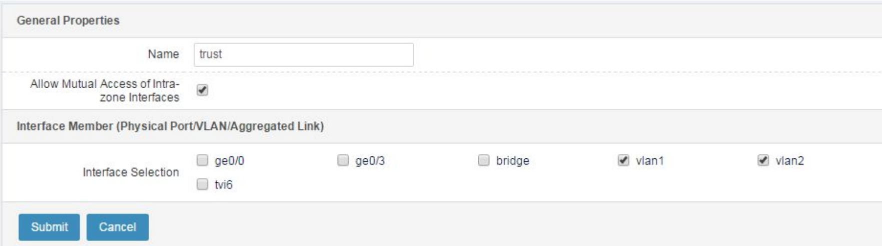
Description:

1. Add a firewall's internal interfaces vlan10, vlan20, and vlan30 to a security zone, and enable access between intra-zone interfaces.

2. Configure a policy to allow intranet users to access external FTP and HTTP services during non-work time.

Procedure:

1. Choose **Network** > **Security zone**. Add internal interfaces to security zone **trust**, and select **Allow access between intra-zone interfaces**.



General Properties

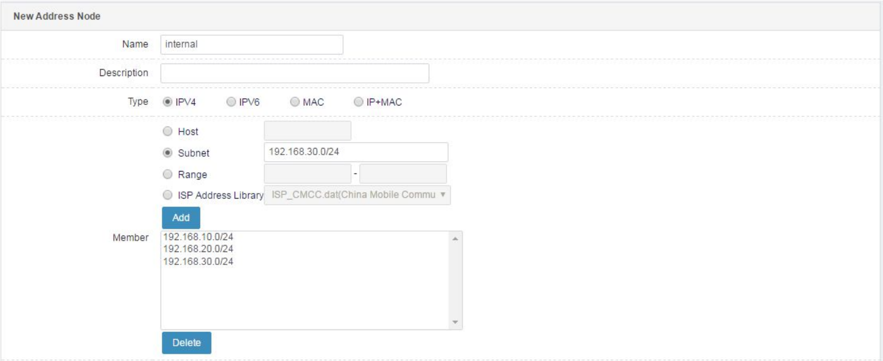
Name: trust

Allow Mutual Access of Intra-zone Interfaces ☑

Interface Member (Physical Port/VLAN/Aggregated Link)

Interface Selection: □ ge0/0 □ ge0/3 □ bridge ☑ vlan1 ☑ vlan2 □ tvi6

2. Choose **Object** > **Address object** > **Address node**, and set **Name** to **Intranet**, as shown in the following figure.



New Address Node

Name: internal

Description:

Type: ● IPV4 ○ IPV6 ○ MAC ○ IP+MAC

○ Host

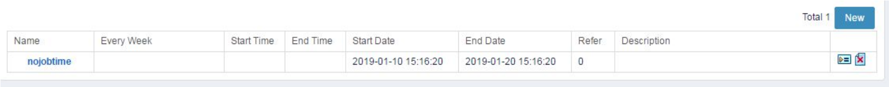
● Subnet 192.168.30.0/24

○ Range -

○ ISP Address Library ISP_CMCC.dat(China Mobile Commu ▾

Member:
192.168.10.0/24
192.168.20.0/24
192.168.30.0/24

3. Choose **Object** > **Time object** > **Cycle** to create a non-work time object, as shown in the following figure.

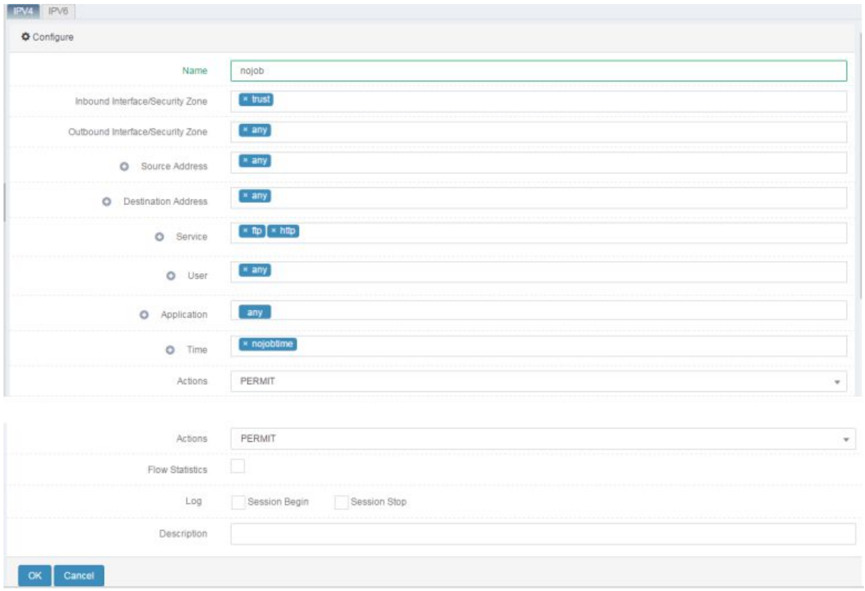


Total 1

Name	Every Week	Start Time	End Time	Start Date	End Date	Refer	Description	
nojobtime				2019-01-10 15:16:20	2019-01-20 15:16:20	0		

4. Choose **Policy** > **Firewall** > **Policy** > **IPv4**, click **New**, and set parameters,

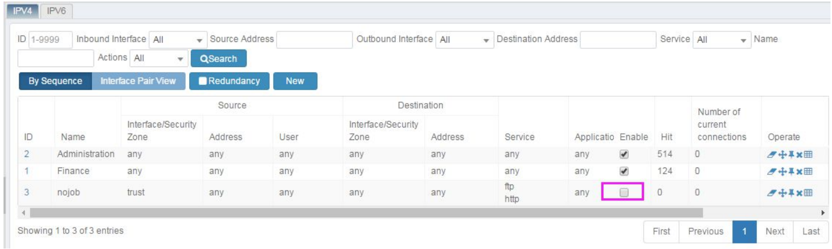
as shown in the following figure.



Name	nojob
Inbound Interface/Security Zone	× trust
Outbound Interface/Security Zone	× any
Source Address	× any
Destination Address	× any
Service	× ftp × http
User	× any
Application	any
Time	× nojobtime
Actions	PERMIT
Actions	PERMIT
Flow Statistics	□
Log	□ Session Begin □ Session Stop
Description	

5. Click **OK.**

6. Choose **Policy** > **Firewall** > **Policy.** The following page appears.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name
Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Applicatio	Enable	Hit	Number of current connections	Operate
2	Administration	any	any	any	any	any	any	any	☑	514	0	
1	Finance	any	any	any	any	any	any	any	☑	124	0	
3	nojob	trust	any	any	any	any	ftp http	any	□	0	0	

Showing 1 to 3 of 3 entries

7. Click **Enable.**

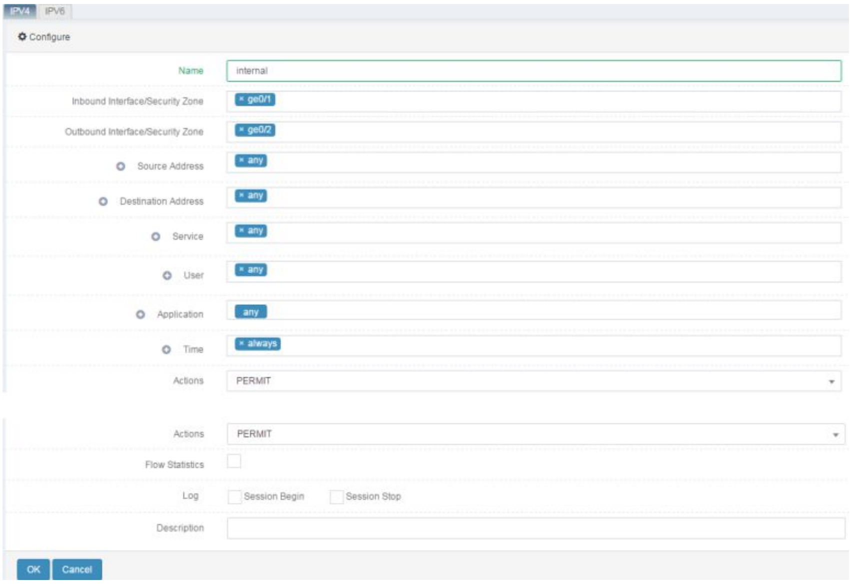
36.4.2 Example 2: Configuring Layer-2 Forwarding Control

Description:

Add a firewall's ge0/1 and ge0/2 interfaces to VLAN 100, and only permit access from ge0/1 to ge0/2.

Procedure:

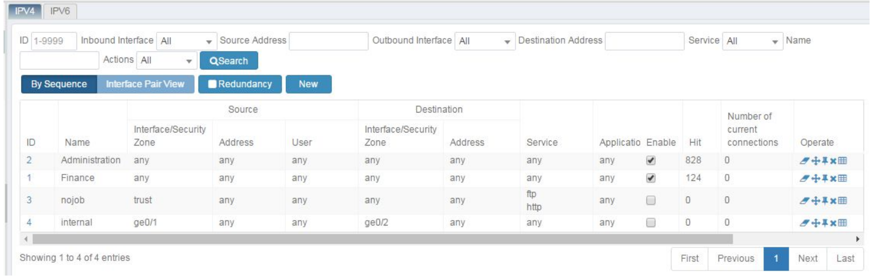
1. Choose **Policy** > **Firewall** > **Policy** > **IPv4** and click **New.** Select **ge0/1** for **Inbound interface** and **ge0/2** for **Outbound interface**, and set **Action** to **PERMIT**, as shown in the following figure.



Name	internal
Inbound Interface/Security Zone	× ge0/1
Outbound Interface/Security Zone	× ge0/2
Source Address	× any
Destination Address	× any
Service	× any
User	× any
Application	any
Time	× always
Actions	PERMIT
Actions	PERMIT
Flow Statistics	□
Log	□ Session Begin □ Session Stop
Description	

2. Click **OK**.

3. Choose **Policy** > **Firewall** > **Policy**. The following page appears.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name

Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Applicatio	Enable	Hit	Number of current connections	Operate
2	Administration	any	any	any	any	any	any	any	☑	828	0	
1	Finance	any	any	any	any	any	any	any	☑	124	0	
3	nojob	trust	any	any	any	any	ftp http	any	□	0	0	
4	internal	ge0/1	any	any	ge0/2	any	any	any	□	0	0	

Showing 1 to 4 of 4 entries

4. Click **Enable**.

36.4.3 Example 3: Configuring Firewall Policy Control for Web Authentication Users

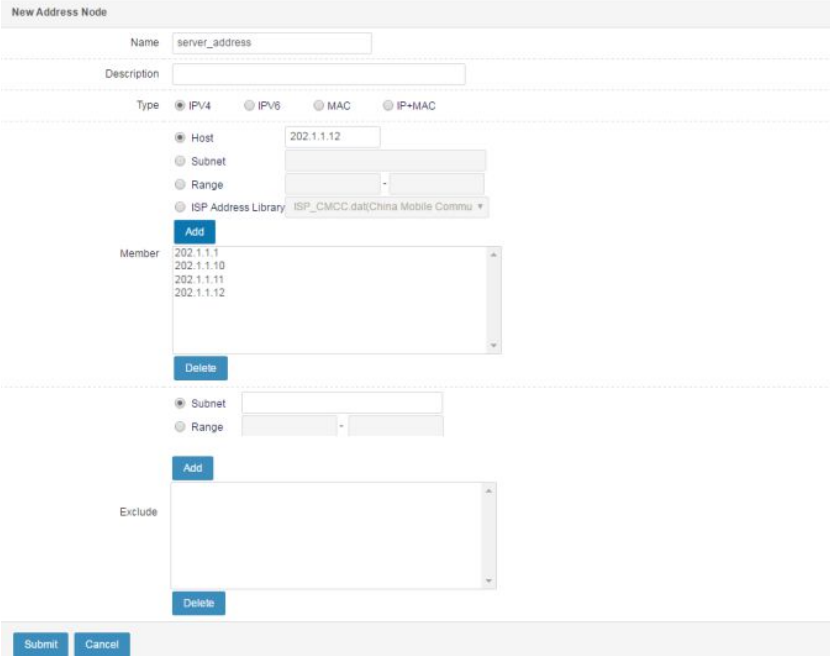
Description:

1. After user 1 and user 2 pass web authentication, allow the users only to access the internal server address.

2. Disable access control for users in group 1 after they pass authentication.

Procedure:

1. Choose **Object** > **Address object** > **Address node**. Set **Name** to **Server address** and enter the server address, as shown in the following figure.



New Address Node

Name: server_address

Description:

Type: ● IPV4 ○ IPV6 ○ MAC ○ IP+MAC

● Host 202.1.1.12
○ Subnet
○ Range -
○ ISP Address Library ISP_CMCC.dat(China Mobile Commu

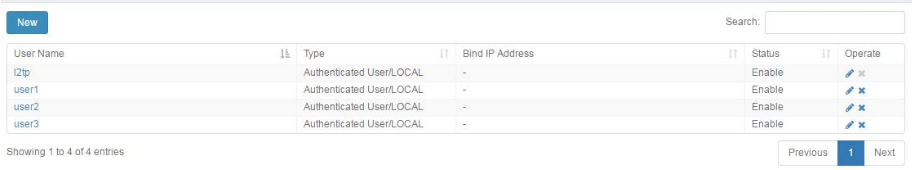
Member:

```
202.1.1.1
202.1.1.10
202.1.1.11
202.1.1.12
```

● Subnet
○ Range -

Exclude:

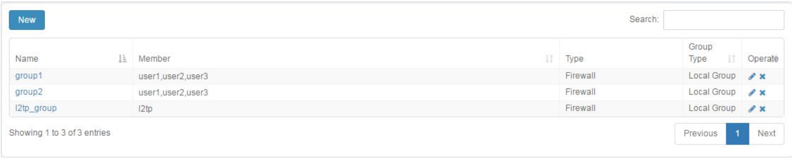
2. Choose **Object** > **User object** > **User** to create user 1, user 2, and user 3, as shown in the following figure.



User Name	Type	Bind IP Address	Status	Operate
l2tp	Authenticated User/LOCAL	-	Enable	✎ ✖
user1	Authenticated User/LOCAL	-	Enable	✎ ✖
user2	Authenticated User/LOCAL	-	Enable	✎ ✖
user3	Authenticated User/LOCAL	-	Enable	✎ ✖

Showing 1 to 4 of 4 entries

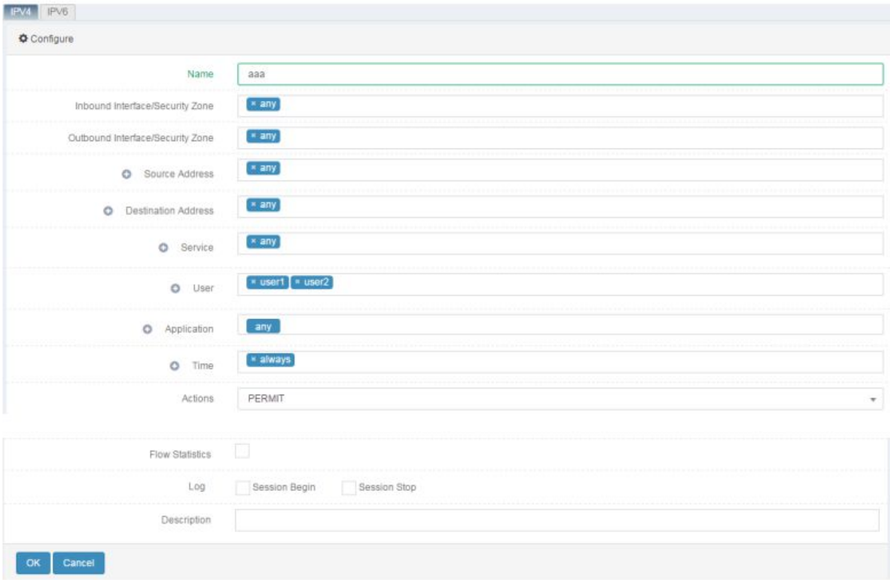
3. Choose **Object** > **User object** > **User group**. Create two user groups and add the three users to the user groups.



Name	Member	Type	Group Type	Operate
group1	user1,user2,user3	Firewall	Local Group	✎ ✖
group2	user1,user2,user3	Firewall	Local Group	✎ ✖
l2tp_group	l2tp	Firewall	Local Group	✎ ✖

Showing 1 to 3 of 3 entries

4. Choose **Policy** > **Firewall** > **Policy** and click **New**. Set parameters. Select user 1 and user 2 for **User**, and select **Server address** for **Destination address**. Configure a firewall policy that user 1 and user 2 will hit after passing authentication using group 1 and group 2.



Name: aaa

Inbound Interface/Security Zone: any

Outbound Interface/Security Zone: any

Source Address: any

Destination Address: any

Service: any

User: user1 user2

Application: any

Time: always

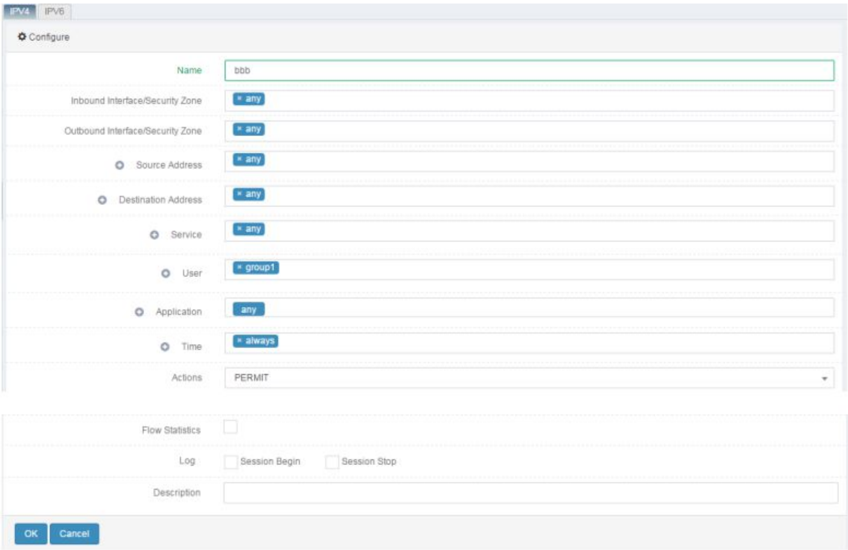
Actions: PERMIT

Flow Statistics □

Log □ Session Begin □ Session Stop

Description:

5. Choose **Policy** > **Firewall** > **Policy** and click **New.** Set parameters. Select group 1 for **User.** Configure a firewall policy that only users use group 1 for authentication will hit.



Name: bbb

Inbound Interface/Security Zone: any

Outbound Interface/Security Zone: any

Source Address: any

Destination Address: any

Service: any

User: group1

Application: any

Time: always

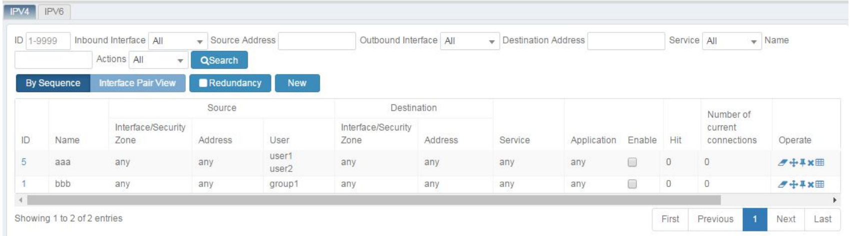
Actions: PERMIT

Flow Statistics □

Log □ Session Begin □ Session Stop

Description:

6. Choose **Policy** > **Firewall** > **Policy**. The following page appears.



ID 1-9999 Inbound Interface All Source Address Outbound Interface All Destination Address Service All Name

Actions All

		Source			Destination							
ID	Name	Interface/Security Zone	Address	User	Interface/Security Zone	Address	Service	Application	Enable	Hit	Number of current connections	Operate
5	aaa	any	any	user1 user2	any	any	any	any	□	0	0	
1	bbb	any	any	group1	any	any	any	any	□	0	0	

Showing 1 to 2 of 2 entries

7. Click **Enable**.

Notice

Before authentication, the packets such as DNS requests that must be permitted are not matched with firewall policies. Packets are matched only after users pass authentication.

36.5 Troubleshooting

36.5.1 Action Not Taken for the Data Flow That Hits a Firewall Policy

Symptom	The corresponding action (Permit or Deny) is not taken for the data flow that hits a firewall policy.
Analysis	The possible causes are as follows: 1. Policy match is not enabled. 2. The policy is not enabled. 3. Because policies are matched from top down as listed on page, the data flow may have hit a previous policy. 4. The policy takes effect for local access. 5. The policy is modified after policy precompiling is enabled.
Solution	1. Enable policy match. 2. Enable the policy. 3. Adjust the order of policies as needed. 4. Firewall policies take effect only for forwarded traffic, but not for local incoming and outgoing traffic. 5. If the policy is modified after policy precompiling is enabled but not precompiled again, the old policy is still effective. In this case, disable policy precompiling or perform policy precompiling again, and then verify policy match.

36.5.2 An Application-based Firewall Policy Is Not Matched

Symptom	permitted.
Analysis	Application identification involves a learning process. Before an application can be identified, the system does not match the policy and proceeds to the following policies. If the session does not hit a Permit policy, the application cannot be identified because the first packet is blocked.
Solution	1. Add a Permit policy to ensure that the application is permitted, properly identified, and hits a policy. 2. Application control policies are recommended to improve the effect of application-based access control.

36.5.3 Some Interfaces Cannot Be Selected for a Firewall Policy

Symptom	Inbound interface vlan20 cannot be selected for a firewall policy.
Analysis	Check whether vlan20 is added to a security zone. Firewall policies only support physical interfaces and other interfaces in security zones.
Solution	Select an interface in a security zone, or remove the interface from the security zone.

37 Protection Policy

37.1 Overview

RAVEN5000 firewalls provide the anti-attack feature to protect network devices from malicious attacks.

Security policies are used to effectively monitor data flows passing a firewall and identify malicious attacks. With security protection enabled, a firewall matches the received packet's source address, destination address, protocol, and service information with configured security policies to determine whether to perform attack detection. If attack detection is required, the firewall associates the data flow with the hit policy and skips policy matching for subsequent packets. The matched packet is processed based on the configured protective function (including anti-attack, intrusion prevention, antivirus, and web protection) to determine which packets to be permitted and which ones dropped.

If no anti-attack policy is configured, by default, the firewall does not enable policy matching for passing packets.

Security policies with the same inbound interface in the IPv4 or IPv6 format are matched from top down as listed on page. Only the packets passing the firewall are processed, whereas the packets sent by the firewall are not limited.

Intrusion prevention, antivirus, and web protection only support IPv4.

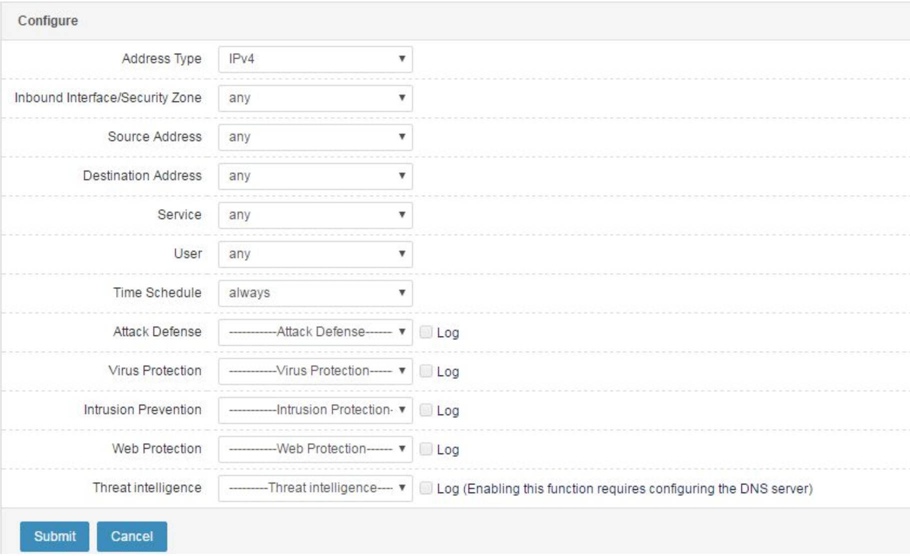
37.2 Configuration

37.2.1 Configuring Basic Policy Elements

The basic elements of a security policy are the match conditions and action. Match conditions include the data flow's inbound interface, source address, destination address, service, and policy effective period. The data flow direction is determined by the inbound interface, source address, and destination address. Service and policy effective period can reference predefined objects.

Procedure:

1. Choose **Policy** > **Security** > **Protection policy** and click **New**.



Configure

Address Type	IPv4 ▾	
Inbound Interface/Security Zone	any ▾	
Source Address	any ▾	
Destination Address	any ▾	
Service	any ▾	
User	any ▾	
Time Schedule	always ▾	
Attack Defense	----------Attack Defense------ ▾	□ Log
Virus Protection	----------Virus Protection----- ▾	□ Log
Intrusion Prevention	----------Intrusion Protection- ▾	□ Log
Web Protection	----------Web Protection------ ▾	□ Log
Threat intelligence	--------Threat intelligence---- ▾	□ Log (Enabling this function requires configuring the DNS server)

Parameter description:

Address type: Security policies are classified into IPv4 and IPv6 types. Packets are matched with policies of the corresponding protocol type.

Inbound interface: Inbound direction of a data flow. You can specify an interface. The option **any** indicates all interfaces.

Source address: Source address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Destination address: Destination address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Service: Service attributes of the data flow, including the protocol, source port, and destination port. You can reference a predefined service, a custom service object or service object group. The option **any** indicates any service.

User: User object. You can reference a predefined user object. The option **any** indicates any user object.

Time: Policy effective time. You can reference an existing time object. The option **always** indicates all time points.

Anti-attack: Enable the anti-attack feature to control matched packets and prevent flood attacks and scan attacks.

Antivirus: Implement real-time virus scan at internal and external ingresses, provide active and passive virus defense for workstations, and support file scan.

Intrusion prevention: Monitor network behaviors and protects the network by actions such as Permit, Deny, and Deny source IP address.

Web protection: Prevent XSS attacks and SQL injection attacks, and permit or deny traffic according to predefined actions.

Log: Configure log filter for the protection modules in a security policy. Logs can be recorded in the local memory, on the syslog server (log control center), and by email. A filter level can be configured for each recording mode. Only logs of the filter level or above are output.

2. Click **Submit** after you complete the settings.

Note

When creating a security policy, you must reference an address object of the same protocol type. An ID is automatically generated to uniquely identify the policy. The IDs of security policies of different protocol types are independent of each other.

Notice

Some modules generate a large amount of logs. Enable logging with caution and select a proper filter level.

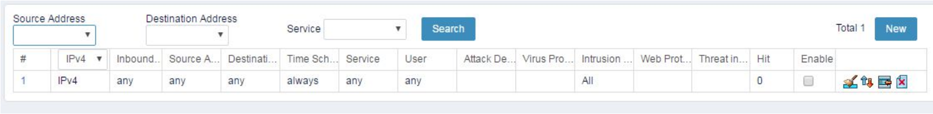
Local logs are stored in the system cache. When the cache is full, old logs are overwritten by new ones.

37.2.2 Enabling a Security Policy

After configuring a security policy, enable it to make it effective.

Procedure:

1. Choose **Policy** > **Security** > **Protection policy.** The following page appears.



Source Address ▾

Destination Address ▾

Service ▾

Search

Total 1

New

#	IPv4 ▾	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
1	IPv4	any	any	any	always	any	any			All			0	□	

2. Check the **Enable** box next to a security policy to enable it.

Notice

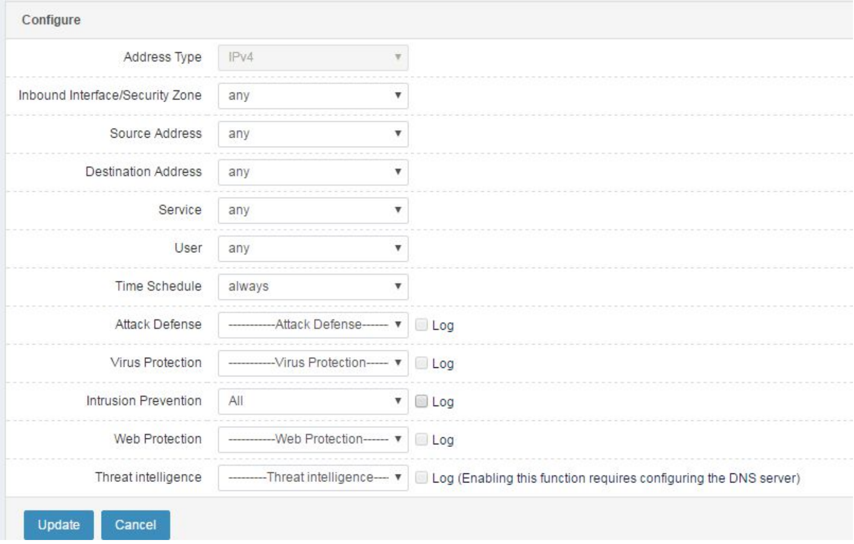
By default, a security policy is in the disabled state after being configured. It must be enabled manually to take effect.

37.2.3 Modifying a Security Policy

Procedure:

1. Choose **Policy** > **Security** > **Protection policy**. Click a policy ID.

2. Modify the information about the security policy. Click **Update** to apply the modification.



Configure

Address Type	IPv4 ▾
Inbound Interface/Security Zone	any ▾
Source Address	any ▾
Destination Address	any ▾
Service	any ▾
User	any ▾
Time Schedule	always ▾
Attack Defense	----------Attack Defense------ ▾ □ Log
Virus Protection	----------Virus Protection----- ▾ □ Log
Intrusion Prevention	All ▾ □ Log
Web Protection	----------Web Protection------ ▾ □ Log
Threat intelligence	---------Threat intelligence---- ▾ □ Log (Enabling this function requires configuring the DNS server)

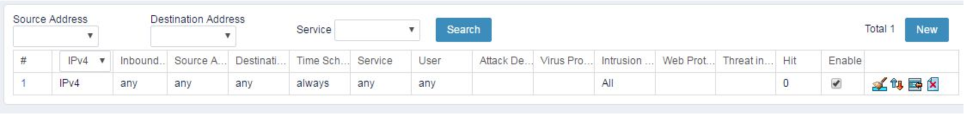
Notice

The address type cannot be changed.

37.2.4 Deleting a Security Policy

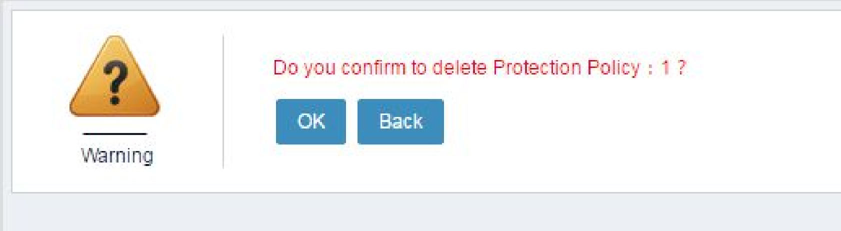
Procedure:

1. Choose **Policy** > **Security** > **Protection policy.** The following page appears.



#	IPv4 ▾	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
1	IPv4	any	any	any	always	any	any			All			0	☑	

2. Click ☒ next to the policy you want to delete. Click **OK**.



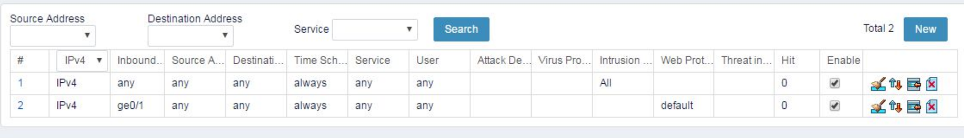
Do you confirm to delete Protection Policy : 1 ?

37.2.5 Adjusting the Order of Security Policies

You can change the match priorities of security policies by adjusting their order. Policies are matched from top down as listed on page.

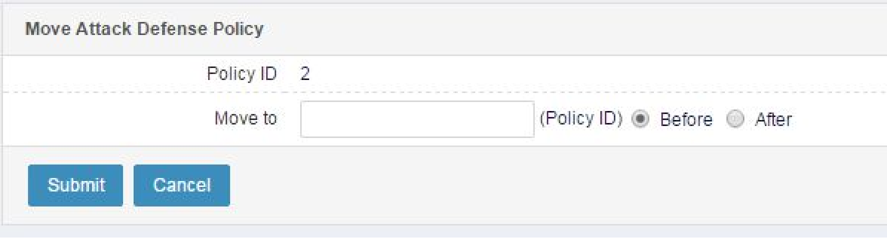
Procedure:

1. Choose **Policy** > **Security** > **Protection policy.** The following page appears.



#	IPv4	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
1	IPv4	any	any	any	always	any	any			All			0	☑	
2	IPv4	ge0/1	any	any	always	any	any				default		0	☑	

2. Click ⇅ next to the policy you want to move.



Policy ID	2
Move to	(Policy ID) ● Before ○ After

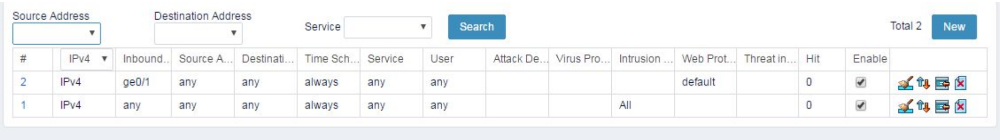
Policy ID: ID of the policy to be moved.

Move to: ID of the reference policy.

Before: Move the policy before the reference policy.

After: Move the policy after the reference policy.

3. Click **Submit**.



Source Address ▾ Destination Address ▾ Service ▾ Search Total 2 New

#	IPv4 ▾	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	any	any				default		0	☑	
1	IPv4	any	any	any	always	any	any			All			0	☑	

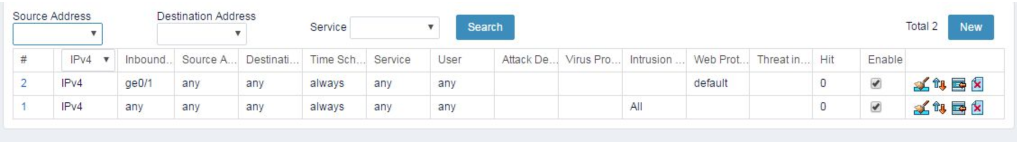
Notice

Only the order of policies of the same protocol type can be adjusted.

37.2.6 Inserting an Anti-attack Policy

Procedure:

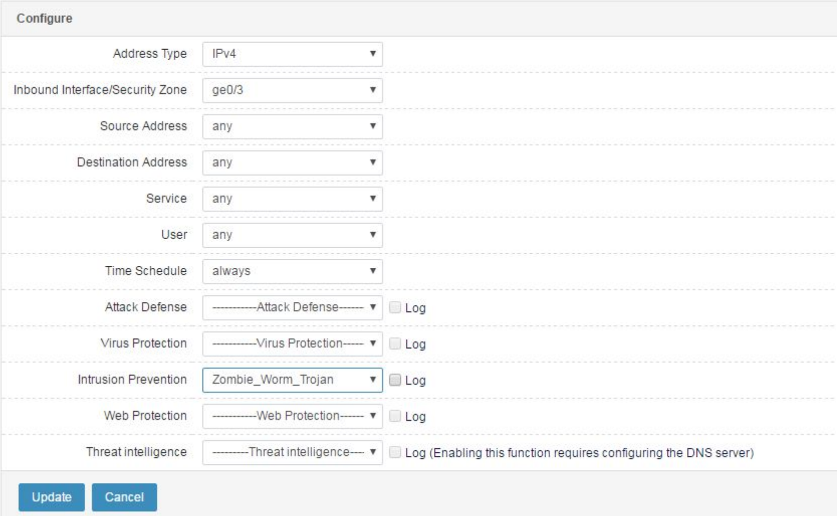
1. Choose **Policy** > **Security** > **Protection policy.** The following page appears.



Source Address ▾ Destination Address ▾ Service ▾ Search Total 2 New

#	IPv4 ▾	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	any	any				default		0	☑	
1	IPv4	any	any	any	always	any	any			All			0	☑	

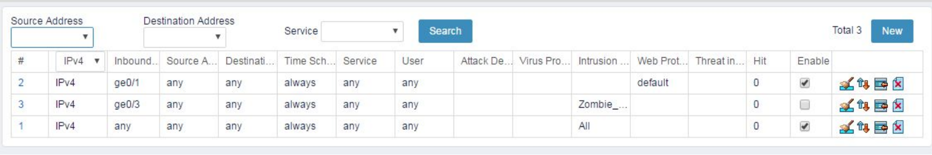
2. Click to insert a new security policy before the reference policy.



Configure

Address Type	IPv4 ▼
Inbound Interface/Security Zone	ge0/3 ▼
Source Address	any ▼
Destination Address	any ▼
Service	any ▼
User	any ▼
Time Schedule	always ▼
Attack Defense	-----------Attack Defense------ ▼ □ Log
Virus Protection	-----------Virus Protection----- ▼ □ Log
Intrusion Prevention	Zombie_Worm_Trojan ▼ □ Log
Web Protection	-----------Web Protection------ ▼ □ Log
Threat intelligence	---------Threat intelligence---- ▼ □ Log (Enabling this function requires configuring the DNS server)

3. Click **Update**.



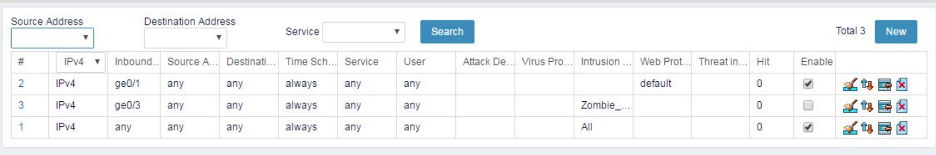
#	IPv4 ▼	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	any	any				default		0	☑	
3	IPv4	ge0/3	any	any	always	any	any			Zombie_...			0	□	
1	IPv4	any	any	any	always	any	any			All			0	☑	

> Notice
>
> The inserted policy must have the same address type, source address, and destination address as the reference policy.

37.2.7 Resetting the Hit Count of a Security Policy

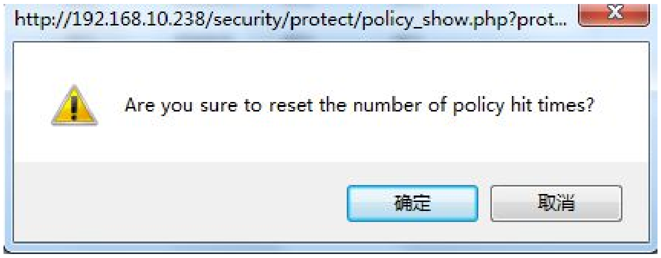
Procedure:

1. Choose **Policy** > **Security** > **Anti-attack** > **Protection policy.** The following page appears.



#	IPv4 ▼	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	any	any				default		0	☑	
3	IPv4	ge0/3	any	any	always	any	any			Zombie_...			0	□	
1	IPv4	any	any	any	always	any	any			All			0	☑	

2. Click ![reset] to reset the hit count of a policy, and click **OK** to confirm the reset operation.



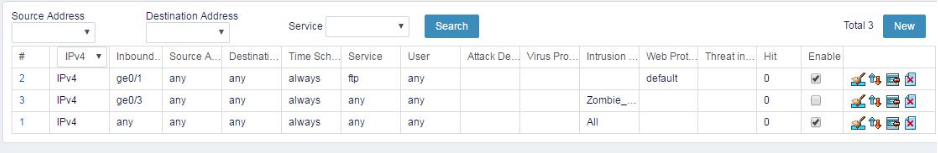
http://192.168.10.238/security/protect/policy_show.php?prot...

Are you sure to reset the number of policy hit times?

37.2.8 Querying Anti-attack Policies

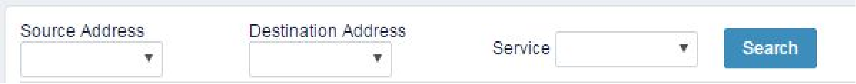
Procedure:

1. Choose **Policy** > **Security** > **Protection policy.** The following page appears.



#	IPv4	Inbound..	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	ftp	any				default		0	☑	
3	IPv4	ge0/3	any	any	always	any	any			Zombie_...			0	☐	
1	IPv4	any	any	any	always	any	any			All			0	☑	

2. Select options for **Source address**, **Destination address**, and **Service**, and click **Search** to search for the security policies that match the criteria.



37.3 Configuration Examples

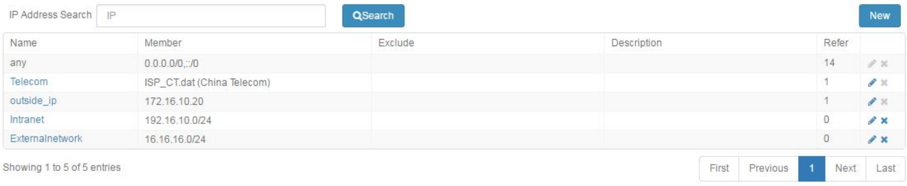
37.3.1 Example 1: Creating a Security Policy

Description:

VLAN 1 of a firewall connects to an intranet, and VLAN 2 connects to an external network. The firewall triggers TCP syncookie when the rate of TCP connection requests per source IP address sent from the external network to the intranet exceeds 100. The firewall checks whether the connection requests come from an attack source. If so, the firewall drops the requests. (Enabling syncookie may consume performance.) The firewall triggers the anti-UDP flood feature when the rate of a DNS connection request sent from the external network to an internal DNS server exceeds 2000, and the firewall drops the request. The firewall triggers the alarm function when the total rate of ICMPrequests sent from the external network to the intranet exceeds 1000. The firewall displays a message indicating the intranet may suffer ICMP attacks. Configure an anti-flood policy to monitor the network status in real time and protect the network from attacks.

Procedure:

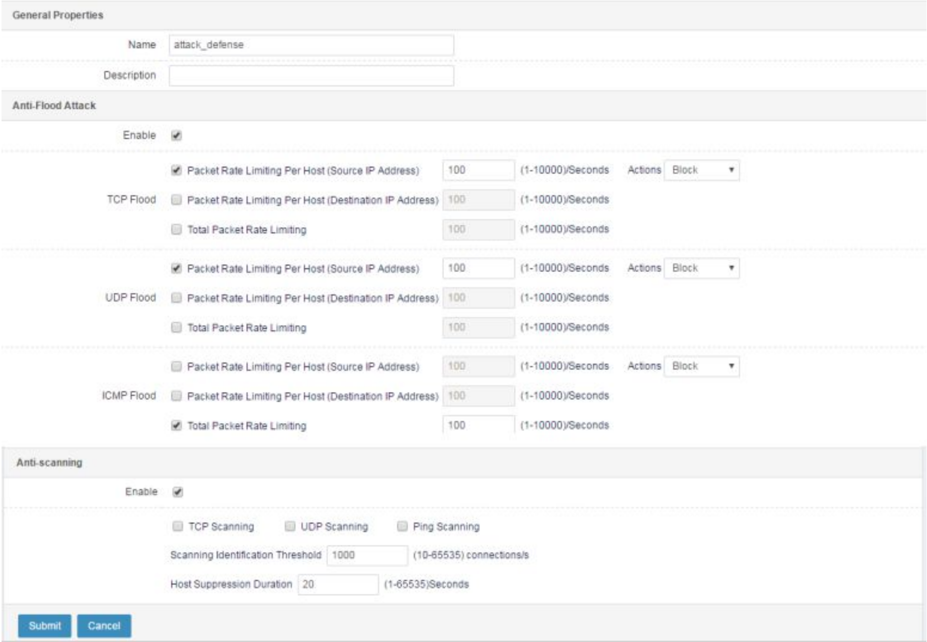
1. Choose **Object** > **Address object** > **Address node**, and configure address objects named **Intranet** and **External network**, as shown in the following figure.



Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			14
Telecom	ISP_CT.dat (China Telecom)			1
outside_ip	172.16.10.20			1
Intranet	192.16.10.0/24			0
Externalnetwork	16.16.16.0/24			0

Showing 1 to 5 of 5 entries

2. Choose **Policy** > **Security** > **Anti-attack** and click **New**.



General Properties

Name: attack_defense

Description:

Anti-Flood Attack

Enable ☑

TCP Flood
- ☑ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- ☐ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- ☐ Total Packet Rate Limiting 100 (1-10000)/Seconds

UDP Flood
- ☑ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- ☐ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- ☐ Total Packet Rate Limiting 100 (1-10000)/Seconds

ICMP Flood
- ☐ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- ☐ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- ☑ Total Packet Rate Limiting 100 (1-10000)/Seconds

Anti-scanning

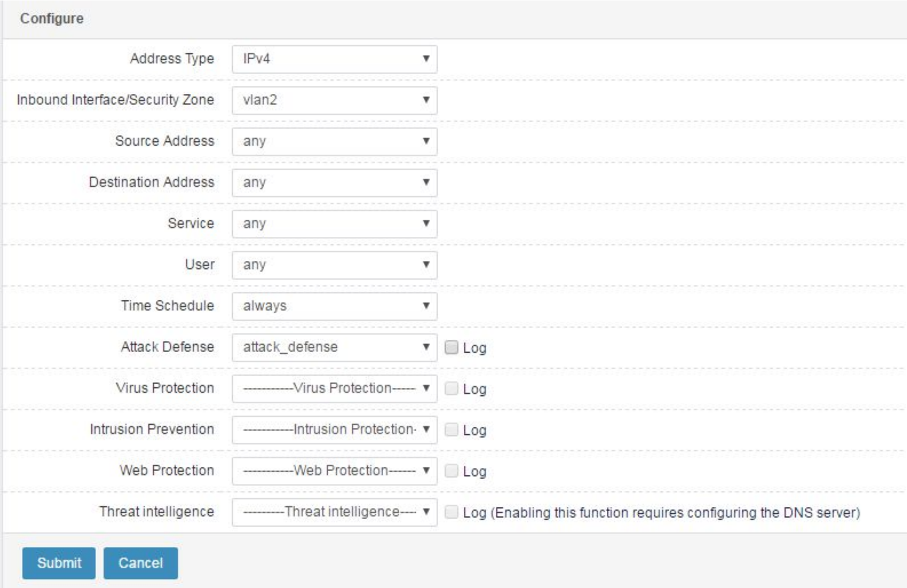
Enable ☑

☐ TCP Scanning ☐ UDP Scanning ☐ Ping Scanning

Scanning Identification Threshold 1000 (10-65535) connections/s

Host Suppression Duration 20 (1-65535)Seconds

3. Choose **Policy** > **Security** > **Protection policy** and click **New**. Set parameters, as shown in the following figure.

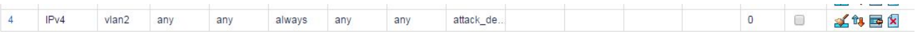


Configure

Address Type	IPv4 ▾	
Inbound Interface/Security Zone	vlan2 ▾	
Source Address	any ▾	
Destination Address	any ▾	
Service	any ▾	
User	any ▾	
Time Schedule	always ▾	
Attack Defense	attack_defense ▾	□ Log
Virus Protection	-----------Virus Protection----- ▾	□ Log
Intrusion Prevention	-----------Intrusion Protection· ▾	□ Log
Web Protection	-----------Web Protection------ ▾	□ Log
Threat intelligence	---------Threat intelligence---- ▾	□ Log (Enabling this function requires configuring the DNS server)

4. Click **Submit**.

5. Choose **Policy** > **Security** > **Protection policy.** Check the **Enable** box, as shown in the following figure.



4	IPv4	vlan2	any	any	always	any	any	attack_de..				0	□	

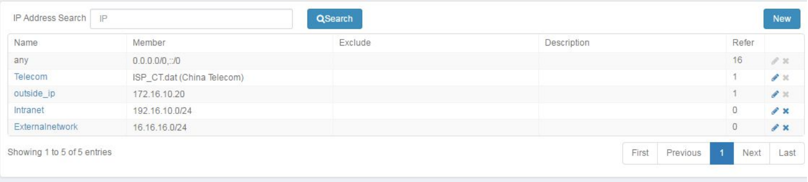
37.3.2 Example 2: Creating an Anti-scan Policy

Description:

VLAN 1 of a firewall connects to an intranet, and VLAN 2 connects to an external network. Enable an anti-scan policy on the firewall to defend against scan attacks from the external network. The firewall triggers the anti-scan feature when an external source address sends TCP or UDP connection requests to more than 1000 different ports of an internal server within 1s. All the TCP or UDP requests sent by the source address are blocked in the next 20s. The firewall triggers the anti-scan feature when an external source address sends ICMP requests to more than 1000 different internal hosts. All the ICMP requests sent by the source address are blocked in the next 20s.

Procedure:

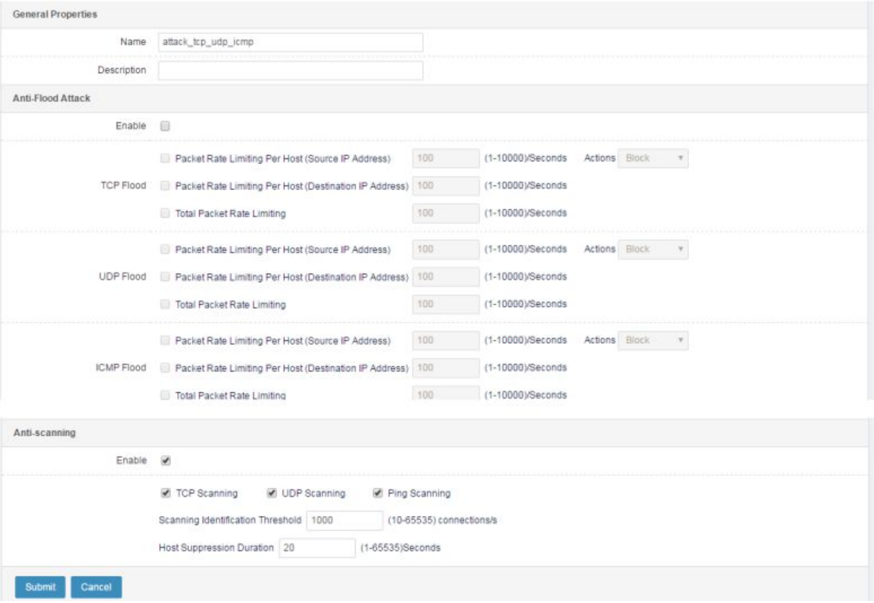
1. Choose **Object** > **Address object** > **Address node**, and configure address objects named **Intranet** and **External network**, as shown in the following figure.



Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			16
Telecom	ISP_CT.dat (China Telecom)			1
outside_ip	172.16.10.20			1
Intranet	192.16.10.0/24			0
Externalnetwork	16.16.16.0/24			0

Showing 1 to 5 of 5 entries

2. Choose **Policy** > **Security** > **Anti-attack** > **Security list** and click **New**.



General Properties

Name: attack_tcp_udp_icmp

Description:

Anti-Flood Attack

Enable □

TCP Flood	□ Packet Rate Limiting Per Host (Source IP Address)	100	(1-10000)/Seconds	Actions	Block
	□ Packet Rate Limiting Per Host (Destination IP Address)	100	(1-10000)/Seconds		
	□ Total Packet Rate Limiting	100	(1-10000)/Seconds		
UDP Flood	□ Packet Rate Limiting Per Host (Source IP Address)	100	(1-10000)/Seconds	Actions	Block
	□ Packet Rate Limiting Per Host (Destination IP Address)	100	(1-10000)/Seconds		
	□ Total Packet Rate Limiting	100	(1-10000)/Seconds		
ICMP Flood	□ Packet Rate Limiting Per Host (Source IP Address)	100	(1-10000)/Seconds	Actions	Block
	□ Packet Rate Limiting Per Host (Destination IP Address)	100	(1-10000)/Seconds		
	□ Total Packet Rate Limiting	100	(1-10000)/Seconds		

Anti-scanning

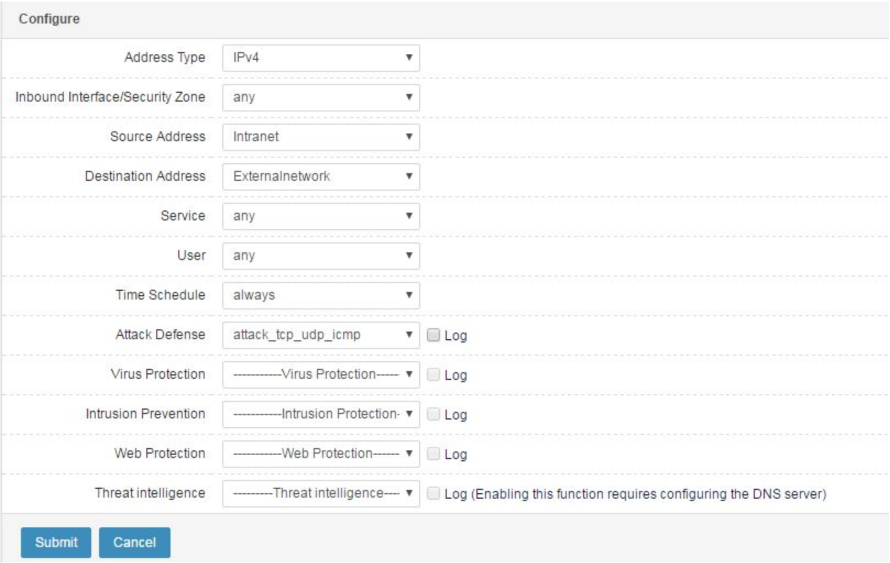
Enable ☑

☑ TCP Scanning ☑ UDP Scanning ☑ Ping Scanning

Scanning Identification Threshold: 1000 (10-65535) connections/s

Host Suppression Duration: 20 (1-65535)Seconds

3. Choose **Policy** > **Security** > **Anti-attack** > **Policy** and click **New**. Set parameters, as shown in the following figure.

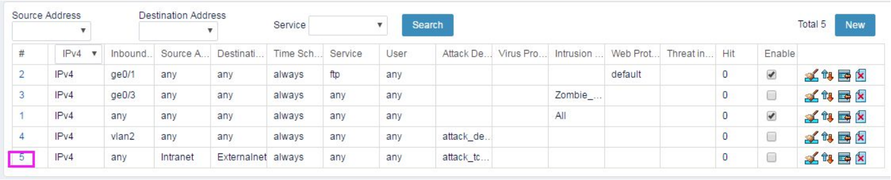


Configure

Address Type	IPv4
Inbound Interface/Security Zone	any
Source Address	Intranet
Destination Address	Externalnetwork
Service	any
User	any
Time Schedule	always
Attack Defense	attack_tcp_udp_icmp □ Log
Virus Protection	-----------Virus Protection----- □ Log
Intrusion Prevention	-----------Intrusion Protection- □ Log
Web Protection	-----------Web Protection------ □ Log
Threat intelligence	---------Threat intelligence---- □ Log (Enabling this function requires configuring the DNS server)

4. Click **Submit**.

5. Choose **Policy** > **Security** > **Anti-attack** > **Policy**. Check the **Enable** box, as shown in the following figure.



#	IPv4	Inbound..	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable
2	IPv4	ge0/1	any	any	always	ftp	any				default		0	☑
3	IPv4	ge0/3	any	any	always	any	any			Zombie_...			0	□
1	IPv4	any	any	any	always	any	any			All			0	☑
4	IPv4	vlan2	any	any	always	any	any	attack_de..					0	□
5	IPv4	any	Intranet	Externalnet	always	any	any	attack_tc...					0	□

37.4 Troubleshooting

37.4.1 A Data Flow Does Not Hit a Policy as Expected

Symptom	The corresponding action is not taken for the data flow that hits a policy. A data flow does not hit a policy as expected.
Analysis	The possible causes are as follows: ➢ The policy is not enabled. ➢ Because policies with the same inbound interface in the IPv4 or IPv6 format are matched from top down as listed on page, the data flow may have hit a previous policy.
Solution	Enable the policy. If the policy conflicts with other policies, modify the policy or adjust the policy order.

38 Anti-attack

38.1 Overview

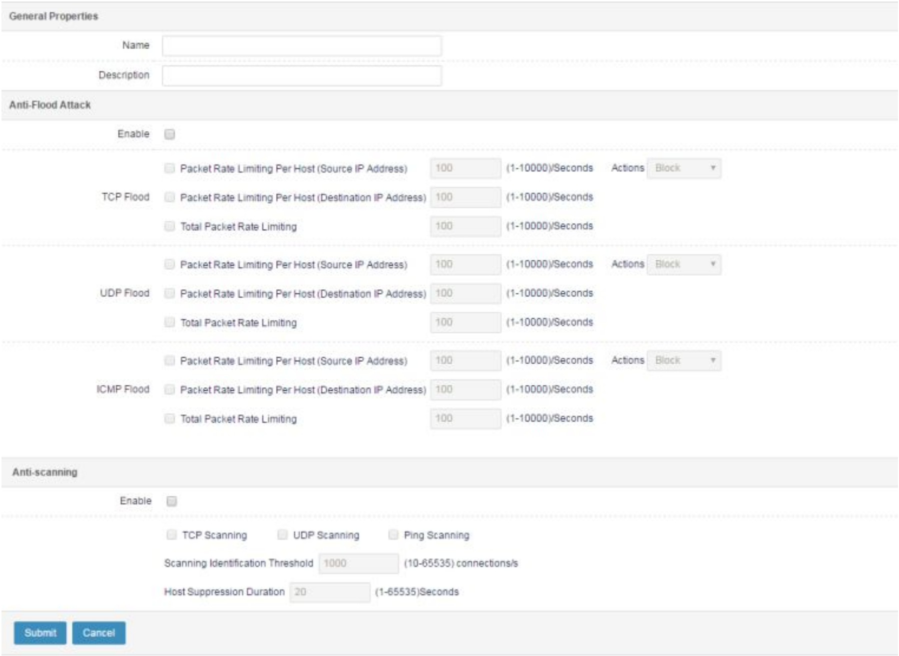
The anti-attack feature provides a configuration template used to prevent flood attacks and scan attacks. The anti-attack feature takes effect only after it is referenced by a security policy. Configured actions such as alarm, drop, and syncookie are taken for packets that hit policies, allowing the system to determine which packets to be permitted and which ones dropped.

38.2 Configuration

38.2.1 Creating an Anti-attack Entry

Procedure:

1. Choose **Policy** > **Security** > **Anti-attack** and click **New**.



General Properties

Name

Description

Anti-Flood Attack

Enable □

TCP Flood
- □ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block ▾
- □ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting 100 (1-10000)/Seconds

UDP Flood
- □ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block ▾
- □ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting 100 (1-10000)/Seconds

ICMP Flood
- □ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block ▾
- □ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting 100 (1-10000)/Seconds

Anti-scanning

Enable □

□ TCP Scanning □ UDP Scanning □ Ping Scanning

Scanning Identification Threshold 1000 (10-65535) connections/s

Host Suppression Duration 20 (1-65535)Seconds

Name: Name of an anti-attack entry.

Description: Brief description about the anti-attack entry.

Anti-Flood Attack: Check the **Enable** box to enable anti-flood.

TCP Flood: Enable anti-TCP flood. TCP flood is also called SYN flood. SYN flood exploits TCP vulnerabilities to send many forged TCP connection requests to a server but gives no responses. As a result, the server runs out of resources quickly and cannot process normal service requests, and will crash in serious cases.

RAVEN 5000 firewalls adopt the industry-leading syncookie technique to effectively protect servers from SYN flood attacks at the cost of few system resources. **Identification threshold**: Maximum number of SYN packets to trigger anti-TCP flood. The default value is **100**. **Action**: The options are **Block**, **Alarm**, and **syncookie**.

UDP Flood: Enable anti-UDP flood. **Identification threshold**: Maximum number of UDP packets to trigger anti-UDP flood. The default value is **100**. **Action**: The options are **Block** and **Alarm**.

ICMP Flood: Enable anti-ICMP flood. **Identification threshold**: Maximum number of ICMP packets to trigger anti-ICMP flood. The default value is **100**.

Action: The options are **Block** and **Alarm**.

Anti-scan: Check the **Enable** box to enable anti-scan.

TCP scan: Configure anti-TCP scan based on the actual network circumstance.

A TCP scan occurs when the number of IP packets with TCP SYN fragments sent from a source IP address to different ports with the same destination IP address or to the same port with different destination IP addresses within 1s exceeds the configured threshold. The system records the scan event and blocks all the TCP SYN packets sent by the source host during the configured period.

Enabling anti-TCP scan may occupy many memory resources.

UDP scan: Configure anti-UDP scan based on the actual network circumstance.

A UDP scan occurs when the number of IP packets with UDP data sent from a source IP address to different ports with the same destination IP address or to the same port with different destination IP addresses within 1s exceeds the configured threshold. The system records the scan event and blocks all the UDP packets sent by the source host during the configured period.

Enabling anti-UDP scan may occupy many memory resources.

Ping scan: Configure anti-ping scan based on the actual network circumstance.

An address scan occurs when the number of ICMP packets sent from a source IP address to different hosts within 1s exceeds the configured threshold. ICMP packets are sent to all hosts to get at least one response and identify the destination address. A firewall records the number of ICMP packets sent from a remote source address to different hosts. After a source IP address is flagged as address scan attack, packets from the address are blocked during the configured period.

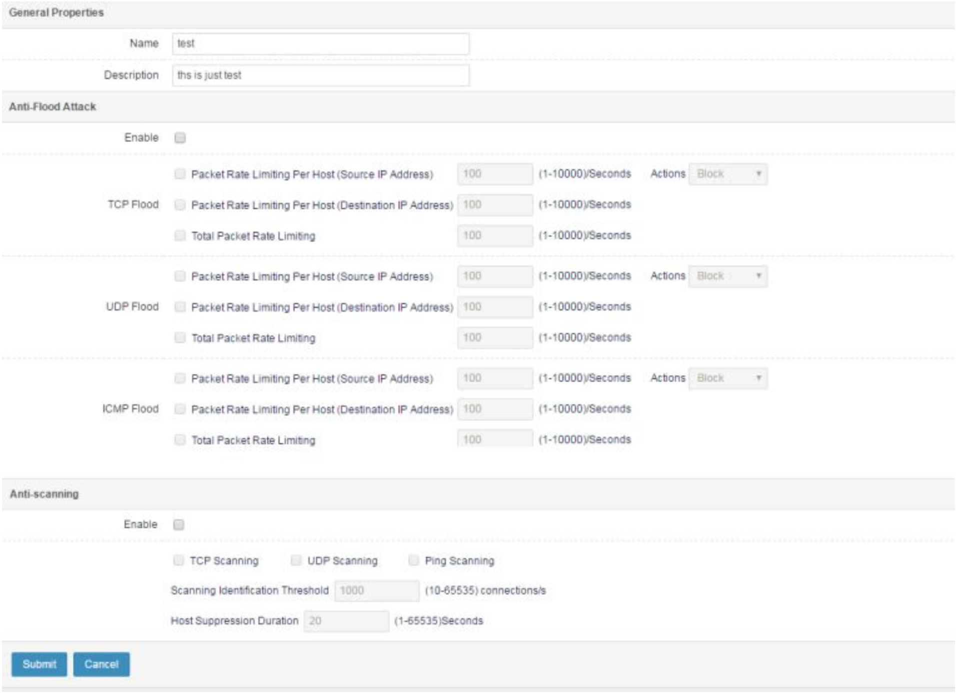
Enabling anti-ping scan may occupy many memory resources.

Host suppression duration: Duration for which packets from a malicious host are blocked after a scan attack is detected. The default value is **20s**.

Scan identification threshold: The source IP address is flagged as scan attack after this threshold is exceeded, and packets from the source address are blocked. The default value is **1000**.

⚠ Notice	Set this parameter properly. If intranet users access the Internet through NAT with the same source IP address, a small threshold may cause anti-flood to take effect.

2. Set **Name**, **Description**, and other parameters.



General Properties

Name: test

Description: ths is just test

Anti-Flood Attack

Enable □

TCP Flood
- □ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- □ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting 100 (1-10000)/Seconds

UDP Flood
- □ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- □ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting 100 (1-10000)/Seconds

ICMP Flood
- □ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- □ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting 100 (1-10000)/Seconds

Anti-scanning

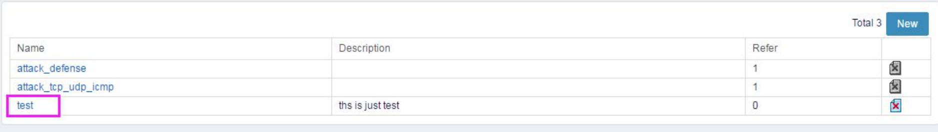
Enable □

□ TCP Scanning □ UDP Scanning □ Ping Scanning

Scanning Identification Threshold 1000 (10-65535) connections/s

Host Suppression Duration 20 (1-65535)Seconds

3. Click **Submit**. The following page appears.

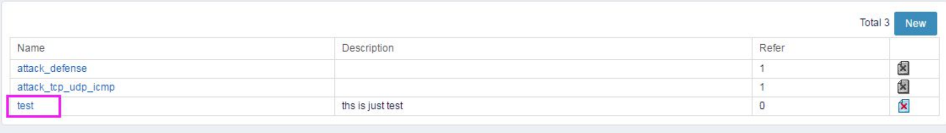


Name	Description	Refer	
attack_defense		1	☒
attack_tcp_udp_icmp		1	☒
test	ths is just test	0	☒

38.2.2 Modifying an Anti-attack Entry

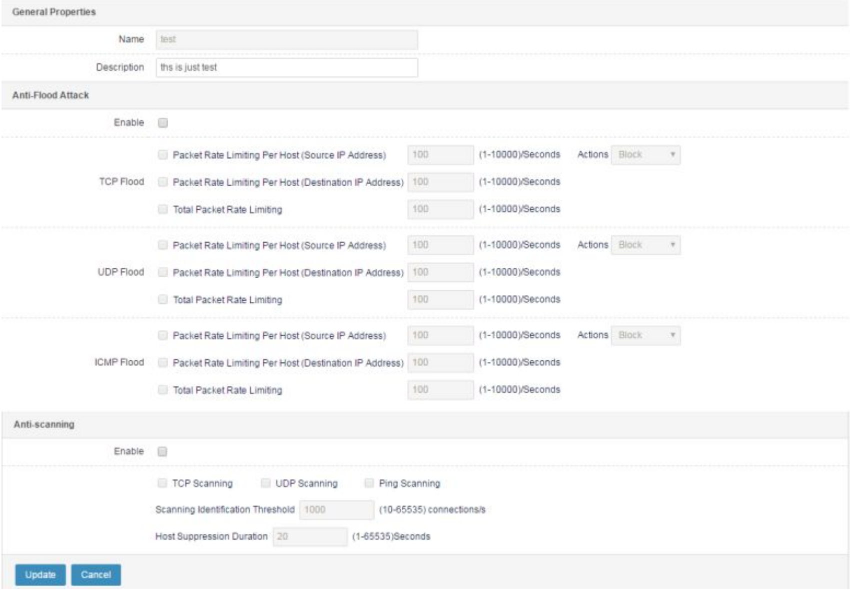
You can modify an existing anti-attack entry.

1. Choose **Policy** > **Security** > **Anti-attack**. The following page appears.



Name	Description	Refer	
attack_defense		1	☒
attack_tcp_udp_icmp		1	☒
test	ths is just test	0	☒

2. Click an anti-attack entry.



General Properties

Name: test

Description: ths is just test

Anti-Flood Attack

Enable □

TCP Flood
□ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
□ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
□ Total Packet Rate Limiting 100 (1-10000)/Seconds

UDP Flood
□ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
□ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
□ Total Packet Rate Limiting 100 (1-10000)/Seconds

ICMP Flood
□ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
□ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
□ Total Packet Rate Limiting 100 (1-10000)/Seconds

Anti-scanning

Enable □

□ TCP Scanning □ UDP Scanning □ Ping Scanning

Scanning Identification Threshold 1000 (10-65535) connections/s

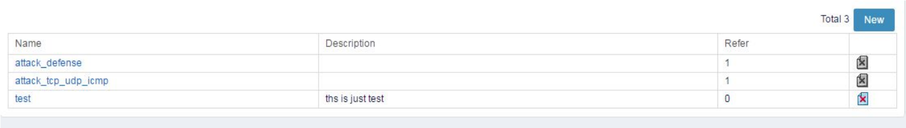
Host Suppression Duration 20 (1-65535)Seconds

Modify the parameters except **Name**.

3. Click **Update** to apply the modification.

38.2.3 Deleting an Anti-attack Entry

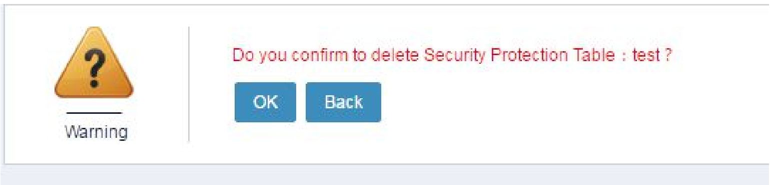
1. Choose **Policy > Security > Anti-attack.** The following page appears.



Total 3

Name	Description	Refer	
attack_defense		1	☒
attack_tcp_udp_icmp		1	☒
test	ths is just test	0	☒

2. Click ☒ next to the anti-attack entry you want to delete.



Do you confirm to delete Security Protection Table : test ?

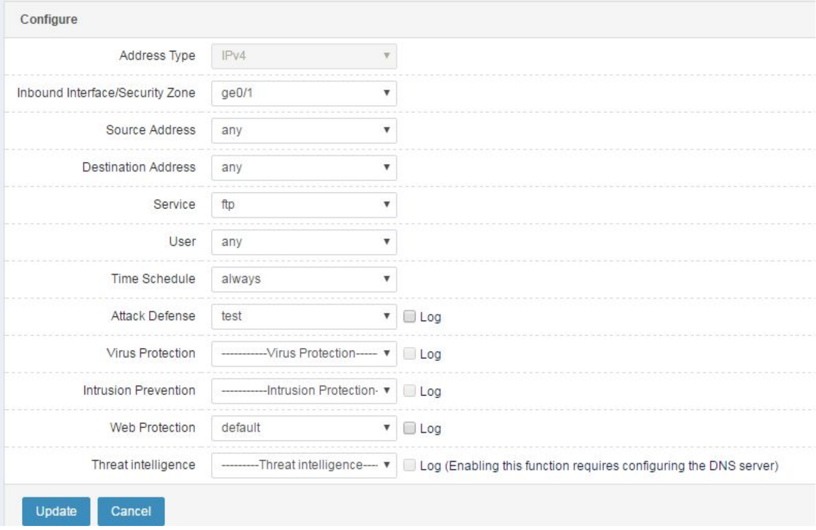
3. Click **OK**.

Notice

For an anti-attack entry referenced by a security policy, its **Delete** button is grayed out .

38.2.4 Referencing an Anti-attack Entry in a Security Policy

The anti-attack feature takes effect only after it is referenced by a security policy. Packets that hit the policy are protected from attacks.



Configure

Address Type	IPv4	
Inbound Interface/Security Zone	ge0/1	
Source Address	any	
Destination Address	any	
Service	ftp	
User	any	
Time Schedule	always	
Attack Defense	test	□ Log
Virus Protection	-----------Virus Protection-----	□ Log
Intrusion Prevention	-----------Intrusion Protection·	□ Log
Web Protection	default	□ Log
Threat intelligence	---------Threat intelligence----	□ Log (Enabling this function requires configuring the DNS server)

38.3 Configuration Examples

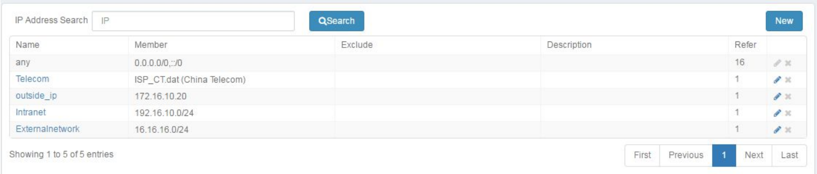
38.3.1 Example 1: Creating an Anti-flood Policy

Description:

VLAN 1 of a firewall connects to an intranet, and VLAN 2 connects to an external network. The firewall triggers TCP syncookie when the rate of TCP connection requests per source IP address sent from the external network to the intranet exceeds 100. The firewall checks whether the connection requests come from an attack source. If so, the firewall drops the requests. (Enabling syncookie may consume performance.) The firewall triggers the anti-UDP flood feature when the rate of a DNS connection request sent from the external network to an internal DNS server exceeds 2000, and the firewall drops the request. The firewall triggers the alarm function when the total rate of ICMP requests sent from the external network to the intranet exceeds 1000. The firewall displays a message indicating the intranet may suffer ICMP attacks. Configure an anti-flood policy to monitor the network status in real time and protect the network from attacks.

Procedure:

1. Choose **Object** > **Address object** > **Address node**, and configure address objects named **Intranet** and **External network**, as shown in the following figure.

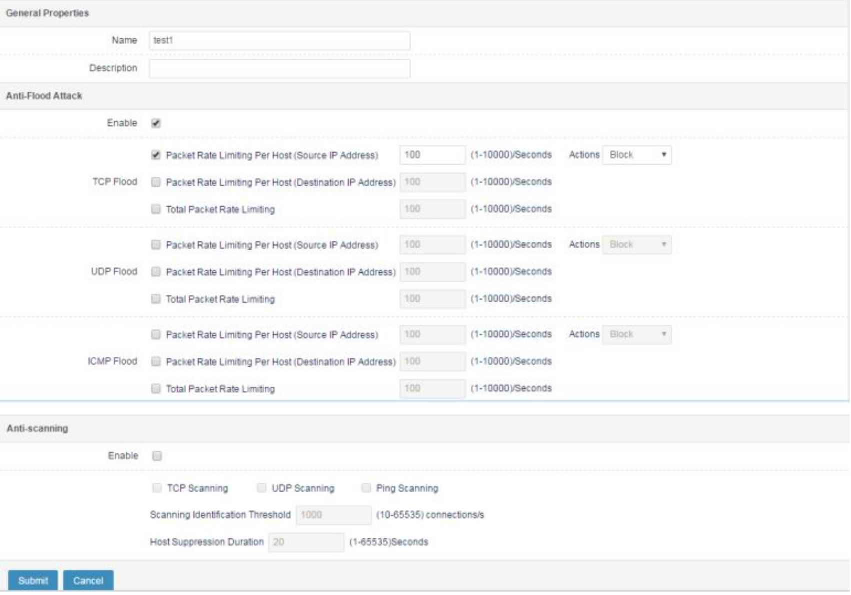


IP Address Search: IP

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			16
Telecom	ISP_CT.dat (China Telecom)			1
outside_ip	172.16.10.20			1
Intranet	192.16.10.0/24			1
Externalnetwork	16.16.16.0/24			1

Showing 1 to 5 of 5 entries

2. Choose **Policy** > **Security** > **Anti-attack** and click **New**.



General Properties

Name: test1

Description:

Anti-Flood Attack

Enable: ☑

TCP Flood
- ☑ Packet Rate Limiting Per Host (Source IP Address): 100 (1-10000)/Seconds Actions: Block
- □ Packet Rate Limiting Per Host (Destination IP Address): 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting: 100 (1-10000)/Seconds

UDP Flood
- □ Packet Rate Limiting Per Host (Source IP Address): 100 (1-10000)/Seconds Actions: Block
- □ Packet Rate Limiting Per Host (Destination IP Address): 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting: 100 (1-10000)/Seconds

ICMP Flood
- □ Packet Rate Limiting Per Host (Source IP Address): 100 (1-10000)/Seconds Actions: Block
- □ Packet Rate Limiting Per Host (Destination IP Address): 100 (1-10000)/Seconds
- □ Total Packet Rate Limiting: 100 (1-10000)/Seconds

Anti-scanning

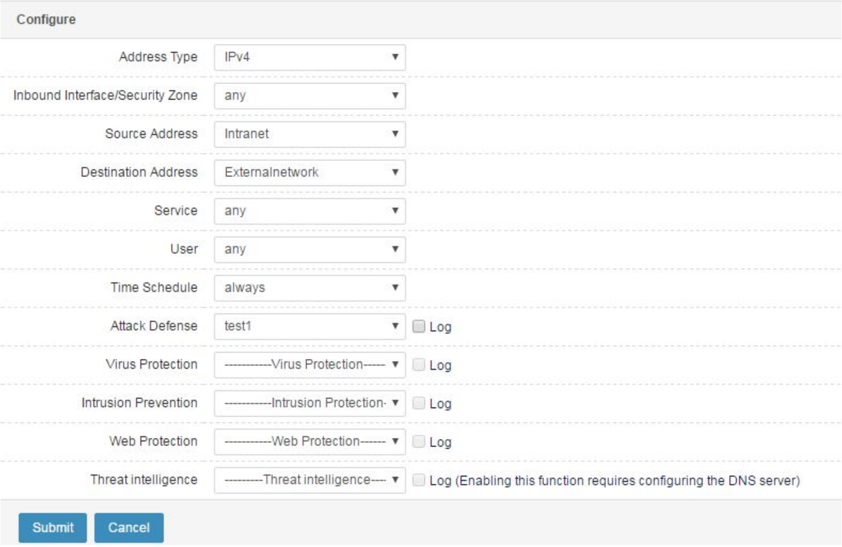
Enable: □

□ TCP Scanning □ UDP Scanning □ Ping Scanning

Scanning Identification Threshold: 1000 (10-65535) connections/s

Host Suppression Duration: 20 (1-65535)Seconds

3. Choose **Policy** > **Security** > **Protection policy** and click **New**. Set parameters, as shown in the following figure.

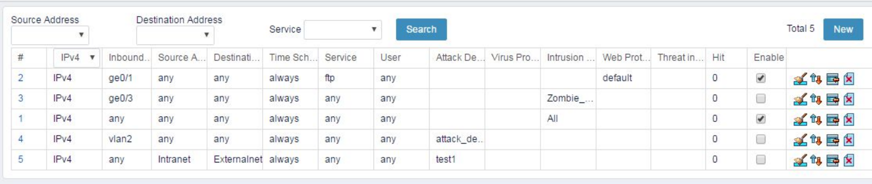


Configure

Address Type	IPv4 ▾
Inbound Interface/Security Zone	any ▾
Source Address	Intranet ▾
Destination Address	Externalnetwork ▾
Service	any ▾
User	any ▾
Time Schedule	always ▾
Attack Defense	test1 ▾ □ Log
Virus Protection	-----------Virus Protection----- ▾ □ Log
Intrusion Prevention	-----------Intrusion Protection· ▾ □ Log
Web Protection	-----------Web Protection------ ▾ □ Log
Threat intelligence	---------Threat intelligence---- ▾ □ Log (Enabling this function requires configuring the DNS server)

4. Click **Submit**.

5. Choose **Policy** > **Security** > **Protection policy.** Check the **Enable** box, as shown in the following figure.



Source Address ▾ Destination Address ▾ Service ▾

#	IPv4 ▾	Inbound..	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	ftp	any				default		0	☑	
3	IPv4	ge0/3	any	any	always	any	any			Zombie_...			0	□	
1	IPv4	any	any	any	always	any	any			All			0	☑	
4	IPv4	vlan2	any	any	always	any	any	attack_de..					0	□	
5	IPv4	any	Intranet	Externalnet	always	any	any	test1					0	□	

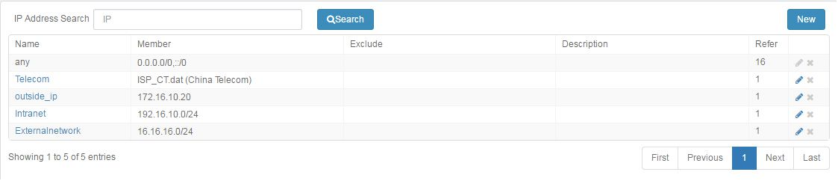
38.3.2 Example 2: Creating an Anti-scan Policy

Description:

VLAN 1 of a firewall connects to an intranet, and VLAN 2 connects to an external network. Enable an anti-scan policy on the firewall to defend against scan attacks from the external network. The firewall triggers the anti-scan feature when an external source address sends TCP or UDP connection requests to more than 1000 different ports of an internal server within 1s. All the TCP or UDP requests sent by the source address are blocked in the next 20s. The firewall triggers the anti-scan feature when an external source address sends ICMP requests to more than 1000 different internal hosts. All the ICMP requests sent by the source address are blocked in the next 20s.

Procedure:

1. Choose **Object** > **Address object** > **Address node**, and configure address objects named **Intranet** and **External network**, as shown in the following figure.

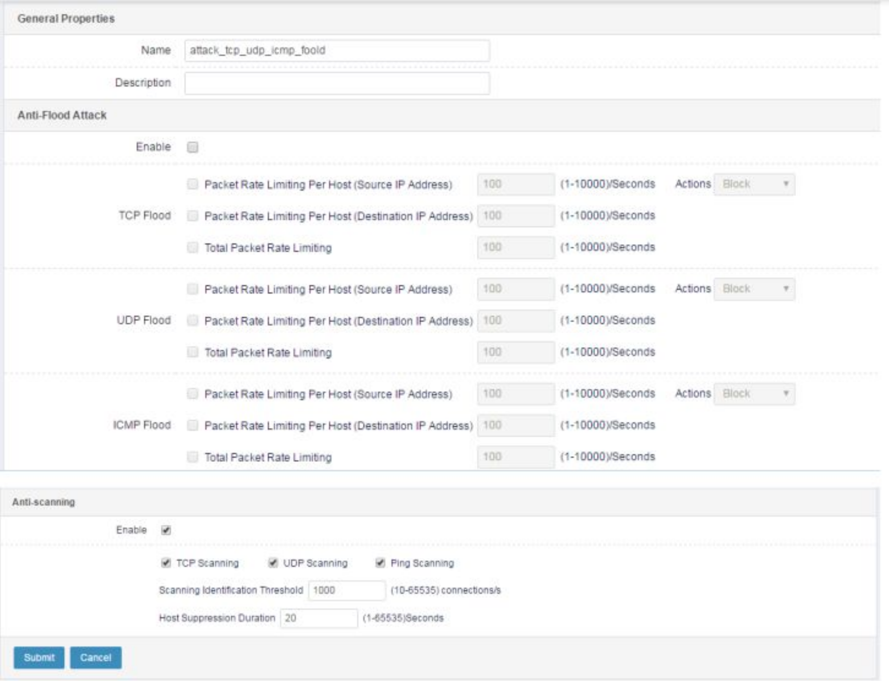


IP Address Search: IP

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			16
Telecom	ISP_CT.dat (China Telecom)			1
outside_ip	172.16.10.20			1
Intranet	192.16.10.0/24			1
Externalnetwork	16.16.16.0/24			1

Showing 1 to 5 of 5 entries

2. Choose **Policy** > **Security** > **Anti-attack** > **Security list** and click **New**.



General Properties

Name: attack_tcp_udp_icmp_foold

Description:

Anti-Flood Attack

Enable ☐

TCP Flood
- ☐ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- ☐ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- ☐ Total Packet Rate Limiting 100 (1-10000)/Seconds

UDP Flood
- ☐ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- ☐ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- ☐ Total Packet Rate Limiting 100 (1-10000)/Seconds

ICMP Flood
- ☐ Packet Rate Limiting Per Host (Source IP Address) 100 (1-10000)/Seconds Actions Block
- ☐ Packet Rate Limiting Per Host (Destination IP Address) 100 (1-10000)/Seconds
- ☐ Total Packet Rate Limiting 100 (1-10000)/Seconds

Anti-scanning

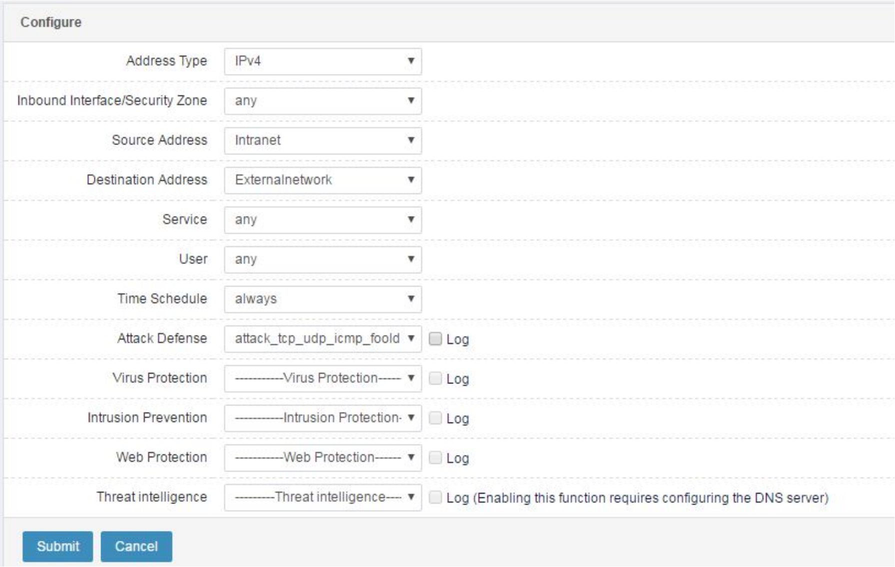
Enable ☑

☑ TCP Scanning ☑ UDP Scanning ☑ Ping Scanning

Scanning Identification Threshold 1000 (10-65535) connections/s

Host Suppression Duration 20 (1-65535)Seconds

3. Choose **Policy** > **Security** > **Anti-attack** > **Policy** and click **New**. Set parameters, as shown in the following figure.

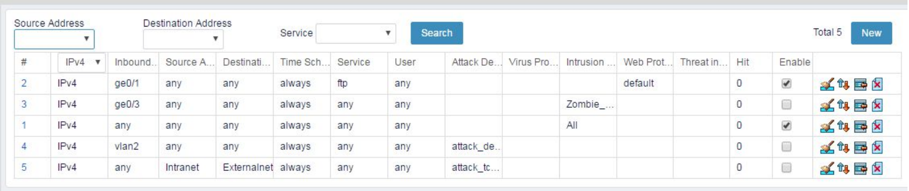


Configure

Address Type	IPv4 ▾	
Inbound Interface/Security Zone	any ▾	
Source Address	Intranet ▾	
Destination Address	Externalnetwork ▾	
Service	any ▾	
User	any ▾	
Time Schedule	always ▾	
Attack Defense	attack_tcp_udp_icmp_foold ▾	□ Log
Virus Protection	-----------Virus Protection----- ▾	□ Log
Intrusion Prevention	-----------Intrusion Protection- ▾	□ Log
Web Protection	-----------Web Protection------ ▾	□ Log
Threat intelligence	---------Threat intelligence---- ▾	□ Log (Enabling this function requires configuring the DNS server)

6. Click **Submit**.

7. Choose **Policy** > **Security** > **Anti-attack** > **Policy**. Check the **Enable** box, as shown in the following figure.

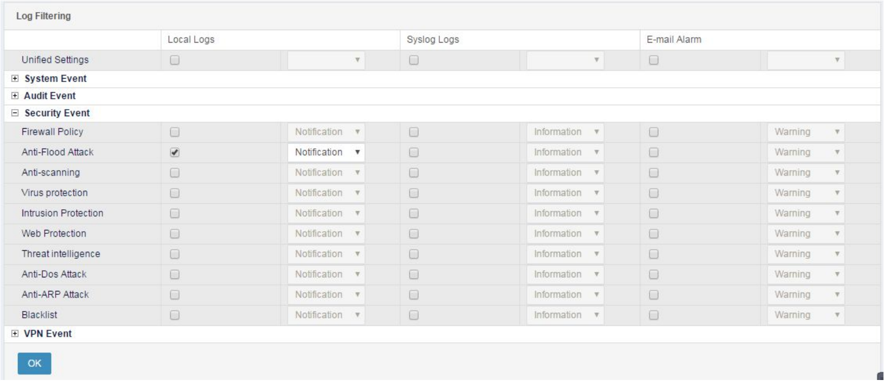


#	IPv4 ▾	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	ftp	any				default		0	☑	
3	IPv4	ge0/3	any	any	always	any	any			Zombie_...			0	□	
1	IPv4	any	any	any	always	any	any			All			0	☑	
4	IPv4	vlan2	any	any	always	any	any	attack_de..					0	□	
5	IPv4	any	Intranet	Externalnet	always	any	any	attack_tc...					0	□	

38.4 Monitoring and Maintenance

38.4.1 Displaying Anti-attack Logs

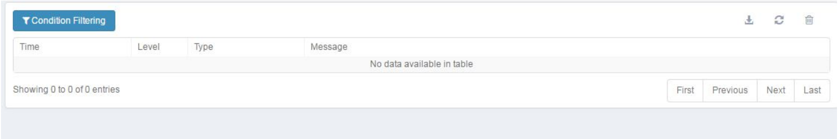
1. Choose **Log** > **Log management** > **Log filter**. Select logs related to the anti-flood module, and set the log level. Click **OK**.



Log Filtering

	Local Logs		Syslog Logs		E-mail Alarm	
Unified Settings	□	▾	□	▾	□	▾
⊞ **System Event**						
⊞ **Audit Event**						
⊟ **Security Event**						
Firewall Policy	□	Notification ▾	□	Information ▾	□	Warning ▾
Anti-Flood Attack	☑	Notification ▾	□	Information ▾	□	Warning ▾
Anti-scanning	□	Notification ▾	□	Information ▾	□	Warning ▾
Virus protection	□	Notification ▾	□	Information ▾	□	Warning ▾
Intrusion Protection	□	Notification ▾	□	Information ▾	□	Warning ▾
Web Protection	□	Notification ▾	□	Information ▾	□	Warning ▾
Threat intelligence	□	Notification ▾	□	Information ▾	□	Warning ▾
Anti-Dos Attack	□	Notification ▾	□	Information ▾	□	Warning ▾
Anti-ARP Attack	□	Notification ▾	□	Information ▾	□	Warning ▾
Blacklist	□	Notification ▾	□	Information ▾	□	Warning ▾
⊞ **VPN Event**						

2. Choose **Log** > **Security log** > **Anti-attack** > **Anti-flood** to display related logs.



Time	Level	Type	Message
No data available in table			

Showing 0 to 0 of 0 entries

38.5 Troubleshooting

38.5.1 Anti-flood Works Abnormally

Symptom	The anti-flood feature works abnormally.
Analysis	When the anti-flood feature works abnormally despite a policy is hit, check whether: ➢ The anti-flood feature is enabled for the protected object. ➢ The proper packet type is selected. The options are **SYN flood**, **UDP flood**, and **ICMP flood**. ➢ The configured threshold is not too large. The anti-flood action is correct.
Solution	Modify configurations

39 Antivirus

39.1 Overview

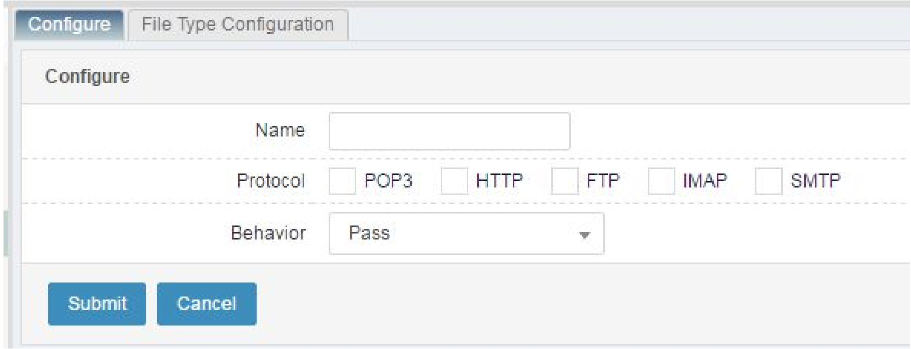
Virus scan is performed in real time at the internal and external ingresses to isolate intranets from viruses and provide active and passive virus defense for workstations. You can scan specified types of files, or scan files when HTTP, FTP, IMAP, POP3, SMTP, and other application protocols are implemented.

39.2 Antivirus Configuration

38.5.2 Creating an Antivirus Template

Procedure:

1. Choose **Policy** > **Security** > **Antivirus** and click **New**.



Parameter description:

Name: Name of the new antivirus template.

Protocol: Application protocol for data flows. Select at least one option.

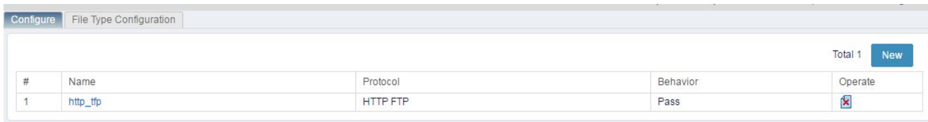
Action: Action to be taken for data flows that meet the match conditions. The options are **Permit** and **Deny**.

2. Click **Submit** after you complete the settings.

38.5.3 Modifying an Antivirus Template

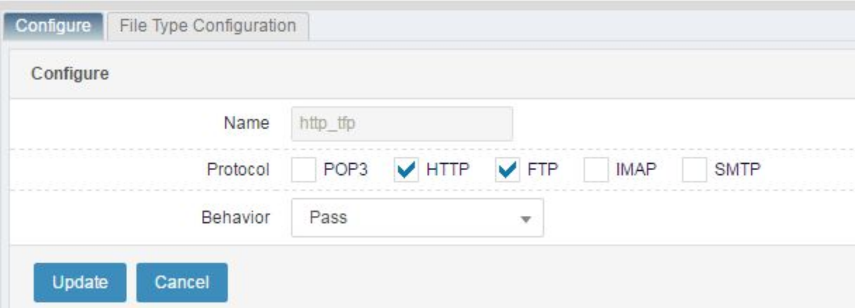
Procedure:

1. Choose **Policy** > **Security** > **Antivirus** and click a template name.



#	Name	Protocol	Behavior	Operate
1	http_tfp	HTTP FTP	Pass	☒

2. Modify **Protocol** and **Action**, and click **Update**.



Name: http_tfp

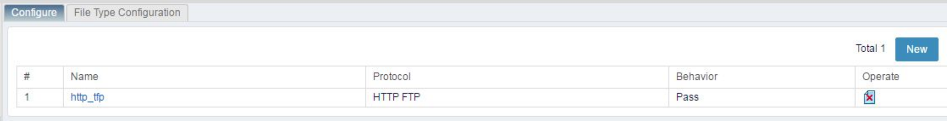
Protocol: □ POP3 ☑ HTTP ☑ FTP □ IMAP □ SMTP

Behavior: Pass

38.5.4 Deleting an Antivirus Template

Procedure:

1. Choose **Policy** > **Security** > **Antivirus**. The following page appears.



#	Name	Protocol	Behavior	Operate
1	http_tfp	HTTP FTP	Pass	☒

2. Click ☒ next to the template you want to delete.

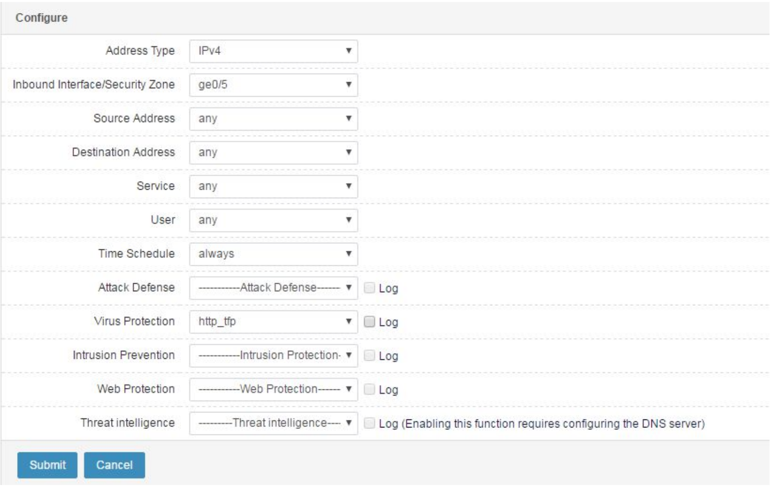
⚠ Notice

A template referenced by a protection policy cannot be deleted.

38.5.5 Referencing an Antivirus Template in a Protection Policy

Procedure:

1. Choose **Policy** > **Security** > **Protection policy** and click **New**. Configure the match conditions and select the antivirus template you want to reference.



Configure

Address Type	IPv4	
Inbound Interface/Security Zone	ge0/5	
Source Address	any	
Destination Address	any	
Service	any	
User	any	
Time Schedule	always	
Attack Defense	-----------Attack Defense------	□ Log
Virus Protection	http_tfp	□ Log
Intrusion Prevention	-----------Intrusion Protection-	□ Log
Web Protection	-----------Web Protection------	□ Log
Threat intelligence	---------Threat intelligence----	□ Log (Enabling this function requires configuring the DNS server)

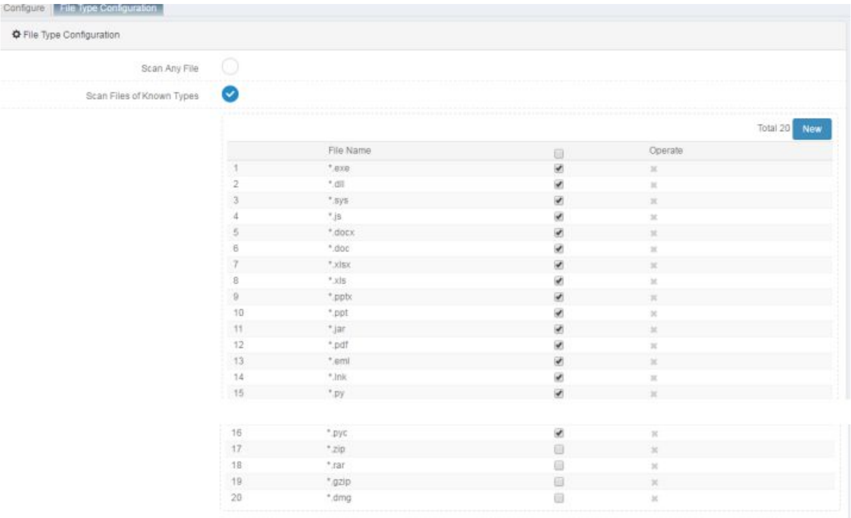
2. Click **Submit.**

39.3File Type Configuration

39.3.1 Configuring File Scan

Procedure:

1. Choose **Policy** > **Security** > **Antivirus** > **File type configuration**. Select **Scan files of known types** to scan files of specified types, including predefined and custom types.



File Type Configuration

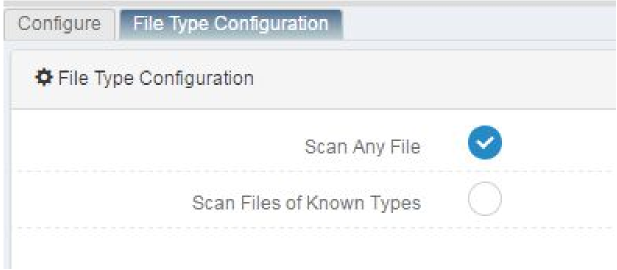
Scan Any File ○

Scan Files of Known Types ●

Total 20 New

	File Name	□	Operate
1	*.exe	☑	×
2	*.dll	☑	×
3	*.sys	☑	×
4	*.js	☑	×
5	*.docx	☑	×
6	*.doc	☑	×
7	*.xlsx	☑	×
8	*.xls	☑	×
9	*.pptx	☑	×
10	*.ppt	☑	×
11	*.jar	☑	×
12	*.pdf	☑	×
13	*.eml	☑	×
14	*.lnk	☑	×
15	*.py	☑	×
16	*.pyc	☑	×
17	*.zip	□	×
18	*.rar	□	×
19	*.gzip	□	×
20	*.dmg	□	×

2. Select **Scan any files** to scan all the files passing the firewall.



File Type Configuration

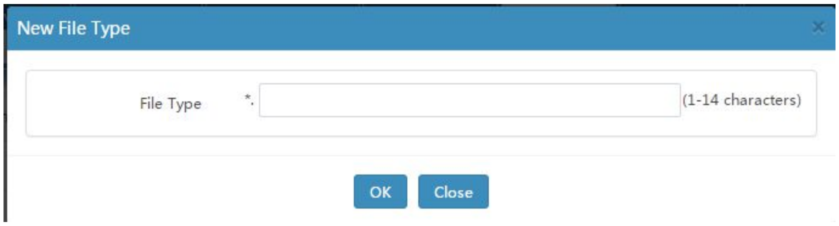
Scan Any File ●

Scan Files of Known Types ○

39.3.2 Adding a File Type

Procedure:

1. Choose **Policy** > **Security** > **Antivirus** > **File type configuration**. Select **Scan files of known types** and click **Add**.



New File Type

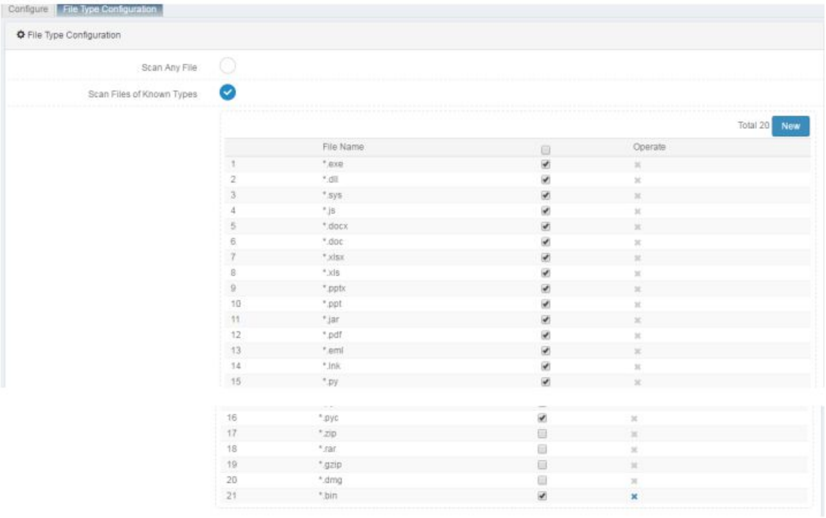
File Type *. (1-14 characters)

2. Click **OK** after you complete the settings.

39.3.3 Deleting a File Type

Procedure:

1. Choose **Policy** > **Security** > **Antivirus** > **File type configuration**. Select **Scan files of known types**.



File Type Configuration

Scan Any File ○

Scan Files of Known Types ●

Total 20 New

	File Name	□	Operate
1	*.exe	☑	✕
2	*.dll	☑	✕
3	*.sys	☑	✕
4	*.js	☑	✕
5	*.docx	☑	✕
6	*.doc	☑	✕
7	*.xlsx	☑	✕
8	*.xls	☑	✕
9	*.pptx	☑	✕
10	*.ppt	☑	✕
11	*.jar	☑	✕
12	*.pdf	☑	✕
13	*.eml	☑	✕
14	*.lnk	☑	✕
15	*.py	☑	✕
16	*.pyc	☑	✕
17	*.zip	□	✕
18	*.rar	□	✕
19	*.gzip	□	✕
20	*.dmg	□	✕
21	*.bin	☑	✕

2. Select the file type you want to delete and click 🗑.

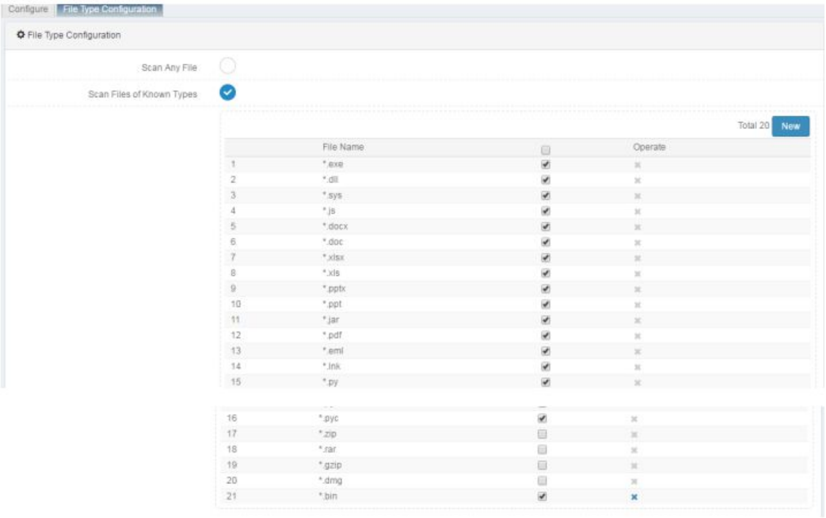
⚠ Notice

The **Delete** button is grayed out for predefined file types.

39.3.4 Enabling or Disabling a File Type

Procedure:

1. Choose **Policy** > **Security** > **Antivirus** > **File type configuration**. Select **Scan files of known types**.



Configure | File Type Configuration

⚙ File Type Configuration

Scan Any File ○

Scan Files of Known Types ☑

Total 20 New

	File Name	□	Operate
1	*.exe	☑	✕
2	*.dll	☑	✕
3	*.sys	☑	✕
4	*.js	☑	✕
5	*.docx	☑	✕
6	*.doc	☑	✕
7	*.xlsx	☑	✕
8	*.xls	☑	✕
9	*.pptx	☑	✕
10	*.ppt	☑	✕
11	*.jar	☑	✕
12	*.pdf	☑	✕
13	*.eml	☑	✕
14	*.lnk	☑	✕
15	*.py	☑	✕
16	*.pyc	☑	✕
17	*.zip	□	✕
18	*.rar	□	✕
19	*.gzip	□	✕
20	*.dmg	□	✕
21	*.bin	☑	✕

2. Select a file type and check the box on the right ☑ to enable it, or uncheck the box □ to disable it.

3. You can also check or uncheck the box on the top to enable or disable all the file types.

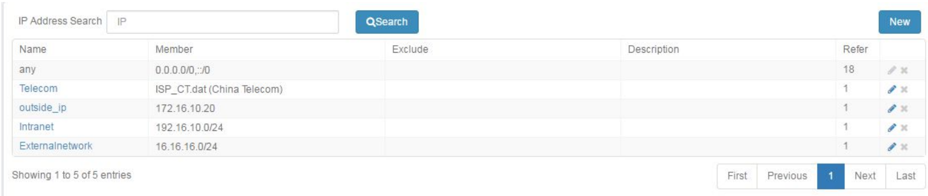
39.4Configuration Example

Description:

VLAN 1 of a firewall connects to an intranet, and VLAN 2 connects to an external network. The firewall triggers the antivirus feature when it detects viruses in a file that an internal host downloads from the external network, and handles the file based on configurations.

Procedure:

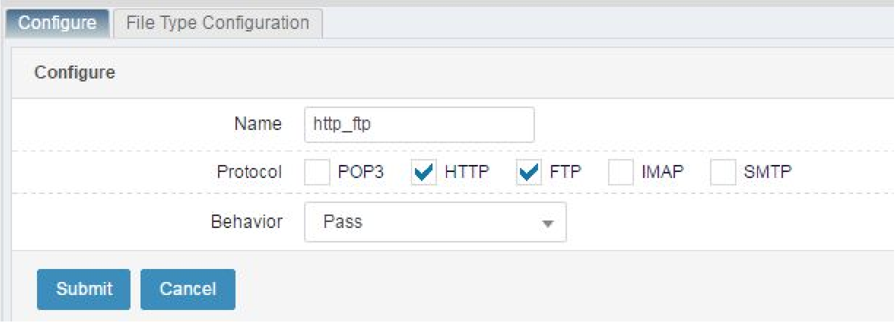
1. Choose **Object** > **Address object** > **Address node**, and configure address objects named **Intranet** and **External network**, as shown in the following figure.



Name	Member	Exclude	Description	Refer	
any	0.0.0.0/0,::/0			18	
Telecom	ISP_CT.dat (China Telecom)			1	
outside_ip	172.16.10.20			1	
Intranet	192.16.10.0/24			1	
Externalnetwork	16.16.16.0/24			1	

Showing 1 to 5 of 5 entries

2. Choose **Policy** > **Security** > **Antivirus** and click **New**.

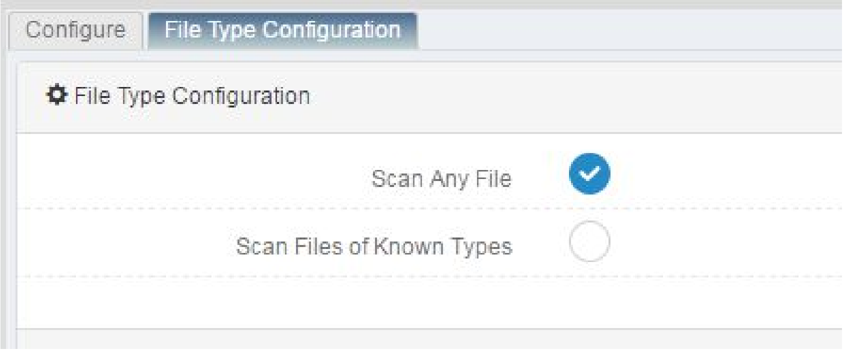


Name: http_ftp

Protocol: □ POP3 ☑ HTTP ☑ FTP □ IMAP □ SMTP

Behavior: Pass

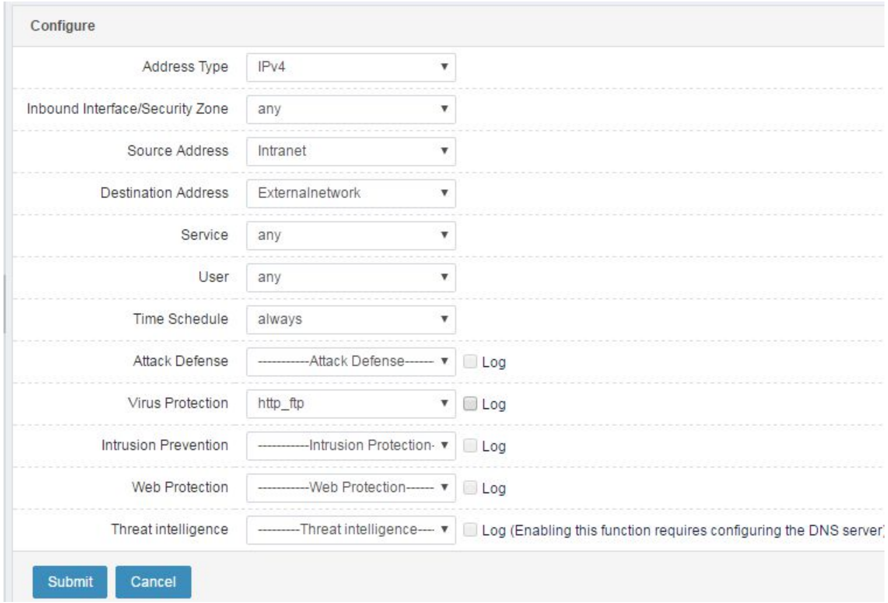
3. Choose **Policy** > **Security** > **Antivirus** > **File type configuration**. Select **Scan any files**.



● Scan Any File

○ Scan Files of Known Types

4. Choose **Policy** > **Security** > **Protection policy** and click **New**. Set parameters, as shown in the following figure.

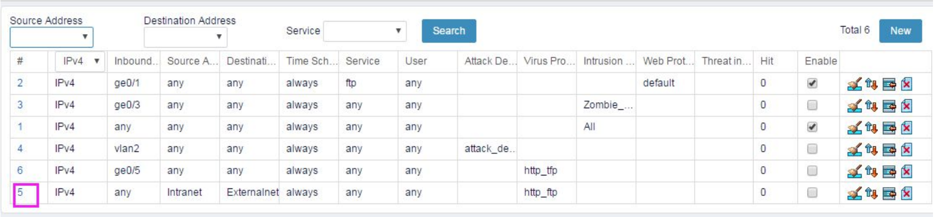


Configure

Address Type	IPv4 ▼	
Inbound Interface/Security Zone	any ▼	
Source Address	Intranet ▼	
Destination Address	Externalnetwork ▼	
Service	any ▼	
User	any ▼	
Time Schedule	always ▼	
Attack Defense	------------Attack Defense------ ▼	□ Log
Virus Protection	http_ftp ▼	□ Log
Intrusion Prevention	------------Intrusion Protection· ▼	□ Log
Web Protection	------------Web Protection------ ▼	□ Log
Threat intelligence	---------Threat intelligence---- ▼	□ Log (Enabling this function requires configuring the DNS server)

5. Click **Submit**.

6. Choose **Policy** > **Security** > **Protection policy.** Check the **Enable** box, as shown in the following figure.



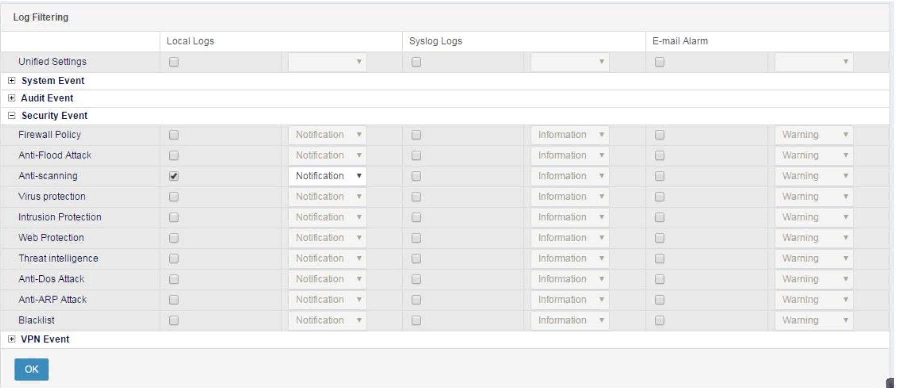
Source Address ▼ Destination Address ▼ Service ▼

#	IPv4 ▼	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
2	IPv4	ge0/1	any	any	always	ftp	any				default		0	☑	
3	IPv4	ge0/3	any	any	always	any	any			Zombie_...			0	□	
1	IPv4	any	any	any	always	any	any			All			0	☑	
4	IPv4	vlan2	any	any	always	any	any	attack_de...					0	□	
6	IPv4	ge0/5	any	any	always	any	any		http_tfp				0	□	
5	IPv4	any	Intranet	Externalnet	always	any	any		http_ftp				0	□	

39.5Monitoring

39.5.1 Displaying Antivirus Logs

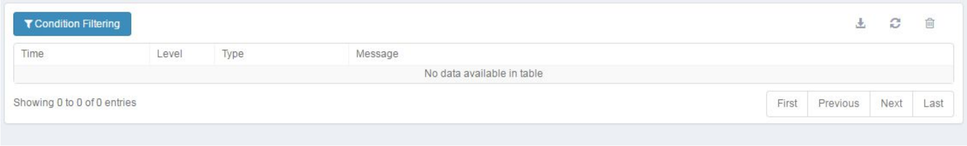
1. Choose **Log** > **Log management** > **Log filter**. Select logs related to the antivirus module, and set the log level. Click **OK.**



Log Filtering

	Local Logs		Syslog Logs		E-mail Alarm	
Unified Settings	☐		☐		☐	
⊞ **System Event**						
⊞ **Audit Event**						
⊟ **Security Event**						
Firewall Policy	☐	Notification	☐	Information	☐	Warning
Anti-Flood Attack	☐	Notification	☐	Information	☐	Warning
Anti-scanning	☑	Notification	☐	Information	☐	Warning
Virus protection	☐	Notification	☐	Information	☐	Warning
Intrusion Protection	☐	Notification	☐	Information	☐	Warning
Web Protection	☐	Notification	☐	Information	☐	Warning
Threat intelligence	☐	Notification	☐	Information	☐	Warning
Anti-Dos Attack	☐	Notification	☐	Information	☐	Warning
Anti-ARP Attack	☐	Notification	☐	Information	☐	Warning
Blacklist	☐	Notification	☐	Information	☐	Warning
⊞ **VPN Event**						

2. Choose **Log** > **Security log** > **Anti-attack** > **Antivirus** to display antivirus logs.



Time	Level	Type	Message
No data available in table			

Showing 0 to 0 of 0 entries

40 Intrusion Prevention

40.1 Overview

With the rapid development of the Internet, network environments become increasingly complex and simple protective measures are no longer effective for handling malicious attacks, Trojan, and worms. An intrusion prevention system (IPS) provides deep and multi-layered network protection for enterprises.

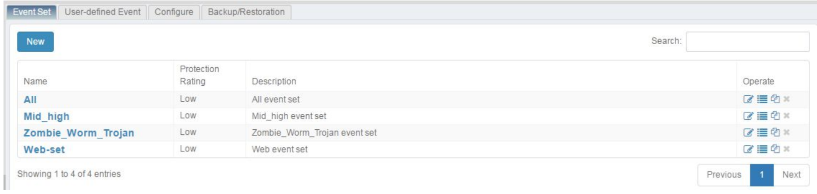
RAVEN 5000 firewalls' intrusion prevention feature uses event signature to monitor specific network behaviors and take Permit, Deny, and Deny source IP address actions to protect the network. The event signature database can be dynamically upgraded on the Belden website to track the latest network threats in real time and protect network security.

40.2 Event Set Configuration

40.2.1 Creating an Event Set

Procedure:

1. Choose **Policy** > **Security** > **Intrusion prevention**. The following page appears.

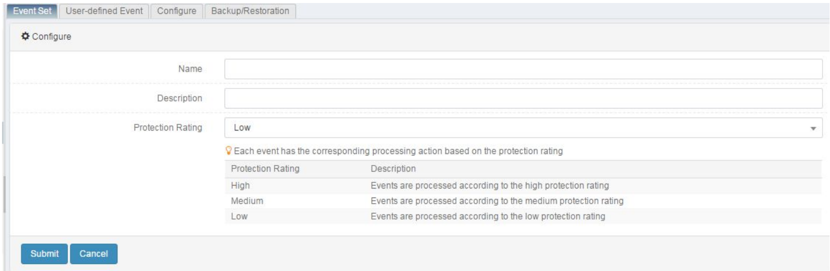


Name	Protection Rating	Description	Operate
All	Low	All event set	✎ ☰ ⧉ ✖
Mid_high	Low	Mid_high event set	✎ ☰ ⧉ ✖
Zombie_Worm_Trojan	Low	Zombie_Worm_Trojan event set	✎ ☰ ⧉ ✖
Web-set	Low	Web event set	✎ ☰ ⧉ ✖

Showing 1 to 4 of 4 entries

The event sets displayed in bold are predefined.

2. Click **New** to create an event set. The following page appears.



Name	
Description	
Protection Rating	Low

Each event has the corresponding processing action based on the protection rating

Protection Rating	Description
High	Events are processed according to the high protection rating
Medium	Events are processed according to the medium protection rating
Low	Events are processed according to the low protection rating

Parameter description:

Name: Name of the new event set.

Description: Description about the event set.

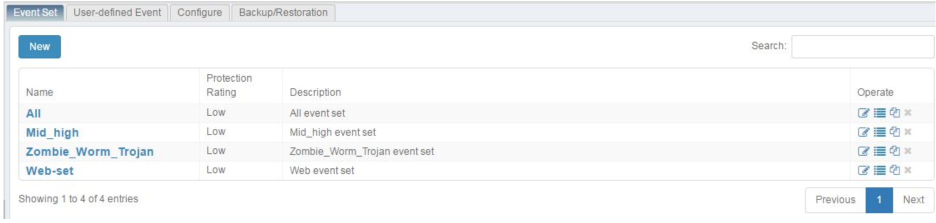
Protection level: Protection level of the event set.

3. Click **Submit** after you complete the settings.

40.2.2 Modifying an Event Set

Procedure:

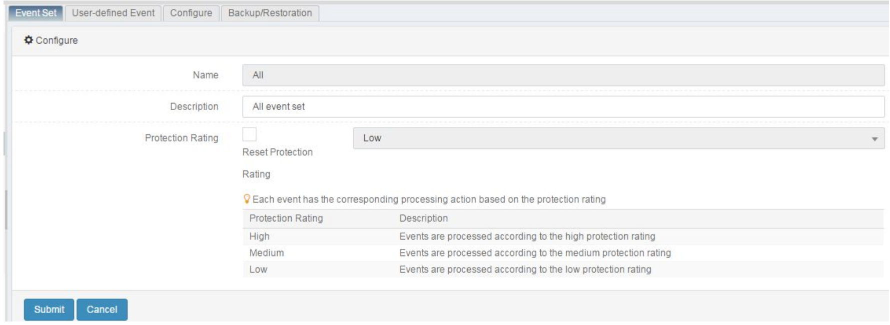
1. Choose **Policy** > **Security** > **Intrusion prevention**. Click ✎ next to an event set.



Name	Protection Rating	Description	Operate
All	Low	All event set	✎ ☰ ⧉ ✖
Mid_high	Low	Mid_high event set	✎ ☰ ⧉ ✖
Zombie_Worm_Trojan	Low	Zombie_Worm_Trojan event set	✎ ☰ ⧉ ✖
Web-set	Low	Web event set	✎ ☰ ⧉ ✖

Showing 1 to 4 of 4 entries

2. Modify **Description** and **Protection level**, and click **Submit**.



Name	All
Description	All event set
Protection Rating	□ Reset Protection Rating Low

Each event has the corresponding processing action based on the protection rating

Protection Rating	Description
High	Events are processed according to the high protection rating
Medium	Events are processed according to the medium protection rating
Low	Events are processed according to the low protection rating

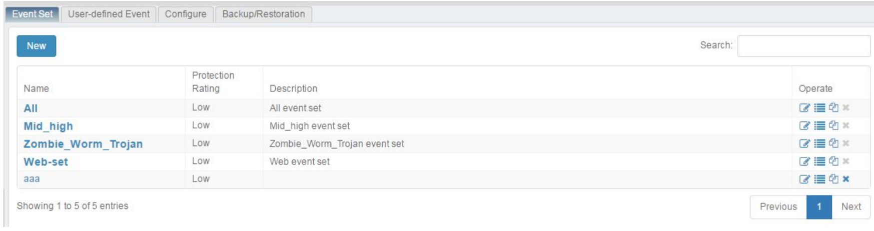
Notice

If you reset the protection level, the action of the event set is reset to the default action specified by the corresponding protection level.

40.2.3 Deleting an Event Set

Procedure:

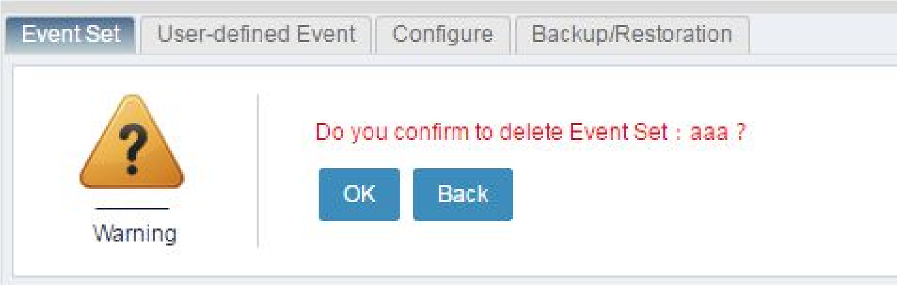
1. Choose **Policy** > **Security** > **Intrusion prevention**. The following page appears.



Name	Protection Rating	Description	Operate
All	Low	All event set	✎ ≡ ⧉ ✖
Mid_high	Low	Mid_high event set	✎ ≡ ⧉ ✖
Zombie_Worm_Trojan	Low	Zombie_Worm_Trojan event set	✎ ≡ ⧉ ✖
Web-set	Low	Web event set	✎ ≡ ⧉ ✖
aaa	Low		✎ ≡ ⧉ ✖

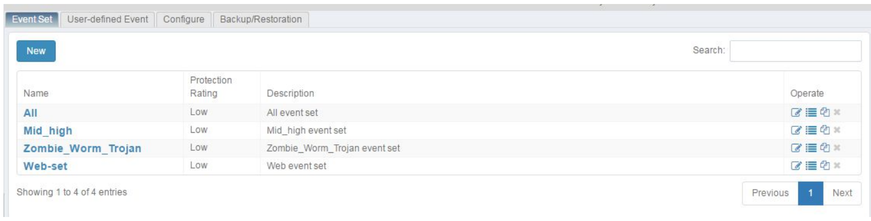
Showing 1 to 5 of 5 entries

2. Click ✖ next to the event set you want to delete.



Do you confirm to delete Event Set : aaa ?

3. Click **OK**, as shown in the following figure.



Name	Protection Rating	Description	Operate
All	Low	All event set	✎ ≡ ⧉ ✖
Mid_high	Low	Mid_high event set	✎ ≡ ⧉ ✖
Zombie_Worm_Trojan	Low	Zombie_Worm_Trojan event set	✎ ≡ ⧉ ✖
Web-set	Low	Web event set	✎ ≡ ⧉ ✖

Showing 1 to 4 of 4 entries

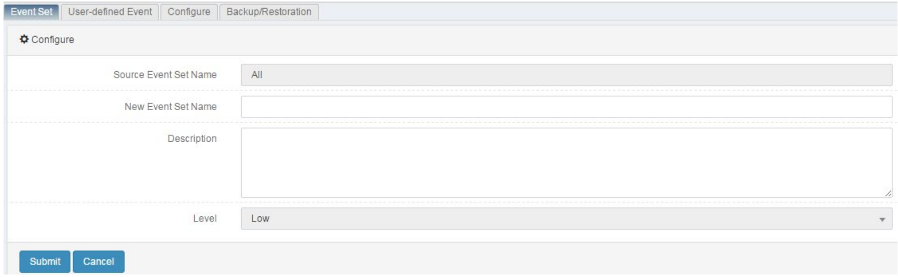
Notice

Predefined event sets and event sets referenced by protection policies cannot be deleted.

40.2.4 Copying an Event Set

Procedure:

1. Choose **Policy** > **Security** > **Intrusion prevention**. Click next to an event set.



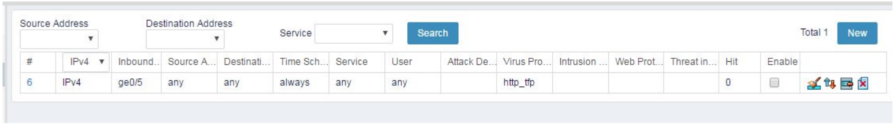
Source Event Set Name	All
New Event Set Name	
Description	
Level	Low

2. Click **Submit** after you complete the settings.

40.2.5 Referencing an Event Set in a Protection Policy

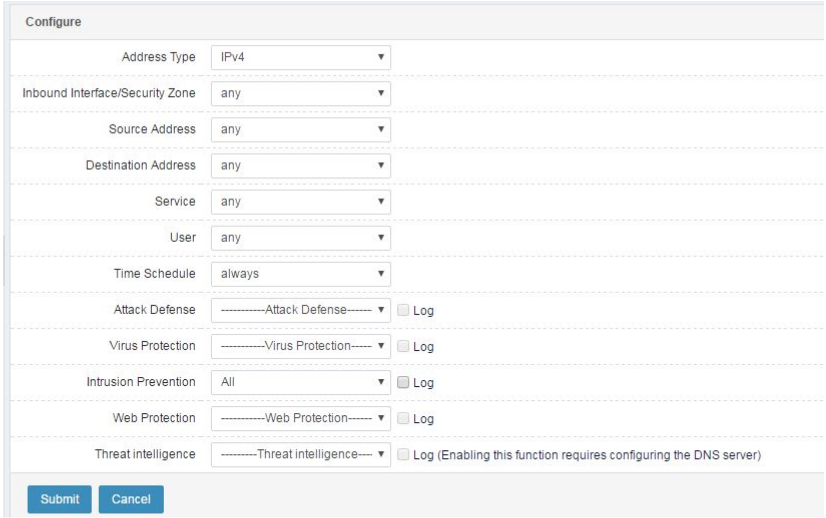
Procedure:

1. Choose **Policy** > **Security** > **Protection policy.** The following page appears.



#	IPv4	Inbound..	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
6	IPv4	ge0/5	any	any	always	any	any		http_tfp				0	□	

2. Click **New** to create a protection policy.



Address Type	IPv4	
Inbound Interface/Security Zone	any	
Source Address	any	
Destination Address	any	
Service	any	
User	any	
Time Schedule	always	
Attack Defense	-----------Attack Defense------	□ Log
Virus Protection	-----------Virus Protection-----	□ Log
Intrusion Prevention	All	□ Log
Web Protection	-----------Web Protection------	□ Log
Threat intelligence	---------Threat intelligence----	□ Log (Enabling this function requires configuring the DNS server)

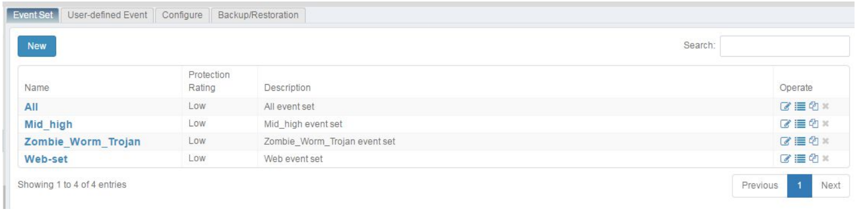
3. Click **Submit** after you complete the settings.

40.3 Event Configuration for Event Sets

40.3.1 Displaying Events

Procedure:

1. Choose **Policy** > **Security** > **Intrusion prevention**. The following page appears.



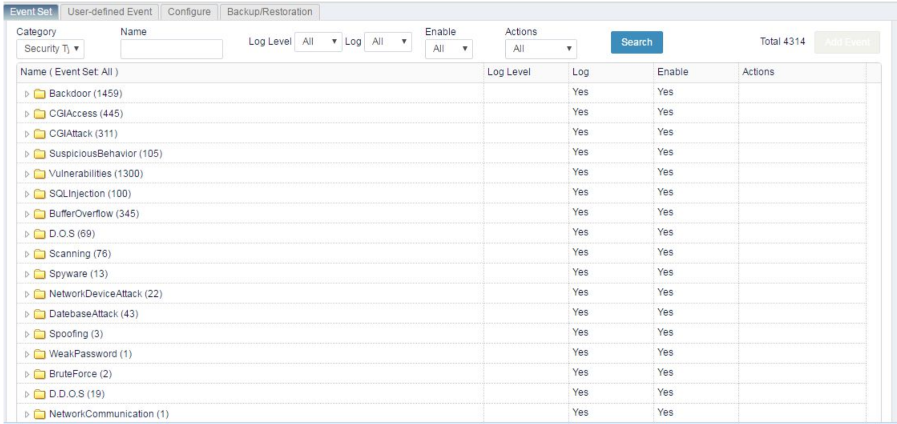
Event Set | User-defined Event | Configure | Backup/Restoration

New   Search:

Name	Protection Rating	Description	Operate
All	Low	All event set	✎ ☰ ⧉ ✕
Mid_high	Low	Mid_high event set	✎ ☰ ⧉ ✕
Zombie_Worm_Trojan	Low	Zombie_Worm_Trojan event set	✎ ☰ ⧉ ✕
Web-set	Low	Web event set	✎ ☰ ⧉ ✕

Showing 1 to 4 of 4 entries   Previous 1 Next

2. Click an event set or ☰ to display the events in an event set.



Event Set | User-defined Event | Configure | Backup/Restoration

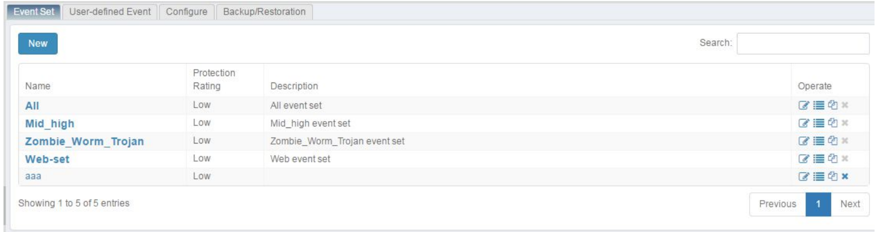
Category: Security T▾ Name: Log Level: All ▾ Log: All ▾ Enable: All ▾ Actions: All ▾ Search Total 4314 Add Event

Name (Event Set: All)	Log Level	Log	Enable	Actions
▷ Backdoor (1459)		Yes	Yes	
▷ CGIAccess (445)		Yes	Yes	
▷ CGIAttack (311)		Yes	Yes	
▷ SuspiciousBehavior (105)		Yes	Yes	
▷ Vulnerabilities (1300)		Yes	Yes	
▷ SQLInjection (100)		Yes	Yes	
▷ BufferOverflow (345)		Yes	Yes	
▷ D.O.S (69)		Yes	Yes	
▷ Scanning (76)		Yes	Yes	
▷ Spyware (13)		Yes	Yes	
▷ NetworkDeviceAttack (22)		Yes	Yes	
▷ DatebaseAttack (43)		Yes	Yes	
▷ Spoofing (3)		Yes	Yes	
▷ WeakPassword (1)		Yes	Yes	
▷ BruteForce (2)		Yes	Yes	
▷ D.D.O.S (19)		Yes	Yes	
▷ NetworkCommunication (1)		Yes	Yes	

40.3.2 Adding Events

Procedure:

1. Choose **Policy** > **Security** > **Intrusion prevention**. The following page appears.



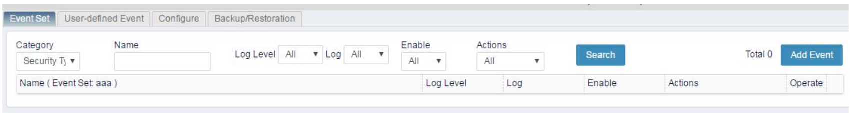
Event Set | User-defined Event | Configure | Backup/Restoration

New   Search:

Name	Protection Rating	Description	Operate
All	Low	All event set	✎ ☰ ⧉ ✕
Mid_high	Low	Mid_high event set	✎ ☰ ⧉ ✕
Zombie_Worm_Trojan	Low	Zombie_Worm_Trojan event set	✎ ☰ ⧉ ✕
Web-set	Low	Web event set	✎ ☰ ⧉ ✕
aaa	Low		✎ ☰ ⧉ ✕

Showing 1 to 5 of 5 entries   Previous 1 Next

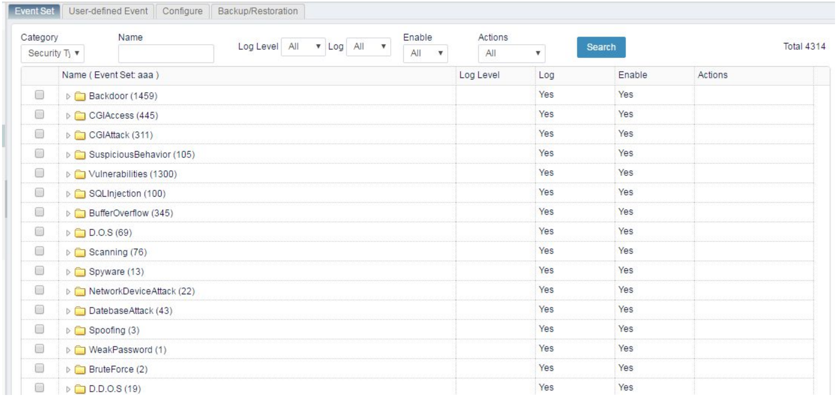
2. Click an event set.



Category: Security Ty ▾ Name: Log Level: All ▾ Log: All ▾ Enable: All ▾ Actions: All ▾ Total 0

Name (Event Set: aaa)	Log Level	Log	Enable	Actions	Operate

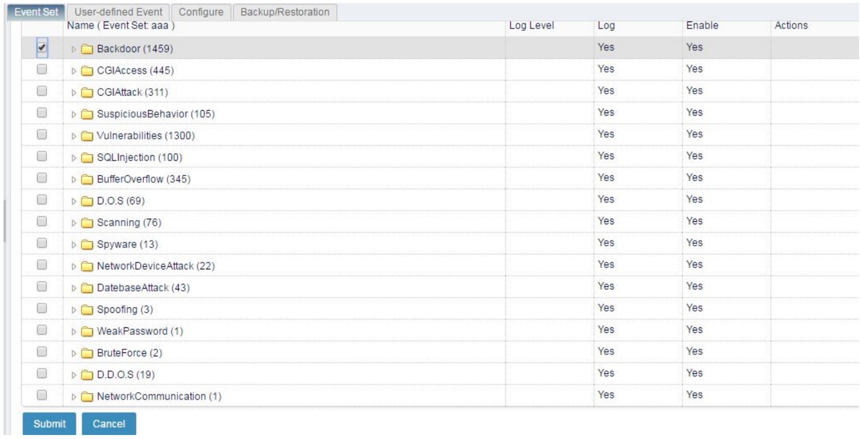
3. Click **Add event**. The page lists the events that can be added, as shown in the following figure.



Category: Security Ty ▾ Name: Log Level: All ▾ Log: All ▾ Enable: All ▾ Actions: All ▾ Total 4314

	Name (Event Set: aaa)	Log Level	Log	Enable	Actions
□	▷ Backdoor (1459)		Yes	Yes	
□	▷ CGIAccess (445)		Yes	Yes	
□	▷ CGIAttack (311)		Yes	Yes	
□	▷ SuspiciousBehavior (105)		Yes	Yes	
□	▷ Vulnerabilities (1300)		Yes	Yes	
□	▷ SQLInjection (100)		Yes	Yes	
□	▷ BufferOverflow (345)		Yes	Yes	
□	▷ D.O.S (69)		Yes	Yes	
□	▷ Scanning (76)		Yes	Yes	
□	▷ Spyware (13)		Yes	Yes	
□	▷ NetworkDeviceAttack (22)		Yes	Yes	
□	▷ DatebaseAttack (43)		Yes	Yes	
□	▷ Spoofing (3)		Yes	Yes	
□	▷ WeakPassword (1)		Yes	Yes	
□	▷ BruteForce (2)		Yes	Yes	
□	▷ D.D.O.S (19)		Yes	Yes	

4. Select the events or event categories you want to add.



	Name (Event Set: aaa)	Log Level	Log	Enable	Actions
☑	▷ Backdoor (1459)		Yes	Yes	
□	▷ CGIAccess (445)		Yes	Yes	
□	▷ CGIAttack (311)		Yes	Yes	
□	▷ SuspiciousBehavior (105)		Yes	Yes	
□	▷ Vulnerabilities (1300)		Yes	Yes	
□	▷ SQLInjection (100)		Yes	Yes	
□	▷ BufferOverflow (345)		Yes	Yes	
□	▷ D.O.S (69)		Yes	Yes	
□	▷ Scanning (76)		Yes	Yes	
□	▷ Spyware (13)		Yes	Yes	
□	▷ NetworkDeviceAttack (22)		Yes	Yes	
□	▷ DatebaseAttack (43)		Yes	Yes	
□	▷ Spoofing (3)		Yes	Yes	
□	▷ WeakPassword (1)		Yes	Yes	
□	▷ BruteForce (2)		Yes	Yes	
□	▷ D.D.O.S (19)		Yes	Yes	
□	▷ NetworkCommunication (1)		Yes	Yes	

5. Click **Submit**.

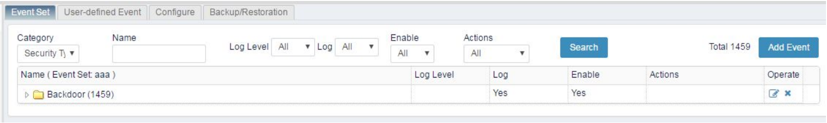
Notice

After an event is added to an event set and you click **Add event**, the event is no longer displayed.

40.3.3 Deleting an Event

Procedure:

1. Choose **Policy** > **Security** > **Intrusion prevention** and click an event set. The following page appears.



Category: Security T ▾ Name: Log Level: All ▾ Log: All ▾ Enable: All ▾ Actions: All ▾ Total 1459

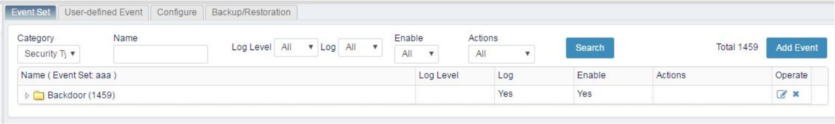
Name (Event Set: aaa)	Log Level	Log	Enable	Actions	Operate
▷ Backdoor (1459)		Yes	Yes		✎ ✖

2. Click ✖ to delete an event or event category.

40.3.4 Modifying an Event

Procedure:

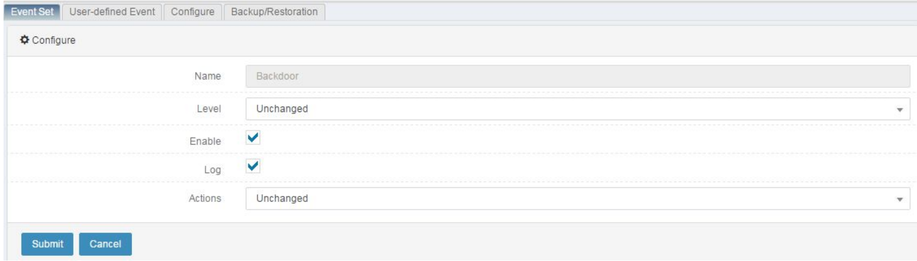
1. Choose **Policy** > **Security** > **Intrusion prevention** and click an event set. The following page appears.



Category: Security T ▾ Name: Log Level: All ▾ Log: All ▾ Enable: All ▾ Actions: All ▾ Total 1459

Name (Event Set: aaa)	Log Level	Log	Enable	Actions	Operate
▷ Backdoor (1459)		Yes	Yes		✎ ✖

2. Click ✎ to modify the settings of an event or event category, as shown in the following figure.



Name: Backdoor

Level: Unchanged

Enable: ☑

Log: ☑

Actions: Unchanged

3. Click **Submit**.

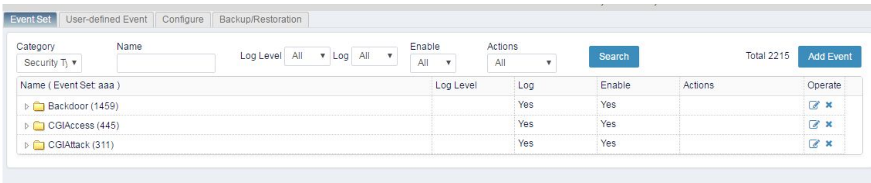
Notice

After an event category is modified, all the event settings under the category are modified.

40.3.5 Searching for Events

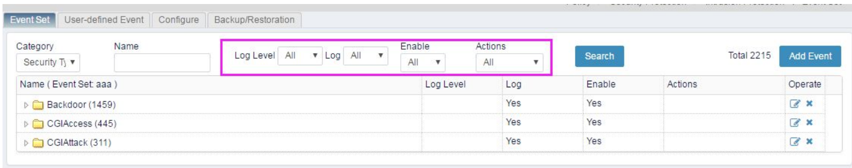
Procedure:

1. Choose **Policy** > **Security** > **Intrusion prevention** and click an event set. The following page appears.



Name (Event Set: aaa)	Log Level	Log	Enable	Actions	Operate
Backdoor (1459)		Yes	Yes		
CGIAccess (445)		Yes	Yes		
CGIAttack (311)		Yes	Yes		

2. Enter search criteria on top and click **Search**, as shown in the following figure.



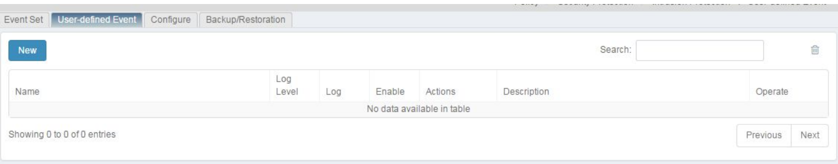
Name (Event Set: aaa)	Log Level	Log	Enable	Actions	Operate
Backdoor (1459)		Yes	Yes		
CGIAccess (445)		Yes	Yes		
CGIAttack (311)		Yes	Yes		

40.4 Custom Event Configuration

40.4.1 Adding a Custom Event

Procedure:

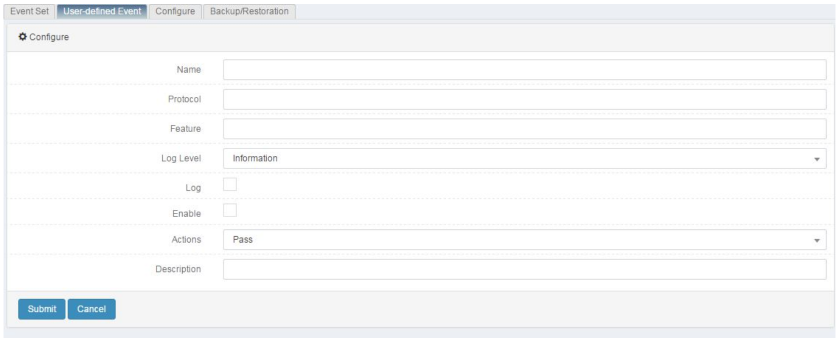
1. Choose **Policy** > **Security** > **Intrusion prevention** > **User-defined Event**. The following page appears.



Name	Log Level	Log	Enable	Actions	Description	Operate
No data available in table						

Showing 0 to 0 of 0 entries

2. Click **New**.



Name	
Protocol	
Feature	
Log Level	Information
Log	□
Enable	□
Actions	Pass
Description	

Parameter description:

Name: Name of a custom event.

Feature: Feature-based matching string. For details, see the following Note.

Level: Level of the custom event.

Enable: Check this box to enable the event.

Log: Check this box to enable logging for the feature event.

Action: Action to be taken for the data that hits the event.

Description: Brief description about the event, no more than 127 characters.

3. Click **Submit** after you complete the settings.

Notice

The following feature string description methods are supported:

1. Conditions connected by AND, for example, icmp_type=8&icmp_payload^abcde
2. OR among multiple values, for example, icmp_type=0,8
3. Search offset and deep definition, for example, icmp_payload[10,100]^abcde
4. Use of multiple operators: equal to (=), greater than (>), smaller than (<), not equal to (~), including (^), and not including (!)
5. Use of the escape character %:
   - Two hexadecimal numbers can be escaped into a byte: icmp_payload^abc%0a%0d.
   - Special characters in an escape expression such as %, [, and] retain their original meanings, for example, icmp_payload^abc%%defwxy.
   - Some symbols with special meanings cannot be escaped into their original meanings. For example, the comma (,), vertical bar (|), and ampersand (&) indicate a logical relationship of an expression and cannot be escaped using %. It is recommended that their original

meanings be expressed using the corresponding hexadecimal numbers with %.

6. Case-sensitive (default) or case-insensitive, which one to apply is indicated by parameters, for example:

■ icmp_payload^aBcD indicates case-sensitive.

■ icmp_payload[,,nocase]^aBcD indicates case-insensitive.

■ icmp_payload[,,case]^aBcD explicitly indicates case-sensitive.

7. Value-type parameters, defined using escape characters by default. You can also choose not to use escape characters by indication in parameters, for example:

■ icmp_payload^abc%0adef

■ icmp_payload^[s]abc%20def

■ icmp_payload=[r]*abc.[c|h]

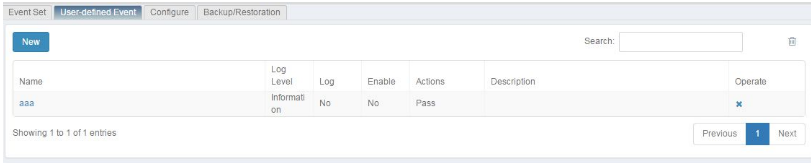
8. Valid value definition, indicated by protocol variables in expressions, for example:

■ telnet_user^root&telnet_passwd

40.4.2 Modifying a Custom Event

Procedure:

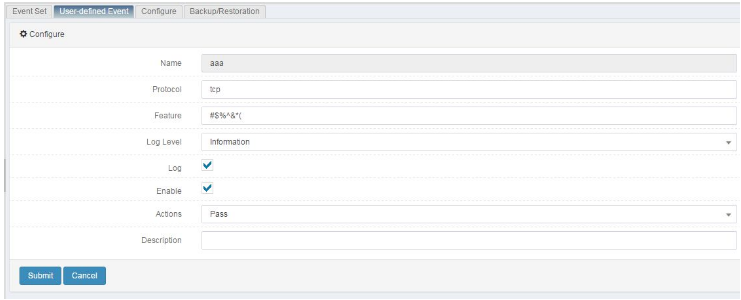
1. Choose **Policy** > **Security** > **Intrusion prevention** >**User-defined Event**. The following page appears.



Name	Log Level	Log	Enable	Actions	Description	Operate
aaa	Information	No	No	Pass		✖

Showing 1 to 1 of 1 entries

2. Click an event name.



Name	aaa
Protocol	tcp
Feature	#$%^&*(
Log Level	Information
Log	☑
Enable	☑
Actions	Pass
Description	

3. Modify the parameters and click **Submit**.

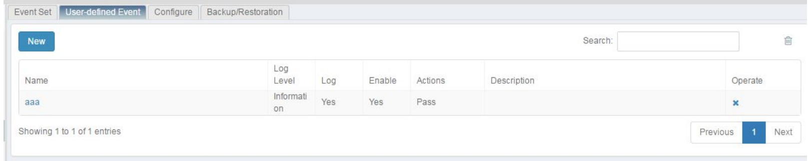
Notice

You cannot create two custom events with the same protocol and features.

40.4.3 Deleting a Custom Event

Procedure:

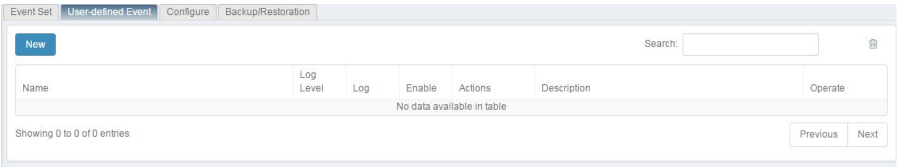
1. Choose **Policy** > **Security** > **Intrusion prevention** > **Custom event**. The following page appears.



Name	Log Level	Log	Enable	Actions	Description	Operate
aaa	Information	Yes	Yes	Pass		✖

Showing 1 to 1 of 1 entries

2. Click 🗑 to clear all custom events.



Name	Log Level	Log	Enable	Actions	Description	Operate
			No data available in table			

Showing 0 to 0 of 0 entries

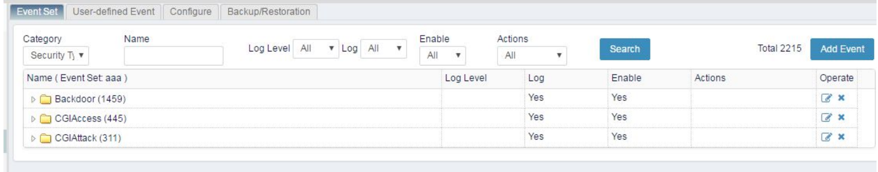
Notice

Custom events referenced by event sets cannot be cleared.

40.4.4 Referencing a Custom Event

Procedure:

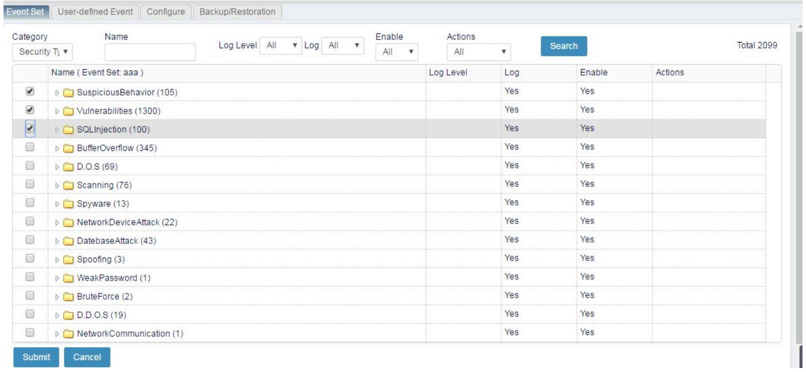
1. Choose **Policy** > **Security** > **Intrusion prevention** and click an event set. The following page appears.



Category: Security T; Name: ; Log Level: All; Log: All; Enable: All; Actions: All; Total 2215

Name (Event Set: aaa)	Log Level	Log	Enable	Actions	Operate
Backdoor (1459)		Yes	Yes		✎ ✖
CGIAccess (445)		Yes	Yes		✎ ✖
CGIAttack (311)		Yes	Yes		✎ ✖

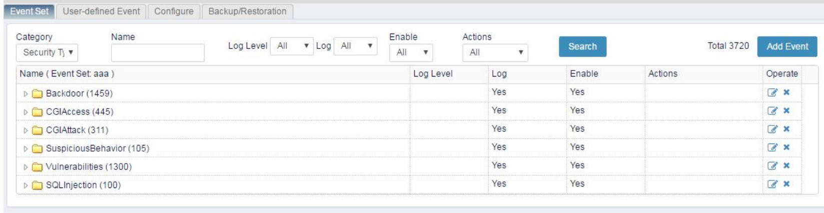
2. Click **Add event.** The page lists the events that can be added.



Category: Security T; Name: ; Log Level: All; Log: All; Enable: All; Actions: All; Search; Total 2099

	Name (Event Set: aaa)	Log Level	Log	Enable	Actions
☑	SuspiciousBehavior (105)		Yes	Yes	
☑	Vulnerabilities (1300)		Yes	Yes	
☑	SQLInjection (100)		Yes	Yes	
□	BufferOverflow (345)		Yes	Yes	
□	D.O.S (69)		Yes	Yes	
□	Scanning (76)		Yes	Yes	
□	Spyware (13)		Yes	Yes	
□	NetworkDeviceAttack (22)		Yes	Yes	
□	DatebaseAttack (43)		Yes	Yes	
□	Spoofing (3)		Yes	Yes	
□	WeakPassword (1)		Yes	Yes	
□	BruteForce (2)		Yes	Yes	
□	D.D.O.S (19)		Yes	Yes	
□	NetworkCommunication (1)		Yes	Yes	

3. Select one or more custom events and click **Submit**.



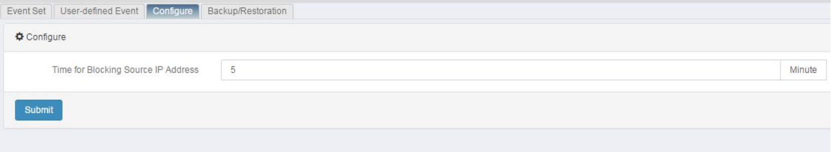
Category: Security T; Name: ; Log Level: All; Log: All; Enable: All; Actions: All; Search; Total 3720

Name (Event Set: aaa)	Log Level	Log	Enable	Actions	Operate
Backdoor (1459)		Yes	Yes		✎ ✖
CGIAccess (445)		Yes	Yes		✎ ✖
CGIAttack (311)		Yes	Yes		✎ ✖
SuspiciousBehavior (105)		Yes	Yes		✎ ✖
Vulnerabilities (1300)		Yes	Yes		✎ ✖
SQLInjection (100)		Yes	Yes		✎ ✖

40.5 Global Configuration: Source IP Address Block Duration

Procedure:

1. Choose **Policy** > **Security** > **Intrusion prevention** > **Configuration.** Set **Source IP address block duration.** The default value is 5 minutes.

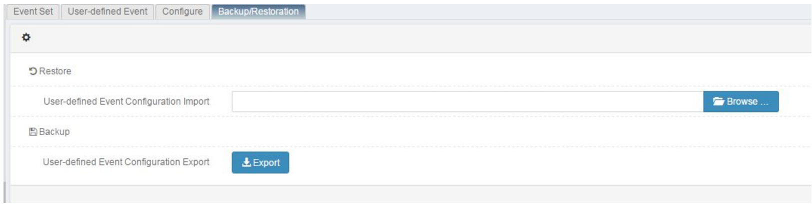


Time for Blocking Source IP Address: 5 Minute

2. Click **Submit**.

40.6 Custom Event Configuration Backup and Restoration

Choose **Policy** > **Security** > **Intrusion prevention** > **Backup and restoration**.



Import Custom event configurations: Select a configuration file to be imported.

Export Custom event configurations: Export a configuration file.

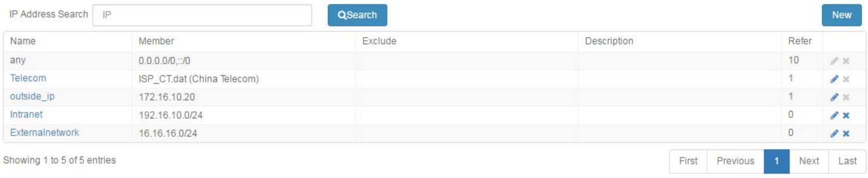
40.7 Configuration Example

Description:

VLAN 1 of a firewall connects to an intranet, and VLAN 2 connects to an external network. When the firewall detects malicious attacks, Trojan, worms, and other security threats in the accessed external services, it triggers intrusion prevention to detect the intrusion event type and handles the intrusion event based on configurations.

Procedure:

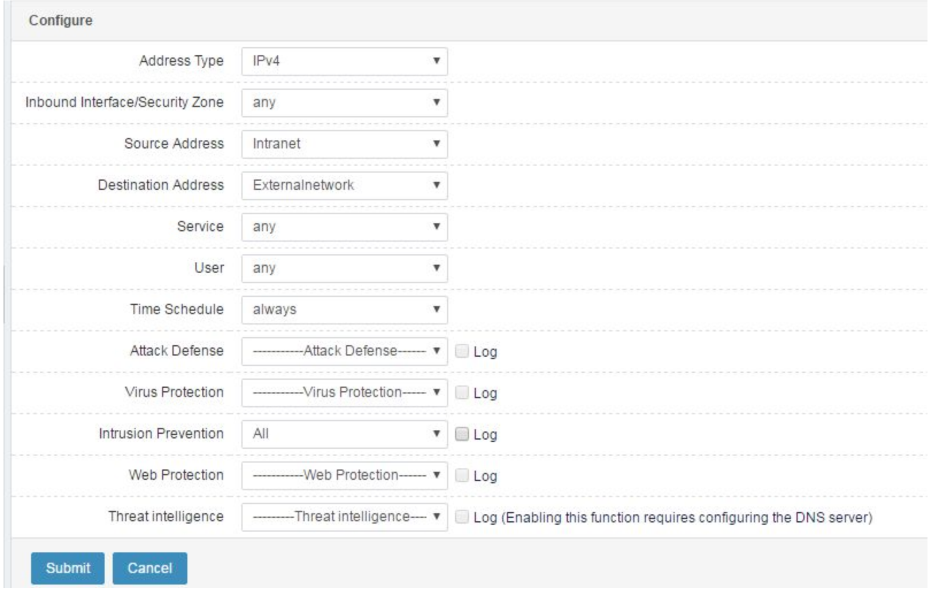
1. Choose **Object** > **Address object** > **Address node**, and configure address objects named **Intranet** and **External network**, as shown in the following figure.



Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			10
Telecom	ISP_CT.dat (China Telecom)			1
outside_ip	172.16.10.20			1
Intranet	192.16.10.0/24			0
Externalnetwork	16.16.16.0/24			0

Showing 1 to 5 of 5 entries

2. Choose **Policy** > **Security** > **Protection policy** and click **New**. Set parameters, as shown in the following figure.

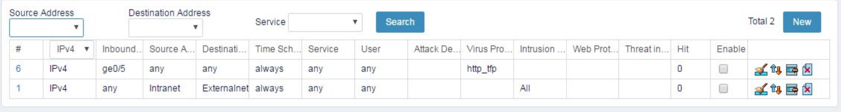


Configure

Address Type	IPv4
Inbound Interface/Security Zone	any
Source Address	Intranet
Destination Address	Externalnetwork
Service	any
User	any
Time Schedule	always
Attack Defense	-----------Attack Defense------ □ Log
Virus Protection	-----------Virus Protection----- □ Log
Intrusion Prevention	All □ Log
Web Protection	-----------Web Protection------ □ Log
Threat intelligence	---------Threat intelligence---- □ Log (Enabling this function requires configuring the DNS server)

3. Click **Submit**.

4. Choose **Policy** > **Security** > **Protection policy.** Check the **Enable** box, as shown in the following figure.



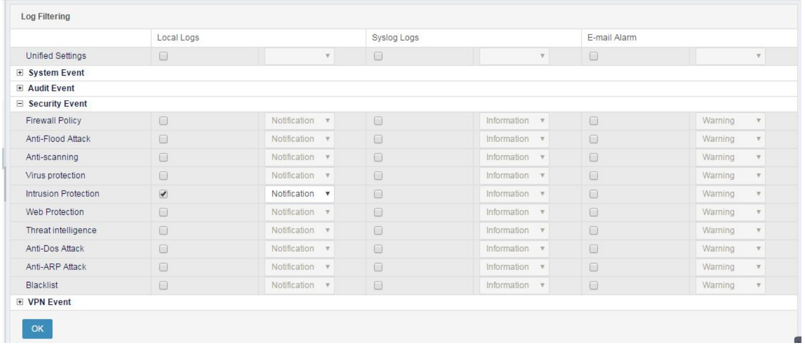
Source Address ▾ Destination Address ▾ Service ▾ Search Total 2 New

#	IPv4 ▾	Inbound...	Source A...	Destinati...	Time Sch...	Service	User	Attack De...	Virus Pro...	Intrusion ...	Web Prot...	Threat in...	Hit	Enable	
6	IPv4	ge0/5	any	any	always	any	any		http_tfp				0	☐	
1	IPv4	any	Intranet	Externalnet	always	any	any			All			0	☐	

40.8 Monitoring

40.8.1 Displaying Intrusion Prevention Logs

1. Choose **Log** > **Log management** > **Log filter**. Select logs related to the intrusion prevention module, and set the log level. Click **OK.**

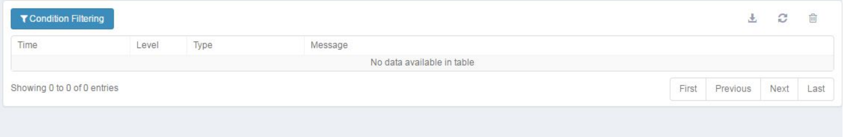


Log Filtering

	Local Logs		Syslog Logs		E-mail Alarm	
Unified Settings	☐	▾	☐	▾	☐	▾
⊞ System Event						
⊞ Audit Event						
⊟ Security Event						
Firewall Policy	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Anti-Flood Attack	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Anti-scanning	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Virus protection	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Intrusion Protection	☑	Notification ▾	☐	Information ▾	☐	Warning ▾
Web Protection	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Threat intelligence	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Anti-Dos Attack	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Anti-ARP Attack	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
Blacklist	☐	Notification ▾	☐	Information ▾	☐	Warning ▾
⊞ VPN Event						

OK

2. Choose **Log** > **Security log** > **Intrusion prevention** to display related logs.



Condition Filtering

Time	Level	Type	Message
			No data available in table

Showing 0 to 0 of 0 entries

First Previous Next Last

41 Web Protection

41.1 Overview

Web protection policies defend against XSS attacks and SQL injection attacks. XSS is a computer vulnerability often seen in web applications. It allows malicious web users to implant code including HTML code and client scripts into pages provided to other users. SQL injection attack is a database attack technique commonly used by hackers by taking advantage of the fact that a large portion of code does not perform validity check on user-input data. An attacker can submit database query code to retrieve desired data based on the program-returned results.

The web protection module defends against XSS attacks and SQL injection attacks based on a feature database. It adopts mode-based matching to check HTTP-submitted information and feature-based matching to detect attacks that match the XSS and SQL features. Once such an attack is detected, the module submits a log and denies or permits the connection based on the predefined action.

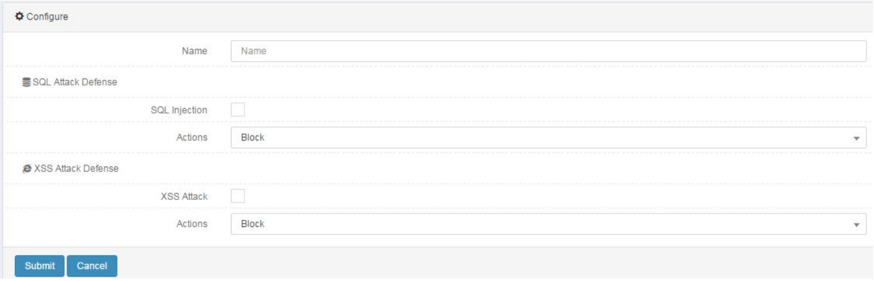
41.2 Configuration

41.2.1 Configuring Basic Policy Elements

The basic elements of a web protection policy are the policy name, anti-SQL injection attack switch, and anti-XSS attack switch. The Permit and Deny actions are supported for handling detected attacks.

Procedure:

1. Choose **Policy** > **Security** > **Web protection** and click **New**.



Configure

Name: Name

SQL Attack Defense

SQL Injection □

Actions: Block

XSS Attack Defense

XSS Attack □

Actions: Block

Parameter description:

Name: Name of the new policy.

SQL injection: Check this box to enable anti-SQL injection attack.

Action: The options are **Permit** and **Deny**.

XSS attack: Check this box to enable anti-XSS attack.

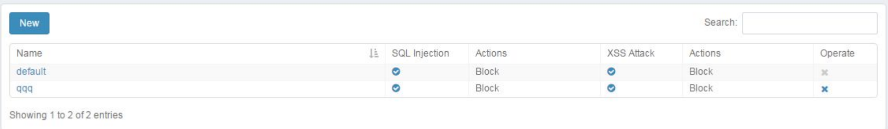
Action: The options are **Permit** and **Deny**.

2. Click **Submit** after you complete the settings.

Note

A web protection policy is uniquely identified by a name.

Anti-SQL injection attack and anti-XSS attack take effect only after being enabled.



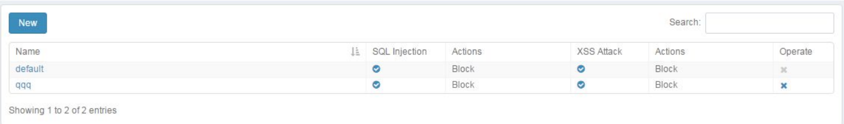
Name	SQL Injection	Actions	XSS Attack	Actions	Operate
default	✓	Block	✓	Block	✕
qqq	✓	Block	✓	Block	✕

Showing 1 to 2 of 2 entries

41.2.2 Modifying a Web Protection Policy

Procedure:

1. Choose **Policy** > **Security** > **Web protection** and click a policy name.



Name	SQL Injection	Actions	XSS Attack	Actions	Operate
default	✓	Block	✓	Block	✕
qqq	✓	Block	✓	Block	✕

Showing 1 to 2 of 2 entries

2. Modify the information about the web protection policy and click **Submit**.

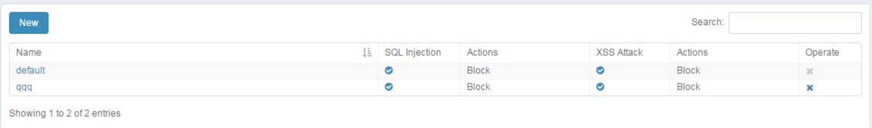
Note

Web protection provides a default template with anti-SQL injection attack and anti-XSS attack enabled.

41.2.3 Deleting a Web Protection Policy

Procedure:

1. Choose **Policy** > **Security** > **Web protection policy.** The following page appears.



Name	SQL Injection	Actions	XSS Attack	Actions	Operate
default	✓	Block	✓	Block	✕
qqq	✓	Block	✓	Block	✕

Showing 1 to 2 of 2 entries

2. Click ✕ next to the web protection policy you want to delete.

42 Anti-DoS

42.1 Overview

Anti-DoS is designed to enable a firewall to block external attacks while ensuring normal communication between internal and external networks. Both devices and intranets are protected. An alert is sent to users when an attack is detected.

Common DoS attacks include ping of death, teardrop attack, Jolt2 attack, SYN fragment, Land-Base, WinNuke, and Smurf.

Scan is a type of network attack. Before mounting a scan attack, the attacker attempts to determine the TCP/UDP ports enabled on the target. A port is usually enabled for an application to run.

Common scan attacks include:

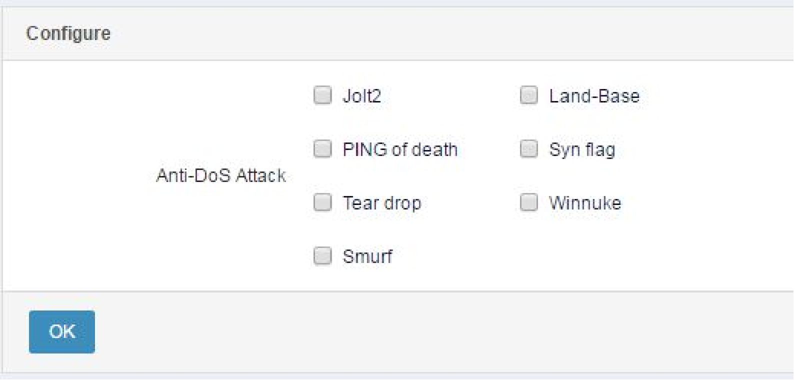
- A vertical scan is targeted at multiple ports of the same host.
- A horizontal scan is targeted at the same port of multiple hosts.
- An ICMP (ping) sweep is aimed to discover active hosts within an address range by sending ping packets.

RAVEN 5000 firewalls effectively prevent the preceding scan events to block external attacks and protect devices and intranets. An alert is sent to users when an attack is detected.

42.2 Configuration

Procedure:

1. Choose **Policy** > **Security** > **Anti-DoS** > **Configuration**.



Configure

Anti-DoS Attack

□ Jolt2 □ Land-Base

□ PING of death □ Syn flag

□ Tear drop □ Winnuke

□ Smurf

Anti-DoS

Jolt2: A Jolt2 attack sends packets with the packet length plus packet offset exceeding 65535 to the target host, making the host crash due to abnormal processing.

A firewall configured with anti-Jolt2 attack can detect Jolt2 attacks, drop attack packets, and output alarms and logs.

Land-Base: A Land-Base attack sends packets with the source address the same as the destination address to the target host, making the host crash after consuming many system resources.

A firewall configured with anti-Land-Base attack can detect Land-Base attacks, drop attack packets, and output alarms and logs.

PING of death: A ping of death attack sends ICMP packets longer than 65535 to the target host, making the host crash due to abnormal processing.

A firewall configured with anti-ping of death attack can detect ping of death attacks, drop attack packets, and output alarms and logs.

Syn flag: An SYN flag attack sends incorrect TCP-identified combined packets to the target host to waste host resources.

A firewall configured with anti-SYN flag attack can detect SYN flag attacks, drop attack packets, and output alarms and logs.

Tear drop: A teardrop attack sends fragmented packets with packet offset overlap to the target host, making the host crash due to abnormal processing.

A firewall configured with anti-teardrop attack can detect teardrop attacks and output alarms and logs. Because normal packets may also have packet offset overlap, RAVEN5000 firewalls do not drop the packets, but tailor and reassemble the packets before sending them.

Winnuke: A WinNuke attack sends outband packets with the TCP emergency flag bit URG set to 1 to ports 139, 138, 137, and 113 of the target host, making the host crash due to abnormal processing.

A firewall configured with anti-WinNuke attack can detect WinNuke attack packets, convert the packet's TCP emergency flag bit to 0 before forwarding the packet, and output alarms and logs.

Smurf: A Smurf attack combines with IP address spoofing and ICMP response to flood the target system with many network transmissions, causing the system to deny normal services. A Smurf attack floods the victim host with ICMP request (ping) packets with the response address changed to the victim network's broadcast address, causing all the hosts in the network to respond to the ICMP request packets, resulting in network congestion.

2. Click **Submit** after you complete the settings.

42.3 Configuration Example

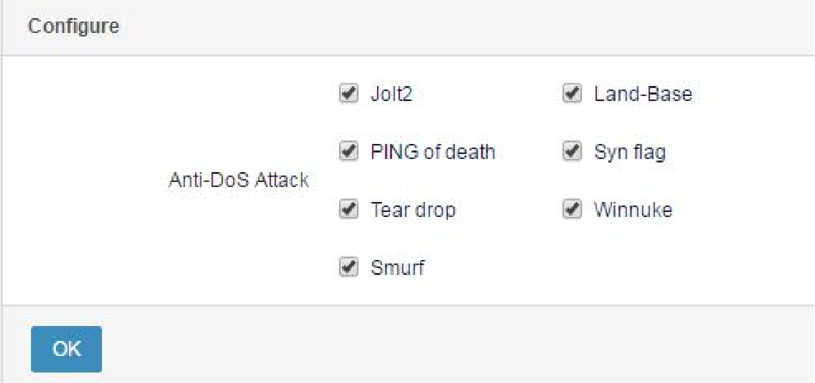
42.3.1 Configuring Anti-DoS

Description:

When a network has many attack packets, you can capture packets or check flow information to determine whether an attack occurs. Attack packets occupy many resources, affecting the performance of the protected hosts and devices. In this case, capture packets or check flow information to identify the attack and enable anti-attack to protect intranets and devices. Configure the firewall to trigger anti-Land-Base attack, drop attack packets, and output alarms and logs when receiving a packet with the source address the same as the destination address.

Procedure:

1. Choose **Policy** > **Security** > **Anti-DoS** > **Configuration**. Complete the settings on the displayed page, as shown in the following figure.



Configure

Anti-DoS Attack

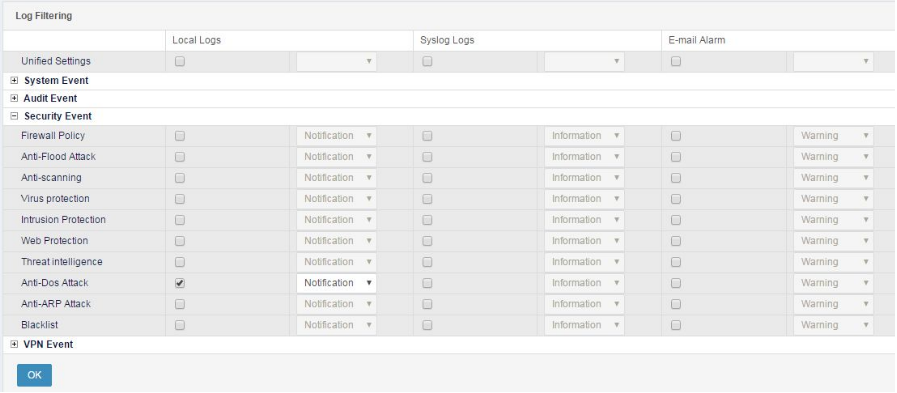
☑ Jolt2 ☑ Land-Base

☑ PING of death ☑ Syn flag

☑ Tear drop ☑ Winnuke

☑ Smurf

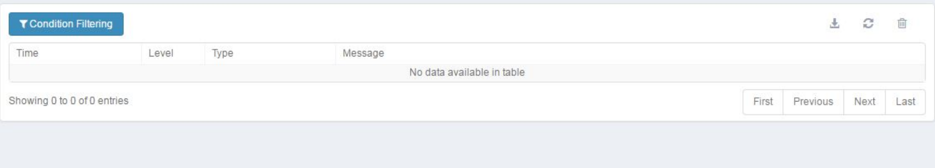
2. Click **OK**.
3. Choose **Log** > **Log management** > **Log filter**. Select logs related to the anti-DoS module, and set the log level. Click **OK**.



Log Filtering

	Local Logs		Syslog Logs		E-mail Alarm	
Unified Settings	□		□		□	
⊞ System Event						
⊞ Audit Event						
⊟ Security Event						
Firewall Policy	□	Notification	□	Information	□	Warning
Anti-Flood Attack	□	Notification	□	Information	□	Warning
Anti-scanning	□	Notification	□	Information	□	Warning
Virus protection	□	Notification	□	Information	□	Warning
Intrusion Protection	□	Notification	□	Information	□	Warning
Web Protection	□	Notification	□	Information	□	Warning
Threat intelligence	□	Notification	□	Information	□	Warning
Anti-Dos Attack	☑	Notification	□	Information	□	Warning
Anti-ARP Attack	□	Notification	□	Information	□	Warning
Blacklist	□	Notification	□	Information	□	Warning
⊞ VPN Event						

4. Choose **Log** > **Security log** > **Anti-attack** > **Anti-DoS** to display related logs.



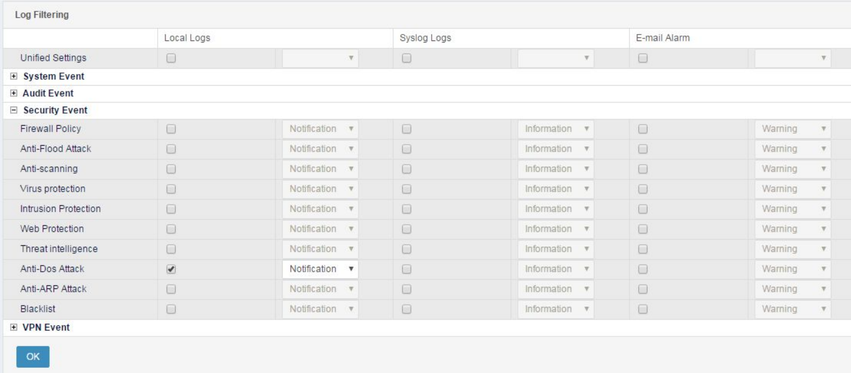
Time	Level	Type	Message
No data available in table			

Showing 0 to 0 of 0 entries

42.4 Monitoring and Maintenance

42.4.1 Displaying Anti-attack Logs

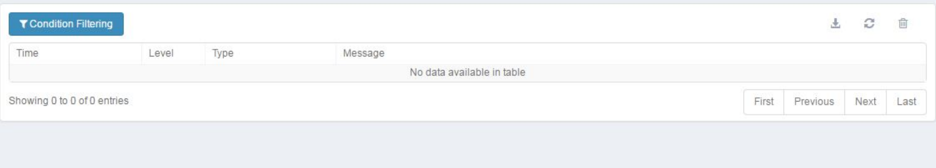
1. Choose **Log** > **Log management** > **Log filter**. Select logs related to the anti-DoS module, and set the log level. Click **OK**.



Log Filtering

	Local Logs		Syslog Logs		E-mail Alarm	
Unified Settings	□		□		□	
⊞ System Event						
⊞ Audit Event						
⊟ Security Event						
Firewall Policy	□	Notification	□	Information	□	Warning
Anti-Flood Attack	□	Notification	□	Information	□	Warning
Anti-scanning	□	Notification	□	Information	□	Warning
Virus protection	□	Notification	□	Information	□	Warning
Intrusion Protection	□	Notification	□	Information	□	Warning
Web Protection	□	Notification	□	Information	□	Warning
Threat intelligence	□	Notification	□	Information	□	Warning
Anti-Dos Attack	☑	Notification	□	Information	□	Warning
Anti-ARP Attack	□	Notification	□	Information	□	Warning
Blacklist	□	Notification	□	Information	□	Warning
⊞ VPN Event						

2. Choose **Log** > **Security log** > **Anti-attack** > **Anti-DoS** to display related logs.



Time	Level	Type	Message
No data available in table			

Showing 0 to 0 of 0 entries

42.5 Troubleshooting

42.5.1 Anti-SYN Flood Fails

Sympto m	The anti-SYN flood feature fails, and SYN flood packets traverse the firewall.
Analysis	Check whether the anti-SYN flood service is disabled or the attack threshold is set to a large value.
Solution	1. Check whether the TCP half-open connections count is displayed. If **-** is displayed, the IP inspect module is disabled. 2. Check whether the anti-SYN flood service is enabled. If not, enable it. 3. Check whether the attack threshold is set to a large value. If yes, reduce the value.

42.5.2 No Alarms Are Generated and No Packets Denied After Anti-scan Is Configured

Symptom	The firewall does not generate an alarm nor denies packets after a scan attack is identified by means of packet capture or flow collection.
Analysis	The possible causes are as follows: 1. The scan identification threshold is set to a large value, and the scan count has not reached the threshold. 2. The TCP half-open connections limit is configured for anti-scan, anti-SYN flood, and session management, which have overlapping functions. The anti-scan feature may not take effect after the other features are triggered.
Solution	Check the configurations, and reduce the threshold value if necessary.

43 Anti-ARP Attack

43.1 Overview

Communication in a LAN requires IP-to-MAC address conversion over ARP. ARP is essential for network security. However, ARP has many potential risks because its design does not fully consider security issues. ARP attacks are common in network environments.

By forging IP and MAC addresses, ARP spoofing generates a large volume of ARP communication to cause network congestion. An attacker can keep sending forged ARP response packets to modify the target host's ARP cache, causing network interruption or man-in-the-middle attacks.

ARP attacks result in abnormal Internet access, ARP packet explosion, abnormal or incorrect MAC addresses, mapping of one MAC address to multiple IP addresses, and IP address conflict. ARP attacks are easy to implement with low technical barrier, and occur frequently in networks. Effective anti-ARP attack is necessary for ensuring smooth network conditions.

RAVEN5000 firewalls provide the anti-ARP attack feature to effectively identify ARP spoofing and ARP floods and generate alarms on suspicious attack behaviors. Anti-ARP attack can be combined with IP-MAC address binding, active packet-sending protection, and ARP learning off features to prevent the damage of ARP attacks.

43.2 Configuration

43.2.1 Default Configurations

By default, the anti-ARP attack feature is disabled. The following table lists the default configurations of anti-ARP attack.

Table 43-1 Default configurations of anti-ARP attack

Parameter	Default Value	Remarks
Enable/Disable anti-ARP attack	Disabled	The default value can be changed.
Enable/Disable active protection	Disabled	The default value

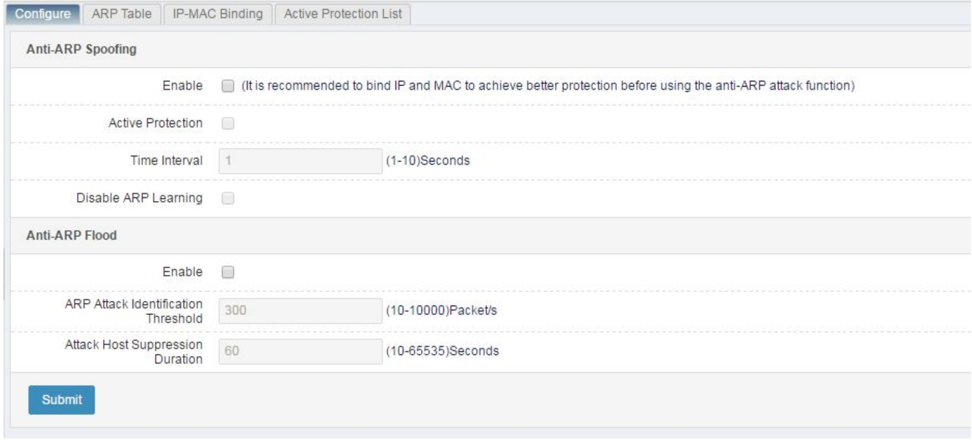
Parameter	Default Value	Remarks
		can be changed.
Active protection interval	1s	The default value can be changed.
Active protection list	Empty	Lists can be added.
Enable/Disable ARP learning	Enabled	The default value can be changed.
Enable/Disable status ARP flood prevention	Disabled	The default value can be changed.
ARP attack identification threshold	300	The default value can be changed.
ARP attacking host suppression duration	60s	The default value can be changed.

43.2.2 Basic Configurations

Anti-ARP attack configuration includes anti-ARP spoofing configuration and anti-ARP flood configuration.

Procedure:

1. Choose **Policy** > **Security** > **Anti-ARP attack** > **Configuration**.



Anti-ARP Spoofing

Enable □ (It is recommended to bind IP and MAC to achieve better protection before using the anti-ARP attack function)

Active Protection □

Time Interval 1 (1-10)Seconds

Disable ARP Learning □

Anti-ARP Flood

Enable □

ARP Attack Identification Threshold 300 (10-10000)Packet/s

Attack Host Suppression Duration 60 (10-65535)Seconds

Parameter description:

Anti-ARP spoofing: Check the **Enable** box to trigger an alarm for detected ARP spoofing.

Active protection: Check this box to enable periodic sending of free ARP packet in the active protection list.

Interval: Interval of sending ARP packets in the active protection list. The default value is 1s.

Disable ARP learning: By default, ARP learning is enabled. After it is disabled, packets that do not match the bound IP-MAC address binding table are dropped.

Anti-ARP flood: Check the **Enable** box to enable anti-ARP flood.

ARP attack identification threshold: APR packets received per second. The default value is **300**.

Attacking host suppression duration: Duration for which packets from a malicious host are blocked after an attack is detected. The default value is **60s**.

2. Click **Submit** after you complete the settings.

Notice

After ARP learning is disabled, packets that do not match the specified IP-MAC address binding table are dropped. Therefore, it is strongly recommended that you create an IP-MAC address binding table before disabling ARP learning.

Note

Active protection and ARP learning can be configured only after anti-ARP spoofing is enabled.

The active packet sending interval can be set only after active protection is enabled.

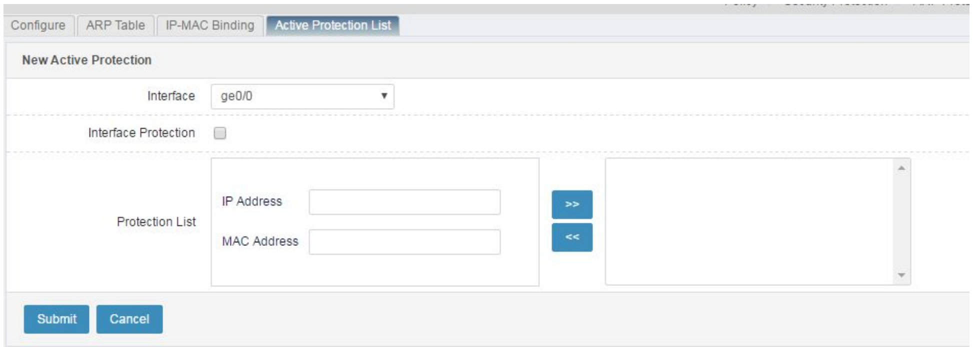
The ARP attack identification threshold and attacking host suppression duration can be set only after anti-ARP flood is enabled.

43.2.3 Configuring an Active Protection List

After you configure an active protection list and enable active protection, the free ARP packets in the list will be sent in broadcast mode.

Procedure:

1. Choose **Policy** > **Security** > **Anti-ARP attack** > **Active protection** and click **New**.



New Active Protection

Interface: ge0/0

Interface Protection ☐

Protection List
IP Address
MAC Address

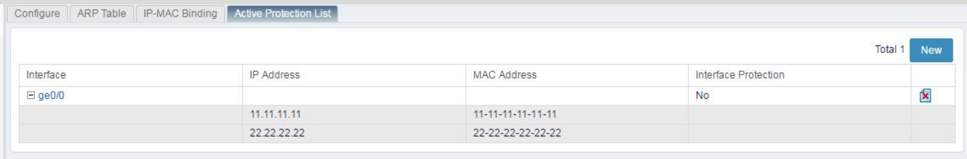
Parameter description:

Interface: Interface that sends ARP packets.

Interface protection: Check this box to add interface addresses to the active protection list.

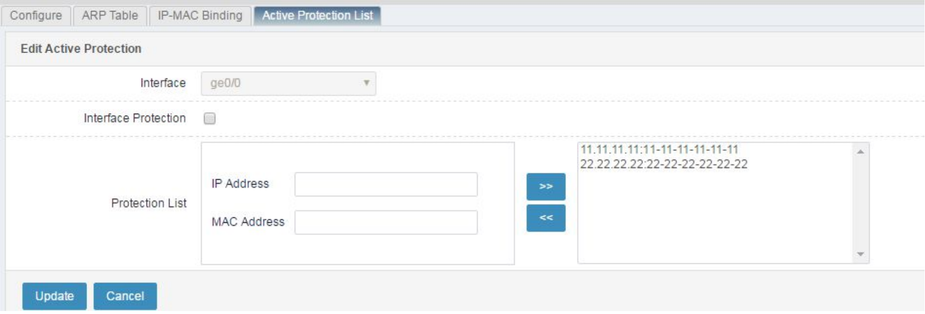
IP address & MAC address: IP address and MAC address that broadcast ARP packets.

2. Click **Submit** after you complete the settings.



Interface	IP Address	MAC Address	Interface Protection	
⊟ ge0/0			No	☒
	11.11.11.11	11-11-11-11-11-11		
	22.22.22.22	22-22-22-22-22-22		

Click an interface name to modify it.



Edit Active Protection

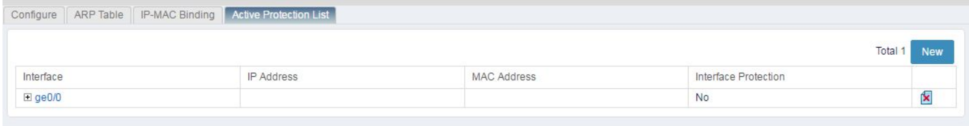
Interface	ge0/0
Interface Protection	□
Protection List	IP Address MAC Address

11.11.11.11:11-11-11-11-11-11
22.22.22.22:22-22-22-22-22-22

The **Interface** parameter cannot be modified. For details about other parameters, see the creation procedure.

Delete an active protection list as follows:

Click ☒ next to an interface to delete its active protection list settings.

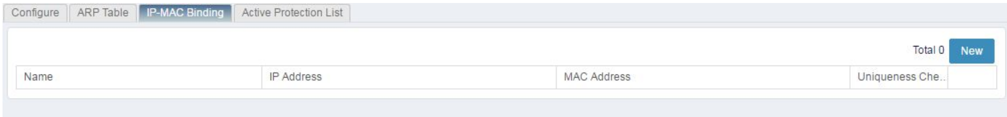


Interface	IP Address	MAC Address	Interface Protection	
⊞ ge0/0			No	☒

43.2.4 Configuring IP-MAC Address Binding

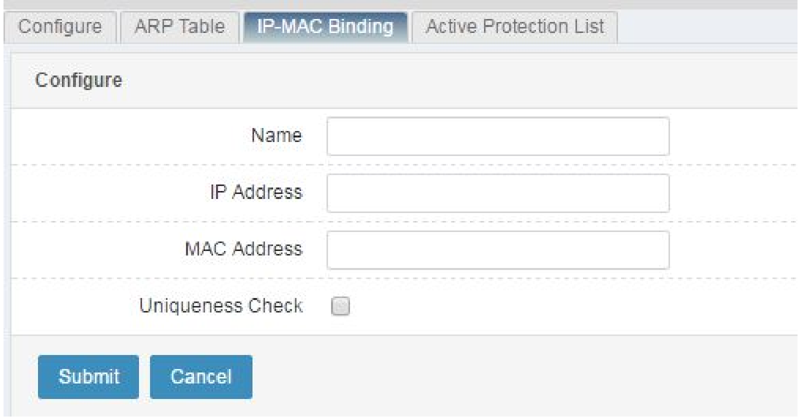
Procedure:

1. Choose **Policy** > **Security** > **Anti-ARP attack** > **IP-MAC address binding**.



Name	IP Address	MAC Address	Uniqueness Che..

Click **New**.



Configure

Name

IP Address

MAC Address

Uniqueness Check □

Parameter description:

Name: Name of an IP-MAC address binding entry.

IP address: Bound IP address.

MAC address: Bound MAC address.

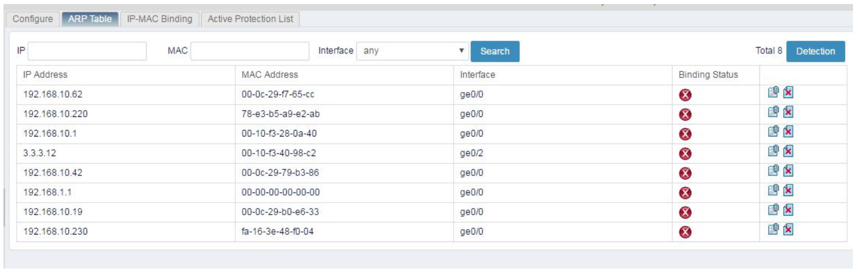
Uniqueness check: Check this box to bind a MAC address to only one IP address.

2. Click **Submit** after you complete the settings.

43.2.5 ARP Table

Choose **Policy** > **Security** > **Anti-ARP attack** > **ARP table**.

Enter an IP address, a MAC address, and an interface, and click **Search**.



IP

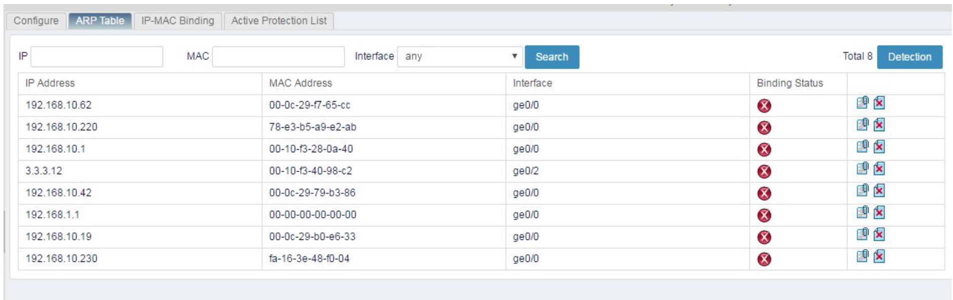
MAC

Interface any

IP Address	MAC Address	Interface	Binding Status	
192.168.10.62	00-0c-29-f7-65-cc	ge0/0	⊗	
192.168.10.220	78-e3-b5-a9-e2-ab	ge0/0	⊗	
192.168.10.1	00-10-f3-28-0a-40	ge0/0	⊗	
3.3.3.12	00-10-f3-40-98-c2	ge0/2	⊗	
192.168.10.42	00-0c-29-79-b3-86	ge0/0	⊗	
192.168.1.1	00-00-00-00-00-00	ge0/0	⊗	
192.168.10.19	00-0c-29-b0-e6-33	ge0/0	⊗	
192.168.10.230	fa-16-3e-48-f0-04	ge0/0	⊗	

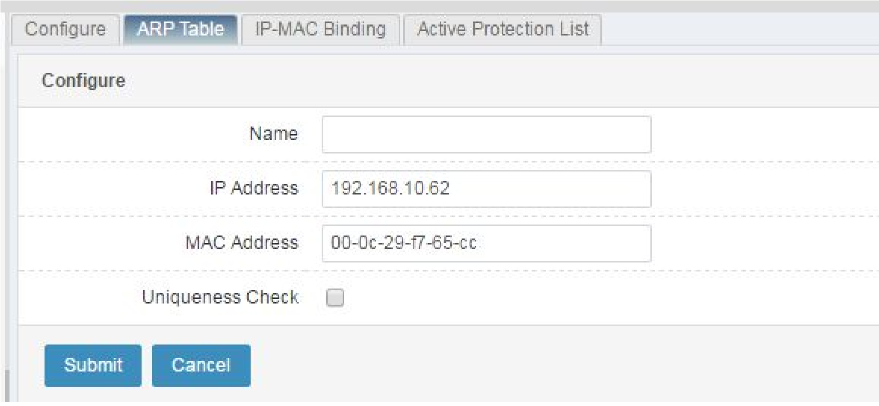
Perform IP-MAC address binding in an ARP table as follows:

Choose **Policy** > **Security** > **ARP table**.



IP Address	MAC Address	Interface	Binding Status	
192.168.10.62	00-0c-29-f7-65-cc	ge0/0	✗	
192.168.10.220	78-e3-b5-a9-e2-ab	ge0/0	✗	
192.168.10.1	00-10-f3-28-0a-40	ge0/0	✗	
3.3.3.12	00-10-f3-40-98-c2	ge0/2	✗	
192.168.10.42	00-0c-29-79-b3-86	ge0/0	✗	
192.168.1.1	00-00-00-00-00-00	ge0/0	✗	
192.168.10.19	00-0c-29-b0-e6-33	ge0/0	✗	
192.168.10.230	fa-16-3e-48-f0-04	ge0/0	✗	

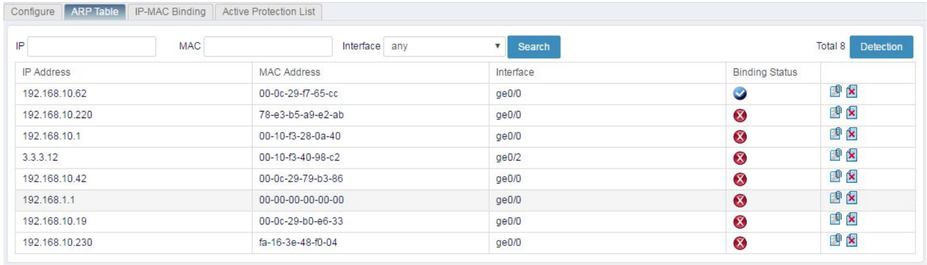
Click to bind an IP address and a MAC address learned by the firewall.



Configure

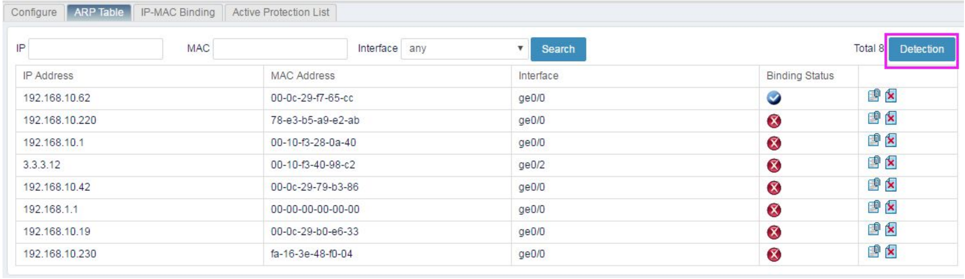
Name	
IP Address	192.168.10.62
MAC Address	00-0c-29-f7-65-cc
Uniqueness Check	□

After successful binding, ✓ is displayed on the **ARP table** tab.

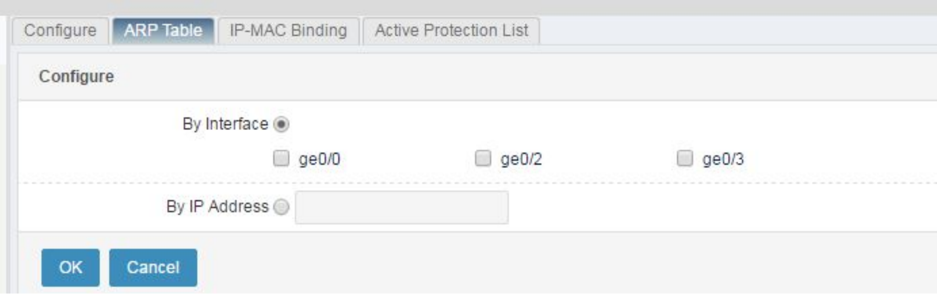


IP Address	MAC Address	Interface	Binding Status	
192.168.10.62	00-0c-29-f7-65-cc	ge0/0	✓	
192.168.10.220	78-e3-b5-a9-e2-ab	ge0/0	✗	
192.168.10.1	00-10-f3-28-0a-40	ge0/0	✗	
3.3.3.12	00-10-f3-40-98-c2	ge0/2	✗	
192.168.10.42	00-0c-29-79-b3-86	ge0/0	✗	
192.168.1.1	00-00-00-00-00-00	ge0/0	✗	
192.168.10.19	00-0c-29-b0-e6-33	ge0/0	✗	
192.168.10.230	fa-16-3e-48-f0-04	ge0/0	✗	

ARP detection: Click **Detection** in the upper-right corner to detect ARP attacks by interface or IP address.



IP Address	MAC Address	Interface	Binding Status	
192.168.10.62	00-0c-29-f7-65-cc	ge0/0	✓	
192.168.10.220	78-e3-b5-a9-e2-ab	ge0/0	✗	
192.168.10.1	00-10-f3-28-0a-40	ge0/0	✗	
3.3.3.12	00-10-f3-40-98-c2	ge0/2	✗	
192.168.10.42	00-0c-29-79-b3-86	ge0/0	✗	
192.168.1.1	00-00-00-00-00-00	ge0/0	✗	
192.168.10.19	00-0c-29-b0-e6-33	ge0/0	✗	
192.168.10.230	fa-16-3e-48-f0-04	ge0/0	✗	



Configure

By Interface ●

□ ge0/0 □ ge0/2 □ ge0/3

By IP Address ○

After you select an interface, the system detects ARP attacks on all the devices connected to the interface.

After you select an IP address, the system detects ARP attacks from the address.

43.3 Configuration Example

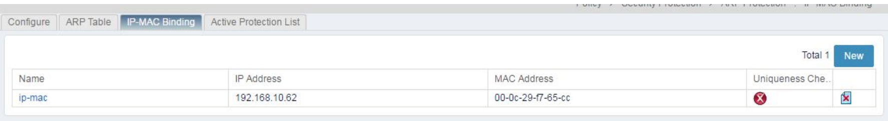
43.3.1 Configuring Anti-ARP Spoofing and Anti-ARP Flood

Description:

Configure anti-ARP spoofing and anti-ARP flood to detect ARP attacks in the network.

Procedure:

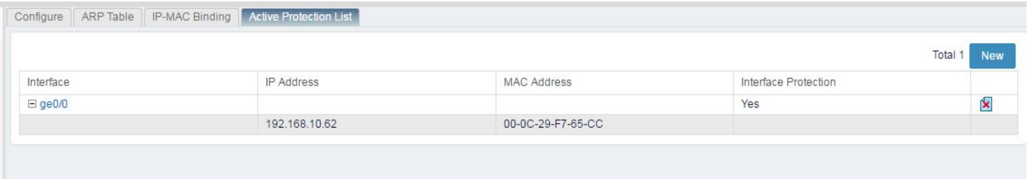
1. Bind IP and MAC addresses. You can bind the IP and MAC addresses learned by the firewall in an ARP table. For offline hosts, you can add IP-MAC address pairs manually.



Total 1

Name	IP Address	MAC Address	Uniqueness Che..	
ip-mac	192.168.10.62	00-0c-29-f7-65-cc	☒	☒

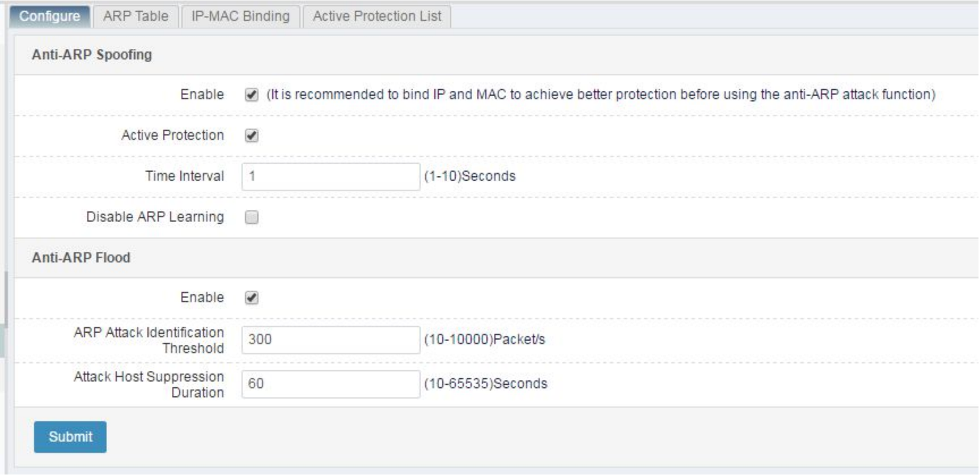
2. Configure an active protection list to protect important internal host resources. ARP spoofing can be prevented by actively sending the ARP information of important hosts. For example, you can add an internal mail server address.



Interface	IP Address	MAC Address	Interface Protection	
⊟ ge0/0			Yes	☒
	192.168.10.62	00-0C-29-F7-65-CC		

Click **Submit**.

3. On the **Configuration** tab, enable anti-ARP spoofing, active protection, and anti-ARP flood.



Anti-ARP Spoofing

Enable ☑ (It is recommended to bind IP and MAC to achieve better protection before using the anti-ARP attack function)

Active Protection ☑

Time Interval 1 (1-10)Seconds

Disable ARP Learning □

Anti-ARP Flood

Enable ☑

ARP Attack Identification Threshold 300 (10-10000)Packet/s

Attack Host Suppression Duration 60 (10-65535)Seconds

Click Submit.

4. **Check whether logs display ARP flood packets.**
5. **Choose Log > Security log > Anti-attack > Anti-ARP attack to display ARP flood logs.Choose Log > Security log > Anti-attack > Anti-ARP attack to display ARP spoofing logs.**

43.4 Troubleshooting

43.4.1 PCs Cannot Access the Internet

Symptom	Internet access fails after anti-ARP spoofing is configured.
Analysis	PCs are not added to the IP-MAC address binding table after ARP learning is disabled.
Solution	Add PCs to the IP-MAC address binding table.

44 Blacklist- based Protection

44.1 Overview

When discovering suspicious traffic, you can configure blacklists on RAVEN5000 firewalls for protection purposes. When the traffic passing a firewall meets the filter criteria of a blacklist, the traffic is blocked at the specified time.

Set the source IP address and effective period when creating a blacklist. Packets sent from the source IP address during the effective period are not delivered and are dropped. You can configure and back up many blacklisted IP addresses by importing and exporting blacklist configurations.

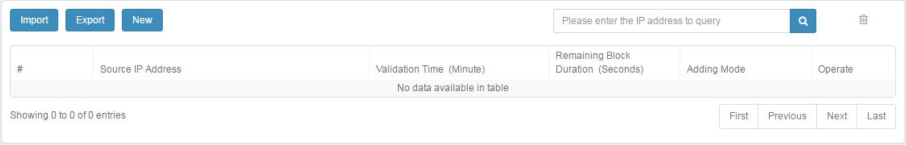
You can click **Block** at the end of the **Statistics** row on the **Session statistics** page to go to the **Create blacklist** page and add a suspicious session to a blacklist. You can block traffic temporarily based on real-time traffic statistics.

44.2 Configuration

44.2.1 Configuring a Blacklist

Procedure:

1. Choose **Policy** > **Security** > **Blacklist**. The following page appears.



#	Source IP Address	Validation Time (Minute)	Remaining Block Duration (Seconds)	Adding Mode	Operate
No data available in table					

Showing 0 to 0 of 0 entries

Source IP address: Source IP address in a blacklist.

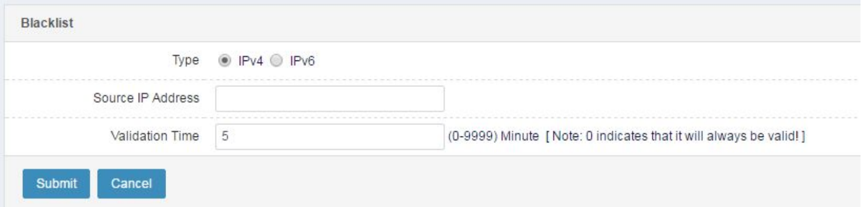
Effective period: Effective period of the blacklist, in minutes.

Remaining block duration: Remaining effective time of the blacklist, in seconds.

How to add: How the blacklist is added. **Add manually** indicates that the blacklist is added manually on the blacklist configuration page. **Add by**

real-time block indicates that the blacklist is added by clicking **Block** on the **Session statistics** page.

2. Click **New** to create a blacklist. The following page appears.



Blacklist

Type ● IPv4 ○ IPv6

Source IP Address

Validation Time 5 (0-9999) Minute [Note: 0 indicates that it will always be valid!]

Parameter description:

Type: A blacklist may be of the IPv4 or IPv6 type.

Source IP address: Source IP address in a blacklist.

Effective period: Effective period of the blacklist. The value ranges from 0 to 9999, in minutes. The default value is 5 minutes. If you set it to **0**, the blacklist is permanently effective.

3. Click **Submit** after you complete the settings.

Note

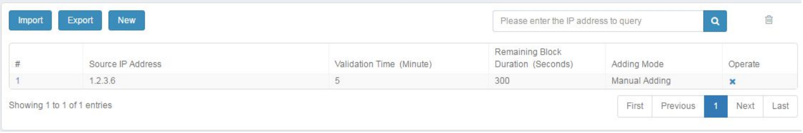
The source IP address must match the blacklist type.

The source IP address cannot be a subnet address, a broadcast address, or an address containing only 0s.

44.2.2 Modifying a Blacklist

Procedure:

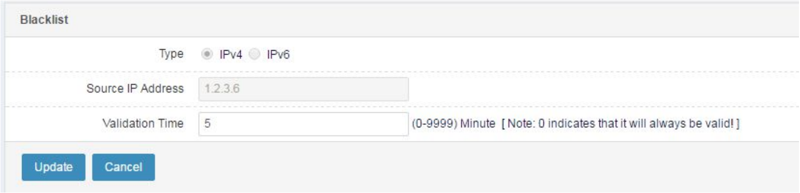
1. Choose **Policy** > **Security** > **Blacklist** and click a blacklist ID.



#	Source IP Address	Validation Time (Minute)	Remaining Block Duration (Seconds)	Adding Mode	Operate
1	1.2.3.6	5	300	Manual Adding	×

Showing 1 to 1 of 1 entries

2. Modify the information about the blacklist and click **Submit**.



Blacklist

Type ● IPv4 ○ IPv6

Source IP Address: 1.2.3.6

Validation Time: 5 (0-9999) Minute [Note: 0 indicates that it will always be valid!]

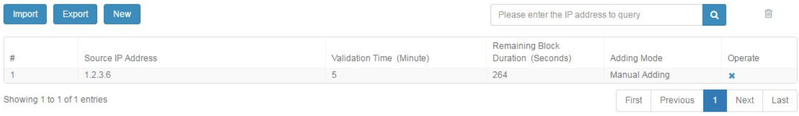
Notice

Type and **Source IP address** cannot be modified.

44.2.3 Deleting a Blacklist

Procedure:

1. Choose **Policy** > **Security** > **Blacklist**. The following page appears.



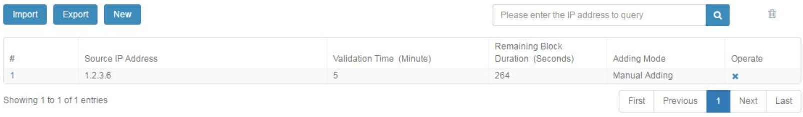
#	Source IP Address	Validation Time (Minute)	Remaining Block Duration (Seconds)	Adding Mode	Operate
1	1.2.3.6	5	264	Manual Adding	✖

Showing 1 to 1 of 1 entries

2. Click ☒ to delete a blacklist, or click 🗑 to delete all blacklists.

44.3 Querying Blacklist Configurations

Choose **Policy** > **Security** > **Blacklist**. The following page appears.



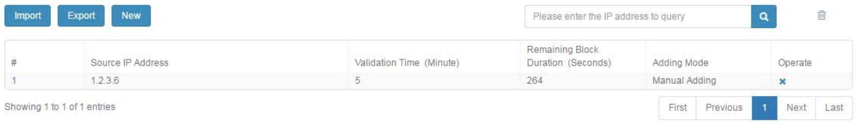
#	Source IP Address	Validation Time (Minute)	Remaining Block Duration (Seconds)	Adding Mode	Operate
1	1.2.3.6	5	264	Manual Adding	✖

Showing 1 to 1 of 1 entries

Enter an IP address and click 🔍.

44.4 Importing and Exporting Blacklist Configurations

Choose **Policy** > **Security** > **Blacklist**. The following page appears.



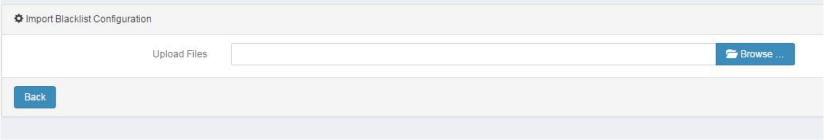
#	Source IP Address	Validation Time (Minute)	Remaining Block Duration (Seconds)	Adding Mode	Operate
1	1.2.3.6	5	264	Manual Adding	✖

Showing 1 to 1 of 1 entries

44.4.1 Importing a Blacklist

Click **Import** to import the text file that contains blacklist configurations. The system reads and delivers the configurations.

Click **Select** to select a blacklist configuration file, as shown in the following figure.



Import Blacklist Configuration

Upload Files

The file size imported at a time cannot exceed 20,480 KB. The required import format is as follows:

- **IPv4 type:**

blacklist-ip x.x.x.x timeout x configtime x-x-xx:x:x

x.x.x.x: IPv4 address

x: Effective period, in minutes

x-x-xx:x:x: Start time, in the format of *year-month-day hours*:*minutes*:*seconds*

- **IPv6 type**

blacklist-ipv6 x:x::x:x timeout x configtime x-x-xx:x:x

x:x::x:x: IPv6 address

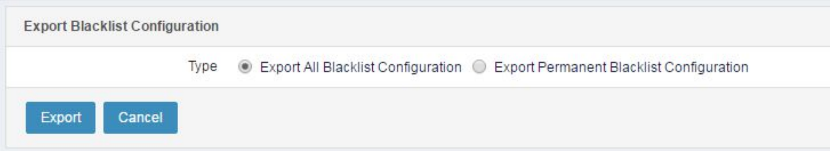
x: Effective period, in minutes

x-x-xx:x:x: Effective time, in the format of *year-month-day hours*:*minutes*:*seconds*

44.4.2 Exporting a Blacklist

Click **Export** to export blacklist configurations to a text file.

See the following figure.



Export Blacklist Configuration

Type ● Export All Blacklist Configuration ○ Export Permanent Blacklist Configuration

Parameter description:

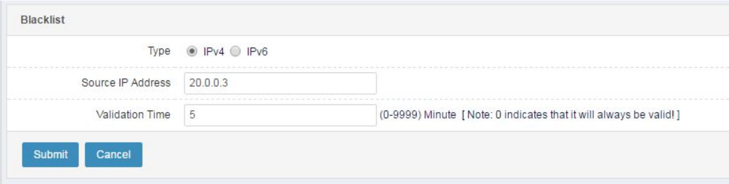
Type: The options are **Export all blacklist configurations** and **Export permanently effective blacklist configurations**.

44.5 Configuration Examples

44.5.1 Example 1: Creating a Blacklist

Procedure:

1. Choose **Policy** > **Security** > **Blacklist**. Configure a blacklist with source IP address 20.0.0.3, as shown in the following figure.



Blacklist

Type ● IPv4 ○ IPv6

Source IP Address 20.0.0.3

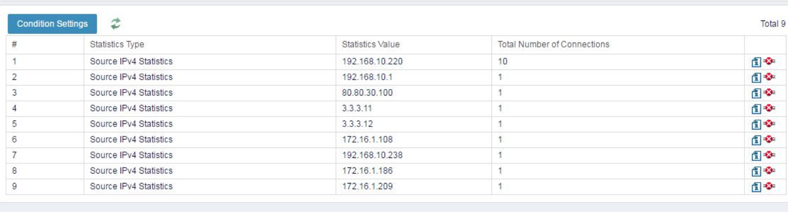
Validation Time 5 (0-9999) Minute [Note: 0 indicates that it will always be valid!]

2. Click **Submit**.

44.5.2 Example 2: Creating a Temporary Block Blacklist

Procedure:

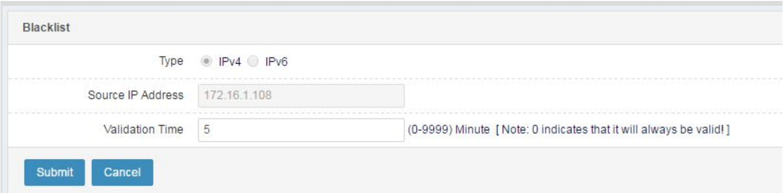
1. Choose **Monitor** > **Session** > **Session statistics**. Set search criteria and click **Search** to search active sessions, as shown in the following figure.



Total 9

#	Statistics Type	Statistics Value	Total Number of Connections	
1	Source IPv4 Statistics	192.168.10.220	10	
2	Source IPv4 Statistics	192.168.10.1	1	
3	Source IPv4 Statistics	80.80.30.100	1	
4	Source IPv4 Statistics	3.3.3.11	1	
5	Source IPv4 Statistics	3.3.3.12	1	
6	Source IPv4 Statistics	172.16.1.108	1	
7	Source IPv4 Statistics	192.168.10.238	1	
8	Source IPv4 Statistics	172.16.1.186	1	
9	Source IPv4 Statistics	172.16.1.209	1	

2. Click ✖ next to a session you want to block temporarily. The blacklist configuration page appears, as shown in the following figure.



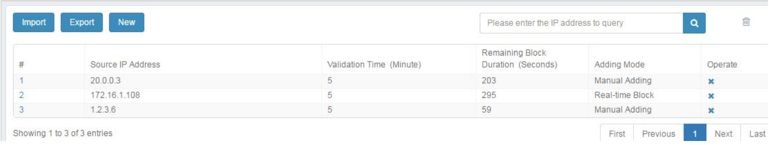
Blacklist

Type ● IPv4 ○ IPv6

Source IP Address 172.16.1.108

Validation Time 5 (0-9999) Minute [Note: 0 indicates that it will always be valid!]

3. Set **Effective period** and click **Submit**. Choose **Policy** > **Security** > **Blacklist** to display the temporary block blacklist, as shown in the following figure.



#	Source IP Address	Validation Time (Minute)	Remaining Block Duration (Seconds)	Adding Mode	Operate
1	20.0.0.3	5	203	Manual Adding	✖
2	172.16.1.108	5	295	Real-time Block	✖
3	1.2.3.6	5	59	Manual Adding	✖

Showing 1 to 3 of 3 entries

⚠ Notice

A firewall supports a maximum of 30,000 blacklists, including IPv4 and IPv6 blacklists.

45 Application Control Policy

45.1 Overview

Application control policies are an extension of security policies and constitute a core module of a firewall. Apart from analysis and control of IP addresses and ports, the module performs protocol analysis and feature identification on packet data to identify the applications to which traffic belongs and filter and audit the traffic of specific applications. For example, the module can control the traffic of P2P download and online video.

Application parameter configuration is at the core of the application control module, and includes the following elements:

- Application: Application to be audited. For details, see the "Application Object" section. Currently, RAVEN5000 firewalls identify more than 1000 applications, many of which are in wide use.
- Application behavior: Auditable action supported by the application, such as login, logout, and file download.
- Application behavior parameter: Auditable parameter supported by the specified application behavior, such as the login user name and downloaded file name.

Traffic data is matched with application control policies based on the preceding parameters. Once a policy is hit, the corresponding action Permit or Deny is taken. You can configure whether to log the process.

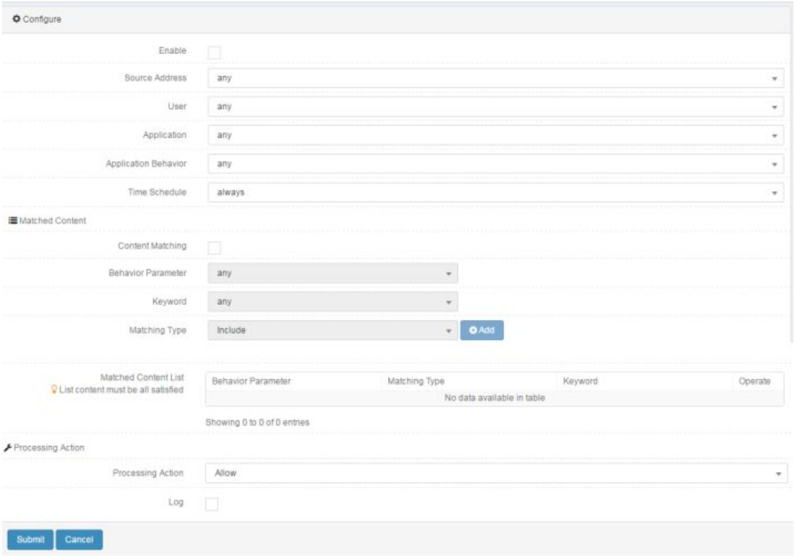
45.2 Configuration

45.2.1 Configuring Basic Policy Elements

The basic elements of an application control policy are the match criteria and action. The match criteria include the address object, application object, application behavior, behavior parameter, keyword matching, and policy effective period. The address object, time range object, and keyword object must be configured using a predefined template. The policy actions are Permit and Deny.

Procedure:

1. Choose **Policy** > **Application control** > **Application control policy** and click **New**.



Configure

Enable □

Source Address: any

User: any

Application: any

Application Behavior: any

Time Schedule: always

Matched Content

Content Matching □

Behavior Parameter: any

Keyword: any

Matching Type: Include

Add

Matched Content List
List content must be all satisfied

Behavior Parameter	Matching Type	Keyword	Operate
No data available in table			

Showing 0 to 0 of 0 entries

Processing Action

Processing Action: Allow

Log □

Submit Cancel

Parameter description:

Enable: Check this box to enable the application control policy.

Source address: Source address object or source address object group. Currently, only the IPv4 address format is supported.

User: User or user group.

Application: Applications are classified into custom applications, predefined application groups, and individual predefined applications. The option **any** indicates all applications. The drop-down list supports fuzzy search.

Application behavior: Action that can be identified by the application feature database, such as login, logout, and file download. The option **any** indicates all application behaviors.

Time: Policy effective time. You can reference an existing time object. The option **always** indicates all time points.

Content matching: Check this box to apply the matched content list.

Behavior parameter: Auditable parameter supported by the configured application behavior, such as the login user name and downloaded file name. The option **any** indicates all the parameters of the application behavior.

Keyword: Reference an existing keyword template. A hit is found when the content retrieved based on the behavior parameter contains the specified keyword (case-sensitive). The option **any** indicates matching any content.

Match type: The options are **Include** and **Not include**.

Matched content list: The behavior parameter, keyword, and match type form a group. A maximum of 10 groups can be configured. A hit is found only when all the groups are satisfied.

Action: Action to be taken for data flows that meet the match conditions.

Log: To enable logging, check this box and enable logging in the log module.

3. Click **Submit** after you complete the settings.

Note

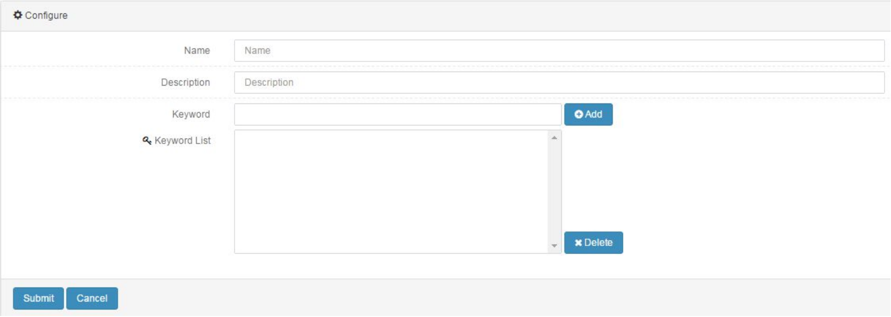
An ID is automatically generated to uniquely identify the new application control policy. A hit is found only when all the combinations in the matched content list are satisfied.

45.2.2 Configuring Keywords

You can reference a keyword template in the **Keyword** drop-down list of the application control template, or create one in the keyword module.

Procedure:

1. Choose **Policy** > **Application control** > **Keyword**. The following page appears.



Parameter description:

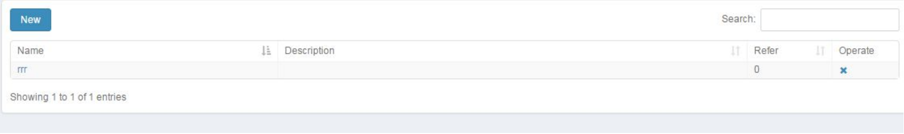
Name: Name of a keyword template.

Description: Keyword description.

Keyword: Keyword used for matching, case-sensitive.

Keyword list: You can enter a maximum of 128 keywords. A hit is found when one keyword is satisfied.

2. Click **Submit** after you complete the settings.



Name	Description	Refer	Operate
rrr		0	✖

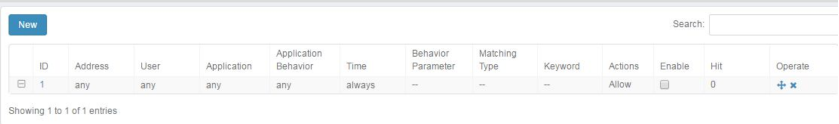
Showing 1 to 1 of 1 entries

45.2.3 Enabling an Application Control Policy

After you configure an application control policy, enable it to make it effective.

Procedure:

1. Choose **Policy** > **Application control** > **Application control policy.** The page shown in the following appears.



New

Search:

	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊟	1	any	any	any	any	always	--	--	--	Allow	□	0	✚ ✖

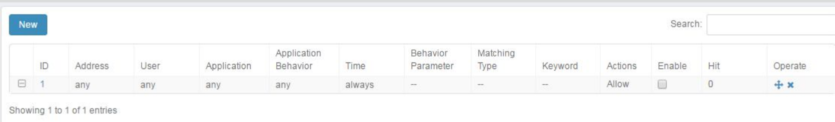
Showing 1 to 1 of 1 entries

2. Check the **Enable** box next to an application control policy to enable it.

45.2.4 Modifying an Application Control Policy

Procedure:

3. Choose **Policy** > **Application control** > **Application control policy** and click a policy ID.



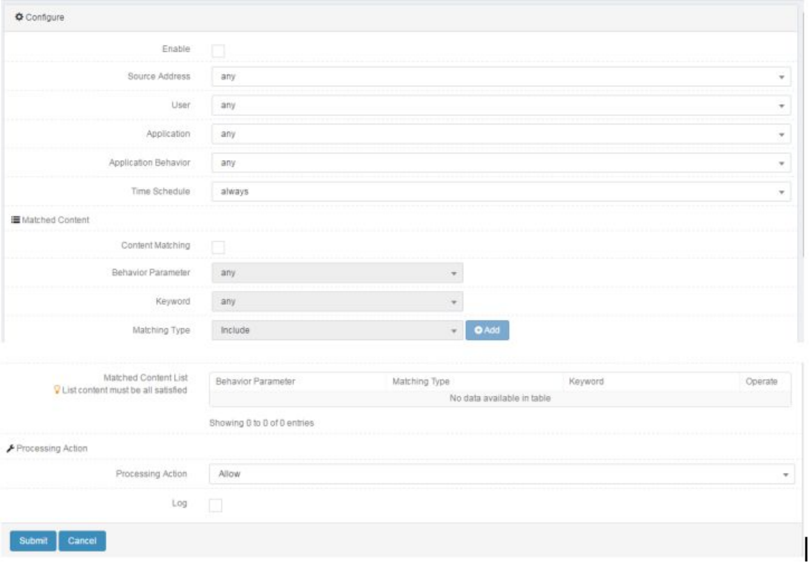
New

Search:

	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊟	1	any	any	any	any	always	--	--	--	Allow	□	0	✚ ✖

Showing 1 to 1 of 1 entries

4. Modify the information about the application control policy and click **Submit**.



Configure

Enable □

Source Address: any

User: any

Application: any

Application Behavior: any

Time Schedule: always

Matched Content

Content Matching □

Behavior Parameter: any

Keyword: any

Matching Type: Include

Add

Matched Content List
List content must be all satisfied

Behavior Parameter	Matching Type	Keyword	Operate
No data available in table			

Showing 0 to 0 of 0 entries

Processing Action

Processing Action: Allow

Log □

Submit Cancel

Note

After an application control policy is modified, its hit count is cleared.

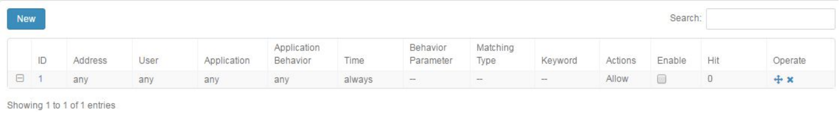
Notice

Application and **Application behavior** cannot be modified.

45.2.5 Deleting an Application Control Policy

Procedure:

1. Choose **Policy** > **Application control** > **Application control policy.** The page shown in the following appears.



	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊟	1	any	any	any	any	always	--	--	--	Allow	□	0	✣ ✖

Showing 1 to 1 of 1 entries

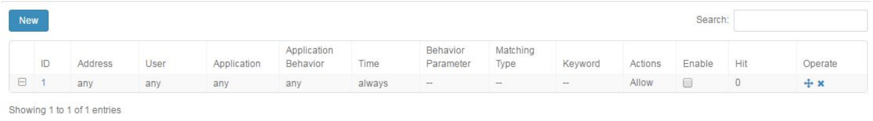
2. Click ✖ next to the application control policy you want to delete.

45.2.6 Adjusting the Order of Application Control Policies

You can change the match priorities of application control policies by adjusting their order. Policies are matched from top down as listed on page.

Procedure:

1. Choose **Policy** > **Application control** > **Application control policy.** The page shown in the following appears.



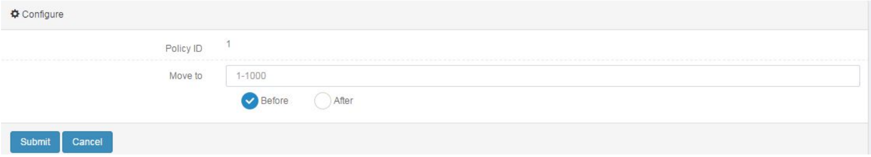
New

Search:

	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊟	1	any	any	any	any	always	--	--	--	Allow	□	0	✥ ✖

Showing 1 to 1 of 1 entries

2. Click ✥ next to the policy you want to move.



Configure

Policy ID: 1

Move to: 1-1000

● Before ○ After

Submit Cancel

Policy ID: ID of the policy to be moved.

Move to: ID of the reference policy.

Before: Move the policy before the reference policy.

After: Move the policy after the reference policy.

3. Click **Submit**.

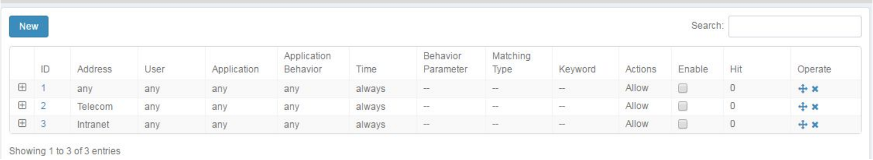
Notice

Policies are matched from top down as listed on page. Once a policy is hit, the remaining ones are not matched.

45.2.7 Querying Application Control Policies

Procedure:

1. Choose **Policy** > **Application control** > **Application control policy**. The page shown in the following appears.



New

Search:

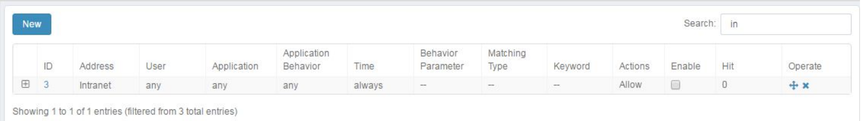
	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊞	1	any	any	any	any	always	--	--	--	Allow	□	0	✥ ✖
⊞	2	Telecom	any	any	any	always	--	--	--	Allow	□	0	✥ ✖
⊞	3	Intranet	any	any	any	always	--	--	--	Allow	□	0	✥ ✖

Showing 1 to 3 of 3 entries

2. Enter a filter criterion in the **Filter** text box in the upper-right corner.

You can filter policies based on the configurations on the page.

The following figure shows filtering HTTP applications.



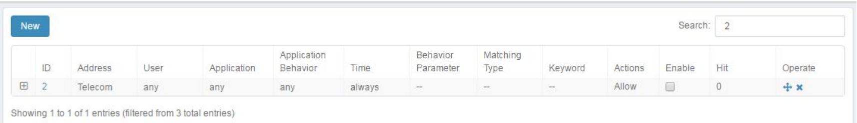
New

Search: in

	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊞	3	Intranet	any	any	any	always	--	--	--	Allow	□	0	✥ ✖

Showing 1 to 1 of 1 entries (filtered from 3 total entries)

The following figure shows filtering by policy ID.



Search: 2

	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊞	2	Telecom	any	any	any	always	--	--	--	Allow	□	0	✢ ✖

Showing 1 to 1 of 1 entries (filtered from 3 total entries)

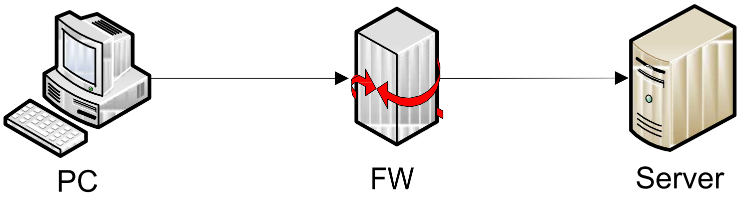
45.3 Configuration Examples

45.3.1 Example 1: Blocking Login by Users Whose QQ Numbers Contain 123456

Description:

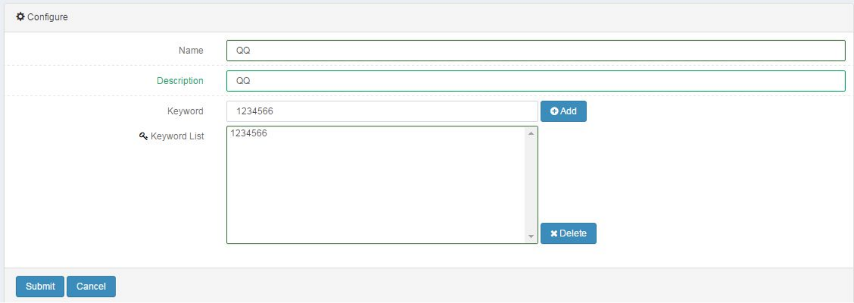
A PC accesses external services through a firewall. Configure an application control policy to block login by users whose QQ numbers contain 123456.

Network diagram:



Procedure:

1. Choose **Policy** > **Application control** > **Keyword**. Complete the settings on the following page.



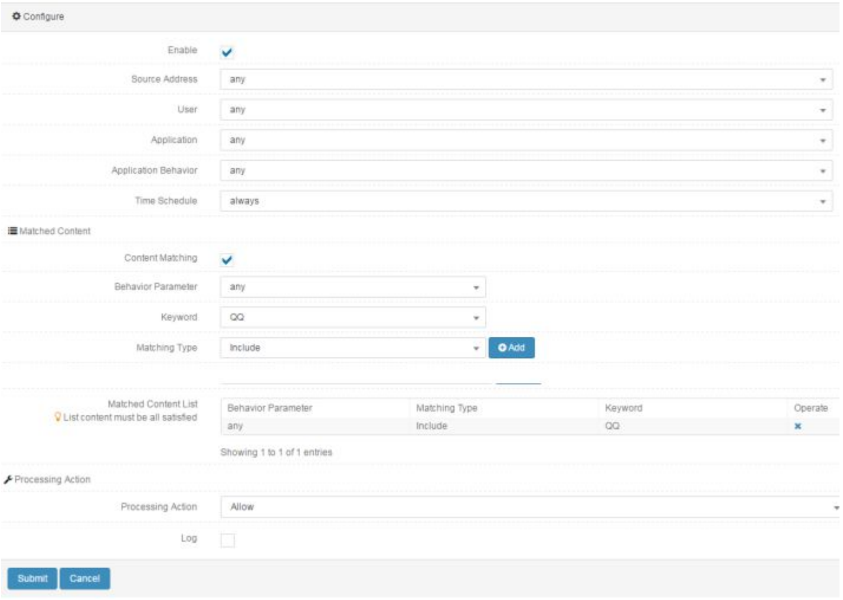
Name: QQ

Description: QQ

Keyword: 1234566

Keyword List: 1234566

2. Choose **Policy** > **Application control** > **Application control policy**. Complete the settings on the following page.



Configure

Enable	☑
Source Address	any
User	any
Application	any
Application Behavior	any
Time Schedule	always

Matched Content

Content Matching	☑
Behavior Parameter	any
Keyword	QQ
Matching Type	Include

Matched Content List
List content must be all satisfied

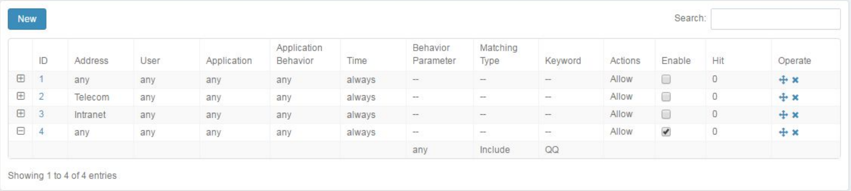
Behavior Parameter	Matching Type	Keyword	Operate
any	Include	QQ	✖

Showing 1 to 1 of 1 entries

Processing Action

Processing Action	Allow
Log	□

3. Click **Submit**. The following page appears.



	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊞	1	any	any	any	any	always	--	--	--	Allow	□	0	✛ ✖
⊞	2	Telecom	any	any	any	always	--	--	--	Allow	□	0	✛ ✖
⊞	3	Intranet	any	any	any	always	--	--	--	Allow	□	0	✛ ✖
⊟	4	any	any	any	any	always	--	--	--	Allow	☑	0	✛ ✖
							any	Include	QQ				

Showing 1 to 4 of 4 entries

4. The configuration is complete.

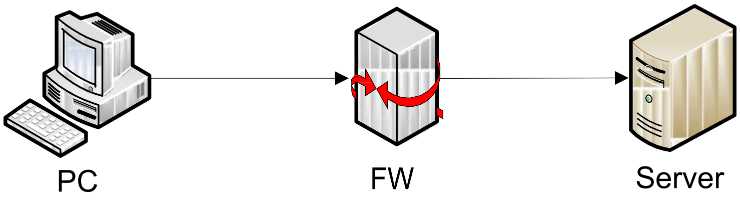
5. Verify that the login by a user whose QQ number contains 123456 from the PC is blocked.

45.3.2 Example 2: Rejecting All Emails

Description:

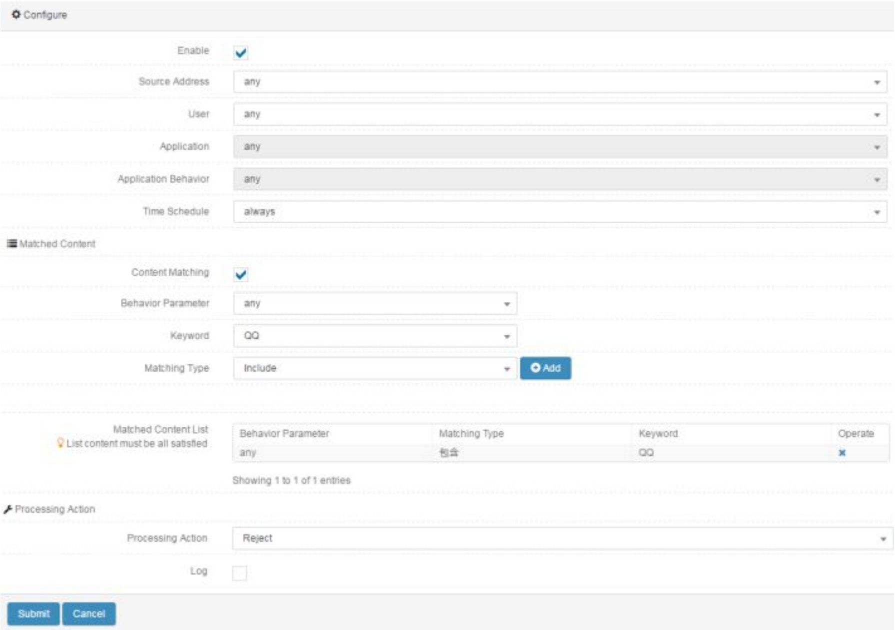
A PC accesses external services through a firewall. Configure an application control policy to reject all emails.

Network diagram:



Procedure:

1. Choose **Policy** > **Application control** > **Application control policy**. Complete the settings on the following page.



Enable: ☑

Source Address: any

User: any

Application: any

Application Behavior: any

Time Schedule: always

Content Matching: ☑

Behavior Parameter: any

Keyword: QQ

Matching Type: Include

Matched Content List

List content must be all satisfied

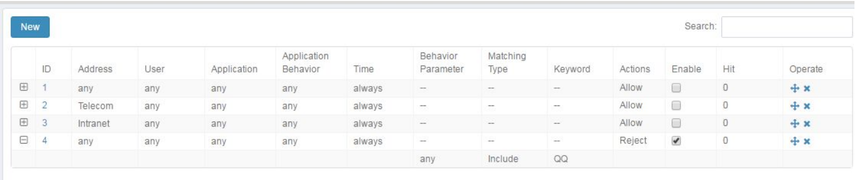
Behavior Parameter	Matching Type	Keyword	Operate
any	包含	QQ	✖

Showing 1 to 1 of 1 entries

Processing Action: Reject

Log: □

2. Click **Submit**. The following page appears.



	ID	Address	User	Application	Application Behavior	Time	Behavior Parameter	Matching Type	Keyword	Actions	Enable	Hit	Operate
⊞	1	any	any	any	any	always	--	--	--	Allow	□	0	✣ ✖
⊞	2	Telecom	any	any	any	always	--	--	--	Allow	□	0	✣ ✖
⊞	3	Intranet	any	any	any	always	--	--	--	Allow	□	0	✣ ✖
⊟	4	any	any	any	any	always	--	--	--	Reject	☑	0	✣ ✖
							any	Include	QQ				

3. The configuration is complete.

4. Verify that the inbox contains no emails in the PC.

45.4 Troubleshooting

45.4.1 No Policy Is Hit

Symptom	A policy is correctly configured but has no hits.

Analysis	Traffic applications are complex and mixed, and a user access may have multiple features. Features may change during traffic transmission. For example, an HTTP access is initially identified as HTTP. After a page is opened and the application engine identifies the Sina application, the traffic application flag is changed. As a result, the HTTP application control policy is not hit. Due to such complexity and change, an application control policy may have zero hit count. The causes are: ➢ Policy order. Policies are matched from top down as listed on page. When configuring policies, place exact policies on top. For example, Sina is more exact than HTTP-web page browsing. ➢ Simplify keywords connected by AND. ➢ Encrypted traffic cannot be audited. Many websites switch

	to HTTPS access, for example, Taobao and Tmall. Traffic must be identified based on certificates. ➢ Firewall policies conflict. When a firewall policy conflicts with an application control policy and both policies specify the Deny action, the application control policy is not hit. Traffic is blocked when the Deny action is specified by either policy. ➢ Traffic is identified as a custom application, which is of the highest priority. ➢ The keyword-matched data exceeds the audit length of the application engine. By default, the application engine can audit up to 20 data packets to ensure performance. Do not enable full traffic identification if possible. ➢ Application features have been updated. Upgrade to the latest application feature database version.
Solution	The following suggestions are proposed: ➢ Upgrade to the latest feature database version. ➢ Configure a coarse-grained policy and check whether it is hit. Verify that the application engine takes effect. ➢ Adjust the policy order properly. ➢ For encrypted access, search for applications with passports, which are certificate features. For example, Taobao uses the Alibaba passport, and NetEase uses the NetEase passport. ➢ Check for highly coarse-grained custom applications and delete them if any. ➢ Check that the problem can be reproduced stably after the range is narrowed down. Collect environment information and operation procedures and send them to the after-sales personnel.

46 Web Control Policy

46.1 Overview

The web access control and audit feature controls users' behavior of publishing information on a specific website or publishing information that contains a specific keyword, and logs the publishing behavior. For example, users are prevented from publishing content with the keyword "violence" on forums, and any such publishing behaviors are logged. Network administrators can formulate proper rules on information transfer to the web based on different users, time points, and publishing behaviors. The system will handle the network traffic that hits a rule based on configurations.

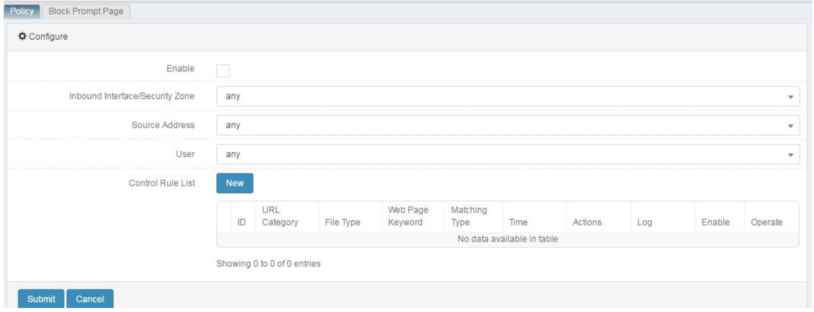
46.2 Configuration

46.2.1 Configuring Basic Policy Elements

The basic elements of a web control policy are the match criteria and action. The match criteria include the source address, inbound interface, user, URL category, file type, behavior parameter, keyword matching, and policy effective period. The address object, time range object, and keyword object must be predefined. The policy actions are Permit and Deny.

Procedure:

1. Choose **Policy** > **Application control** > **Web control policy** and click **New**.



Enable □

Inbound Interface/Security Zone any

Source Address any

User any

Control Rule List

	ID	URL Category	File Type	Web Page Keyword	Matching Type	Time	Actions	Log	Enable	Operate
No data available in table										

Showing 0 to 0 of 0 entries

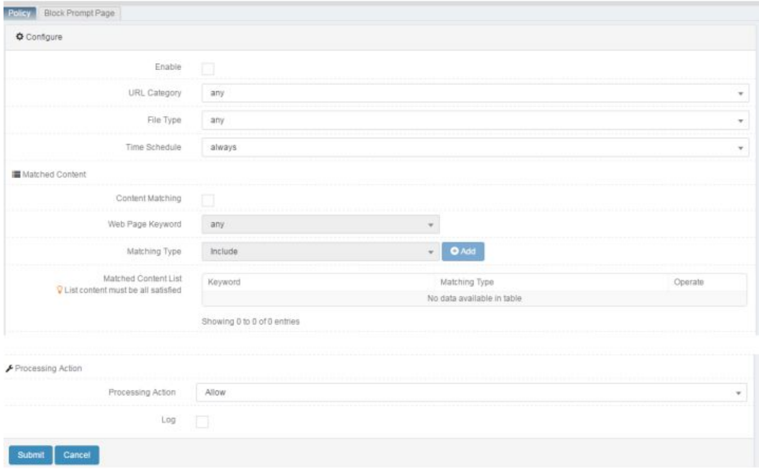
Parameter description:

Enable: Check this box to enable the web control policy.

Source address: Source address object or source address object group. Currently, only the IPv4 address format is supported.

User: User or user group.

2. Choose **Policy** > **Application control** > **Web control policy** > **Control rule list** and click **New**.



Enable □

URL Category: any

File Type: any

Time Schedule: always

Content Matching □

Web Page Keyword: any

Matching Type: Include

Matched Content List
List content must be all satisfied

Keyword	Matching Type	Operate
No data available in table		

Showing 0 to 0 of 0 entries

Processing Action: Allow

Log □

Parameter description:

Enable: Check this box to enable the rule.

URL category: URL categories are classified into the predefined URL category, custom URL category, and predefined URL category group. The option **any** indicates all URL categories. The drop-down list supports fuzzy search.

File type: Reference an existing keyword template. A hit is found when the content retrieved based on the behavior parameter contains the specified keyword (case-sensitive). The option **any** indicates matching any content.

Time: Policy effective time. You can reference an existing time object. The option **always** indicates all time points.

Content matching: Check this box to apply the matched content list.

Web page keyword: Reference an existing keyword template. A hit is found when the content retrieved based on the behavior parameter contains the specified keyword (case-sensitive). The option **any** indicates matching any content.

Match type: The options are **Include** and **Not include**.

Matched content list: The behavior parameter, keyword, and match type form a group. A maximum of 10 groups can be configured. A hit is found only when all the groups are satisfied.

Action: Action to be taken for data flows that meet the match conditions. The options are **Permit** and **Deny**.

Log: To enable logging, check this box and enable logging in the log module.

3. Click **Submit** after you complete the settings.

Note

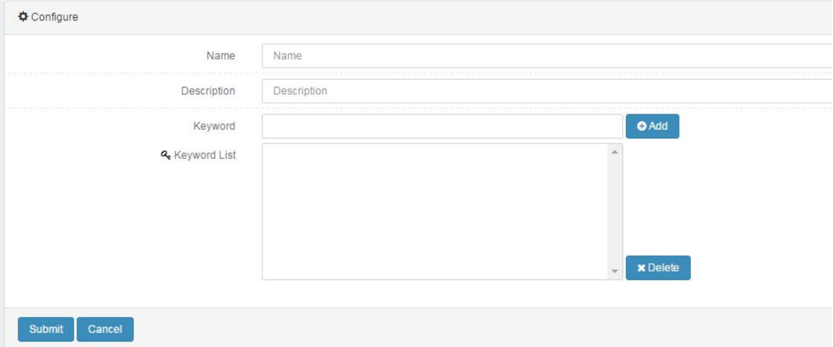
An ID is automatically generated to uniquely identify the new web control policy. A hit is found only when all the combinations in the matched content list are satisfied.

46.2.2 Configuring Keywords

You can reference a keyword template in the **Keyword** drop-down list of the application control template, or create one in the keyword module.

Procedure:

1. Choose **Policy** > **Application control** > **Keyword**. The following page appears.



Parameter description:

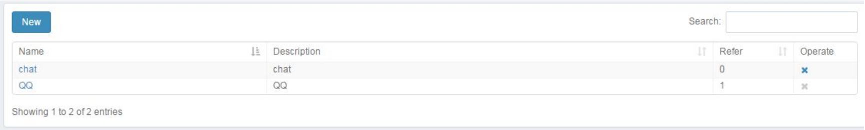
Name: Name of a keyword template.

Description: Keyword description.

Keyword: Keyword used for matching, case-sensitive.

Keyword list: You can enter a maximum of 128 keywords. A hit is found when one keyword is satisfied.

2. Click **Submit** after you complete the settings.



Name	Description	Refer	Operate
chat	chat	0	✖
QQ	QQ	1	✖

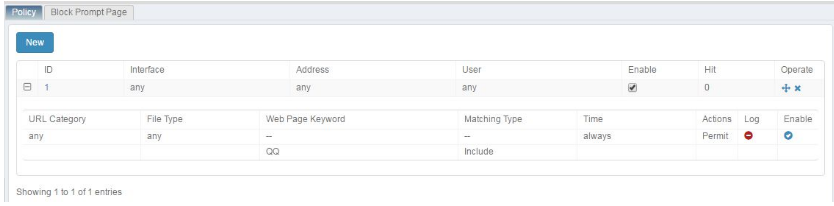
Showing 1 to 2 of 2 entries

46.2.3 Enabling a Web Control Policy

After you configure a web control policy, enable it to make it effective.

Procedure:

1. Choose **Policy** > **Application control** > **Web control policy**. The following page appears.



Policy | Block Prompt Page

New

	ID	Interface	Address	User	Enable	Hit	Operate
⊟	1	any	any	any	☑	0	✚ ✖

URL Category	File Type	Web Page Keyword	Matching Type	Time	Actions	Log	Enable
any	any	--	--	always	Permit	⊖	✓
		QQ	Include				

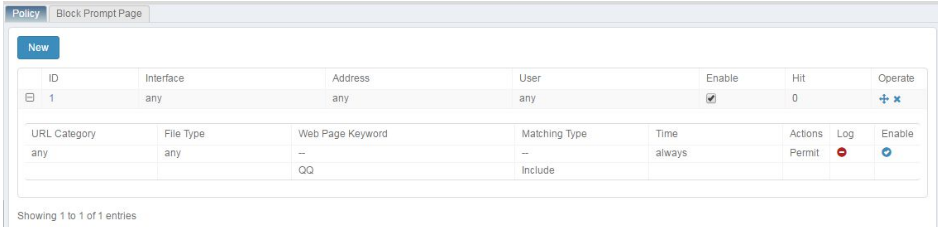
Showing 1 to 1 of 1 entries

2. Check the **Enable** box next to a web control policy to enable it.

46.2.4 Modifying a Web Control Policy

Procedure:

1. Choose **Policy** > **Application control** > **Web control policy** and click a policy ID.



Policy | Block Prompt Page

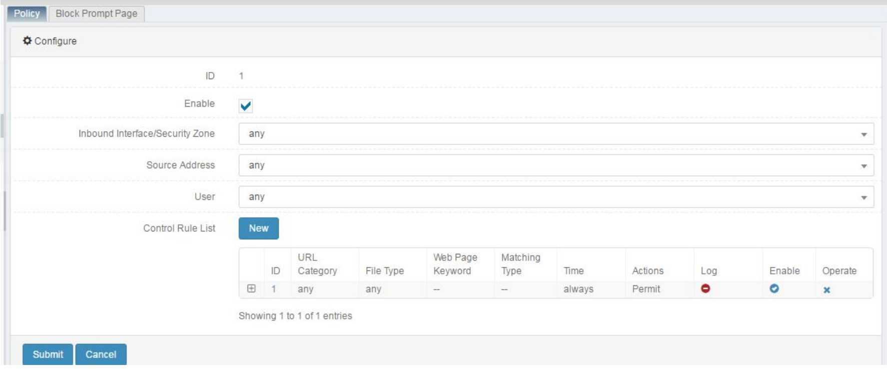
New

	ID	Interface	Address	User	Enable	Hit	Operate
⊟	1	any	any	any	☑	0	✚ ✖

URL Category	File Type	Web Page Keyword	Matching Type	Time	Actions	Log	Enable
any	any	--	--	always	Permit	⊖	✓
		QQ	Include				

Showing 1 to 1 of 1 entries

2. Modify the information about the web control policy and click **Submit**.



Policy | Block Prompt Page

⚙ Configure

ID: 1

Enable: ☑

Inbound Interface/Security Zone: any

Source Address: any

User: any

Control Rule List: New

	ID	URL Category	File Type	Web Page Keyword	Matching Type	Time	Actions	Log	Enable	Operate
⊞	1	any	any	--	--	always	Permit	⊖	✓	✖

Showing 1 to 1 of 1 entries

Submit | Cancel

Note

After a web control policy is modified, its hit count is cleared.

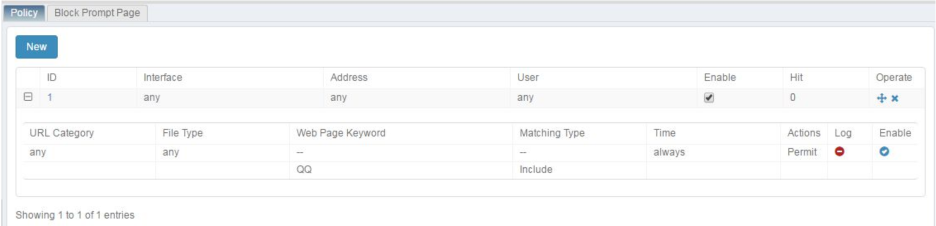
Notice

When you modify a policy, you must enable the rules in the control rule list to make the modified policy effective. Rules of higher priority are listed in front of rules of lower priority.

46.2.5 Deleting a Web Control Policy

Procedure:

1. Choose **Policy** > **Application control** > **Web control policy**. The following page appears.



	ID	Interface	Address	User	Enable	Hit	Operate
⊟	1	any	any	any	☑	0	✛ ✖

URL Category	File Type	Web Page Keyword	Matching Type	Time	Actions	Log	Enable
any	any	--	--	always	Permit	⛔	✓
		QQ	Include				

Showing 1 to 1 of 1 entries

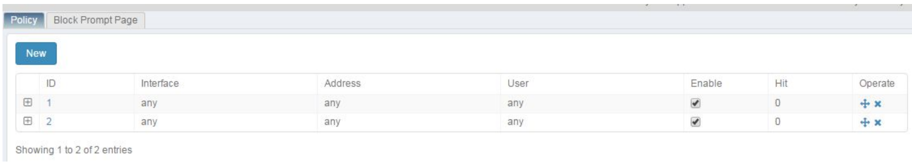
2. Click ✖ next to the web control policy you want to delete.

46.2.6 Adjusting the Order of Web Control Policies

You can change the match priorities of web control policies by adjusting their order. Policies are matched from top down as listed on page.

Procedure:

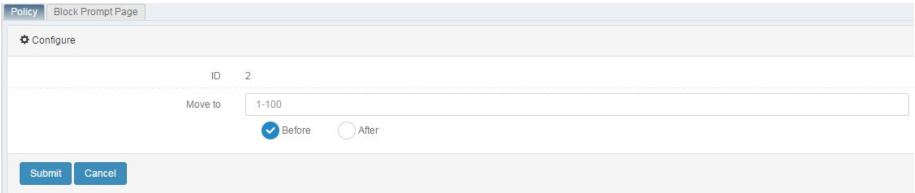
1. Choose **Policy** > **Application control** > **Web control policy**. The following page appears.



	ID	Interface	Address	User	Enable	Hit	Operate
⊞	1	any	any	any	☑	0	✛ ✖
⊞	2	any	any	any	☑	0	✛ ✖

Showing 1 to 2 of 2 entries

2. Click ✛ next to the policy you want to move.



ID 2

Move to 1-100

● Before ○ After

Policy ID: ID of the policy to be moved.

Move to: ID of the reference policy.

Before: Move the policy before the reference policy.

After: Move the policy after the reference policy.

3. Click **Submit**.

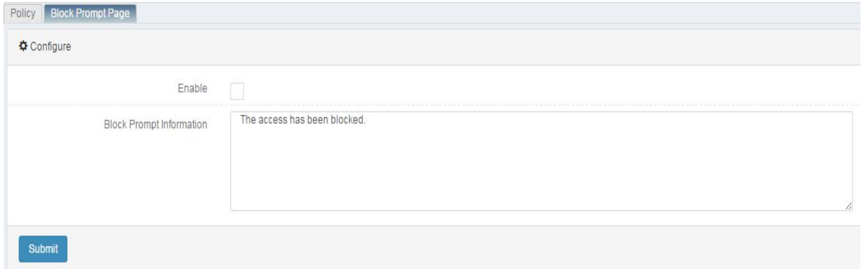
Notice

Policies are matched from top down as listed on page. Once a policy is hit, the remaining ones are not matched.

46.2.7 Block Prompt Page

Procedure:

Choose **Policy** > **Application control** > **Web control policy**. The following page appears.



Enable □

Block Prompt Information: The access has been blocked.

Parameter description:

Enable: Check this box to enable the block prompt page.

Block prompt message: Custom prompt message displayed when the Deny action is taken.

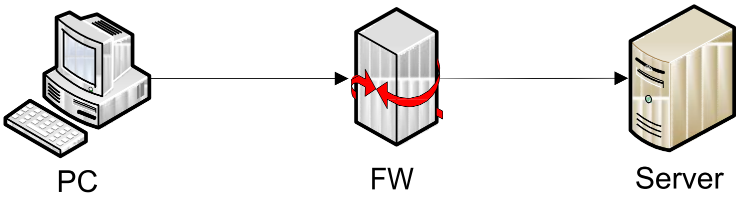
46.3 Configuration Example

46.3.1 Blocking All News Web Pages with a Prompt of News Browsing Denied

Description:

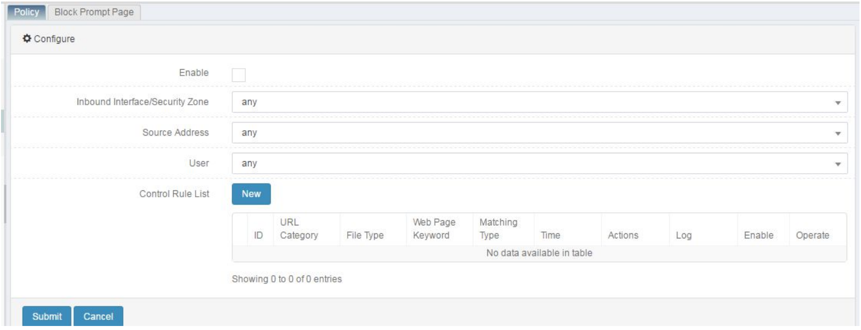
A PC accesses external services through a firewall. Configure a policy to block all news web pages with a prompt of news browsing denied.

Network diagram:



Procedure:

1. Choose **Policy** > **Application control** > **Web control policy**. The following page appears.



Enable □

Inbound Interface/Security Zone any

Source Address any

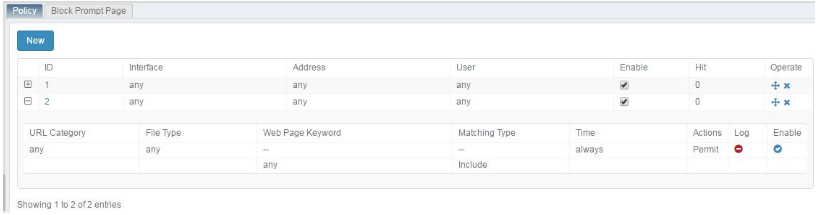
User any

Control Rule List

	ID	URL Category	File Type	Web Page Keyword	Matching Type	Time	Actions	Log	Enable	Operate
No data available in table										

Showing 0 to 0 of 0 entries

2. Click **Submit** after you complete the settings. The following page appears.



	ID	Interface	Address	User	Enable	Hit	Operate
⊞	1	any	any	any	☑	0	✥ ✖
⊟	2	any	any	any	☑	0	✥ ✖

URL Category	File Type	Web Page Keyword	Matching Type	Time	Actions	Log	Enable
any	any	--	--	always	Permit	⛔	✓
		any	Include				

Showing 1 to 2 of 2 entries

1. The configuration is complete.

2. The PC blocks access to news web pages.

46.4 Troubleshooting

46.4.1 No Policy Is Hit

Symptom	A policy is correctly configured but has no hits.
Analysis	➢ The multi-keyword match logic is incorrect. ➢ Encrypted traffic cannot be audited. Many websites switch to HTTPS access, for example, Taobao and Tmall. ➢ Firewall policies conflict. When a firewall policy conflicts with a web control policy and both policies specify the Deny action, the web control policy is not hit. Traffic is blocked when the Deny action is specified by either policy. ➢ The keyword-matched data exceeds the audit length of the application engine. By default, the application engine can audit up to 20 data packets to ensure performance. Do not enable full traffic identification if possible. ➢ The URL feature database has expired.
Solution	The following suggestions are proposed: ➢ Upgrade to the latest URL feature database version. ➢ Configure a coarse-grained policy and check whether it is hit. Verify that the application engine takes effect.

	➢ Adjust the policy order properly.

47 APT Association

47.1 Overview

APT products detect malicious behaviors in files transferred in networks. RAVEN 5000 firewalls provide the APT association feature to restore passing network data and send the restored files to an APT device for detection purposes. The firewalls also trace and record malicious files and support quick query of APT file detection results.

Currently, the T-series firewalls' APT association module interoperates only with Belden's APT products.

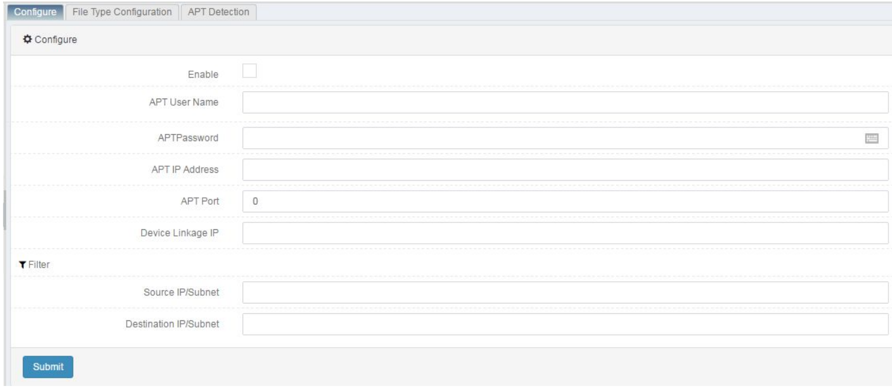
47.2 Configuration

47.2.1 Configuring Basic Association Elements

The basic elements of APT association are the peer APT device's user name, password, IP address, and port, and the local device's IP address.

Procedure:

1. Choose **Policy** > **Security** Linkage > **APT** Linkage. Complete the settings on the following page.



Parameter description:

Enable: Check this box to enable APT association.

APT user name: User name of the peer APT device.

APT password: Password of the peer APT device.

APT IP address: IP address of the peer APT device.

APT port: Port number of the peer APT device.

Device association IP address: IP address of the local device used to communicate with the APT device.

Filter:

Source IP address/Subnet: Source IP address used to filter detected files.

Destination IP address/Subnet: Destination IP address used to filter detected files.

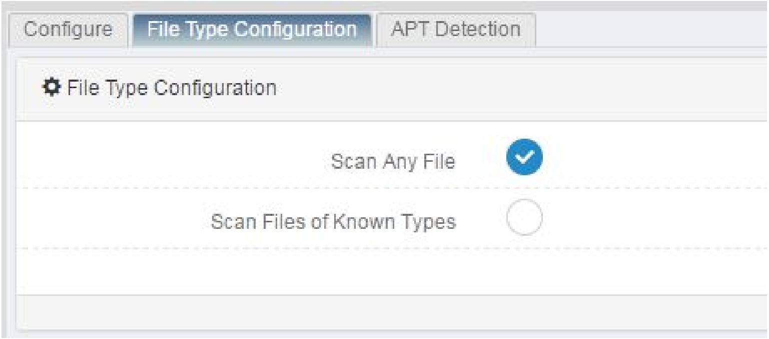
2. Click **Submit** after you complete the settings.

Note

If you do not configure **Filter**, the system will detect files with any IP addresses.

47.2.2 Configuring APT File Type Filter

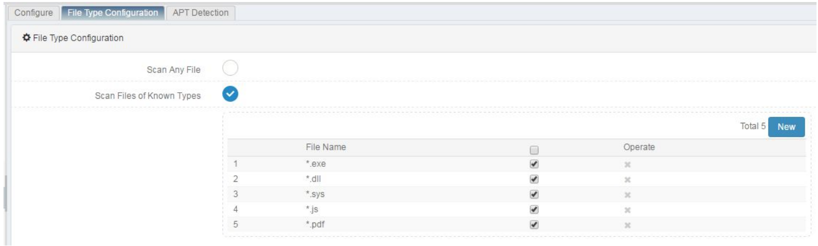
Procedure:



File Type Configuration

Scan Any File ●

Scan Files of Known Types ○



File Type Configuration

Scan Any File ○

Scan Files of Known Types ●

	File Name	□	Operate
1	*.exe	☑	×
2	*.dll	☑	×
3	*.sys	☑	×
4	*.js	☑	×
5	*.pdf	☑	×

Parameter description:

Scan any files: Detect all files without type filter.

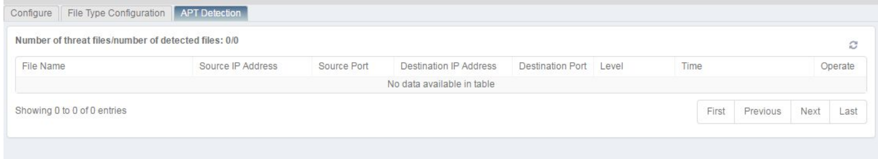
Scan known file types: Detect files of configured and enabled types. You can add or delete custom file types.

Note

File types must be enabled before being applied to filter.

47.2.3 APT Monitoring

APT monitoring shows the information about detected malicious files.



Number of threat files/number of detected files: 0/0

File Name	Source IP Address	Source Port	Destination IP Address	Destination Port	Level	Time	Operate
No data available in table							

Showing 0 to 0 of 0 entries

Parameter description:

File name: Name of a detected malicious file.

Source IP address: Source IP address of the malicious file.

Source port: Source port number of the malicious file.

Destination IP address: Destination IP address of the malicious file.

Destination port: Destination port number of the malicious file.

Level: Risk level of the malicious file, which may be low risk, medium risk, or high risk.

Time: Detection time of the malicious file.

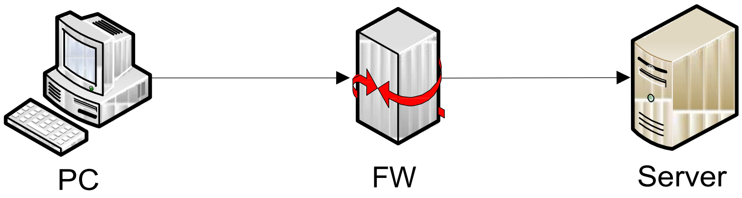
47.3 Configuration Example

47.3.1 Configuring APT Association to Detect and Generate an Alarm on Downloading Virus Infected Files by PCs from External Networks Through a Firewall

Description:

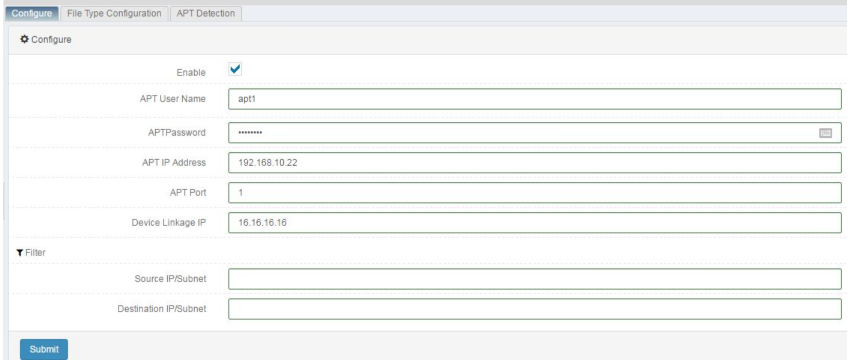
Configure APT association to detect and generate an alarm on downloading virus infected files by PCs from external networks through a firewall.

Network diagram:



Procedure:

1. Choose **Policy** > **Security association** > **APT association** > **Configuration**. Complete the settings on the following page.



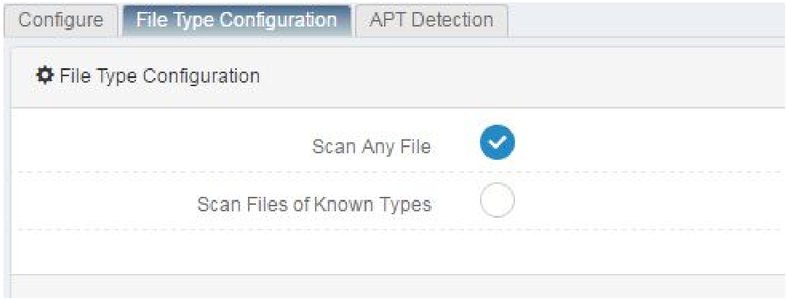
Configure

Enable	☑
APT User Name	apt1
APTPassword	••••••••
APT IP Address	192.168.10.22
APT Port	1
Device Linkage IP	16.16.16.16

Filter

Source IP/Subnet	
Destination IP/Subnet	

2. Choose **Policy** > **Security association** > **APT association** > **File type configuration**. Complete the settings on the following page.

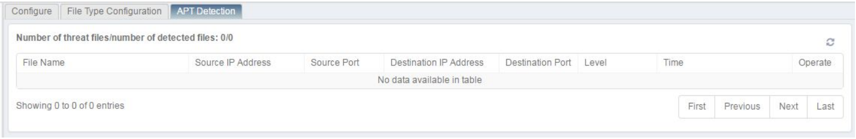


File Type Configuration

Scan Any File	●
Scan Files of Known Types	○

3. The configuration is complete.

4. The following figure shows the detection results.



Number of threat files/number of detected files: 0/0

File Name	Source IP Address	Source Port	Destination IP Address	Destination Port	Level	Time	Operate
No data available in table							

Showing 0 to 0 of 0 entries

47.4 Troubleshooting

47.4.1 The File to Be Detected Is Missed

Symptom	The file to be detected is missed.
Analysis	The default APT detection protocol is HTTP. The possible cause is that no protocol settings or file type settings are available.
Solution	Set http.imap.smtp.pop3, and check whether the file type to be matched is enabled.

48 IDS Association

48.1 Overview

A firewall receives dynamic filter rules from an IDS product to provide dynamic security features for the network.

RAVEN 5000 firewalls' IDS association module can receive filter rules from multiple IDS devices. Currently, the module interoperates only with Belden's IDS products.

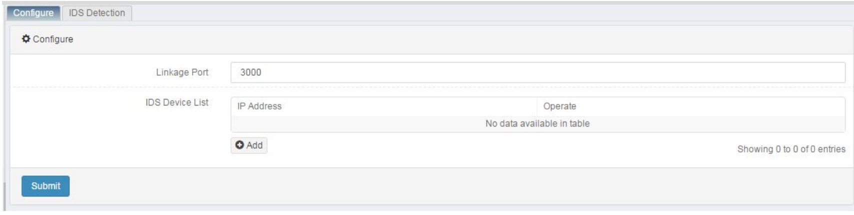
48.2 Configuration

48.2.1 Configuring Basic Association Elements

The basic elements of IDS association are the IDS device's port number and IP address.

Procedure:

1. Choose **Policy** > **Security** Linkage> **IDS** Linkage. Complete the settings on the following page.



Linkage Port: 3000

IDS Device List

IP Address	Operate
No data available in table	

Showing 0 to 0 of 0 entries

Parameter description:

Association port: The default value is **3000**. The value ranges from **1** to **65535**. The default value applies when it is not set.

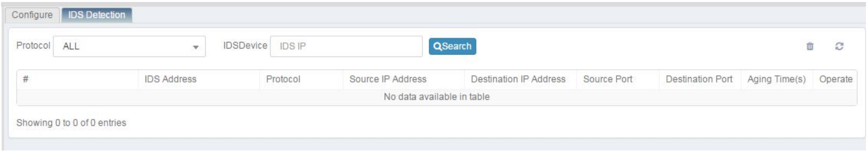
IP address: IP address of the IDS device. You can enter the IP addresses of 100 IDS devices at most.

2. Set the parameters properly.
3. Click **Submit**.

48.2.2 IDS Monitoring

Procedure:

Choose **Policy** > **Security association** > **IDS association** > **IDS Monitoring**.



#	IDS Address	Protocol	Source IP Address	Destination IP Address	Source Port	Destination Port	Aging Time(s)	Operate
No data available in table								

Showing 0 to 0 of 0 entries

The page displays the firewall's dynamic rules based on their generation order. You can filter the rules by protocol or by IDS device IP address.

Click ✖ to delete a rule, or click 🗑 to delete all the rules.

48.3 Configuration Example

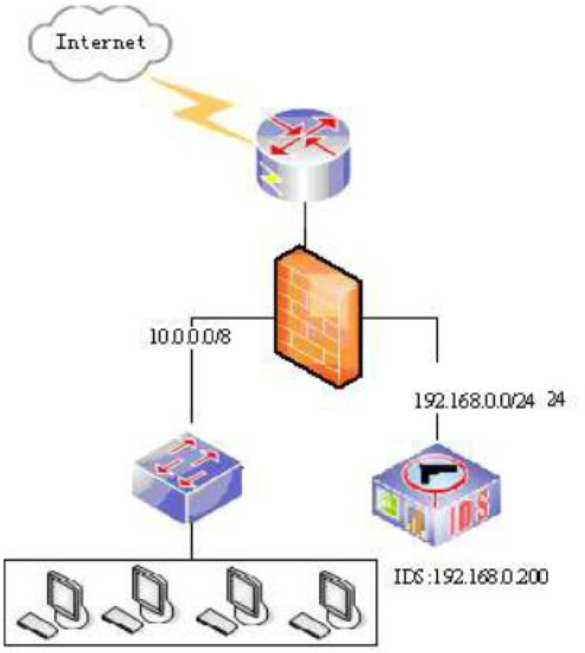
48.3.1 Configuring Association Between a Firewall and an IDS Device in a Light-traffic Network

Description:

In a network with light traffic, configure an IDS device to monitor all the communication data in the network and send association rules to a firewall.

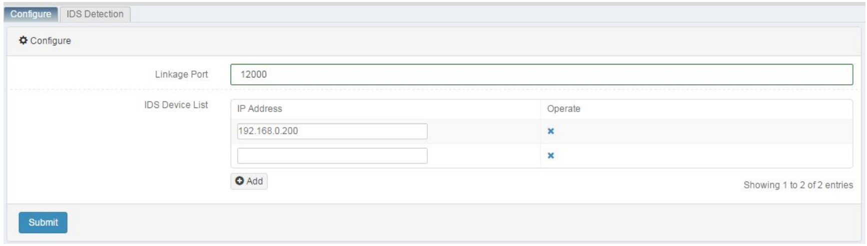
Basic principle: The IDS device is located in the firewall protected network and monitors the network data.

Users use 10.0.0.0/8 for work purposes. The IDS device and firewall use 192.168.0.0/16 for control and collaboration purposes. It is recommended that the control and collaboration network be isolated from the service network to ensure security and real-time services. However, the two networks can be in the same network segment.



Procedure:

1. Choose **Policy** > **Security association** > **IDS association** > **Configuration**.



Configure | IDS Detection

⚙ Configure

Linkage Port: 12000

IDS Device List

IP Address	Operate
192.168.0.200	✖
	✖

2. Set the parameters properly.

3. Click **Submit**.

48.4 Troubleshooting

48.4.1 NG-FW Fails to Block Traffic Despite Dynamic Rules Sent by IDS

Symptom	The NG-FW fails to block related packets after the IDS device sends association rules.

Analysis	The possible causes are: 1. The status of data encryption and authentication between the IDS device and NG-FW is inconsistent. 2. The IDS device and firewall have inconsistent communication port settings. 3. The IP address of the IDS device is not added to the NG-FW's IDS device IP address list.
Solution	1. Check and ensure consistent configurations of the IDS device and NG-FW. 2. Run **debug ids-interaction** to check the interaction between the IDS device and NG-FW. 3. Operate the IDS device to perform encryption and authentication with the NG-FW again.

49 SNMP

49.1 Overview

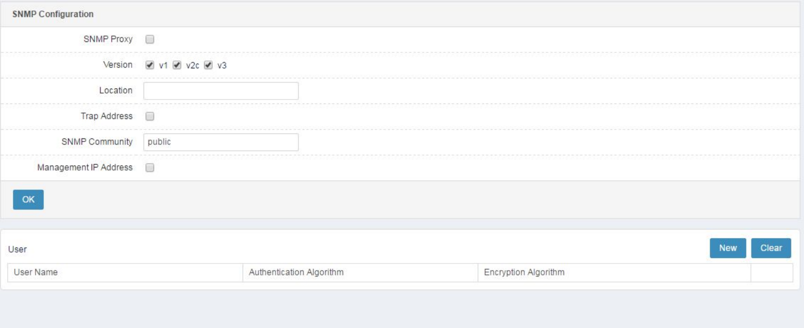
The Simple Network Management Protocol (SNMP) is a set of network management standards. It is compatible with network management systems to monitor devices in a network.

49.2 Configuration

49.2.1 Configuring SNMP

Procedure:

1. Choose **System** > **SNMP**.



SNMP Configuration

SNMP Proxy □

Version ☑ v1 ☑ v2c ☑ v3

Location

Trap Address □

SNMP Community public

Management IP Address □

OK

User

New Clear

User Name	Authentication Algorithm	Encryption Algorithm	

SNMP proxy: Check this box to enable SNMP proxy.

Version: Select an SNMP version. The options include **v1**, **v2c**, and **v3**.

Location: Enter the physical location of the system, in the str ing format.

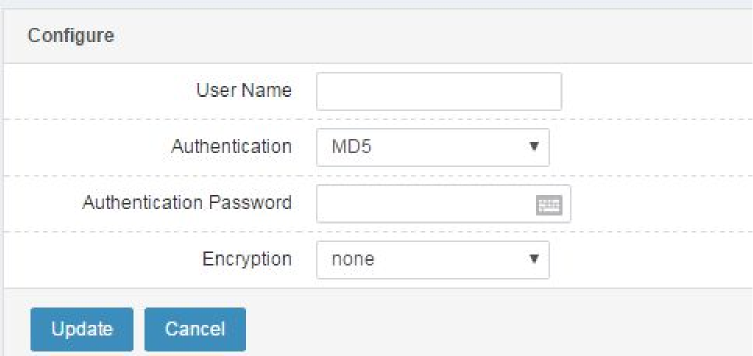
Trap address: Enter the IP address of the trap message receiver.

SNMP community: Enter the SNMP proxy authentication password. The default value is **public**.

Management IP address: Check this box and add IP addresses to enable management IP address filter.

IP address: Add management IP addresses for filter purposes.

User: Create a management user to set the SNMPv3 permissions.



User Name:

Authentication: MD5

Authentication Password:

Encryption: none

User name: User name for SNMPv3 authentication.

Authentication: Authentication mode. The options include **None**, **MD5**, and **SHA**.

Authentication password: Enter an authentication password.

Encryption: Select an encryption mode. The options include **None**, **DES**, and **AES**.

Encryption password: Enter an encryption password when **Encryption** is not set to **None**.

Notice

The authentication mode and password of the SNMPv3 authentication user must be the same as those on the SNMP client.

Procedure:

1. Check the **SNMP proxy** box.
2. Select an SNMP version.
3. Set **Location**.
4. Enter a trap address.
5. Set **SNMP community**.

6. Click **OK**.
7. Click **New** if SNMPv3 authentication is required.
8. On the displayed page, set **User name**, **Authentication**, **Authentication password**, **Encryption**, and **Encryption password.**
9. Click **Update**.

49.2.2 Configuration Example

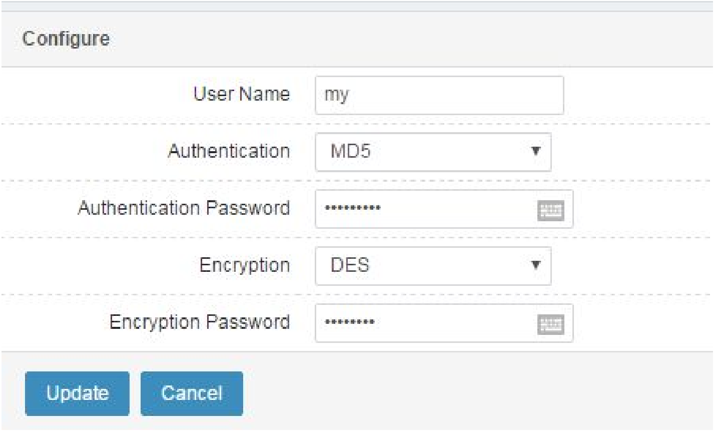
Configuring SNMP

Description:

Enable SNMP proxy, and set **Location** to **beijing**, **Trap address** to **192.168.31.111**, and **SNMP community** to **public**. Create an SNMPv3 authentication user named **my**, select the MD5 authentication algorithm and DES encryption algorithm, and set the authentication password and encryption password to **1234578**.

Procedure:

1. Choose **System management** > **SNMP** to configure an SNMPv3 authentication user.



Configure

User Name: my

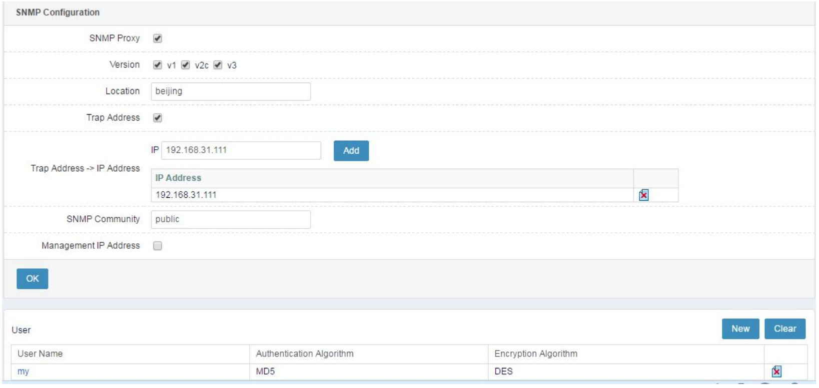
Authentication: MD5

Authentication Password: •••••••••

Encryption: DES

Encryption Password: ••••••••

2. Set parameters, enable SNMP proxy, and select SNMPv3, as shown in the following figure.



SNMP Configuration

SNMP Proxy ☑

Version ☑ v1 ☑ v2c ☑ v3

Location: beijing

Trap Address ☑

Trap Address -> IP Address: IP 192.168.31.111

IP Address	
192.168.31.111	☒

SNMP Community: public

Management IP Address □

User

User Name	Authentication Algorithm	Encryption Algorithm	
my	MD5	DES	☒

After configuration, SNMP clients such as the MIB browser can access the SNMP feature of the firewall. After SNMPv3 user information is configured on the client, it can acquire firewall information.

By default, an SNMP client has the RFC1213 MIB. If you want to read the firewall's private information, import the proprietary MIB file

50 Flow Control Policy

50.1 Overview

The rapid development of network technologies boosts the growth of more complex network applications. Diverse applications are consuming more and more network resources. The fast increase in network traffic results in network congestion and reduced bandwidth utilization.

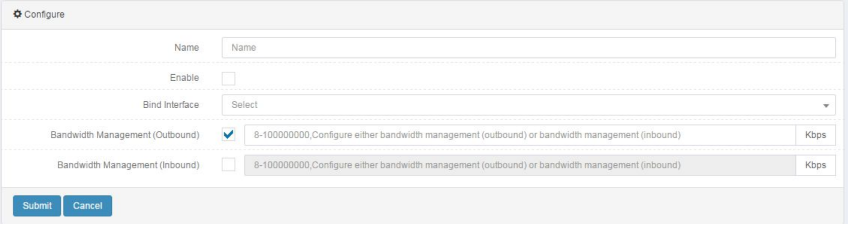
Flow control supports data flow categorization and implements bandwidth sharing and exclusive modes with flexibility based on the containment relationship between categories and subcategories. Bandwidth guarantee is a method to dynamically guarantee bandwidth for important services and employees with network access priority. When such services and employees no longer require bandwidth, it is available for use by other services or employees. The important services and employees can access the Internet at faster speeds and with improved quality without increasing bandwidth. Bandwidth control is a method to reserve bandwidth for specified hosts or services, implement a bandwidth cap, enable even allocation of bandwidth resources, and implement priority management, which effectively improves bandwidth usage and user experience.

50.2 Line Policy Configuration

50.2.1 Configuring a Line Policy

Procedure:

1. Choose **Policy** > **Flow control** > **Line setting** and click **New**.



Configure

Name	Name	
Enable	□	
Bind Interface	Select	
Bandwidth Management (Outbound)	☑ 8-100000000,Configure either bandwidth management (outbound) or bandwidth management (inbound)	Kbps
Bandwidth Management (Inbound)	□ 8-100000000,Configure either bandwidth management (outbound) or bandwidth management (inbound)	Kbps

Name: Name of a line policy.

Enable: Check this box to enable the line policy. The policy will be scheduled only after it is enabled.

Bound interface: Interface bound to the line policy. Only the packets received or sent by the interface are matched with the line policy.

Bandwidth management (outgoing): Maximum bandwidth of outgoing traffic matched with the line policy. The value ranges from **8** to **100000000**, in Kbps.

Bandwidth management (incoming): Maximum bandwidth of incoming traffic matched with the line policy. The value ranges from **8** to **100000000**, in Kbps.

2. Click **Submit** after you complete the settings.

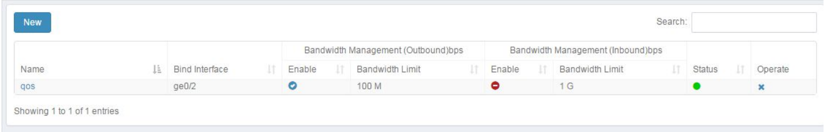
Notice

1. Either **Bandwidth management (outgoing)** or **Bandwidth management (incoming)** must be set.
2. An interface can be bound to only one line policy.
3. A default channel policy is generated for the new line policy.
4. If bandwidth is not set, the default value 10000000 Kbps applies.

50.2.2 Modifying a Line Policy

Procedure:

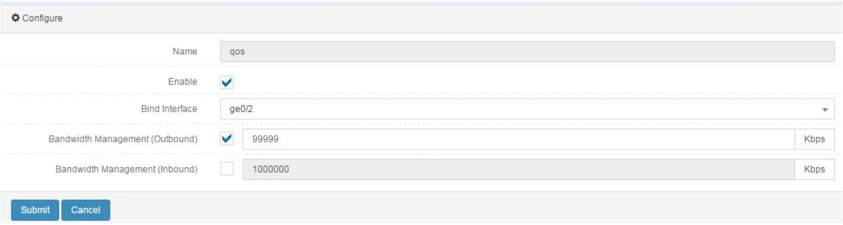
1. Choose **Policy** > Traffic**control** > **Line setting** and click a policy name.



		Bandwidth Management (Outbound)bps		Bandwidth Management (Inbound)bps			
Name	Bind Interface	Enable	Bandwidth Limit	Enable	Bandwidth Limit	Status	Operate
qos	ge0/2	✓	100 M	⊖	1 G	●	✕

Showing 1 to 1 of 1 entries

2. Modify the information about the line policy and click **Submit**.



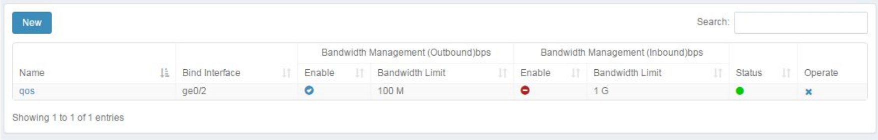
Configure

Name	qos
Enable	☑
Bind Interface	ge0/2
Bandwidth Management (Outbound)	☑ 99999 Kbps
Bandwidth Management (Inbound)	□ 1000000 Kbps

50.2.3 Deleting a Line Policy

Procedure:

1. Choose **Policy** > **Flow control** > **Line setting**. The following page appears.



		Bandwidth Management (Outbound)bps		Bandwidth Management (Inbound)bps			
Name	Bind Interface	Enable	Bandwidth Limit	Enable	Bandwidth Limit	Status	Operate
qos	ge0/2	✓	100 M	⛔	1 G	●	✖

Showing 1 to 1 of 1 entries

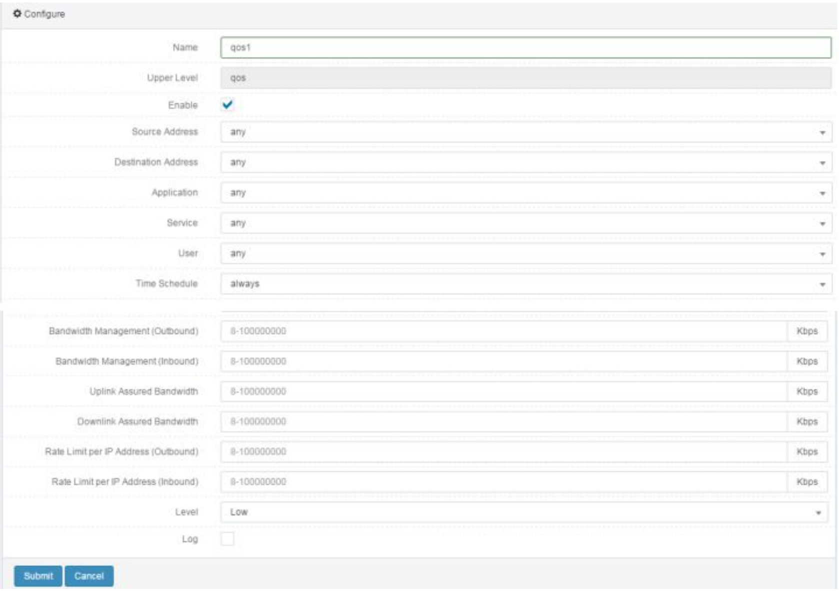
Click ✖ next to the line policy you want to delete.

50.3 Channel Policy Configuration

50.3.1 Configuring a Channel Policy

Procedure:

1. Choose **Policy** > Traffic **control** > **Flow control policy.** Select a line policy and click **New**.



Name	qos1
Upper Level	qos
Enable	☑
Source Address	any
Destination Address	any
Application	any
Service	any
User	any
Time Schedule	always
Bandwidth Management (Outbound)	8-100000000 Kbps
Bandwidth Management (Inbound)	8-100000000 Kbps
Uplink Assured Bandwidth	8-100000000 Kbps
Downlink Assured Bandwidth	8-100000000 Kbps
Rate Limit per IP Address (Outbound)	8-100000000 Kbps
Rate Limit per IP Address (Inbound)	8-100000000 Kbps
Level	Low
Log	□

Name: Name of a channel policy.

Upper level: Parent policy of the channel policy.

Enable: Check this box to enable the channel policy. The policy will be scheduled only after it is enabled.

Source address: Source address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Destination address: Destination address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Application: Application attribute of the data flow. You can reference a predefined application object or application object group. The option **any** indicates any application.

Service: Service attributes of the data flow, including the protocol, source port, and destination port. You can reference a predefined service, a custom service object or service object group. The option **any** indicates any service.

User: User attribute of the data flow. You can reference a user object or a user object group. The option **any** indicates any user.

Time: Policy effective time. You can reference an existing time object. The option **always** indicates all time points.

Maximum bandwidth management (outgoing): Maximum bandwidth of outgoing traffic matched with the channel policy. The value ranges from **8** to **100000000**, in Kbps.

Maximum bandwidth management (incoming): Maximum bandwidth of incoming traffic matched with the channel policy. The value ranges from **8** to **100000000**, in Kbps.

Uplink guaranteed bandwidth: Guaranteed bandwidth of outgoing traffic matched with the channel policy. The value ranges from **8** to **100000000**, in Kbps.

Downlink guaranteed bandwidth: Guaranteed bandwidth of incoming traffic matched with the channel policy. The value ranges from **8** to **100000000**, in Kbps.

Rate limit per IP address (outgoing): Maximum bandwidth of outgoing traffic of each host matched with the policy. Hosts are differentiated by IP addresses. The value ranges from **8** to **100000000**, in Kbps.

Rate limit per IP address (incoming): Maximum bandwidth of incoming traffic of each host matched with the policy. Hosts are differentiated by IP addresses. The value ranges from **8** to **100000000**, in Kbps.

Priority: Priority of the traffic that hits the policy. The options are **High**, **Medium**, and **Low**. The default value is **Low**.

Log: Check this box to enable logging.

2. Click **Submit** after you complete the settings.

⚠ Notice

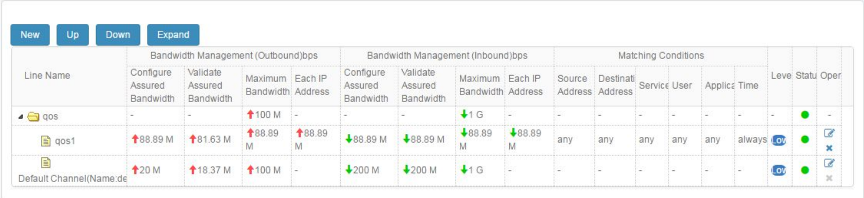
1. When creating a channel policy, select a parent policy, based on which a child policy will be created.
2. When configuring bandwidth, ensure that the child policy's maximum bandwidth and guaranteed bandwidth are not greater than those of the parent policy, and the guaranteed bandwidth is not greater than the maximum bandwidth.
3. A maximum of 32 line policies and 256 channel policies (excluding default policies) can be configured.
4. Each line policy supports level 4 channel policies at most.
5. To schedule a channel policy, enable the policy and its parent policy and upper-level policies.
6. Outgoing traffic and incoming traffic are the traffic transmitted in the outbound and inbound directions of the interface.

50.3.2 Modifying a Channel Policy

Procedure:

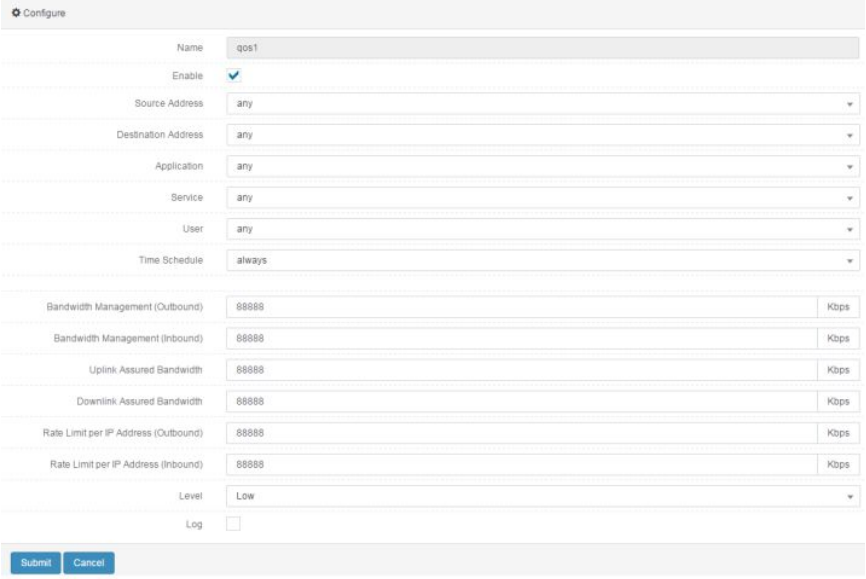
1. Choose **Policy** > Traffic **control** > **Flow control policy** and click 📝 next to

a channel policy.



Line Name	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Matching Conditions						Leve	Statu	Oper
	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Source Address	Destinati Address	Service	User	Applica	Time			
qos	-	-	↑100 M	-	-	-	↓1 G	-	-	-	-	-	-	-	-	●	-
qos1	↑88.89 M	↑81.63 M	↑88.89 M	↑88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	any	any	any	any	any	always	Low	●	✎ ✖
Default Channel(Name:de	↑20 M	↑18.37 M	↑100 M	-	↓200 M	↓200 M	↓1 G	-	-	-	-	-	-	-	Low	●	✎ ✖

2. Modify the information about the channel policy and click **Submit**.

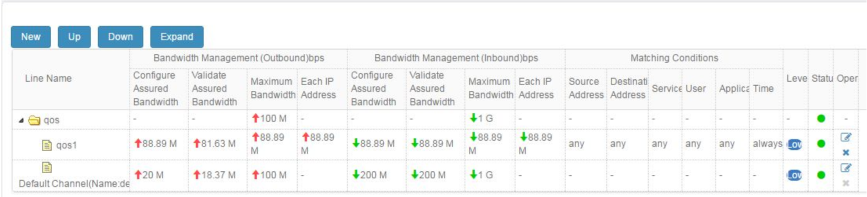


Configure

Name	qos1	
Enable	☑	
Source Address	any	
Destination Address	any	
Application	any	
Service	any	
User	any	
Time Schedule	always	
Bandwidth Management (Outbound)	88888	Kbps
Bandwidth Management (Inbound)	88888	Kbps
Uplink Assured Bandwidth	88888	Kbps
Downlink Assured Bandwidth	88888	Kbps
Rate Limit per IP Address (Outbound)	88888	Kbps
Rate Limit per IP Address (Inbound)	88888	Kbps
Level	Low	
Log	□	

50.3.3 Deleting a Channel Policy

1. Choose **Policy** > **Flow control** > **Flow control policy**. The following page appears.



Line Name	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Matching Conditions						Leve	Statu	Oper
	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Source Address	Destinati Address	Service	User	Applica	Time			
qos	-	-	↑100 M	-	-	-	↓1 G	-	-	-	-	-	-	-	-	●	-
qos1	↑88.89 M	↑81.63 M	↑88.89 M	↑88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	any	any	any	any	any	always	Low	●	✎ ✖
Default Channel(Name:de	↑20 M	↑18.37 M	↑100 M	-	↓200 M	↓200 M	↓1 G	-	-	-	-	-	-	-	Low	●	✎ ✖

2. Click ✖ next to the channel policy you want to delete.

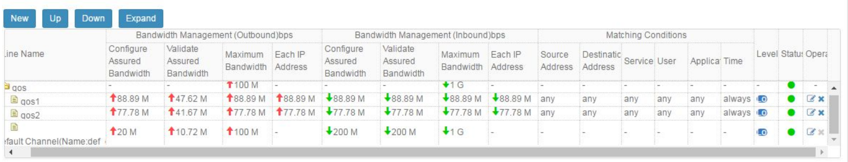
Notice

1. The default channel policy cannot be deleted.
2. When a channel policy is deleted, the lower-level policies are also deleted.

50.3.4 Moving a Channel Policy

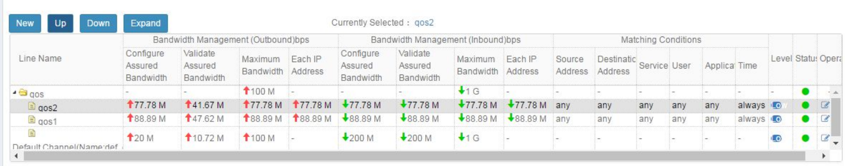
You can change the match priorities of channel policies by adjusting their order. Policies are matched from top down as listed on page.

1. Choose **Policy** > Traffic **control** > **Flow control policy**. The following page appears.



	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Matching Conditions								
ine Name	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Source Address	Destinatic Address	Service	User	Applica	Time	Level	Statu	Opera
qos	-	-	↑100 M	-	-	-	↓1 G	-	-	-	-	-	-	-	-	●	-
qos1	↑88.89 M	↑47.62 M	↑88.89 M	↑88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	any	any	any	any	any	always		●	✎ ✖
qos2	↑77.78 M	↑41.67 M	↑77.78 M	↑77.78 M	↓77.78 M	↓77.78 M	↓77.78 M	↓77.78 M	any	any	any	any	any	always		●	✎ ✖
fault Channel(Name:def	↑20 M	↑10.72 M	↑100 M	-	↓200 M	↓200 M	↓1 G	-	-	-	-	-	-	-		●	✎ ✖

2. Select a policy and click Up or Down .



Currently Selected： qos2

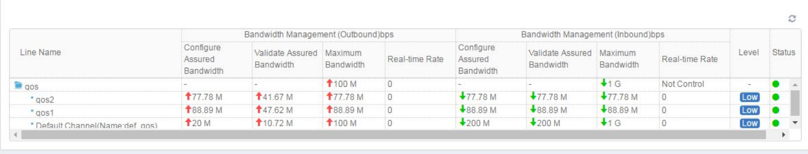
	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Matching Conditions								
Line Name	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Source Address	Destinatic Address	Service	User	Applica	Time	Level	Statu	Opera
qos	-	-	↑100 M	-	-	-	↓1 G	-	-	-	-	-	-	-	-	●	-
qos2	↑77.78 M	↑41.67 M	↑77.78 M	↑77.78 M	↓77.78 M	↓77.78 M	↓77.78 M	↓77.78 M	any	any	any	any	any	always		●	✎
qos1	↑88.89 M	↑47.62 M	↑88.89 M	↑88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	↓88.89 M	any	any	any	any	any	always		●	✎
Default Channel(Name:def	↑20 M	↑10.72 M	↑100 M	-	↓200 M	↓200 M	↓1 G	-	-	-	-	-	-	-		●	✎

Notice

1. Only the order of channel policies of the same levels can be adjusted.
2. The default channel policy cannot be moved.

50.4 Flow Control Monitoring

Choose **Policy** > Traffic **control** > **Flow control monitoring**. A page appears to display the flow control results, as shown in the following figure.



Line Name	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Level	Status
	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Real-time Rate	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Real-time Rate		
qos	-	-	↑100 M	0	-	-	↓1 G	Not Control	-	●
qos2	↑77.78 M	↑41.67 M	↑77.78 M	0	↓77.78 M	↓77.78 M	↓77.78 M	0	Low	●
qos1	↑88.89 M	↑47.62 M	↑88.89 M	0	↓88.89 M	↓88.89 M	↓88.89 M	0	Low	●
Default Channel(Name:def_qos)	↑20 M	↑10.72 M	↑100 M	0	↓200 M	↓200 M	↓1 G	0	Low	●

Click 🔄 to refresh the statistics.

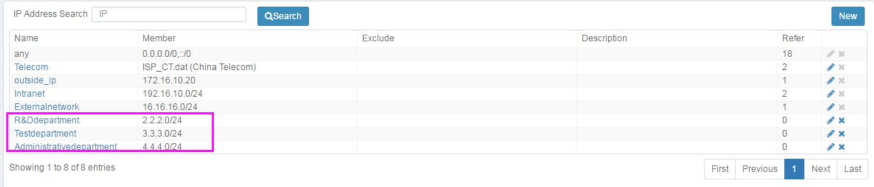
50.5 Configuration Example

Description:

A company has 10 Mbit/s bandwidth and connects to the Internet through NIC eth0. The company wants to allocate 2 Mbit/s bandwidth to the R&D department, 5 Mbit/s bandwidth to the test department, and 3 Mbit/s bandwidth to the administrative department. Within the departments, to allow key applications to run stably and important employees to use network smoothly, it is necessary to limit work-unrelated traffic, prevent bandwidth overuse, and limit and guarantee traffic based on service types. For the R&D department, limit bandwidth consumed by chatting to 0.5 Mbit/s, ensure 1 Mbit/s bandwidth for email exchange, and limit the download bandwidth to 0.5 Mbit/s.

Procedure:

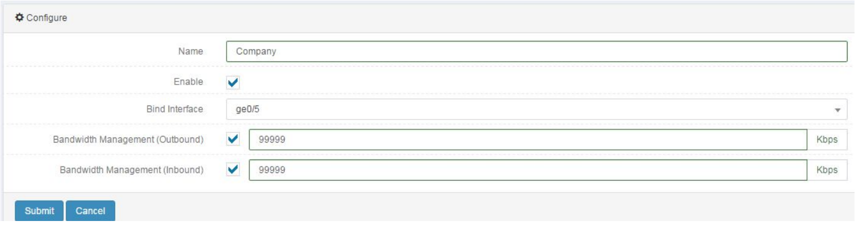
1. Choose **Object** > **Address object** > **Address node**, and configure address objects named **R&D department**, **Test department**, and **Administrative department**, as shown in the following figure.



Name	Member	Exclude	Description	Refer	
any	0.0.0.0/0,::/0			18	✎ ✖
Telecom	ISP_CT.dat (China Telecom)			2	✎ ✖
outside_ip	172.16.10.20			1	✎ ✖
Intranet	192.16.10.0/24			2	✎ ✖
Externalnetwork	16.16.16.0/24			1	✎ ✖
R&Ddepartment	2.2.2.0/24			0	✎ ✖
Testdepartment	3.3.3.0/24			0	✎ ✖
Administrativedepartment	4.4.4.0/24			0	✎ ✖

Showing 1 to 8 of 8 entries

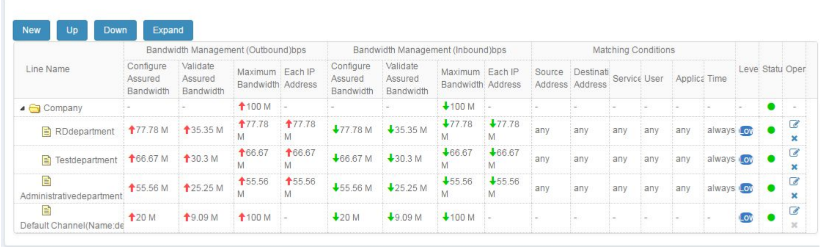
2. Choose **Policy** > Traffic **control** > **Line setting** and click **New**. Set parameters, as shown in the following figure.



Configure

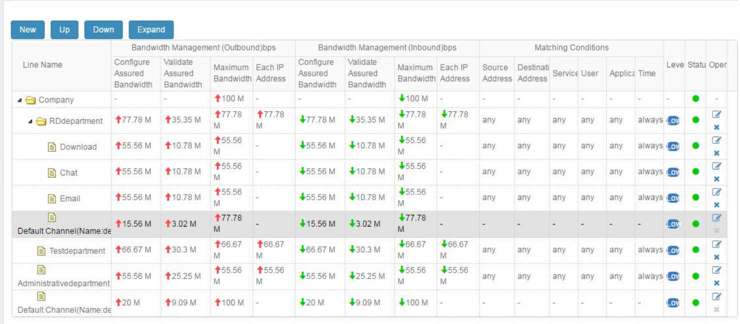
Name	Company	
Enable	☑	
Bind Interface	ge0/5	
Bandwidth Management (Outbound)	☑ 99999	Kbps
Bandwidth Management (Inbound)	☑ 99999	Kbps

Choose **Policy** > **Flow control** > **Flow control policy**. Under the line policy named **Company**, configure flow control policies named **R&D department**, **Test department**, and **Administrative department**, as shown in the following figure.



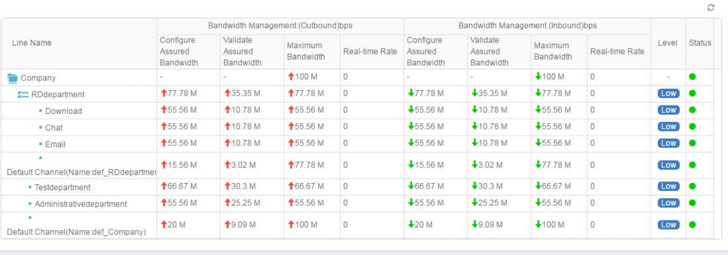
Line Name	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Matching Conditions						Leve	Statu	Oper
	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Source Address	Destinati Address	Service	User	Applica	Time			
Company	-	-	↑100 M	-	-	-	↓100 M	-	-	-	-	-	-	-	-	●	-
RDdepartment	↑77.78 M	↑35.35 M	↑77.78 M	↑77.78 M	↓77.78 M	↓35.35 M	↓77.78 M	↓77.78 M	any	any	any	any	any	always	Low	●	
Testdepartment	↑66.67 M	↑30.3 M	↑66.67 M	↑66.67 M	↓66.67 M	↓30.3 M	↓66.67 M	↓66.67 M	any	any	any	any	any	always	Low	●	
Administrativedepartment	↑55.56 M	↑25.25 M	↑55.56 M	↑55.56 M	↓55.56 M	↓25.25 M	↓55.56 M	↓55.56 M	any	any	any	any	any	always	Low	●	
Default Channel(Name:de	↑20 M	↑9.09 M	↑100 M	-	↓20 M	↓9.09 M	↓100 M	-	-	-	-	-	-	-	Low	●	

3. Choose **Policy** > **Flow control** > **Flow control policy**. Under the flow control policy named **R&D department**, configure flow control policies named **Download**, **Chat**, and **Email**, as shown in the following figure.



Line Name	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Matching Conditions						Leve	Statu	Oper
	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Each IP Address	Source Address	Destinati Address	Service	User	Applica	Time			
Company	-	-	↑100 M	-	-	-	↓100 M	-	-	-	-	-	-	-	-	●	-
RDdepartment	↑77.78 M	↑35.35 M	↑77.78 M	↑77.78 M	↓77.78 M	↓35.35 M	↓77.78 M	↓77.78 M	any	any	any	any	any	always	Low	●	
Download	↑55.56 M	↑10.78 M	↑55.56 M	-	↓55.56 M	↓10.78 M	↓55.56 M	-	any	any	any	any	any	always	Low	●	
Chat	↑55.56 M	↑10.78 M	↑55.56 M	-	↓55.56 M	↓10.78 M	↓55.56 M	-	any	any	any	any	any	always	Low	●	
Email	↑55.56 M	↑10.78 M	↑55.56 M	-	↓55.56 M	↓10.78 M	↓55.56 M	-	any	any	any	any	any	always	Low	●	
Default Channel(Name:de	↑15.56 M	↑3.02 M	↑77.78 M	-	↓15.56 M	↓3.02 M	↓77.78 M	-	-	-	-	-	-	-	Low	●	
Testdepartment	↑66.67 M	↑30.3 M	↑66.67 M	↑66.67 M	↓66.67 M	↓30.3 M	↓66.67 M	↓66.67 M	any	any	any	any	any	always	Low	●	
Administrativedepartment	↑55.56 M	↑25.25 M	↑55.56 M	↑55.56 M	↓55.56 M	↓25.25 M	↓55.56 M	↓55.56 M	any	any	any	any	any	always	Low	●	
Default Channel(Name:de	↑20 M	↑9.09 M	↑100 M	-	↓20 M	↓9.09 M	↓100 M	-	-	-	-	-	-	-	Low	●	

4. After the configuration is complete, choose **Policy** > **Flow control** > **Flow control monitoring** to check the flow control results.



Line Name	Bandwidth Management (Outbound)bps				Bandwidth Management (Inbound)bps				Level	Status
	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Real-time Rate	Configure Assured Bandwidth	Validate Assured Bandwidth	Maximum Bandwidth	Real-time Rate		
Company	-	-	↑100 M	0	-	-	↓100 M	0	-	●
RDdepartment	↑77.78 M	↑35.35 M	↑77.78 M	0	↓77.78 M	↓35.35 M	↓77.78 M	0	Low	●
Download	↑55.56 M	↑10.78 M	↑55.56 M	0	↓55.56 M	↓10.78 M	↓55.56 M	0	Low	●
Chat	↑55.56 M	↑10.78 M	↑55.56 M	0	↓55.56 M	↓10.78 M	↓55.56 M	0	Low	●
Email	↑55.56 M	↑10.78 M	↑55.56 M	0	↓55.56 M	↓10.78 M	↓55.56 M	0	Low	●
Default Channel(Name:def_RDdepartmer	↑15.56 M	↑3.02 M	↑77.78 M	0	↓15.56 M	↓3.02 M	↓77.78 M	0	Low	●
Testdepartment	↑66.67 M	↑30.3 M	↑66.67 M	0	↓66.67 M	↓30.3 M	↓66.67 M	0	Low	●
Administrativedepartment	↑55.56 M	↑25.25 M	↑55.56 M	0	↓55.56 M	↓25.25 M	↓55.56 M	0	Low	●
Default Channel(Name:def_Company)	↑20 M	↑9.09 M	↑100 M	0	↓20 M	↓9.09 M	↓100 M	0	Low	●

51 Session Control Policy

51.1 Overview

RAVEN5000firewalls introduce session control policies to control the sessions of data flows.

You can control new connections or concurrent connections to protect connection tables from attacks, and limit the bandwidth consumed by some services or applications.

Session control can be based on the inbound interface, source address, destination address, time, service, or application combination. Session control includes source host connections limit, source host connection rate limit, destination host connections limit, destination host connection rate limit, total connections limit, and total connection rate limit.

You can configure session control policies on a firewall to effectively control the data flows passing the firewall. When receiving a packet, the firewall matches the packet's source address, destination address, and service information to the configured session control policies to determine whether to limit the data flow. The firewall associates the data flow with the hit policy to determine how to process subsequent packets.

Session control policies of the IPv4 or IPv6 type are matched from top down as listed on page. The policies are only applied to the packets passing a firewall, but not to the packets sent by the firewall.

51.2 Configuration

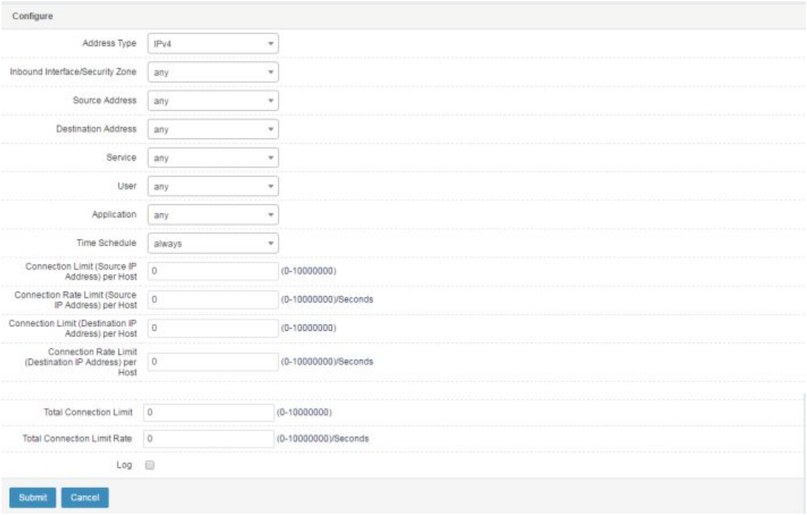
51.2.1 Configuring Basic Policy Elements

A session control policy has two basic elements: match conditions and session limit. The match conditions include a data flow's inbound interface, source address, destination address, service, application, and policy effective period. The inbound interface, source address, destination address, service, application, and policy effective period can reference predefined objects.

Session control includes source host connections limit, source host connection rate limit, destination host connections limit, destination host connection rate limit, total connections limit, and total connection rate limit, which are configurable.

Procedure:

1. Choose **Policy** > **Session control** and click **New**.



Configure

Address Type	IPv4	
Inbound Interface/Security Zone	any	
Source Address	any	
Destination Address	any	
Service	any	
User	any	
Application	any	
Time Schedule	always	
Connection Limit (Source IP Address) per Host	0	(0-10000000)
Connection Rate Limit (Source IP Address) per Host	0	(0-10000000)/Seconds
Connection Limit (Destination IP Address) per Host	0	(0-10000000)
Connection Rate Limit (Destination IP Address) per Host	0	(0-10000000)/Seconds
Total Connection Limit	0	(0-10000000)
Total Connection Limit Rate	0	(0-10000000)/Seconds
Log	□	

Parameter description:

Address type: Session control policies are classified into IPv4 and IPv6 types. Packets are matched with policies of the corresponding protocol type.

Inbound interface: Inbound direction of a data flow. You can specify an interface. The option **any** indicates all interfaces.

Source address: Source address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Destination address: Destination address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Service: Service attributes of the data flow, including the protocol, source port, and destination port. You can reference a predefined service, a custom service object or service object group. The option **any** indicates any service.

User: User attribute of the data flow. You can reference a predefined user object or user group. The option **any** indicates any user.

Application: Application attribute of the data flow. You can reference a predefined application. The option **any** indicates any application.

Time: Policy effective time. You can reference an existing time object. The option **always** indicates all time points.

Connections limit per host (source IP address): Connections limit by source address for the data flow that hits the policy. The value **0** indicates no limit.

Connection rate limit per host (source IP address): Connection rate limit by source address for the data flow that hits the policy. The value **0** indicates no limit.

Connections limit per host (destination IP address): Connections limit by destination address for the data flow that hits the policy. The value **0** indicates no limit.

Connection rate limit per host (destination IP address) : Connection rate limit by destination address for the data flow that hits the policy. The value **0** indicates no limit.

Total connections limit: Total connections limit for the data flow that hits the policy. The value **0** indicates no limit.

Total connection rate limit: Total connection rate limit for the data flow that hits the policy. The value **0** indicates no limit.

Log: Check this box to enable logging. If the data flow hits the policy, the block information will be sent to a syslog server or a device-level local log will be generated. The log priority is Info.

2. Click **Submit** after you complete the settings.

Note

The inbound interface cannot be a trunk interface.

Note

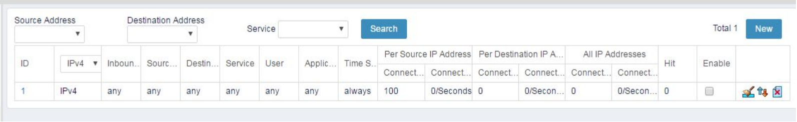
1. When creating a session control policy, you must reference an address object of the same protocol type.
2. An ID is automatically generated to uniquely identify the session control policy. The IDs of session control policies of different protocol types are independent of each other.

51.2.2 Enabling a Session Control Policy

After you configure a session control policy, enable it to make it effective.

Procedure:

1. Choose **Policy** > **Session control**. The following page appears.



Source Address ▼ | Destination Address ▼ | Service ▼ | Search | Total 1 | New

ID	IPv4 ▼	Inboun...	Sourc...	Destin...	Service	User	Applic...	Time S...	Per Source IP Address		Per Destination IP A...		All IP Addresses		Hit	Enable	
									Connect...	Connect...	Connect...	Connect...	Connect...	Connect...			
1	IPv4	any	any	any	any	any	any	always	100	0/Seconds	0	0/Secon...	0	0/Secon...	0	□	

2. Check the **Enable** box next to a session control policy to enable it.

Notice

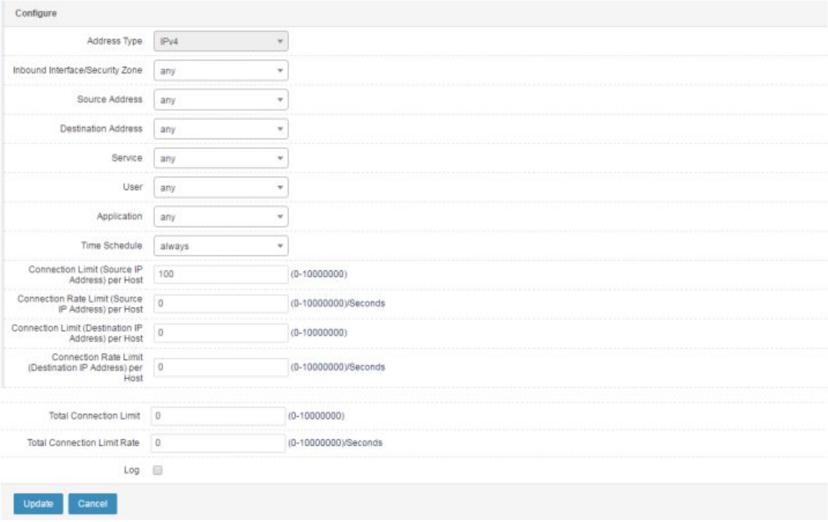
By default, a session control policy is in the disabled state after being configured. It must be enabled manually to take effect.

51.2.3 Modifying a Session Control Policy

Procedure:

1. Choose **Policy** > **Session control** and click a policy ID.

2. Modify the information about the session control policy and click **Submit**.



Configure

Address Type	IPv4 ▼	
Inbound Interface/Security Zone	any ▼	
Source Address	any ▼	
Destination Address	any ▼	
Service	any ▼	
User	any ▼	
Application	any ▼	
Time Schedule	always ▼	
Connection Limit (Source IP Address) per Host	100	(0-10000000)
Connection Rate Limit (Source IP Address) per Host	0	(0-10000000)/Seconds
Connection Limit (Destination IP Address) per Host	0	(0-10000000)
Connection Rate Limit (Destination IP Address) per Host	0	(0-10000000)/Seconds
Total Connection Limit	0	(0-10000000)
Total Connection Limit Rate	0	(0-10000000)/Seconds
Log	□	

Update | Cancel

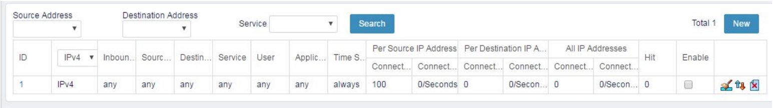
Notice

The address type cannot be changed.

51.2.4 Deleting a Session Control Policy

Procedure:

1. Choose **Policy** > **Session control**. The following page appears.



ID	IPv4	Inboun...	Sourc...	Destin...	Service	User	Applic...	Time S...	Per Source IP Address		Per Destination IP A...		All IP Addresses		Hit	Enable	
									Connect...	Connect...	Connect...	Connect...	Connect...	Connect...			
1	IPv4	any	any	any	any	any	any	always	100	0/Seconds	0	0/Secon...	0	0/Secon...	0	□	

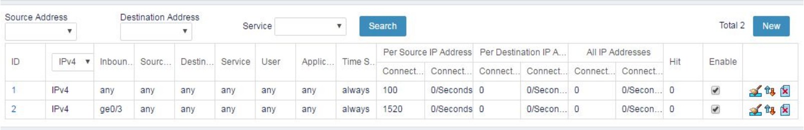
2. Click next to the session control policy you want to delete.

51.2.5 Adjusting the Order of Session Control Policies

You can change the match priorities of session control policies by adjusting their order. Policies are matched from top down as listed on page.

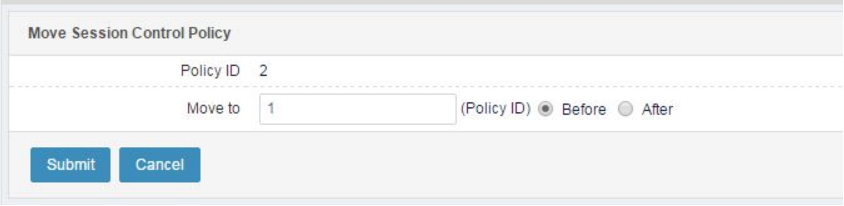
Procedure:

1. Choose **Policy** > **Session control**. The following page appears.



ID	IPv4	Inboun...	Sourc...	Destin...	Service	User	Applic...	Time S...	Per Source IP Address		Per Destination IP A...		All IP Addresses		Hit	Enable	
									Connect...	Connect...	Connect...	Connect...	Connect...	Connect...			
1	IPv4	any	any	any	any	any	any	always	100	0/Seconds	0	0/Secon...	0	0/Secon...	0	☑	
2	IPv4	ge0/3	any	any	any	any	any	always	1520	0/Seconds	0	0/Secon...	0	0/Secon...	0	☑	

2. Click next to the policy you want to move.



Move Session Control Policy

Policy ID 2

Move to 1 (Policy ID) ● Before ○ After

Policy ID: ID of the policy to be moved.

Move to: ID of the reference policy.

Before: Move the policy before the reference policy.

After: Move the policy after the reference policy.

3. Click **Submit**.

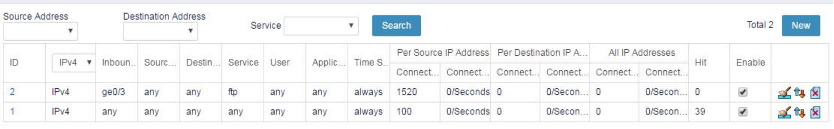
Notice

Only the order of policies of the same protocol type can be adjusted.

51.2.6 Querying Session Control Policies

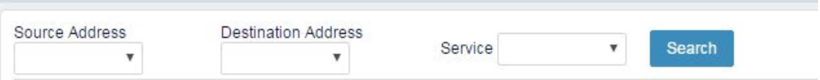
Procedure:

1. Choose **Policy** > **Session control**. The following page appears.



ID	IPv4	Inboun...	Sourc...	Destin...	Service	User	Applic...	Time S...	Per Source IP Address		Per Destination IP A...		All IP Addresses		Hit	Enable	
									Connect...	Connect...	Connect...	Connect...	Connect...	Connect...			
2	IPv4	ge0/3	any	any	ftp	any	any	always	1520	0/Seconds	0	0/Secon...	0	0/Secon...	0	☑	
1	IPv4	any	any	any	any	any	any	always	100	0/Seconds	0	0/Secon...	0	0/Secon...	39	☑	

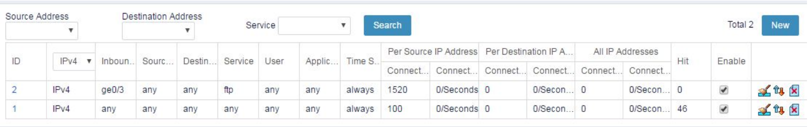
2. Select options for **Source address**, **Destination address**, and **Service** , and click **Search** to search for the session control policies that match the criteria.



51.3 Monitoring and Maintenance

51.3.1 Displaying Session Control Policies

Choose **Policy** > **Session control** to display existing session control policies by protocol type.



ID	IPv4	Inboun...	Sourc...	Destin...	Service	User	Applic...	Time S...	Per Source IP Address		Per Destination IP A...		All IP Addresses		Hit	Enable	
									Connect...	Connect...	Connect...	Connect...	Connect...	Connect...			
2	IPv4	ge0/3	any	any	ftp	any	any	always	1520	0/Seconds	0	0/Secon...	0	0/Secon...	0	☑	
1	IPv4	any	any	any	any	any	any	always	100	0/Seconds	0	0/Secon...	0	0/Secon...	46	☑	

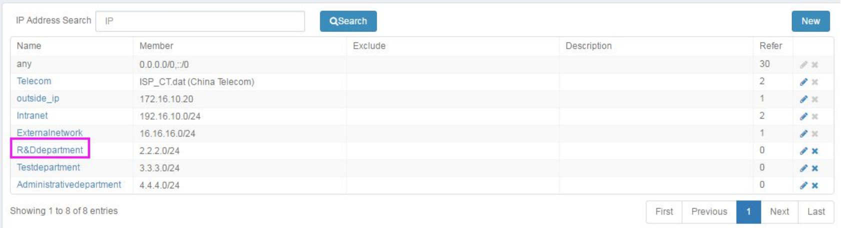
51.4 Configuration Example

51.4.1 Creating an IPv4 Session Control Policy to Limit the Total Connection Rate

Create an IPv4 session control policy to limit the total connection rate of sessions initiated by the R&D department for external service access through a firewall.

Procedure:

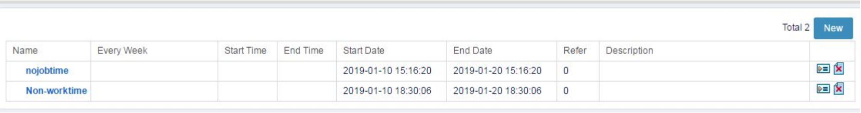
1. Choose **Object** > **Address object** > **Address node**, and configure an address object named **R&D department**, as shown in the following figure.



Name	Member	Exclude	Description	Refer	
any	0.0.0.0/0,::/0			30	
Telecom	ISP_CT.dat (China Telecom)			2	
outside_ip	172.16.10.20			1	
Intranet	192.16.10.0/24			2	
Externalnetwork	16.16.16.0/24			1	
R&Ddepartment	2.2.2.0/24			0	
Testdepartment	3.3.3.0/24			0	
Administrativedepartment	4.4.4.0/24			0	

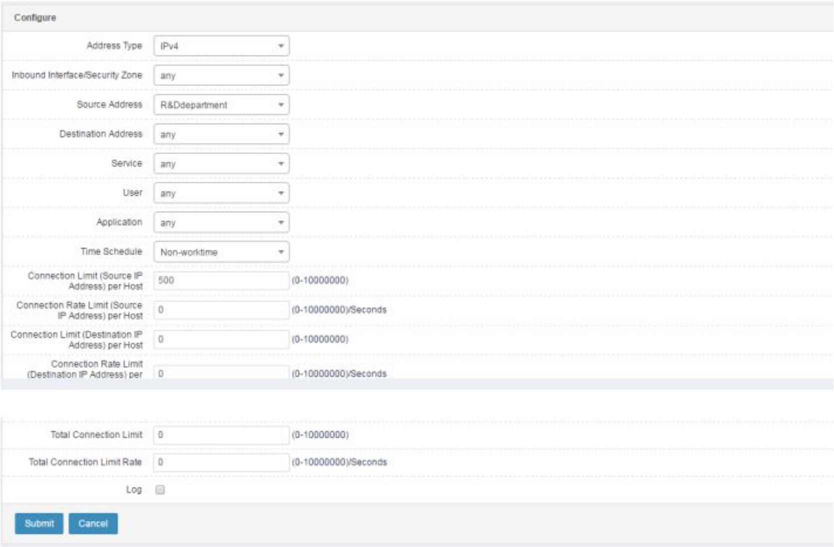
Showing 1 to 8 of 8 entries

2. Choose **Object** > **Time object** > **Absolute time**, and configure a time object named **Non-work time**, as shown in the following figure.



Name	Every Week	Start Time	End Time	Start Date	End Date	Refer	Description
nojobtime				2019-01-10 15:16:20	2019-01-20 15:16:20	0	
Non-worktime				2019-01-10 18:30:06	2019-01-20 18:30:06	0	

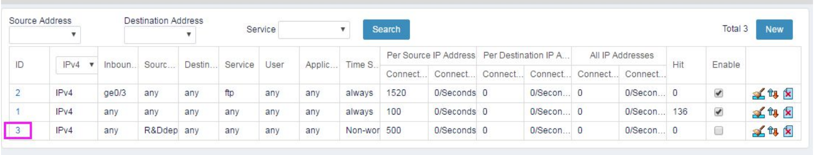
3. Choose **Policy** > **Session control** and click **New**. Set parameters, as shown in the following figure.


Configure

Address Type	IPv4	
Inbound Interface/Security Zone	any	
Source Address	R&Ddepartment	
Destination Address	any	
Service	any	
User	any	
Application	any	
Time Schedule	Non-worktime	
Connection Limit (Source IP Address) per Host	500	(0-10000000)
Connection Rate Limit (Source IP Address) per Host	0	(0-10000000)/Seconds
Connection Limit (Destination IP Address) per Host	0	(0-10000000)
Connection Rate Limit (Destination IP Address) per	0	(0-10000000)/Seconds
Total Connection Limit	0	(0-10000000)
Total Connection Limit Rate	0	(0-10000000)/Seconds
Log	□	

4. Click **Submit**.

5. Choose **Policy** > **Session control**. The following page appears.



ID	IPv4	Inboun...	Sourc...	Destin...	Service	User	Applic...	Time S...	Per Source IP Address		Per Destination IP A...		All IP Addresses		Hit	Enable	
									Connect...	Connect...	Connect...	Connect...	Connect...	Connect...			
2	IPv4	ge0/3	any	any	ftp	any	any	always	1520	0/Seconds	0	0/Secon...	0	0/Secon...	0	☑	
1	IPv4	any	any	any	any	any	any	always	100	0/Seconds	0	0/Secon...	0	0/Secon...	136	☑	
3	IPv4	any	R&Ddep	any	any	any	any	Non-wor	500	0/Seconds	0	0/Secon...	0	0/Secon...	0	□	

6. Click **Enable**.

51.5 Troubleshooting

51.5.1 A Data Flow That Hits a Policy Is Not Limited

Symptom	The corresponding action is not taken for the data flow that hits a policy.
Analysis	The possible causes are as follows: ➢ The policy is not enabled. ➢ Because policies with the same inbound interface in the IPv4 or IPv6 format are matched from top down as listed on page, the data flow may have hit a previous policy.

Solution	Enable the policy. If the policy conflicts with other policies, modify the policy or adjust the policy order.

52 Web Authentication Policy

52.1 Overview

Before configuring a web authentication policy, configure an authentication user group and an authentication server. You can configure an authentication user or an authentication user group. However, web authentication policies only support user groups. Web authentication policies are used to filter out the packets of unauthenticated users. The packets of authenticated users are forwarded.

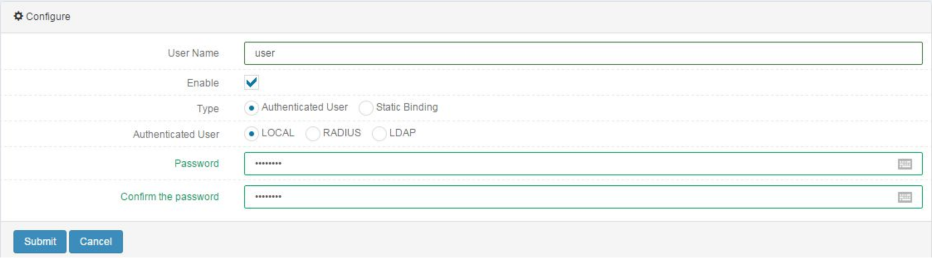
52.2 Configuration

52.2.1 Configuring a User

You can configure an authentication user or a statically bound user.

Procedure for creating an authentication user:

1. Choose **Object** > **User object** > **User** and click **New**.



Configure

User Name	user
Enable	☑
Type	● Authenticated User ○ Static Binding
Authenticated User	● LOCAL ○ RADIUS ○ LDAP
Password	••••••••
Confirm the password	••••••••

Parameter description:

User name: Name of a user.

Enable: Check this box to enable the user object.

Type: The options are **Authentication user** and **Static binding**.

Authentication user: If you select this option, select one of the following server types:

LOCAL: Local authentication. You can add the user name to the firewall's user database, and set a password to allow the user to perform authentication using the internal database.

RADIUS: Server authentication. You can add a RADIUS server and select **RADIUS** to allow the user to perform authentication using the specified server.

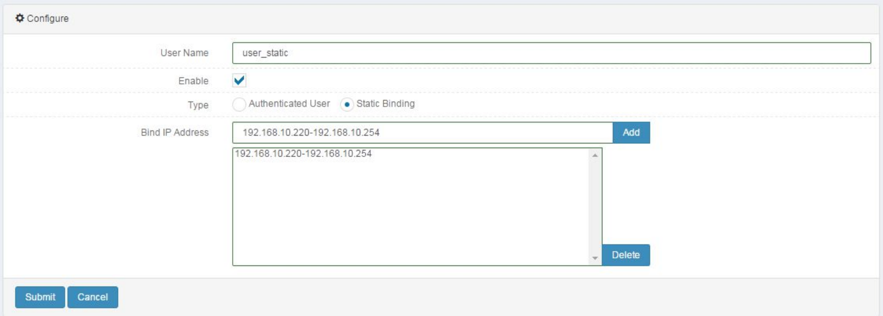
LDAP: Server authentication. You can add an LDAP server and select **LDAP** to allow the user to perform authentication using the specified server.

Password: Enter a password for the user.

Confirm password: Enter the password again.

Procedure for creating a statically bound user:

2. Choose **Object** > **User object** > **User** and click **New**.



User Name: user_static

Enable: ☑

Type: ○ Authenticated User ● Static Binding

Bind IP Address: 192.168.10.220-192.168.10.254

192.168.10.220-192.168.10.254

Parameter description:

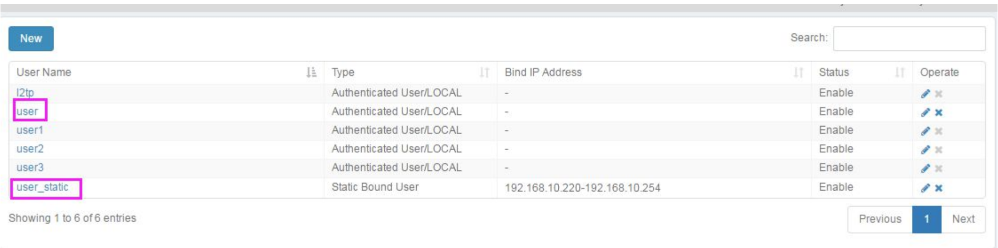
User name: Name of a user.

Enable: Check this box to enable the user object.

Type: The options are **Authentication user** and **Static binding**.

Bound IP address: You can bind an IP address or an IP address segment.

3. Click **Submit** after you complete the user object settings. The following page appears.

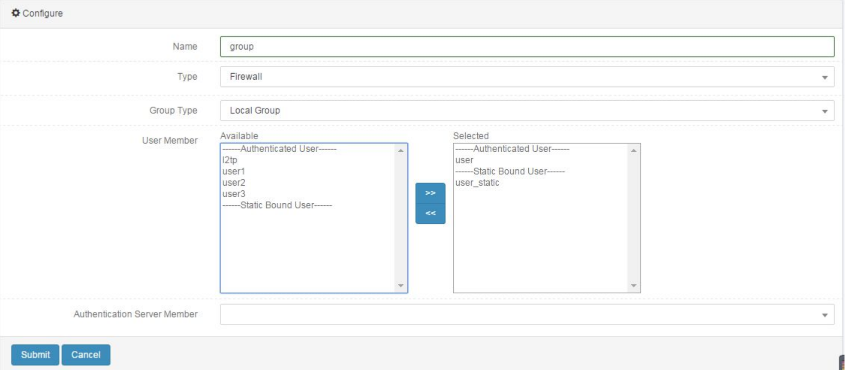


User Name	Type	Bind IP Address	Status	Operate
l2tp	Authenticated User/LOCAL	-	Enable	✎ ✖
user	Authenticated User/LOCAL	-	Enable	✎ ✖
user1	Authenticated User/LOCAL	-	Enable	✎ ✖
user2	Authenticated User/LOCAL	-	Enable	✎ ✖
user3	Authenticated User/LOCAL	-	Enable	✎ ✖
user_static	Static Bound User	192.168.10.220-192.168.10.254	Enable	✎ ✖

Showing 1 to 6 of 6 entries

52.2.2 Configuring a User Group

1. Choose **Object** > **User object** > **User group** and click **New.**



Name	group
Type	Firewall
Group Type	Local Group
User Member	Available: ------Authenticated User------ l2tp user1 user2 user3 ------Static Bound User------ Selected: ------Authenticated User------ user ------Static Bound User------ user_static
Authentication Server Member	

Parameter description:

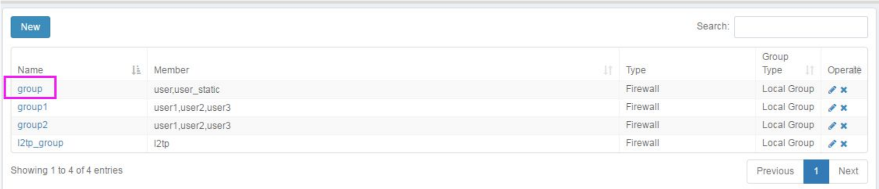
User name: Name of a user group.

Description: Description about the user group.

Members: Add existing users to the user group.

Authentication server members: Select authentication servers. Local authentication is applied by default.

2. Click **Submit** after you complete the user group settings. The following page appears.

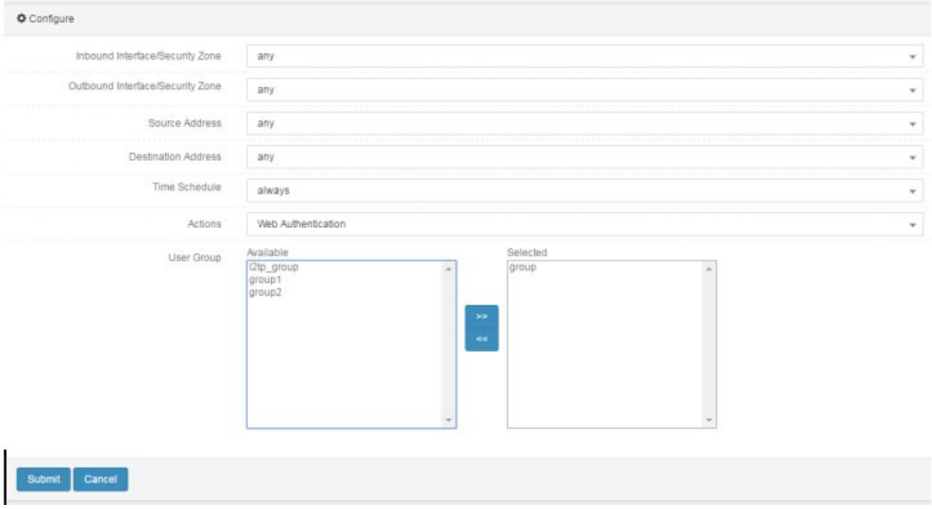


Name	Member	Type	Group Type	Operate
group	user,user_static	Firewall	Local Group	✎ ✖
group1	user1,user2,user3	Firewall	Local Group	✎ ✖
group2	user1,user2,user3	Firewall	Local Group	✎ ✖
l2tp_group	l2tp	Firewall	Local Group	✎ ✖

Showing 1 to 4 of 4 entries

52.2.3 Configuring a Web Authentication Policy

1. Choose **Policy** > **Web authentication** > **Policy** and click **New.**



Inbound Interface/Security Zone: any

Outbound Interface/Security Zone: any

Source Address: any

Destination Address: any

Time Schedule: always

Actions: Web Authentication

User Group: Available: l2tp_group, group1, group2; Selected: group

Parameter description:

Inbound interface/Security zone: Inbound direction of a data flow. You can specify an interface. The option **any** indicates all interfaces.

Outbound interface/Security zone: Outbound direction of a data flow. You can specify an interface. The option **any** indicates all interfaces.

Source address: Source address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Destination address: Destination address of the data flow. You can reference a predefined address object or address object group. The option **any** indicates any address.

Time: Policy effective time. You can reference an existing time object. The option **always** indicates all time points.

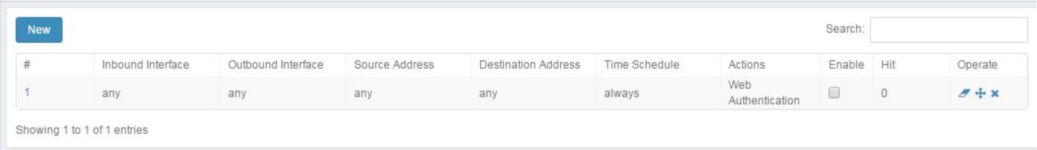
Action: Action to be taken when the policy is hit. The options are **Web authentication** and **Permit**.

User group: User group object. You can reference predefined user group objects.

⚠ Notice

User group must be specified when **Web authentication** is selected for **Action**.

2. Click **Submit** after you complete the settings. The following page appears.



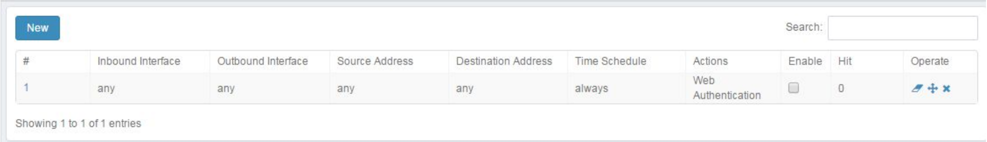
#	Inbound Interface	Outbound Interface	Source Address	Destination Address	Time Schedule	Actions	Enable	Hit	Operate
1	any	any	any	any	always	Web Authentication	□	0	

Showing 1 to 1 of 1 entries

52.2.4 Modifying a Web Authentication Policy

You can modify an existing web authentication policy.

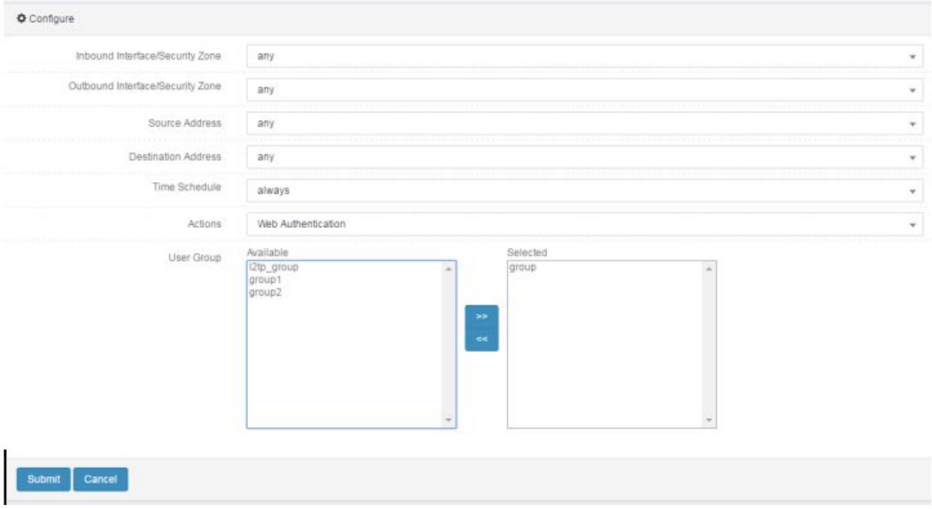
1. Choose **Policy** > **Web authentication** > **Policy**. The following page appears.



#	Inbound Interface	Outbound Interface	Source Address	Destination Address	Time Schedule	Actions	Enable	Hit	Operate
1	any	any	any	any	always	Web Authentication	□	0	

Showing 1 to 1 of 1 entries

2. Click a policy ID.



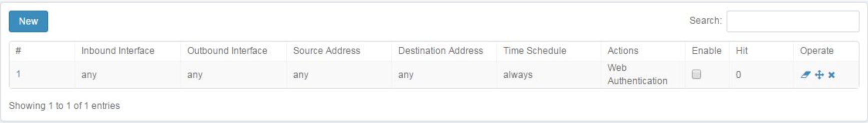
Inbound Interface/Security Zone	any
Outbound Interface/Security Zone	any
Source Address	any
Destination Address	any
Time Schedule	always
Actions	Web Authentication
User Group	Available: l2tp_group group1 group2 Selected: group

Modify the information about the web authentication policy

3. Click **Submit**.

52.2.5 Deleting a Web Authentication Policy

1. Choose **Policy** > **Web authentication** > **Policy**. The following page appears.



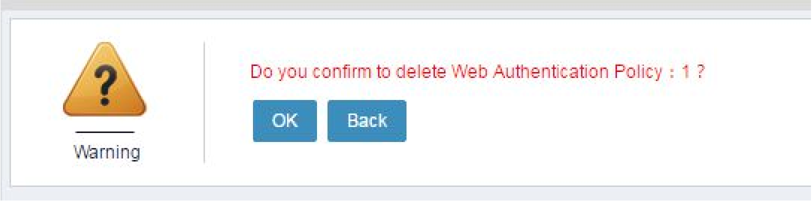
New

Search:

#	Inbound Interface	Outbound Interface	Source Address	Destination Address	Time Schedule	Actions	Enable	Hit	Operate
1	any	any	any	any	always	Web Authentication	□	0	✎ ✣ ✖

Showing 1 to 1 of 1 entries

2. Click ✖ next to the policy you want to delete.



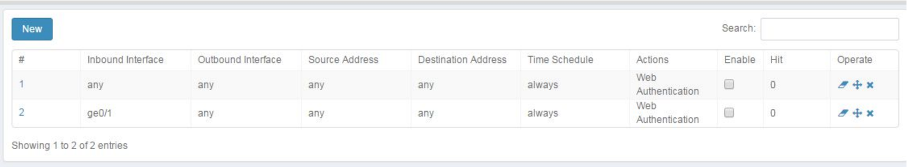
Do you confirm to delete Web Authentication Policy : 1 ?

OK Back

2. Click **OK**.

52.2.6 Moving a Web Authentication Policy

1. Choose **Policy** > **Web authentication** > **Policy**. The following page appears.



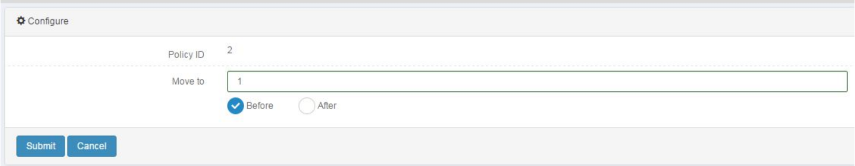
New

Search:

#	Inbound Interface	Outbound Interface	Source Address	Destination Address	Time Schedule	Actions	Enable	Hit	Operate
1	any	any	any	any	always	Web Authentication	□	0	✎ ✣ ✖
2	ge0/1	any	any	any	always	Web Authentication	□	0	✎ ✣ ✖

Showing 1 to 2 of 2 entries

2. Click ✣ next to the web authentication policy you want to move.



Configure

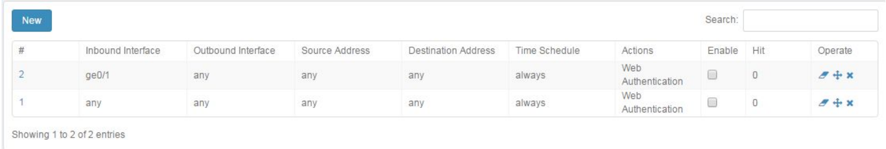
Policy ID 2

Move to 1

● Before ○ After

Submit Cancel

3. Click **Submit** after you complete the settings. A successful prompt is displayed.



New

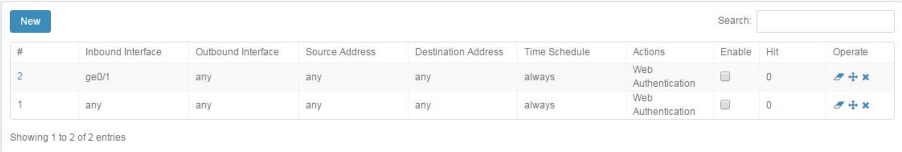
Search:

#	Inbound Interface	Outbound Interface	Source Address	Destination Address	Time Schedule	Actions	Enable	Hit	Operate
2	ge0/1	any	any	any	always	Web Authentication	□	0	✎ ✣ ✖
1	any	any	any	any	always	Web Authentication	□	0	✎ ✣ ✖

Showing 1 to 2 of 2 entries

52.2.7 Clearing the Hit Count of a Web Authentication Policy

1. Choose **Policy** > **Web authentication** > **Policy**. The following page appears.



New

Search:

#	Inbound Interface	Outbound Interface	Source Address	Destination Address	Time Schedule	Actions	Enable	Hit	Operate
2	ge0/1	any	any	any	always	Web Authentication	□	0	✎ ✥ ✖
1	any	any	any	any	always	Web Authentication	□	0	✎ ✥ ✖

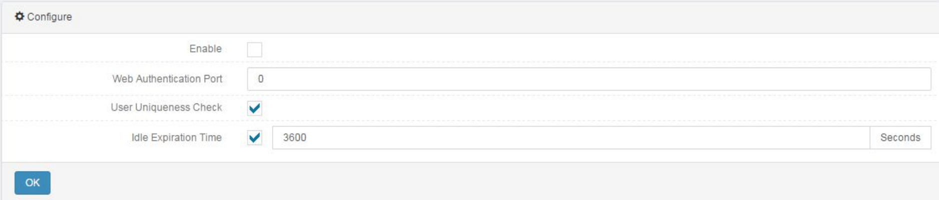
Showing 1 to 2 of 2 entries

2. Click ✎ next to the web authentication policy whose hit count you want to clear.

3. Click **OK**.

52.2.8 Modifying Web Authentication Configurations

1. Choose **Policy** > **Web authentication** > **Configuration**. The following page appears.



⚙ Configure

Enable	□
Web Authentication Port	0
User Uniqueness Check	☑
Idle Expiration Time	☑ 3600 Seconds

OK

Parameter description:

Enable: Check this box to enable the portal authentication page. The page is disabled by default.

Web authentication port: Listening port of the authentication service. The default value is **0**.

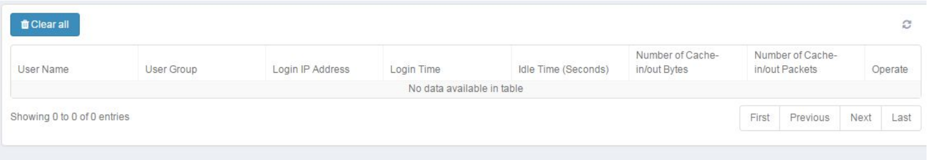
User uniqueness check: Check this box to prevent multiple users from logging in to the same account at the same time.

Idle timeout period: A user is forced offline if the user generates no traffic during this period. The default value is 3600s.

2. Click **OK**.

52.2.9 Clearing All Online Users

1. Choose **Policy** > **Web authentication** > **Online information**. The following page appears.



User Name	User Group	Login IP Address	Login Time	Idle Time (Seconds)	Number of Cache-in/out Bytes	Number of Cache-in/out Packets	Operate
No data available in table							

Showing 0 to 0 of 0 entries

2. Click Clear all to clear all online users.

3. Click ↻ to refresh the page.

52.3 Configuration Example

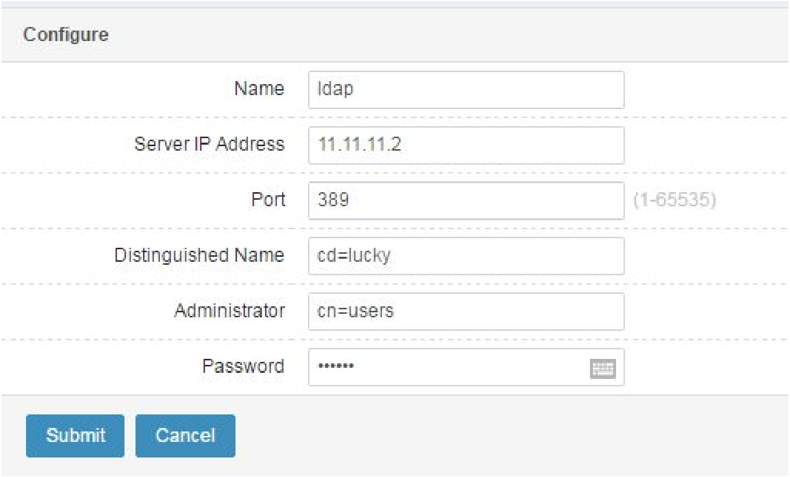
52.3.1 Configuring LDAP Authentication for Employees Accessing the Internet

Description: Configure mandatory authentication on an LDAP server for all the employees who access the Internet through a firewall, and configure a corresponding authentication policy. The external network port is ge1/3, and the LDAP server address is 11.11.11.2/24.

Procedure:

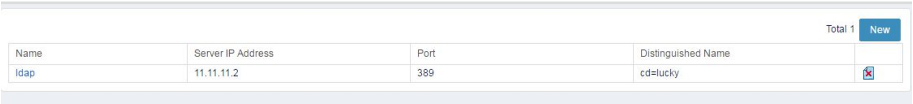
1. Configure an LDAP server.

Choose **Object** > **Authentication server** > **LDAP** to configure an LDAP server.



Configure

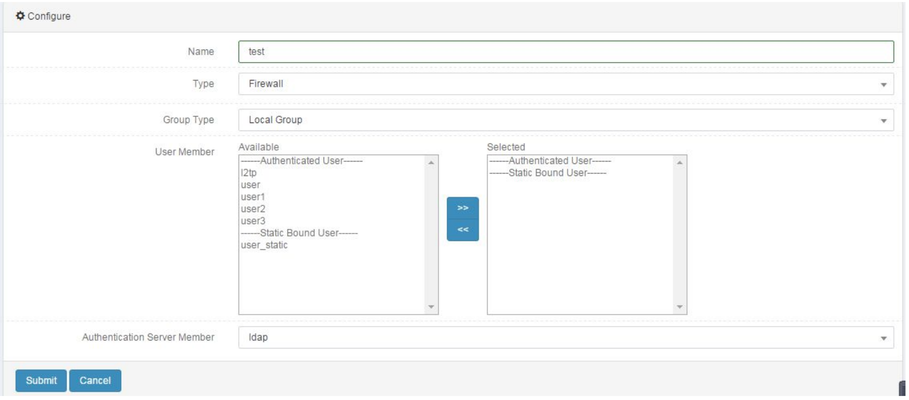
Name	ldap
Server IP Address	11.11.11.2
Port	389 (1-65535)
Distinguished Name	cd=lucky
Administrator	cn=users
Password	••••••



Name	Server IP Address	Port	Distinguished Name	
ldap	11.11.11.2	389	cd=lucky	☒

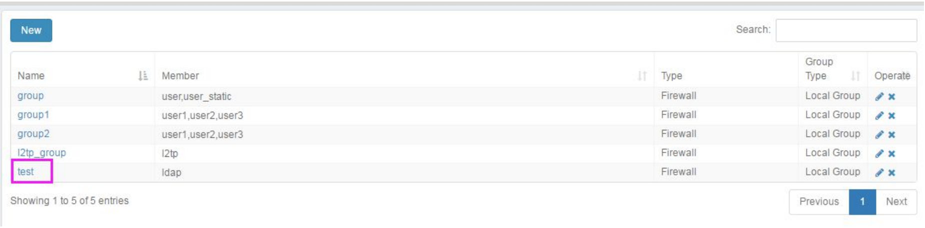
2. Configure a user group and reference the LDAP server.

Choose **Object** > **User object** > **User group** to add a user group named **test**.



Configure

Name	test
Type	Firewall
Group Type	Local Group
User Member	Available: ------Authenticated User------ l2tp user user1 user2 user3 ------Static Bound User------ user_static Selected: ------Authenticated User------ ------Static Bound User------
Authentication Server Member	ldap

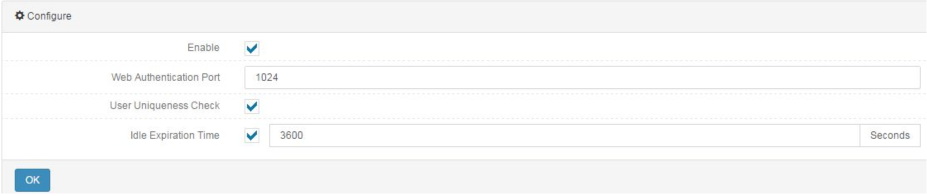


Name	Member	Type	Group Type	Operate
group	user,user_static	Firewall	Local Group	✎ ✖
group1	user1,user2,user3	Firewall	Local Group	✎ ✖
group2	user1,user2,user3	Firewall	Local Group	✎ ✖
l2tp_group	l2tp	Firewall	Local Group	✎ ✖
test	ldap	Firewall	Local Group	✎ ✖

Showing 1 to 5 of 5 entries

3. Enable web authentication.

Choose **Policy** > **Web authentication** > **Configuration** to enable web authentication.



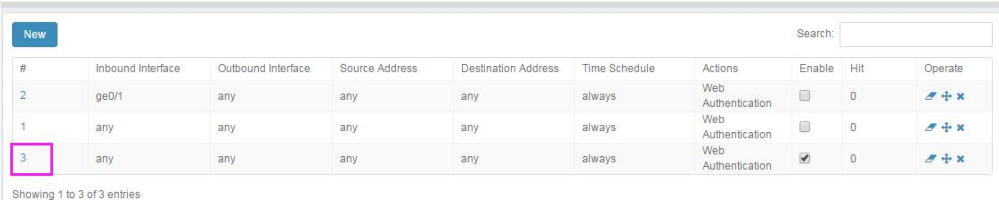
Enable	☑
Web Authentication Port	1024
User Uniqueness Check	☑
Idle Expiration Time	☑ 3600 Seconds

> Notice
>
> After user uniqueness check is enabled, the system prevents multiple users from logging in to the same account at the same time. A user name maps one IP address.

4. Configure a web authentication policy.

Choose **Policy** > **Web authentication** > **Policy** to configure a web authentication policy.

5. Click **Enable**.



#	Inbound Interface	Outbound Interface	Source Address	Destination Address	Time Schedule	Actions	Enable	Hit	Operate
2	ge0/1	any	any	any	always	Web Authentication	☐	0	✎ ✥ ✖
1	any	any	any	any	always	Web Authentication	☐	0	✎ ✥ ✖
3	any	any	any	any	always	Web Authentication	☑	0	✎ ✥ ✖

Showing 1 to 3 of 3 entries

52.4 Troubleshooting

52.4.1 An Authentication User Fails to Perform Authentication

Symptom	An authentication user fails to perform authentication.
Analysis	1. The password is incorrect. 2. The user is disabled. 3. The user name of the authentication user is not saved locally, and the corresponding user group is not added to the RADIUS server. 4. The RADIUS or LDAP server is incorrectly configured. For example, the shared key or IP address is incorrect. 5. The RADIUS or LDAP server cannot be connected. For example, they cannot be pinged. 6. The user does not exist on the RADIUS or LDAP server.
Solution	1. Check the user name and password, and enter them correctly. 2. Enable the user. 3. Add the user group to the RADIUS and LDAP servers. 4. Modify the configurations of the RADIUS and LDAP servers. 5. Ensure that the firewall USG communicates with the RADIUS and LDAP servers normally and the ping test is successful. 6. Add the user to the RADIUS and LDAP servers.

53 Address Object

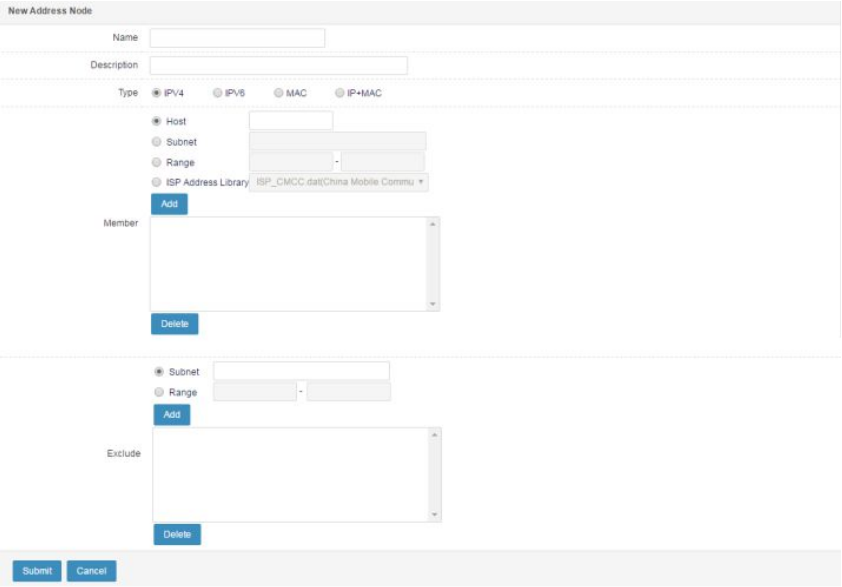
53.1 Overview

RAVEN 5000 firewalls introduce address objects to facilitate configuration and management. Address objects are classified into address nodes and address groups. An address group is a set of address nodes. You can reference address objects to define the effective conditions of configurations when configuring firewall policies, NAT rules, routing policies, and other features.

53.2 Configuring an Address Node

Address nodes are classified into the following types: IPv4, IPv6, MAC address, and IP+MAC address.

1. Choose **Object** > **Address object** > **Address node** and click **New**. The following page appears.



Name: Name of the new address node, no more than 63 characters.

Description: Description about the address node, no more than 127 characters.

Type: Type of the address node. The options are **IPv4**, **IPv6**, **MAC address**, and **IP+MAC address**.

Address node:

Members: Members of the address node.

An IPv4 address node includes:

- **Host**: IPv4 address of a host.
- **Subnet**: IPv4 network segment address.
- **Range**: Range of an IPv4 address pool.
- ISP address library in the IPv4 format.

An IPv6 address node includes:

- **Host**: IPv6 address of a host.
- **Subnet**: IPv6 network address.

- **Range**: IPv6 address range.

An address node of the MAC address type contains MAC addresses.

An address node of the IP+MAC address type contains IPv4 addresses and MAC addresses.

Exclude: Members excluded from the address node.

IPv4 address node:

- **Subnet**: IPv4 network segment address.
- **Range**: Range of an IPv4 address pool.

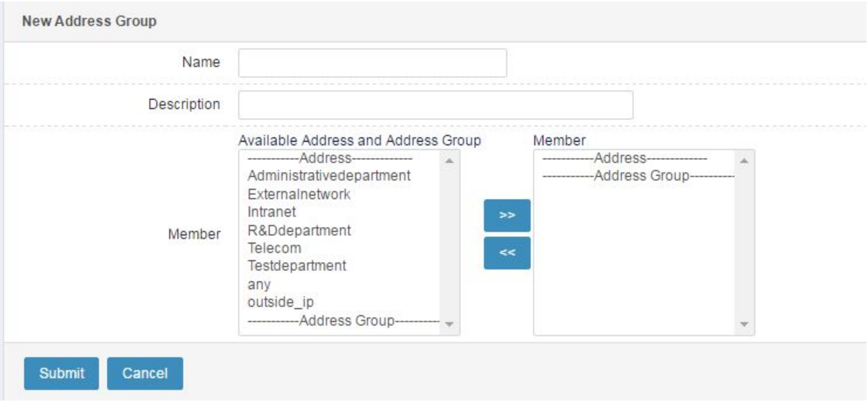
2. Click **Submit**.

53.3 Configuring an Address Group

An address group is a set of address nodes. You can configure an address group to manage address-related rules with ease.

Procedure:

Choose **Object** > **Address object** > **Address group** and click **New**. The following page appears.


New Address Group
Name
Description
Member
Available Address and Address Group
-----------Address------------
Administrativedepartment
Externalnetwork
Intranet
R&Ddepartment
Telecom
Testdepartment
any
outside_ip
-----------Address Group---------
Member
-----------Address------------
-----------Address Group---------
>>
<<
Submit
Cancel

Name: Name of the new address group, no more than 63 characters.

Description: Description about the address group, no more than 127 characters.

Available addresses and address groups: Existing address nodes and address groups.

Members: Members of the address group.

Click **Submit** after you complete the settings.

53.4 Configuration Examples

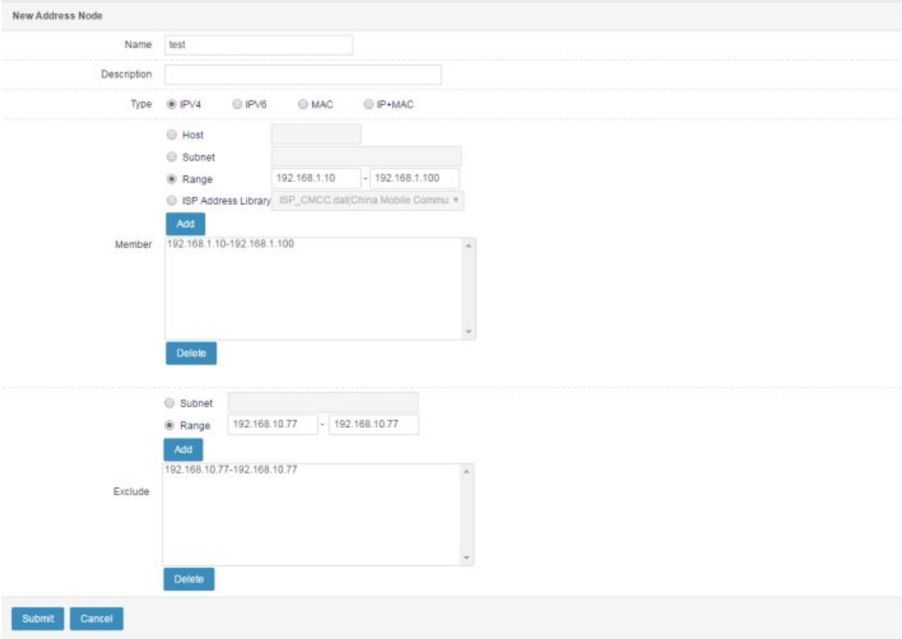
53.4.1 Example 1: Adding an IPv4 Address Node

Description:

Add an IPv4 address object to include some internal network segments while excluding some hosts or network segments.

Procedure:

1. Choose **Object** > **Address object** > **Address node** and click **New**. The following page appears.



New Address Node

Name: test

Description:

Type: ● IPV4 ○ IPV6 ○ MAC ○ IP+MAC

○ Host

○ Subnet

● Range 192.168.1.10 - 192.168.1.100

○ ISP Address Library ISP_CMCC.dat(China Mobile Commu ▾

Add

Member: 192.168.1.10-192.168.1.100

Delete

○ Subnet

● Range 192.168.10.77 - 192.168.10.77

Add

Exclude: 192.168.10.77-192.168.10.77

Delete

Submit Cancel

2. Set parameters.
3. Click **Submit**.

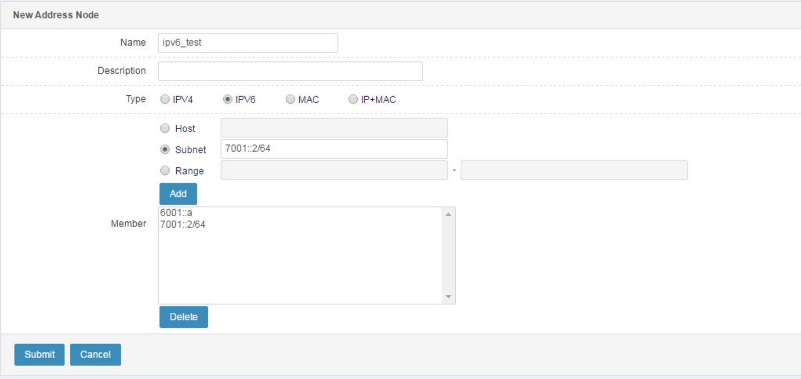
53.4.2 Example 2: Adding an IPv6 Address Node

Description:

Add an IPv6 address object to include the subnet where an intranet is located.

Procedure:

1. Choose **Object** > **Address object** > **Address node** and click **New**. The following page appears.



New Address Node

Name	ipv6_test
Description	
Type	○ IPV4 ● IPV6 ○ MAC ○ IP+MAC
	○ Host
	● Subnet 7001::2/64
	○ Range -
Member	6001::a 7001::2/64

2. Set parameters.
3. Click **Submit**.

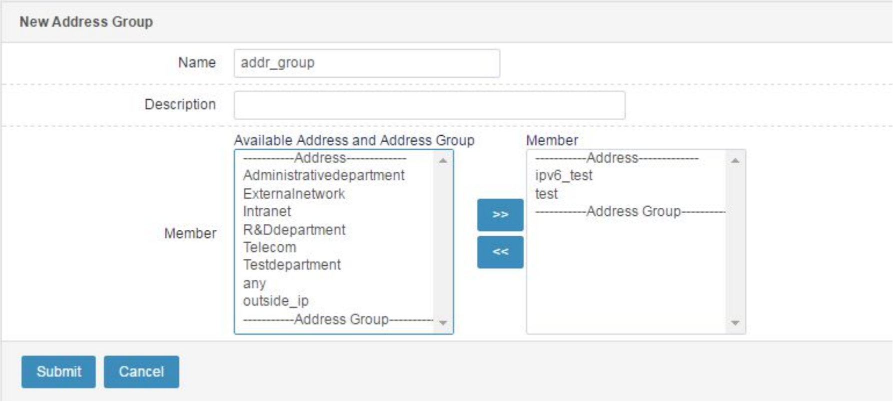
53.4.3 Example 3: Adding an Address Object Group

Description:

Add address objects to an address object group.

Procedure:

1. Choose **Object** > **Address object** > **Address group** and click **New**. The following page appears.



New Address Group

Name: addr_group

Description:

Member

Available Address and Address Group
-----------Address-------------
Administrativedepartment
Externalnetwork
Intranet
R&Ddepartment
Telecom
Testdepartment
any
outside_ip
-----------Address Group---------

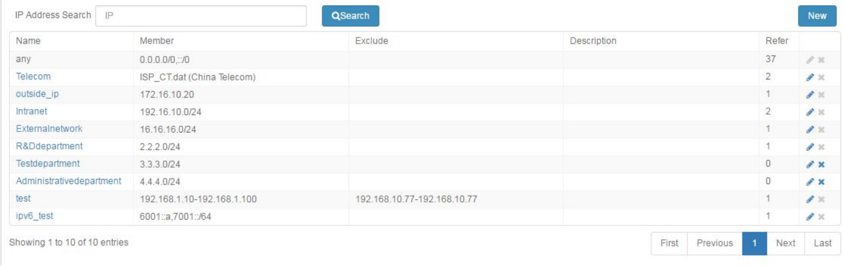
Member
-----------Address-------------
ipv6_test
test
-----------Address Group---------

2. Select address nodes in **Available addresses and address groups** and click >> to add them to **Members**.
3. Click **Submit**.

53.5 Monitoring and Maintenance

53.5.1 Displaying Address Nodes

1. Choose **Object** > **Address object** > **Address node**. The following page appears.

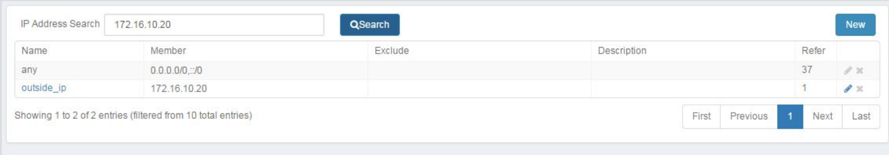


IP Address Search: IP

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			37
Telecom	ISP_CT.dat (China Telecom)			2
outside_ip	172.16.10.20			1
Intranet	192.16.10.0/24			2
Externalnetwork	16.16.16.0/24			1
R&Ddepartment	2.2.2.0/24			1
Testdepartment	3.3.3.0/24			0
Administrativedepartment	4.4.4.0/24			0
test	192.168.1.10-192.168.1.100	192.168.10.77-192.168.10.77		1
ipv6_test	6001::a,7001::/64			1

Showing 1 to 10 of 10 entries

2. Enter an IP address in the **Search for IP address** text box and click **Search** to display specified address nodes, as shown in the following figure.



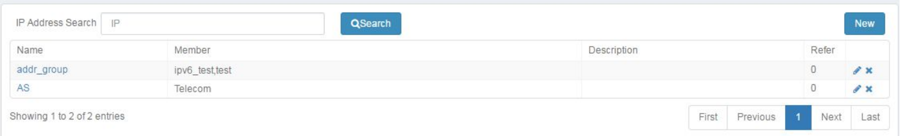
IP Address Search: 172.16.10.20

Name	Member	Exclude	Description	Refer
any	0.0.0.0/0,::/0			37
outside_ip	172.16.10.20			1

Showing 1 to 2 of 2 entries (filtered from 10 total entries)

53.5.2 Displaying Address Groups

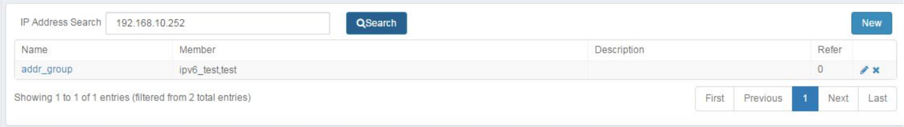
1. Choose **Object** > **Address object** > **Address group**. The following page appears.



Name	Member	Description	Refer
addr_group	ipv6_test,test		0
AS	Telecom		0

Showing 1 to 2 of 2 entries

2. Enter an IP address in the **Search for IP address** text box and click **Search** to display specified address groups, as shown in the following figure.



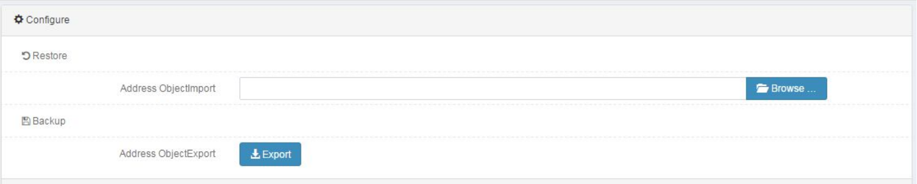
IP Address Search: 192.168.10.252

Name	Member	Description	Refer
addr_group	ipv6_test,test		0

Showing 1 to 1 of 1 entries (filtered from 2 total entries)

53.5.3 Backing Up and Restoring Address Objects

Choose **Object** > **Address object** > **Backup and restoration**. The following page appears.



Parameter description:

Click **Restore** to import the text file that contains address object configurations. The system reads and delivers the configurations. The following address object formats are supported:

- **IPv4 address object:**

```
address NAME
host-address A.B.C.D
        net-address A.B.C.D/M
        range-address A.B.C.D E.F.G.H isp-
        address NAME
net-address-exp A.B.C.D/M
range-address-exp A.B.C.D E.F.G.H
```

- **IPv6 address object**

```
address-v6 NAME host-
    v6 X:X::X:X
    net-v6 X:X::X:X/M
    range-v6 X:X::X:X X:X::X:X
```

- **MAC address object**

```
address-mac NAME
mac-host FF-FF-FF-FF-FF-FF
```

- **IP+MAC address object**

```
address-ip-mac NAME
bind A.B.C.D FF-FF-FF-FF-FF-FF
```

- **Address group**

```
address-group NAME
address-object NAME
```

Click **Backup** to export address object configurations to a text file.

53.6 Troubleshooting

53.6.1 Failed to Submit Settings

Symptom	The settings fail to be submitted after the **Submit** button is clicked.
Analysis	Check whether the address is valid.
Solution	Enter a valid address.

54 ISP Address

54.1 Overview

An ISP address library is a set of public addresses provided by an operator and can be referenced by address objects. Address objects are referenced by PBR and used for load balancing among outbound links. The destination address of outgoing traffic is matched with the ISP address library to divert the traffic to the most suitable link.

Notice

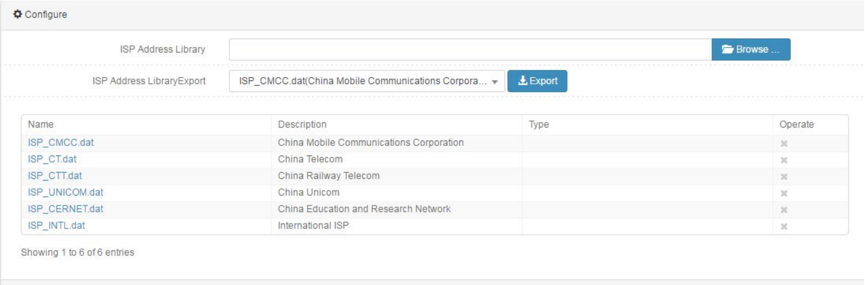
1. When an ISP address library is used by load balancing among outbound links, do not apply the address library to source address objects.
2. An ISP address library can only be in the format *A.B.C.D-A.B.C.D*. Other formats will result in a loading error.

54.2 Configuration

ISP address libraries are classified into predefined and custom libraries. Predefined libraries come with the system and cannot be deleted regardless of whether they are referenced by address objects. Custom libraries are uploaded by users and can be deleted if not referenced by address objects.

54.2.1 Configuring an ISP Address Library

Choose **Object** > **ISP address library**.



ISP Address LibraryExport: ISP_CMCC.dat(China Mobile Communications Corpora...

Name	Description	Type	Operate
ISP_CMCC.dat	China Mobile Communications Corporation		✕
ISP_CT.dat	China Telecom		✕
ISP_CTT.dat	China Railway Telecom		✕
ISP_UNICOM.dat	China Unicom		✕
ISP_CERNET.dat	China Education and Research Network		✕
ISP_INTL.dat	International ISP		✕

Showing 1 to 6 of 6 entries

Name: Name of an ISP address library. Chinese characters are not allowed.

Description: Description about the ISP address library, no more than 127 characters.

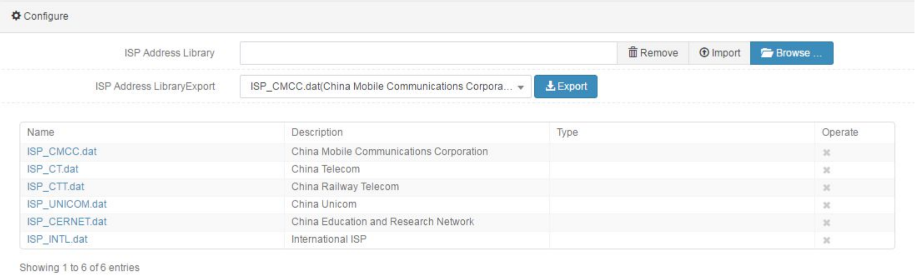
Type: Type of the ISP address library.

Import ISP address library: Import an ISP address library.

Export ISP address library: Export an ISP address library.

54.2.2 Importing an ISP Address Library

Choose **Object** > **ISP address library.** The following page appears.



ISP Address Library:

ISP Address LibraryExport: ISP_CMCC.dat(China Mobile Communications Corpora...

Name	Description	Type	Operate
ISP_CMCC.dat	China Mobile Communications Corporation		✕
ISP_CT.dat	China Telecom		✕
ISP_CTT.dat	China Railway Telecom		✕
ISP_UNICOM.dat	China Unicom		✕
ISP_CERNET.dat	China Education and Research Network		✕
ISP_INTL.dat	International ISP		✕

Showing 1 to 6 of 6 entries

Browser: Select a valid ISP address library file. If the file name does not start with **ISP**, it is added with **ISP_** after the file is uploaded.

Import: Click this button to upload the file to the system's storage device.

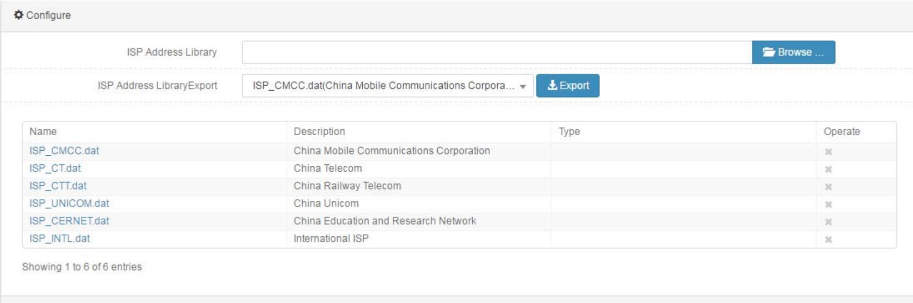
Remove: Click this button to remove the selected file and select another file.

Notice

1. The ISP address library file to be imported cannot exceed 10 MB in size. If the size limit is exceeded, import will fail.
2. After an ISP address library is imported, it will be loaded only when it is referenced by an address object. If an ISP address library has more than 10,000 lines, only the first 10,000 lines are loaded, and the remaining lines are not loaded and do not take effect.

54.2.3 Exporting an ISP Address Library

Choose **Object** > **ISP address library.** The following page appears.



Configure

ISP Address Library: [ ] Browse ...

ISP Address LibraryExport: ISP_CMCC.dat(China Mobile Communications Corpora... Export

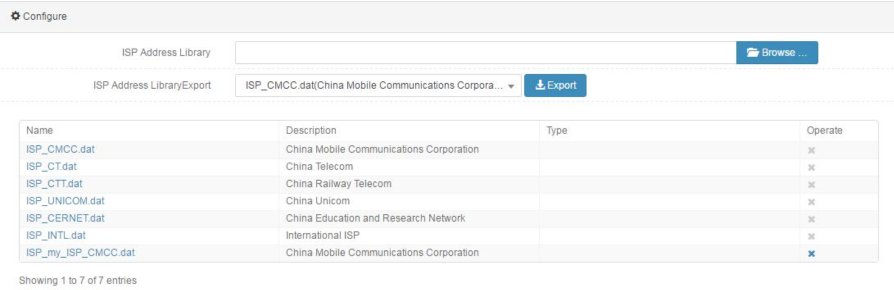
Name	Description	Type	Operate
ISP_CMCC.dat	China Mobile Communications Corporation		✖
ISP_CT.dat	China Telecom		✖
ISP_CTT.dat	China Railway Telecom		✖
ISP_UNICOM.dat	China Unicom		✖
ISP_CERNET.dat	China Education and Research Network		✖
ISP_INTL.dat	International ISP		✖

Showing 1 to 6 of 6 entries

Export: Click this button to select the ISP address library file you want to export to the local device.

54.2.4 Deleting an ISP Address Library

Choose **Object** > **ISP address library.** The following page appears.



Configure

ISP Address Library: [ ] Browse ...

ISP Address LibraryExport: ISP_CMCC.dat(China Mobile Communications Corpora... Export

Name	Description	Type	Operate
ISP_CMCC.dat	China Mobile Communications Corporation		✖
ISP_CT.dat	China Telecom		✖
ISP_CTT.dat	China Railway Telecom		✖
ISP_UNICOM.dat	China Unicom		✖
ISP_CERNET.dat	China Education and Research Network		✖
ISP_INTL.dat	International ISP		✖
ISP_my_ISP_CMCC.dat	China Mobile Communications Corporation		✖

Showing 1 to 7 of 7 entries

Click ✖ next to the ISP address library you want to delete.

⚠ Notice	If the **Delete** button is grayed out, the ISP address library is referenced by an address object or is a predefined library, so it cannot be deleted.

54.3 Troubleshooting

54.3.1 The Loaded ISP Addresses Are Incomplete

Symptom	An ISP address library referenced by an address object is parsed and loaded to the memory. However, some addresses in the library are missing.

Solution	The ISP address library has more than 10,000 lines, and the lines exceeding the limit are not parsed and loaded. In this case, split the ISP address library file.

55 Service Object

55.1 Overview

RAVEN 5000 firewalls introduce service objects to facilitate configuration and management. You can reference service objects to define the effective conditions of configurations when configuring firewall policies, NAT rules, routing policies, and other features.

Service objects are classified into predefined services, custom services, and service groups.

A predefined service is a service that the system adds in advance and cannot be modified or deleted manually.

A custom service must be added manually.

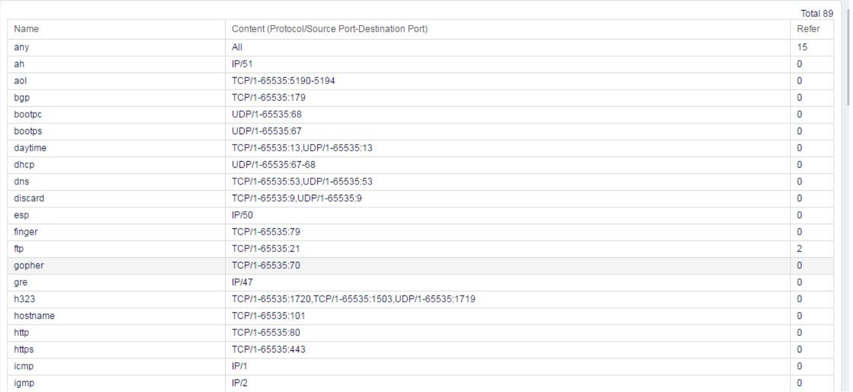
A service group is a set of services.

55.2 Configuration

55.2.1 Predefined Service

Choose **Object** > **Service object** > **Predefined service** to display predefined services.

The following page lists some predefined services.



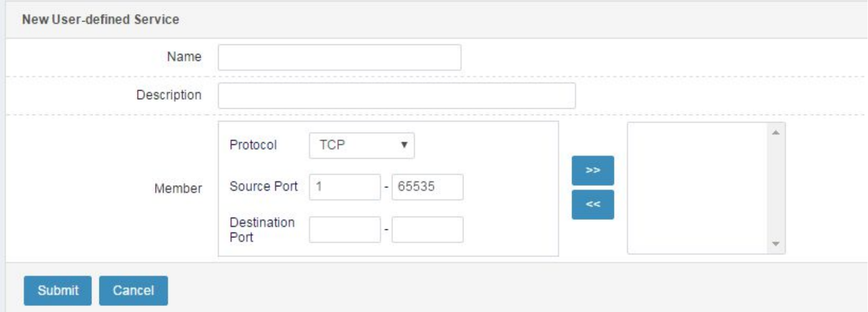
Total 89

Name	Content (Protocol/Source Port-Destination Port)	Refer
any	All	15
ah	IP/51	0
aol	TCP/1-65535:5190-5194	0
bgp	TCP/1-65535:179	0
bootpc	UDP/1-65535:68	0
bootps	UDP/1-65535:67	0
daytime	TCP/1-65535:13,UDP/1-65535:13	0
dhcp	UDP/1-65535:67-68	0
dns	TCP/1-65535:53,UDP/1-65535:53	0
discard	TCP/1-65535:9,UDP/1-65535:9	0
esp	IP/50	0
finger	TCP/1-65535:79	0
ftp	TCP/1-65535:21	2
gopher	TCP/1-65535:70	0
gre	IP/47	0
h323	TCP/1-65535:1720,TCP/1-65535:1503,UDP/1-65535:1719	0
hostname	TCP/1-65535:101	0
http	TCP/1-65535:80	0
https	TCP/1-65535:443	0
icmp	IP/1	0
igmp	IP/2	0

55.2.2 Configuring a Custom Service

Procedure:

Choose **Object** > **Service object** > **User-defined service** and click **New**.
The following page appears.



New User-defined Service

Name

Description

Member

Protocol: TCP

Source Port: 1 - 65535

Destination Port: -

Name: Name of the new custom service.

Description: Description about the custom service.

Protocol: Custom service protocol. The options are **TCP**, **UDP**, **ICMP**, and **IP**.

Source port: Source port number of the protocol.

Destination port: Destination port number of the protocol.

Click **Submit** after you complete the settings.

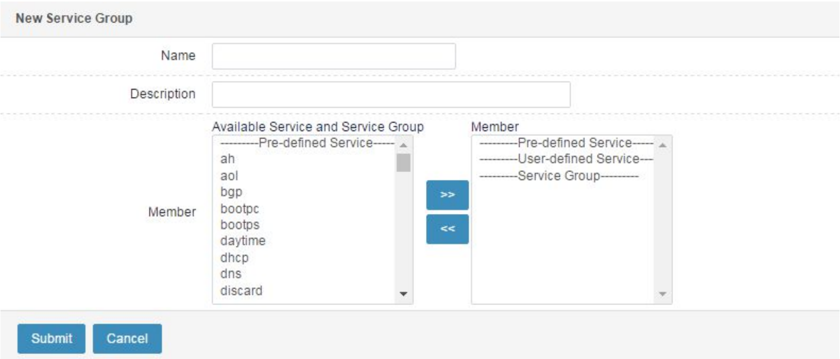
Note

If you want to specify only one port for the protocol, enter the same port number on both sides of **-**.

55.2.3 Configuring a Service Group

Procedure:

Choose **Object** > **Service object** > **Service group** and click **New**. The following page appears.


New Service Group

Name

Description

Member

Available Service and Service Group

---------Pre-defined Service-----
ah
aol
bgp
bootpc
bootps
daytime
dhcp
dns
discard

Member

---------Pre-defined Service-----
---------User-defined Service---
---------Service Group---------

Name: Name of the new service group.

Description: Description about the service group.

Available services and service groups: Select predefined services and custom services and add them to the service group.

Click **Submit** after you complete the settings.

Note

A service group can be included in multiple service groups, but a service group inclusion can have only one nesting.

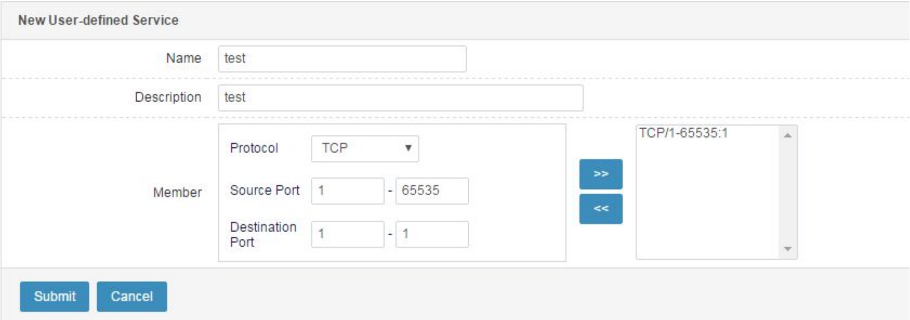
55.3 Configuration Examples

55.3.1 Example 1: Adding a Custom Service

Description:

Add a custom TCP service.

1. Choose **Object** > **Service object** > **Custom service** and click **New**. The following page appears.


New User-defined Service

Name: test

Description: test

Member

Protocol: TCP

Source Port: 1 - 65535

Destination Port: 1 - 1

TCP/1-65535:1

2. Click >> to add members.

3. Click **Submit**.

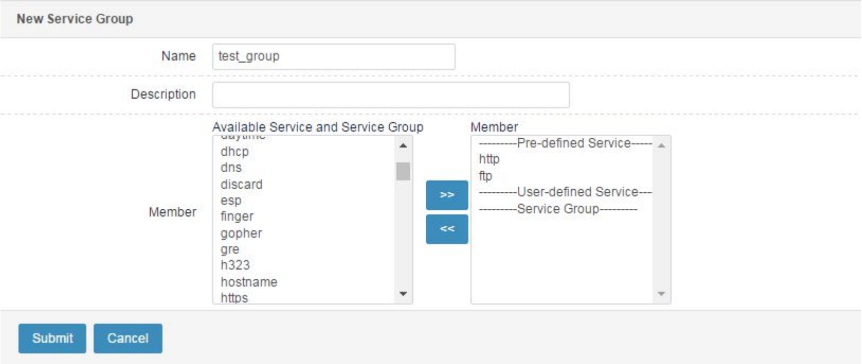
55.3.2 Example 2: Adding a Service Group

Description:

A service group is a set of services. Configure a service group to facilitate management.

Procedure:

1. Choose **Object** > **Service object** > **Service group** and click **New**. The following page appears.



New Service Group

Name: test_group

Description:

Member:

Available Service and Service Group: daytime, dhcp, dns, discard, esp, finger, gopher, gre, h323, hostname, https

Member: ---------Pre-defined Service----- http ftp ---------User-defined Service--- ---------Service Group---------

2. Add FTP, HTTP, and the custom email service to the service group.

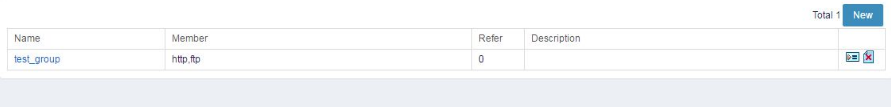
3. Click >> to add members.

4. Click **Submit**.

55.4 Monitoring and Maintenance

55.4.1 Displaying Service Groups

Choose **Object** > **Service object** > **Service group**. The following page appears.



Total 1

Name	Member	Refer	Description
test_group	http,ftp	0	

55.5 Troubleshooting

55.5.1 Failed to Submit Settings

Symptom	The settings fail to be submitted after the **Submit** button is clicked.
Analysis	Check whether the port number is correct.

56 Application object

56.1 Overview

RAVEN 5000 firewalls introduce application objects to facilitate configuration and management. During policy configuration, you can reference application objects to group applications, which facilitates control.

Application objects are classified into predefined applications, custom applications, and application groups.

- A predefined application is a specific user application, such as download software and instant communication software. Currently there are more than 1000 applications under 20 categories. The application feature database is updated. Manual configuration is not required.
- A custom application must be configured manually.
- An application group must be configured manually, and it can reference predefined and custom applications.

In actual use, application objects are referenced by policies.

Application objects can be used with firewall policies, application control policies, flow control policies, and session control policies to block and rate-limit the application traffic.

Application objects can also be used with routing policies to divert the application traffic to a specified link. Application traffic diversion is very practical in actual network environments. For example, a network environment has two links, one of which is of high quality. Measures are usually taken to ensure bandwidth for the high-quality link and prevent bandwidth overuse by applications with heavy traffic consumption, such as P2P download.

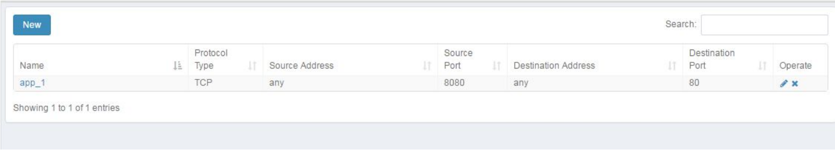
56.2 Configuration

56.2.1 Configuring a Custom Application

Procedure:

1. Choose **Object** > **Application object** > **User-defined application**.

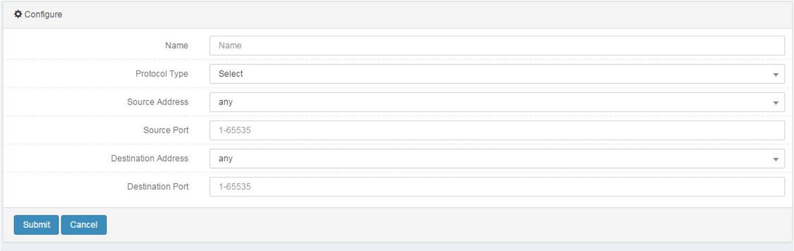
A page appears to display existing custom applications.



Name	Protocol Type	Source Address	Source Port	Destination Address	Destination Port	Operate
app_1	TCP	any	8080	any	80	✎ ✖

Showing 1 to 1 of 1 entries

2. Click **New** to configure a custom application.



Name	Name
Protocol Type	Select
Source Address	any
Source Port	1-65535
Destination Address	any
Destination Port	1-65535

Name: Name of the new custom application, no more than 63 characters.

Protocol type: The options are **TCP** and **UDP**.

Source address: Source address of the application. You can reference a predefined address object or address object group. The option **any** indicates any address.

Source port: Source port of the application. The value ranges from **1** to **65535**.

Destination address: Destination address of the application. You can reference a predefined address object or address object group. The option **any** indicates any address.

Destination port: Destination port of the application. The value ranges from **1** to **65535**.

3. Click **Submit**.

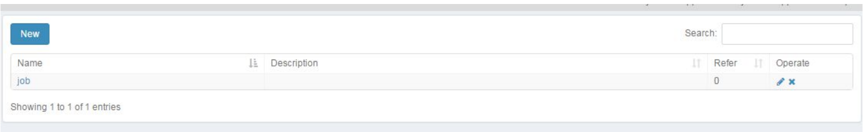
⚠ Notice	Custom objects are of the highest priority. The parameters must be set accurately; otherwise, other traffic may be identified as custom applications, which affects the matching of other application control policies.

56.2.2 Configuring an Application Group

Procedure:

1. Choose **Object** > **Application object** > **Application group**.

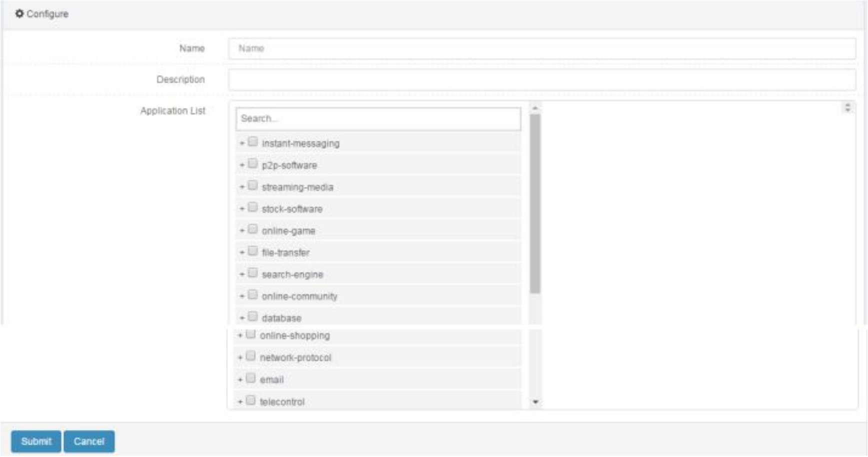
A page appears to display existing application groups.



Name	Description	Refer	Operate
job		0	

Showing 1 to 1 of 1 entries

2. Click **New** to configure an application group.



Name: Name

Description:

Application List:

Search...

- □ instant-messaging
- □ p2p-software
- □ streaming-media
- □ stock-software
- □ online-game
- □ file-transfer
- □ search-engine
- □ online-community
- □ database
- □ online-shopping
- □ network-protocol
- □ email
- □ telecontrol

Name: Name of the new application group, no more than 63 characters.

Description: Description about the application group, no more than 127 characters.

Application list: All the supported applications. See the preceding figure.

Select desired applications and click **Submit**.

Note

Only existing custom applications are listed.

56.3 Configuration Examples

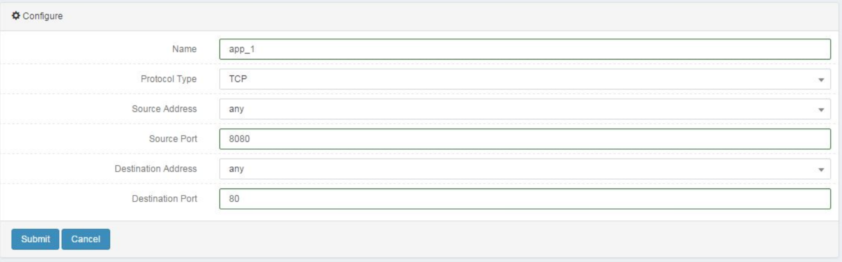
56.3.1 Example 1: Adding a Custom Application

Description:

Add a custom application to be referenced by policies.

Procedure:

1. Choose **Object** > **Application object** > **User-defined application** and click **New**. The following page appears.



Configure

Name: app_1

Protocol Type: TCP

Source Address: any

Source Port: 8080

Destination Address: any

Destination Port: 80

2. Set parameters.
3. Click **Submit**.

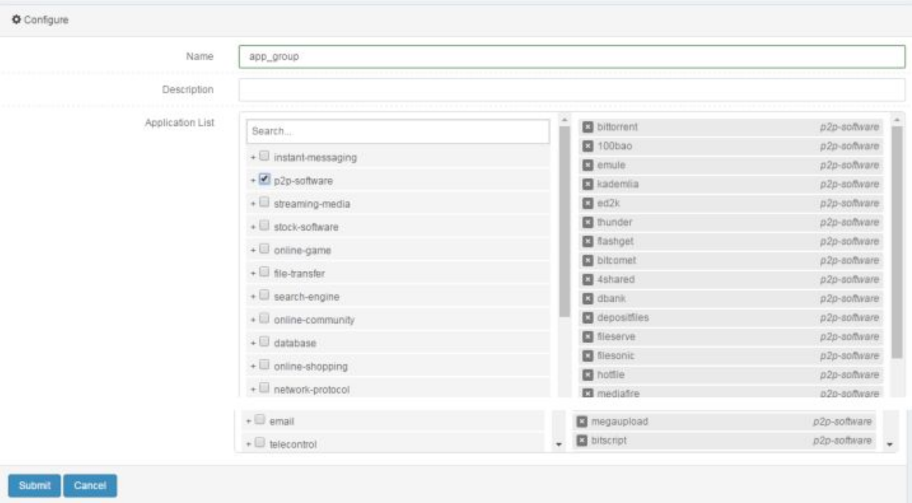
56.3.2 Example 2: Adding an Application Group

Description:

Configure an application group and reference the online video category so that the policies which reference the application group take effect for video traffic.

Procedure:

1. Choose **Object** > **Application object** > **Application group** and click **New**. The following page appears.



Configure

Name: app_group

Description:

Application List

Search...

+ □ instant-messaging
+ ☑ p2p-software
+ □ streaming-media
+ □ stock-software
+ □ online-game
+ □ file-transfer
+ □ search-engine
+ □ online-community
+ □ database
+ □ online-shopping
+ □ network-protocol
+ □ email
+ □ telecontrol

☒ bittorrent	p2p-software
☒ 100bao	p2p-software
☒ emule	p2p-software
☒ kademlia	p2p-software
☒ ed2k	p2p-software
☒ thunder	p2p-software
☒ flashget	p2p-software
☒ bitcomet	p2p-software
☒ 4shared	p2p-software
☒ dbank	p2p-software
☒ depositfiles	p2p-software
☒ fileserve	p2p-software
☒ filesonic	p2p-software
☒ hotfile	p2p-software
☒ mediafire	p2p-software
☒ megaupload	p2p-software
☒ bitscript	p2p-software

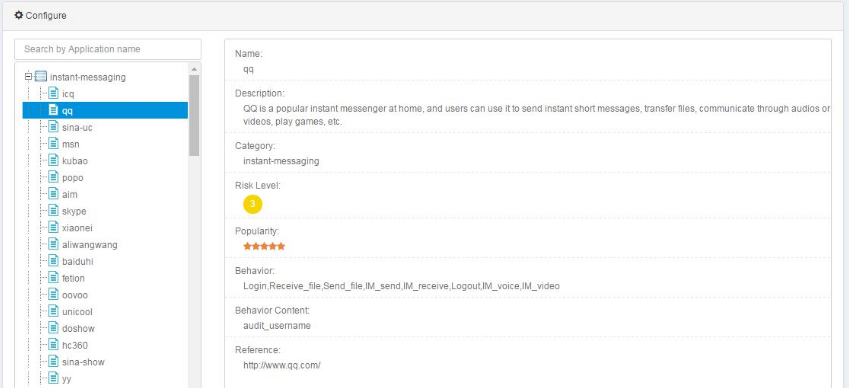
2. Specify the group name and description, and select the online video category.

3. Click **Submit**.

56.4 Monitoring and Maintenance

56.4.1 Displaying Predefined Applications

Choose **Object** > **Application object** > **Predefined application**. Select applications from the left-side tree directory, as shown in the following figure.



Name:
qq

Description:
QQ is a popular instant messenger at home, and users can use it to send instant short messages, transfer files, communicate through audios or videos, play games, etc.

Category:
instant-messaging

Risk Level:
3

Popularity:
★★★★★

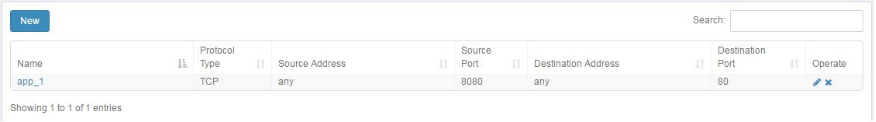
Behavior:
Login,Receive_file,Send_file,IM_send,IM_receive,Logout,IM_voice,IM_video

Behavior Content:
audit_username

Reference:
http://www.qq.com/

56.4.2 Displaying Custom Applications

Choose **Object** > **Application object** >User-defined **application**. The following page appears.

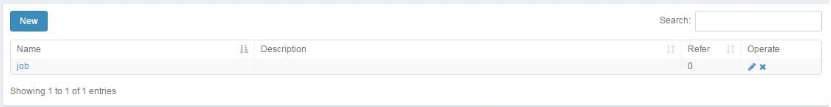


Name	Protocol Type	Source Address	Source Port	Destination Address	Destination Port	Operate
app_1	TCP	any	8080	any	80	✎ ✖

Showing 1 to 1 of 1 entries

56.4.3 Displaying Application Groups

Choose **Object** > **Application object** > **Application group**. The following page appears.



Name	Description	Refer	Operate
job		0	✎ ✖

Showing 1 to 1 of 1 entries

57 User Object

57.1 Overview

RAVEN 5000 firewalls introduce user objects to facilitate configuration and management. You can reference user objects to define the effective conditions of configurations when configuring web authentication, L2TP, and other features.

User objects are classified into users and user groups.

Users are classified into authentication users and statically bound users. Authentication users are classified into local users, RADIUS users, and LDAP users.

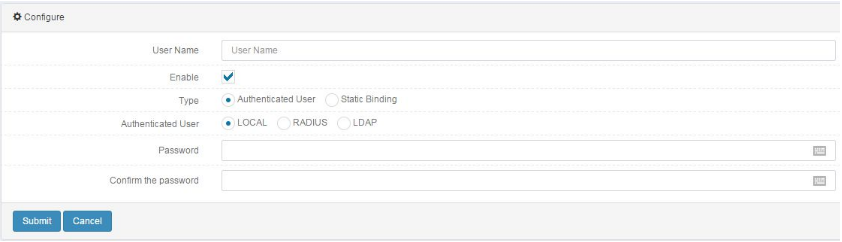
A user group is a set of users.

57.2 User Object Configuration

57.2.1 Configuring a Local Authentication User Object

Configure a local user object as follows:

Choose **Object** > **User object** > **User** and click **New**.



Configure

User Name	User Name
Enable	☑
Type	● Authenticated User ○ Static Binding
Authenticated User	● LOCAL ○ RADIUS ○ LDAP
Password	
Confirm the password	

User name: User name displayed after the user is authenticated.

Enable: Check this box to make the user name effective.

Type: The options are **Authentication user** and **Static binding**.

Authentication user: The options are **LOCAL**, **RADIUS**, and **LDAP**.

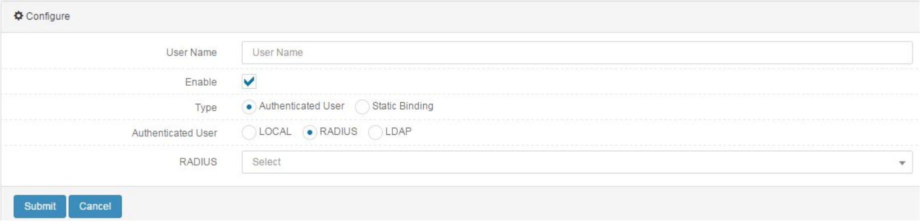
Password: Enter a password for authentication.

Confirm password: Enter the password again.

57.2.2 Configuring a RADIUS User Object

Configure a RADIUS user object as follows:

Choose **Object** > **User object** > **User** and click **New**.



Configure

User Name: User Name

Enable: ☑

Type: ● Authenticated User ○ Static Binding

Authenticated User: ○ LOCAL ● RADIUS ○ LDAP

RADIUS: Select

User name: User name on the RADIUS server.

Enable: Check this box to make the user name effective.

Type: Select **Authentication user**.

Authentication user: Select **RADIUS**.

RADIUS: RADIUS server object.

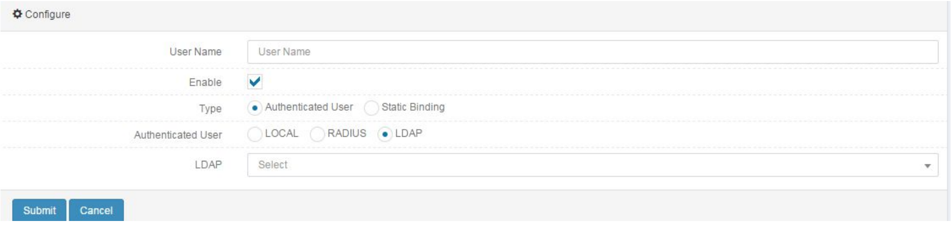
Note

When configuring a RADIUS user, ensure that a RADIUS server object exists. For how to configure a RADIUS server object, see the corresponding section.

57.2.3 Configuring an LDAP User Object

Configure an LDAP user object as follows:

Choose **Object** > **User object** > **User** and click **New**.



Configure

User Name: User Name

Enable: ☑

Type: ● Authenticated User ○ Static Binding

Authenticated User: ○ LOCAL ○ RADIUS ● LDAP

LDAP: Select

User name: User name on the LDAP server.

Enable: Check this box to make the user name effective.

Type: Select **Authentication user**.

Authentication user: Select **LDAP**.

LDAP: LDAP server object.

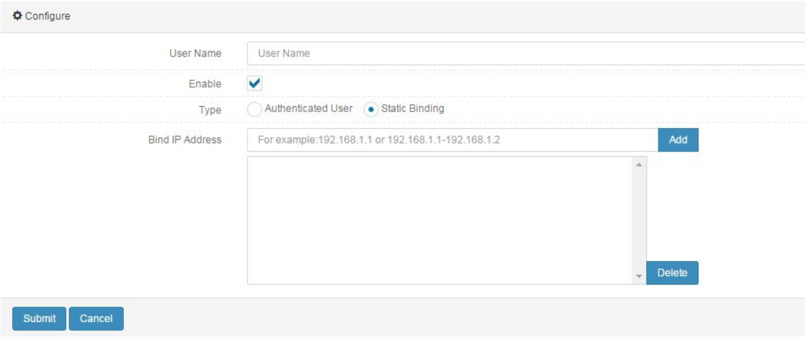
Note

When configuring an LDAP user, ensure that an LDAP server object exists. For how to configure an LDAP server object, see the corresponding section.

57.2.4 Configuring a Static User Object

Configure a static user object as follows:

Choose **Object** > **User object** > **User** and click **New**.


Configure

User Name: User Name

Enable: ☑

Type: ○ Authenticated User ● Static Binding

Bind IP Address: For example:192.168.1.1 or 192.168.1.1-192.168.1.2

User name: User name referenced by policies.

Enable: Check this box to make the user name effective.

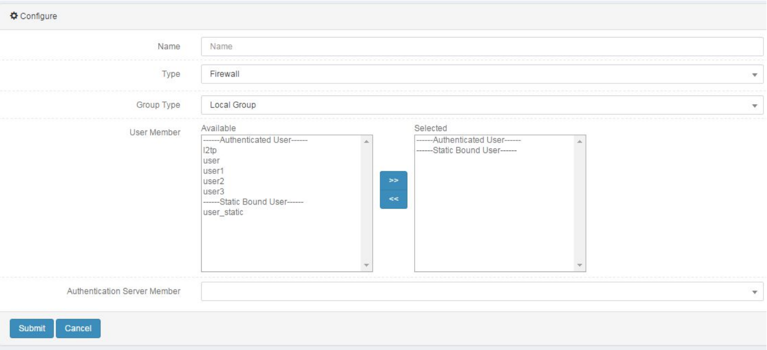
Type: Select **Statically bound**.

Bound IP address: Binding relationship between the user name and an IP address.

57.3 Configuring a User Group Object

Web authentication and L2TP configuration adopt user group objects.

Choose **Object** > **User object** > **User group** and click **New**.


Configure

Name: Name

Type: Firewall

Group Type: Local Group

User Member

Available:
------Authenticated User------
l2tp
user
user1
user2
user3
------Static Bound User------
user_static

Selected:
------Authenticated User------
------Static Bound User------

Authentication Server Member

Name: Name of a user group.

User members: User object members, including authentication users and static users.

Authentication server members: Select RADIUS or LDAP users.

58 Authentication Server Object

58.1 Overview

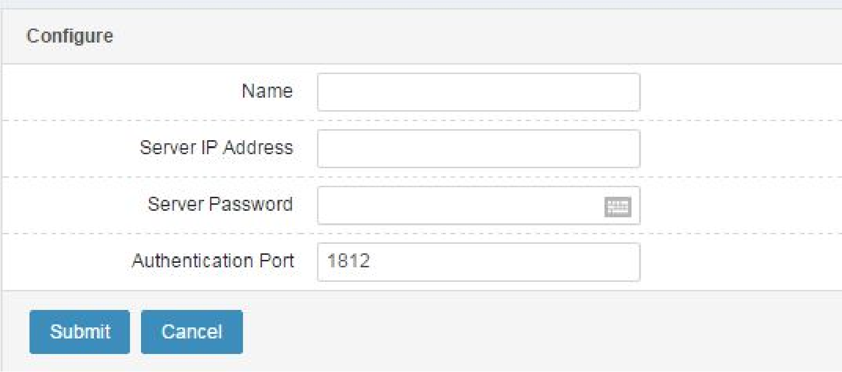
RAVEN 5000 firewalls support user authentication using the RADIUS server and LDAP server. 1. You can add a RADIUS server to allow users to perform authentication using the specified server. 2. You can add an LDAP server to allow users to perform authentication using the specified server. During web authentication and administrator authentication, you can select the configured server object to perform remote authentication. 3. You can use an AD domain synchronization policy to synchronize the user groups on the LDAP server to the firewall.

58.2 Configuring an Authentication Server Object

58.2.1 Configuring a RADIUS Server Object

With RADIUS configured, when a web authentication user or an administrator is configured to use a RADIUS server for authentication, the firewall connects to the server for authentication.

Choose **Object** > **Authentication server** > **RADIUS** and click **New**.



Configure

Name	
Server IP Address	
Server Password	
Authentication Port	1812

Name: Name of a RADIUS server.

Server IP address: IP address of the RADIUS server.

Server password: Shared key of the RADIUS server.

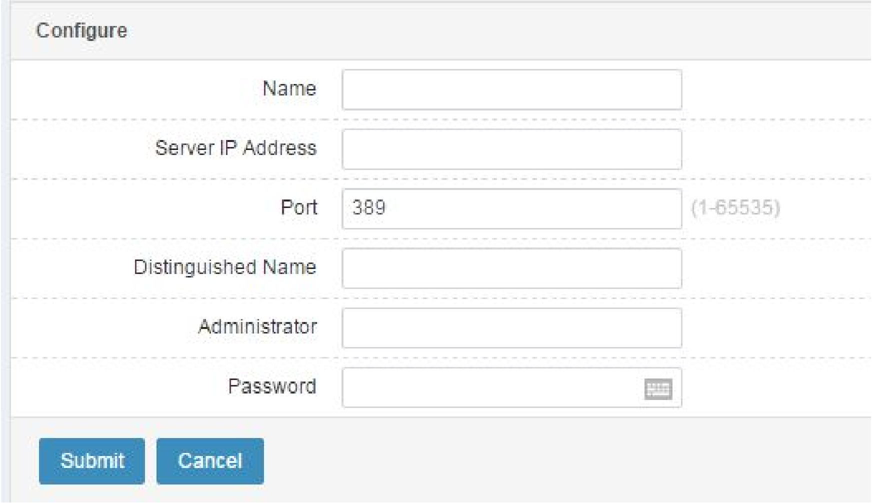
Authentication port: Port of the RADIUS server for authentication. The default value is **1812**.

Click the **RADIUS configuration** tab of **Authentication server** to list all the configured RADIUS servers.

58.2.2 Configuring an LDAP Server

With LDAP configured, when a web authentication user or an administrator is configured to use an LDAP server for authentication, the firewall connects to the server for authentication.

Choose **Object** > **Authentication server** > **LDAP** and click **New**.



Configure

Name		
Server IP Address		
Port	389	(1-65535)
Distinguished Name		
Administrator		
Password		

Name: Name of an LDAP server.

Server IP address: IP address of the LDAP server.

Port: Port of the LDAP server for authentication. The default value is **389**.

Distinguished name: Start position to search data on the LDAP server. For example, if user 2 exists in the **users** container in the **test.com** path of the LDAP server, then enter **dc=test, dc=com**.

Administrator: User with the administrator role on the LDAP server. For example, if the user name and password used to log in to the LDAP server are **administrator** and **111111**, and the user exists in the **users** container in the **test.com** path of the LDAP server, then **enter** **cn=administrator,cn=users,dc=test,dc=com** for **Administrator** and **111111**

for **Password**.

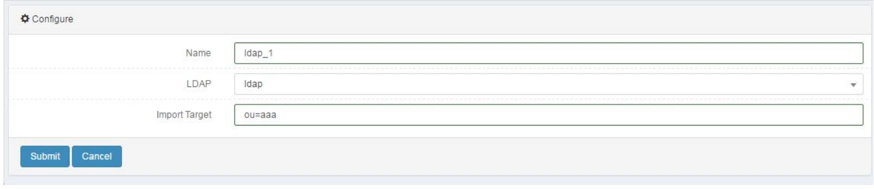
Password: Password of the user with the administrator role on the LDAP server.

Click the **LDAP** tab of **Authentication user** to list all the configured LDAP servers.

58.3 Configuring an AD Domain Synchronization Policy

58.3.1 Creating a Synchronization Policy

1. Choose **Object** > **Authentication server** > **AD domain synchronization** and click **New**.



Configure

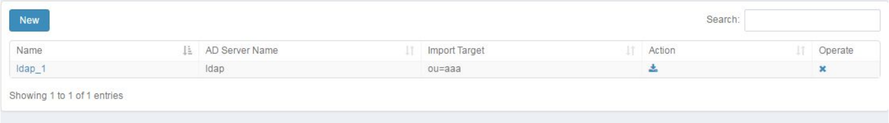
Name	ldap_1
LDAP	ldap
Import Target	ou=aaa

Name: Name of a synchronization policy.

LDAP: Name of an LDAP server.

Import target: Distinguished name (DN) of the user group to be synchronized in a specific path of the LDAP server.

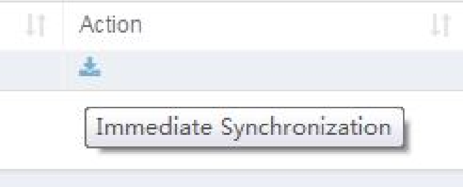
2. Click **Submit**. The following page appears.



Name	AD Server Name	Import Target	Action	Operate
ldap_1	ldap	ou=aaa	⭳	✖

Showing 1 to 1 of 1 entries

3. Click **Synchronize now**.



4. Click **OK** to synchronize the user group.

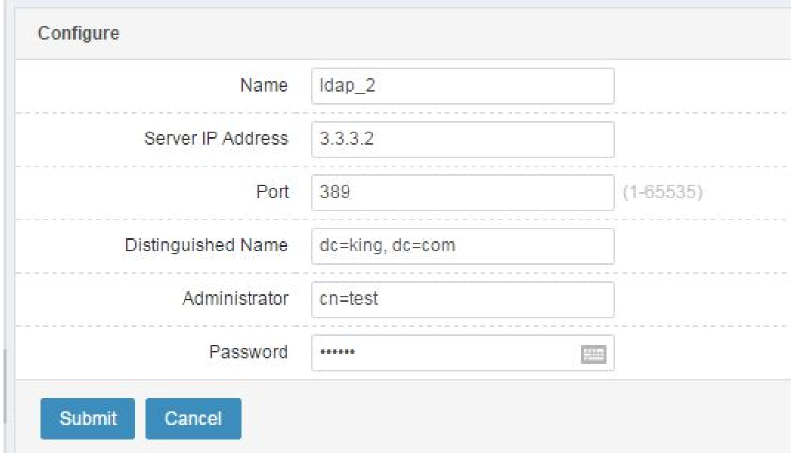
58.3.2 Configuration Example

Description:

Synchronize the user group in the path **dc=king, dc=com** of the server with the IP address 3.3.3.2.

Procedure:

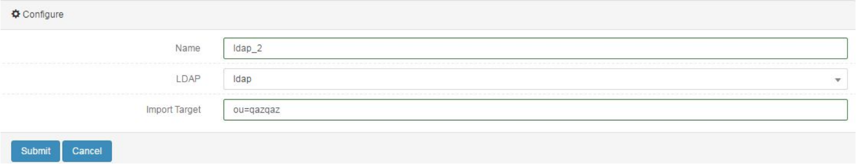
1. Choose **Object** > **Authentication server** > **LDAP** to create an LDAP server.



Configure

Name	ldap_2
Server IP Address	3.3.3.2
Port	389 (1-65535)
Distinguished Name	dc=king, dc=com
Administrator	cn=test
Password	••••••

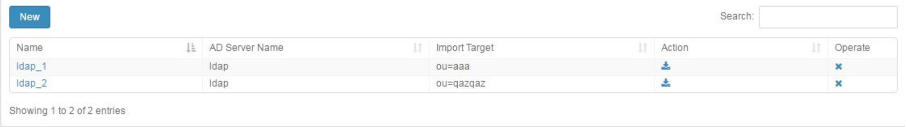
2. Choose **Object** > **Authentication server** > **AD domain synchronization** to create a synchronization policy.



Configure

Name	ldap_2
LDAP	ldap
Import Target	ou=qazqaz

3. Click **Synchronize now**.



Name	AD Server Name	Import Target	Action	Operate
ldap_1	ldap	ou=aaa	⭳	✖
ldap_2	ldap	ou=qazqaz	⭳	✖

Showing 1 to 2 of 2 entries

4. Check the synchronization results. The synchronized group is flagged as **Synchronized group**.

59 URL Category

59.1 Overview

RAVEN5000firewalls introduce URL categories to facilitate configuration and management. During policy configuration, you can reference URL categories to define the effective conditions of configurations, which facilitates control.

Application objects are classified into predefined URL categories, custom URL categories, and URL groups.

- Predefined URL categories include common URLs such as entertainment, finance, and Internet portals. They are updated using the URL feature database and require no manual configuration.
- Custom URL categories must be configured manually.
- A URL group must be configured manually, and it can reference predefined and custom URL categories.

In actual use, URL categories and URL groups are referenced by policies.

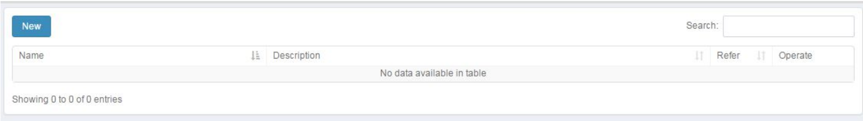
URL categories can be used with application control policies to block and rate-limit the application traffic.

59.2 Configuring URL Categories

59.2.1 Configuring a Custom URL Category

Procedure:

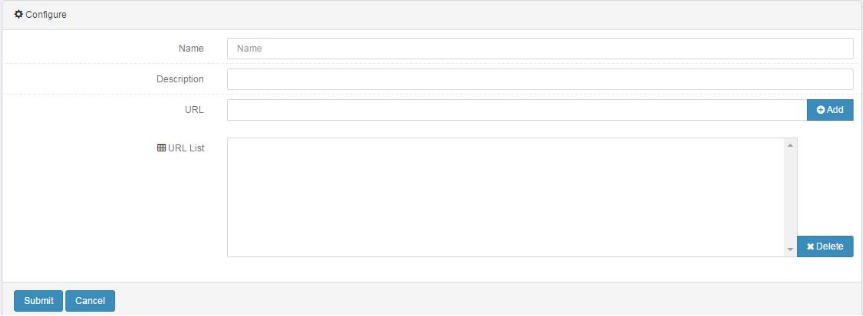
1. Choose **Object** > **URL category** > **User-defined URL category**. A page appears to display existing custom URL categories.



Name	Description	Refer	Operate
No data available in table			

Showing 0 to 0 of 0 entries

2. Click **New** to configure a custom URL category.



Name: Name of the new custom URL category, no more than 63 characters.

Description: Description about the custom URL category, no more than 127 characters.

URL: URL string under the category, no more than 127 characters.

URL list: URL string list under the category.

3. Click **Submit** after you complete the settings.

⚠ Notice

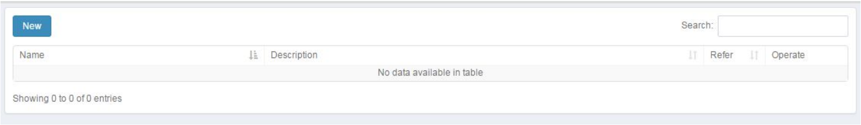
Custom URL categories are of the highest priority. The proper URL string must be added to the custom URL category; otherwise, other access may be identified as custom URL categories, which affects the matching of other control policies.

59.2.2 Configuring a URL Group

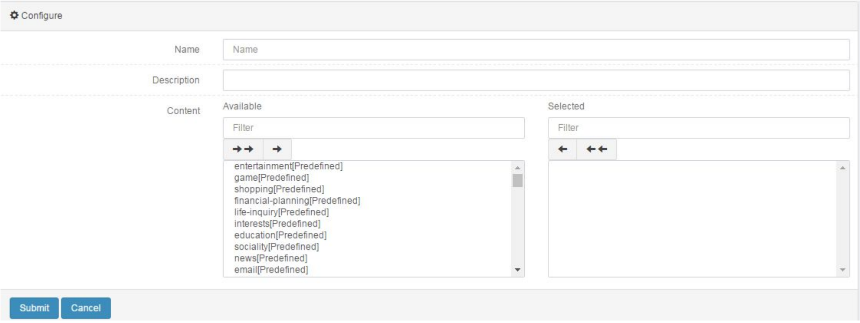
Procedure:

1. Choose **Object** > **URL category** > **URL group**.

A page appears to display existing URL groups.



2. Click **New** to configure a URL group.



Name: Name of the new URL group, no more than 63 characters.

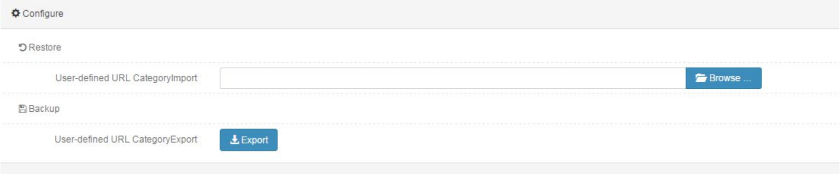
Description: Description about the URL group, no more than 127 characters.

Content: Existing custom URL categories and all predefined URL categories.

Select desired URL categories and click **Submit**.

59.3 Backing Up and Restoring Custom URL Category Configurations

Choose **Object** > **URL category** > **Backup and restoration**.


Configure
Restore
User-defined URL CategoryImport
Browse ...
Backup
User-defined URL CategoryExport
Export

Import system configurations: Select a configuration file to be imported.

Export system configurations: Export a configuration file.

59.4 Configuration Examples

59.4.1 Example 1: Adding a Custom URL Category

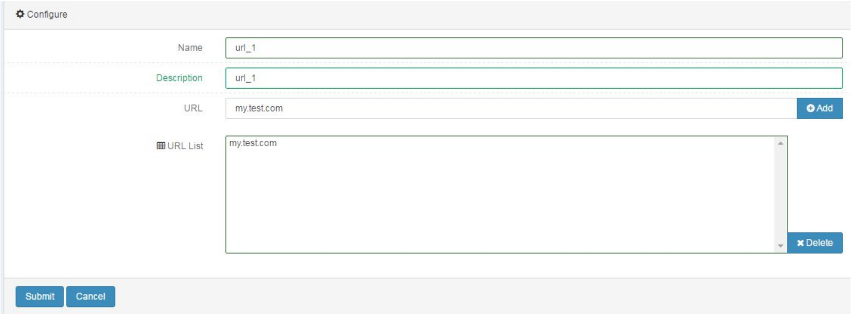
Description:

Add a custom URL category to be referenced by policies.

Procedure:

1. Choose **Object** > **URL category** >**User-defined URL category** and click

New. The following page appears.



Configure

Name: url_1

Description: url_1

URL: my.test.com

URL List: my.test.com

2. Set parameters.

3. Click **Submit**.

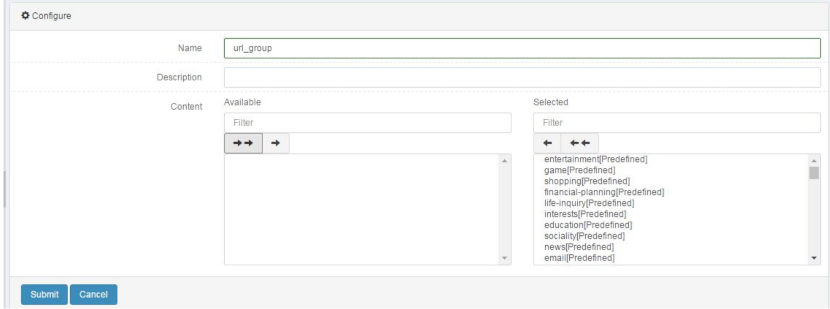
59.4.2 Example 2: Adding a URL Group

Description:

Configure a URL group and reference the Internet portal category so that the policies which reference the URL group take effect for the access to Internet portals.

Procedure:

1. Choose **Object** > **URL category** > **URL group** and click **New**. The following page appears.



Name: url_group

Description:

Content:

Selected:
entertainment[Predefined]
game[Predefined]
shopping[Predefined]
financial-planning[Predefined]
life-inquiry[Predefined]
interests[Predefined]
education[Predefined]
sociality[Predefined]
news[Predefined]
email[Predefined]

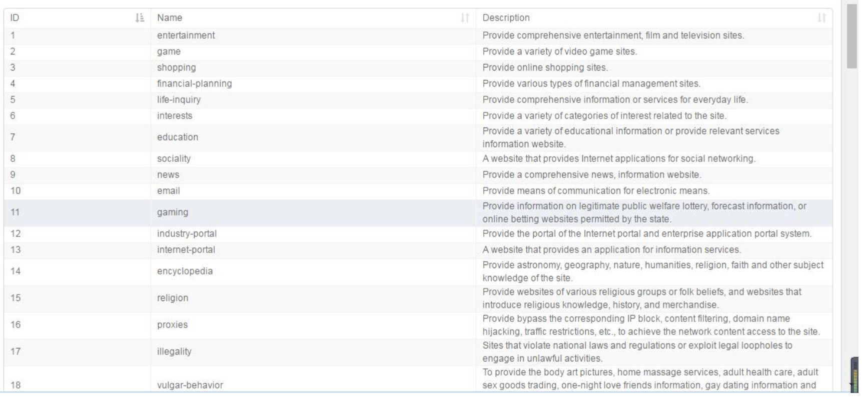
2. Specify the URL group name and description, and select the Internet portal category.

3. Click **Submit**.

59.5 Monitoring and Maintenance

59.5.1 Displaying Predefined URL Categories

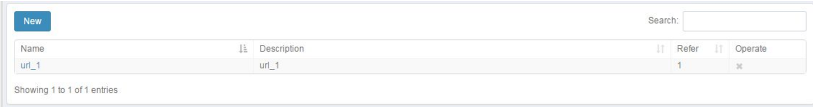
Choose **Object** > **URL category** > **Predefined URL category**. The following page appears.



ID	Name	Description
1	entertainment	Provide comprehensive entertainment, film and television sites.
2	game	Provide a variety of video game sites.
3	shopping	Provide online shopping sites.
4	financial-planning	Provide various types of financial management sites.
5	life-inquiry	Provide comprehensive information or services for everyday life.
6	interests	Provide a variety of categories of interest related to the site.
7	education	Provide a variety of educational information or provide relevant services information website.
8	sociality	A website that provides Internet applications for social networking.
9	news	Provide a comprehensive news, information website.
10	email	Provide means of communication for electronic means.
11	gaming	Provide information on legitimate public welfare lottery, forecast information, or online betting websites permitted by the state.
12	industry-portal	Provide the portal of the Internet portal and enterprise application portal system.
13	internet-portal	A website that provides an application for information services.
14	encyclopedia	Provide astronomy, geography, nature, humanities, religion, faith and other subject knowledge of the site.
15	religion	Provide websites of various religious groups or folk beliefs, and websites that introduce religious knowledge, history, and merchandise.
16	proxies	Provide bypass the corresponding IP block, content filtering, domain name hijacking, traffic restrictions, etc., to achieve the network content access to the site.
17	illegality	Sites that violate national laws and regulations or exploit legal loopholes to engage in unlawful activities.
18	vulgar-behavior	To provide the body art pictures, home massage services, adult health care, adult sex goods trading, one-night love friends information, gay dating information and

59.5.2 Displaying Custom URL Categories

Choose **Object** > **URL category** >**User-defined URL category**. The following page appears.

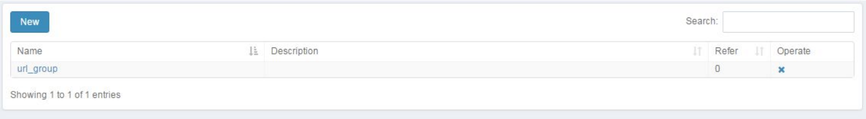


Name	Description	Refer	Operate
url_1	url_1	1	×

Showing 1 to 1 of 1 entries

59.5.3 Displaying URL Groups

Choose **Object** > **URL category** > **URL group**. The following page appears.

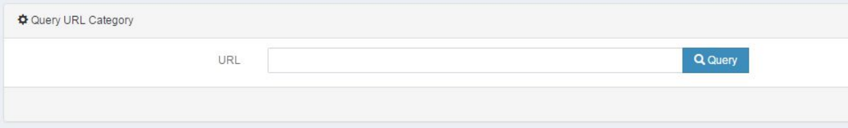


Name	Description	Refer	Operate
url_group		0	×

Showing 1 to 1 of 1 entries

59.5.4 Querying URL Categories

Choose **Object** > **URL category** > **URL category query**. The following page appears.



URL: URL to be queried, no more than 127 characters.

Enter a URL and click **Query**.

60 Domain Name Object

60.1 Overview

RAVEN 5000 firewalls introduce domain name objects to facilitate configuration and management. During policy configuration, you can reference domain name objects to facilitate control.

Domain name objects are classified into custom domain names and domain name groups.

- A custom domain name must be configured manually.
- A domain name group must be configured manually and it can reference custom domain names.

In actual use, domain name objects are referenced by policies.

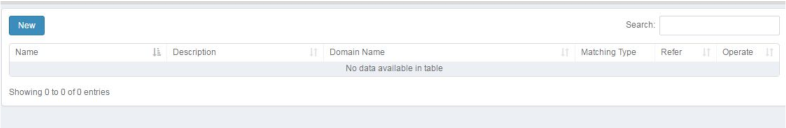
Domain name objects can be used with routing policies to divert the traffic of accessing a domain name to a specified link, which is very practical in actual network environments.

60.2 Configuration

60.2.1 Configuring a Custom Domain Name

Procedure:

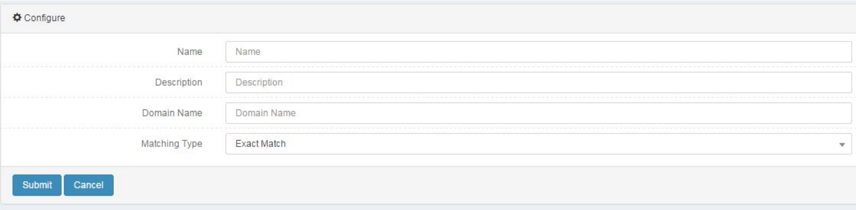
1. Choose **Object** > **Domain name object** > **User-defined domain name**. A page appears to display existing custom domain names.



Name	Description	Domain Name	Matching Type	Refer	Operate
No data available in table					

Showing 0 to 0 of 0 entries

2. Click **New** to configure a custom domain name.



Matching Type: Exact Match

Name: Name of the new custom domain name, no more than 63 characters.

Description: Description about the custom domain name, no more than 127 characters.

Domain name: Domain name match string.

Match type: Domain name match type. The options are **Full match** and **Include**.

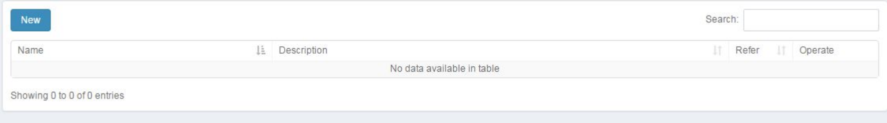
3. Click **Submit** after you complete the settings.

60.2.2 Configuring a Domain Name Group

Procedure:

1. Choose **Object** > **Domain name object** > **Domain name group**.

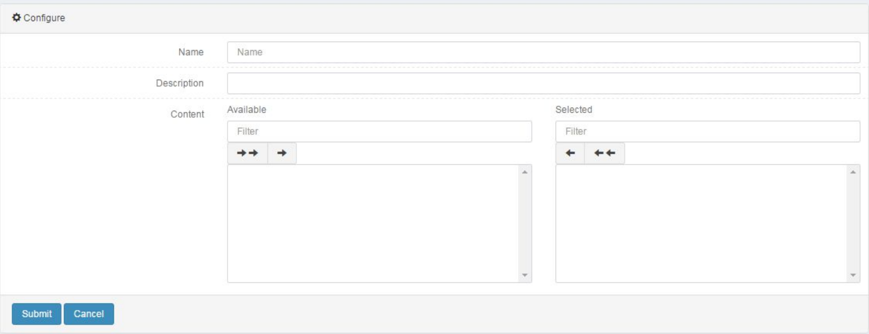
A page appears to display existing domain name groups.



Name	Description	Refer	Operate
No data available in table			

Showing 0 to 0 of 0 entries

2. Click **New** to configure a domain name group.



Name: Name of the new domain name group, no more than 63 characters.

Description: Description about the domain name group, no more than 127 characters.

Content: Existing custom domain names. See the preceding figure.

Select desired applications and click **Submit**.

60.3 Configuration Examples

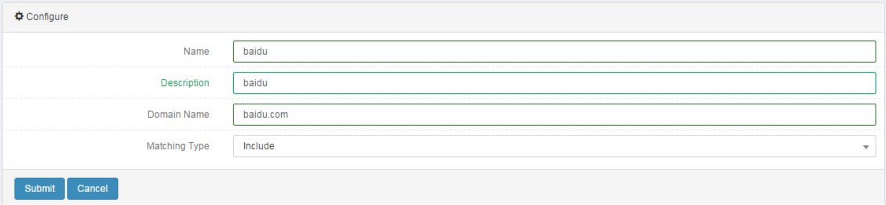
60.3.1 Example 1: Adding a Custom Domain Name

Description:

Add a custom domain name to be referenced by policies.

Procedure:

1. Choose **Object** > **Domain name object** >**User-defined domain name** and click **New**. The following page appears.



Name: baidu

Description: baidu

Domain Name: baidu.com

Matching Type: Include

2. Set parameters.
3. Click **Submit**.

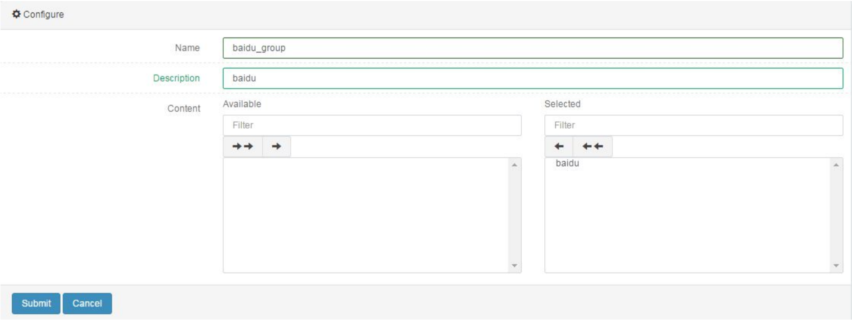
60.3.2 Example 2: Adding a Domain Name Group

Description:

Configure a domain name group and reference custom domain names so that the policies which reference the domain name group take effect for the traffic of accessing the domain names.

Procedure:

1. Choose **Object** > **Domain name object** > **Domain name group** and click **New**. The following page appears.



Name	baidu_group
Description	baidu

Content

Available	Selected
	baidu

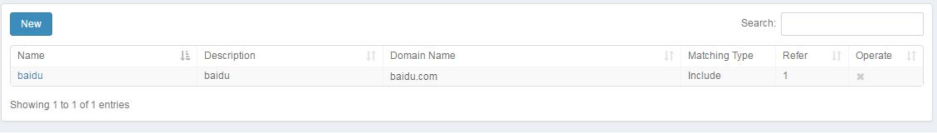
2. Specify the group name and description, and select custom domain names.

3. Click **Submit**.

60.4 Monitoring and Maintenance

60.4.1 Displaying Custom Domain Names

Choose **Object** > **Domain name object** > **User-defined domain name**. The following page appears.

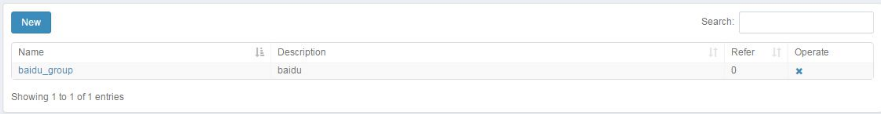


Name	Description	Domain Name	Matching Type	Refer	Operate
baidu	baidu	baidu.com	Include	1	✖

Showing 1 to 1 of 1 entries

60.4.2 Displaying Domain Name Groups

Choose **Object** > **Domain name object** > **Domain name group**. The following page appears.



Name	Description	Refer	Operate
baidu_group	baidu	0	✖

Showing 1 to 1 of 1 entries

61 Time Object

61.1 Overview

RAVEN 5000 firewalls introduce time objects to facilitate configuration and management. Time objects are classified into absolute time and cycle time. During feature configuration, you can reference time objects to define the effective conditions of configurations.

Absolute time: Services take effect during a specified period.

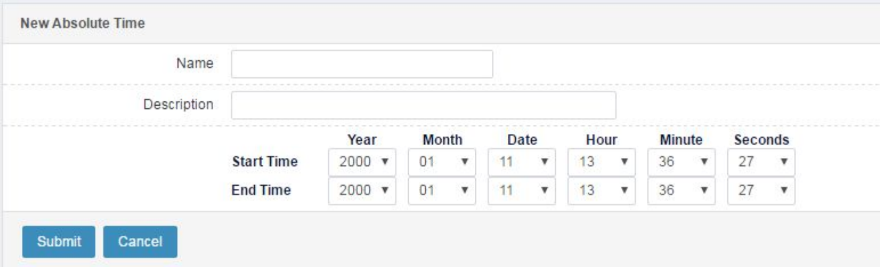
Cycle time: Services are executed at a specified cycle (Monday to Sunday) within a time range.

61.2 Configuration

61.2.1 Configuring an Absolute Time Object

Only one effective time range can be configured for absolute time.

Choose **Object** > **Time object** > **Absolute time** and click **New**. The following page appears.



New Absolute Time

Name

Description

	Year	Month	Date	Hour	Minute	Seconds
Start Time	2000	01	11	13	36	27
End Time	2000	01	11	13	36	27

Name: Name of the new absolute time object.

Description: Description about the absolute time object.

Start time: Time when the absolute time starts, in the format of *year-month-day hours*:*minutes*.

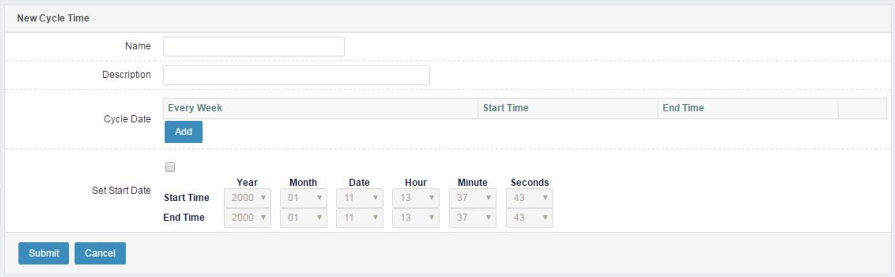
End time: Time when the absolute time ends, in the format of *year-month-day hours*:*minutes*.

Click **Submit** after you complete the settings.

61.2.2 Configuring a Cycle Time Object

You can define an effective time range and one or more effective periods for absolute time. The effective periods are of the OR relationship, and only one of them needs to be satisfied. The effective time range and effective periods are of the AND relationship, and both of them must be satisfied.

1. Choose **Object** > **Time object** > **Cycle time** and click **New**. The following page appears.



	Year	Month	Date	Hour	Minute	Seconds
Start Time	2000	01	11	13	37	43
End Time	2000	01	11	13	37	43

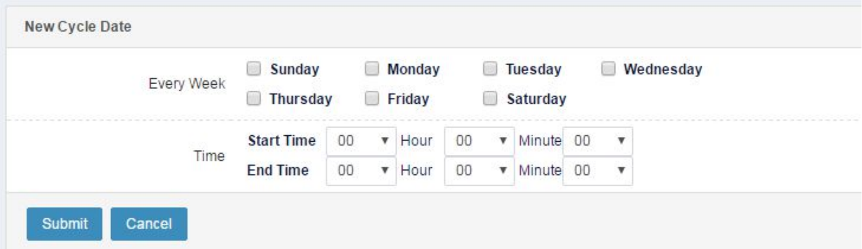
Name: Name of the new cycle time object.

Description: Description about the cycle time object.

Start time: Time when the cycle time starts, in the format of *year-month-day hours*:*minutes*.

End time: Time when the cycle time ends, in the format of *year-month-day hours*:*minutes*.

Cycle: Click **Add** to add effective periods, as shown in the following figure.



Start Time	00	Hour	00	Minute	00
End Time	00	Hour	00	Minute	00

2. Click **Submit** after you complete the settings.

61.3 Configuration Examples

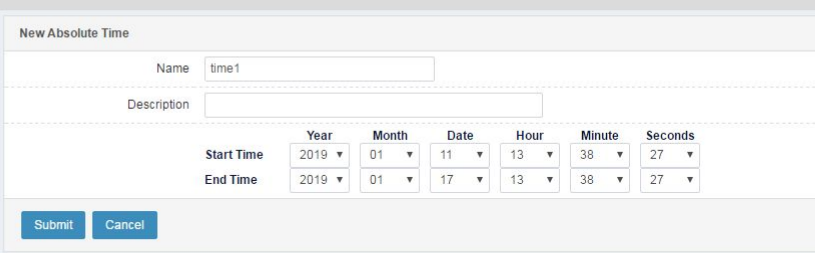
61.3.1 Example 1: Adding an Absolute Time Object

Description:

Add an absolute time object to be referenced by firewall policies so that the policies take effect only during a specified period.

Procedure:

1. Choose **Object** > **Time object** > **Absolute time** and click **New**. The following page appears.



New Absolute Time

Name: time1

Description:

	Year	Month	Date	Hour	Minute	Seconds
Start Time	2019	01	11	13	38	27
End Time	2019	01	17	13	38	27

2. Set parameters.

3. Click **Submit**.

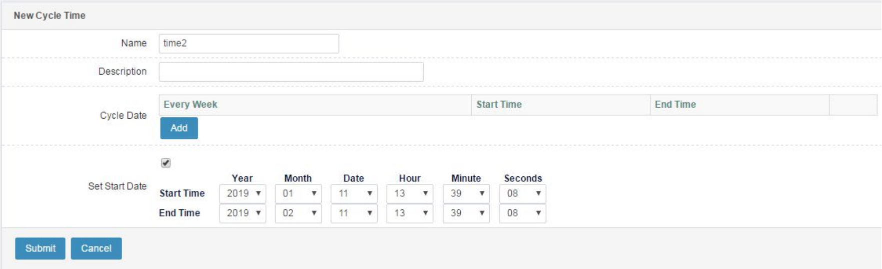
61.3.2 Example 2: Adding a Cycle Time Object

Description:

Add a cycle time object so that the policies which reference it take effect at a cycle.

Procedure:

1. Choose **Object** > **Time object** > **Cycle time** and click **New**. The following page appears.



New Cycle Time

Name: time2

Description:

Cycle Date

Every Week	Start Time	End Time

Set Start Date ☑

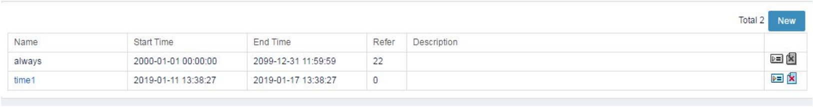
	Year	Month	Date	Hour	Minute	Seconds
Start Time	2019	01	11	13	39	08
End Time	2019	02	11	13	39	08

2. Click **Submit** after you complete the settings.

61.4 Monitoring and Maintenance

61.4.1 Displaying Absolute Time Objects

Choose **Object** > **Time object** > **Absolute time**. The following page appears.



Name	Start Time	End Time	Refer	Description	
always	2000-01-01 00:00:00	2099-12-31 11:59:59	22		
time1	2019-01-11 13:38:27	2019-01-17 13:38:27	0		

61.5 Troubleshooting

61.5.1 Failed to Submit Settings

Symptom	The settings fail to be submitted after the **Submit** button is clicked.
Analysis	The end time is earlier than the start time.
Solution	Change the end time to be later than the start time.

62 Health Check

62.1 Overview

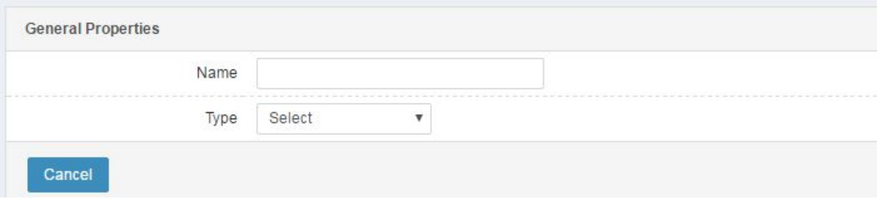
Health check is performed on next hops or remote devices to determine their health status. If health check finds a link or device faulty, traffic is not routed to the link or device.

Health check supports ICMP, TCP, UDP, HTTP, HTTPS, RADIUS, LDAP, FTP, POP3, and SMTP. Connectivity can be monitored over ICMP, and services can be monitored accurately in corresponding check modes.

RAVEN5000 firewalls provide health check of IPv4 and IPv6 servers.

62.2 Configuration

Choose **Object** > **Health check** and click **New**.



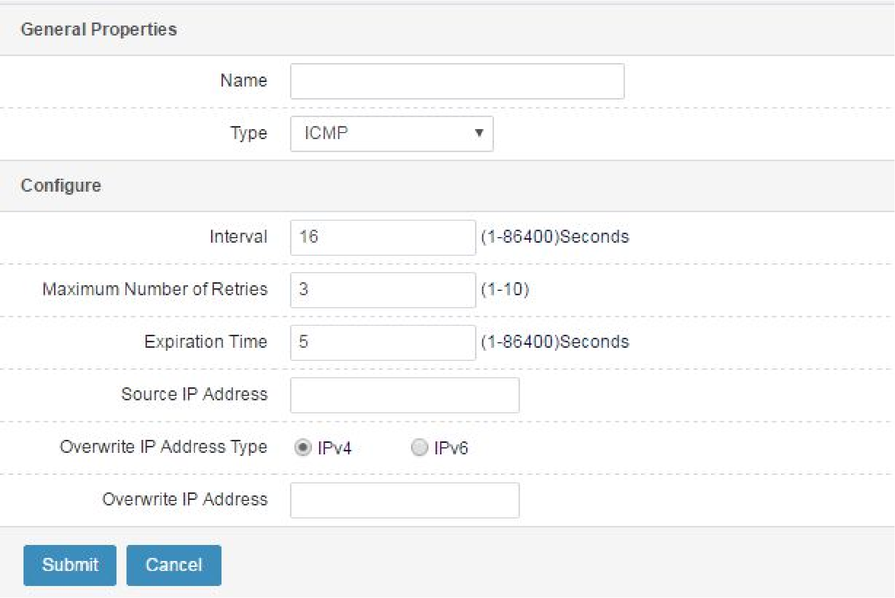
Name: Name of a health check template.

Type: Type of health check. After you select a type, the page shows the corresponding template configuration.

Procedure:

1. Set **Name**.
2. Select an option for **Type**.

When **ICMP** is selected for **Type**, the configuration page is as follows:



General Properties

Name	
Type	ICMP ▾

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
Source IP Address		
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Source IP address: Source IP address that sends detection packets. Set this parameter if a source IP address is required by health check.

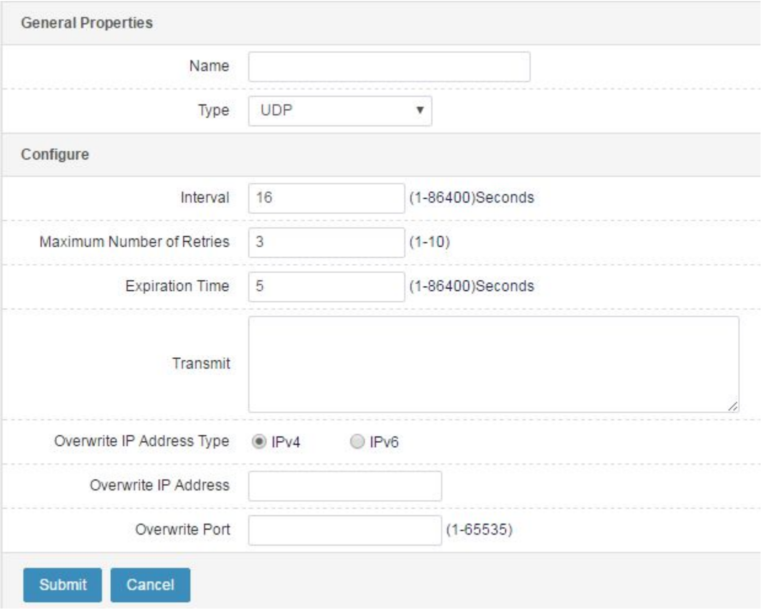
Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host or link with another IP address.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Select an option for **Included IP address type**.
5. Set **Included IP address**.
6. Click **Submit**.

When **UDP** is selected for **Type**, the configuration page is as follows:



General Properties

Name

Type UDP ▼

Configure

Interval 16 (1-86400)Seconds

Maximum Number of Retries 3 (1-10)

Expiration Time 5 (1-86400)Seconds

Transmit

Overwrite IP Address Type ● IPv4 ○ IPv6

Overwrite IP Address

Overwrite Port (1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Send: Content in a sent UDP packet.

Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host or link with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

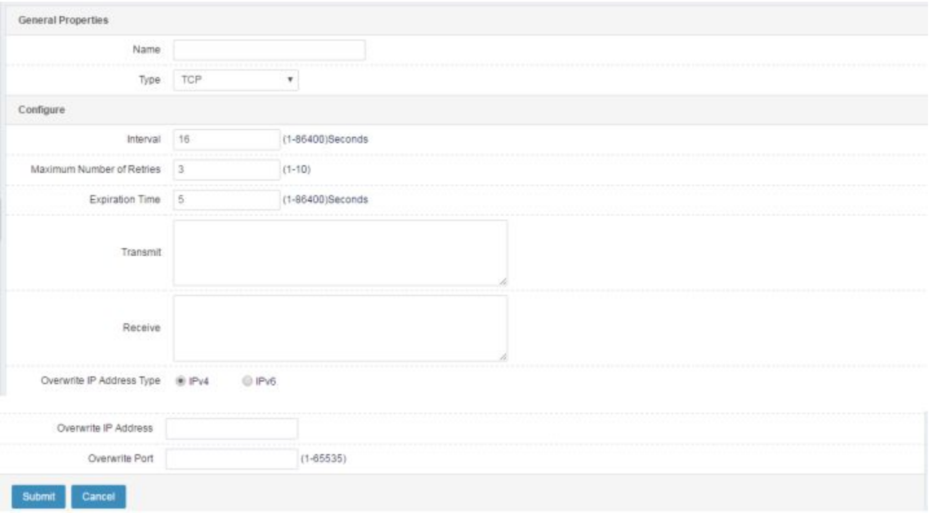
1. Set **Interval**.
2. Set **Maximum retry times.**
3. Set **Timeout period**.
4. Set **Send**.
5. Select an option for **Included IP address type**.

6. Set **Included IP address** and **Included port**.7. Click **Submit**.

Note

UDP health check must be performed with other health check modes, such as ICMP, because the symptom in UDP mode is the same when service is unavailable or the detected address does not exist.

When **TCP** is selected for **Type**, the configuration page is as follows:



General Properties

Name	
Type	TCP ▾

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
Transmit		
Receive		
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		
Overwrite Port		(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Send: Content in a sent TCP packet.

Receive: Content in a received packet. The status is Down when the received packet does not have the specified content.

Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host or link with another IP

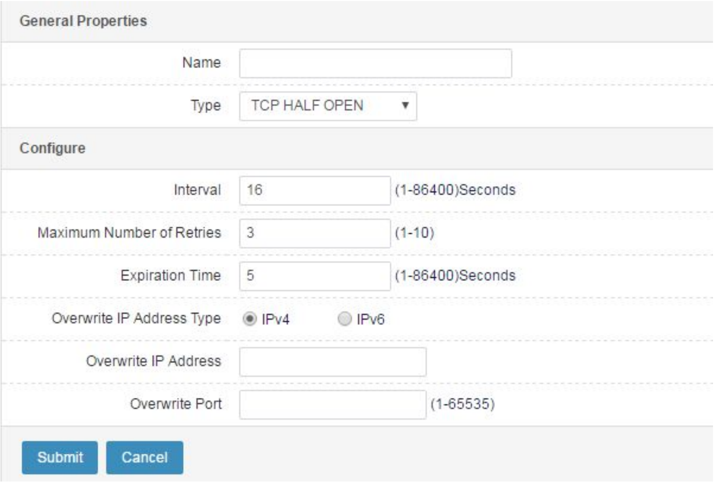
address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Set **Send**.
5. Set **Receive**.
6. Select an option for **Included IP address type**.
7. Set **Included IP address** and **Included port**.
8. Click **Submit**.

When **TCP HALF OPEN** is selected for **Type**, the configuration page is as follows:



General Properties

Name	
Type	TCP HALF OPEN ▾

Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	
Overwrite Port	(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host or link with another IPaddress.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

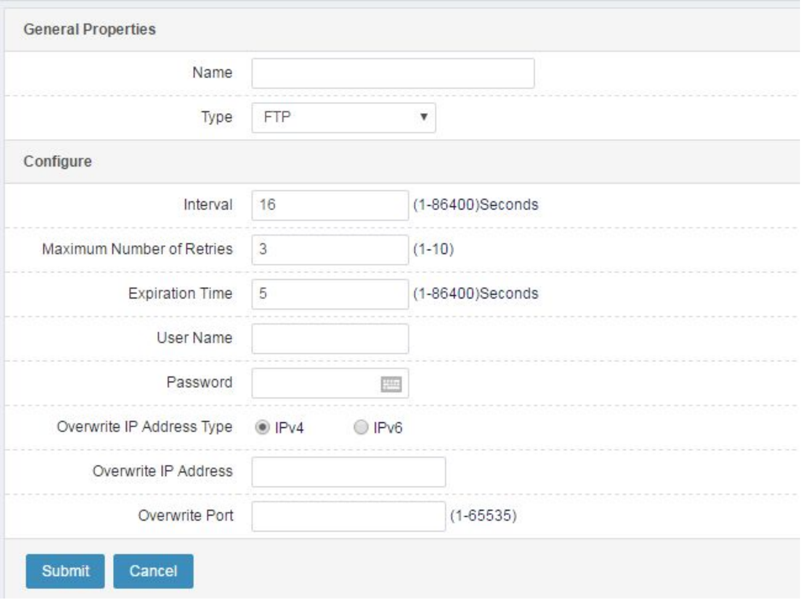
Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Select an option for **Included IP address type**.
5. Set **Included IP address**.
6. Click **Submit**.

Note

Different from TCP health check, TCP HALF OPEN health check requires no connection between the firewall and server, which reduces exchanged packets.

When **FTP** is selected for **Type**, the configuration page is as follows:



General Properties

Name		
Type	FTP ▾	

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
User Name		
Password		
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		
Overwrite Port		(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.**Timeout period** (seconds): If detection packets get no response within the timeout period, then health check fails.

User name: User name for FTP authentication.

Password: Password of the FTP user.

Included IP address type: The options are **IPv4** and **IPv6**.

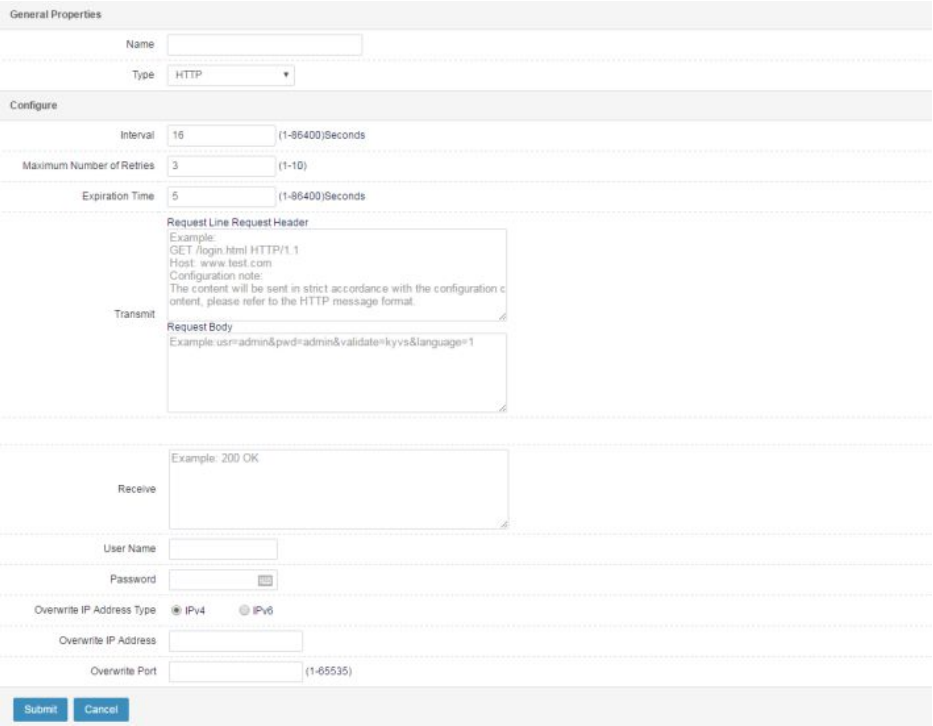
Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host or link with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Set **User name**.
5. Set **Password**.
6. Select an option for **Included IP address type**.
7. Set **Included IP address** and **Included port**.
8. Click **Submit**.

When **HTTP/HTTPS** is selected for **Type**, the configuration page is as follows:



General Properties

Name	
Type	HTTP ▾

Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Transmit	Request Line Request Header Example: GET /login.html HTTP/1.1 Host: www.test.com Configuration note: The content will be sent in strict accordance with the configuration content, please refer to the HTTP message format. Request Body Example:usr=admin&pwd=admin&validate=kyvs&language=1
Receive	Example: 200 OK
User Name	
Password	
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	
Overwrite Port	(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Send: Content in a sent HTTP/HTTPS packet.

Receive: Content in a received packet. The status is Down when the received packet does not have the specified content.

User name: User name for HTTP/HTTPS authentication.

Password: Password of the HTTP/HTTPS user.

Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host or link with another IP

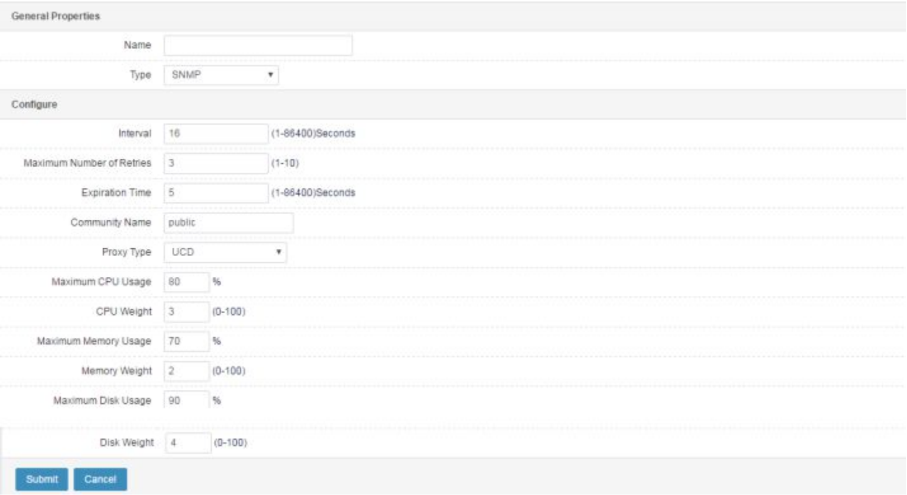
address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Set **Send**.
5. Set **Receive**.
6. Set **User name**.
7. Set **Password**.
8. Select an option for **Included IP address type**.
9. Set **Included IP address** and **Included port**.
10. Click **Submit**.

When **SNMP** is selected for **Type**, the configuration page is as follows:



General Properties

Name		
Type	SNMP ▾	

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
Community Name	public	
Proxy Type	UCD ▾	
Maximum CPU Usage	80	%
CPU Weight	3	(0-100)
Maximum Memory Usage	70	%
Memory Weight	2	(0-100)
Maximum Disk Usage	90	%
Disk Weight	4	(0-100)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Retry times allowed after a detection packet gets no response. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Community name: Password for SNMP proxy authentication.

Proxy type: The options are **UCD (Linux)** and **Windows**.

CPU limit: CPU usage threshold. The server is deemed unavailable when the threshold is exceeded.

CPU weight: Weight ratio of the CPU in load calculation based on CPU, memory, and disk space.

Memory limit: Memory usage threshold. The server is deemed unavailable when the threshold is exceeded.

Memory weight: Weight ratio of the memory in load calculation based on CPU, memory, and disk space.

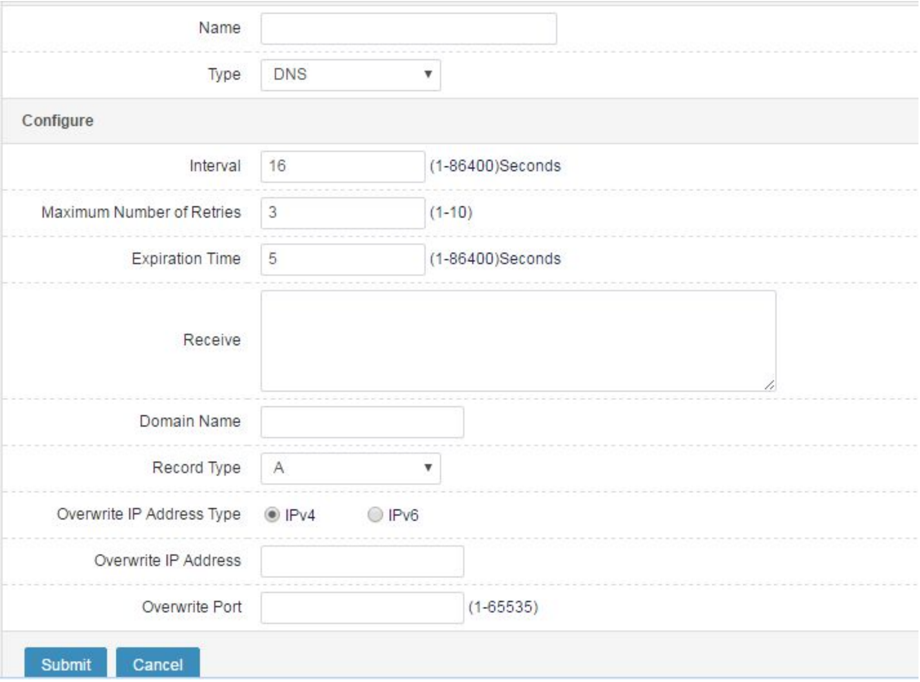
Disk limit: Disk usage threshold. The server is deemed unavailable when the threshold is exceeded.

Disk weight: Weight ratio of the disk space in load calculation based on CPU, memory, and disk space.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Set **Community name**.
5. Select an option for **Proxy type**.
6. Set **CPU limit**.
7. Set **CPU weight**.
8. Set **Memory limit**.
9. Set **Memory weight**.
10. Set **Disk limit**.
11. Set **Disk weight**.
12. Click **Submit**.

When **DNS** is selected for **Type**, the configuration page is as follows:



Name	
Type	DNS ▾
Configure	
Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Receive	
Domain Name	
Record Type	A ▾
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	
Overwrite Port	(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Receive: Content in a received packet. Health check fails when the received packet does not have the specified content.

Domain name: Domain name resolved by the DNS server.

Record type: Select a DNS record type.

Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host with another IP address.

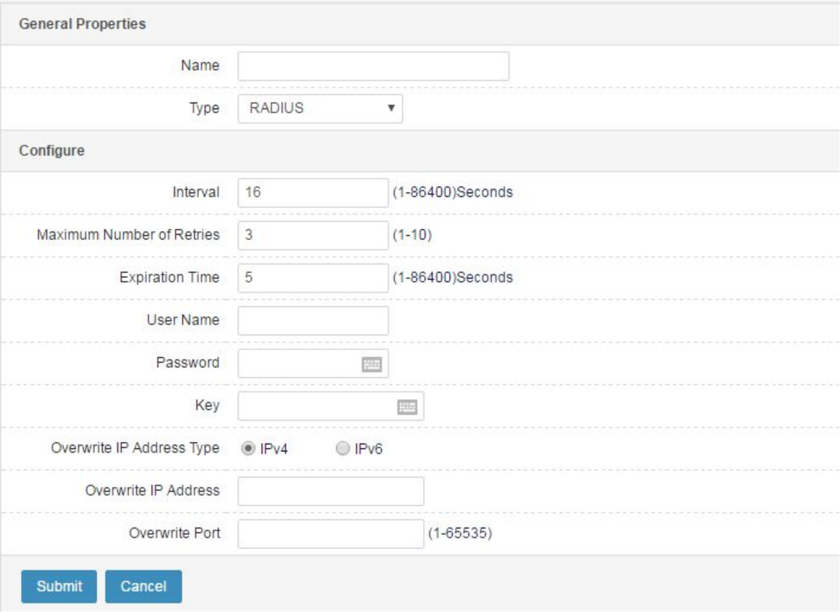
Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.

3. Set **Timeout period**.
4. Set **Receive**.
5. Set **Domain name**.
6. Select an option for **Included IP address type**.
7. Set **Included IP address** and **Included port**.
8. Click **Submit**.

When **RADIUS** is selected for **Type**, the configuration page is as follows:



General Properties

Name	
Type	RADIUS ▾

Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
User Name	
Password	
Key	
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	
Overwrite Port	(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

User name: User name for RADIUS authentication.

Password: Password of the RADIUS user.

Key: Key for negotiation with the RADIUS server.

Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host or link with another IP

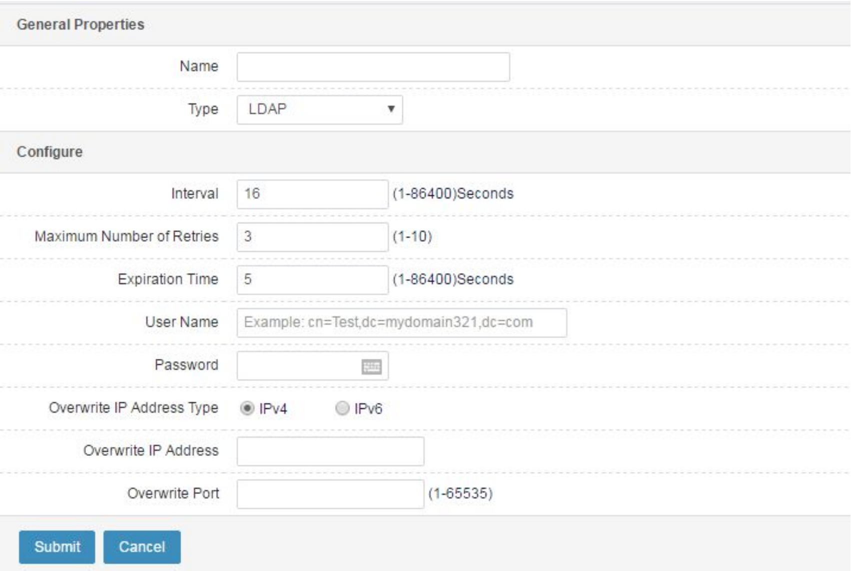
address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Set **User name**.
5. Set **Password**.
6. Set **Key**.
7. Select an option for **Included IP address type**.
8. Set **Included IP address**.
9. Set **Included port**.
10. Click **Submit**.

When **LDAP** is selected for **Type**, the configuration page is as follows:



General Properties

Name		
Type	LDAP ▾	

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
User Name	Example: cn=Test,dc=mydomain321,dc=com	
Password		
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		
Overwrite Port		(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

User name: LDAP user name.

Password: Password of the LDAP user.

Included IP address type: The options are **IPv4** and **IPv6**.

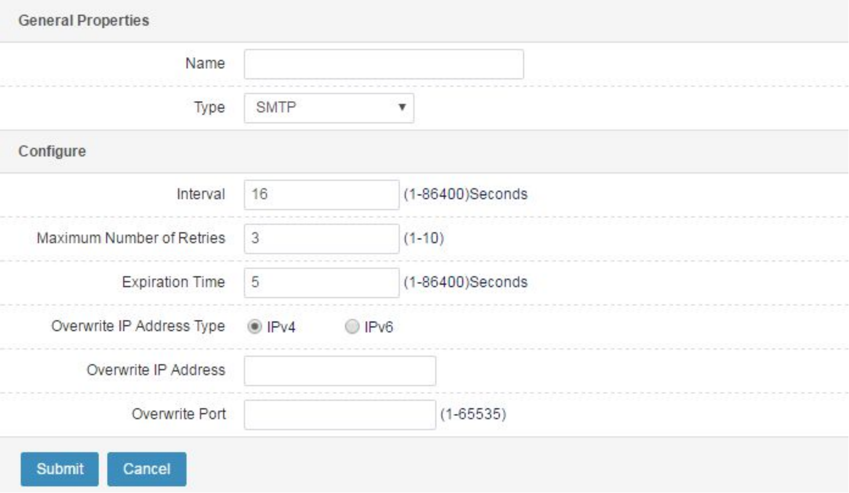
Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Set **User name**.
5. Set **Password**.
6. Select an option for **Included IP address type**.
7. Set **Included IP address**.
8. Set **Included port**.
9. Click **Submit**.

When **SMTP** is selected for **Type**, the configuration page is as follows:



General Properties

Name		
Type	SMTP ▾	

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		
Overwrite Port		(1-65535)

3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Included IP address type: The options are **IPv4** and **IPv6**.

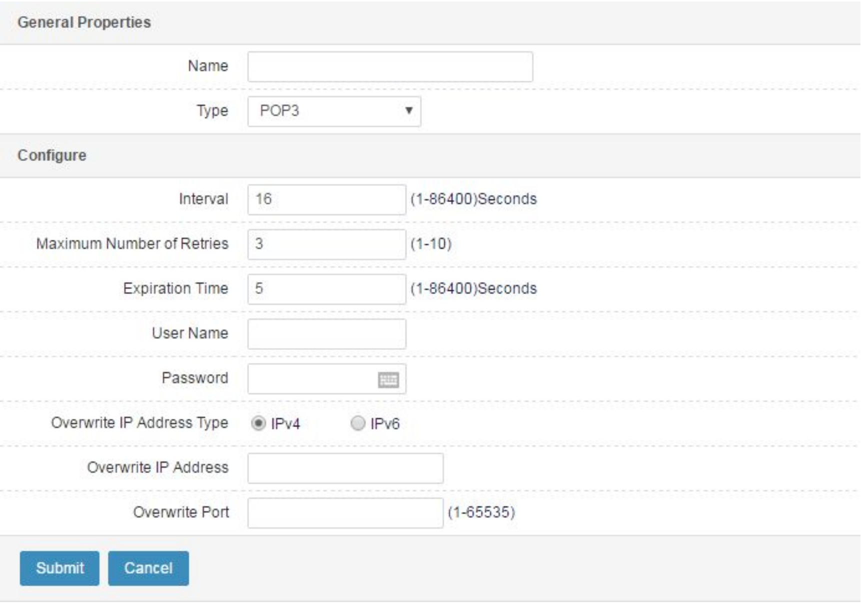
Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Select an option for **Included IP address type**.
5. Set **Included IP address**.
6. Set **Included port**.
7. Click **Submit**.

When **POP3** is selected for **Type**, the configuration page is as follows:



General Properties

Name		
Type	POP3 ▾	

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
User Name		
Password		
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		
Overwrite Port		(1-65535)

3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

User name: POP3 user name.

Password: Password of the POP3 user.

Included IP address type: The options are **IPv4** and **IPv6**.

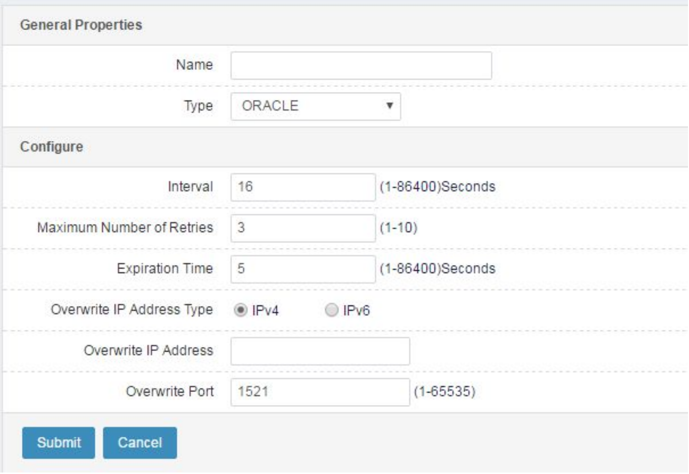
Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times.**
3. Set **Timeout period**.
4. Set **User name**.
5. Set **Password**.
6. Select an option for **Included IP address type**.
7. Set **Included IP address**.
8. Set **Included port**.
9. Click **Submit**.

When **ORACLE** is selected for **Type**, the configuration page is as follows:



General Properties

Name	
Type	ORACLE ▼

Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	
Overwrite Port	1521 (1-65535)

Name: Name of the new health check template.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Included IP address type: The options are **IPv4** and **IPv6**.

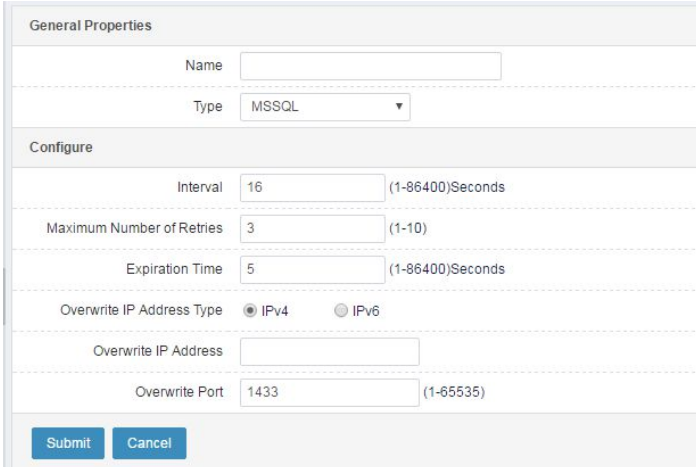
Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports. The default port is 1521.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Select an option for **Included IP address type**.
5. Set **Included IP address**.
6. Click **Submit**.

When **MSSQL** is selected for **Type**, the configuration page is as follows:



General Properties

Name		
Type	MSSQL ▾	

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		
Overwrite Port	1433	(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Included IP address type: The options are **IPv4** and **IPv6**.

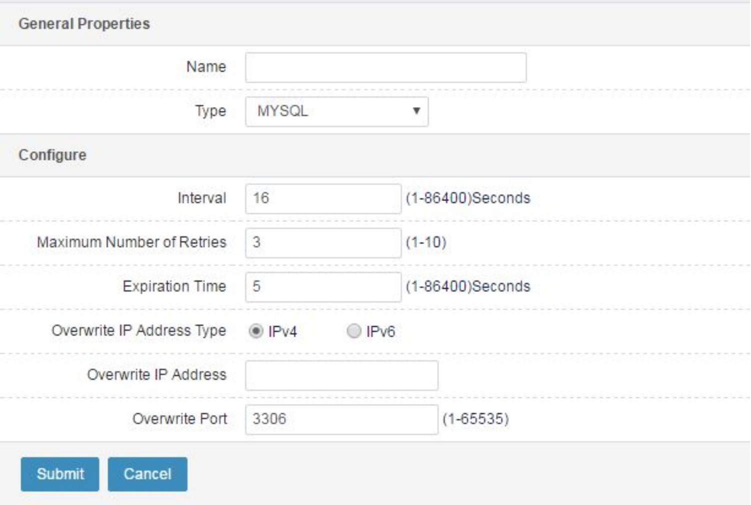
Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports. The default port is 1433.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times.**
3. Set **Timeout period**.
4. Select an option for **Included IP address type**.
5. Set **Included IP address.**
6. Click **Submit**.

When **MYSQL** is selected for **Type**, the configuration page is as follows:



General Properties

Name		
Type	MYSQL ▾	

Configure

Interval	16	(1-86400)Seconds
Maximum Number of Retries	3	(1-10)
Expiration Time	5	(1-86400)Seconds
Overwrite IP Address Type	● IPv4 ○ IPv6	
Overwrite IP Address		
Overwrite Port	3306	(1-65535)

Name: Name of the new health check template.

Type: Protocol type of the health check template.

Interval: Interval at which status detection packets are sent, in seconds.

Maximum retry times: Maximum retry times after detection fails. The default value is **3**, indicating if three detection packets get no response or detection fails 3 times, then health check fails.

Timeout period (seconds): If detection packets get no response within the timeout period, then health check fails.

Included IP address type: The options are **IPv4** and **IPv6**.

Included IP address: Detected IP address. Set this parameter if the health status of the referenced object depends on the host with another IP address.

Included port: Detected port. Set **Included port** and **Included IP address** if the health status of the referenced object depends on other ports. The de fault port is 3306.

Procedure:

1. Set **Interval**.
2. Set **Maximum retry times**.
3. Set **Timeout period**.
4. Select an option for **Included IP address type**.
5. Set **Included IP address**.
6. Click **Submit**.

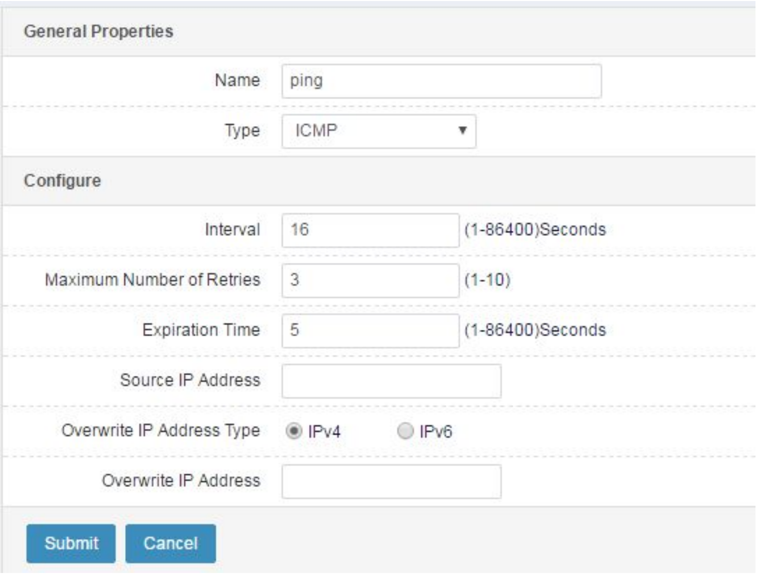
62.3 Configuration Example

Description:

Create an ICMP health check template and reference the template in PBR to detect next hops and return results.

Procedure:

1. Create an ICMP health check template.



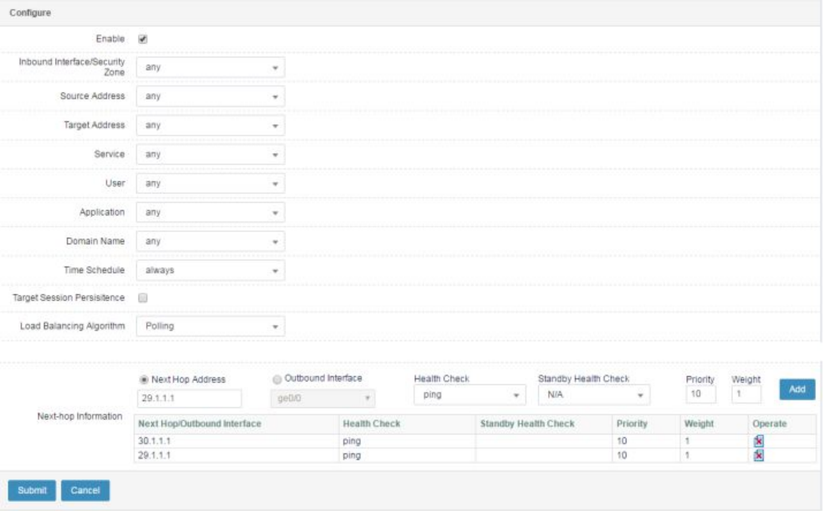
General Properties

Name	ping
Type	ICMP ▾

Configure

Interval	16 (1-86400)Seconds
Maximum Number of Retries	3 (1-10)
Expiration Time	5 (1-86400)Seconds
Source IP Address	
Overwrite IP Address Type	● IPv4 ○ IPv6
Overwrite IP Address	

2. Reference the ICMP template in PBR.



Configure

Enable	☑
Inbound Interface/Security Zone	any
Source Address	any
Target Address	any
Service	any
User	any
Application	any
Domain Name	any
Time Schedule	always
Target Session Persisitence	☐
Load Balancing Algorithm	Polling

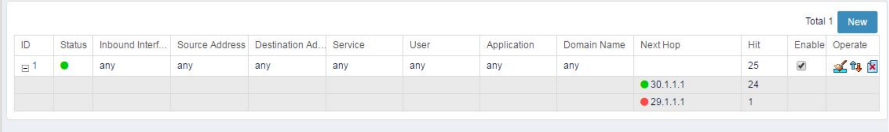
Next-hop Information

● Next Hop Address: 29.1.1.1 ○ Outbound Interface: ge0/0 Health Check: ping Standby Health Check: N/A Priority: 10 Weight: 1

Next Hop/Outbound Interface	Health Check	Standby Health Check	Priority	Weight	Operate
30.1.1.1	ping		10	1	☒
29.1.1.1	ping		10	1	☒

3. View the health check results.

The next hop 30.1.1.1 can be pinged, so health check is successful, as shown in the following figure. The next hop 29.1.1.1 cannot be pinged, so health check fails.



Total 1

ID	Status	Inbound Interf...	Source Address	Destination Ad...	Service	User	Application	Domain Name	Next Hop	Hit	Enable	Operate
⊟ 1	●	any	any	any	any	any	any	any		25	☑	
									● 30.1.1.1	24		
									● 29.1.1.1	1		

63 CA Certificate

63.1 Overview

The public key interface (PKI) uses a certificate management public key and binds a user's public key and other identification information (such as the user name, email, and ID card number) through a third-party trusted organization called certificate authority (CA) to verify the user's identity on the Internet. A digital certificate created on the PKI is used to encrypt and sign the digital information to be transmitted to ensure information confidentiality, authenticity, integrity, and non-repudiation, which guarantees information security.

To configure a PKI local certificate on a firewall, import a user certificate, a third-party CA certificate, and a third-party certificate revocation list (CRL). You can import different local certificates, CA certificates, and CRLs. When you verify a terminal certificate, you must import the corresponding CA certificate and CRL.

63.2 Configuration

This section describes how to import and export the client certificate, third-party CA certificate, and third-party CRL required by a firewall.

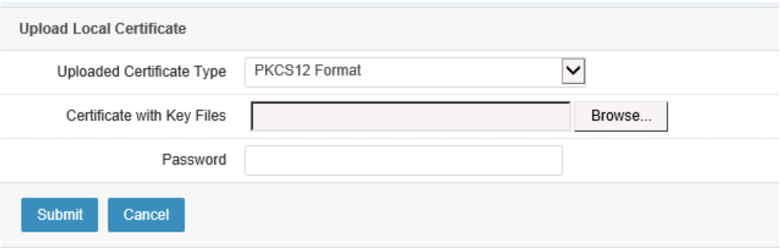
63.2.1 Configuring a Local Certificate

Upload a certificate as follows:

1. Choose **Object** > **CA certificate** > **Local certificate**, and click **Import local certificate**.

Select one of the three certificate formats.

Import a PKCS12 certificate.


Upload Local Certificate

Uploaded Certificate Type: PKCS12 Format

Certificate with Key Files:

Password:

Parameter description:

Uploaded certificate type: The options are **PKCS12 format**, **Certificate-key separation**, and **Certificate chain**.

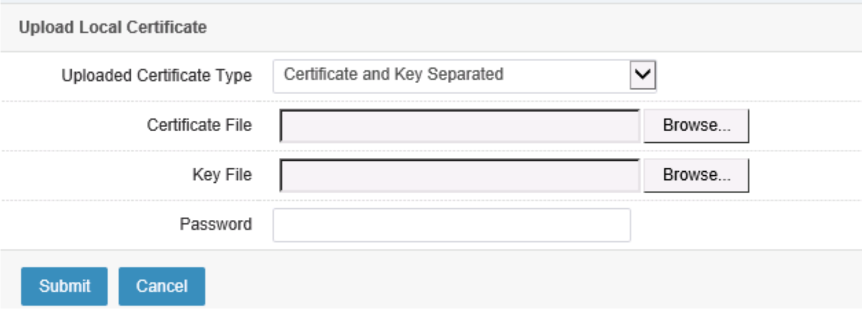
Certificate with key file: Select a PKCS12 file.

Password: Password of the digital certificate.

Note

To ensure key security, check that the imported PKCS12 certificate is protected by a password.

Import a certificate with certificate-key separation.


Upload Local Certificate

Uploaded Certificate Type: Certificate and Key Separated

Certificate File:

Key File:

Password:

Parameter description:

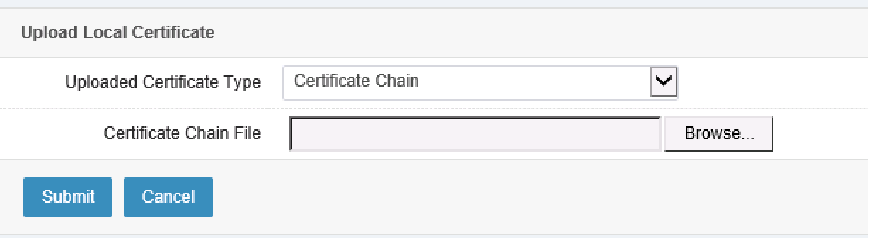
Uploaded certificate type: The options are **PKCS12 format**, **Certificate-key separation**, and **Certificate chain**.

Certificate file: Select the digital certificate file.

Key file: Select the private key file for the digital certificate.

Password: Password of the digital certificate.

Import a certificate chain.



Upload Local Certificate

Uploaded Certificate Type	Certificate Chain
Certificate Chain File	

Parameter description:

Uploaded certificate type: The options are **PKCS12 format**, **Certificate-key separation**, and **Certificate chain**.

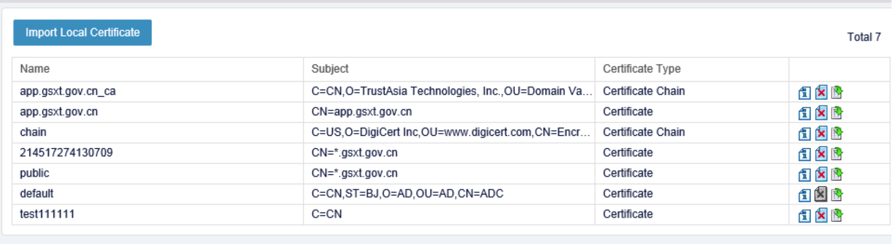
Certificate chain file: Select the certificate chain file.

2. Click **Submit**.

Display certificates as follows:

1. Choose **Object** > **CA certificate** > **Local certificate**.

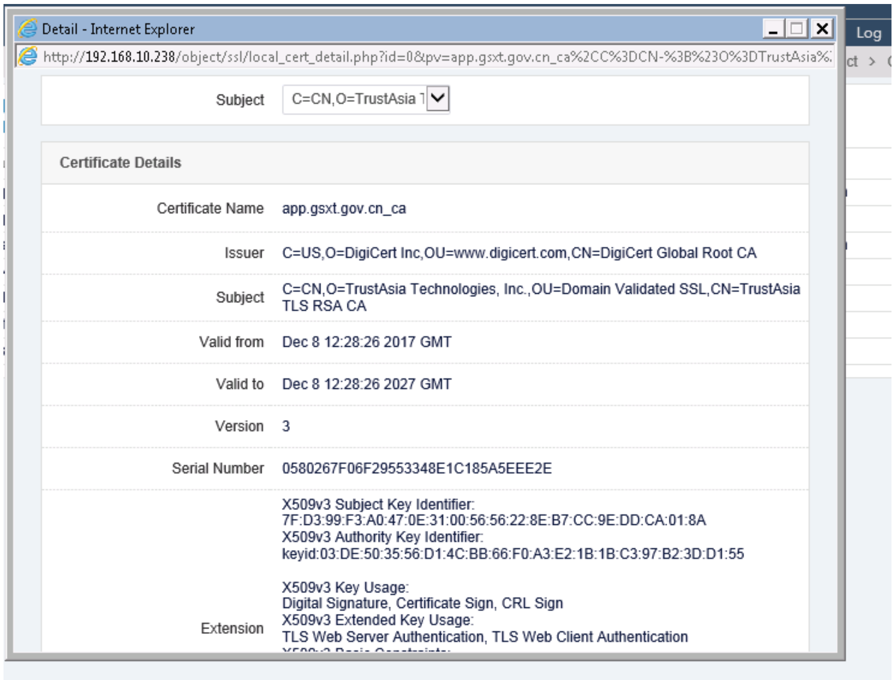
A page appears to display imported digital certificates.



Total 7

Name	Subject	Certificate Type	
app.gsxt.gov.cn_ca	C=CN,O=TrustAsia Technologies, Inc.,OU=Domain Va...	Certificate Chain	
app.gsxt.gov.cn	CN=app.gsxt.gov.cn	Certificate	
chain	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=Encr...	Certificate Chain	
214517274130709	CN=*.gsxt.gov.cn	Certificate	
public	CN=*.gsxt.gov.cn	Certificate	
default	C=CN,ST=BJ,O=AD,OU=AD,CN=ADC	Certificate	
test111111	C=CN	Certificate	

2. Click ⓘ to display the information about a certificate.



Detail - Internet Explorer
http://192.168.10.238/object/ssl/local_cert_detail.php?id=0&pv=app.gsxt.gov.cn_ca%2CC%3DCN-%3B%23O%3DTrustAsia%
Log

Subject: C=CN,O=TrustAsia T

Certificate Details

Certificate Name	app.gsxt.gov.cn_ca
Issuer	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=DigiCert Global Root CA
Subject	C=CN,O=TrustAsia Technologies, Inc.,OU=Domain Validated SSL,CN=TrustAsia TLS RSA CA
Valid from	Dec 8 12:28:26 2017 GMT
Valid to	Dec 8 12:28:26 2027 GMT
Version	3
Serial Number	0580267F06F29553348E1C185A5EEE2E
Extension	X509v3 Subject Key Identifier: 7F:D3:99:F3:A0:47:0E:31:00:56:56:22:8E:B7:CC:9E:DD:CA:01:8A X509v3 Authority Key Identifier: keyid:03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 X509v3 Key Usage: Digital Signature, Certificate Sign, CRL Sign X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication

Parameter description:

Subject: Certificate subject list. For a certificate chain, you can select multiple subjects from the drop-down list to switch certificates.

Certificate name: Name of a certificate.

Issuer: Issuer of the certificate.

Subject: Subject of the certificate.

Start time: Time when the certificate takes effect.

End time: Time when the certificate expires.

Version: Version of the certificate.

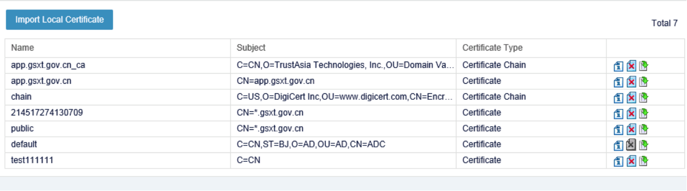
SN: SN of the certificate.

Extension: Extended information about the certificate.

Export a certificate as follows:

1. Choose **Object** > **CA certificate** > **Local certificate**.

A page appears to display imported digital certificates.



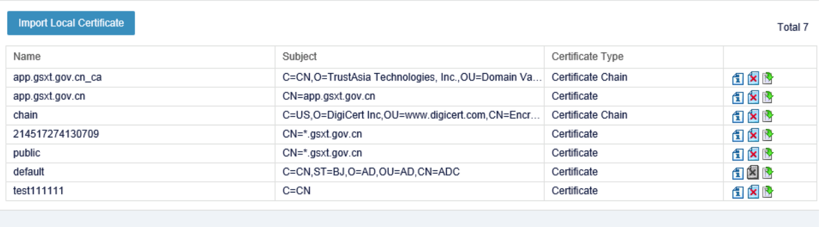
Name	Subject	Certificate Type	
app.gsxt.gov.cn_ca	C=CN,O=TrustAsia Technologies, Inc.,OU=Domain Va...	Certificate Chain	
app.gsxt.gov.cn	CN=app.gsxt.gov.cn	Certificate	
chain	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=Encr...	Certificate Chain	
214517274130709	CN=*.gsxt.gov.cn	Certificate	
public	CN=*.gsxt.gov.cn	Certificate	
default	C=CN,ST=BJ,O=AD,OU=AD,CN=ADC	Certificate	
test111111	C=CN	Certificate	

1. Click to export a certificate. In the displayed dialog box, select a path to save the certificate and click **OK**.

Delete a certificate as follows:

2. Choose **Object** > **CA certificate** > **Local certificate**.

A page appears to display imported digital certificates.



Import Local Certificate

Total 7

Name	Subject	Certificate Type	
app.gsxt.gov.cn_ca	C=CN,O=TrustAsia Technologies, Inc.,OU=Domain Va...	Certificate Chain	
app.gsxt.gov.cn	CN=app.gsxt.gov.cn	Certificate	
chain	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=Encr...	Certificate Chain	
214517274130709	CN=*.gsxt.gov.cn	Certificate	
public	CN=*.gsxt.gov.cn	Certificate	
default	C=CN,ST=BJ,O=AD,OU=AD,CN=ADC	Certificate	
test111111	C=CN	Certificate	

3. Click to delete a certificate.

4. Click **OK**.

Note

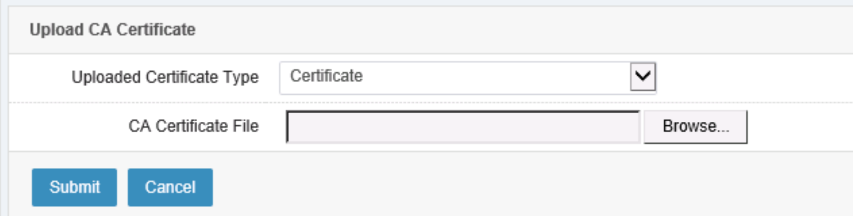
If the **Delete** button is grayed out , the certificate is referenced or it is a default certificate and cannot be deleted.

63.2.2 Configuring a CA Certificate

Upload a certificate as follows:

1. Choose **Object** > **CA certificate** > **CA**. Click **Import CA center certificate**. CA certificates can be uploaded in two ways.

Import a single CA certificate as follows:



Upload CA Certificate

Uploaded Certificate Type	Certificate
CA Certificate File	Browse...

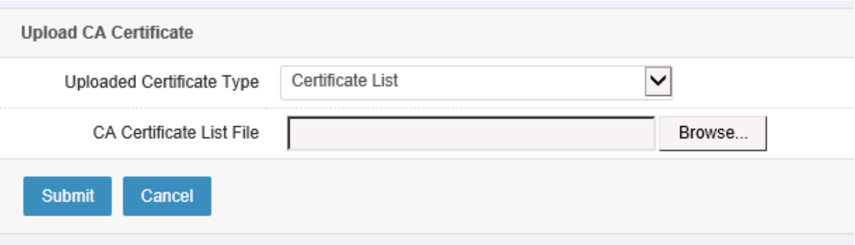
Submit Cancel

Parameter description:

Uploaded certificate type: The options are **Certificate** and **Certificate set**.

CA certificate file: Select the CA certificate file to be uploaded.

Import a CA certificate set as follows:



Upload CA Certificate

Uploaded Certificate Type	Certificate List
CA Certificate List File	

Parameter description:

Uploaded certificate type: The options are **Certificate** and **Certificate set**.

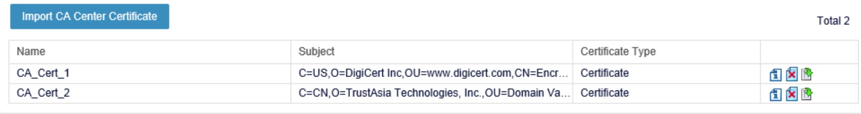
CA certificate set file: Select the CA certificate set file to be uploaded.

2. Click **Submit**.

Display certificates as follows:

1. Choose **Object** > **CA certificate** > **CA**.

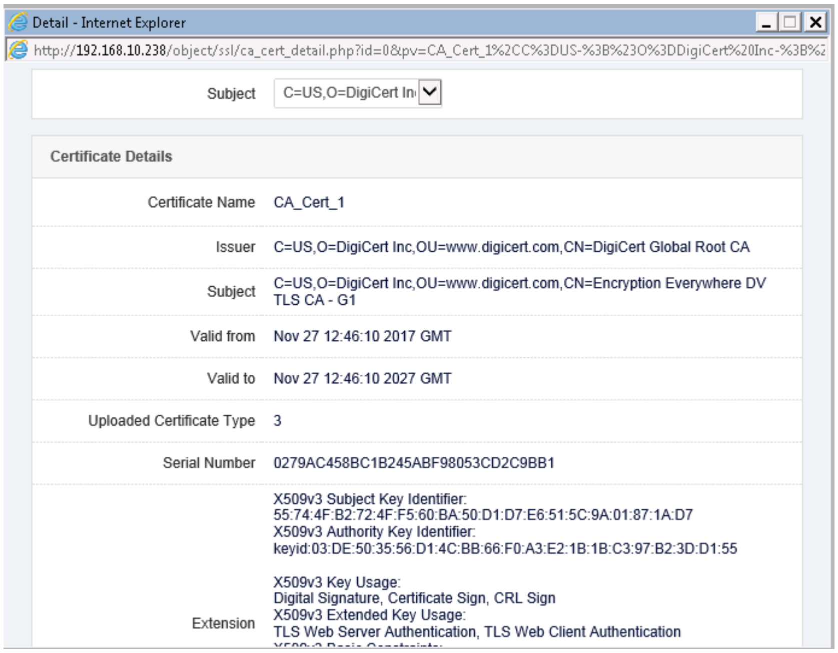
A page appears to display imported CA certificates.



Total 2

Name	Subject	Certificate Type	
CA_Cert_1	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=Encr...	Certificate	ℹ ☒ 📄
CA_Cert_2	C=CN,O=TrustAsia Technologies, Inc.,OU=Domain Va...	Certificate	ℹ ☒ 📄

2. Click ℹ to display the information about a CA certificate.



http://192.168.10.238/object/ssl/ca_cert_detail.php?id=0&pv=CA_Cert_1%2CC%3DUS-%3B%23O%3DDigiCert%20Inc-%3B%2

Subject	C=US,O=DigiCert In

Certificate Details

Certificate Name	CA_Cert_1
Issuer	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=DigiCert Global Root CA
Subject	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=Encryption Everywhere DV TLS CA - G1
Valid from	Nov 27 12:46:10 2017 GMT
Valid to	Nov 27 12:46:10 2027 GMT
Uploaded Certificate Type	3
Serial Number	0279AC458BC1B245ABF98053CD2C9BB1
Extension	X509v3 Subject Key Identifier: 55:74:4F:B2:72:4F:F5:60:BA:50:D1:D7:E6:51:5C:9A:01:87:1A:D7 X509v3 Authority Key Identifier: keyid:03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 X509v3 Key Usage: Digital Signature, Certificate Sign, CRL Sign X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints:

Parameter description:

Subject: Certificate subject list. For a CA certificate set, you can select a subject from the drop-down list to switch certificates.

Certificate name: Name of a certificate.

Issuer: Issuer of the certificate.

Subject: Subject of the certificate.

Start time: Time when the certificate takes effect.

End time: Time when the certificate expires.

Version: Version of the certificate.

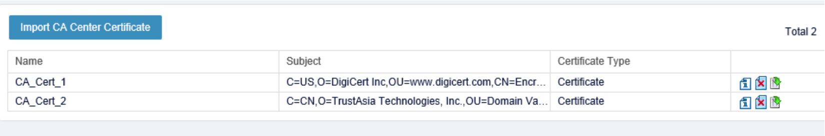
SN: SN of the certificate.

Extension: Extended information about the certificate.

Export a certificate as follows:

1. Choose **Object** > **CA certificate** > **CA**.

A page appears to display imported CA certificates.



Import CA Center Certificate

Total 2

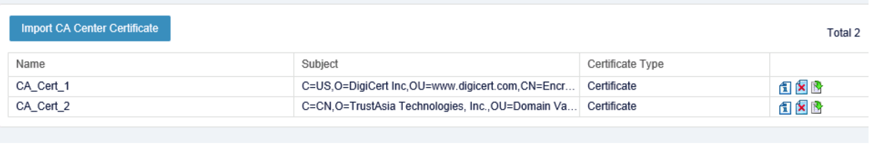
Name	Subject	Certificate Type	
CA_Cert_1	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=Encr...	Certificate	ⓘ ☒ 📤
CA_Cert_2	C=CN,O=TrustAsia Technologies, Inc.,OU=Domain Va...	Certificate	ⓘ ☒ 📤

2. Click 📤 to export a certificate. In the displayed dialog box, select a path to save the certificate and click **OK**.

Delete a certificate as follows:

1. Choose **Object** > **CA certificate** > **CA**.

A page appears to display imported CA certificates.



Import CA Center Certificate

Total 2

Name	Subject	Certificate Type	
CA_Cert_1	C=US,O=DigiCert Inc,OU=www.digicert.com,CN=Encr...	Certificate	ⓘ ☒ 📤
CA_Cert_2	C=CN,O=TrustAsia Technologies, Inc.,OU=Domain Va...	Certificate	ⓘ ☒ 📤

2. Click ☒ to delete a certificate.

3. Click **OK**.

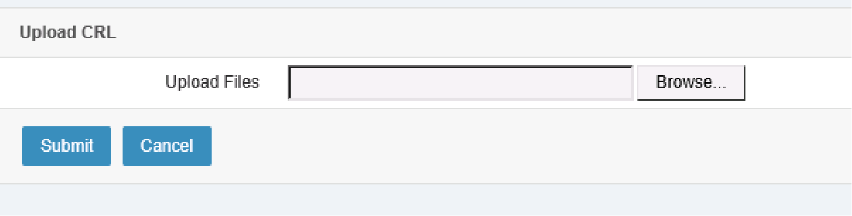
Note

If the **Delete** button is grayed out ☒, the certificate is referenced and cannot be deleted.

63.2.3 Configuring a CRL Certificate

Upload a CRL certificate as follows:

1. Choose **Object** > **CA certificate** > **CRL**, and click **Import CRL**.



Upload CRL

Upload Files	Browse...

Submit Cancel

Parameter description:

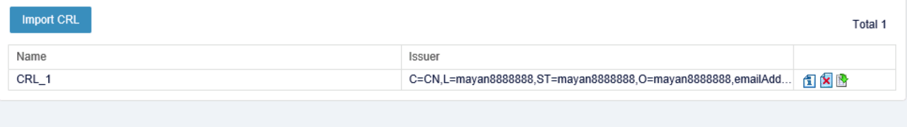
Upload file: Select the CRL certificate file to be uploaded.

2. Click **Submit**.

Display CRL certificates as follows:

1. Choose **Object** > **CA certificate** > **CRL**.

A page appears to display imported CRL certificates.

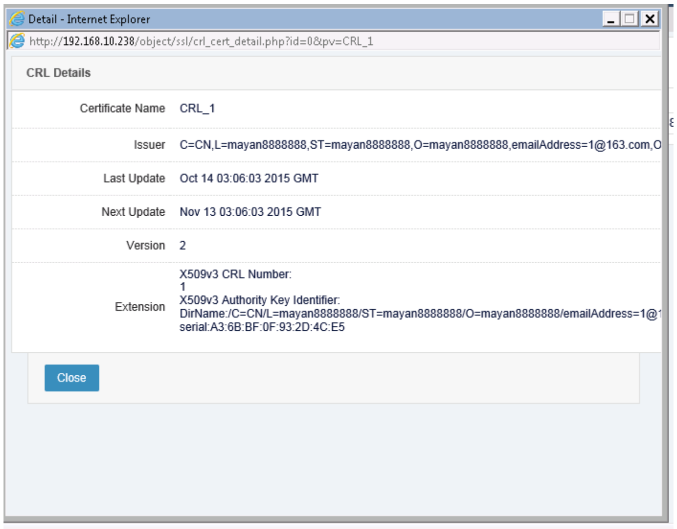


Import CRL

Total 1

Name	Issuer	
CRL_1	C=CN,L=mayan8888888,ST=mayan8888888,O=mayan8888888,emailAdd...	

2. Click ℹ to display the information about a CRL certificate.



Detail - Internet Explorer

http://192.168.10.238/object/ssl/crl_cert_detail.php?id=0&pv=CRL_1

CRL Details

Certificate Name	CRL_1
Issuer	C=CN,L=mayan8888888,ST=mayan8888888,O=mayan8888888,emailAddress=1@163.com,O
Last Update	Oct 14 03:06:03 2015 GMT
Next Update	Nov 13 03:06:03 2015 GMT
Version	2
Extension	X509v3 CRL Number: 1 X509v3 Authority Key Identifier: DirName:/C=CN/L=mayan8888888/ST=mayan8888888/O=mayan8888888/emailAddress=1@1 serial:A3:6B:BF:0F:93:2D:4C:E5

Close

Parameter description:

Certificate name: Name of a certificate.

Issuer: Issuer of the certificate.

Last update: Time when the certificate was last updated.

Next update: Time when the certificate will be updated next time.

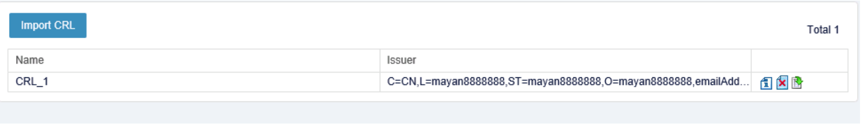
Version: Version of the certificate.

Extension: Extended information about the certificate.

Export a CRL certificate as follows:

1. Choose **Object** > **CA certificate** > **CRL**.

A page appears to display imported CRL certificates.



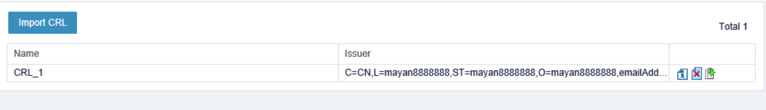
Name	Issuer	
CRL_1	C=CN,L=mayan8888888,ST=mayan8888888,O=mayan8888888,emailAdd...	

2. Click to export a CRL certificate. In the displayed dialog box, select a path to save the certificate and click **OK**.

Delete a CRL certificate as follows:

1. Choose **Object** > **CA certificate** > **CRL**.

A page appears to display imported CRL certificates.



Name	Issuer	
CRL_1	C=CN,L=mayan8888888,ST=mayan8888888,O=mayan8888888,emailAdd...	

2. Click to delete a CRL certificate.

3. Click **OK**.

Note

If the **Delete** button is grayed out , the certificate is referenced and cannot be deleted.

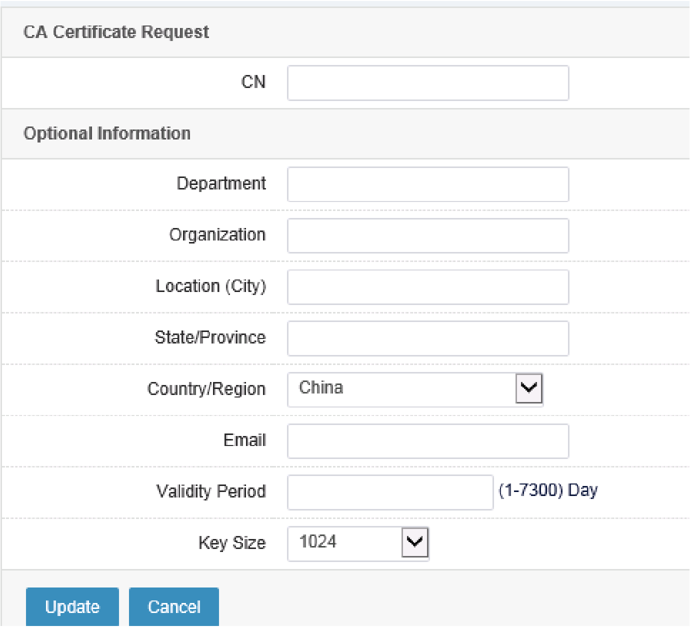
63.2.4 Configuring Root CA Certificate Management

Generate a root CA certificate as follows:

1. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.

2.Click **Generate root CA certificate**. In the displayed dialog box, confirm to overwrite the original root CA certificate. The **CA certificate request** page appears.



CA Certificate Request

CN	

Optional Information

Department	
Organization	
Location (City)	
State/Province	
Country/Region	China
Email	
Validity Period	(1-7300) Day
Key Size	1024

Parameter description:

CN: Common name of a certificate.

Department: Department for the certificate.

Organization: Organization for the certificate.

Location (city): Location of the certificate.

State/Province: State or province for the certificate.

Country/Region: Country or region for the certificate.

Email: Email address of the certificate.

Effective period: Effective period of the certificate. The value ranges from **1** to **7300**, in days.

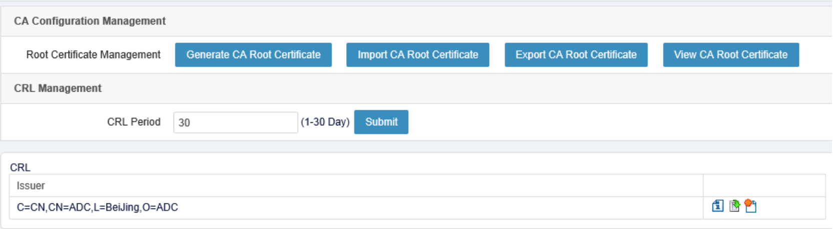
Key size: Size of the certificate key. The options are **1024** and **2048**, in bits.

3. Click **Update** to generate a root CA certificate.

Import a root CA certificate as follows:

1. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.



CA Configuration Management

Root Certificate Management

CRL Management

CRL Period 30 (1-30 Day)

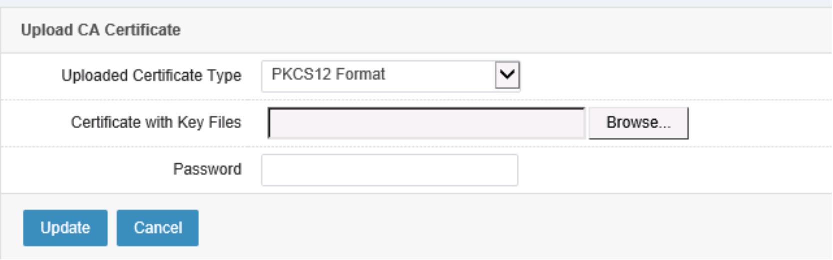
CRL

Issuer	
C=CN,CN=ADC,L=BeiJing,O=ADC	

Generate CA Root Certificate
Import CA Root Certificate
Export CA Root Certificate
View CA Root Certificate
Submit

2. Click **Import root CA certificate**. In the displayed dialog box, confirm to overwrite the original root CA certificate. The certificate import page appears. The import modes are PKCS12 format and certificate-key separation.

The following page allows you to import a root CA certificate in PKCS12 format.



Upload CA Certificate

Uploaded Certificate Type: PKCS12 Format

Certificate with Key Files

Password

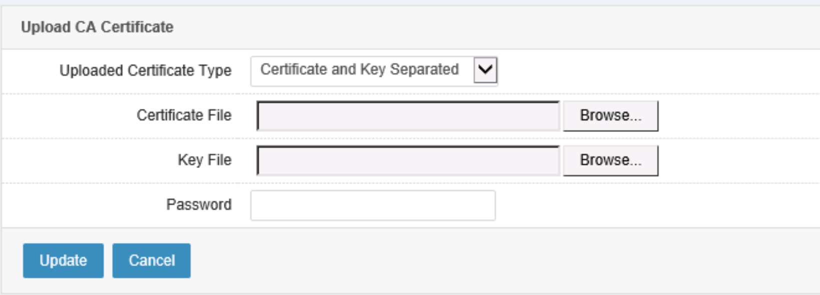
Parameter description:

Uploaded certificate type: The options are **PKCS12 format** and **Certificate-key separation**.

Certificate with key file: Select a path to save the certificate file.

Password: Password of the certificate file.

The following page allows you to import a root CA certificate with certificate-key separation.



Upload CA Certificate

Uploaded Certificate Type: Certificate and Key Separated

Certificate File: Browse...

Key File: Browse...

Password

Parameter description:

Uploaded certificate type: The options are **PKCS12 format** and **Certificate-key separation**.

Certificate file: Select a path to save the certificate file.

Key file: Select a path to save the key file.

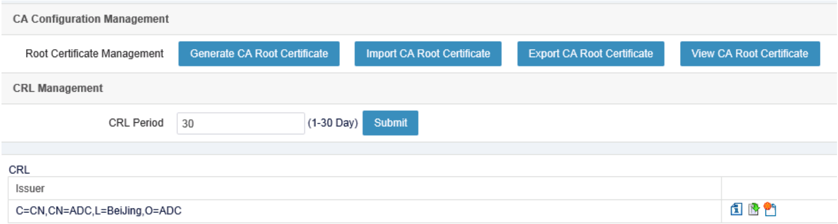
Password: Password of the key file.

1. Click **Update** to upload the root CA certificate.

Export a root CA certificate as follows:

1. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.



CA Configuration Management

Root Certificate Management

Generate CA Root Certificate
Import CA Root Certificate
Export CA Root Certificate
View CA Root Certificate

CRL Management

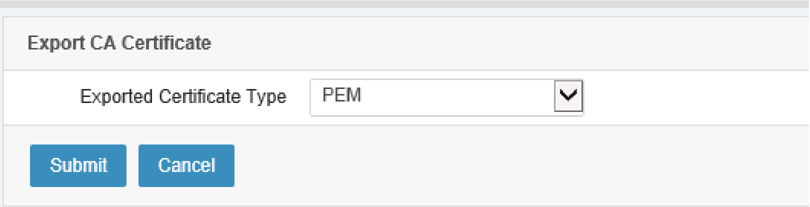
CRL Period: 30 (1-30 Day)

CRL

Issuer	
C=CN,CN=ADC,L=BeiJing,O=ADC	

2. Click **Export root CA certificate**. The **Export root CA certificate** page appears. You can export a certificate in the PEM or P12 format. A PEM certificate does not have a key file.

The following page allows you to export a PEM certificate.



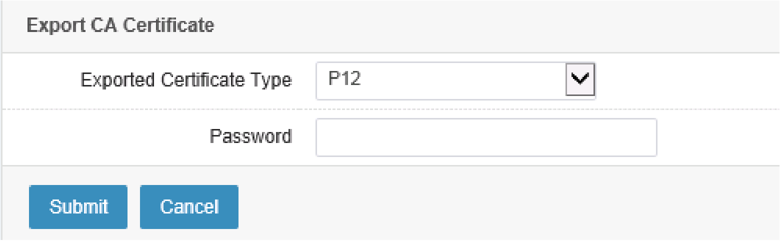
Export CA Certificate

Exported Certificate Type: PEM

Parameter description:

Exported certificate type: The options are **PEM** and **P12**.

The following page allows you to export a P12 certificate.



Export CA Certificate

Exported Certificate Type: P12

Password:

Parameter description:

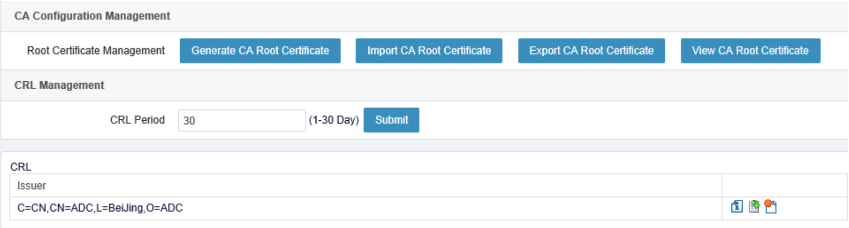
Exported certificate type: The options are **PEM** and **P12**.

Password: Password of the exported P12 certificate.

Display root CA certificates as follows:

1. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.



CA Configuration Management

Root Certificate Management

Generate CA Root Certificate
Import CA Root Certificate
Export CA Root Certificate
View CA Root Certificate

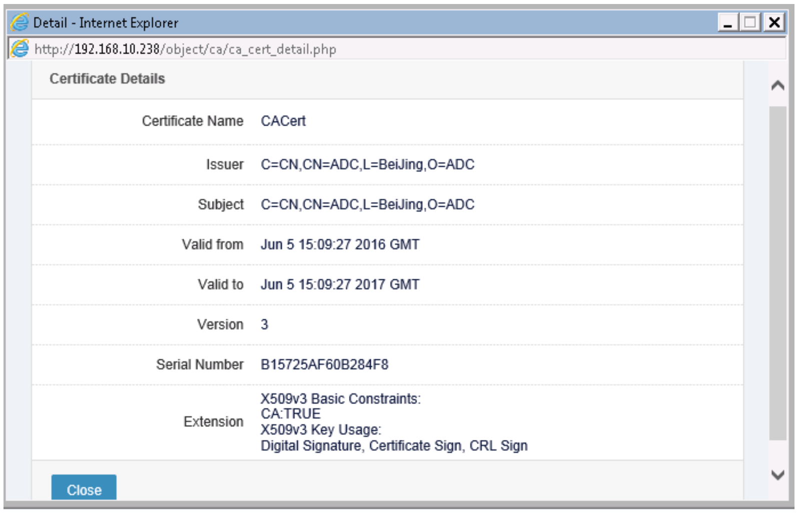
CRL Management

CRL Period: 30 (1-30 Day)

CRL

Issuer	
C=CN,CN=ADC,L=BeiJing,O=ADC	

2. Click **Show root CA certificate** to display root CA certificates.


Detail - Internet Explorer
http://192.168.10.238/object/ca/ca_cert_detail.php
Close

Certificate Details

Certificate Name	CACert
Issuer	C=CN,CN=ADC,L=BeiJing,O=ADC
Subject	C=CN,CN=ADC,L=BeiJing,O=ADC
Valid from	Jun 5 15:09:27 2016 GMT
Valid to	Jun 5 15:09:27 2017 GMT
Version	3
Serial Number	B15725AF60B284F8
Extension	X509v3 Basic Constraints: CA:TRUE X509v3 Key Usage: Digital Signature, Certificate Sign, CRL Sign

Parameter description:

Certificate name: Name of a certificate.

Issuer: Issuer of the certificate.

Subject: Subject of the certificate.

Start time: Time when the certificate takes effect.

End time: Time when the certificate expires.

Version: Version of the certificate.

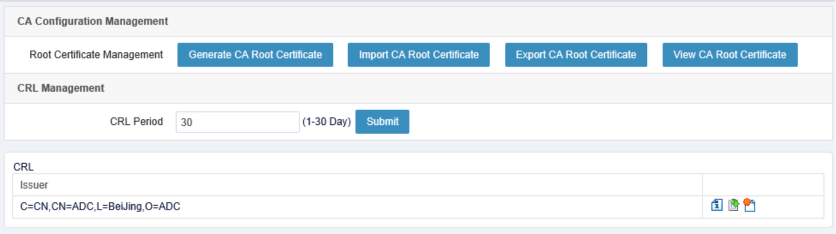
SN: SN of the certificate.

Extension: Extended information about the certificate.

Manage root CA CRL certificates as follows:

1. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.


Generate CA Root Certificate
Import CA Root Certificate
Export CA Root Certificate
View CA Root Certificate
Submit

CA Configuration Management

Root Certificate Management

CRL Management

CRL Period 30 (1-30 Day)

CRL

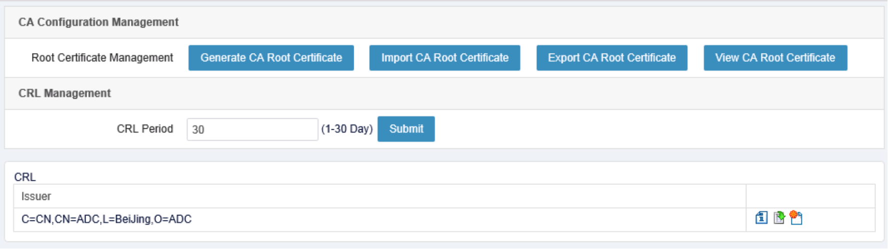
Issuer	
C=CN,CN=ADC,L=BeiJing,O=ADC	

In **CRL management**, you can set the automatic CRL update period in the range 1 to 30, in days.

Display CRL certificate details as follows:

2. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.



CA Configuration Management

Root Certificate Management: Generate CA Root Certificate | Import CA Root Certificate | Export CA Root Certificate | View CA Root Certificate

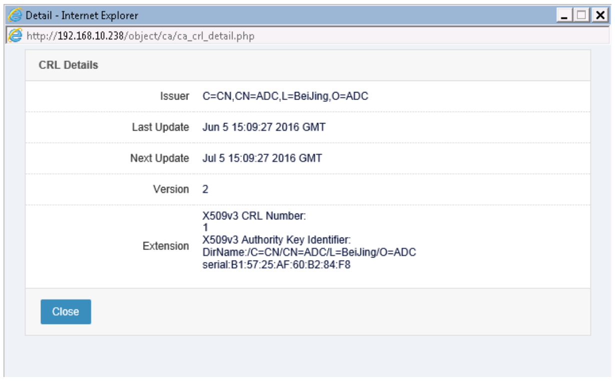
CRL Management

CRL Period: 30 (1-30 Day) Submit

CRL

Issuer	
C=CN,CN=ADC,L=BeiJing,O=ADC	

In **CRL**, click ℹ to display the details about a CRL certificate.



Detail - Internet Explorer

http://192.168.10.238/object/ca/ca_crl_detail.php

CRL Details

Issuer	C=CN,CN=ADC,L=BeiJing,O=ADC
Last Update	Jun 5 15:09:27 2016 GMT
Next Update	Jul 5 15:09:27 2016 GMT
Version	2
Extension	X509v3 CRL Number: 1 X509v3 Authority Key Identifier: DirName:/C=CN/CN=ADC/L=BeiJing/O=ADC serial:B1:57:25:AF:60:B2:84:F8

Close

Parameter description:

Issuer: Issuer of the certificate.

Last update: Time when the certificate was last updated.

Next update: Time when the certificate will be updated next time.

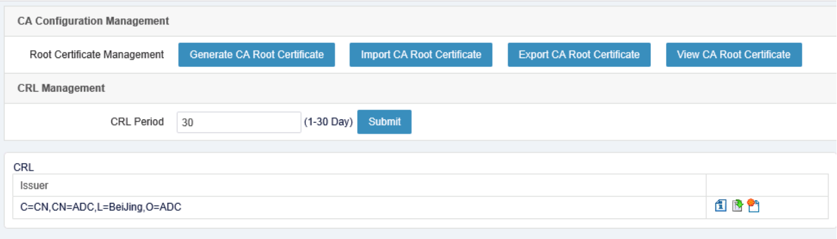
Version: Version of the certificate.

Extension: Extended information about the certificate.

Export a CRL certificate as follows:

1. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.


CA Configuration Management
Root Certificate Management
Generate CA Root Certificate
Import CA Root Certificate
Export CA Root Certificate
View CA Root Certificate
CRL Management
CRL Period
(1-30 Day)
Submit
CRL

CRL Period: 30

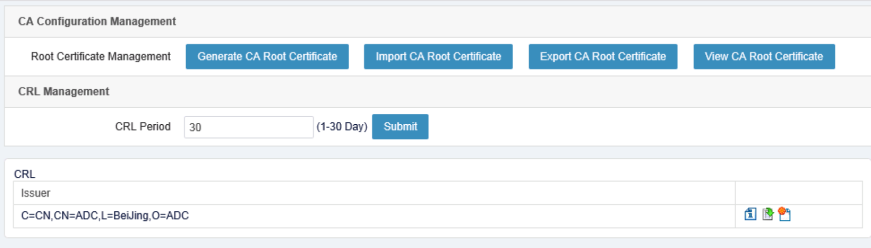
Issuer	
C=CN,CN=ADC,L=BeiJing,O=ADC	

In CRL, click to export a CRL file.

Update CRL configurations as follows:

1. Choose **Object** > **CA certificate** > **Root CA configuration management**.

The page shows the root CA configuration center.


CA Configuration Management
Root Certificate Management
Generate CA Root Certificate
Import CA Root Certificate
Export CA Root Certificate
View CA Root Certificate
CRL Management
CRL Period
(1-30 Day)
Submit
CRL

CRL Period: 30

Issuer	
C=CN,CN=ADC,L=BeiJing,O=ADC	

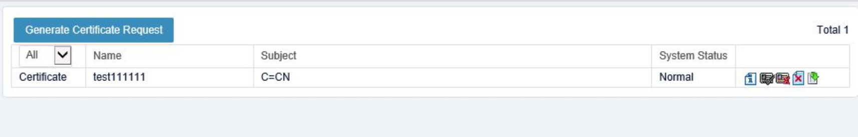
In **CRL**, click to update CRL configurations manually.

63.2.5 Configuring User Certificate Management

Generate a user certificate request as follows:

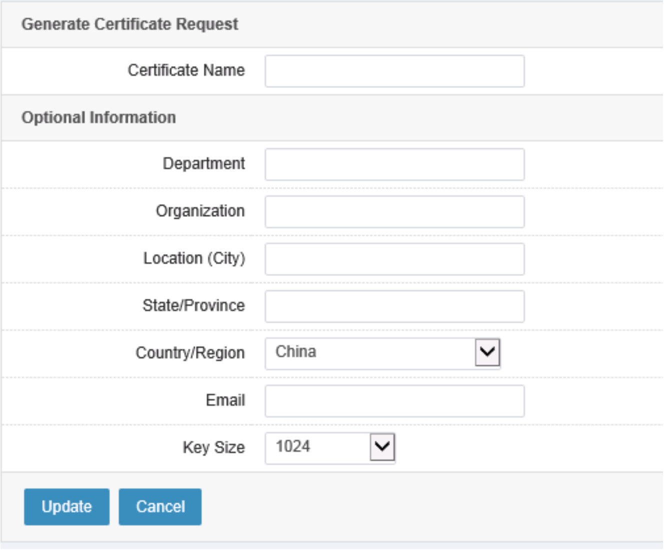
1. Choose **Object** > **CA certificate** > **User certificate management**.

A page appears to display user certificates.



All	Name	Subject	System Status	
Certificate	test111111	C=CN	Normal	

2. Click **Generate certificate request**. The certificate request configuration page appears.



Generate Certificate Request

Certificate Name	

Optional Information

Department	
Organization	
Location (City)	
State/Province	
Country/Region	China
Email	
Key Size	1024

Parameter description:

Certificate name: Common name of a certificate

Password: Password of the digital certificate.

Confirm password: Enter the password again.

Department: Department for the certificate.

Organization: Organization for the certificate.

Location (city): Location of the certificate.

State/Province: State or province for the certificate.

Country/Region: Country or region for the certificate.

Common name (domain name): Common name or domain name of the certificate.

Email: Email address of the certificate.

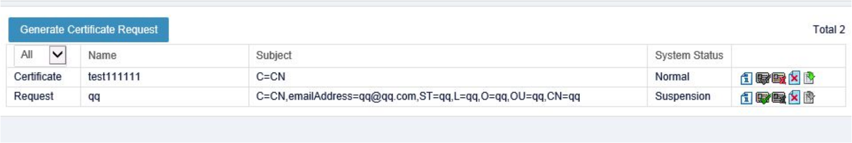
Key size: Size of the certificate key. The options are **1024** and **2048**, in bits.

3. Click **Update** to generate a certificate request.

Sign a user certificate as follows:

1. Choose **Object** > **CA certificate** > **User certificate management**.

A page appears to display user certificates.



Generate Certificate Request

Total 2

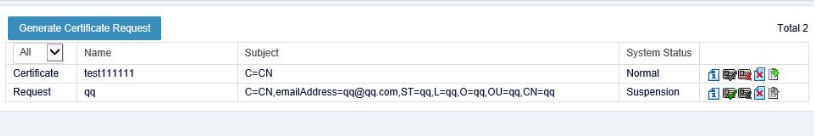
All	Name	Subject	System Status	
Certificate	test111111	C=CN	Normal	
Request	qq	C=CN,emailAddress=qq@qq.com,ST=qq,L=qq,O=qq,OU=qq,CN=qq	Suspension	

Click next to an unsigned user certificate request.

Revoke a user certificate as follows:

1. Choose **Object** > **CA certificate** > **User certificate management**.

A page appears to display user certificates.

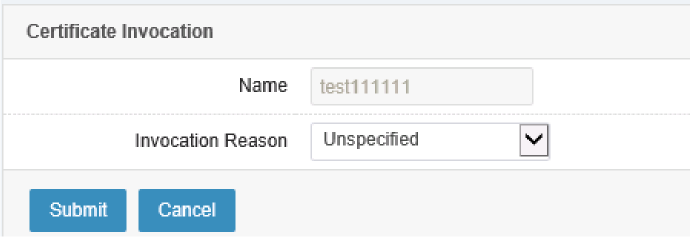


Generate Certificate Request

Total 2

All	Name	Subject	System Status	
Certificate	test111111	C=CN	Normal	
Request	qq	C=CN,emailAddress=qq@qq.com,ST=qq,L=qq,O=qq,OU=qq,CN=qq	Suspension	

Click next to a normal user certificate. The certificate revocation page appears.



Certificate Invocation

Name: test111111

Invocation Reason: Unspecified

Parameter description:

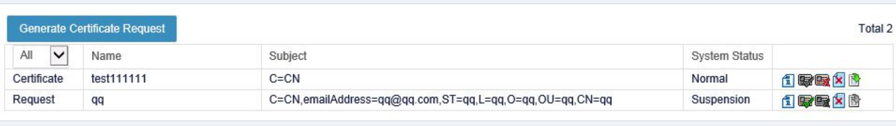
Revocation reason: Reason to revoke the certificate. The options are **Unspecified**, **Key leaked**, **CA key leaked**, and **Dependency changed**.

2. Click **Submit**.

Delete a user certificate as follows:

1. Choose **Object** > **CA certificate** > **User certificate management**.

A page appears to display user certificates.



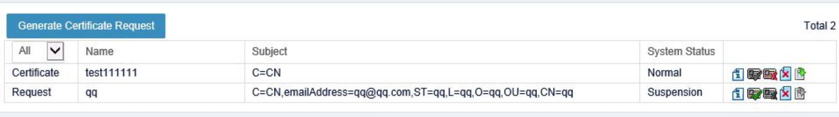
All	Name	Subject	System Status	
Certificate	test111111	C=CN	Normal	
Request	qq	C=CN,emailAddress=qq@qq.com,ST=qq,L=qq,O=qq,OU=qq,CN=qq	Suspension	

Click ☒ next to the certificate or certificate request you want to delete.

Display user certificate information as follows:

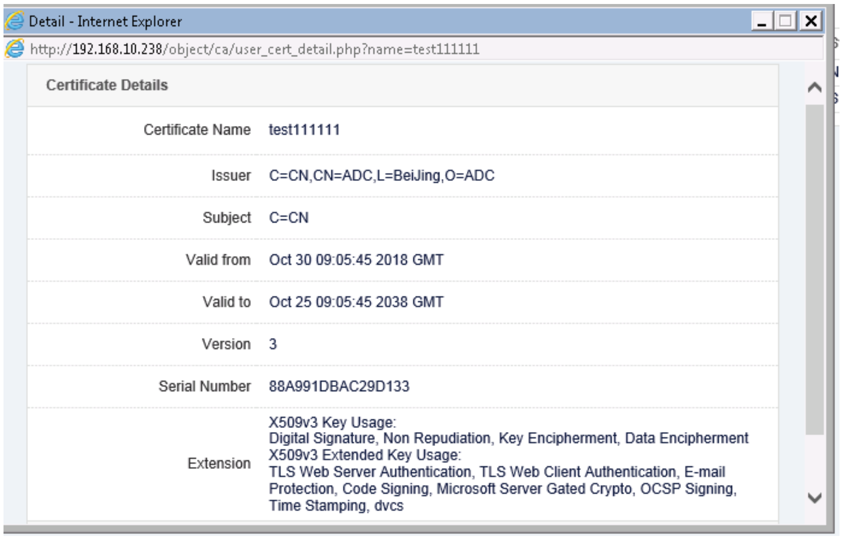
1. Choose **Object** > **CA certificate** > **User certificate management**.

A page appears to display user certificates.



All	Name	Subject	System Status	
Certificate	test111111	C=CN	Normal	
Request	qq	C=CN,emailAddress=qq@qq.com,ST=qq,L=qq,O=qq,OU=qq,CN=qq	Suspension	

Click ℹ next to the certificate or certificate request you want to check.



Detail - Internet Explorer
http://192.168.10.238/object/ca/user_cert_detail.php?name=test111111

Certificate Details

Certificate Name	test111111
Issuer	C=CN,CN=ADC,L=BeiJing,O=ADC
Subject	C=CN
Valid from	Oct 30 09:05:45 2018 GMT
Valid to	Oct 25 09:05:45 2038 GMT
Version	3
Serial Number	88A991DBAC29D133
Extension	X509v3 Key Usage: Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication, E-mail Protection, Code Signing, Microsoft Server Gated Crypto, OCSP Signing, Time Stamping, dvcs

Parameter description:

Certificate name: Name of a certificate.

Issuer: Issuer of the certificate.

Subject: Subject of the certificate.

Start time: Time when the certificate takes effect.

End time: Time when the certificate expires.

Version: Version of the certificate.

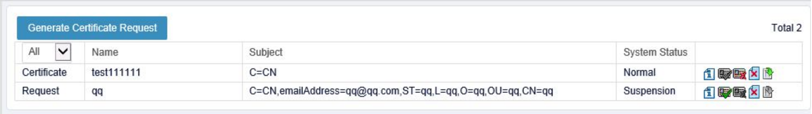
SN: SN of the certificate.

Extension: Extended information about the certificate.

Export a user certificate as follows:

1. Choose **Object** > **CA certificate** > **User certificate management**.

A page appears to display user certificates.



Generate Certificate Request

Total 2

All	Name	Subject	System Status	
Certificate	test111111	C=CN	Normal	
Request	qq	C=CN,emailAddress=qq@qq.com,ST=qq,L=qq,O=qq,OU=qq,CN=qq	Suspension	

Click next to a normal certificate you want to export.

63.3 Configuration Example

Description:

Upload a local certificate and the corresponding certificate chain. The local certificate is signed by the intermediate CA, which is signed by the root CA.

Method:

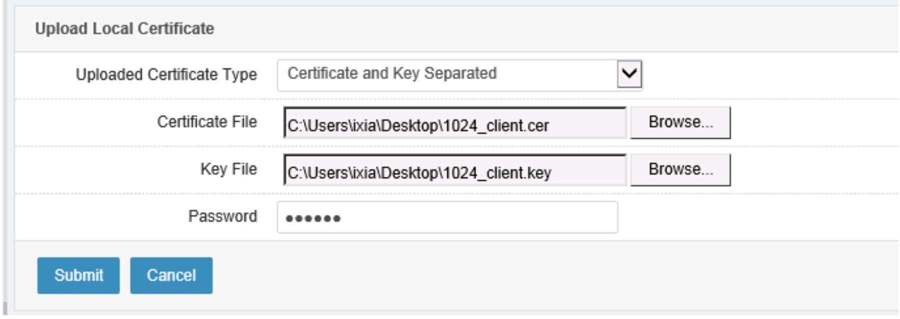
To ensure that the certificate is signed by the root CA, you must upload a digital certificate and a certificate chain (root CA certificate and intermediate CA certificate).

Procedure:

1. Obtain a root CA certificate and an intermediate CA certificate, and prepare a certificate chain based on the two certificates.

2. Choose **Object** > **CA certificate** > **Local certificate**.

3. Click **Import local certificate**. Import a local certificate in the specified format.

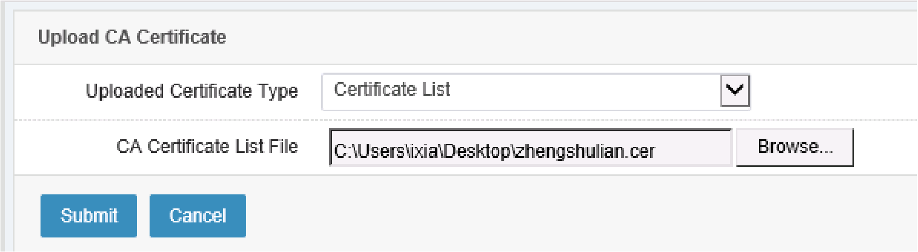


Upload Local Certificate

Uploaded Certificate Type	Certificate and Key Separated
Certificate File	C:\Users\ixia\Desktop\1024_client.cer
Key File	C:\Users\ixia\Desktop\1024_client.key
Password	••••••

4. Choose **Object** > **CA certificate** > **CA**.

5. Click **Import CA center certificate**. Import the certificate chain file to the CA.


Upload CA Certificate

Uploaded Certificate Type: Certificate List

CA Certificate List File: C:\Users\ixia\Desktop\zhengshulian.cer

63.4 Troubleshooting

63.4.1 Failed to Import a Certificate Chain

Symptom	A certificate chain fails to be imported.
Analysis	1. The certificate chain is incorrect. 2. The certificate chain does not have a root CA certificate.
Solution	1. Check that each level of the certificate chain can be verified. 2. Check that the certificate chain has a root CA certificate.

64 Log Management

64.1 Overview

The logs displayed on RAVEN5000 firewalls are classified into five categories: system event, audit event, VPN event, configuration audit, and security event. Local logs and email logs are provided in the standard syslog format, allowing you to monitor the system operating status.

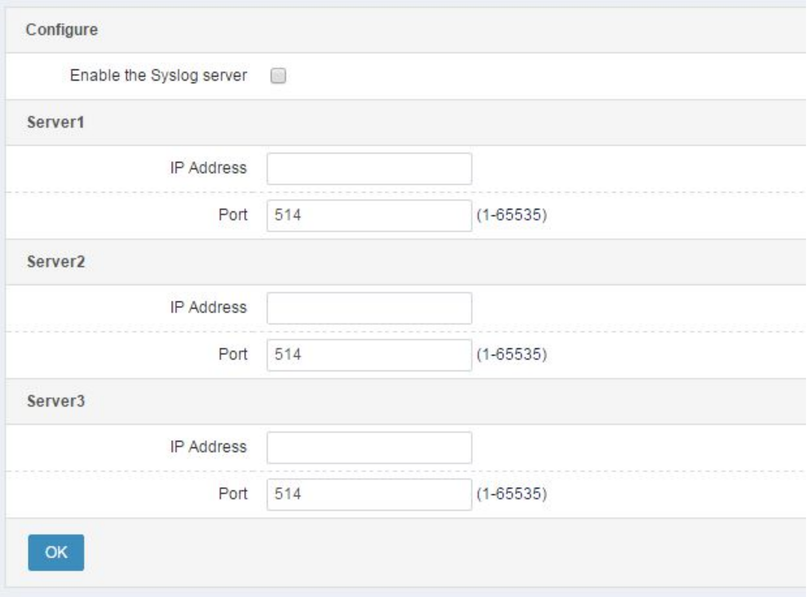
64.2 Configuration

64.2.1 Default Configurations

Parameter	Default Value	Remarks
Local log filter	Disabled	The default value can be changed.
Email log filter	Disabled	The default value can be changed.
Syslog filter	Disabled	The default value can be changed.
Syslog server	Disabled	The default value can be changed.
Syslog server port	514	The default value can be changed.

64.2.2 Configuring a Syslog Server

Choose **Log** > **Log management** > **Log server**. The following page appears.



Configure

Enable the Syslog server □

Server1

IP Address

Port 514 (1-65535)

Server2

IP Address

Port 514 (1-65535)

Server3

IP Address

Port 514 (1-65535)

Parameter description:

Enable syslog server: Check this box to enable a syslog server.

IP address: IP address of the syslog server.

Port: Port number of the syslog server.

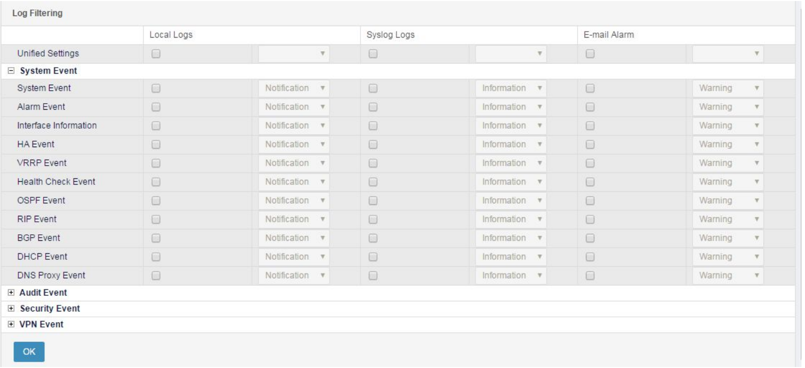
Server 1, **Server 2**, and **Server 3** indicate the syslog servers that can receive logs. They are independent of each other.

Procedure:

1. Set **IP address**.
2. Set **Port**.
3. Check the **Enable syslog server** box.
4. Click **OK**.

64.3 Configuring Log Filter

Choose **Log** > **Log management** > **Log filter**. The following page appears.



Log Filtering

	Local Logs		Syslog Logs		E-mail Alarm	
Unified Settings	□	▾	□	▾	□	▾
⊟ System Event						
System Event	□	Notification ▾	□	Information ▾	□	Warning ▾
Alarm Event	□	Notification ▾	□	Information ▾	□	Warning ▾
Interface Information	□	Notification ▾	□	Information ▾	□	Warning ▾
HA Event	□	Notification ▾	□	Information ▾	□	Warning ▾
VRRP Event	□	Notification ▾	□	Information ▾	□	Warning ▾
Health Check Event	□	Notification ▾	□	Information ▾	□	Warning ▾
OSPF Event	□	Notification ▾	□	Information ▾	□	Warning ▾
RIP Event	□	Notification ▾	□	Information ▾	□	Warning ▾
BGP Event	□	Notification ▾	□	Information ▾	□	Warning ▾
DHCP Event	□	Notification ▾	□	Information ▾	□	Warning ▾
DNS Proxy Event	□	Notification ▾	□	Information ▾	□	Warning ▾
⊞ Audit Event						
⊞ Security Event						
⊞ VPN Event						

Parameter description:

Module name: Name of a module.

Local log: Check this box to enable the local log feature and the log level.

Syslog: Check this box to enable the syslog feature and the log level.

Email log: Check this box to enable the email log feature and the log level.

Procedure:

1. Select a module, and enable the local log feature and the log level.
2. Select a module, and enable the syslog feature and the log level.
3. Select a module, and enable the email log feature and the log level.
4. Click **OK**.

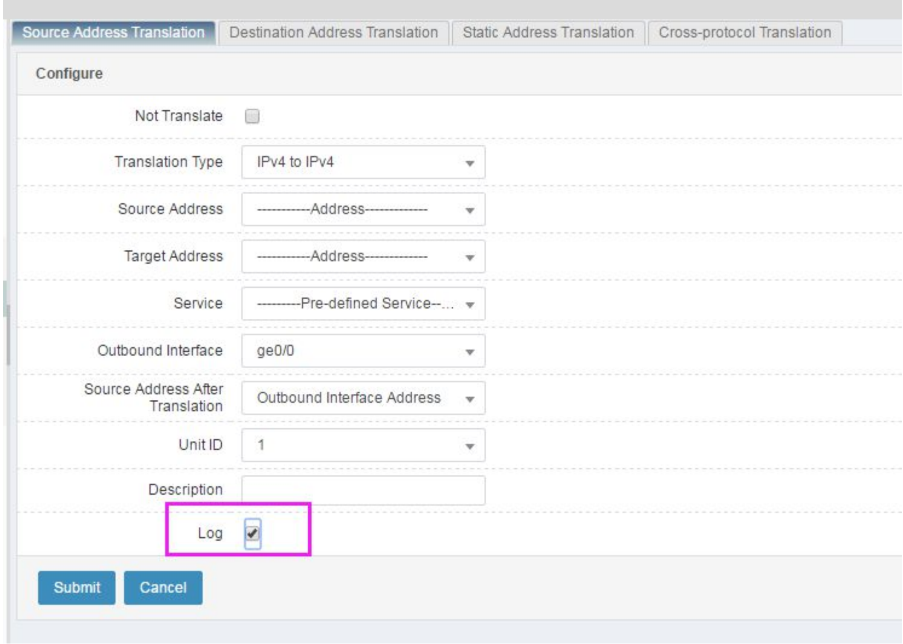
Note

1. Log filter takes effect for logs at the specified level and above.
2. Log filter only covers some of the modules that send logs.

64.4 Precautions on Log Configuration for Some Modules

For some modules, logs can be generated only after log filter is enabled and logging is also enabled in the module.

NAT (info level): To report NAT logs, you must enable NAT logging in log filter and enable logging in NAT configuration. Only logs of the Info level are reported. See the following figure.


Source Address Translation
Destination Address Translation
Static Address Translation
Cross-protocol Translation
Configure

Not Translate ☐

Translation Type: IPv4 to IPv4

Source Address: -----------Address------------

Target Address: -----------Address------------

Service: ---------Pre-defined Service--...

Outbound Interface: ge0/0

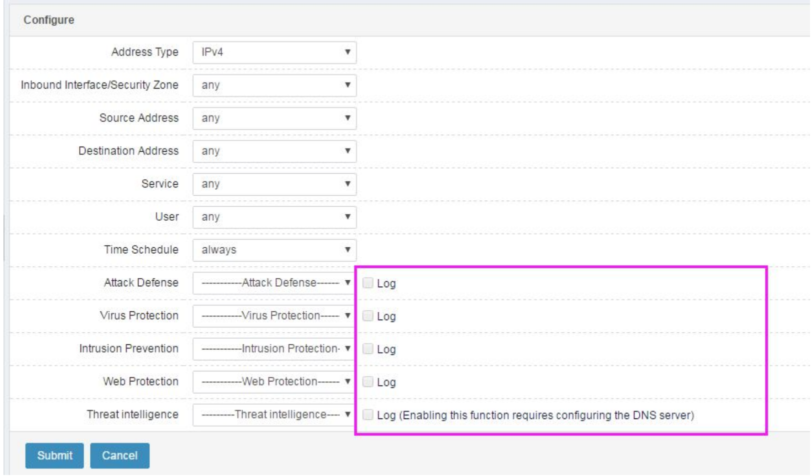
Source Address After Translation: Outbound Interface Address

Unit ID: 1

Description:

Log ☑

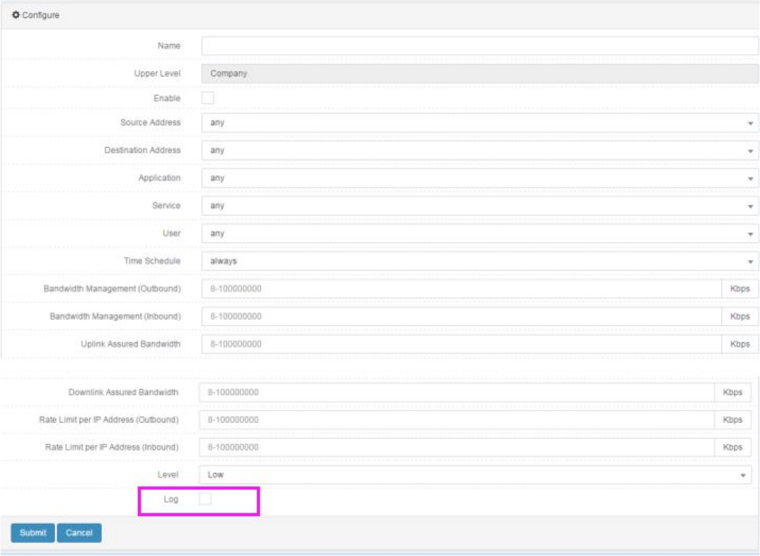
For anti-attack, antivirus, intrusion prevention, and web protection, you must enable logging in protection policies.



Configure

Address Type	IPv4 ▾	
Inbound Interface/Security Zone	any ▾	
Source Address	any ▾	
Destination Address	any ▾	
Service	any ▾	
User	any ▾	
Time Schedule	always ▾	
Attack Defense	-----------Attack Defense------ ▾	□ Log
Virus Protection	-----------Virus Protection----- ▾	□ Log
Intrusion Prevention	-----------Intrusion Protection- ▾	□ Log
Web Protection	-----------Web Protection------ ▾	□ Log
Threat intelligence	---------Threat intelligence---- ▾	□ Log (Enabling this function requires configuring the DNS server)

For QoS (flow control) policies, you must enable logging during policy configuration.



Configure

Name		
Upper Level	Company	
Enable	□	
Source Address	any ▾	
Destination Address	any ▾	
Application	any ▾	
Service	any ▾	
User	any ▾	
Time Schedule	always ▾	
Bandwidth Management (Outbound)	8-100000000	Kbps
Bandwidth Management (Inbound)	8-100000000	Kbps
Uplink Assured Bandwidth	8-100000000	Kbps
Downlink Assured Bandwidth	8-100000000	Kbps
Rate Limit per IP Address (Outbound)	8-100000000	Kbps
Rate Limit per IP Address (Inbound)	8-100000000	Kbps
Level	Low ▾	
Log	□	

For application control, web control, and session control, you must enable logging internally.

64.5 Monitoring and Maintenance

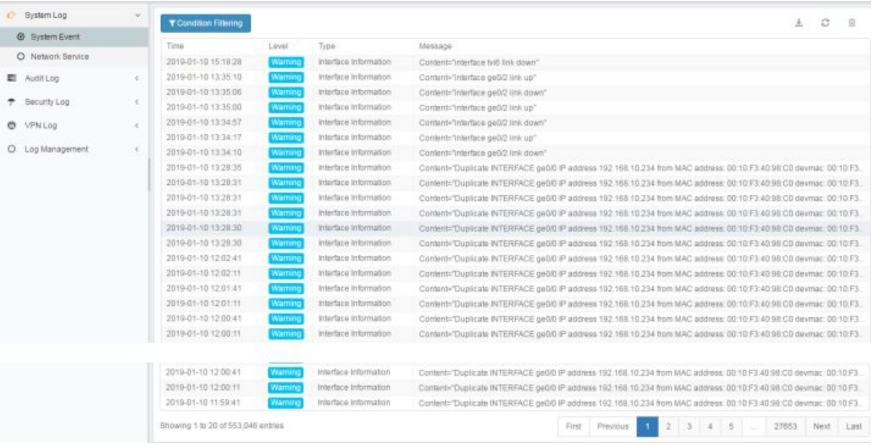
64.5.1 Displaying Logs

The logs displayed on RAVEN5000 firewalls are classified into five categories: system log, audit log, VPN log, configuration audit, and security log. System logs include system events and network services. Audit logs include NAT events, flow control, application control, web control, session control, and web authentication. Security logs include firewall policies and anti-attack. Anti-attack logs are classified into anti-flood, anti-scan, antivirus, intrusion prevention, web protection, anti-DDoS, anti-ARP attack, and blacklist. To view logs of a specific category, select the category in **Log**. On the category tab, you can set filter criteria to display logs of a specific level that are generated for a log module during a specified period.

You can view and modify the log content and settings of configuration audit only as an audit user.

The log feature and format are the same for system logs, audit logs, security logs, VPN logs, and configuration audit. System logs are used as an example.

Choose **Log** > **System log** > **System event**. The following page appears.



Time	Level	Type	Message
2019-01-10 15:18:28	Warning	Interface Information	Content="interface tvi6 link down"
2019-01-10 13:35:10	Warning	Interface Information	Content="interface ge0/2 link up"
2019-01-10 13:35:06	Warning	Interface Information	Content="interface ge0/2 link down"
2019-01-10 13:35:00	Warning	Interface Information	Content="interface ge0/2 link up"
2019-01-10 13:34:57	Warning	Interface Information	Content="interface ge0/2 link down"
2019-01-10 13:34:17	Warning	Interface Information	Content="interface ge0/2 link up"
2019-01-10 13:34:10	Warning	Interface Information	Content="interface ge0/2 link down"
2019-01-10 13:28:35	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 13:28:31	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 13:28:31	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 13:28:31	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 13:28:30	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 13:28:30	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:02:41	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:02:11	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:01:41	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:01:11	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:00:41	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:00:11	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:00:41	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 12:00:11	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...
2019-01-10 11:59:41	Warning	Interface Information	Content="Duplicate INTERFACE ge0/0 IP address 192.168.10.234 from MAC address: 00:10:F3:40:98:C0 devmac: 00:10:F3...

Showing 1 to 20 of 553,046 entries

Parameter description:

Time: Time when the log is generated.

Level: Level of the log.

Type: Module type of the log.

Message: Content of the log.

Statistics: Number of logs under a category.

Click ⤓ to export logs in the TXT, XML, and CSV formats. Filtered and unfiltered logs can be exported.

Click ⟳ to refresh log messages.

Click 🗑 to clear all the logs under a category.

Click [Condition Filtering] to set the filter criteria. For details, see section 64.5.2. "Setting Log Filter Criteria."

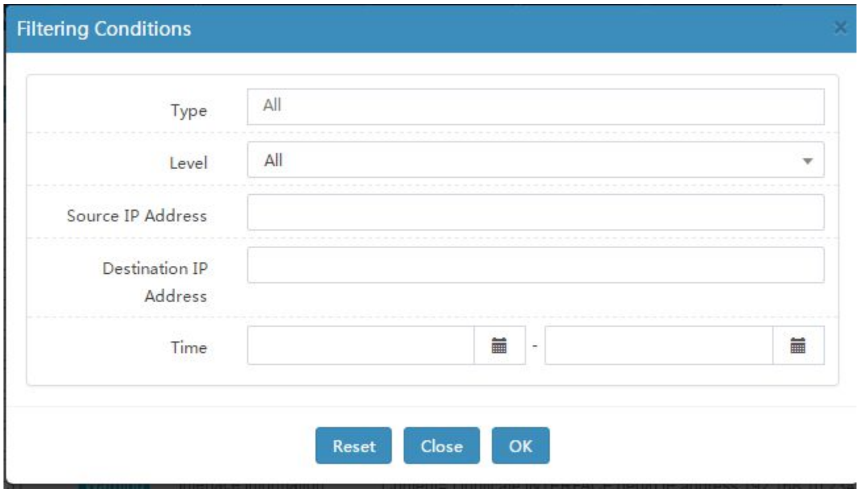
Note

1. Logs are classified into five categories: system event, audit event, VPN event, configuration audit, and security event. For details about log configuration under the audit event, VPN event, configuration audit, and security event categories, see the log configuration under the system event category.
2. You can view configuration audit logs only as an audit user.

64.5.2 Setting Log Filter Criteria

On the log display page, you can set filter criteria to display specified logs. If no filter criteria are set, all logs are displayed. To cancel filter criteria, click **Reset**.

Choose **Log** > **System log** > **System event** and click **Filter criteria**. The following page appears.


Filtering Conditions

Type: All

Level: All

Source IP Address:

Destination IP Address:

Time: -

Type: Log module to be displayed.

Level: Log level. The default value is **Any**, indicating all log levels. If you select a level, only logs of the level are displayed.

Source IP address: Source IP address that triggers logging. You can enter an IP address or a network segment address with a mask.

Destination IP address: Destination IP address that triggers logging. You can enter an IP address or a network segment address with a mask.

Time: Period during which logs are generated.

Procedure:

1. Set **Type**.

2. Set **Level**.

3. **Set** Source IP address.4. Set **Destination IP address**.

5. Set **Time**.

6. **OK**

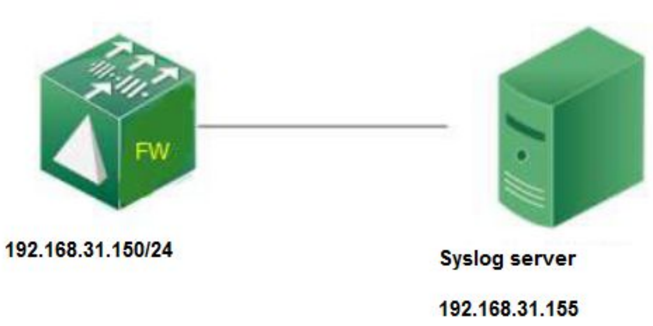
64.6 Configuration Example

64.6.1 Configuring Syslog for the Health Check Module

Description:

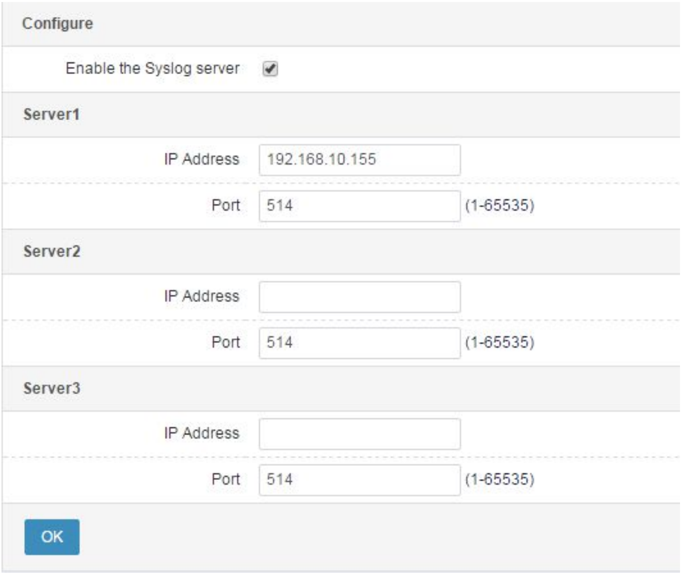
Configure the health check module to send logs to the syslog server.

Network diagram:



Procedure:

1. Choose **Log** > **Log management** > **Log server**. The following page appears.



Configure

Enable the Syslog server ☑

Server1

IP Address 192.168.10.155

Port 514 (1-65535)

Server2

IP Address

Port 514 (1-65535)

Server3

IP Address

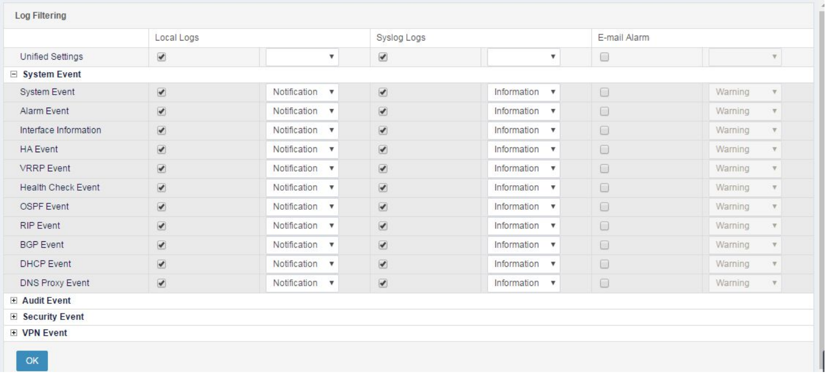
Port 514 (1-65535)

2. Set parameters.

Set **IP address** to the IP address (192.168.31.155) of the syslog server. Set **Port** to the port number (514) of the syslog server.Select **Enable syslog server**.

3. Click **OK**.

4. Choose **Log** > **Log filter**. The following page appears.



Log Filtering

	Local Logs		Syslog Logs		E-mail Alarm	
Unified Settings	☑	▾	☑	▾	□	▾
⊟ **System Event**						
System Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
Alarm Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
Interface Information	☑	Notification ▾	☑	Information ▾	□	Warning ▾
HA Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
VRRP Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
Health Check Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
OSPF Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
RIP Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
BGP Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
DHCP Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
DNS Proxy Event	☑	Notification ▾	☑	Information ▾	□	Warning ▾
⊞ **Audit Event**						
⊞ **Security Event**						
⊞ **VPN Event**						

5. Set Parameters

Click **OK**.

⚠ After health check is performed, the syslog server displays logs generated by the health check module.

Notice

64.7 Troubleshooting

64.7.1 The Syslog Feature Fails

Symptom	The syslog server does not display corresponding module logs.

Analysis	1. Check whether the IP address and port number of the syslog server are correct. 2. Check whether the log category and level are specified on the syslog server.
Solution	1. Set the IP address and port number of the syslog server correctly. 2. Specify the log category and level on the syslog server.

64.7.2 The Email Log Feature Fails

Symptom	No email with corresponding module logs is sent.
Analysis	1. Check whether the alert email parameters are correctly set. 2. Check whether the email log feature is enabled for the module. 3. Check whether the generated logs are at the alert level or above.
Solution	1. Set the alert email parameters, email sending route, and DNS correctly. Ensure that the test email is successfully sent. 2. Enable the email log feature for the module. 3. Ensure that the generated logs are at the alert level and above. No email is sent if the logs are not at the alert level.

65 System Configuration

65.1 Overview

This chapter describes the basic firewall configuration for management purposes. The system configuration includes the following:

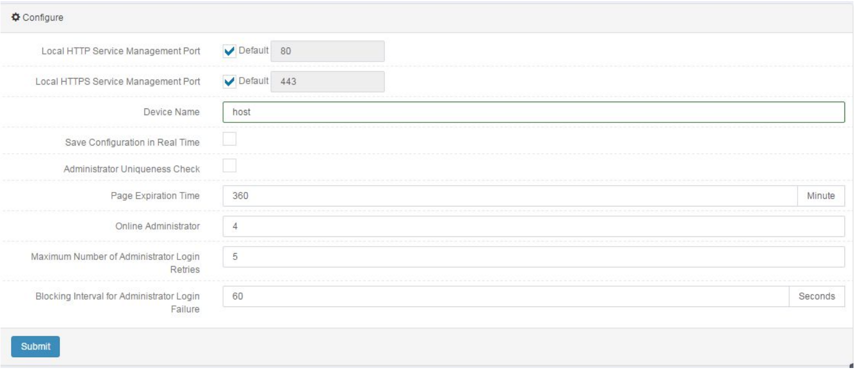
1. Device. You can configure the host name, administrator login limit, and real-time saving of web configurations.
2. System monitoring. You can configure the monitoring thresholds of system resources such as memory and CPU. When a threshold is exceeded, logs are sent to administrators so that they know the device status.
3. Time configuration. You can configure the system time and time zone. The system time can be set manually or obtained from an NTP server.
4. DNS configuration. You can configure a DNS server to resolve domain names. The domain name of the NTP server is resolved by the DNS server.
5. Backup and restoration. You can import existing configurations to facilitate operation, or export configurations for future use or for use by other devices.
6. Alert email configuration. You can configure to send logs of the email type or send feedback via email.
7. Feedback. Specify the receiver and content of feedback.
8. Device restart. You can restart the device, or restore the default settings and restart the device.
9. Operation record. You can record the firewall operation information for troubleshooting.

65.2 Configuration

65.2.1 Device Configuration

Procedure:

Choose **System** > **Configuration** > **Device**.



Local HTTP Service Management Port	☑ Default 80
Local HTTPS Service Management Port	☑ Default 443
Device Name	host
Save Configuration in Real Time	□
Administrator Uniqueness Check	□
Page Expiration Time	360 Minute
Online Administrator	4
Maximum Number of Administrator Login Retries	5
Blocking Interval for Administrator Login Failure	60 Seconds

Local HTTP service management port: The default value is **80**, which need not be modified normally. You can modify it when necessary.

Local HTTPS service management port: The default value is **443**, which need not be modified normally. You can modify it when necessary.

Host name: Name of the device.

Save configurations in real time: After you check this box, web configurations will be saved in real time.

Administrator uniqueness check: After you check this box, an administrator can log in to only one PC at a time.

Page timeout period: Users automatically log out when no web operation is performed during this period. The default value is 10 minutes.

Online administrators: Maximum number of administrators that can log in at the same time. The default value is **4.**

Maximum login attempts per administrator: The default value is 5 times.

Block duration after failed administrator login: Duration for which an administrator is prevented from logging in when the maximum login attempts threshold is reached.

Procedure:

1. If the device's HTTP or HTTPS service management port is not the default 80 or 443, you can set **Local HTTP service management port** or **Local HTTPS service management port**. Normally, use the default value.

2. Set **Host name**. The default value is **Host**.

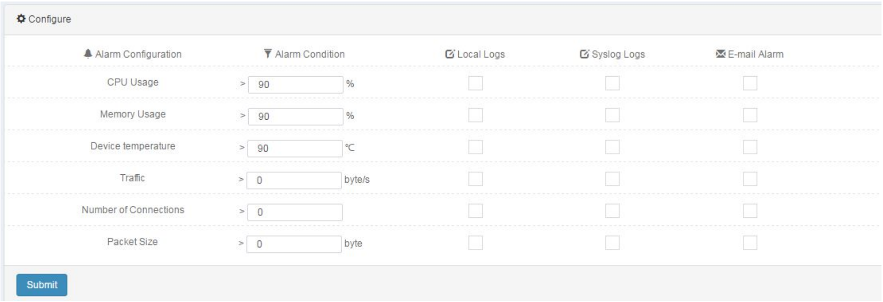
3. If you want to save configurations in real time, select **Save configurations in real time**.

4. If you want to prevent the same administrator from logging in to different PCs at the same time, select **Administrator uniqueness check**.

5. Set **Page timeout period**. The default value is 10 minutes.
6. Set **Online administrators**.
7. Set **Maximum login attempts per administrator**.
8. Set **Block duration after failed administrator login**.
9. Click **Submit**.

65.2.2 System Monitoring

Choose **System** > **Configuration** > **System monitoring**.



Configure

Alarm Configuration	Alarm Condition	Local Logs	Syslog Logs	E-mail Alarm
CPU Usage	> 90 %	□	□	□
Memory Usage	> 90 %	□	□	□
Device temperature	> 90 ℃	□	□	□
Traffic	> 0 byte/s	□	□	□
Number of Connections	> 0	□	□	□
Packet Size	> 0 byte	□	□	□

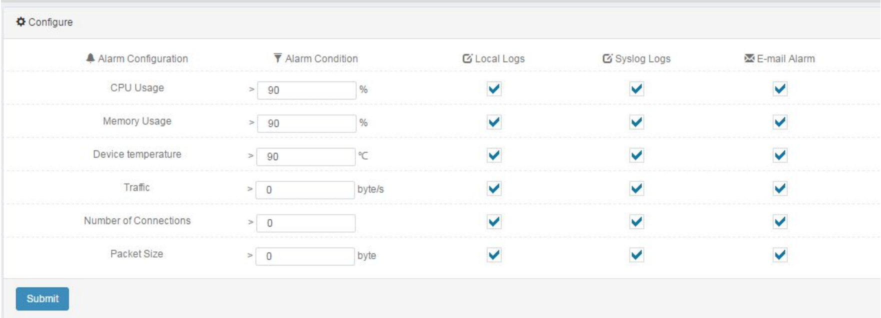
On the displayed page, you can set **CPU usage**, **Memory usage**, **Traffic**, **Connections**, and **Packet size**, and configure logging when the threshold is reached. By default, logs are sent every 5 minutes.

Procedure:

1. Set **CPU usage**, indicating the average usage of service core.
2. Set **Memory usage**, indicating the usage of shared memory.
3. Set **Traffic**.
4. Set **Connections**.
5. Set **Packet size**.
6. Select a log type. The options are **Local log**, **Syslog**, and **Email log**.

Syslogs are sent to a log module. You must configure a syslog server. Logs can be sent via email to the configured address.

7. Click **Submit**.

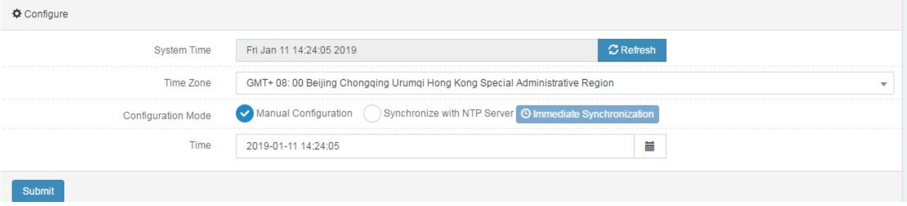


Configure

Alarm Configuration	Alarm Condition	Local Logs	Syslog Logs	E-mail Alarm
CPU Usage	> 90 %	☑	☑	☑
Memory Usage	> 90 %	☑	☑	☑
Device temperature	> 90 ℃	☑	☑	☑
Traffic	> 0 byte/s	☑	☑	☑
Number of Connections	> 0	☑	☑	☑
Packet Size	> 0 byte	☑	☑	☑

65.2.3 Time Configuration

Choose **System** > **Configuration** > **Time configuration**.



Configure

System Time: Fri Jan 11 14:24:05 2019

Time Zone: GMT+ 08: 00 Beijing Chongqing Urumqi Hong Kong Special Administrative Region

Configuration Mode: ● Manual Configuration ○ Synchronize with NTP Server

Time: 2019-01-11 14:24:05

System time: Current system time.

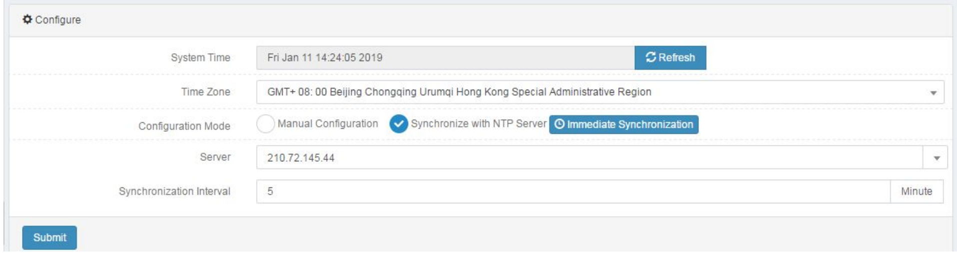
Time zone: Time zone where the device is located.

Configuration mode: The options are **Set manually** and **Synchronize from NTP server**.

Procedure:

1. Set **Configuration mode**. Select **Set manually** or **Synchronize from NTP server**.
2. If you select **Set manually**, enter time.
3. If you select **Synchronize from NTP server**, specify the NTP server domain name and synchronization interval.

   Configure a default route and DNS in advance.
4. Click **Submit**.



Configure

System Time: Fri Jan 11 14:24:05 2019

Time Zone: GMT+ 08: 00 Beijing Chongqing Urumqi Hong Kong Special Administrative Region

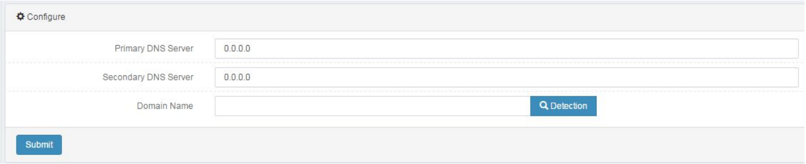
Configuration Mode: ○ Manual Configuration ● Synchronize with NTP Server

Server: 210.72.145.44

Synchronization Interval: 5 Minute

65.2.4 DNS Configuration

Choose **System** > **Configuration** > **DNS**.



⚙ Configure

Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Domain Name	

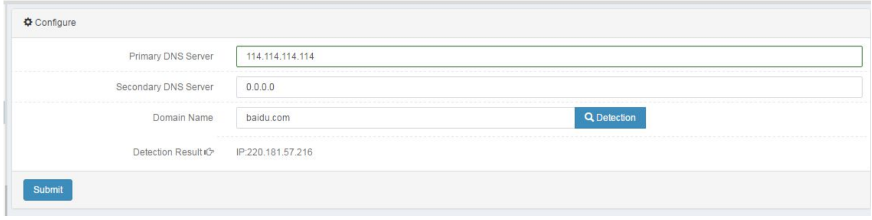
Preferred DNS server: Enter a DNS server address.

Alternate DNS server: Enter a DNS server address.

Domain name: Enter a domain name to test whether the DNS servers are available. Check whether the DNS servers are reachable in advance.

Procedure:

1. Set **Preferred DNS server**.
2. Set **Alternate DNS server**.
3. Click **Submit**.

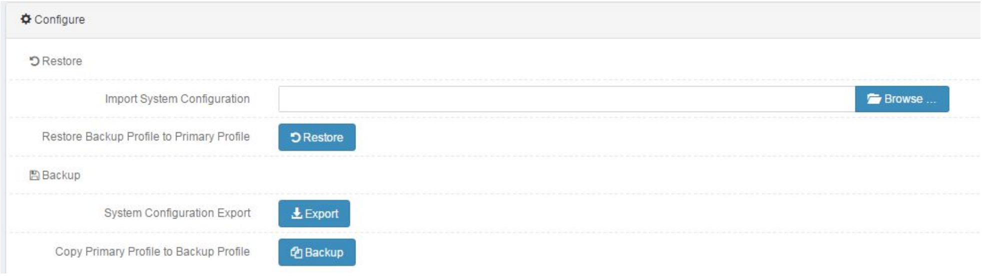


⚙ Configure

Primary DNS Server	114.114.114.114
Secondary DNS Server	0.0.0.0
Domain Name	baidu.com
Detection Result	IP:220.181.57.216

65.2.5 Backup and Restoration

Choose **System** > **Configuration** > **Backup and restoration**.



⚙ Configure

Restore

Import System Configuration	Browse ...
Restore Backup Profile to Primary Profile	Restore

Backup

System Configuration Export	Export
Copy Primary Profile to Backup Profile	Backup

Import system configurations: Select a configuration file to be imported.

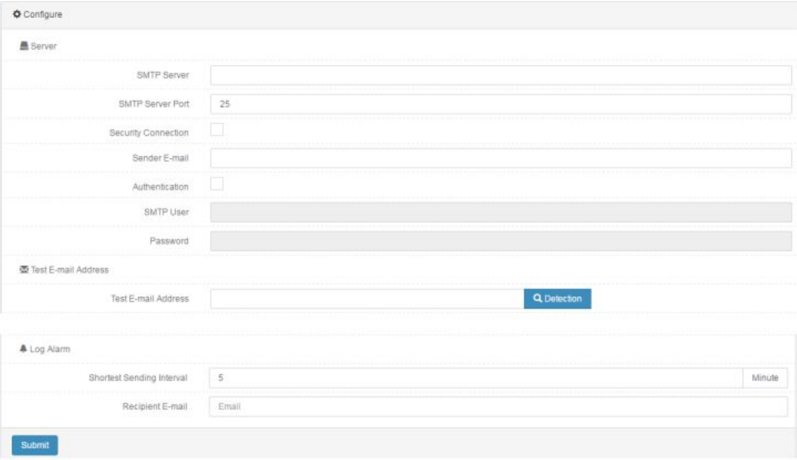
Restore the backup configurations to the main configuration file: Overwrite the main configurations with backup configurations.

Export system configurations: Export a configuration file.

Copy the main configuration file to the backup configuration file: Back up the main configurations.

65.2.6 Alert Email Configuration

Choose **System** > **Configuration** > **Alert email configuration**.



Configure

Server

SMTP Server	
SMTP Server Port	25
Security Connection	□
Sender E-mail	
Authentication	□
SMTP User	
Password	

Test E-mail Address

Test E-mail Address	Detection

Log Alarm

Shortest Sending Interval	5 Minute
Recipient E-mail	Email

Submit

SMTP server: Mail server address.

SMTP server port: Port number of the mail server.

Security link: Check this box to enable security link.

Sender email: Email address of the sender.

Authentication: Check this box to enable mail authentication.

SMTP user: User name of the sender for email login.

Password: Password of the sender for email login.

Test email address: A test email is sent to this address to check whether it is reachable.

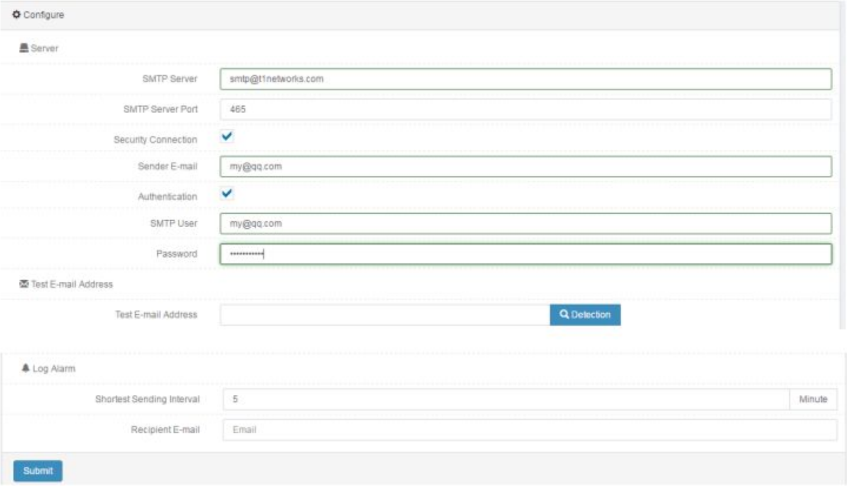
Minimum sending interval: Minimum interval at which log messages are sent via email. The value ranges from **1** to **60**, in minutes.

Receiver email: Email address of the receiver. Separate multiple email addresses with semicolons (;).

Procedure:

1. Set **SMTP server**.

2. Set **SMTP server port.** The default value is **25**.
3. Select **Security link** as needed.
4. Set **Sender email.**
5. Select **Authentication** as needed.
6. Set **SMTP user**.
7. Set **Password**.
8. Set **Minimum sending interval**.
9. Set **Receiver email.**
10. Click **Submit.**



SMTP Server: smtp@t1networks.com

SMTP Server Port: 465

Security Connection: ☑

Sender E-mail: my@qq.com

Authentication: ☑

SMTP User: my@qq.com

Password: ••••••••••

Test E-mail Address:

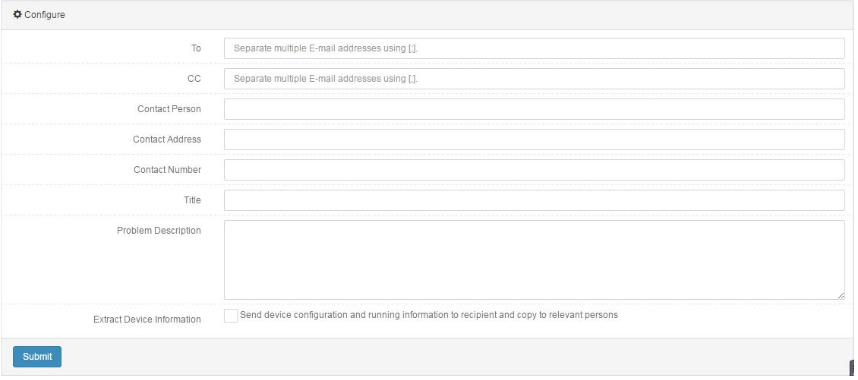
Shortest Sending Interval: 5 Minute

Recipient E-mail: Email

65.2.7 Feedback

Procedure:

Choose **System** > **Configuration** > **Feedback**.



Configure

To	Separate multiple E-mail addresses using [;].
CC	Separate multiple E-mail addresses using [;].
Contact Person	
Contact Address	
Contact Number	
Title	
Problem Description	
Extract Device Information	□ Send device configuration and running information to recipient and copy to relevant persons

Receiver: Email address of the receiver.

CC: CC of feedback.

Subject: Email subject.

Description: Problem description.

Contact: Name of a contact.

Address: Address of the contact.

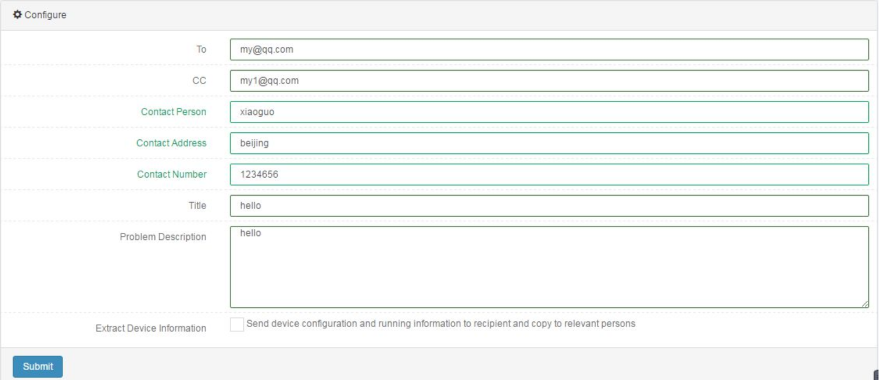
Tel: Phone number of the contact.

Retrieve device info: Check this box to send the device configurations and operation information to the receiver and CC.

Procedure:

Complete the settings in section 65.2.6 "Alert Email Configuration" and ensure that a test email is successfully sent in advance.

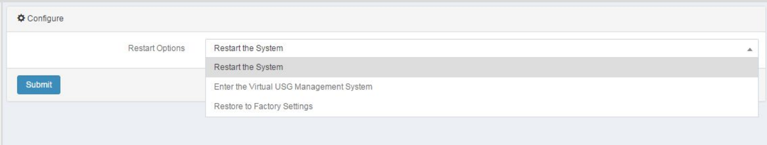
1. Set **Receiver**.
2. Set **CC**.
3. Set **Contact**, **Address**, and **Tel**.
4. Set **Subject**.
5. Set **Description**.
6. Select **Retrieve device info** as needed.
7. Click **Submit**.



To	my@qq.com
CC	my1@qq.com
Contact Person	xiaoguo
Contact Address	beijing
Contact Number	1234656
Title	hello
Problem Description	hello
Extract Device Information	□ Send device configuration and running information to recipient and copy to relevant persons

65.2.8 Device Restart

Choose **System** > **Configuration** > **Device restart**.



Configure
Restart Options
Restart the System
Restart the System
Enter the Virtual USG Management System
Restore to Factory Settings
Submit

On the displayed page, you can choose to restart the device, access the virtual USG management system, or restore the default settings and restart the device.

65.2.9 Device Operation Record

You can configure device operation records, export log files of device operation records, and export system operation logs. The health status of device operation is recorded.

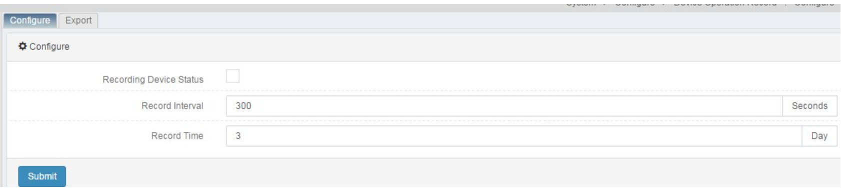
Configure device operation records: This function is used to configure device operation records to generate operation logs.

Export log files of device operation records: This function records the real-time information about the device, including the version, interfaces, and traffic. You can export logs and compressed files.

Export system operation logs: You can export system operation record files as encrypted compressed packages.

Procedure:

1. Choose **System** > **Configuration** > **Device operation record**. Click the **Configuration** tab.



Recording Device Status □

Record Interval 300 Seconds

Record Time 3 Day

Parameter description:

Record device operating status: Check this box to enable the function.

Generation interval: Interval at which information is recorded, including the version, interfaces, and traffic. A new log file named after date is generated every day.

Save time : Record duration, in days. If it is set to **3**, information is recorded for three consecutive days, and three log files are saved to a disk. Earlier files are overwritten by new files.

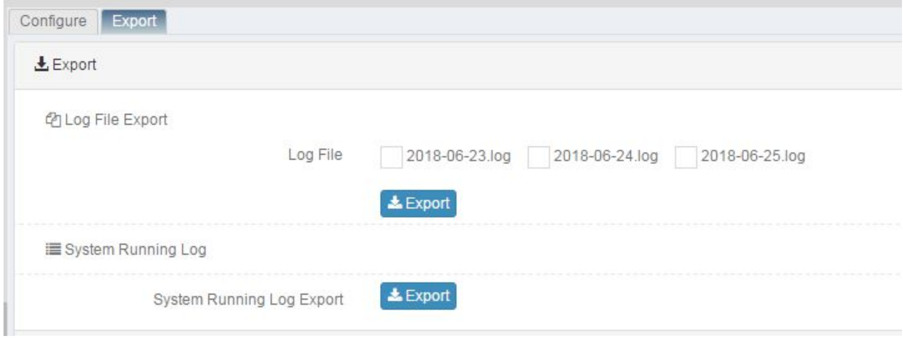
2 Click **Submit** after you complete the settings.

The record function is only available in a device with a disk.

Export device operation records as follows:

Procedure:

1. Choose **System** > **Configuration** > **Device operation record**. Click the **Export** tab.



Log File □ 2018-06-23.log □ 2018-06-24.log □ 2018-06-25.log

System Running Log Export

Parameter description:

Export log files: Export log files on one or more days.

Export system operation logs: Export system operation logs.

65.3 Configuration Example

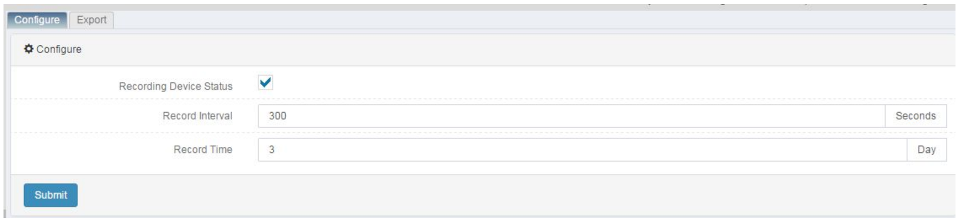
65.3.1 Configuring and Exporting Device Operation Records

Description:

Set **Generation interval** to **60** and **Save time** to **3** days, and enable the device operation record function. Export the generated log files.

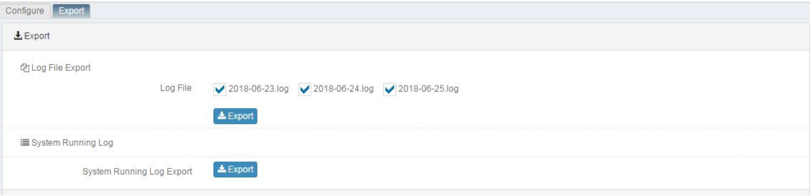
Procedure:

1. Choose **System** > **Configuration** > **Device operation record**. Click the **Configuration** tab.



Recording Device Status ☑
Record Interval 300 Seconds
Record Time 3 Day

2. Click **Submit** after you complete the settings.
3. Choose **System** > **Configuration** > **Device operation record**. Click the **Export** tab.



Log File ☑ 2018-06-23.log ☑ 2018-06-24.log ☑ 2018-06-25.log

4. Select the log file to be exported and click **Export**

66 Administrator

66.1 Overview

RAVEN5000firewalls support the use of local user databases and support user authentication using the RADIUS server and LDAP server. (1) You can add the user name to the firewall's user database, and set a password to allow the user to perform authentication using the internal database. (2) You can add a RADIUS server and select RADIUS to allow the user to perform authentication using the specified server. (3) You can add an LDAP server and select LDAP to allow the user to perform authentication using the specified server. After a user enters the correct user name and password, the user is successfully authenticated.

If RADIUS is selected and the entered user name and password match those on the RADIUS server, the user is successfully authenticated.

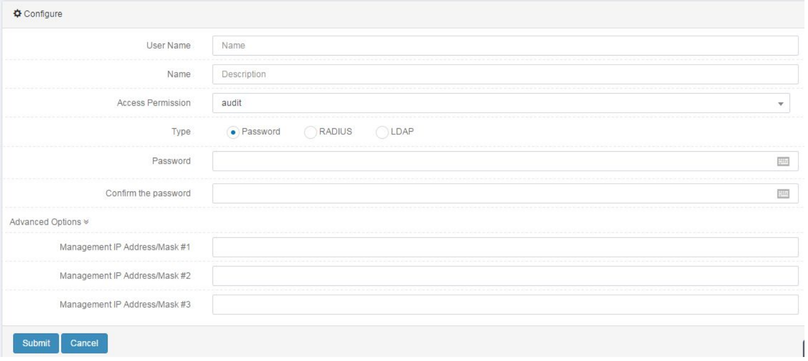
If LDAP is selected with LDAP support configured and the entered user name and password match those on the LDAP server, the user is successfully authenticated.

66.2 Administrator Configuration

66.2.1 Configuring an Administrator

You can configure an administrator for authentication.

Choose **System** > **Administrator** > **Administrator**.



Configure

User Name	Name
Name	Description
Access Permission	audit
Type	● Password ○ RADIUS ○ LDAP
Password	
Confirm the password	

Advanced Options

Management IP Address/Mask #1	
Management IP Address/Mask #2	
Management IP Address/Mask #3	

User name: Administrator name.

Description: Administrator description.

ACL: Access control list (ACL) of the administrator. The default ACL contains audit, admin, and useradmin. You can select a custom ACL.

Type: Type of administrator authentication. The options are **Password**, **RADIUS**, and **LDAP**.

Notice

Password: If you select this option, the user name and password of the created user are saved locally. Enter the same password in **Password** and **Confirm password**.

RADIUS: If you select this option, only the user name is saved locally. The user must perform authentication on a specified RADIUS server and must exist on the server. Select a RADIUS server from the drop-down list.

LDAP: If you select this option, only the user name is saved locally. The user must perform authentication on a specified LDAP server and must exist on the server. Select an LDAP server from the drop-down list.

Management IP address/Mask #1: Network segment where users are allowed to log in.

Management IP address/Mask #2: Network segment where users are allowed to log in.

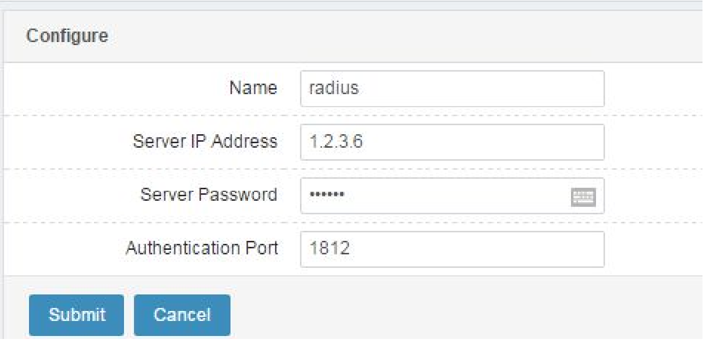
Management IP address/Mask #3: Network segment where users are allowed to log in.

66.3 RADIUS Server Configuration

With RADIUS configured, when a user is configured to use a RADIUS server for authentication, the firewall connects to the server for authentication.

66.3.1 Configuring a RADIUS Server

Choose **Object** > **Authentication server** > **RADIUS** and click **New**.



Configure

Name	radius
Server IP Address	1.2.3.6
Server Password	••••••
Authentication Port	1812

Name: Name of a RADIUS server.

Server IP address: IP address of the RADIUS server.

Server password: Shared key of the RADIUS server.

Authentication port: Port of the RADIUS server for authentication. The default value is **1812**.

Note

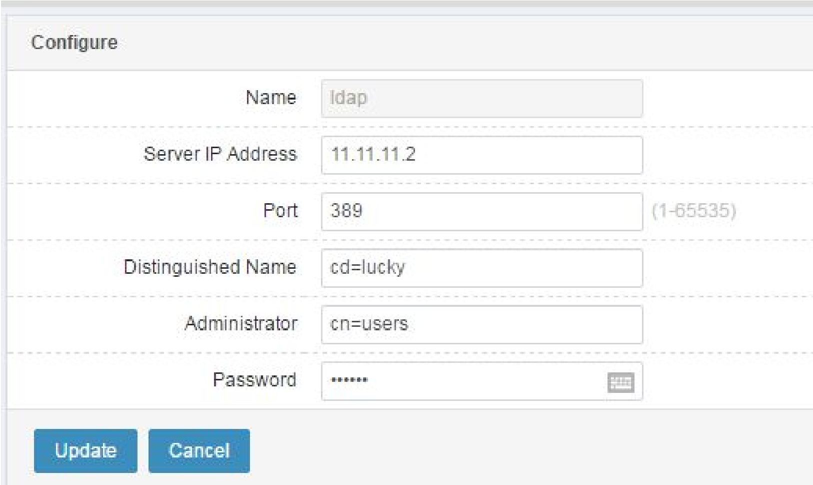
Click the **RADIUS configuration** tab of **Authentication server** to list all the configured RADIUS servers.

66.4 LDAP Server Configuration

With LDAP configured, when a user is configured to use an LDAP server for authentication, the firewall connects to the server for authentication.

66.4.1 Configuring an LDAP Server

Choose **Object** > **Authentication server** > **LDAP** and click **New**.



Configure

Name	ldap	
Server IP Address	11.11.11.2	
Port	389	(1-65535)
Distinguished Name	cd=lucky	
Administrator	cn=users	
Password	••••••	

Name: Name of an LDAP server.

Server IP address: IP address of the LDAP server.

Port: Port of the LDAP server for authentication. The default value is **389**.

Distinguished name: Start position to search data on the LDAP server. For example, if user 2 exists in the **users** container in the **test.com** path of the LDAP server, then enter **dc=test, dc=com**.

Administrator: User with the administrator role on the LDAP server. For example, if the user name and password used to log in to the LDAP server are **administrator** and **111111**, and the user exists in the **users** container in the **test.com** path of the LDAP server, then **enter** **cn=administrator,cn=users,dc=test,dc=com** for **Administrator** and **111111** for **Password**.

Password: Password of the user with the administrator role on the LDAP server.

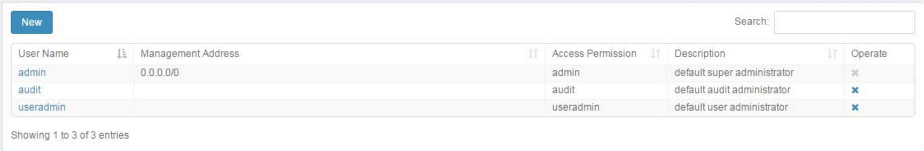
Note

Click the **LDAP** tab of **Authentication user** to list all the configured LDAP servers.

66.5 Monitoring and Maintenance

66.5.1 Displaying Administrator Information

Choose **System** > **Administrator** > **Administrator** to display administrator information.



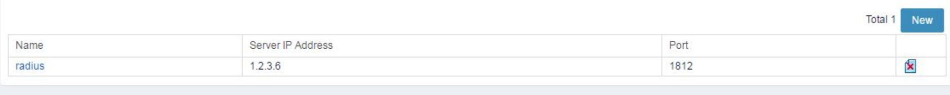
User Name	Management Address	Access Permission	Description	Operate
admin	0.0.0.0/0	admin	default super administrator	✖
audit		audit	default audit administrator	✖
useradmin		useradmin	default user administrator	✖

Showing 1 to 3 of 3 entries

A page appears to show the user names, management addresses, ACLs, and description.

66.5.2 Displaying RADIUS Server Information

Choose **Object** > **Authentication server** > **RADIUS** to display RADIUS server information.

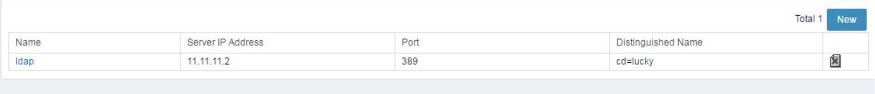


Name	Server IP Address	Port	
radius	1.2.3.6	1812	☒

A page appears to show RADIUS server names, IP addresses, and ports.

66.5.3 Displaying LDAP Server Information

Choose **Object** > **Authentication server** > **LDAP** to display LDAP server information.

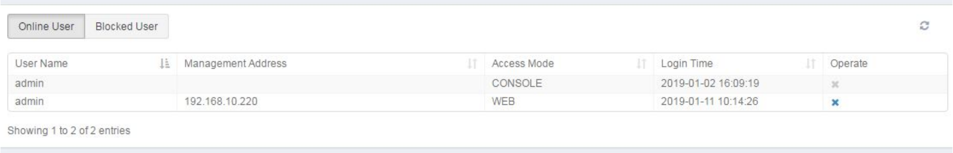


Name	Server IP Address	Port	Distinguished Name	
ldap	11.11.11.2	389	cd=lucky	☒

A page appears to show LDAP server names, IP addresses, ports, and distinguished names.

66.5.4 Displaying Online Administrator Information

Choose **System** > **Administrator** > **Online information** to display online administrator information.



User Name	Management Address	Access Mode	Login Time	Operate
admin		CONSOLE	2019-01-02 16:09:19	✕
admin	192.168.10.220	WEB	2019-01-11 10:14:26	✕

Showing 1 to 2 of 2 entries

A page appears to show information about online administrators and blocked administrators.

66.6 Troubleshooting

66.6.1 A System User Fails to Pass RADIUS Authentication

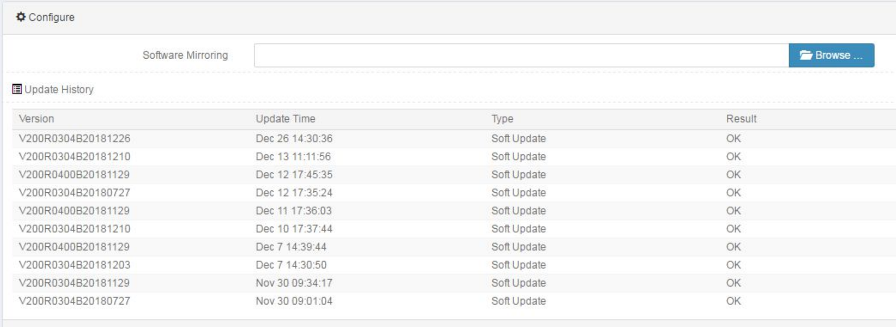
Symptom	A RADIUS user fails to log in to a T-series firewall.
Analysis	1. The password is incorrect. 2. The RADIUS server is incorrectly configured. For example, the shared key or IP address is incorrect. 3. The RADIUS server cannot be connected. For example, it cannot be pinged. 4. The user does not exist on the RADIUS server.
Solution	1. Check the user name and password, and enter them correctly. 2. Modify the configurations of the RADIUS server. 3. Ensure that the firewall communicates with the RADIUS server normally and the ping test is successful. 4. Add the user to the RADIUS server.

67 Version Management

67.1 Version Management

67.1.1 Managing Versions

1. Choose **System** > **Version management** > **Software version**.



Version	Update Time	Type	Result
V200R0304B20181226	Dec 26 14:30:36	Soft Update	OK
V200R0304B20181210	Dec 13 11:11:56	Soft Update	OK
V200R0400B20181129	Dec 12 17:45:35	Soft Update	OK
V200R0304B20180727	Dec 12 17:35:24	Soft Update	OK
V200R0400B20181129	Dec 11 17:36:03	Soft Update	OK
V200R0304B20181210	Dec 10 17:37:44	Soft Update	OK
V200R0400B20181129	Dec 7 14:39:44	Soft Update	OK
V200R0304B20181203	Dec 7 14:30:50	Soft Update	OK
V200R0304B20181129	Nov 30 09:34:17	Soft Update	OK
V200R0304B20180727	Nov 30 09:01:04	Soft Update	OK

Select an upgrade package and click **Upgrade** to upgrade the version. The page lists the latest 10 upgrade records in the lower part.

Procedure:

1. Select an upgrade package.
2. Click **Upgrade**.
3. In the displayed dialog box, click **OK** to start upgrade, or click **Cancel** to cancel the upgrade.

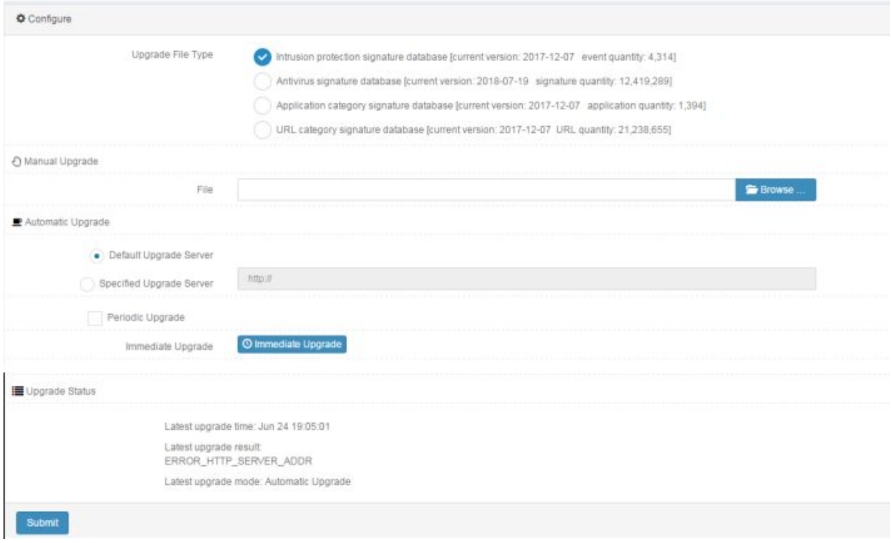
67.1.2 Upgrading the Feature Database

The feature database can be upgraded manually or automatically.

Note

The feature database of the latest version is loaded by default.

Choose **System** > **Version management** > **Feature database version**. The following page appears.



Configure

Upgrade File Type
- ● Intrusion protection signature database [current version: 2017-12-07 event quantity: 4,314]
- ○ Antivirus signature database [current version: 2018-07-19 signature quantity: 12,419,289]
- ○ Application category signature database [current version: 2017-12-07 application quantity: 1,394]
- ○ URL category signature database [current version: 2017-12-07 URL quantity: 21,238,655]

Manual Upgrade

File

Automatic Upgrade

● Default Upgrade Server

○ Specified Upgrade Server http://

□ Periodic Upgrade

Immediate Upgrade

Upgrade Status

Latest upgrade time: Jun 24 19:05:01

Latest upgrade result:
ERROR_HTTP_SERVER_ADDR

Latest upgrade mode: Automatic Upgrade

Upgrade file type: Select the type of the feature database to be upgraded.

Manual upgrade:

File: Select a feature database file and click **Upgrade**.

Note

Ensure that the upgrade file is a valid feature database file.

Automatic upgrade:

Default upgrade server: Set the upgrade server as the default upgrade server.

Specify an upgrade server: Set the upgrade server address.

Periodic upgrade: Enable periodic automatic upgrade.

Weekly: Select weekdays.

Monthly: Select months.

Time: Time of automatic upgrade.

Click **Submit** after you complete the settings.

Upgrade now: Start automatic upgrade immediately.

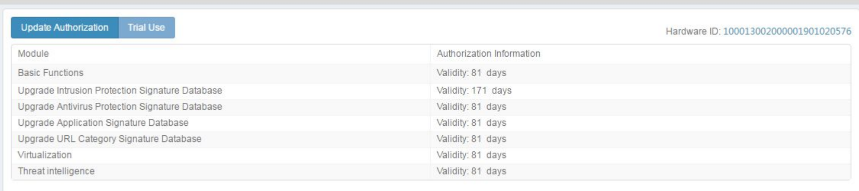
68 License Management

68.1 Overview

Some add-on modules of RAVEN5000 firewalls are controlled by licenses. If licenses are not imported, these modules cannot be configured and take effect. The following modules are controlled by licenses: intrusion prevention feature database, antivirus feature database upgrade, application feature database upgrade, URL category feature database upgrade, and virtualization.

68.2 License Import

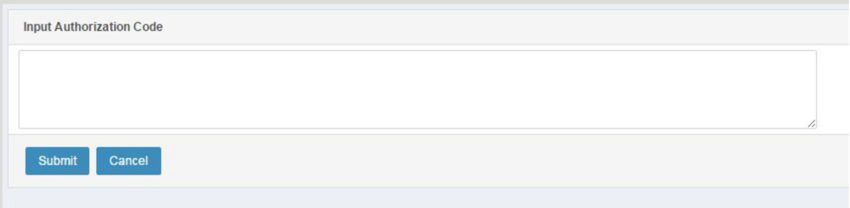
Choose **System** > **License management**. The following page appears.



Hardware ID: 100013002000001901020576

Module	Authorization Information
Basic Functions	Validity: 81 days
Upgrade Intrusion Protection Signature Database	Validity: 171 days
Upgrade Antivirus Protection Signature Database	Validity: 81 days
Upgrade Application Signature Database	Validity: 81 days
Upgrade URL Category Signature Database	Validity: 81 days
Virtualization	Validity: 81 days
Threat intelligence	Validity: 81 days

Click **Update authorization**. Copy and paste an official license code in the text box.



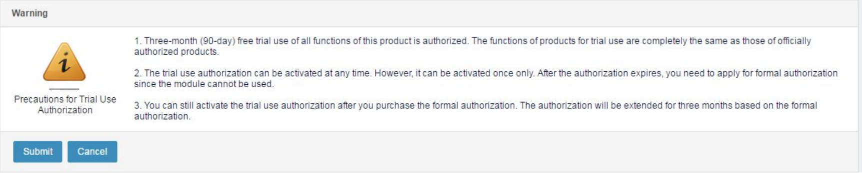
Click **Submit**.

Note

A failure message is displayed if the license code is invalid. If the license code is valid, the page shows the module's license information.

68.3 License Trial Use

Click **Trial use** in **License management** to activate license trial use. A page appears to show the precautions on license trial use.



Warning

Precautions for Trial Use Authorization

1. Three-month (90-day) free trial use of all functions of this product is authorized. The functions of products for trial use are completely the same as those of officially authorized products.

2. The trial use authorization can be activated at any time. However, it can be activated once only. After the authorization expires, you need to apply for formal authorization since the module cannot be used.

3. You can still activate the trial use authorization after you purchase the formal authorization. The authorization will be extended for three months based on the formal authorization.

69 High Availability

69.1 Overview

High availability (HA) is a technique to ensure high network reliability by allowing two firewalls to work in active/standby or active/active mode based on different networking requirements.

In active/standby mode, the active firewall forwards traffic, whereas the standby firewall is in the non-operating state but keeps the same configurations with the active firewall and monitors its running status. Once the active firewall encounters failures such as power-off and system crash, the standby firewall takes over the active one to forward traffic, thus ensuring service continuity.

In active/active mode, two firewalls forward traffic. The traffic distribution ratio depends on the routing configurations of neighboring network devices and the firewall configurations, such as floating IP addresses. Each firewall forwards the traffic with the same unit ID.

The two firewalls send heartbeat packets using configured IP addresses to detect the peer's running status. Firewalls support switchover conditions based on gateway monitoring, interface monitoring, and link aggregation monitoring. If an operating firewall finds its monitoring status is of lower priority than the peer, it enters the standby state, and all traffic is taken over by the other firewall. Preemption is supported in active/standby mode. You can specify active and standby firewalls. Normally, the active and standby states are determined by configurations.

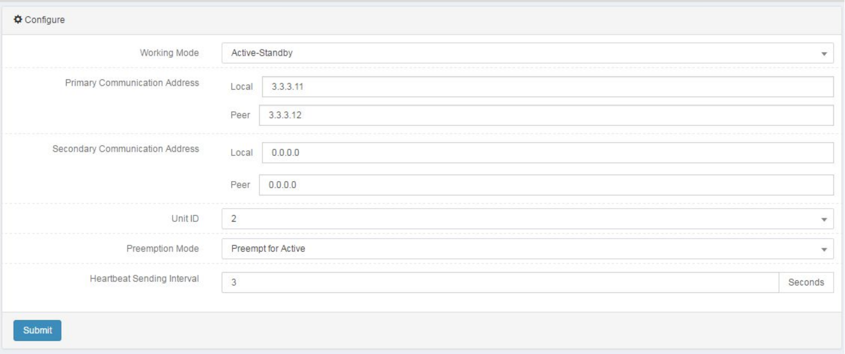
This chapter describes how to configure HA on the web-based management page.

69.2 Basic HA Configurations

The basic HA configurations of a firewall include the operation mode, heartbeat address, and unit ID.

Procedure:

Choose **System management** > **High availability** > **Configuration**. Go to the **Configuration** page.



Configure

Working Mode: Active-Standby

Primary Communication Address: Local 3.3.3.11; Peer 3.3.3.12

Secondary Communication Address: Local 0.0.0.0; Peer 0.0.0.0

Unit ID: 2

Preemption Mode: Preempt for Active

Heartbeat Sending Interval: 3 Seconds

Operation mode: HA operation mode. The options include **Active/Standby** and **Active/Active**.

Preferred communication address: HA heartbeat communication address, used to send and receive heartbeat packets. A local address must be a local interface address. A non-service interface address is recommended.

(Optional) **Alternate communication address**: Alternate communication address for HA heartbeats. After an alternate communication address is specified, the preferred and alternate addresses send and receive heartbeat packets to ensure communication between two firewalls.

Unit ID: Unit ID of a firewall in cluster mode. The optional values are **1** and **2**. The default value is **1**.

Preemptive mode: Preemption status in HA active/standby mode. After preemption is enabled, select active preemption or standby preemption. When the monitored objects are normal, this option determines which firewall takes the active role and which one takes the standby role. It is disabled by default.

Heartbeat sending interval: Interval at which heartbeat packets are sent between two firewalls. The value ranges from 1s to 3s. The default value is 3s.

Click **OK**.

⚠ Notice

1. The communication addresses of the two firewalls must be configured in pair, and they cannot be specified as the floating IP addresses of interfaces.
2. The unit IDs of two firewalls in active/active mode must be different.
3. The preemptive modes of two firewalls in active/standby

mode must be configured in pair.

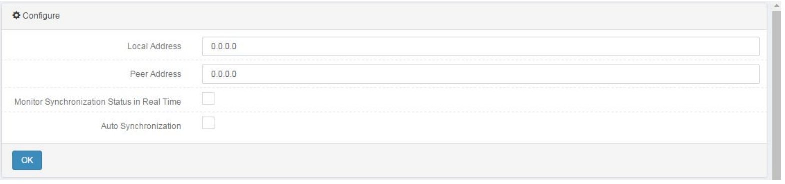
4. The heartbeat sending intervals of the two firewalls must be the same.

69.3 Configuring Synchronization

The HA feature supports manual and automatic synchronization of configurations between firewalls, which reduces the configuration workload and ensures consistent configurations between two firewalls.

Procedure:

Choose **System** > **High availability** > **Configuration synchronization**. Go to the configuration synchronization page.



Configure

Local Address: 0.0.0.0

Peer Address: 0.0.0.0

Monitor Synchronization Status in Real Time □

Auto Synchronization □

Local address: Local address to receive configurations. The firewall will listen to this address.

Peer address: Address to which the firewall sends local configurations.

Monitor synchronization in real time: Check this box to enable periodic detection of consistent configurations at the local and peer end. The default detection interval is 1 minute.

Automatic synchronization: Check this box to automatically synchronize configurations to the peer end.

Click **OK**.

Note

1. The local and peer addresses can be the same as the HA communication addresses, but they cannot be specified as the floating IP addresses of interfaces.
2. After you specify the local and peer addresses, you can manually synchronize configurations on the HA monitoring page.

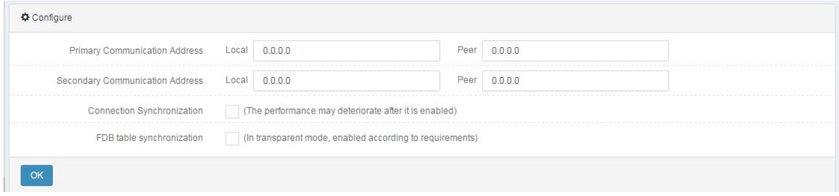
3. If **Monitor synchronization in real time** is selected, the HA monitoring page displays the monitoring results.
4. Real-time monitoring can be enabled on either firewall.
5. The following configurations are not synchronized: HA configurations, dynamic routes, CA certificates, VRRP, and configurations in **Network configuration • •Interface•** .

69.4 Configuring Connection Synchronization

Connection synchronization includes Layer-4 flow synchronization. It protects established connections during failure switchover.

Procedure:

Choose **System** > **High availability** > **Connection synchronization**. Go to the connection synchronization page.



Configure

Primary Communication Address	Local	0.0.0.0	Peer	0.0.0.0
Secondary Communication Address	Local	0.0.0.0	Peer	0.0.0.0
Connection Synchronization	□ (The performance may deteriorate after it is enabled)			
FDB table synchronization	□ (In transparent mode, enabled according to requirements)			

Preferred communication address:

Local: Source address that sends connection synchronization packets.

Peer: Destination address that sends connection synchronization packets.

Alternate communication address:

Local: Source address that sends connection synchronization packets.

Peer: Destination address that sends connection synchronization packets.

Alternate communication address is optional. When packet sending fails using the preferred address, the alternate address is used, improving the reliability of connection synchronization. With connection synchronization enabled, if there are many connections to be synchronized, the device performance will be seriously affected.

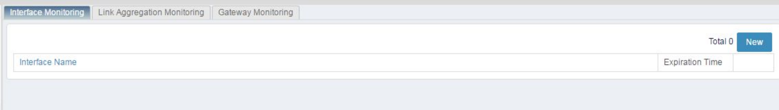
69.5 Configuring HA Monitoring

HA monitoring is divided into gateway monitoring, interface monitoring, and link aggregation monitoring. The device running status is monitored in real time. When a failure is detected, the device status is switched to ensure service continuity.

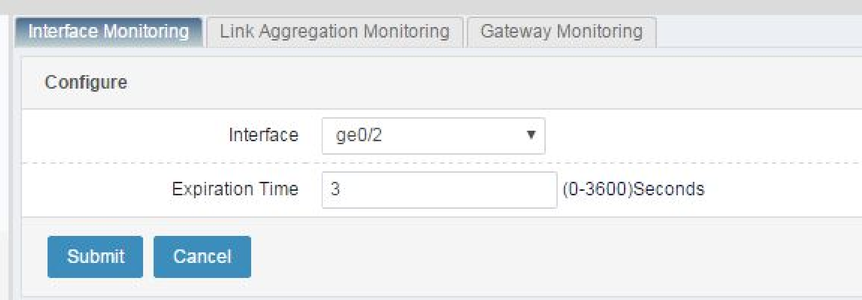
69.5.1 Configuring Interface Monitoring

Procedure:

Choose **System** > **High availability** > **Fault detection**. Click the **Interface monitoring** tab.



Click **New**.



Interface ge0/2

Expiration Time 3 (0-3600)Seconds

Interface: Name of the physical interface or VLAN interface to be monitored. You can monitor all the important VLAN interfaces and physical interfaces except the management interface. The Up and Down states of physical interfaces or VLAN interfaces are monitored. It is recommended that you monitor the upstream and downstream interfaces directly connected to the device. Failure of these interfaces will cause service interruption, in which case failure switchover is required.

Timeout period: Wait time after a fault is detected, which is intended to avoid frequent switchover between the Up and Down states of an interface within a short time, which may cause frequent switchover of the HA status and make the device instable.

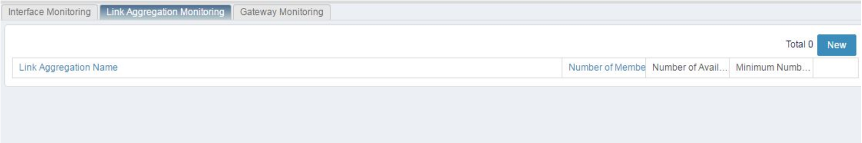
1. Select the interface to be monitored.
2. Set **Timeout period**.

Click **Submit**.

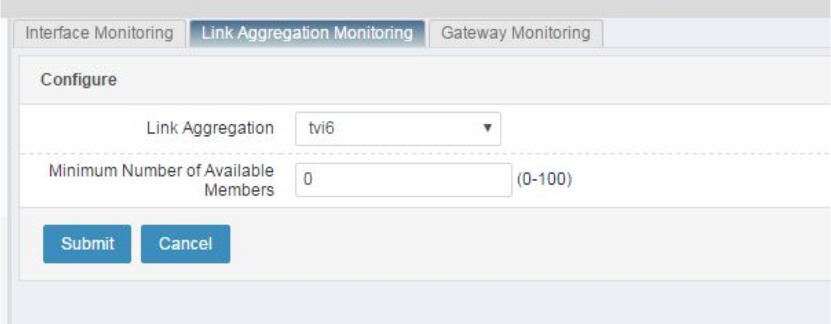
69.5.2 Configuring Link Aggregation Monitoring

Procedure:

Choose **System** > **High availability** > **Fault detection**. Click the **Link aggregation monitoring** tab.



Click **New**.



Link Aggregation: tvi6

Minimum Number of Available Members: 0 (0-100)

Link aggregation: Select the link aggregation interface to be monitored.

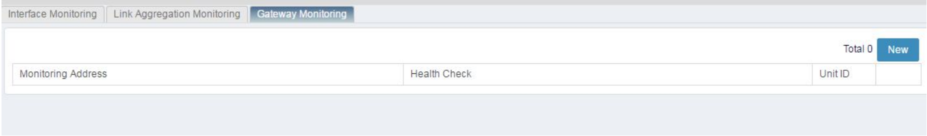
Minimum available members: Enter the minimum number of available members of the link aggregation interface. When the available members are less than this value, the link aggregation interface is faulty.

1. Select the link aggregation interface to be monitored.
2. Set **Minimum available members**.
3. Click **Submit**.

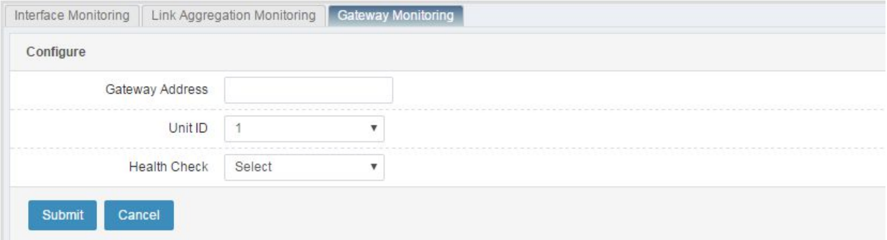
69.5.3 Configuring Gateway Monitoring

Procedure:

Choose **System** > **High availability** > **Fault detection**. Click the **Gateway monitoring** tab.



Click **New**.



Configure

Gateway Address	
Unit ID	1
Health Check	Select

Gateway address: Select the gateway address to be monitored.

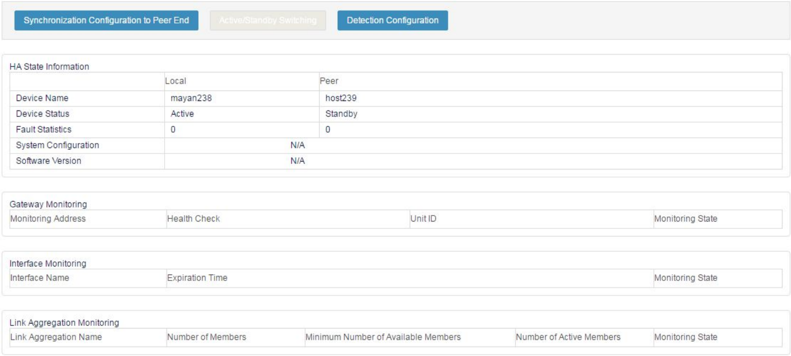
Unit ID: Identifies the device ID in gateway monitoring in active/active mode. Monitoring takes effect when the unit ID is the same as the device ID. When the unit ID is different from the device ID, monitoring takes effect only in active A mode.

Health check: Select the desired health check template from the drop-down list. For how to configure a health check template, see chapter 62 "Health Check."

1. Select the gateway address to be monitored.
2. Select the ID of the device to be monitored.
3. Select a health check template.
4. Click **Submit**.

69.6 HA Status Control

Choose **System** > **High availability** > **Monitoring**. A page appears to display the HA status at the local and peer end.



HA State Information

	Local	Peer
Device Name	mayan238	host239
Device Status	Active	Standby
Fault Statistics	0	0
System Configuration	N/A	
Software Version	N/A	

Gateway Monitoring

Monitoring Address	Health Check	Unit ID	Monitoring State

Interface Monitoring

Interface Name	Expiration Time	Monitoring State

Link Aggregation Monitoring

Link Aggregation Name	Number of Members	Minimum Number of Available Members	Number of Active Members	Monitoring State

Synchronize configurations to the peer: Click this button after completing configuration at the local end to synchronize the configurations to the peer end.

Active/Standby switchover: Click this button to enable active/standby switchover when the peer device exists. The active device enters the standby state, and the standby device takes over the active device.

Check configurations: Click this button to check whether configurations are synchronized between the local and peer end.

Notice

1. After you click **Synchronize configurations to the peer**, the page will return synchronization results after a time. Do not leave the page before results are returned.
2. After configurations are synchronized to the peer end, restart the peer device to make the configurations take effect.
3. Active/Standby switchover is not supported in active/active mode.
4. Active/Standby switchover is not supported in active/standby mode if preemption is configured.

69.7 Configuration Examples

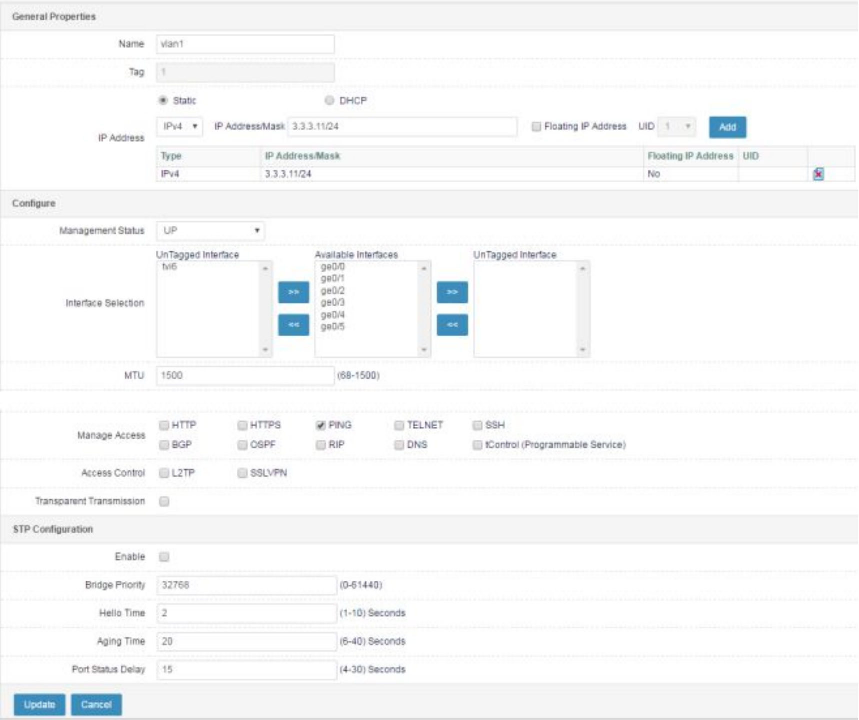
69.7.1 Example 1: Configuring the Basic Active/Standby Settings

Description:

Configure FW_A and FW_B separately to enable them to work in active/standby mode and negotiate the active state and standby state properly. You can configure FW_A as the active device and configure the HA module of FW_B. Then synchronize configurations from FW_A to FW_B manually. Enable real-time synchronization monitoring and floating MAC address mapping.

Procedure:

1. Configure FW_A: Choose **Network** > **Interface** > **VLAN**. Go to the VLAN list page and click **New** to configure the interface IP address required by HA.



General Properties

Name: vlan1

Tag: 1

IP Address: ● Static ○ DHCP

IPv4 ▾ IP Address/Mask: 3.3.3.11/24 □ Floating IP Address UID 1 ▾ Add

Type	IP Address/Mask	Floating IP Address	UID	
IPv4	3.3.3.11/24	No		☒

Configure

Management Status: UP ▾

Interface Selection: UnTagged Interface: tvi6 — Available Interfaces: ge0/0, ge0/1, ge0/2, ge0/3, ge0/4, ge0/5 — UnTagged Interface

MTU: 1500 (68-1500)

Manage Access: □ HTTP □ HTTPS ☑ PING □ TELNET □ SSH □ BGP □ OSPF □ RIP □ DNS □ tControl (Programmable Service)

Access Control: □ L2TP □ SSLVPN

Transparent Transmission: □

STP Configuration

Enable: □

Bridge Priority: 32768 (0-61440)

Hello Time: 2 (1-10) Seconds

Aging Time: 20 (6-40) Seconds

Port Status Delay: 15 (4-30) Seconds

Tag: VLAN ID. Enter **1**.

IP address: Enter **3.3.3.11**.

Mask: Enter a 24-bit mask.

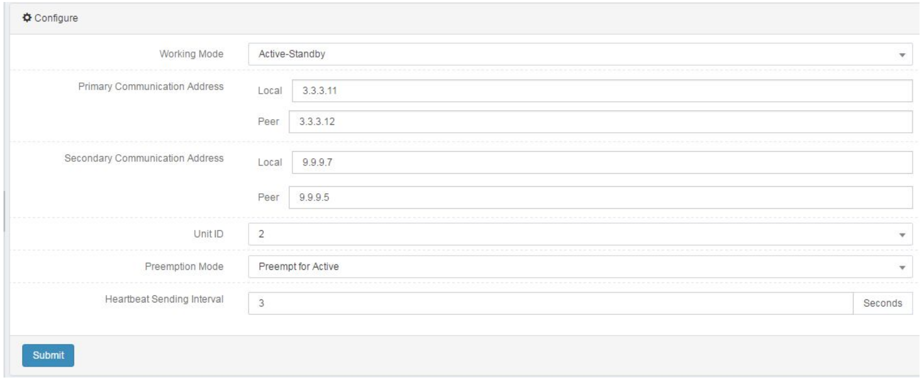
Floating IP address: Uncheck this box.

Interface selection: Select physical interfaces and add them to the VLAN in tag or untag mode.

For details about other parameters, see related sections.

2. Click **Update** to create IP address 3.3.3.11. Repeat the preceding procedure to create IP address 9.9.9.7. Bind 3.3.3.11 to VLAN 1 as the heartbeat address of the active device, and bind 9.9.9.7 to VLAN 2 as the heartbeat address of the standby address.

3. Configure FW_A: Choose **System** > **High availability** > **Configuration.** Go to the **Configuration** page.



Configure

Working Mode: Active-Standby

Primary Communication Address: Local 3.3.3.11 Peer 3.3.3.12

Secondary Communication Address: Local 9.9.9.7 Peer 9.9.9.5

Unit ID: 2

Preemption Mode: Preempt for Active

Heartbeat Sending Interval: 3 Seconds

Operation mode: Select **Active/Standby**.

Preferred communication address: Use 3.3.3.5 created in Steps 1 and 2 as the local communication address. Create IP address 3.3.3.3 on the peer device.

Alternate communication address: Use 9.9.9.7 created in Steps 1 and 2 as the local communication address.

Create IP address 9.9.9.7 on the peer device.

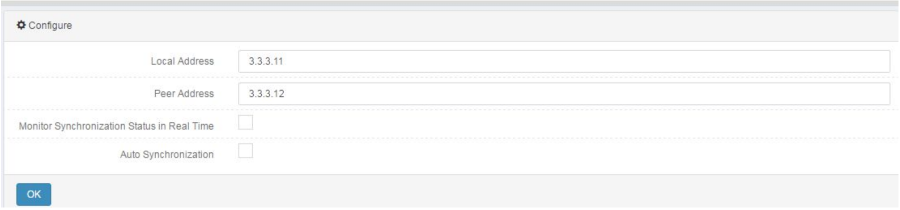
Unit ID: Enter **1**.

Preemptive mode: Select **Active preemption** so that FW_A becomes the active device.

Heartbeat sending interval: Enter **3**. A heartbeat packet will be sent every 3s.

Floating MAC address: You can enable or disable floating MAC address mapping.

4. Configure FW_A: Choose **System** > **High availability.** Go to the configuration synchronization page.



Configure

Local Address: 3.3.3.11

Peer Address: 3.3.3.12

Monitor Synchronization Status in Real Time: □

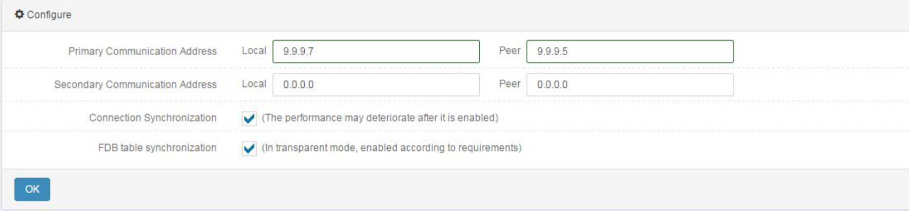
Auto Synchronization: □

Local address: Enter the same IP address as the preferred communication address. You can also repeat Steps 1 and 2 to create an IP address.

Peer address: Create IP address 3.3.3.3 on the peer device.

Monitor synchronization in real time: Check this box to enable monitoring of different configurations between the local and peer end.

5. Configure FW_A: Choose **System** > **High availability**. Go to the connection synchronization page.



Configure

Primary Communication Address Local 9.9.9.7 Peer 9.9.9.5

Secondary Communication Address Local 0.0.0.0 Peer 0.0.0.0

Connection Synchronization ☑ (The performance may deteriorate after it is enabled)

FDB table synchronization ☑ (In transparent mode, enabled according to requirements)

OK

Preferred communication address: Reuse the alternate communication address 9.9.9.7 as the local address. Configure IP address 9.9.9.9 on the peer device.

(Optional) **Alternate communication address**: It is not set in this example.

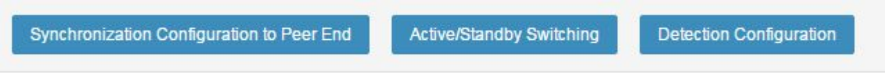
Synchronize connection: Check this box to synchronize connection information in real time.

6. Configure FW_B in the same way as FW_A.

The configuration of the HA active/standby mode is complete.

7. Choose **System** > **High availability** > **Monitoring** to display HA monitoring results.

8. Choose **System** > **High availability** > **Monitoring** to check HA status management.



Synchronize configurations to the peer: Click this button after completing configuration at the local end to synchronize the configurations to the peer end. After configurations are synchronized, restart the peer device to make the configurations take effect.

Active/Standby switchover: Click this button to enable the active device to enter the standby state and the peer device to enter the active state. You can switch between the active and standby states manually. This button is grayed out if preemption is enabled.

Check configurations: Click this button to check whether configurations are consistent at the local and peer end. If not, synchronize the configurations.

This completes the basic configuration of the HA active/standby mode. If you want to configure fault monitoring, then configure interface monitoring, link aggregation monitoring, or gateway monitoring in accordance with section 69.5 "Configuring HA Monitoring." To enable service forwarding, you need to configure interfaces, routes, NAT, and other features. For details, see related sections.

69.7.2 Example 2: Configuring the Basic Active/Active Settings

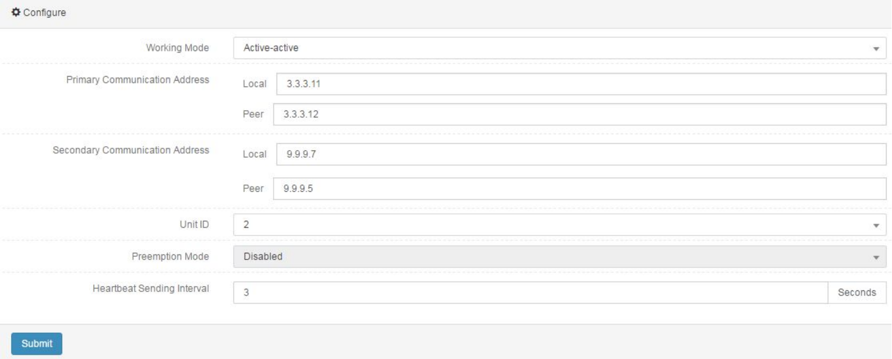
Description:

Configure FW_A and FW_B separately to enable them to work in active/active mode and negotiate the active/active state properly. Two devices in active/active mode forward traffic separately, and they are differentiated by unit IDs. Enable automatic synchronization and floating MAC address mapping.

Procedure:

1. Configure device IP addresses in active/active mode in the same way as in active/standby mode.

2. Configure FW_A: Choose **System** > **High availability** > **Configuration**. Go to the **Configuration** page.



Configure

Working Mode	Active-active	
Primary Communication Address	Local	3.3.3.11
	Peer	3.3.3.12
Secondary Communication Address	Local	9.9.9.7
	Peer	9.9.9.5
Unit ID	2	
Preemption Mode	Disabled	
Heartbeat Sending Interval	3	Seconds

Operation mode: Select **Active/Active**.

Preferred communication address: Enter the address configured in Step 1.

Alternate communication address: Enter the address configured in Step 1.

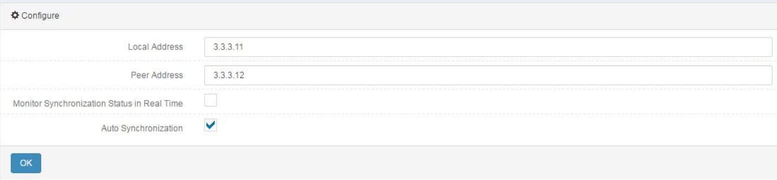
Unit ID: Enter **2**. The unit IDs of the two devices must be different. A floating IP address has a unit ID, and it takes effect on the device only when its unit ID is the same as that of the device.

Preemptive mode: Preemption does not take effect in active/active mode.

Heartbeat sending interval: Enter **3**. A heartbeat packet will be sent every 3s.

Floating MAC address: You can enable or disable floating MAC address mapping.

3. Configure FW_A: Choose **System** > **High availability**. Go to the configuration synchronization page.



Configure

Local Address: 3.3.3.11

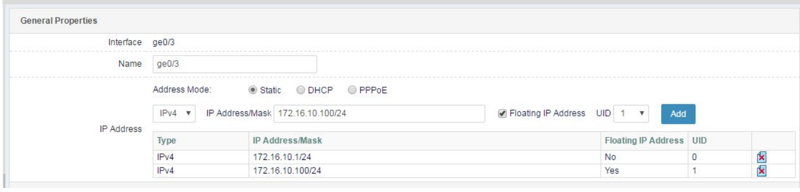
Peer Address: 3.3.3.12

Monitor Synchronization Status in Real Time ☐

Auto Synchronization ☑

4. Configure FW_A: Choose **System** > **High availability**. Go to the connection synchronization page. Perform configuration in active/active mode in the same way as in active/standby mode.

5. Configure FW_A: If a floating IP address is configured, set its unit ID to be the same as the device's unit ID so that the floating IP address takes effect on the device. Choose **Network** > **Interface** > **VLAN list**. Select the desired floating IP address.



General Properties

Interface: ge0/3

Name: ge0/3

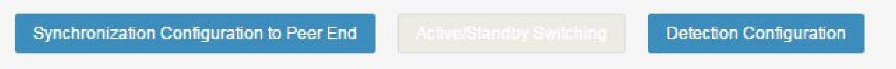
IP Address

Address Mode: ● Static ○ DHCP ○ PPPoE

IPv4 IP Address/Mask 172.16.10.100/24 ☑ Floating IP Address UID 1

Type	IP Address/Mask	Floating IP Address	UID	
IPv4	172.16.10.1/24	No	0	☒
IPv4	172.16.10.100/24	Yes	1	☒

6. Choose **System** > **High availability** > **Monitoring** to check HA status management.



Synchronize configurations to the peer: Click this button to synchronize the configurations to the peer end. Restart the peer device to make the configurations take effect.

Active/Standby switchover: This button is grayed out in active/active mode.

Check configurations: Click this button to check whether configurations are consistent between the local and peer end. If not, synchronize the configurations.

7. Configure FW_B in the same way as FW_A.

⚠ Notice	In active/active mode, unit IDs are used to differentiate the services and configurations on the two devices. If unit IDs are incorrect, services may be abnormal. Modify floating IP addresses together with unit IDs.

This completes the basic configuration of the HA active/active mode. If you want to configure fault monitoring, then configure interface monitoring, link aggregation monitoring, or gateway monitoring in accordance with section 69.5 "Configuring HA Monitoring." To enable service forwarding, you need to configure interfaces, routes, NAT, and other features. For details, see related sections.

70 VRRP

70.1 Overview

Introduction

Normally, all the hosts in the same network segment are configured with the same default route with a gateway as the next hop. Packets sent by the hosts to other network segments are diverted to the gateway along the default route for forwarding, which enables communication between the hosts and external networks. When the gateway is faulty, the hosts cannot communicate with external networks.

The default route facilitates configuration but poses high stability requirements for the gateway. Adding egress gateways is a common method to improve system reliability, but raises the issue of route selection among multiple egresses.

The Virtual Router Redundancy Protocol (VRRP) adds routers with the gateway function to a backup group to form a virtual router. The VRRP election mechanism determines which router will assume the forwarding role. The hosts in a LAN only need to configure the virtual router as the default gateway.

VRRP provides fault tolerance, improves reliability, and simplifies host configuration. In a multicast or broadcast LAN, such as the Ethernet, VRRP ensures high reliability of the default link even when a device is faulty, and avoids network interruption resulting from single link failure. You do not need to modify dynamic routing protocols and route discovery protocols.

VRRP backup group

A backup group is a set of routers in a VRRP-enabled LAN. Among the routers, one is the master router and the others are backup routers. T he backup group is equivalent to a virtual router.

Virtual IP address

A virtual router has an IP address. After hosts in the LAN know the IP address of the virtual router and set it as the next-hop address of the default route, the hosts can communicate with external networks through the virtual router.

Router priority in the backup group

VRRP determines the role (master or backup) of each router in the backup group based on priority. A router with higher priority is more likely to become the master router.

Operation mode of routers in a backup group

The routers in a backup group operate in two modes:

Non-preemptive mode: While the master router operates properly, any backup router configured with a higher priority than the master router will not become the master router.

Preemptive mode: Once a backup router finds that its priority is higher than the master router, the backup router sends a VRRP advertisement packet. A new master is elected in the backup group, and the original master router becomes a backup router.

Authentication mode of routers in a backup group

VRRP provides two authentication modes:

Text: Simple character authentication. You can configure text authentication in a network that may suffer security threats. A router adds an authentication key to the VRRP packet to be sent. The receiving router compares the authentication key in the VRRP packet with the local authentication key. If the two authentication keys are the same, the received packet is authentic and valid; otherwise, it is invalid.

MD5: MD5 authentication. You can configure MD5 authentication in a highly unsafe network. A router uses an authentication key and MD5 algorithm to encrypt the VRRP packet to be sent, and stores the encrypted packet in the authentication header. The receiving router decrypts the packet using an authentication key and checks the packet validity.

You can choose not to configure authentication in a secure network.

⚠ Notice

Authentication is not supported in VRRPv3.

VRRP timer

1. Timer for advertisement packet transfer

You can configure a VRRP timer to adjust the interval at which the master router sends VRRP advertisement packets. If a backup router receives no VRRP advertisement packets after three intervals, it considers itself as the master router and sends a VRRP advertisement packet to initiate master router election.

2. Timer for preemption delay

In a network with unstable performance, the backup routers may fail to receive packets from the master router due to network congestion, causing frequent master/backup switchover in the backup group. You can configure VRRP preemption delay to address this issue.

Backup routers wait until three packet sending intervals and preemption delay elapse. If a backup router receives no VRRP advertisement packets during the wait time, it considers itself as the master router and sends a VRRP advertisement packet to initiate master router election.

VRRP packet format

VRRPv2 and VRRPv3 packet formats are supported.

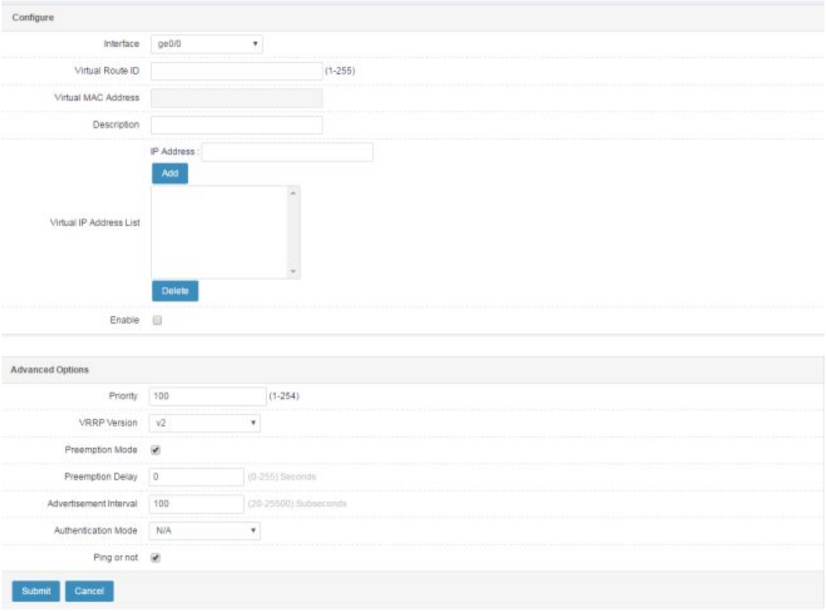
70.2 VRRP Configuration

70.2.1 Configuring VRRP

Procedure:

1. Choose **Network** > **Interface** > **VLAN**. Configure an IP address for a VLAN interface.
2. Create a VRRP backup group.

Choose **System** > **VRRP** and click **New**. The following page appears.



Configure

Interface	ge0/0 ▾
Virtual Route ID	(1-255)
Virtual MAC Address	
Description	
Virtual IP Address List	IP Address : Add Delete
Enable	□

Advanced Options

Priority	100 (1-254)
VRRP Version	v2 ▾
Preemption Mode	☑
Preemption Delay	0 (0-255) Seconds
Advertisement Interval	100 (20-25500) Subseconds
Authentication Mode	N/A ▾
Ping or not	☑

Interface: Select an interface from the drop-down list.

Virtual route ID: Set the ID of the VRRP backup group. The value ranges from 1 to 255.

Each VRID must be unique under an interface, but VRIDs can be reused under different interfaces.

Virtual MAC address: It takes effect after **Virtual route ID** is set.

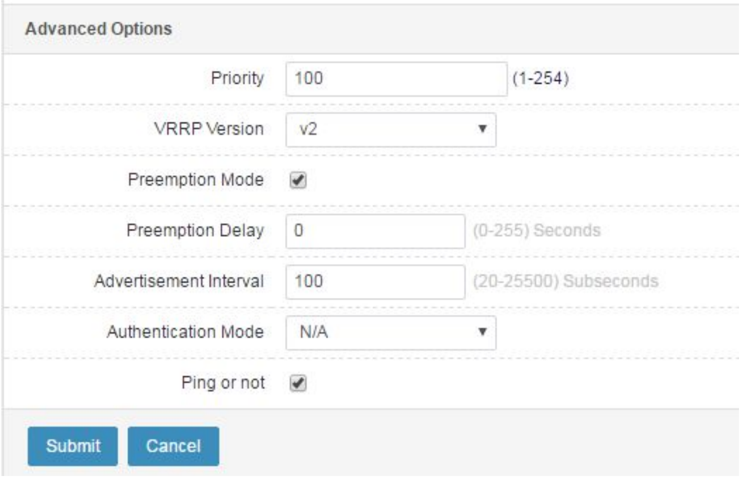
Description: Enter description to facilitate management.

Virtual IP address list: Set the virtual IP address of the backup group.

- The IP address of the virtual router may be an available IP address in the network segment where the backup group is located, or it may be the same as the interface IP address of a router in the backup group.
- The router whose interface IP address is the same as the virtual IP address is called the IP address owner, and its priority is forcibly set to 255, the highest priority.
- Only one IP address owner is allowed in the same VRRP backup group.
- If the interface connects to multiple subnets, you can configure multiple virtual IP addresses for the backup group to back up the routers in different subnets.
- The following addresses cannot be configured as a virtual IP address: address only containing zeros (0.0.0.0), broadcast address (255.255.255.255), loopback address, non-A/B/C category address, and invalid IP address, such as 0.0.0.1.
- The backup group operates properly only when the virtual IP address is a valid host address and is in the same network segment as the interface IP address. The backup group does not take effect if the virtual IP address is in a different network segment from the interface IP address or is a network address or broadcast address in the network segment where the interface IP address is located, though in which case the virtual IP address can still be configured.

Enable: Check this box to enable VRRP.

Advanced options: Configure advanced settings, as shown in the following figure.



Advanced Options

Priority	100	(1-254)
VRRP Version	v2 ▾	
Preemption Mode	☑	
Preemption Delay	0	(0-255) Seconds
Advertisement Interval	100	(20-25500) Subseconds
Authentication Mode	N/A ▾	
Ping or not	☑	

Priority: The VRRP priority ranges from 0 to 255 (the greater the value, the higher the priority). The configurable range is 1 to 254. Priority 0 is reserved for special use. Priority 255 is reserved for the IP address owner. A router which is the IP address owner always has priority 255. Therefore, the IP address owner (if any) in a backup group is always the master router as long as it operates properly.

VRRP version: VRRPv2 or VRRPv3 packet format.

Preemptive mode and **Preemption delay**: After preemption is enabled, the preemption delay ranges from 0 to 255, in seconds.

Advertisement interval: The value ranges from 10 to 25500, in subseconds (1 subsecond = 1/100 seconds).

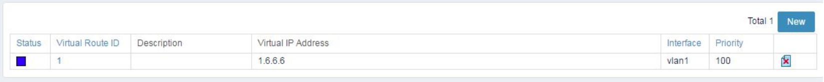
Authentication mode: In VRRPv2, the options include **None** (no authentication), **Text** (simple character authentication), and **MD5** (MD5 authentication). In VRRPv3, authentication is not supported.

Pingable?: According to VRRP, the virtual IP address is unpingable if it is different from any real IP address on the interface. If you want to ping the gateway and virtual IP address, check the **Pingable?** box.

3. Click **Submit**.

70.2.2 Modifying a VRRP Backup Group

Click the ID (in blue) of the VRRP backup group you want to modify, as shown in the following figure.



Status	Virtual Route ID	Description	Virtual IP Address	Interface	Priority	
■	1		1.6.6.6	vlan1	100	☒

Modify the group information. **Interface** and **Virtual route ID** cannot be modified.

70.2.3 Deleting a VRRP Backup Group

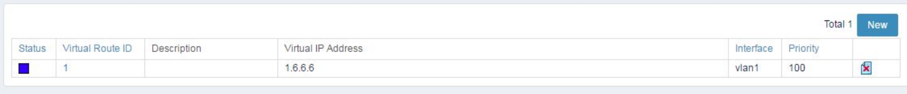
Click ☒ next to the VRRP backup group you want to delete. Click **OK** in the confirmation prompt box.

⚠ Notice

If an interface is canceled (for example, a physical interface in a VLAN is removed in hot swap mode or a VLAN interface is deleted), then all the backup groups under the interface are automatically deleted.

70.2.4 Displaying VRRP Backup Groups

Go to the VRRP configuration page, as shown in the following figure.



Total 1 New

Status	Virtual Route ID	Description	Virtual IP Address	Interface	Priority	
■	1		1.6.6.6	vlan1	100	☒

Status: Initialize (■), Backup (○), or Master (●). The latter two are operating states.

Virtual route ID: Backup group ID.

Virtual IP address: Multiple virtual IP address are listed.

Interface: VRRP-enabled VLAN interface.

Priority: Priority.

70.3 Configuration Examples

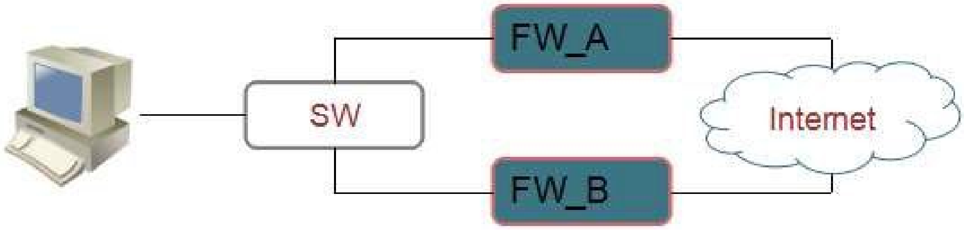
70.3.1 Example 1: Configuring a Single Backup Group

Description:

In single backup group mode, only the master router processes services. When the master router is faulty, a backup router is elected as the new master to take over services. Only one backup group is required in active/standby mode. Different routers in the backup group have different priorities. The router with the highest priority becomes the master router.

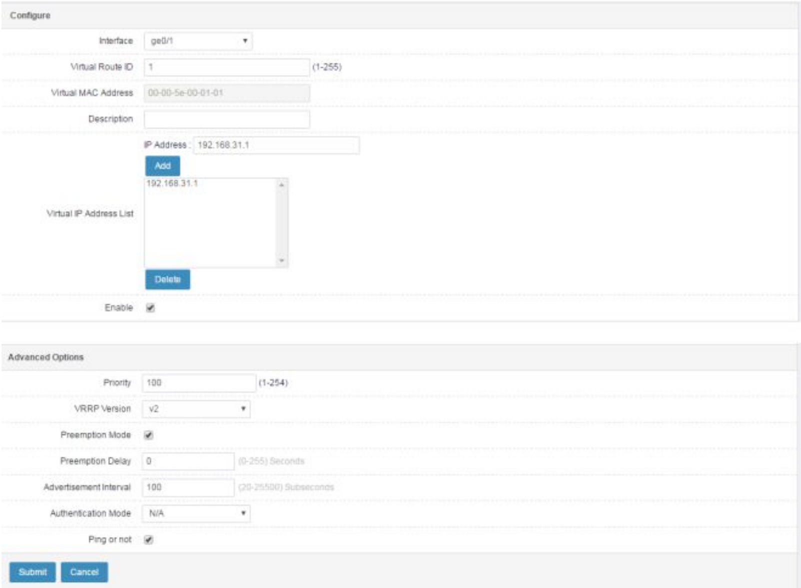
Hosts in a LAN use IP address 192.168.31.1 as their default gateway. Configure FW_A and FW_B as backup group 1.

Network diagram:



Procedure:

1. On FW_A, choose **System** > **VRRP** and click **New**. Complete the settings on the following page.



Configure

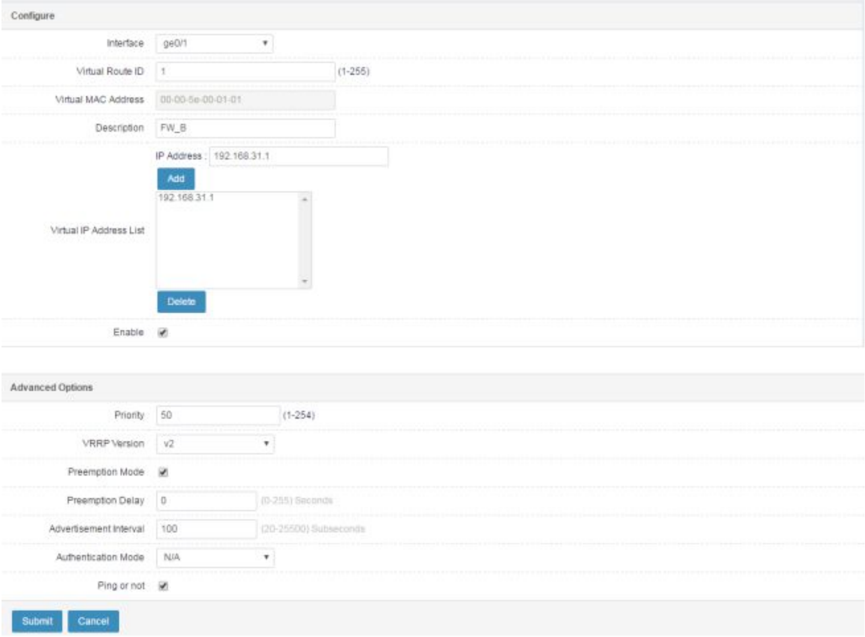
Interface	ge0/1 ▾
Virtual Route ID	1 (1-255)
Virtual MAC Address	00-00-5e-00-01-01
Description	
Virtual IP Address List	IP Address : 192.168.31.1 Add 192.168.31.1 Delete
Enable	☑

Advanced Options

Priority	100 (1-254)
VRRP Version	v2 ▾
Preemption Mode	☑
Preemption Delay	0 (0-255) Seconds
Advertisement Interval	100 (20-25500) Subseconds
Authentication Mode	N/A ▾
Ping or not	☑

Set **VRID** to **1**, **Priority** to **100**, and **Virtual IP address** to **192.168.31.1**. Check the **Enable** box. Click **Submit**.

2. On FW_B, choose **System** > **VRRP** and click **New**. Complete the settings on the following page.



Configure

Interface	ge0/1 ▾
Virtual Route ID	1 (1-255)
Virtual MAC Address	00-00-5e-00-01-01
Description	FW_B
Virtual IP Address List	IP Address : 192.168.31.1 Add 192.168.31.1 Delete
Enable	☑

Advanced Options

Priority	50 (1-254)
VRRP Version	v2 ▾
Preemption Mode	☑
Preemption Delay	0 (0-255) Seconds
Advertisement Interval	100 (20-25500) Subseconds
Authentication Mode	N/A ▾
Ping or not	☑

Set **VRID** to **1**, **Priority** to **50**, and **Virtual IP address** to **192.168.31.1.** Check the **Enable** box. Click **Submit.**

3. After configuration, check that FW_A is the master router, and FW_B is the backup router.

70.3.2 Example 2: Configuring Multiple Backup Groups for Load Sharing

Description:

Configure multiple backup groups on an interface so that a router is the master router in one backup group and is a backup router in the other backup groups.

In load sharing mode, services are distributed to multiple routers, which requires two or more backup groups. Each backup group has a master router and several backup routers. The backup groups may have different master routers.

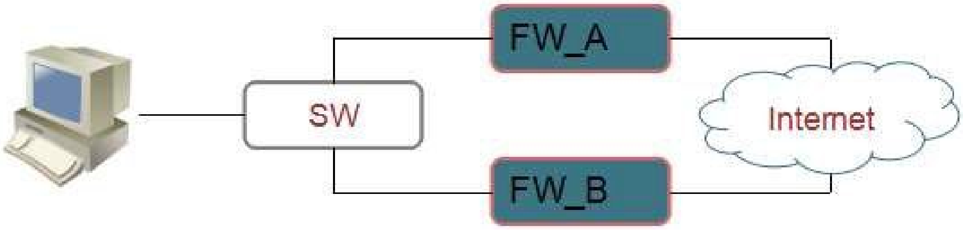
Configure FW_A and FW_B in the LAN to form two backup groups.

Backup group 1: Configure FW_A as the master router and FW_B as the backup router, with virtual IP address 192.168.31.1.

Backup group 2: Configure FW_A as the backup router and FW_B as the master router, with virtual IP address 192.168.31.2.

To enable load sharing between FW_A and FW_B, configure the default gateways for the hosts in the LAN as 192.168.31.1 and 192.168.31.2. When configuring priority, ensure that the VRRP priorities of the routers in the two backup groups map to one another.

Network diagram:

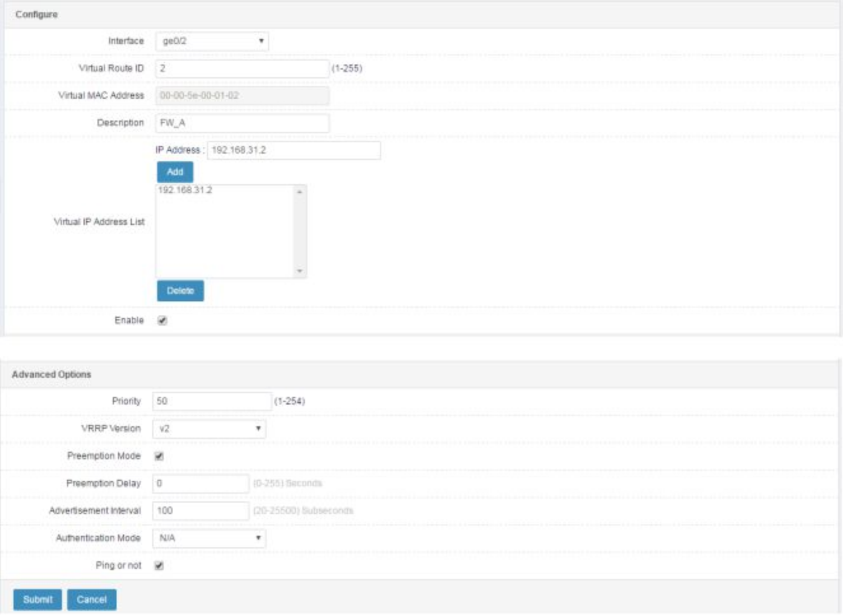


Procedure:

1. On FW_A, choose **System** > **VRRP** and click **New**. Complete the settings in the same ways as in Example 1.

   Set **VRID** to **1**, **Priority** to **100**, and **Virtual IP address** to **192.168.31.1**. Check the **Enable** box. Click **Submit**.

2. Configure backup group 2 on FW_A. Complete the settings on the following page.



Configure

Interface	ge0/2 ▾
Virtual Route ID	2 (1-255)
Virtual MAC Address	00-00-5e-00-01-02
Description	FW_A
Virtual IP Address List	IP Address : 192.168.31.2 192.168.31.2
Enable	☑

Advanced Options

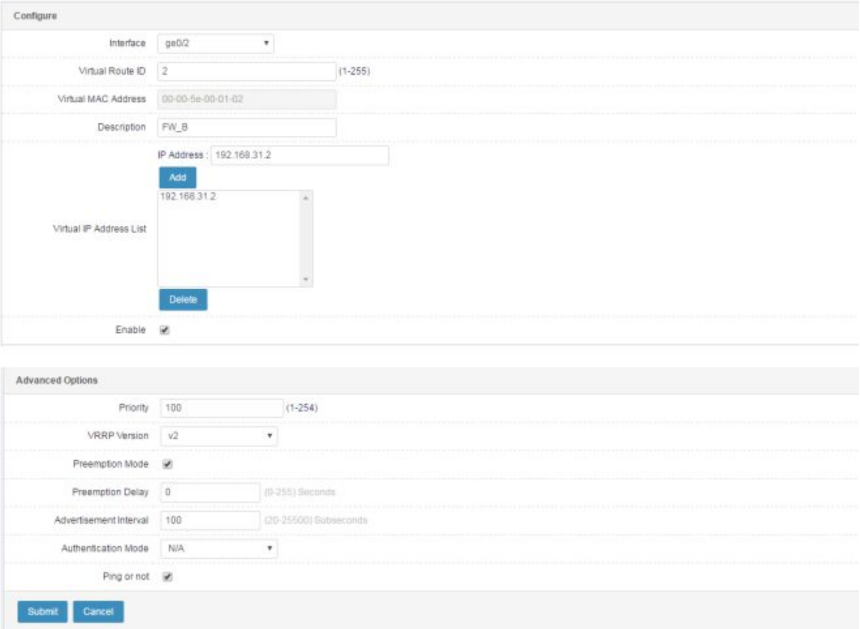
Priority	50 (1-254)
VRRP Version	v2 ▾
Preemption Mode	☑
Preemption Delay	0 (0-255) Seconds
Advertisement Interval	100 (20-25500) Subseconds
Authentication Mode	N/A ▾
Ping or not	☑

Set **VRID** to **2**, **Priority** to **50**, and **Virtual IP address** to **192.168.31.2**. Check the **Enable** box. Click **Submit**.

3. On FW_B, choose **System** > **VRRP** and click **New**. Complete the settings in the same ways as in Example 1.

Set **VRID** to **1**, **Priority** to **50**, and **Virtual IP address** to **192.168.31.1**. Check the **Enable** box. Click **Submit**.

4. Configure backup group 2 on FW_B. Complete the settings on the following page.



Configure

Interface	ge0/2 ▾	
Virtual Route ID	2	(1-255)
Virtual MAC Address	00-00-5e-00-01-02	
Description	FW_B	
Virtual IP Address List	IP Address : 192.168.31.2 192.168.31.2	
Enable	☑	

Advanced Options

Priority	100	(1-254)
VRRP Version	v2 ▾	
Preemption Mode	☑	
Preemption Delay	0	(0-255) Seconds
Advertisement Interval	100	(20-25500) Subseconds
Authentication Mode	N/A ▾	
Ping or not	☑	

Set **VRID** to **2**, **Priority** to **100**, and **Virtual IP address** to **192.168.31.2**. Check the **Enable** box. Click **Submit**.

70.4 Troubleshooting

A Backup Group Does Not Work After Being Enabled

Symptom	A backup group is always in the Initialize state after being enabled.
Analysis	The interface to which the backup group belongs is not up, or the network cable is not properly inserted.
Solution	In some cases, a backup group does not work even after it is enabled. To enter the running state, the backup group must meet the following conditions: 1. The interface is up. 2. Carrier signals are detected on the network cable connected to the interface. 3. At least one real IP address is configured on the interface. 4. At least one virtual IP address is configured for the backup group. 5. The backup group is enabled. If any of the preceding conditions is not met, the backup group does not work.