RG-WALL 1600 Series Next-Generation Firewall Cook Book V1.2

Copyright Statement

Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Obtaining Technical Assistance

- Ruijie Networks website: http://www.ruijienetworks.com/
- Ruijie Networks service portal: http://caseportal.ruijienetworks.com

1 Table of Contents

2 Firewall Maintenance

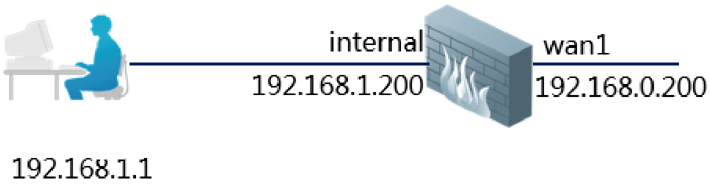
2.1 Device Management

2.1.1 Web-based Management

Networking Requirements

Via a Web visual interface, you can configure the firewall, for example, configure the management function of the wan1 interface.

Network Topology



Configuration Tips

The default IP address of the NGFW is 192.168.1.200, and you can perform Web management via HTTPS (the default user name is **admin**, and the default password is **firewall**). The models of management interfaces are as follows:

```
RG-WALL 1600-X9300:   mgmt1 interface
RG-WALL 1600-X8500:    mgmt1 interface
RG-WALL 1600-X6600:    mgmt1 interface
RG-WALL 1600-M5100:   mgmt interface
RG-WALL 1600-S3600:    internal interface, corresponding to the switching interfaces 1
to 14
RG-WALL 1600-S3100:   internal interface, corresponding to the switching interfaces 1
to 7
```

All switching interfaces of the S3100 and S3600 are Layer-3 internal interfaces; only internal interfaces are suitable for Layer-3 configurations, for example, IP address configurations.

Set the IP address of the PC to 192.168.1.1/24, connect to the internal interface or MGMT interface, open the IE browser, enter https://192.168.1.200 to log in to the NGFW management page, and enter the user name **admin** and password **firewall** to open the NGFW page. If you forget the password, you can restore the initial password as instructed in the section “Firewall Maintenance” > “Password Recovery”.

After you log in to the device, enable the management function of the wan1 interface.

By default, other interfaces have no IP addresses, and other management functions (for example, HTTPS) are not enabled on other interfaces.

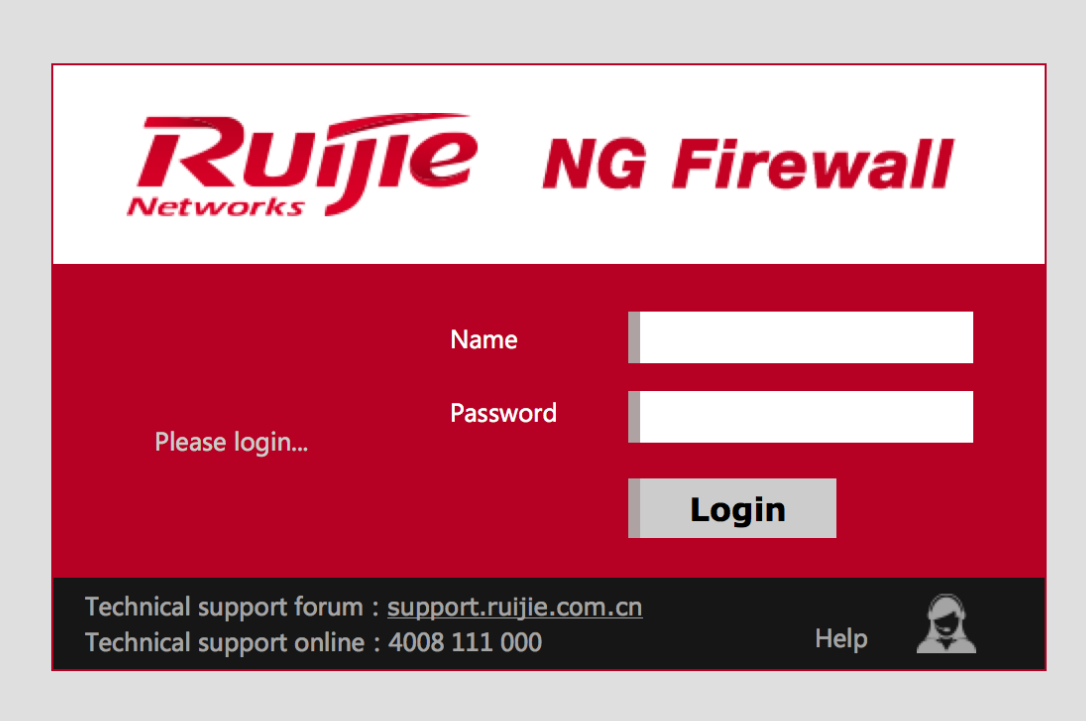
If the firewall interface address is modified but you forget the new password, you can enter the CLI to view the current configurations.

It is recommended that you use Firefox or IE10 (or above). If you use a third-party browser (for example, 360 and Travel), use the top speed mode.

Configuration Steps

1. When the NGFW is configured with default values, set the IP address of the PC to **192.168.1.1**, and set the IP address of the gateway to **192.168.1.200**;

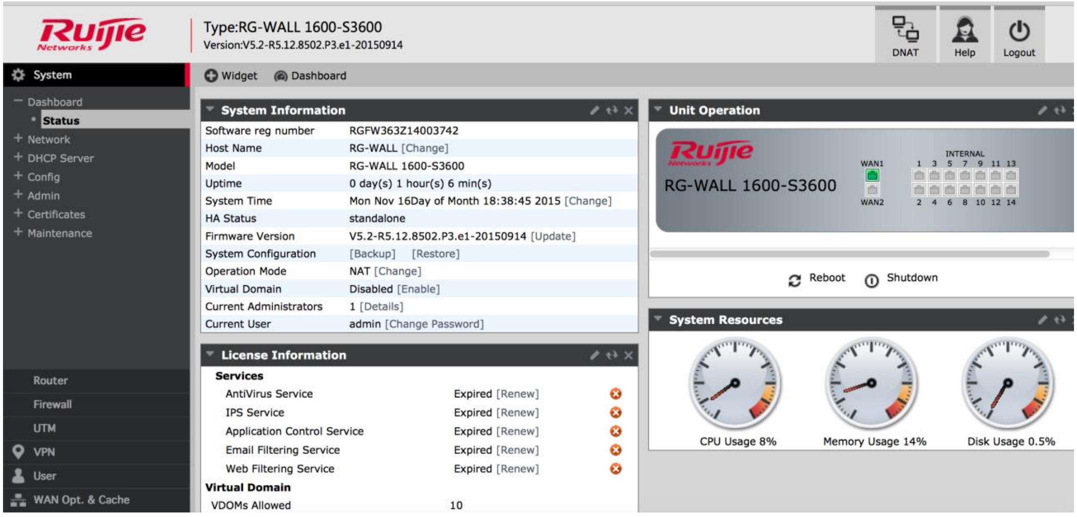
In the address bar of the IE browser, enter **https://192.168.1.200**, and the firewall login page pops up.



Please login...

Technical support forum : support.ruijie.com.cn
Technical support online : 4008 111 000

Enter the user name **admin** and default password **firewall**, and then the homepage of the firewall pops up.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

System Information

Software reg number	RGFW363Z14003742
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3600
Uptime	0 day(s) 1 hour(s) 6 min(s)
System Time	Mon Nov 16Day of Month 18:38:45 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.12.8502.P3.e1-20150914 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

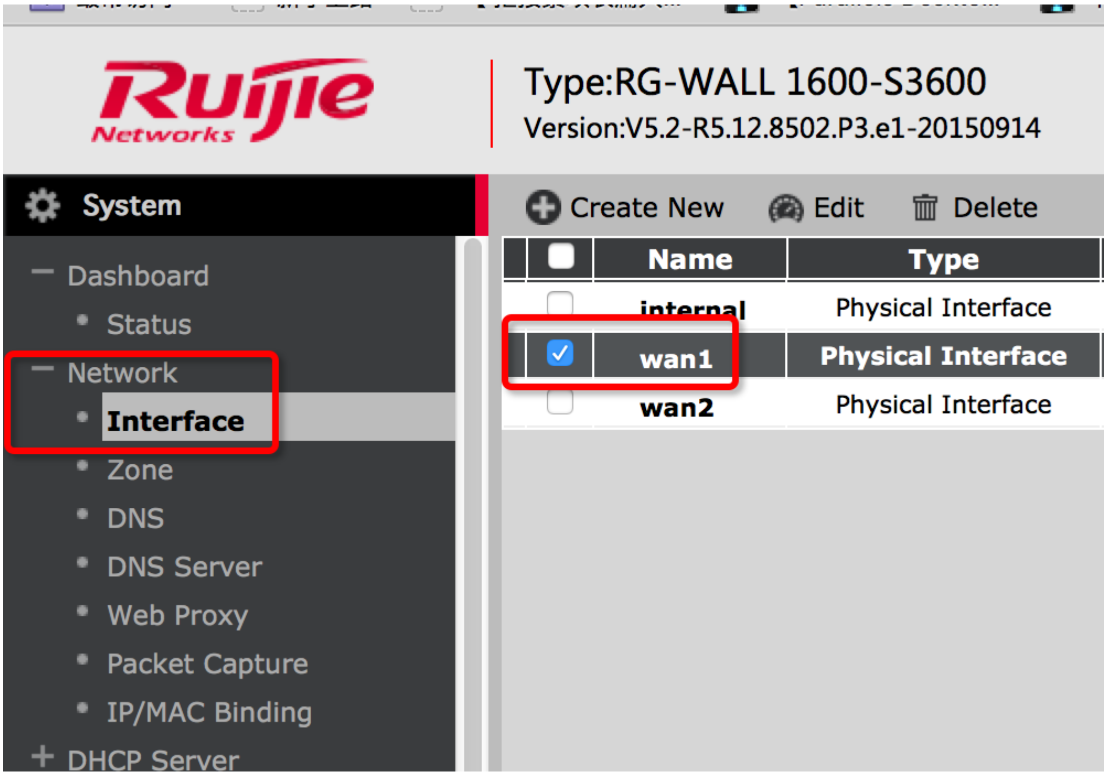
License Information

Services	
AntiVirus Service	Expired [Renew]
IPS Service	Expired [Renew]
Application Control Service	Expired [Renew]
Email Filtering Service	Expired [Renew]
Web Filtering Service	Expired [Renew]
Virtual Domain	
VDOMs Allowed	10

CPU Usage 8%
Memory Usage 14%
Disk Usage 0.5%

2. Set the IP address of the wan1 interface to **192.168.33.51/24**, and enable the management function of the internal interface.

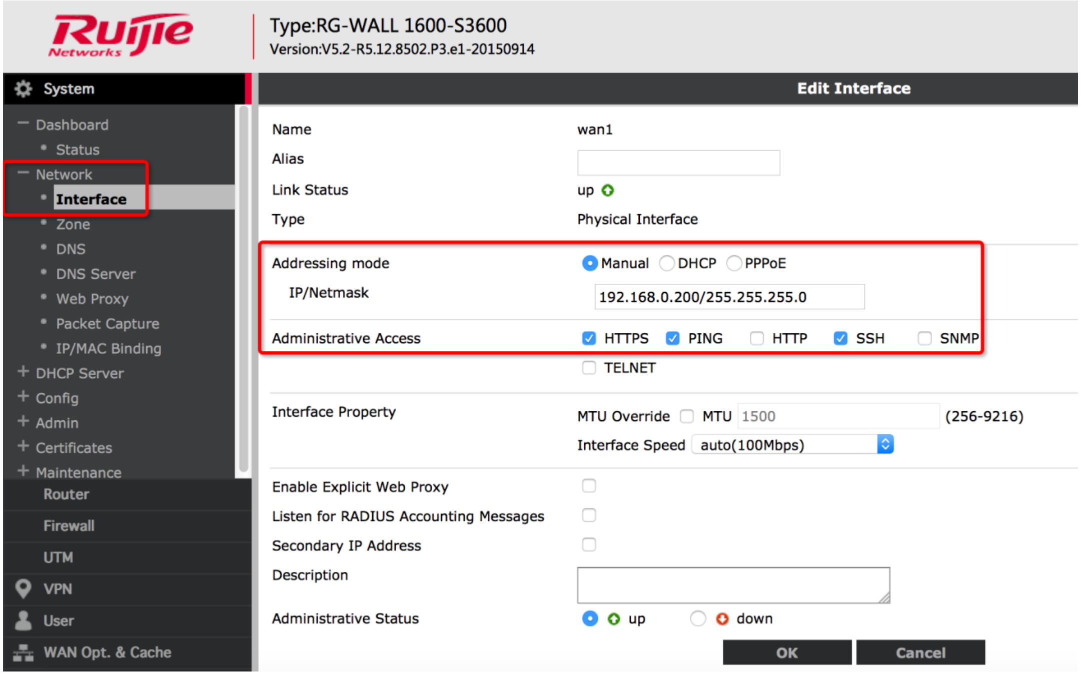
Choose the **System** > **Network** > **Interface** menu.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

☐	Name	Type
☐	internal	Physical Interface
☑	wan1	Physical Interface
☐	wan2	Physical Interface

Double-click the wan1 interface to edit the following parameters:



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Interface

Name	wan1
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.0.200/255.255.255.0
Administrative Access	☑ HTTPS ☑ PING ☐ HTTP ☑ SSH ☐ SNMP ☐ TELNET
Interface Property	MTU Override ☐ MTU 1500 (256-9216) Interface Speed auto(100Mbps)
Enable Explicit Web Proxy	☐
Listen for RADIUS Accounting Messages	☐
Secondary IP Address	☐
Description	
Administrative Status	● up ○ down

OK Cancel

Set the IP address of the interface to **192.168.0.200/24**.

Administrative Access: Select **HTTPS**, **PING**, and **SSH**. Their meanings are as follows:

HTTPS: Allow users to use https://192.168.0.200 to manage the device;

Ping: Users are allowed to ping this interface address. If it is deselected, the interface address cannot be pinged through even if the interface address is reachable;

HTTP: Allow users to use http://192.168.0.200 to manage the device;

SSH: Allow users to use ssh 192.168.0.200 to manage the device;

SNMP: Allow users to perform SNMP management via the interface;

TELNET: Allow users to use telnet 192.168.0.200 to manage the device.

Verification

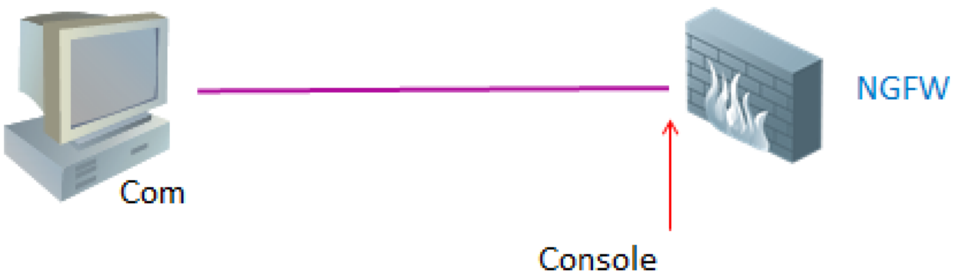
Enter https://192.168.0.200 in the browser, and then verify the configurations.

2.1.2 Console Management

Networking Requirements

To perform configuration management, you can use HyperTerminal or CRT to enter the CLI via a Console cable. By default, the firewall allows Console management.

Network Topology



Configuration Tips

1. Prepare a Console cable and a PC.
2. Connect the Console cable.

Connect the RJ45 connector end of the Console cable to the Console port of the PC, and connect the other end of the Console cable to the com port of the PC.

3. Configure the HyperTerminal

a) A PC under Windows XP is equipped with built-in HyperTerminal; for a PC under Windows 7, you need to install HyperTerminal separately.

b) By default, the Windows Sever 2003 is not equipped with HyperTerminal. You need to install it in **Control Panel** > **Add/Delete Program**, or directly download it from **Attachment 1**.

c) If you fail to enter the CLI after configurations, check whether the Console cable is connected to the Console port, whether the data bits of HyperTerminal are configured correctly, and whether you click Restore Defaults. If you nevertheless fail to center the CLI after performing the above operations, attempt to replace the PC, Console cable and HyperTerminal.

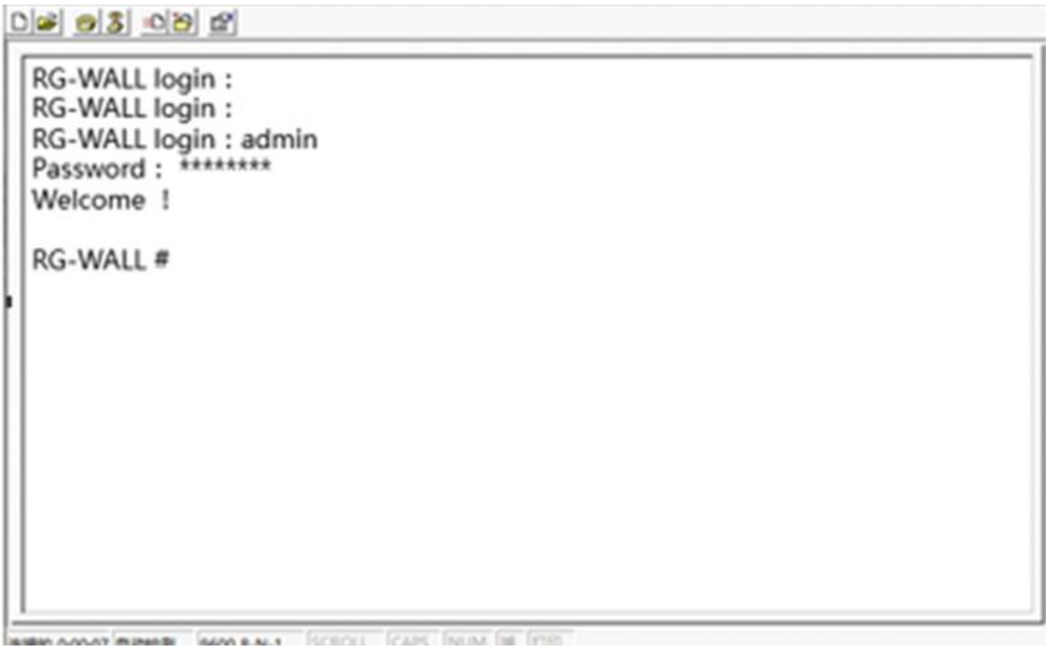
Operation Steps

1. Prepare a Console cable and a PC
2. Connect the Console cable

   Insert the RJ45 connector end of the Console cable to the Console port of the network device (the Console port is usually beside the Ethernet port of the network device, and is marked with **Console**), and then insert the DB9 port of the Console cable to the Com port of the PC.
3. Configure the HyperTerminal

Verification

Press the **Enter** key, and the system displays **RG-WALL login**, prompting you to enter the username **admin** and password **firewall** (if the password is changed or you forget the password, you can do as instructed in the section “Password Recovery”).



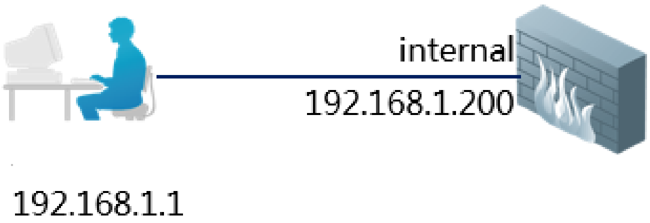
```
RG-WALL login :
RG-WALL login :
RG-WALL login : admin
Password :  ********
Welcome  !

RG-WALL #
```

2.1.3 SSH/Telnet

Networking Requirements

If you want to enter the CLI of a device to configure or gather the related information, you can manage the device remotely via Telnet or SSH when no Console cable is available or you are far away from the device.

Network Topology



Configuration Tips

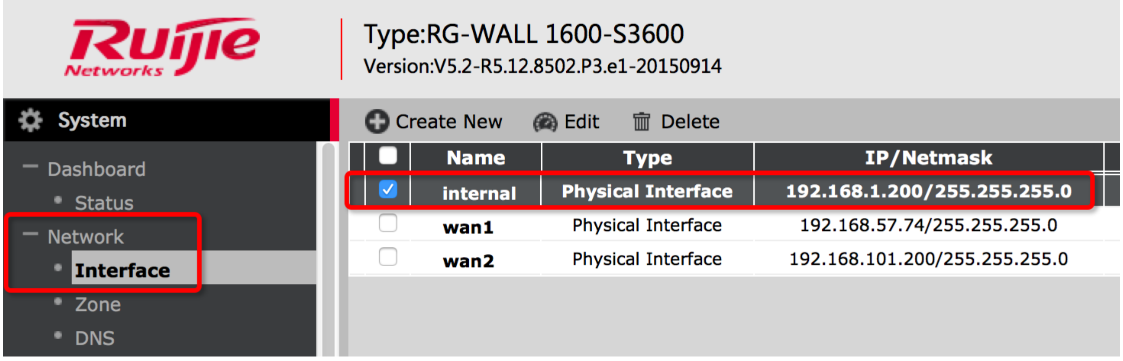
To use the Telnet or SSH mode, first ensure a high connectivity between the management host and the interface address of the device. You can tick the Ping function of the interface. If the device can ping through the management interface, it indicate that the connectivity between them is normal.

1. Enable the Telnet and SSH functions on the interface.
2. Telnet the management device.
3. SSH the management device.

Configuration Steps

1. Enable the Telnet and SSH functions on the interface

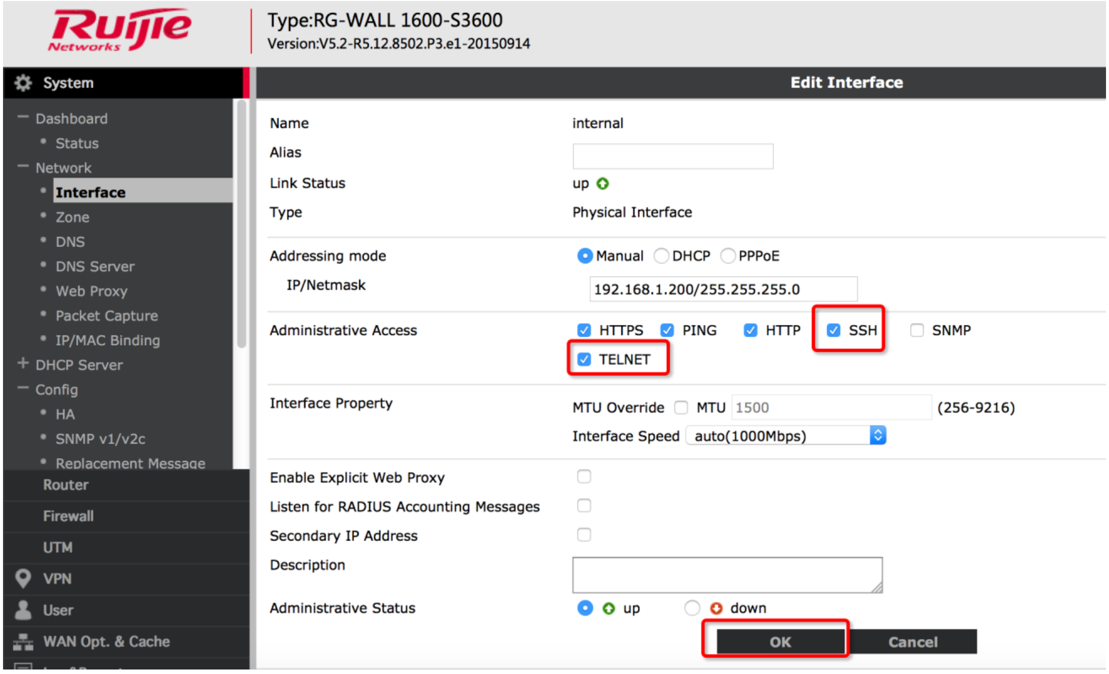
Choose the **System** > **Network** > **Interface** menu, and edit the internal interface by double-clicking it, as shown in the following figures:



Type:RG-WALL 1600-S3600

Version:V5.2-R5.12.8502.P3.e1-20150914

□	Name	Type	IP/Netmask
☑	internal	Physical Interface	192.168.1.200/255.255.255.0
□	wan1	Physical Interface	192.168.57.74/255.255.255.0
□	wan2	Physical Interface	192.168.101.200/255.255.255.0



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Interface

Name: internal
Alias:
Link Status: up
Type: Physical Interface
Addressing mode: ● Manual ○ DHCP ○ PPPoE
IP/Netmask: 192.168.1.200/255.255.255.0
Administrative Access: ☑ HTTPS ☑ PING ☑ HTTP ☑ SSH □ SNMP ☑ TELNET
Interface Property: MTU Override □ MTU 1500 (256-9216)
Interface Speed: auto(1000Mbps)
Enable Explicit Web Proxy □
Listen for RADIUS Accounting Messages □
Secondary IP Address □
Description:
Administrative Status: ● up ○ down

Tick **SSH** and **TELNET** (by default, the Telnet and ping functions of the interface are disabled), and click **OK**.

2.2 Administrator Settings

I. Requirements

According to the factory settings, the default account is admin (with all privileges), and the default password is firewall. The requirements are as follows:

Change the admin password to ruijie@123, and set the host IP address of the admin account to 172.18.10.108/32. It indicates that only this host (172.18.10.108) can use the admin account to manage devices.

Create a monitor account with "read-only" privilege. Set the password to 123456a!. Set no limit to IP address for the management host which allows admin login from all hosts, and set the permission to read-only.

Define the password policy which specifies password complexity.

Set the timeout interval of the Web page. If an administrator does not perform any operation within 90 minutes for example, the administrator will automatically log out.

II. Configuration Tips

Change the admin password and set management IP addresses.

Set **Admin Profile** to **readonly**.

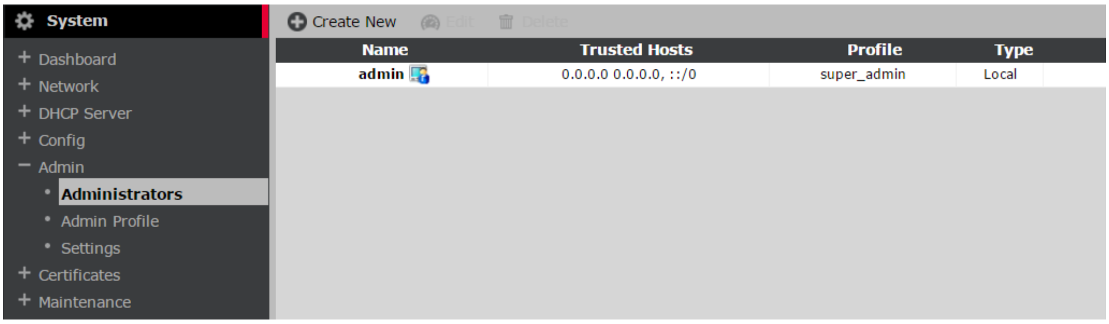
Create a **monitor** account.

Define the password policy and change administrator settings.

III. Configuration Steps

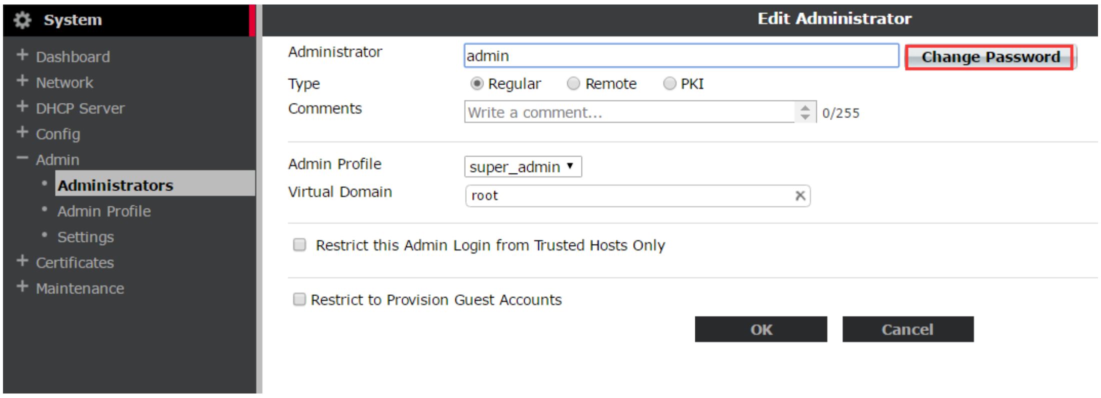
Change the admin password and set management IP addresses.

Choose **System** > **Admin** > **Administrators**.



Name	Trusted Hosts	Profile	Type
admin	0.0.0.0 0.0.0.0, ::/0	super_admin	Local

Click or double-click the editing button to set the administrator name to **admin**, and then click **Change Password**.



Administrator: admin

Type: ● Regular ○ Remote ○ PKI

Comments: Write a comment... 0/255

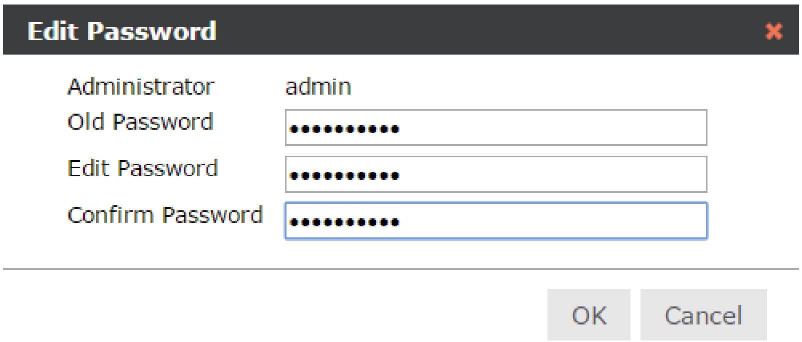
Admin Profile: super_admin

Virtual Domain: root

□ Restrict this Admin Login from Trusted Hosts Only

□ Restrict to Provision Guest Accounts

In the **Edit Password** dialog box that is displayed, change the password to **ruijie@123**, and then click **OK**.



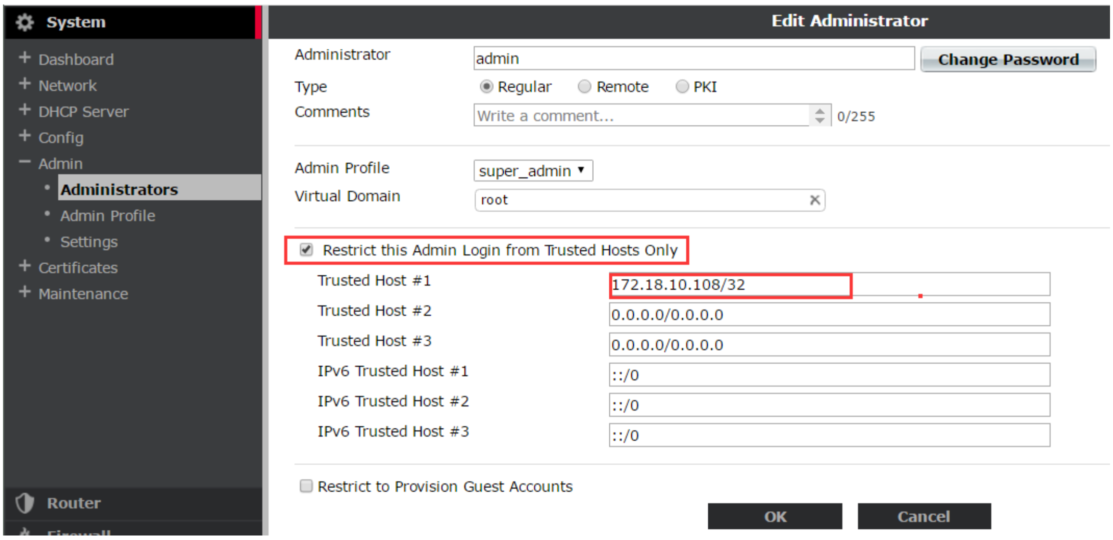
Administrator: admin

Old Password: ••••••••••

Edit Password: ••••••••••

Confirm Password: ••••••••••

Tick **Restrict this Admin Login from Trusted Hosts Only**, enter the management IP address **172.18.10.108/32** in **Trusted Host #1**, and then click **OK**.



Administrator: admin

Type: ● Regular ○ Remote ○ PKI

Comments: Write a comment... 0/255

Admin Profile: super_admin

Virtual Domain: root

☑ Restrict this Admin Login from Trusted Hosts Only

Trusted Host #1: 172.18.10.108/32

Trusted Host #2: 0.0.0.0/0.0.0.0

Trusted Host #3: 0.0.0.0/0.0.0.0

IPv6 Trusted Host #1: ::/0

IPv6 Trusted Host #2: ::/0

IPv6 Trusted Host #3: ::/0

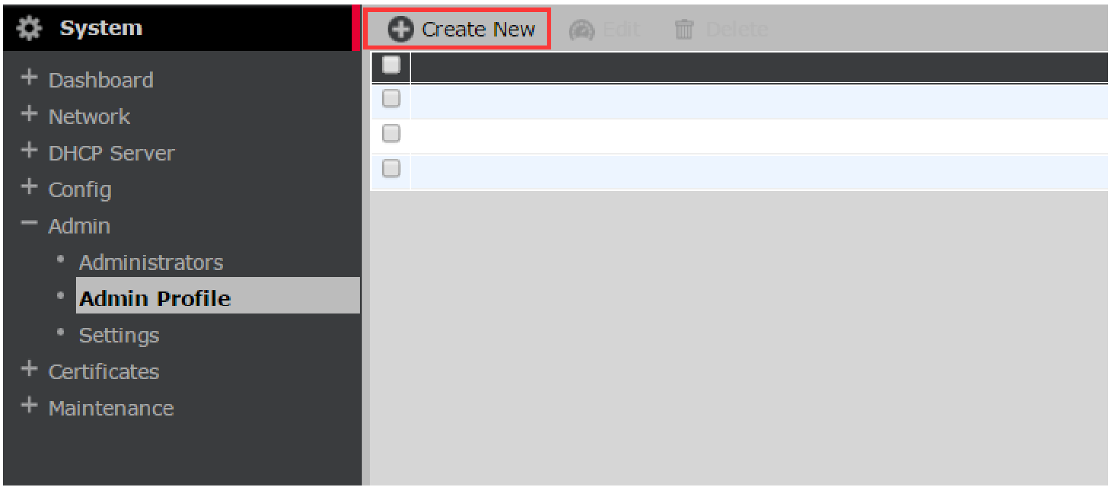
□ Restrict to Provision Guest Accounts

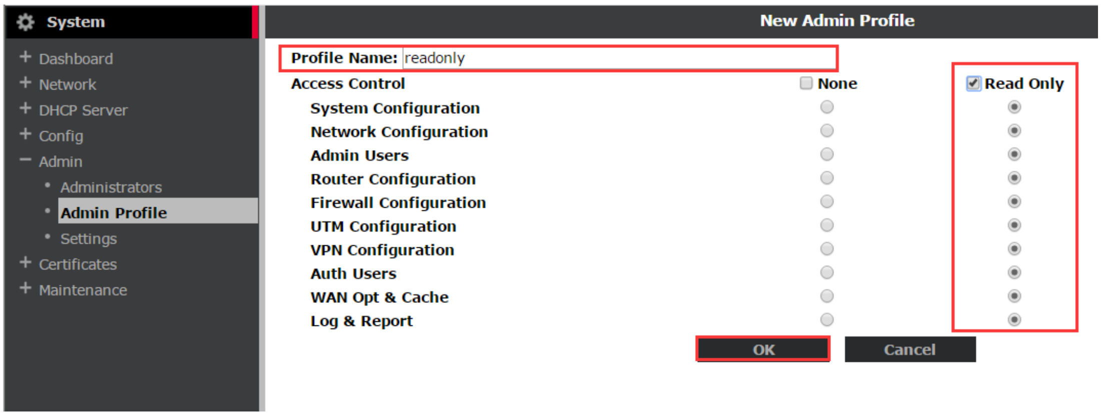
Three trusted hosts can be added on this page. Add up to 10 trusted hosts by running corresponding commands. `RG-WALL # config system admin`

```
RG-WALL (admin) # edit admin
RG-WALL (admin) # set trusthost1 172.18.10.108 255.255.255.255
RG-WALL (admin) # set trusthost2 172.19.10.108 255.255.255.255
RG-WALL (admin) # set trusthost3 172.119.10.108 255.255.255.255
RG-WALL (admin) # end
```

Set Admin Profile to readonly.

Choose **System** > **Admin** > **Admin Profile**, and then click **Create New**.





New Admin Profile

Profile Name: readonly

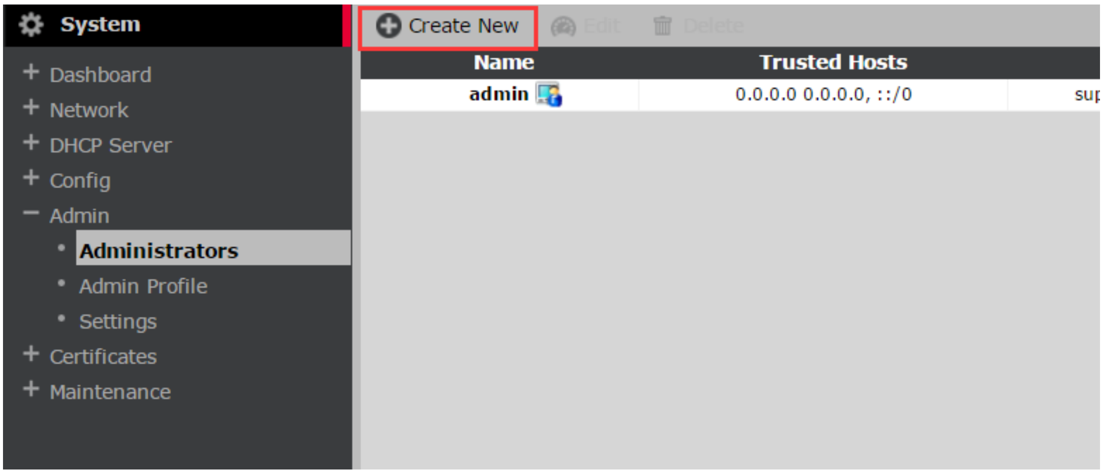
Access Control	□ None	☑ Read Only
System Configuration	○	●
Network Configuration	○	●
Admin Users	○	●
Router Configuration	○	●
Firewall Configuration	○	●
UTM Configuration	○	●
VPN Configuration	○	●
Auth Users	○	●
WAN Opt & Cache	○	●
Log & Report	○	●

Profile Name: Set it to **readonly**.

Tick **Read Only** for all items.

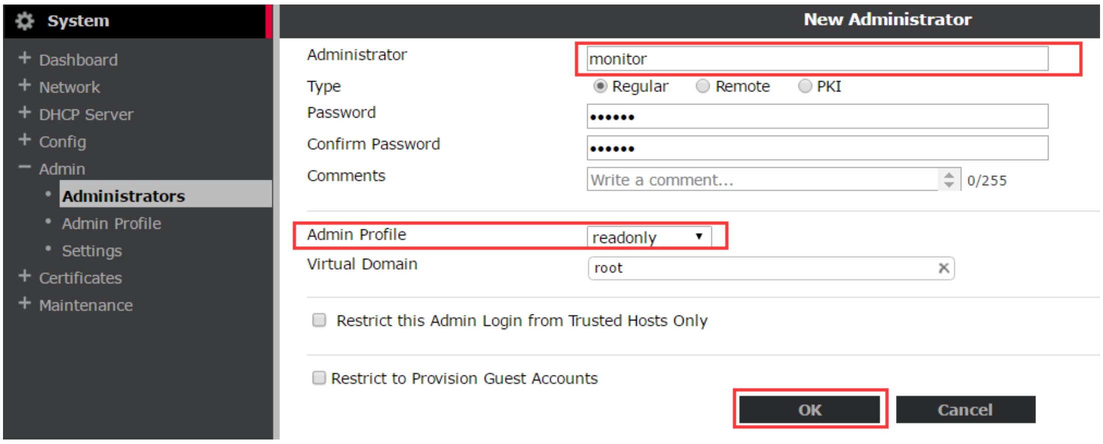
Create a monitor account.

Choose **System** > **Admin** > **Administrators**, and then click **Create New**.



Name	Trusted Hosts	
admin	0.0.0.0 0.0.0.0, ::/0	sup

Create a monitor account, set the password to **123456a!**, set **Admin Profile** to **readonly**, and set no limit to IP addresses for the management hosts, as shown in the following figure.



New Administrator

Administrator	monitor
Type	● Regular ○ Remote ○ PKI
Password	••••••
Confirm Password	••••••
Comments	Write a comment... 0/255
Admin Profile	readonly
Virtual Domain	root

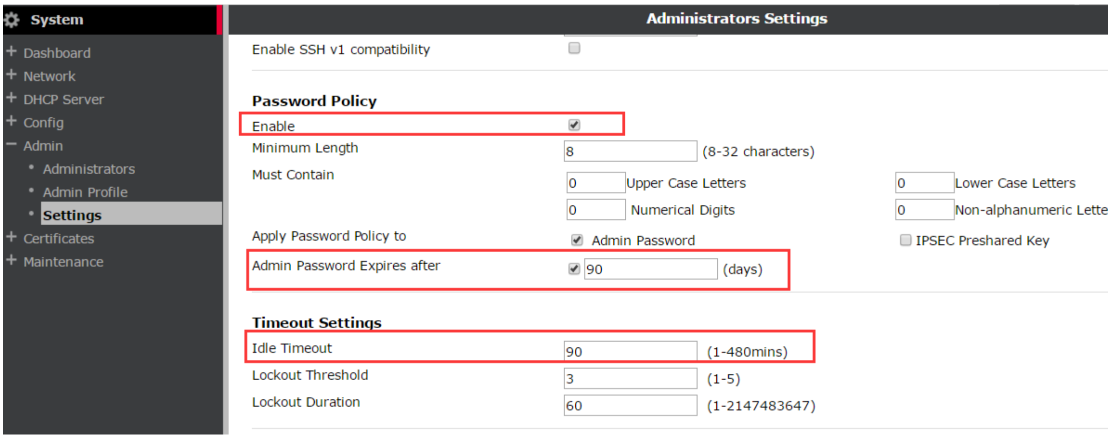
□ Restrict this Admin Login from Trusted Hosts Only

□ Restrict to Provision Guest Accounts

Define the password policy and change administrator settings.

If a password must contain at least 6 characters comprising letters, digits, and special characters (such as !@#$%&'), set the password policy as follows.

Choose **System** > **Admin** > **Settings**, as shown in the following figure.



Administrators Settings

Enable SSH v1 compatibility □

Password Policy

Enable ☑

Minimum Length 8 (8-32 characters)

Must Contain 0 Upper Case Letters 0 Lower Case Letters

0 Numerical Digits 0 Non-alphanumeric Lette

Apply Password Policy to ☑ Admin Password □ IPSEC Preshared Key

Admin Password Expires after ☑ 90 (days)

Timeout Settings

Idle Timeout 90 (1-480mins)

Lockout Threshold 3 (1-5)

Lockout Duration 60 (1-2147483647)

Enable: Tick **Enable**.

Minimum Length: It indicates the minimum length of a password.

Must Contain: It indicates limits to the number of letters, digits, and special characters)

Apply Password Policy to: Enter the admin password.

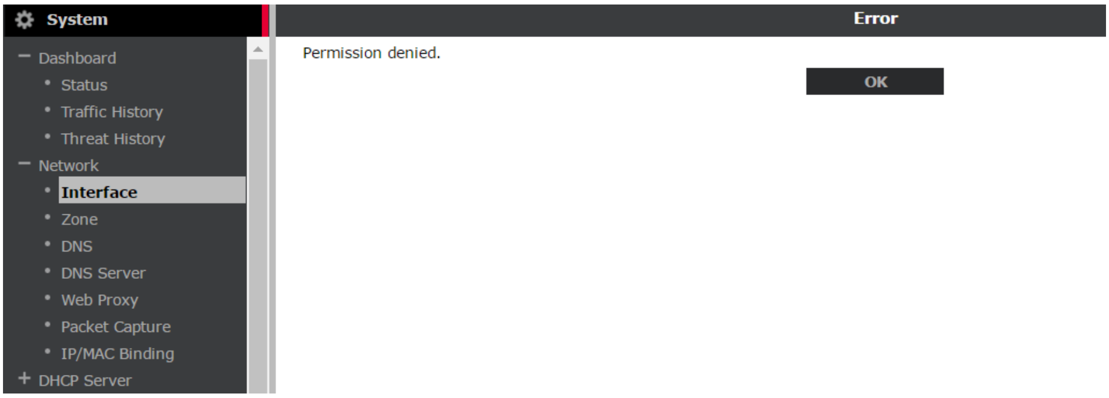
Admin Password Expires after: Configure the expiry date of a password. The system prompts the administrator to change the password after the expiry date.

Idle Timeout: If an administrator does not perform any operation within the specified time, the administrator will automatically log out.

Note: The total length of uppercase letters, lowercase letters, digits, and special characters should be less than or equal to the maximum length; otherwise, the policy setting is invalid.

IV. Verification

Log in to the monitor account and change the settings. An error prompt **Permission denied** is displayed.



Error

Permission denied.

2.3 Upgrading Software

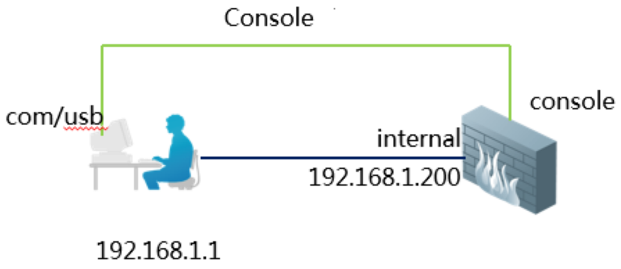
2.3.1 TFTP Upgrade

Networking Requirements

The firewall system can be upgraded via a Web interface or TFTP CLI. Here, the firewall system needs to be upgraded via TFTP.

Before the upgrade, be sure to back up the firewall configurations. For details, refer to the section “Firewall Maintenance” > “Configuration Backup and Recovery”.

Network Topology



Configuration Tips

1. Prepare tools and connect the Console cable;
2. Connect the network cable, and ensure that network communication is normal;
3. Set up the TFTP server;
4. Begin the upgrade.

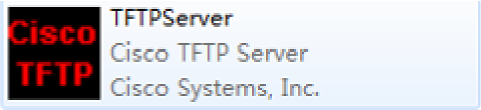
Configuration Steps

1. Prepare tools

Prepare the Console cable, network cable, upgrade file, TFTP tool, and cable for USB conversion (the PC has no Com port), and install the driver;

2. Connect the network cable, and ensure that network communication is normal;
3. Set up the TFTP server;
4. Begin the upgrade.

You can download the Cisco TFTP server from the attachment.



TFTPServer
Cisco TFTP Server
Cisco Systems, Inc.

Run the Cisco TFTP software, and save the upgrade firmware into the folder in the red frame below (when you install the software, the system will specify a folder), for example, c:\tftp.

Restart the device, and perform the following steps:

5. Enter M (press **Shift** + **m**), and enter the BIOS menu:

```
...
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  Configuration and information.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.
```

6. Select **F** to set format to the Flash card;

```
Enter Selection [G]:

Enter G,F,B,I,Q,or H:  F                              // Select F to set format to the
Flash card. Optional

All data will be erased,continue:[Y/N]?Y
```

7. Select **G** to download the mirror file:

```
Enter G,F,B,I,Q,or H:  G                              // Select G to download the
mirror file from the server.
Please connect TFTP server to Ethernet port "MGMT1".       // Connect the PC to the MGMT1
port of the firewall.

Enter TFTP server address [192.168.1.1]:                 // Enter the address of the TFTP
server.
Enter local address [192.168.1.200]:                      // Assign a temporary IP address
to MGMT1.
Enter firmware image file name [image.out]: Ruijie_XXX_ .bin    // Enter the name of the
mirror file.
MAC:14144B7EE172
###########################################
```

8. The TFTP server prompts successful download:

```
Total 45387871 bytes data downloaded.
Verifying the integrity of the firmware image.

Total 262144kB unzipped.
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?d        // Serve
as the default boot file.
Programming the boot device now.
.........................................................................................
.........................................................................................
........................................................................
Reading boot image 1401958 bytes.
Initializing firewall...
System is starting...
Resizing shared data partition...done
Formatting shared data partition ...  done!
```

2.3.2 Web-based Upgrade

Networking Requirements

The current system software version is outdated, so it needs to be upgraded via a Web interface.

Before the upgrade, be sure to back up the device configurations. For details, refer to the section “Firewall Maintenance” > “Configuration Backup and Recovery”.

Configuration Points

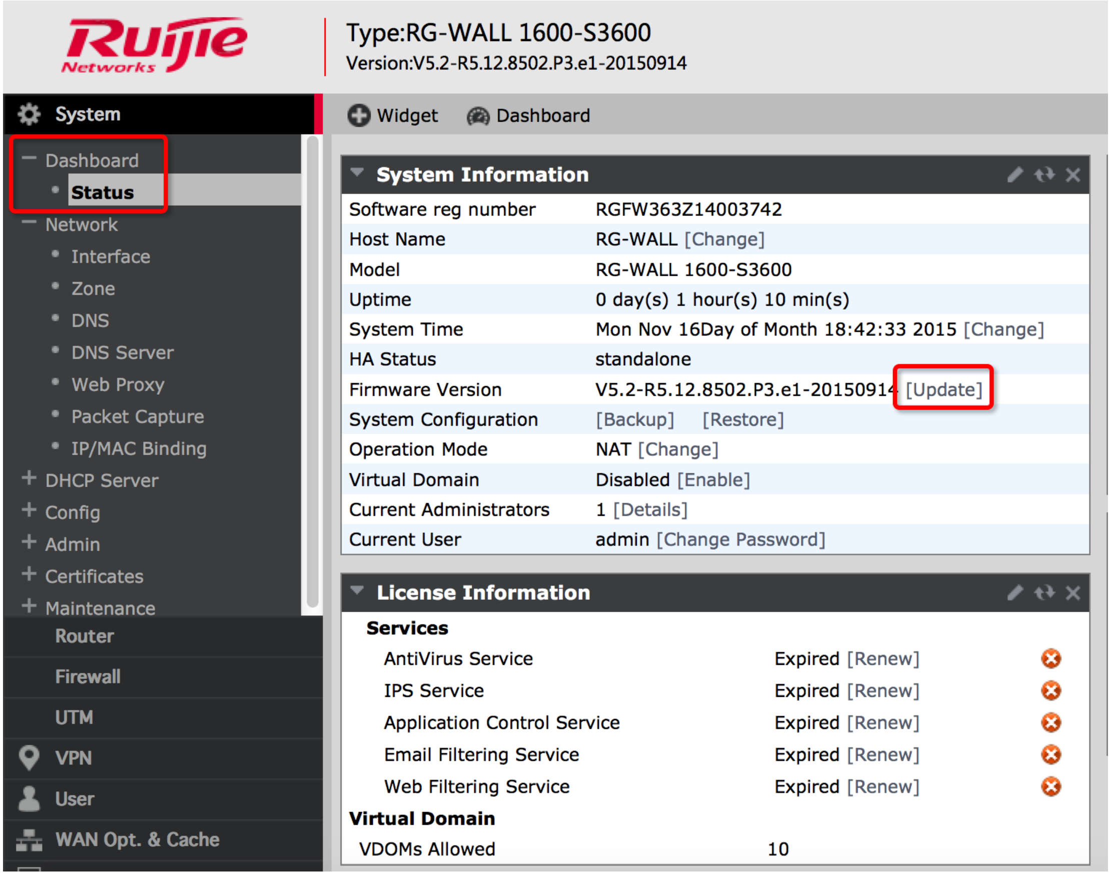
1. RG-WALL: It is a next-generation firewall. Each model of the device has a separate version file; before the upgrade, confirm the current device model.
2. The postfix of the upgrade package must be “.bin”, and its prefix is not restricted;
3. Before the upgrade, prepare a Console cable, so as to take measures in case of upgrade failure;
4. During the upgrade process, do not switch to other interfaces, nor power off or restart the device; the upgrade process usually takes less than five minutes;
5. After the new version is imported, the device is automatically restarted, and then the upgrade takes effect.

The upgrade will cause network interrupt. During the upgrade process, follow the upgrade procedure strictly; misoperations will cause system missing.

Upgrade Procedure

1. Log in to the Web interface of the NGFW

Choose the **System** > **Dashboard Status** > **Firmware Version** menu, and click the **Update** button;



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

System Information

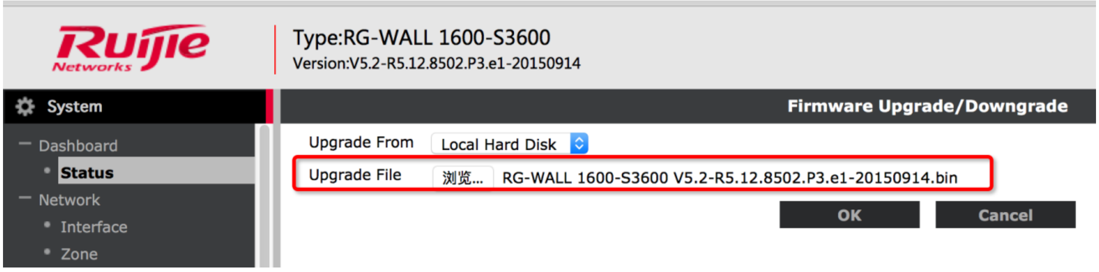
Software reg number	RGFW363Z14003742
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3600
Uptime	0 day(s) 1 hour(s) 10 min(s)
System Time	Mon Nov 16Day of Month 18:42:33 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.12.8502.P3.e1-20150914 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

License Information

Services	
AntiVirus Service	Expired [Renew]
IPS Service	Expired [Renew]
Application Control Service	Expired [Renew]
Email Filtering Service	Expired [Renew]
Web Filtering Service	Expired [Renew]
Virtual Domain	
VDOMs Allowed	10

2. Select the related OS files

Click **OK**, and then the system is automatically restarted.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Firmware Upgrade/Downgrade

Upgrade From: Local Hard Disk
Upgrade File: 浏览... RG-WALL 1600-S3600 V5.2-R5.12.8502.P3.e1-20150914.bin

Verification

The system will be restarted via the newly loaded OS.

Precautions

The P3 version makes many changes over the previous versions; you need to use the following upgrade mode:

1. Before the upgrade, be sure to disable the auto-ipsec management property of the wan1 and wan2 interfaces via a CLI (if the management property is not disabled, the system will reports errors on the switching of the transparent mode of the P3 version).

   1) View the management property of interfaces

```
RG-WALL # show system interface
config system interface
    edit "wan1"
        set vdom "root"
        set ip 192.168.57.74 255.255.255.0
set allowaccess ping https ssh telnet auto-ipsec
        set type physical
        set snmp-index 1
    next
    edit "wan2"
        set vdom "root"
        set ip 192.168.101.200 255.255.255.0
        set allowaccess ping auto-ipsec
        set type physical
        set snmp-index 2
```

   2) Disable the auto ipsec property of the wan1 and wan2 interfaces

```
RG-WALL # config system interface
RG-WALL (interface) # edit wan1
RG-WALL (wan1) # set allowaccess ping https ssh
RG-WALL (wan1) # next
RG-WALL (interface) # edit wan2
RG-WALL (wan2) # set allowaccess ping
RG-WALL (wan2) # end
```

2. Upgrade the P0, P1 or P2 version to the P3 version via a Web interface (the upgrade process takes about five minutes);

3. To attain complete upgrade, you need to upgrade the P3 version again on a Web interface;

   1) During the upgrade to the P3 version, a formatting action is added, so as to ensure complete upgrade;

   2) The formatting operation will not clear the original configurations;

   3) The subsequent versions are not affected by this; only the P3 version requires two upgrades;

   4) The upgrade process takes about 5 minutes.

4. Upgrade flowchart: p0, p1 or p2 to p3 to P3.

5. auto-ipsec is enabled or disabled, depending on specific model of the device:

    1) S3100: By default, auto-ipsec is enabled on wan1 and wan2;

    2) S3600: By default, auto-ipsec is enabled on wan1 and wan2;

    3) M5100: By default, auto-ipsec is enabled on wan1;

    4) M6600 and X9300: auto-ipsec is not enabled on the interfaces.

2.4 License Service Registration

I. Description

1. There is only one kind of license service, namely RG-WALL1600-XXXXX (model)-LIS-1Y, which is sent in an envelope with the term of 1 year. This is a compound license service, containing virus signature upgrade service, IPS signature upgrade service, URL signature upgrade service, application signature upgrade service, and spam signature upgrade service.

2. License service registration is online registration of a service license for UTM-related functions (such as anti-virus, IPS, application detection, email filtering, Web filtering, and data leakage prevention) purchased by customers, which enables customers to upgrade rules repository and use the online detection function during the license term. You cannot handle license service registration by yourselves. Instead, you need provide relevant information to our engineer for registration. Then ,when your devices are connected to the Internet, you can find that the license has been activated, and UTM functions can be used.

II. License Service Registration Process

Step 1: Send registration information.

When you purchase the service, you will receive an envelope enclosed with an authorization code. If you need registration, send the **software SN (16 digits), model, authentication code, project name, and customer name** of the device to be registered to **rgngfw3@ruijie.com.cn** according to instructions of the envelope.

1. Collect related information according to samples in the following table.

	Software SN (16 digits)	Model	Authorization Code (12 digits)	Project Name	Customer Name
Sample	DB99KKK124667235	Sample*	Sample*	Sample	Sample*

Explanation:

Software SN: It is a string of code with 16 digits starting with RGFW on the Web page.

Model: It can be obtained from the dashboard or Web page.

Please send the table information in Step 1 and your contact information to the technical support email address: rgngfw3@ruijie.com.cn titled "License Activation for WALL 1600 (model)".

We will finish license activation based on the table information provided by you within 1 working day. If your application is filed on weekends or holidays, we will finish license activation before 12:00 on the subsequent working day.

When you receive an email about successful activation, it indicates that your license has been activated and you can use the upgrade service.

Notes:

1. The authorization code is only applicable to a certain model in RG-WALL 1600 series.
2. Please do activate your license within 10 months after receipt of the license envelope. Otherwise, Ruijie Cloud Server will automatically activate it for you.
3. The authorization code can be activated only once. If you fail to activate it, please contact Ruijie engineers for license migration.

Step 2: Operate on the device.

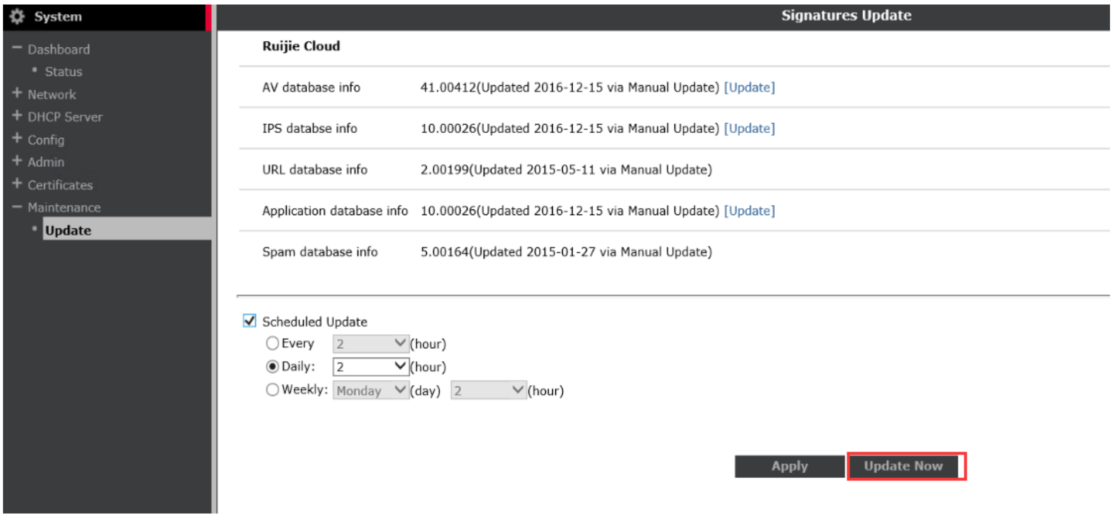
Ensure that the firewall is connected to the Internet and configured with the correct DNS address. The server domain name is automatically updated to fwupdate.ruijie.com.cn and port 8890 by default.

Run the following commands to change the default setting to automatically find the server (using servers distributed globally):

```
RG-WALL # show system central-management
config system central-management
    set Ruijiemanager-fds-override enable
    set fmg "fwupdate.ruijie.com.cn"
end

RG-WALL # config system central-management
RG-WALL (central-management) # unset fmg
RG-WALL (central-management) # set Ruijiemanager-fds-override disable
RG-WALL # show system  central-management  //Indicates that the default update address is disabled and it will automatically find the nearest server.
```

1. Perform initial manual update.

After receipt of the registration success email from Ruijie official reply, log in to the firewall to perform initial manual update.



Signatures Update

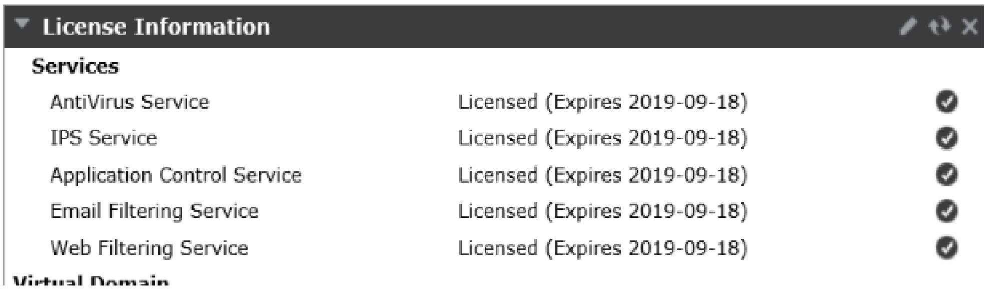
Ruijie Cloud

AV database info	41.00412(Updated 2016-12-15 via Manual Update) [Update]
IPS databse info	10.00026(Updated 2016-12-15 via Manual Update) [Update]
URL database info	2.00199(Updated 2015-05-11 via Manual Update)
Application database info	10.00026(Updated 2016-12-15 via Manual Update) [Update]
Spam database info	5.00164(Updated 2015-01-27 via Manual Update)

☑ Scheduled Update
○ Every 2 (hour)
● Daily: 2 (hour)
○ Weekly: Monday (day) 2 (hour)

Confirm license information.

Choose **System** > **Status** to view **License Information** which indicates **Licensed**. Confirm the expiry date of each service.



License Information

Services

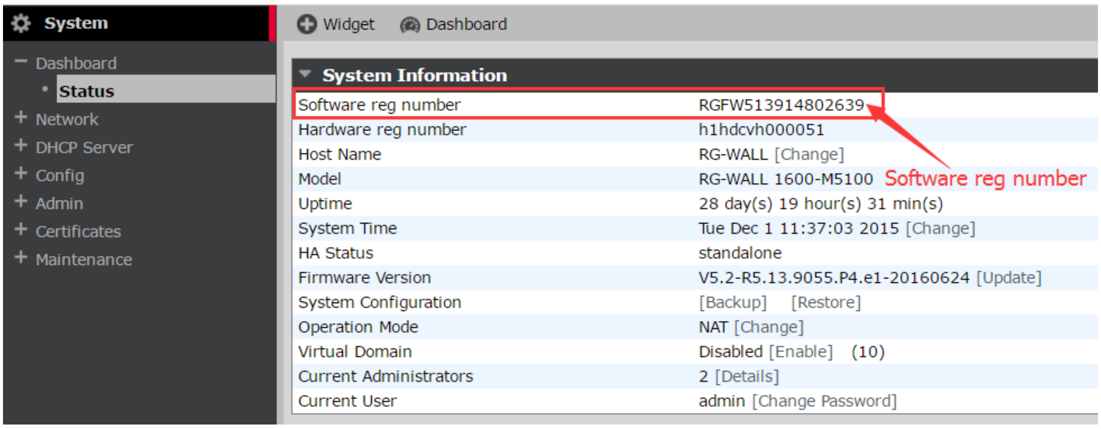
AntiVirus Service	Licensed (Expires 2019-09-18)	✓
IPS Service	Licensed (Expires 2019-09-18)	✓
Application Control Service	Licensed (Expires 2019-09-18)	✓
Email Filtering Service	Licensed (Expires 2019-09-18)	✓
Web Filtering Service	Licensed (Expires 2019-09-18)	✓

Virtual Domain

IV. Information Acquisition Method

1. Software SN

Log in to device. Choose **System** > **Dashboard** > **Status** > **System Information** to view the software SN (software reg number).

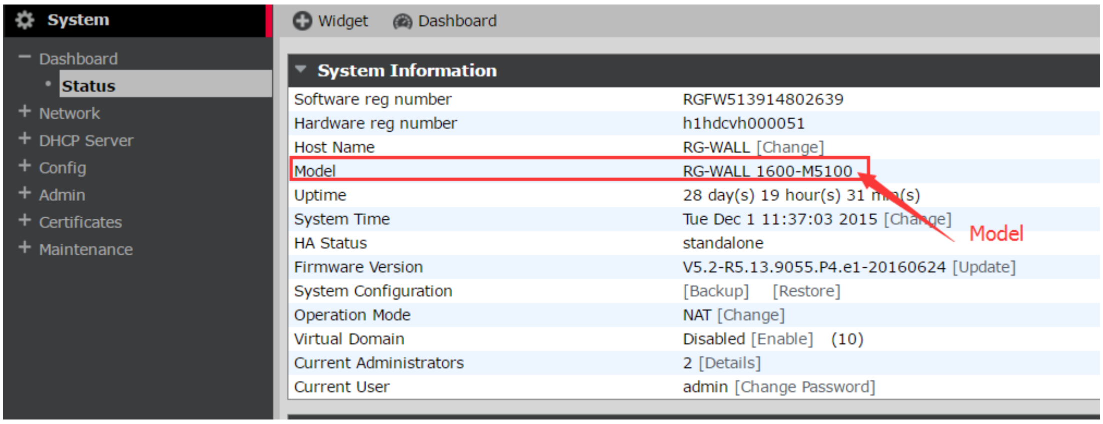


System Information

Software reg number	RGFW513914802639
Hardware reg number	h1hdcvh000051
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-M5100
Uptime	28 day(s) 19 hour(s) 31 min(s)
System Time	Tue Dec 1 11:37:03 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.13.9055.P4.e1-20160624 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable] (10)
Current Administrators	2 [Details]
Current User	admin [Change Password]

Model

View the model on the dashboard or Web page. On the Web page, choose **System** > **Dashboard** > **Status** > **System Information** to view the model.



System Information

Software reg number	RGFW513914802639
Hardware reg number	h1hdcvh000051
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-M5100
Uptime	28 day(s) 19 hour(s) 31 min(s)
System Time	Tue Dec 1 11:37:03 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.13.9055.P4.e1-20160624 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable] (10)
Current Administrators	2 [Details]
Current User	admin [Change Password]

Authorization Code

Obtain the authorization code from the envelope.

2.5 Configuration Backup and Recovery

Networking Requirements

Save the current configurations of the firewall, and export them for backup, so as to restore the configurations in case of need.

Configuration Tips

1. Save the configurations
2. Export the configurations
3. Restore the configurations

. The imported configuration files must be in conf format; otherwise, they cannot be identified.

2. After you import the configurations, you must restart the system so that the imported configurations take effect.

3. You must remember the password for the backup configurations; otherwise, they cannot be imported or restored. 1

Configuration Steps

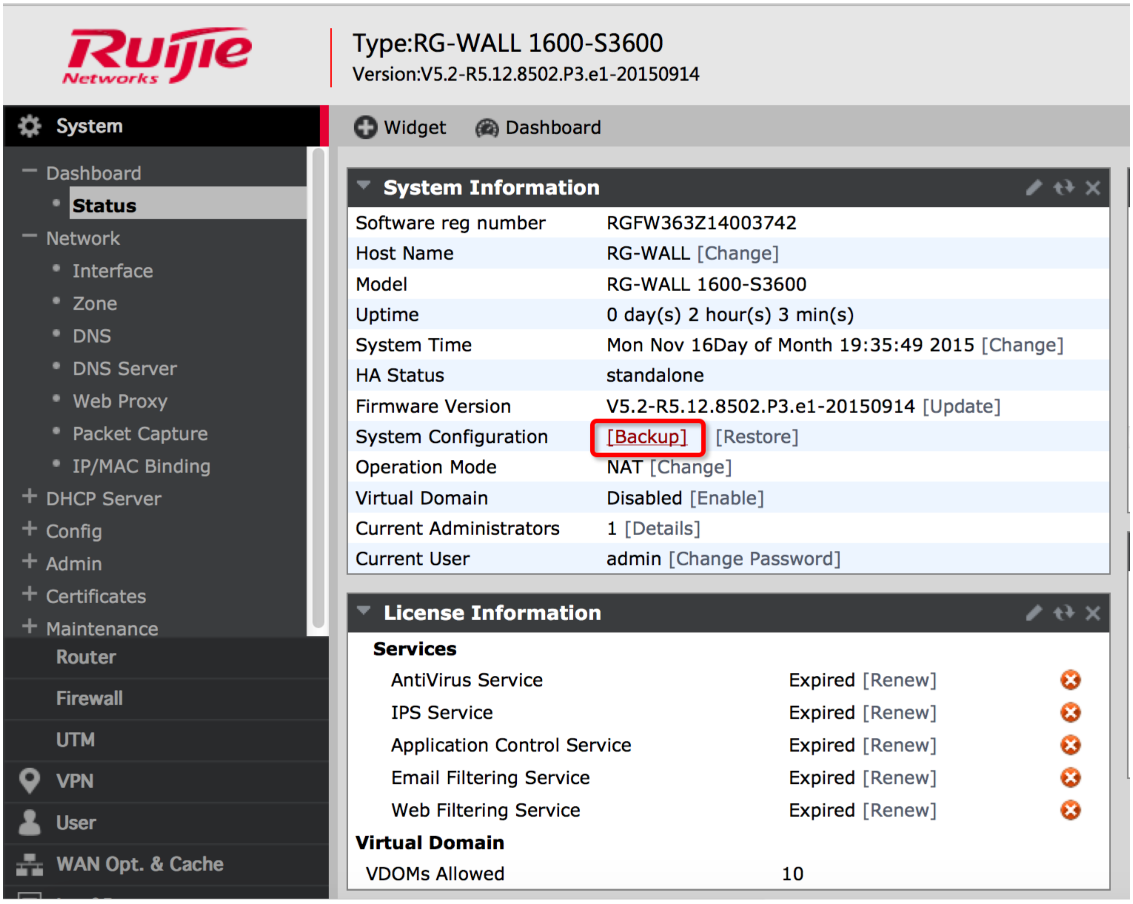
1. Save the configurations

Web: Via the Web interface, the configurations can take effect timely, and be saved automatically. Every time you modify configurations and click **OK**, the new configurations are automatically saved.

CLI: Enter **next** and **end** on the CLI, the new configurations take effect and are automatically saved.

2. Export the configurations

Choose the **System** > **Dashboard** > **Status** menu, and the **System Information** page pops up. Then, click **Backup** after **System Configuration**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

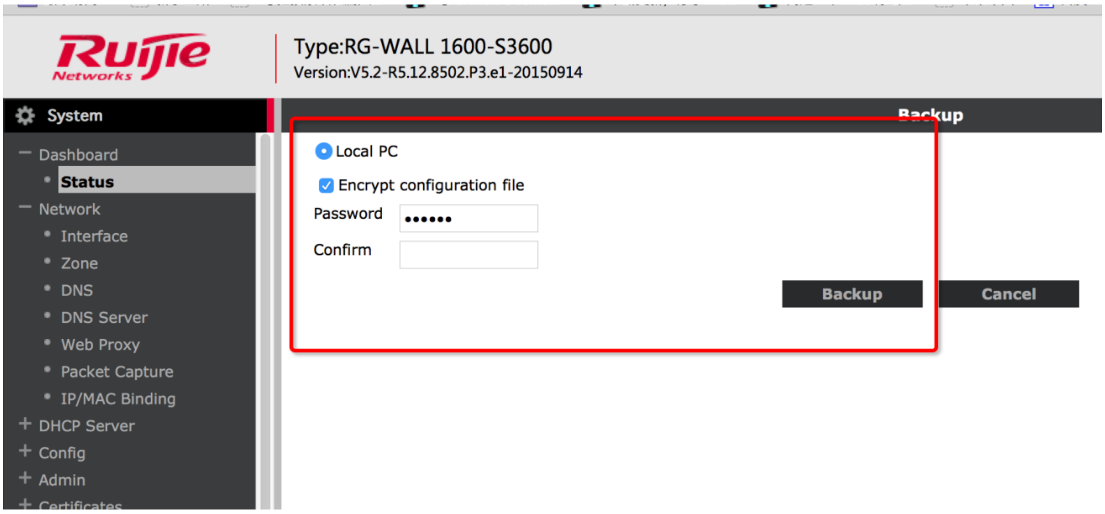
System Information

Software reg number	RGFW363Z14003742
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3600
Uptime	0 day(s) 2 hour(s) 3 min(s)
System Time	Mon Nov 16Day of Month 19:35:49 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.12.8502.P3.e1-20150914 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

License Information

Services		
AntiVirus Service	Expired [Renew]	✖
IPS Service	Expired [Renew]	✖
Application Control Service	Expired [Renew]	✖
Email Filtering Service	Expired [Renew]	✖
Web Filtering Service	Expired [Renew]	✖
Virtual Domain		
VDOMs Allowed	10	

The updated P2 version allows you to choose whether to encrypt configuration files (in the P1 version, configuration files must be encrypted by default). You can select or deselect **Encrypt configuration file** (if selected, you need to set a password) according to actual needs, and click **Backup**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

● Local PC

☑ Encrypt configuration file

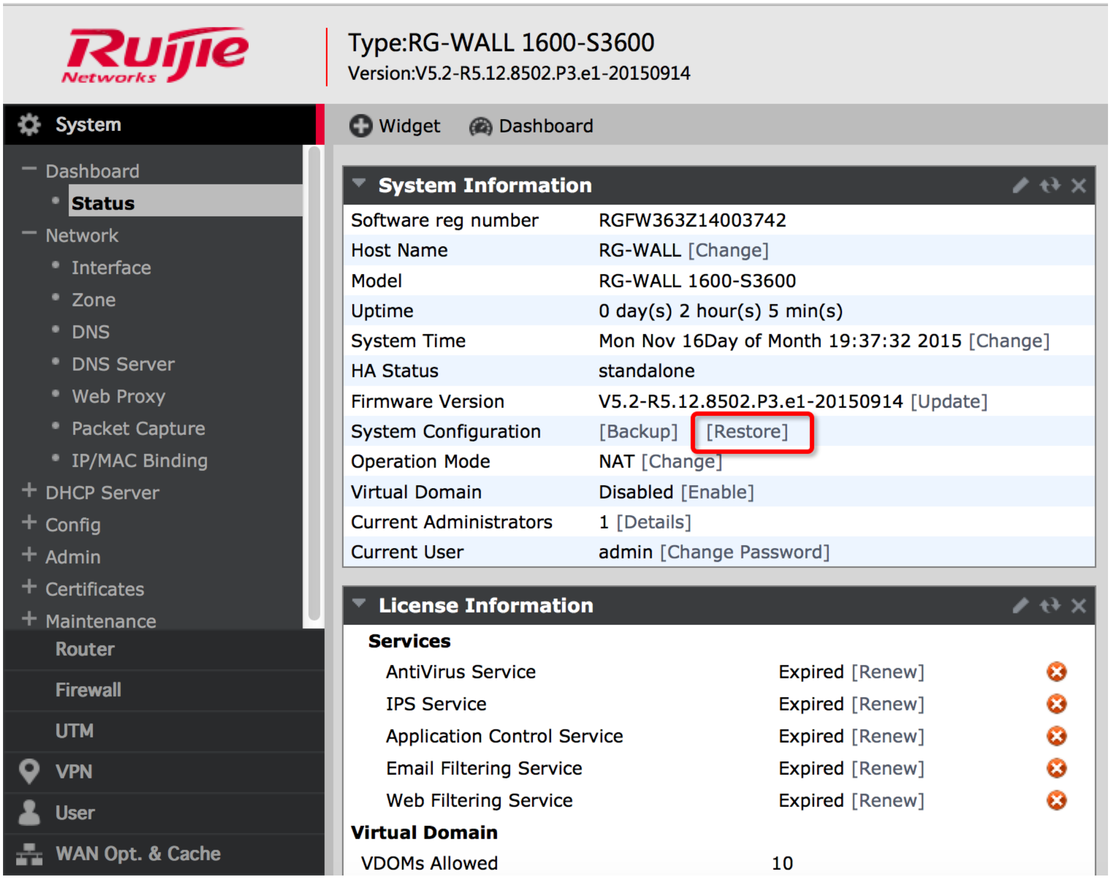
Password ••••••

Confirm

The configuration files will be backed up to the local disk.

3. Restore the configurations

Choose the **System** > **Dashboard** > **Status** menu, and the **System Information** page pops up. Then, click **Restore** after **System Configuration**, so as to use the locally stored configuration files to restore the firewall configurations.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

System Information

Software reg number	RGFW363Z14003742
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3600
Uptime	0 day(s) 2 hour(s) 5 min(s)
System Time	Mon Nov 16Day of Month 19:37:32 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.12.8502.P3.e1-20150914 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

License Information

Services		
AntiVirus Service	Expired [Renew]	✖
IPS Service	Expired [Renew]	✖
Application Control Service	Expired [Renew]	✖
Email Filtering Service	Expired [Renew]	✖
Web Filtering Service	Expired [Renew]	✖
Virtual Domain		
VDOMs Allowed	10	

After the import is successful, the system prompts that you need to restart the system.

Verification

After the system is restarted, the previous configurations are restored.

2.6 Configuring SNMP

Networking Requirements

If the intranet is equipped with a network management server that monitors and manages the network devices, you need to enable the SNMP function on the NGFW, so that the network management server can monitor the NGFW via the SNMP function.

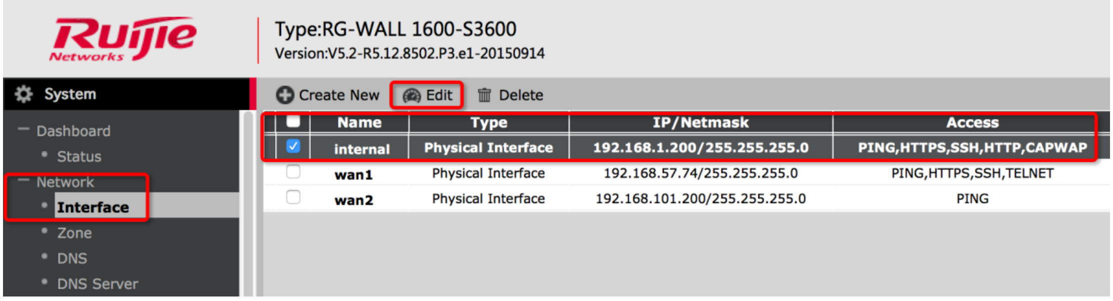
Configuration Tips

1. Enable the SNMP management function on the network interface;
2. Enable the SNMP local agent.
3. Configure the SNMP Community.

Configuration Steps

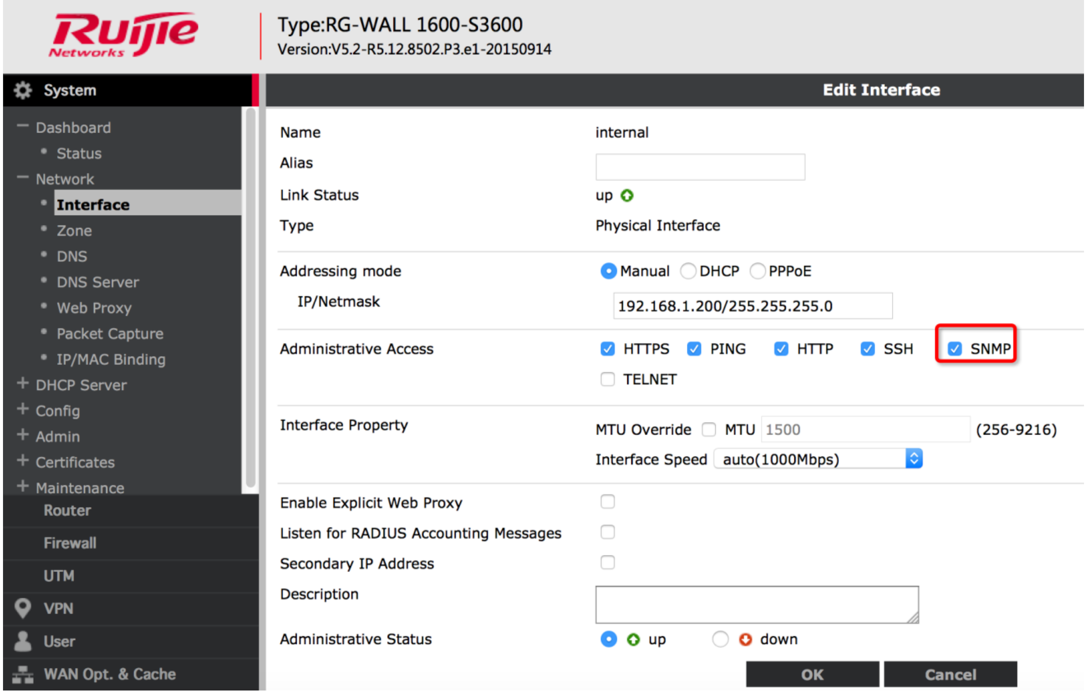
1. Enable the SNMP management function on the network interface

Choose the **System** > **Network** > **Interface** menu, edit the menu used for SNMP management; in the **Manage the Access** option, select **SNMP**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

	Name	Type	IP/Netmask	Access
☑	internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP,CAPWAP
□	wan1	Physical Interface	192.168.57.74/255.255.255.0	PING,HTTPS,SSH,TELNET
□	wan2	Physical Interface	192.168.101.200/255.255.255.0	PING



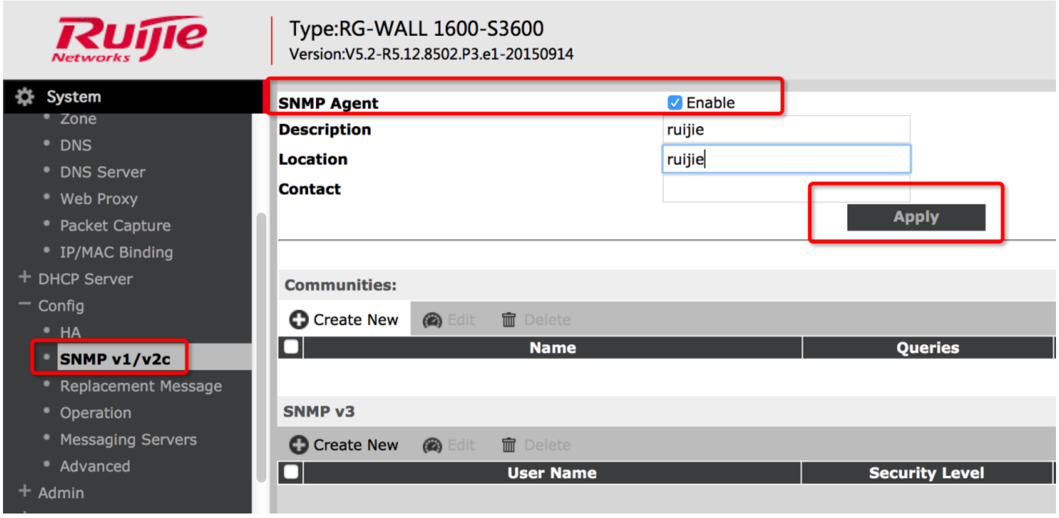
Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Interface

Name	internal
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.1.200/255.255.255.0
Administrative Access	☑ HTTPS ☑ PING ☑ HTTP ☑ SSH ☑ SNMP □ TELNET
Interface Property	MTU Override □ MTU 1500 (256-9216) Interface Speed auto(1000Mbps)
Enable Explicit Web Proxy	□
Listen for RADIUS Accounting Messages	□
Secondary IP Address	□
Description	
Administrative Status	● up ○ down

2. Enable the SNMP local agent

Choose the **System** > **Config** > **SNMPv1/v2** menu, select **SNMP Agent**, enter the related description information, and click **Apply**.

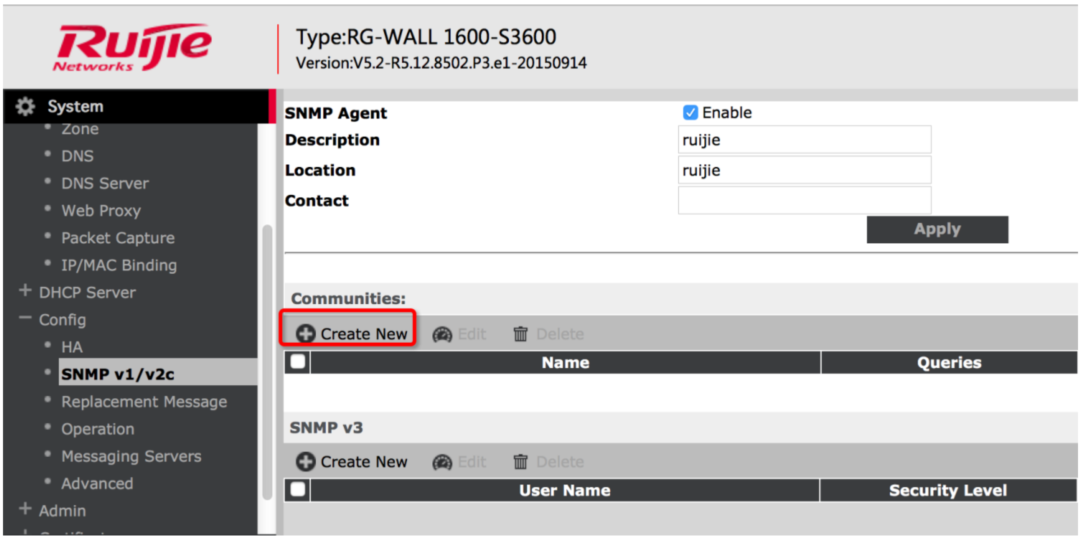


Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

SNMP Agent ☑ Enable
Description ruijie
Location ruijie
Contact

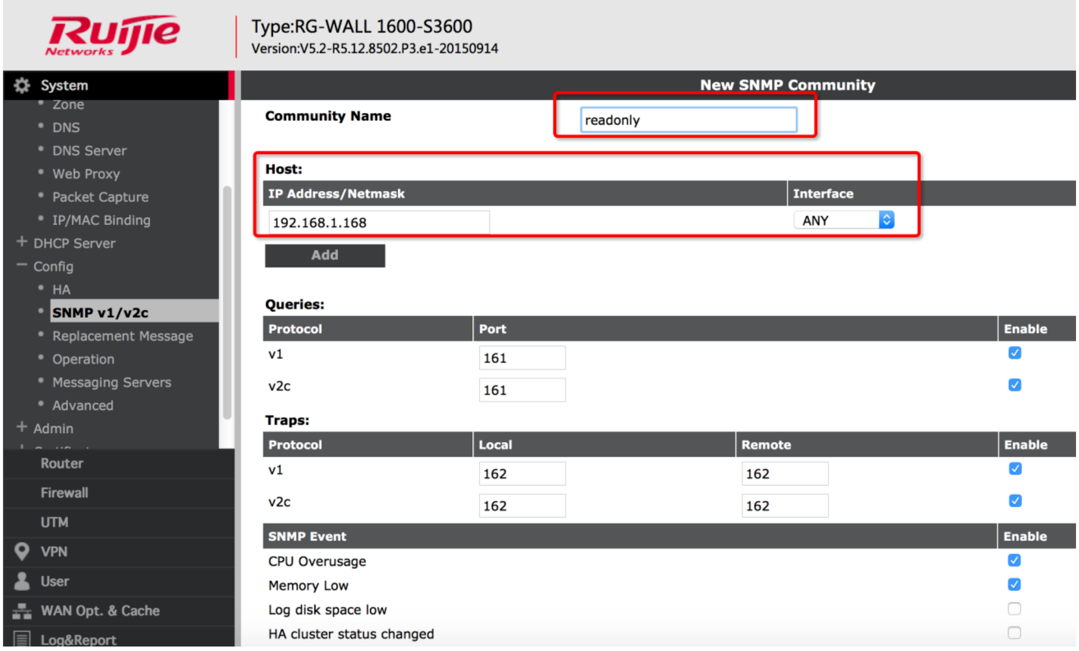
3. Configure the SNMP Community

On the interface of Step 2, click the **Create New** button below **SNMP Communities**. Then, the New SNMP Community configuration page pops up.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

SNMP Agent ☑ Enable
Description ruijie
Location ruijie
Contact



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New SNMP Community

Community Name: readonly

Host:

IP Address/Netmask	Interface
192.168.1.168	ANY

Add

Queries:

Protocol	Port	Enable
v1	161	☑
v2c	161	☑

Traps:

Protocol	Local	Remote	Enable
v1	162	162	☑
v2c	162	162	☑

SNMP Event	Enable
CPU Overusage	☑
Memory Low	☑
Log disk space low	☐
HA cluster status changed	☐

Community Name: It is set to **readonly** (read the character string).

Host management: Enter the address of the SNMP server (the address is mandatory, for example, **192.168.1.168**); then, the host is only allowed to perform SNMP management by using the character string, and the address is used as the address for receiving the Trap information.

Interface: If you select an interface, the system only allows SNMP management by using the character string via the selected interface. **any** refers to any interface.

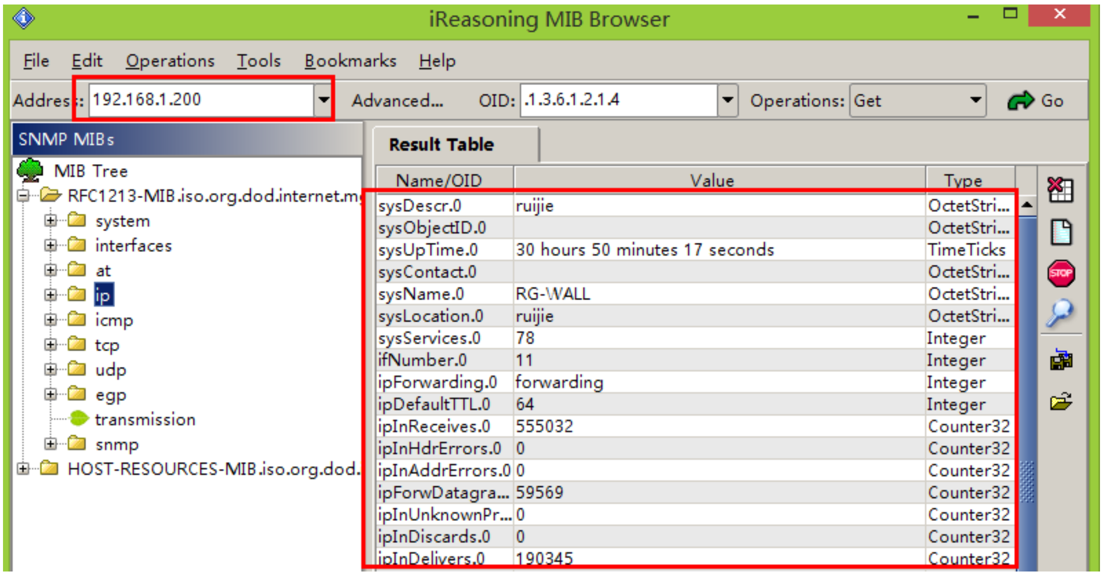
Queries: It refers to the interface used for SNMP queries.

Trap: It refers to the interface that the SNMP uses to send a Trap.

SNMP Event: It refers to an event of sending a SNMP Trap. By default, all events are selected. It is recommended that you should not modify the default setting.

Verification

As shown in the following figure, connect the **mibbrowser** to the firewall via SNMP, and view the related information of the device. You can view the device name and run time of the firewall:



Address: 192.168.1.200

OID: .1.3.6.1.2.1.4

Operations: Get

Name/OID	Value	Type
sysDescr.0	ruijie	OctetStri...
sysObjectID.0		OctetStri...
sysUpTime.0	30 hours 50 minutes 17 seconds	TimeTicks
sysContact.0		OctetStri...
sysName.0	RG-WALL	OctetStri...
sysLocation.0	ruijie	OctetStri...
sysServices.0	78	Integer
ifNumber.0	11	Integer
ipForwarding.0	forwarding	Integer
ipDefaultTTL.0	64	Integer
ipInReceives.0	555032	Counter32
ipInHdrErrors.0	0	Counter32
ipInAddrErrors.0	0	Counter32
ipForwDatagra...	59569	Counter32
ipInUnknownPr...	0	Counter32
ipInDiscards.0	0	Counter32
ipInDelivers.0	190345	Counter32

2.7 Password Recovery

Networking Requirements

1. If you forget the password of the device, you need to recover the password by using a Console cable.

2. After recovering the password, you need to restart the device on the bottom menu of the device. This will cause network interrupt. Therefore, perform the restart operation at a convenient time.

3. After you recover the password, the current configurations will not be changed.

Configuration Tips

1. Connect to the firewall serial port via the HyperTerminal or CRT;

2. Power off the device to restart it, and enter the built-in account **ruijie** to log in.

3. Set a new password for the administrator.

Configuration Steps

1. **Connect the Console cable, and set the HyperTerminal**

   a) Prepare a Console cable and a PC with a Com port;

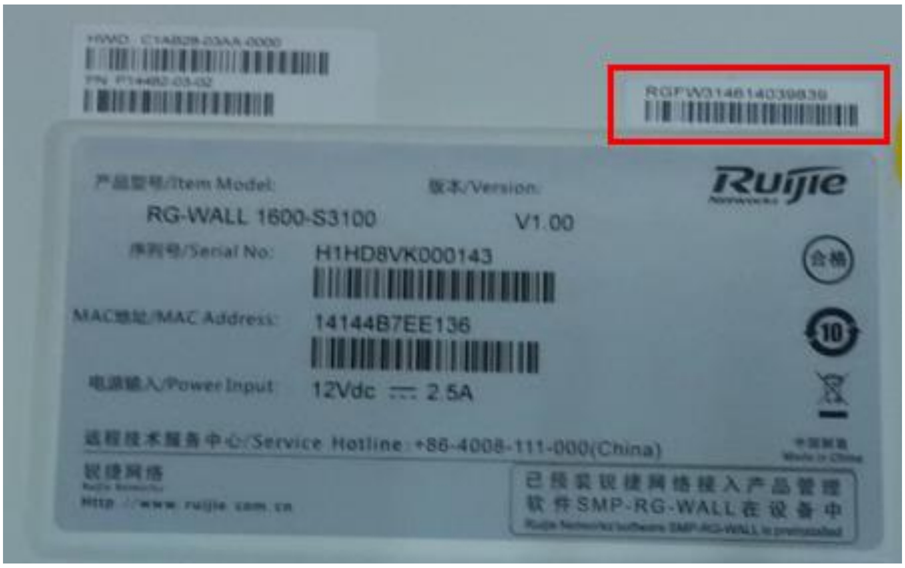
   b) Connect the Console cable;

   Insert the RJ45 connector end of the Console cable to the Console port of the network device (the Console port is usually beside the Ethernet port of the network device, and is marked with **Console**), and then insert the DB9 port of the Console cable to the Com port of the PC.

   c) Configure the HyperTerminal.

2. Power off to restart the device

Within 15 seconds after system restart, enter the user name **ruijie** and the password (the password is the software registration number, which is usually a string of 16 characters starting with **RJFW**). The serial No. of the product is available on the bottom or one side of the device, as shown below.



```
RG-WALL login: ruijie
Password: RGFW314614039839
RG-WALL #
```

The account is valid only within 15 seconds after system restart, and must be used via the Console interface.

3. Change the account and password for the administrator

```
RG-WALL # config system admin
RG-WALL (admin) # edit admin
RG-WALL (admin) # set pass 123455@!@#
RG-WALL (admin) # end
```

Verification

Use the new admin account and password to log in to the firewall via HTTPS or SSH.

2.8 Restoring Factory Settings

Networking Requirements

If you want to delete all current configurations of the device, you can restore the factory default. If you are that you want to restore the factory default, you are recommended to back up the current configurations. For details about the backup operation, refer to the section “Firewall Maintenance” > “Configuration Backup and Recovery”.

The license information of the device is saved on the cloud. After restoring the factory default, you can obtain the license information again if connecting the device to the Internet.

Configuration Tips

1. After you restore the factory default, all current configurations will be removed and the system will be automatically restarted.
2. After you restore the factory default, the IP address of the internal or MGMT interface is restored to 192.168.1.200.

Configuration Steps

Mode 1: CLI

Enter the CLI, run the **execute factoryreset** command, and press the **Enter** button. Then, the system prompts whether you want to continue. Enter **y** to continue the operation.

```
RG-WALL # execute  factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n) y
```

Mode 1: Press the **Reset** button on the device (this is only available on the S3100 and S3600, but not other models).

Within 30 seconds after the firewall system is normally started, press and hold the **Reset** button. The system will be automatically restarted, and you can restore the factory default.

Verification

After you restore the factory default, the IP address of the management interface is restored to 192.168.1.200. Via this address, you can log in to https://192.168.1.200. The user name and password are restored to the default **admin** and **firewall**.

Precautions

After you restore the factory default, the disk log is not be removed and only the current configurations are removed.

2.9 Common Commands

I. Command Structure

```
config      Configure object.  Configures policies and objects.
get         Get dynamic and system information.        Shows settings of specific objects.
show        Show configuration.          Shows the configuration file.
diagnose    Diagnose facility.  Indicates diagnosis commands.
execute     Execute static commands.Indicates common commands, such as ping.
exit        Exit the CLI.  Exits the CLI.
```

II. Common Commands

1. Configure an interface address.

```
RG-WALL # config system interface
RG-WALL (interface) # edit lan
RG-WALL (lan) # set ip 192.168.100.99/24
RG-WALL (lan) # end
```

2. Configure a static route.

```
RG-WALL (static) # edit 1
RG-WALL (1) # set device wan1
RG-WALL (1) # set dst 10.0.0.0 255.0.0.0
RG-WALL (1) # set gateway 192.168.57.1
RG-WALL (1) # end
```

3. Configure a default route.

```
RG-WALL (1) # set gateway 192.168.57.1
RG-WALL (1) # set device wan1
RG-WALL (1) # end
```

4. Configure a firewall address.

```
RG-WALL # config firewall address
RG-WALL (address) # edit clientnet
new entry ’clientnet’ added
RG-WALL (clientnet) # set subnet 192.168.1.0 255.255.255.0
RG-WALL (clientnet) # end
```

5. Configure an IP pool.

```
RG-WALL (ippool) # edit nat-pool
new entry ’nat-pool’ added
RG-WALL (nat-pool) # set startip 100.100.100.1
```

```
RG-WALL (nat-pool) # set endip 100.100.100.100
RG-WALL (nat-pool) # end
```

6. **Configure a virtual IP address.**

```
RG-WALL # config firewall vip
RG-WALL (vip) # edit webserver
new entry 'webserver' added
RG-WALL (webserver) # set extip 202.0.0.167
RG-WALL (webserver) # set extintf wan1
RG-WALL (webserver) # set mappedip 192.168.0.168
RG-WALL (webserver) # end
```

7. **Configure the Internet access policy.**

```
RG-WALL # config firewall policy
RG-WALL (policy) # edit 1
RG-WALL (1)#set srcintf internal //Indicates the source interface.
       RG-WALL (1)#set dstintf wan1    ///Indicates the destination interface.
       RG-WALL (1)#set srcaddr all        //Indicates the source address.
       RG-WALL (1)#set dstaddr all       //Indicates the destination address.
       RG-WALL (1)#set action accept      //Indicates the action.
       RG-WALL (1)#set schedule always    //Indicates the schedule.
       RG-WALL (1)#set service ALL          //Indicates the service.
       RG-WALL (1)#set logtraffic disable     //Enables or disables logs.
       RG-WALL (1)#set nat enable   //Enables NAT.
       end
```

8. **Configure the mapping policy.**

```
      RG-WALL # config firewall policy
      RG-WALL (policy) #edit 2
      RG-WALL (2)#set srcintf wan1  //Indicates the source interface.
      RG-WALL (2)#set dstintf internal //Indicates the destination interface.
      RG-WALL (2)#set srcaddr all          //Indicates the source address.
      RG-WALL (2)#set dstaddr ngfw1  //Indicates the destination address used for virtual
IP address mapping, which is added beforehand.
       RG-WALL (2)#set action accept      //Indicates the action.
       RG-WALL (2)#set schedule always    //Indicates the schedule.
       RG-WALL (2)#set service ALL          //Indicates the service.
       RG-WALL (2)#set logtraffic disable     //Enables or disables logs.
      end
```

9. Change the internal switching interface to the routing interface.

```
Ensure that routing, DHCP, and firewall policies of the internal interface are deleted.

RG-WALL # config system global

RG-WALL (global) # set internal-switch-mode interface

RG-WALL (global) #end

Restart

--------------------------------------
```

10. View the host name and management port.

```
     RG-WALL # show system global
```

11. View the system status and available resources.

```
       RG-WALL # get system performance status
```

12. View the application traffic statistics.

```
       RG-WALL # get system performance firewall statistics
```

13. View the ARP table.

```
RG-WALL # get system arp
```

14. View ARP details.

```
RG-WALL # diagnose ip arp list
```

15. Clear the ARP cache.

```
RG-WALL # execute clear system arp table
```

16. View the current session table.

```
RG-WALL # diagnose sys session stat or RG-WALL # diagnose sys session full-stat;
```

17. View the session list.

```
RG-WALL # diagnose sys session list
```

18. View the physical interface status.

```
       RG-WALL # get system interface physical
```

19. View settings of the default route.

```
        RG-WALL # show router static
```

20. View the static route in the routing table.

```
       RG-WALL # get router info routing-table static
```

21. View OSPF configuration.

```
       RG-WALL # show router ospf
```

22. View the global routing table.

```
        RG-WALL # get router info routing-table all

-----------------------------------------------
```

23. View HA status.

```
    RG-WALL # get system ha status
```

24. Check synchronization of active and standby routers.

```
    RG-WALL # diagnose sys ha showcsum
---------------------------------------------------
```

25. Diagnosis commands:

```
RG-WALL #diagnose debug enable //Enables debugging.
RG-WALL # diagnose debug application ike -1 //Debugs packets of Phase 1 of IPSec to check
whether an IPSec VPN is created.
RG-WALL #dia debug  reset  //Resets debugging.
   ---------------------------------------------------
Execute Commands:


RG-WALL #execute  ping  8.8.8.8   //Indicates the common ping command.


RG-WALL #execute  ping-options source  192.168.1.200    //Specifies 192.168.1.200 as the
source address of ping packets.
RG- WALL #execute  ping  8.8.8.8    //Enters the destination address of ping packets to
execute the ping command via the specified source address 192.168.1.200.


RG-WALL #execute  traceroute   8.8.8.8
RG-WALL #execute  telnet 2.2.2.2      //Gets access via Telnet.
RG-WALL #execute  ssh  2.2.2.2        //Gets access via SSH.
RG-WALL #execute  factoryreset        //Restores factory settings.
RG-WALL #execute  reboot  //Reboots the device.
RG-WALL #execute  shutdown//Shuts down the device.
```

3 Configuring Routing Mode

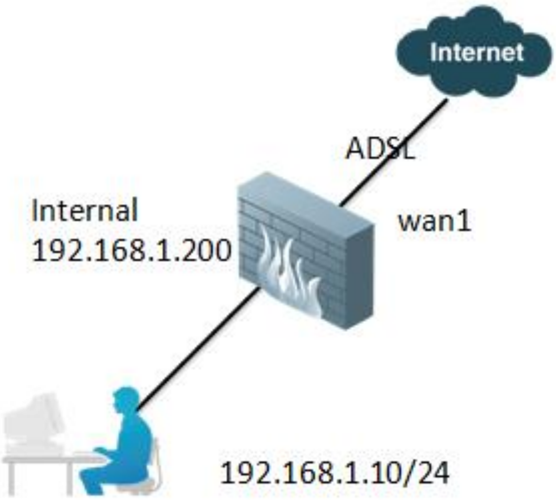
3.1 Internet Access via a Single Line

3.1.1 Configuring Internet Access via a Single ADSL Line

Networking Requirements

The extranet interface uses ADSL for dial-up and the intranet belongs to 192.168.1.0/24 segment. Intranet users can access the Internet.

Network Topology



Configuration Tips

1. Configure interfaces.

wan1 interface: It is used to access ADSL. The **Retrieve default gateway from server** option is mandatory. After ADSL dial-up succeeds, the device generates a default route without manual configuration.

Internal interface: Configure an IP address formatted as 192.168.1.200/24. If necessary, enable the management function on the interface.

2. Configure address object lan. with address 192.168.1.0/24.

3. Configure the policy for the data transmitted from the internal interface to wan1 interface and enable NAT.

Configuration Steps

1. Configure interface address.

Choose **System**>**Network**>**Interface**. Tick **wan1** and click **Edit** to display the **Edit Interface** page.

Addressing mode: Select PPPoE.

Username: Enter the user name.

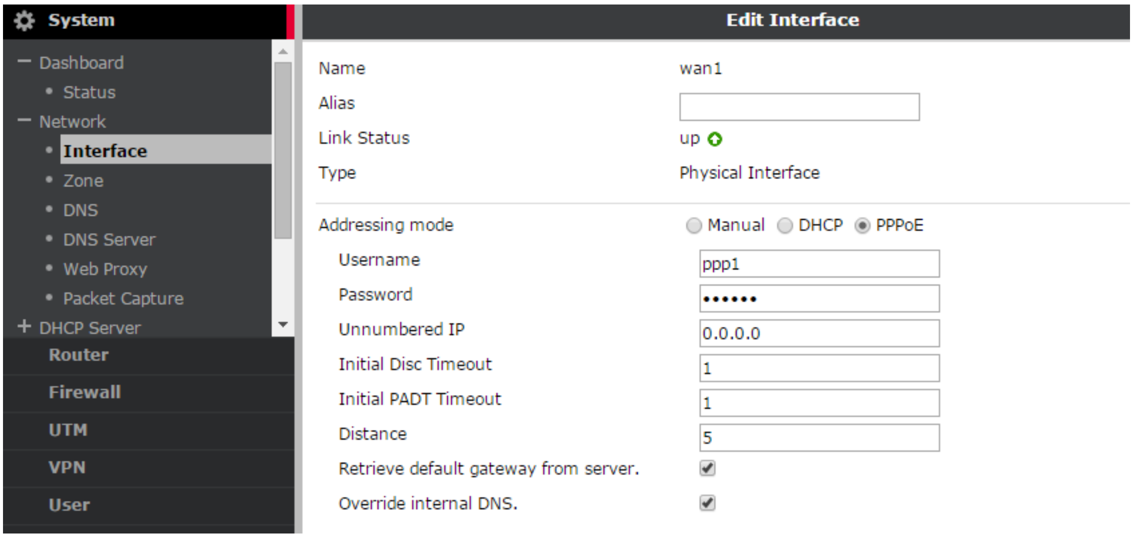
Password: Enter the password.

Initial Disc Timeout: The waiting time before beginning a new PPPoE discovery .

Initial PADT Timeout: If the idle time exceeds the defined time, PPPoE will be disabled. PADT function requires the support from the ISP.

Retrieve default gateway from server (mandatory): After dial-up succeeds, the firewall will obtain one default route.

Override internal DNS: If the company does not have its own DNS server, this option is mandatory.

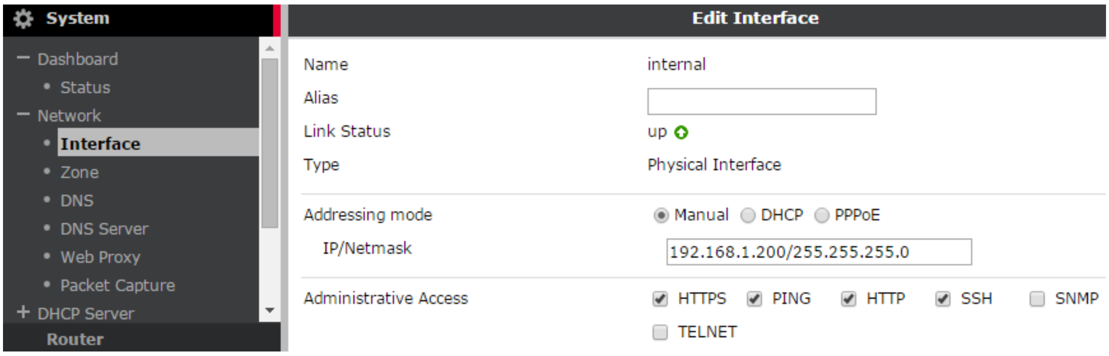


Edit Interface

Name	wan1
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	○ Manual ○ DHCP ● PPPoE
Username	ppp1
Password	••••••
Unnumbered IP	0.0.0.0
Initial Disc Timeout	1
Initial PADT Timeout	1
Distance	5
Retrieve default gateway from server.	☑
Override internal DNS.	☑

Edit the internal interface. The default IP address of the internal interface is 192.168.1.200/24, which shall be changed according to the actual situations.

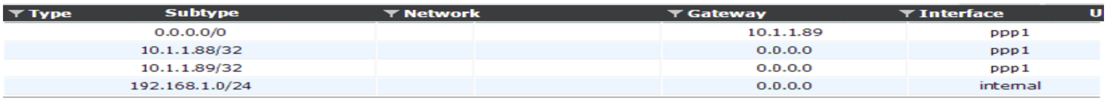
You can enable the management function on the interface if necessary. It recommended to enable HTTPS, SSH, and PING services.



Edit Interface

Name	internal
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.1.200/255.255.255.0
Administrative Access	☑ HTTPS ☑ PING ☑ HTTP ☑ SSH □ SNMP □ TELNET

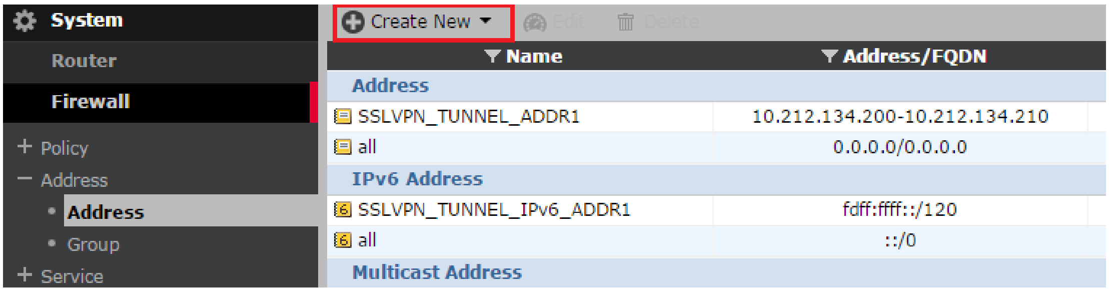
After dial-up succeeds, choose **Router**>**Monitor**>**Routing Monitor** to check the default route obtained by the PPPoE client.



Type	Subtype	Network	Gateway	Interface	U
	0.0.0.0/0		10.1.1.89	ppp1	
	10.1.1.88/32		0.0.0.0	ppp1	
	10.1.1.89/32		0.0.0.0	ppp1	
	192.168.1.0/24		0.0.0.0	intemal	

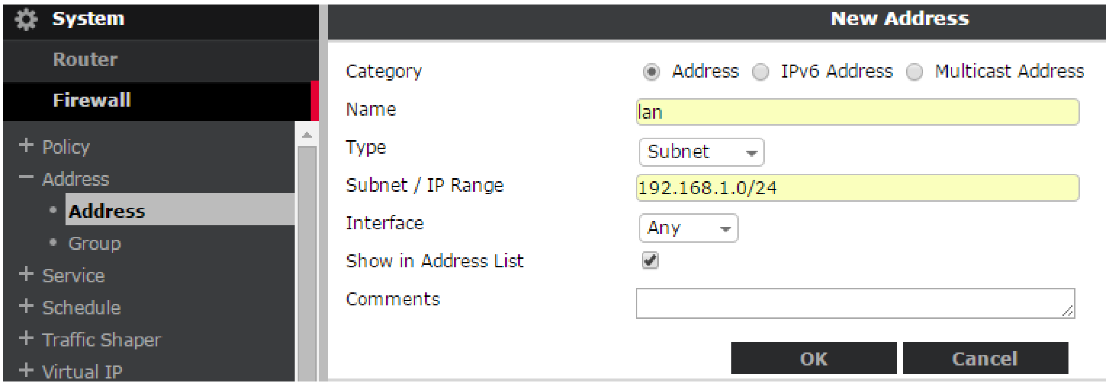
2. Configure address resources.

Choose **Firewall**>**Address**>**Address**, and then click **Create New**, as shown in the following figure:



Name	Address/FQDN
Address	
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210
all	0.0.0.0/0.0.0.0
IPv6 Address	
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120
all	::/0
Multicast Address	

Set **Name** to **lan**. Choose **Subnet** from **Type**. Set **Subnet/IP Range** to **192.168.1.0/24**. Click **OK**. See the following figure:

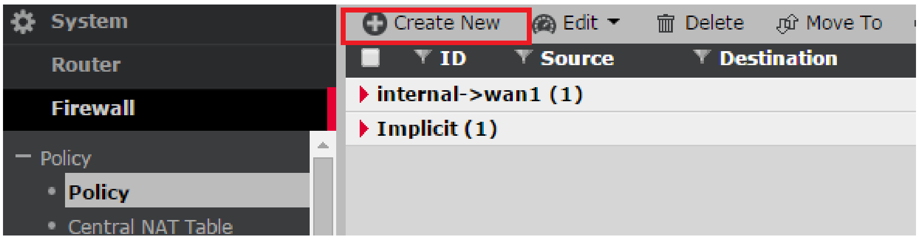


Category	● Address ○ IPv6 Address ○ Multicast Address
Name	lan
Type	Subnet
Subnet / IP Range	192.168.1.0/24
Interface	Any
Show in Address List	☑
Comments	

3. Configure the policy.

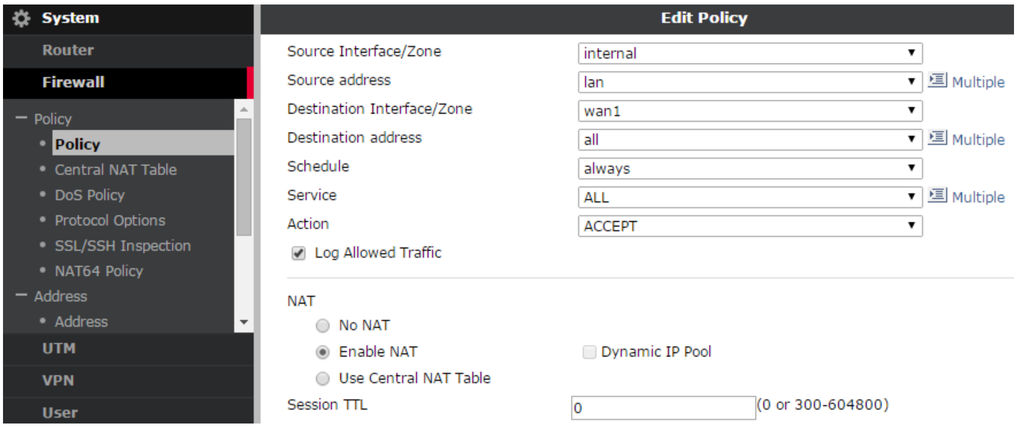
For some low-end models, the system provides an NAT policy from the internal interface to wan1 interface by default.

Choose **Firewall**>**Policy**>**Policy**, and then click **Create New**, as shown in the following figure:



□	ID	Source	Destination
internal->wan1 (1)			
Implicit (1)			

On the **Edit Policy** page, add one policy as shown in the following figure:



Source Interface/Zone	internal
Source address	lan
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT

☑ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Session TTL 0 (0 or 300-604800)

Source Interface/Zone: Choose **internal.**

Source address: Choose **lan.**

Destination Interface/Zone: Choose **wan1.**

Source address: Choose **lan.**

Destination address: Choose **all**, which indicates all the addresses.

Service: Choose **ALL**.

NAT: Tick Enable **ANT**. The system automatically converts the IP address of the intranet lan to the IP address of wan1 interface for Internet access.

Click **OK**. The system automatically saves configuration and the policy takes effect.

Log Allowed Traffic once enabled consumes extra system resources. Therefore, tick this item only when necessary.

Verification

Set the IP address of the PC to 192.168.1.1/24, the gateway address to 192.168.1.200, and the DNS address to 202.106.196.115, 8.8.8.8. (In general, you can set the DNS to the local DNS.)

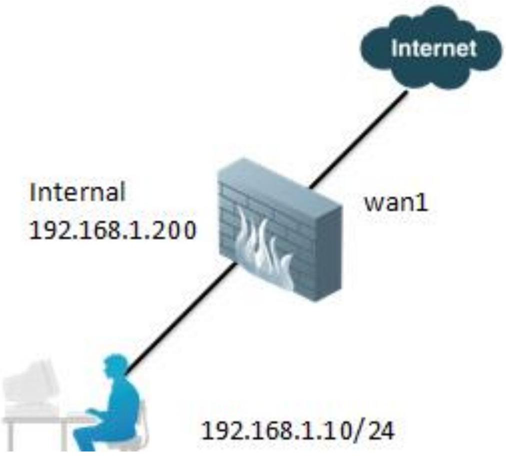
Then the PC can access the Internet.

3.1.2 Configuring Internet Access via a Static Link

Networking Requirements

The extranet interface is connected to a private line and configured with a static address assigned by the carrier. The intranet belongs to 192.168.1.0/24 segment. Intranet users can access the Internet.

Network Topology



Assume that the IP addresses assigned by the carrier are as follows:

Network segment: 202.1.1.8/29 Assigned IP address: 202.1.1.10 Gateway address: 202.1.1.9 DNS address: 202.106.196.115

Configuration Tips

1. Configure interfaces.

wan1 interface: Configure the IP address assigned by the carrier.

Internal interface: Configure an IP address formatted as 192.168.1.200/24. If necessary, enable the management function on the interface.

2. Configure a static routing table.

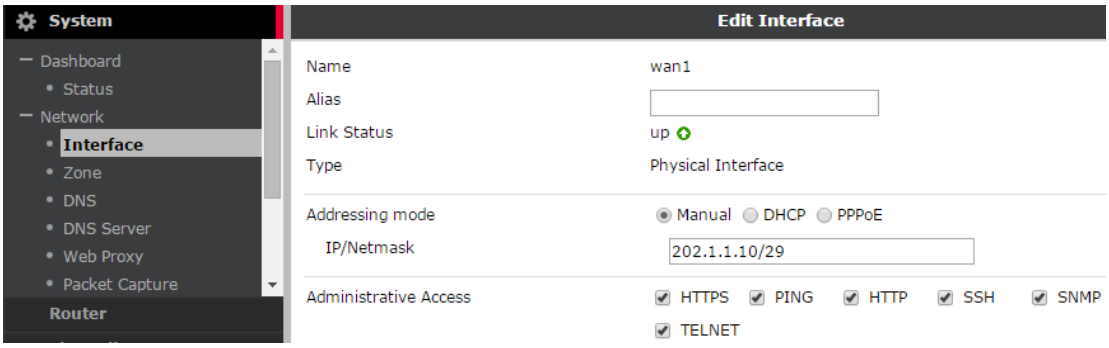
3. Configure address object lan with address 192.168.1.0/24.

4. Configure the policy for the data transmitted from the internal interface to wan1 interface and enable NAT.

Configuration Steps

1. Configure interface address.

Choose **System**>**Network**>**Interface**. Tick **wan1** and click **Edit** to display the **Edit Interface** page, as shown in the following figure:



Edit Interface

Name wan1

Alias

Link Status up

Type Physical Interface

Addressing mode ● Manual ○ DHCP ○ PPPoE

IP/Netmask 202.1.1.10/29

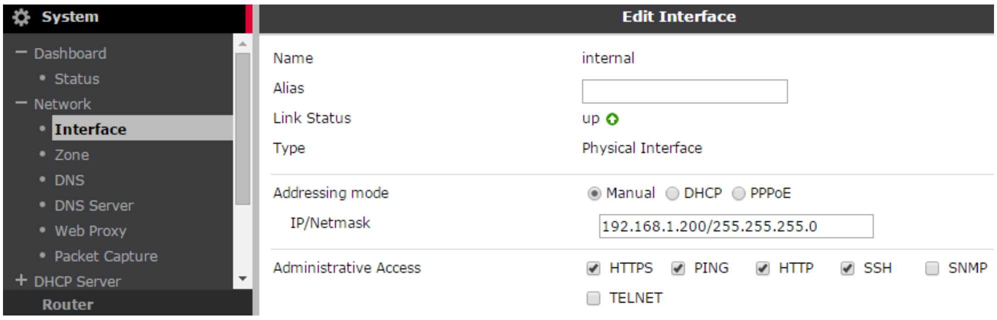
Administrative Access ☑ HTTPS ☑ PING ☑ HTTP ☑ SSH ☑ SNMP ☑ TELNET

In the 202.1.1.8/29 network segment, 2202.1.1.8 is the network address and 202.1.1.15 is the broadcast address, which cannot be used. 202.1.1.9 is the carrier's gateway address. The available IP address range is from 202.1.1.9 to 202.1.1.14.

Set the IP address of wan1 interface to 202.1.1.10.

Edit internal interface. The default IP address of internal interface is 192.168.1.200/24, which shall be changed according to the actual situations.

You can enable the management function on the interface if necessary. It is recommended to enable HTTPS, SSH, and PING services.



Edit Interface

Name: internal

Alias:

Link Status: up

Type: Physical Interface

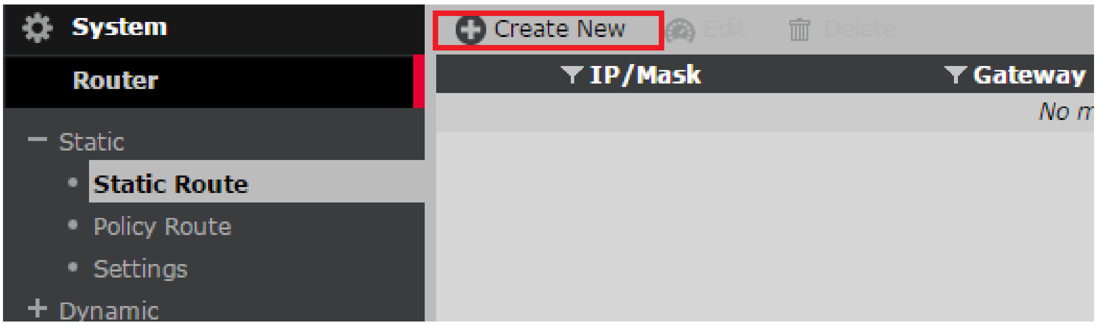
Addressing mode: ● Manual ○ DHCP ○ PPPoE

IP/Netmask: 192.168.1.200/255.255.255.0

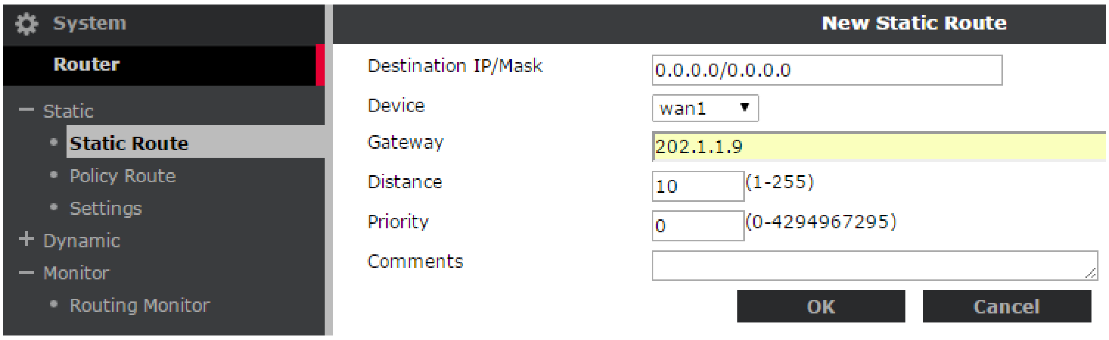
Administrative Access: ☑ HTTPS ☑ PING ☑ HTTP ☑ SSH □ SNMP □ TELNET

2. Configure a static routing table.

Choose **Router**>**Static**>**Static Route**, and then click **Create New**, as shown in the following figure:



Create a routing table, as shown in the following figure:



New Static Route

Destination IP/Mask: 0.0.0.0/0.0.0.0

Device: wan1

Gateway: 202.1.1.9

Distance: 10 (1-255)

Priority: 0 (0-4294967295)

Comments:

Destination IP/Mask: Keep the default value **0.0.0.0/0.0.0.0**.

Device: Choose **wan1**, which is related to this route. It must be set correctly. Otherwise, the route cannot work.

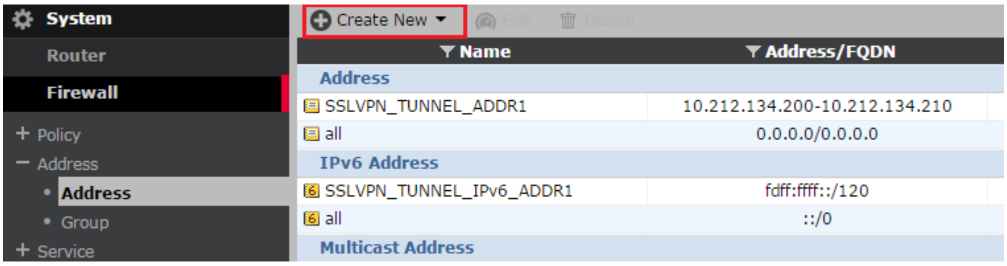
Gateway: The IP address of the next hop, that is, the IP address of the peer device corresponding to wan1 interface.

Distance: The default value is **10**.

Priority: The default value is **0**.

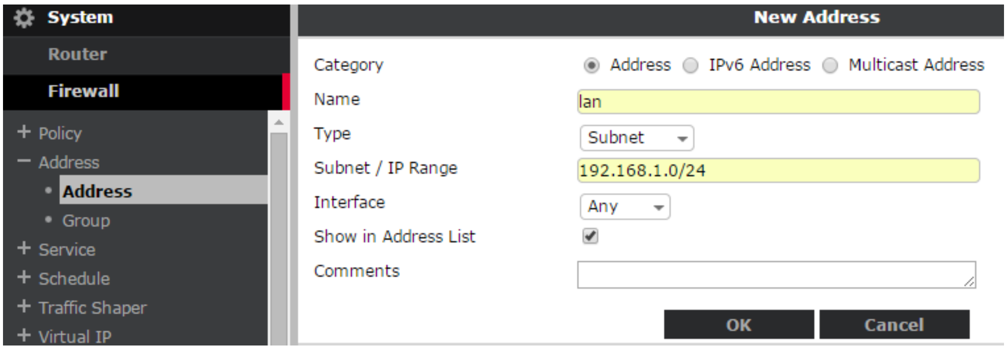
3. Configure address resources.

Choose **Firewall**>**Address**>**Address**, and then click **Create New**, as shown in the following figure:



Name	Address/FQDN
Address	
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210
all	0.0.0.0/0.0.0.0
IPv6 Address	
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120
all	::/0
Multicast Address	

Set **Name** to **lan**. Choose **Subnet** from **Type**. Set **Subnet/IP Range** to **192.168.1.0/24**. Click **OK**. See the following figure:



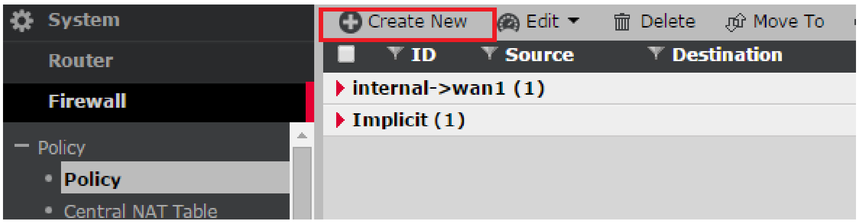
New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	lan
Type	Subnet
Subnet / IP Range	192.168.1.0/24
Interface	Any
Show in Address List	☑
Comments	

4. Configure the policy.

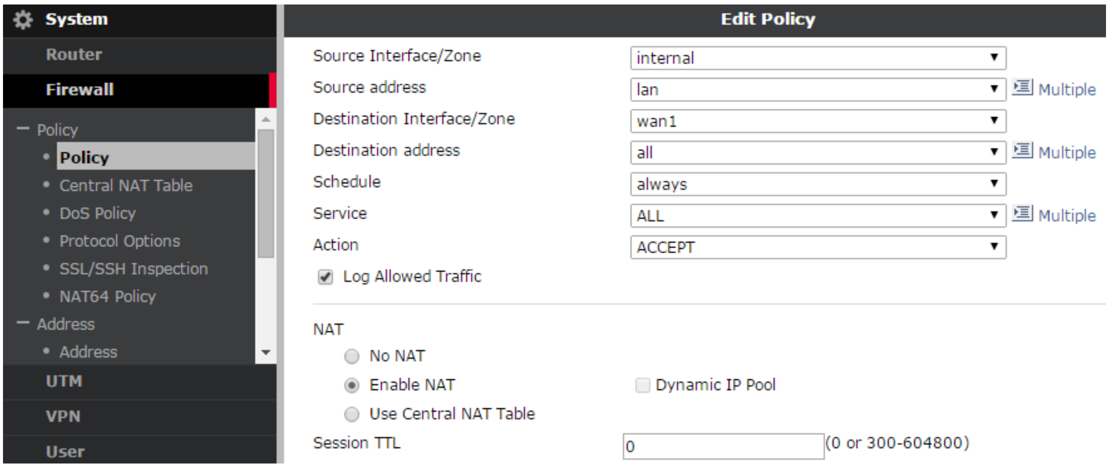
For some low-end models, the system provides an NAT policy from internal interface to wan1 interface by default.

Choose **Firewall**>**Policy**>**Policy**, and then click **Create New**, as shown in the following figure:



ID	Source	Destination
internal->wan1 (1)		
Implicit (1)		

On the **Edit Policy** page, add one policy as shown in the following figure:



Edit Policy

Source Interface/Zone: internal

Source address: lan (Multiple)

Destination Interface/Zone: wan1

Destination address: all (Multiple)

Schedule: always

Service: ALL (Multiple)

Action: ACCEPT

☑ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Session TTL: 0 (0 or 300-604800)

Source Interface/Zone: Choose **internal**.

Source address: Choose **lan**.

Destination Interface/Zone: Choose **wan1**.

Destination address: Choose **all**, which indicates all the addresses.

Service: Choose **ALL**.

NAT: Tick **Enable ANT**. The system automatically converts the IP address of the intranet lan to 202.1.1.10, the IP address of wan1 interface for Internet access.

Click **OK**. The system automatically saves configuration and the policy takes effect.

Log Allowed Traffic once enabled consumes extra system resources. Therefore, tick this item only when necessary.

Verification

Set the IP address of the PC to 192.168.1.1/24, the gateway address to 192.168.1.200, and the DNS address to 8.8.8.8. (In general, you can set the DNS to the local DNS.)

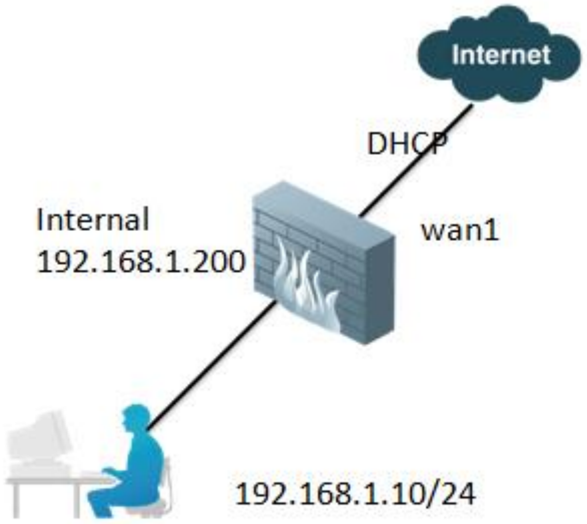
Then the PC can access the Internet.

3.1.3 Configuring Internet Access via a DHCP Line

Networking Requirements

The extranet interface uses DHCP and the intranet belongs to 192.168.1.0/24 segment. Intranet users can access the Internet.

Network Topology



Configuration Tips

1. Configure interfaces.

Wan1 interface: The **Retrieve default gateway from server** option is mandatory. After obtaining a DHCP address, the device generates a default route without manual configuration.

Internal interface: Configure an IP address formatted as 192.168.1.200/24. If necessary, enable the management function on the interface.

2. Configure address object lan with address 192.168.1.0/24.
3. Configure the policy for the data transmitted from the internal interface to wan1 interface and enable NAT.

Configuration Steps

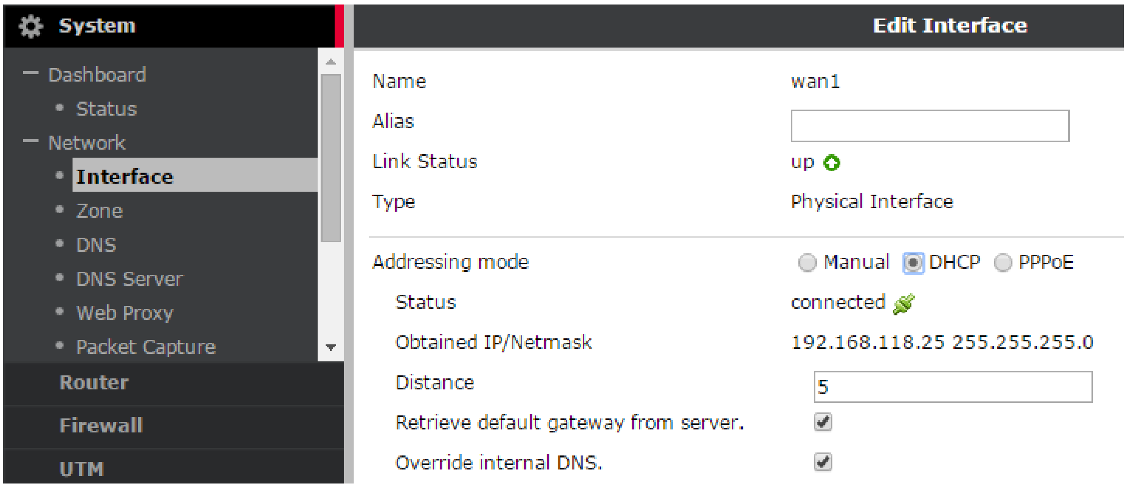
1) Configure interfaces.

Choose **System**>**Network**>**Interface**. Tick **wan1** and click **Edit** to display the **Edit Interface** page.

Addressing mode: Choose **DHCP**.

Retrieve default gateway from server (mandatory): After dial-up succeeds, the firewall will obtain one default route.

Override internal DNS: If the company does not have its own DNS server, this option is mandatory. The DHCP successfully obtains an IP address, as shown in the following figure:

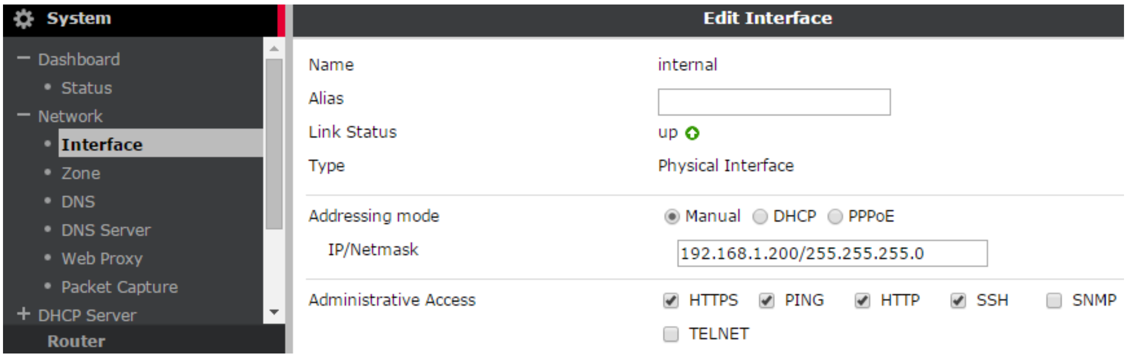


Edit Interface

Name	wan1
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	○ Manual ● DHCP ○ PPPoE
Status	connected
Obtained IP/Netmask	192.168.118.25 255.255.255.0
Distance	5
Retrieve default gateway from server.	☑
Override internal DNS.	☑

Edit the internal interface. The default IP address of the internal interface is 192.168.1.200/24, which shall be changed according to the actual situations.

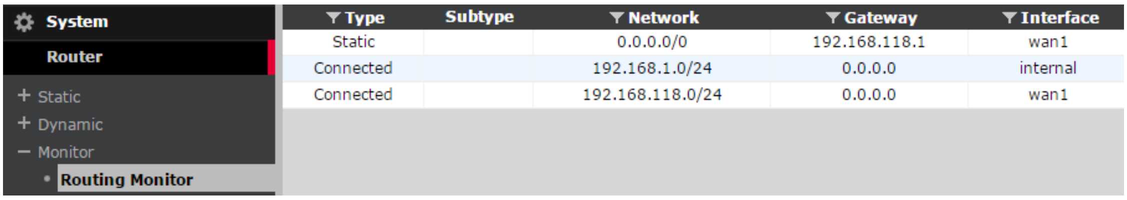
You can enable the management function on the interface if necessary. It is recommended to enable HTTPS, SSH, and PING services.



Edit Interface

Name	internal
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.1.200/255.255.255.0
Administrative Access	☑ HTTPS ☑ PING ☑ HTTP ☑ SSH □ SNMP □ TELNET

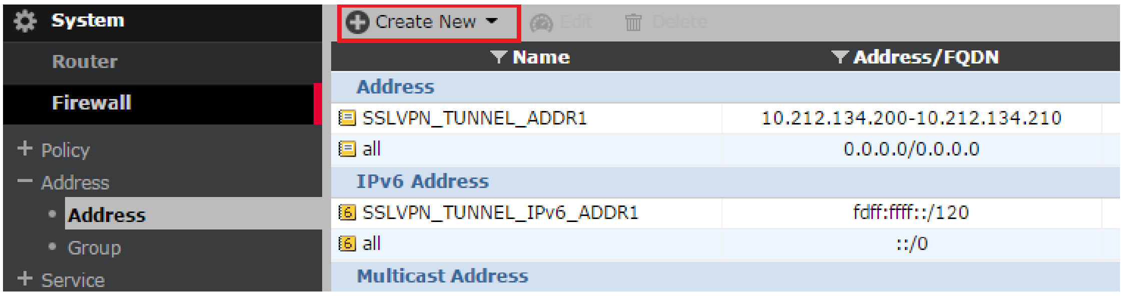
After the IP address is obtained, choose **Router**>**Monitor**>**Routing Monitor** to check the default route, as shown in the following figure:



Type	Subtype	Network	Gateway	Interface
Static		0.0.0.0/0	192.168.118.1	wan1
Connected		192.168.1.0/24	0.0.0.0	internal
Connected		192.168.118.0/24	0.0.0.0	wan1

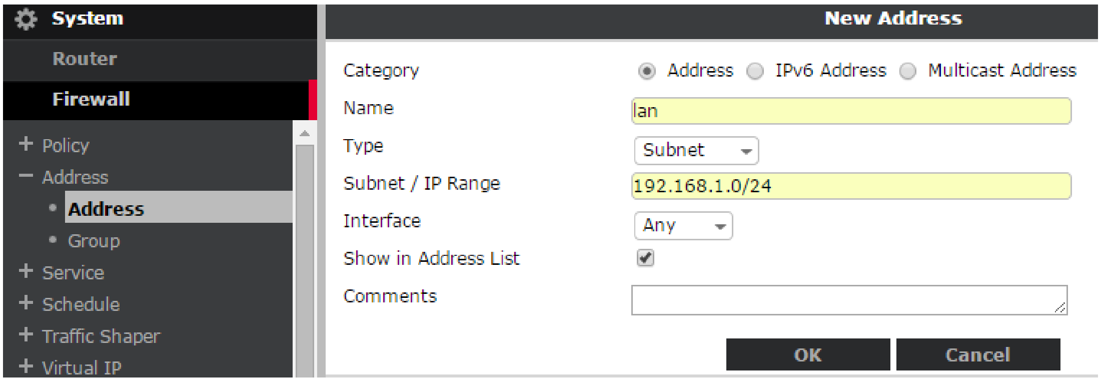
2) Configure address resources.

Choose **Firewall**>**Address**>**Address**, and then click **Create New**, as shown in the following figure:



Name	Address/FQDN
Address	
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210
all	0.0.0.0/0.0.0.0
IPv6 Address	
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120
all	::/0
Multicast Address	

Set **Name** to **lan**. Choose **Subnet** from **Type**. Set **Subnet/IP Range** to **192.168.1.0/24**. Click **OK**. See the following figure:



New Address

Category: ● Address ○ IPv6 Address ○ Multicast Address

Name: lan

Type: Subnet

Subnet / IP Range: 192.168.1.0/24

Interface: Any

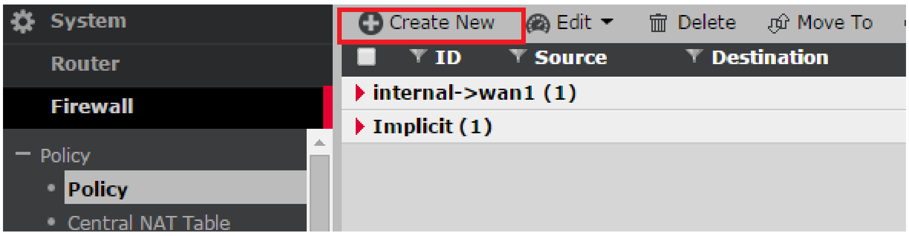
Show in Address List: ☑

Comments:

3) Configure the policy.

For some low-end models, the system provides an NAT policy from the internal interface to wan1 interface by default.

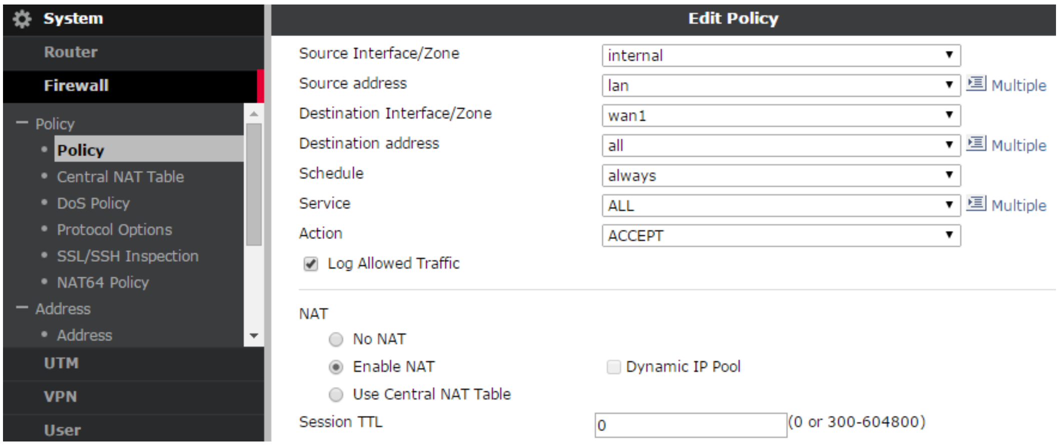
Choose **Firewall**>**Policy**>**Policy**, and then click **Create New**, as shown in the following figure:



internal->wan1 (1)

Implicit (1)

On the **Edit Policy** page, add one policy as shown in the following figure:



Edit Policy

Source Interface/Zone: internal

Source address: lan

Destination Interface/Zone: wan1

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

☑ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Session TTL: 0 (0 or 300-604800)

Source Interface/Zone: Choose **internal**.

Source address: Choose **lan**.

Destination Interface/Zone: Choose **wan1**.

Source address: Choose **lan**.

Destination address: Choose **all**, which indicates all the addresses.

Service: Choose **ALL**.

NAT: Tick **Enable ANT**. The system automatically converts the IP address of intranet lan to the IP address of wan1 interface for Internet access.

Click **OK**. The system automatically saves configuration and the policy takes effect.

If you select **Log Allowed Traffic**, extra resource consumption of the system is caused. Therefore, tick this item only when necessary.

Verification

Set the IP address of the PC to 192.168.1.1/24, the gateway address to 192.168.1.200, and the DNS address to 202.106.196.115, 8.8.8.8. (In general, you can set the DNS to the local DNS.)

Then the PC can access the Internet.

3.2 Internet Access via Multiple Links

3.2.1 Configuring Internet Access via Dual Lines of the Same Carrier

Networking Requirements

Two lines provided by China Telecom are used on the current device with the same bandwidth. They back up each other, and work in load-balancing mode.

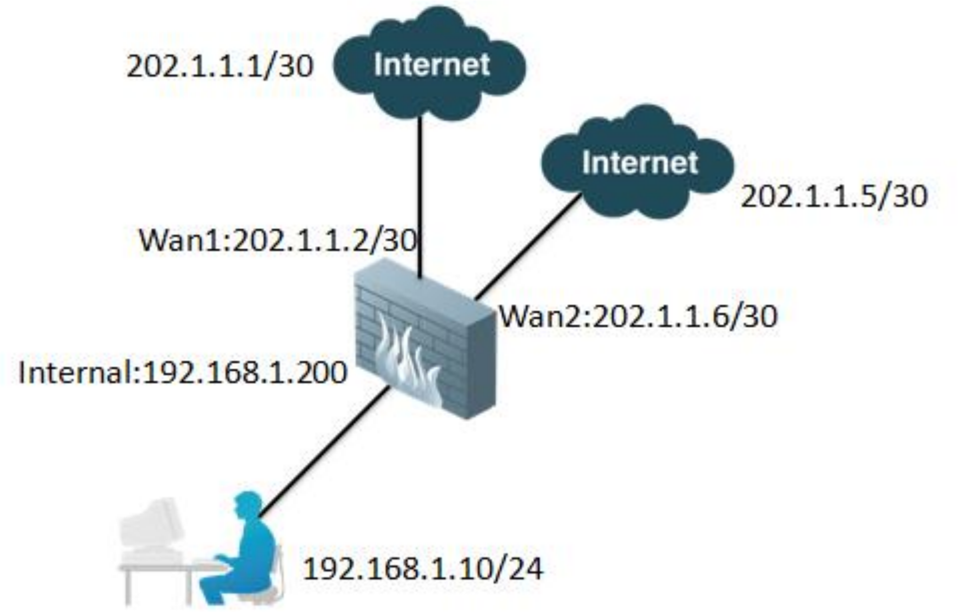
Telecom line 1: wan1 interface, IP address 202.1.1.2/30; gateway address 202.1.1.1

Telecom line 2: wan2 interface, IP address 202.1.1.6/30; gateway address 202.1.1.5

Internal interface: intranet

In this example, the Internet interface address is used as NAT. If there is a need to use the address pool as NAT, see section 1.2.2 “Configuring Internet Access via Dual Lines of Different Carriers” for the policy configuration,.

Network Topology



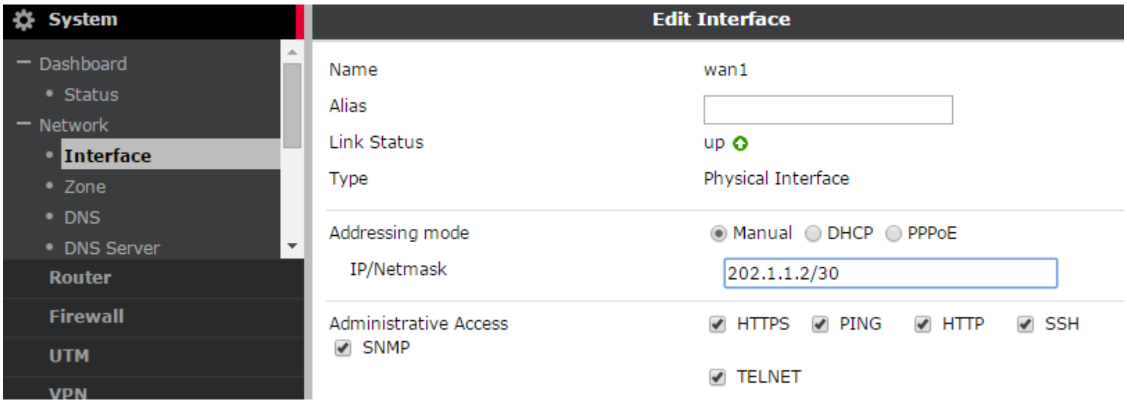
Configuration Tips

1. Configure interface address.
2. Configure a route.
3. Configure zones (untrust and trust zones).
4. Configure the policy.
5. Configure ECMP load-balancing mode.

Configuration Steps

1) Configure interface address.

Choose **System**>**Network**>**Interface**. Tick **wan1** and click **Edit** to display the **Edit Interface** page, as shown in the following figure:



Edit Interface

Name: wan1

Alias:

Link Status: up

Type: Physical Interface

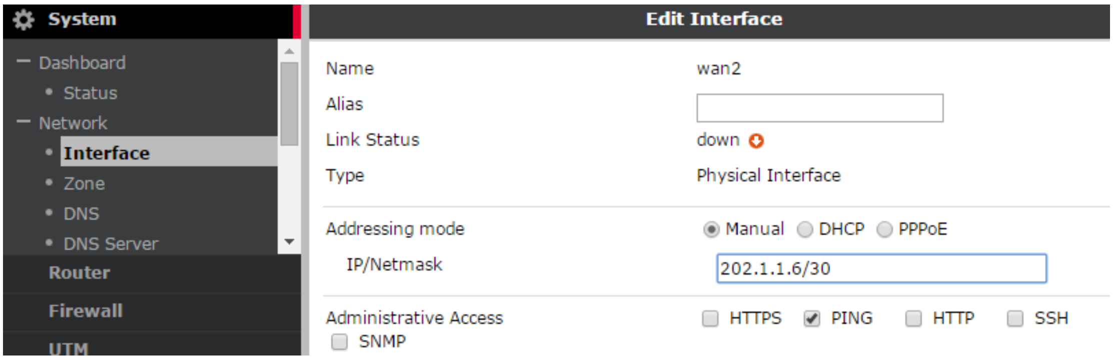
Addressing mode: ● Manual ○ DHCP ○ PPPoE

IP/Netmask: 202.1.1.2/30

Administrative Access: ☑ HTTPS ☑ PING ☑ HTTP ☑ SSH ☑ SNMP ☑ TELNET

Configure IP address and subnet mask to 202.1.1.2/30.

Choose **System**>**Network**>**Interface**. Tick **wan1** and click **Edit** to display the **Edit Interface** page, as shown in the following figure:

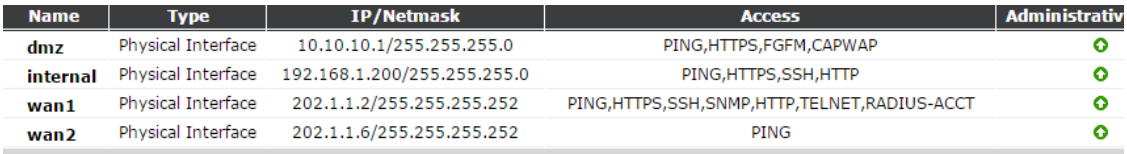


Edit Interface

Name	wan2
Alias	
Link Status	down
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	202.1.1.6/30
Administrative Access	□ HTTPS ☑ PING □ HTTP □ SSH □ SNMP

IP address of wan2 interface is 202.1.1.6/30, and the gateway address is 202.1.1.5.

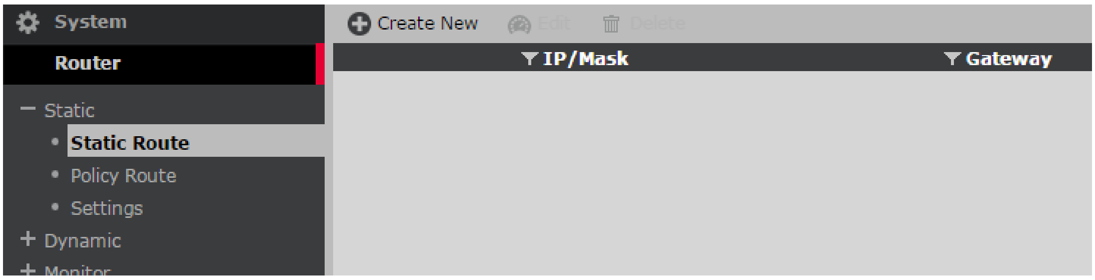
The configuration is as follows:



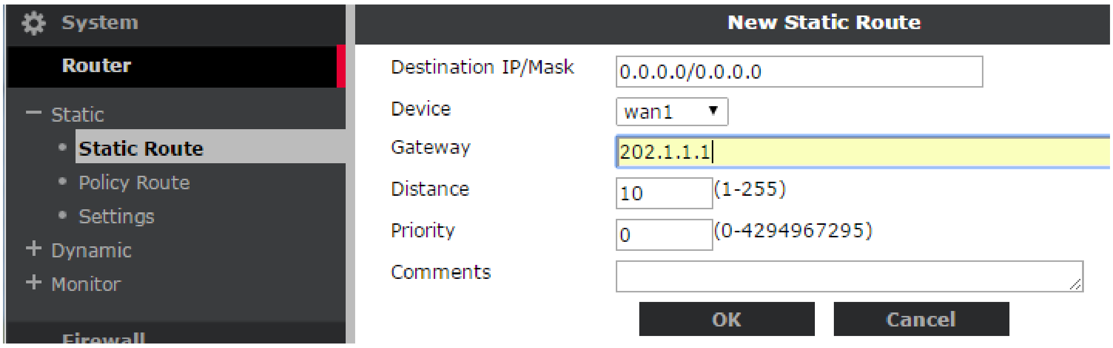
Name	Type	IP/Netmask	Access	Administrativ
dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFM,CAPWAP	●
internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP	●
wan1	Physical Interface	202.1.1.2/255.255.255.252	PING,HTTPS,SSH,SNMP,HTTP,TELNET,RADIUS-ACCT	●
wan2	Physical Interface	202.1.1.6/255.255.255.252	PING	●

2) Configure a route.

Choose **Router**>**Static**>**Static Route**, and then click **Create New**, as shown in the following figure:



Create two routing tables, as shown in the following figure:



New Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan1
Gateway	202.1.1.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

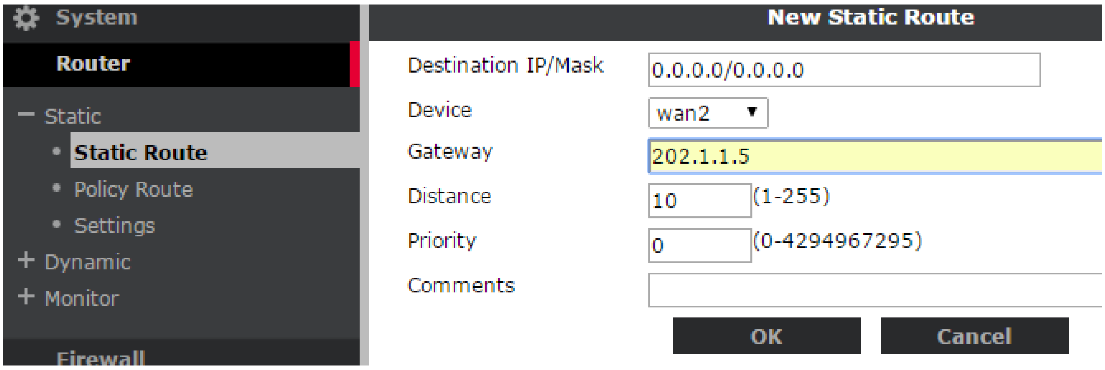
Destination IP/Mask: Keep the default value **0.0.0.0/0.0.0.0**.

Device: Choose **wan1**, which is related to this route. It must be set correctly. Otherwise, the route cannot work.

Gateway: The IP address of the next hop, that is, the IP address of the peer device corresponding to wan1 interface.

Distance: The default value is 10. The route with a shorter distance will be put into the routing table.

Priority: The default value is 0. The route with a smaller priority is used preferentially.



New Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan2
Gateway	202.1.1.5
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Destination IP/Mask: Keep the default value **0.0.0.0/0.0.0.0**.

Device: Choose **wan2**, which is related to this route. It must be set correctly. Otherwise, the route cannot work.

Gateway: The IP address of the next hop, that is, the IP address of the peer device corresponding to wan2 interface.

Distance: The default value is 10. The route with a shorter distance will be put into the routing table.

Priority: The default value is 0. The route with a smaller priority is used preferentially.

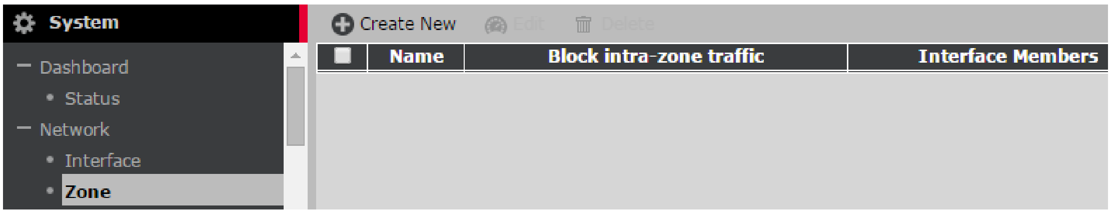
(1) To enable both egress lines to work, ensure that two routing tables have the same path distances. Otherwise, the routing entries with a longer distance will not be put into the routing table.

(2) Besides, their priorities must be the same. With the same distance and different priority, both routes are put into the routing table. The firewall will choose the route with a lower priority preferentially. Therefore, traffic over two links cannot be balanced.

3) Configure zones.

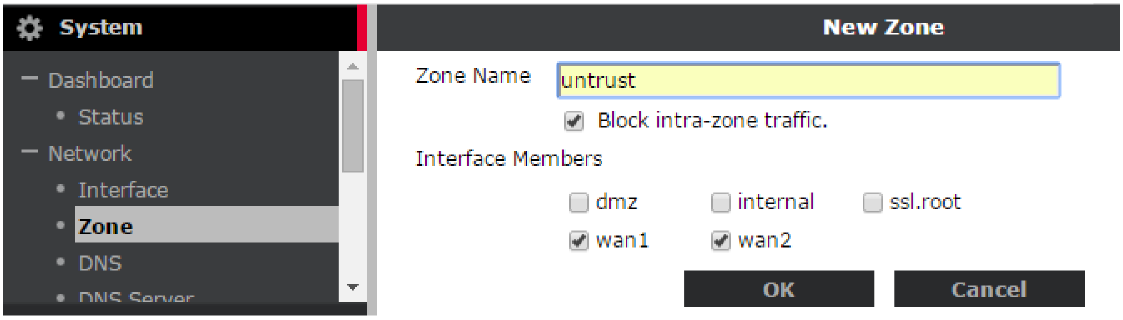
The usage of zones facilitates and simplifies configuration. If Internet access is based on physical interfaces, multiple firewall policies are required.

Choose **System**>**Network**>**Zone**, and then click **Create New**, as shown in the following figure:



□	Name	Block intra-zone traffic	Interface Members

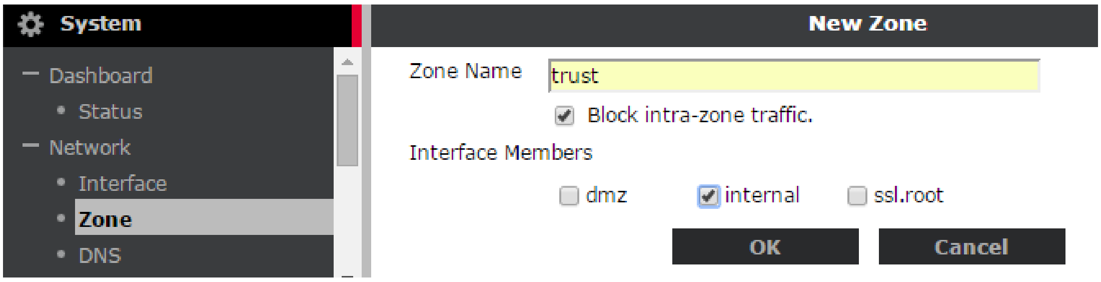
Create untrust and trust zones, as shown in the following figure. The zone can be regarded as an interface group and zone name is user defined.



Zone Name: untrust

☑ Block intra-zone traffic.

Interface Members: □ dmz □ internal □ ssl.root ☑ wan1 ☑ wan2

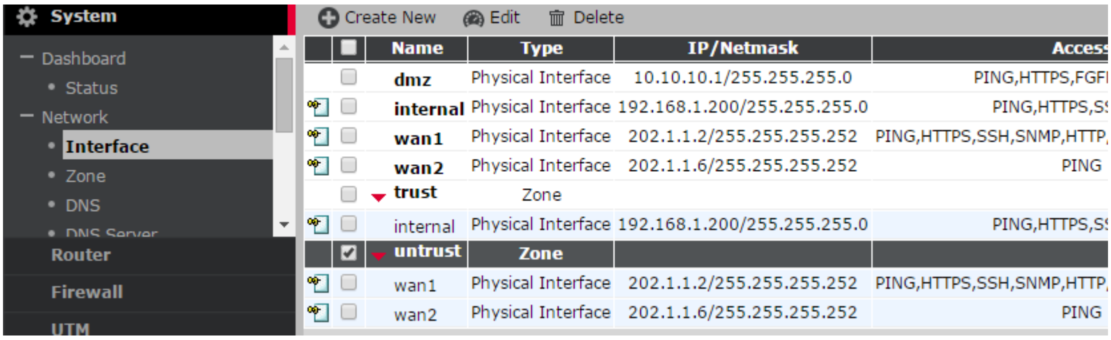


Zone Name: trust

☑ Block intra-zone traffic.

Interface Members: □ dmz ☑ internal □ ssl.root

After configuration, interfaces is displayed as shown in the following figure:

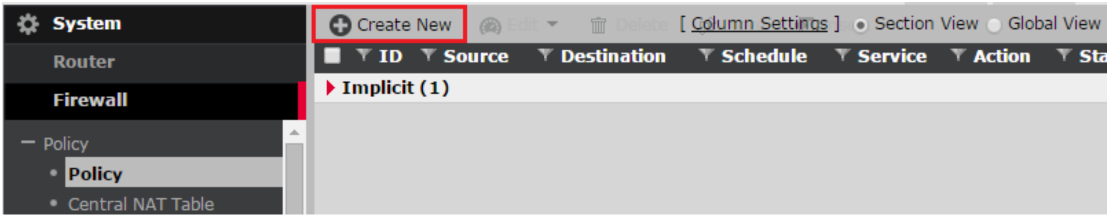


□	Name	Type	IP/Netmask	Access
□	dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFI
□	internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SS
□	wan1	Physical Interface	202.1.1.2/255.255.255.252	PING,HTTPS,SSH,SNMP,HTTP,
□	wan2	Physical Interface	202.1.1.6/255.255.255.252	PING
□	trust	Zone		
□	internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SS
☑	untrust	Zone		
□	wan1	Physical Interface	202.1.1.2/255.255.255.252	PING,HTTPS,SSH,SNMP,HTTP,
□	wan2	Physical Interface	202.1.1.6/255.255.255.252	PING

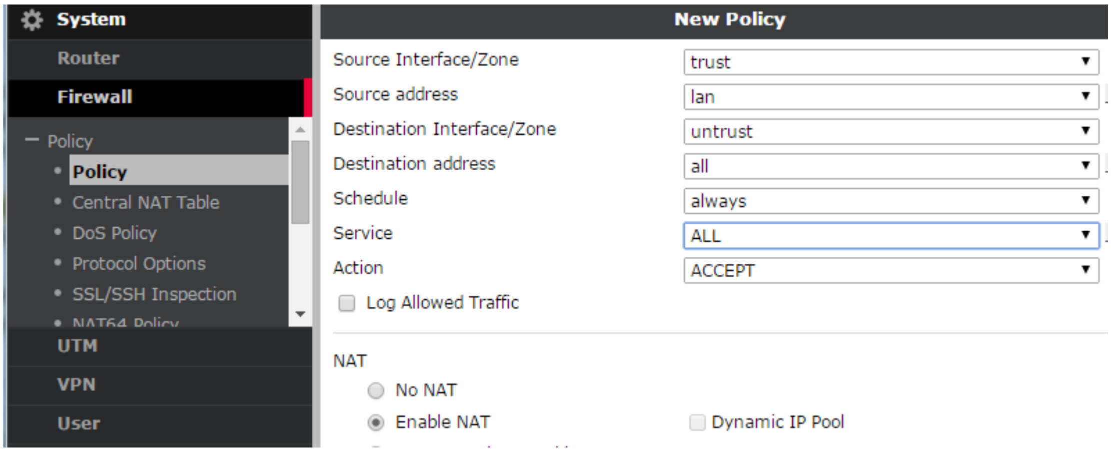
4) Configure the policy.

For some low-end models, the system provides a policy from internal interface to wan1 interface by default. Follow the following steps to add a default route if there is no one.

Choose **Firewall**>**Policy**>**Policy**, and then click **Create New**.



Create a policy, as shown in the following figure:



New Policy

Source Interface/Zone: trust

Source address: lan

Destination Interface/Zone: untrust

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

Source Interface/Zone: Choose **trust**.

Source address: Choose **lan**, which indicates internal network address.

Destination Interface/Zone: Choose **untrust**.

Destination address: Choose **all**, which indicates all the addresses.

Service: Choose **any**.

Log Allowed Traffic: This item is ticked by default. It is recommended to untick it.

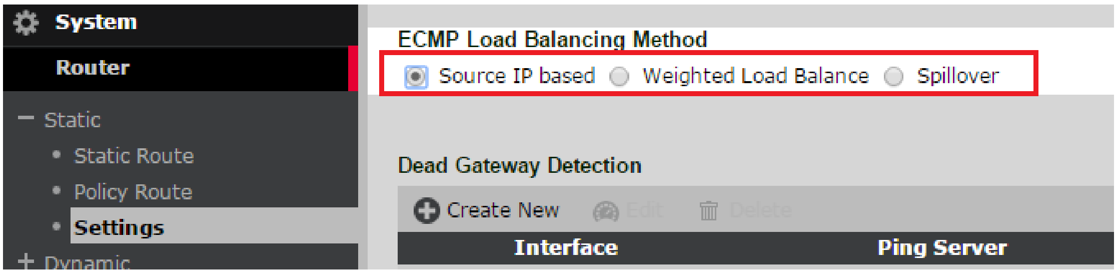
NAT: Tick **Enable ANT**. The system automatically converts the IP address of intranet lan into the IP address of wan1 interface or wan2 interface for Internet access.

Click **OK**. The system automatically saves configuration and the policy takes effect.

Log Allowed Traffic once enabled consumes extra system resources. Therefore, tick this item only when necessary.

5) Configure ECMP load-balancing mode.

The firewall supports the following three load balancing modes:

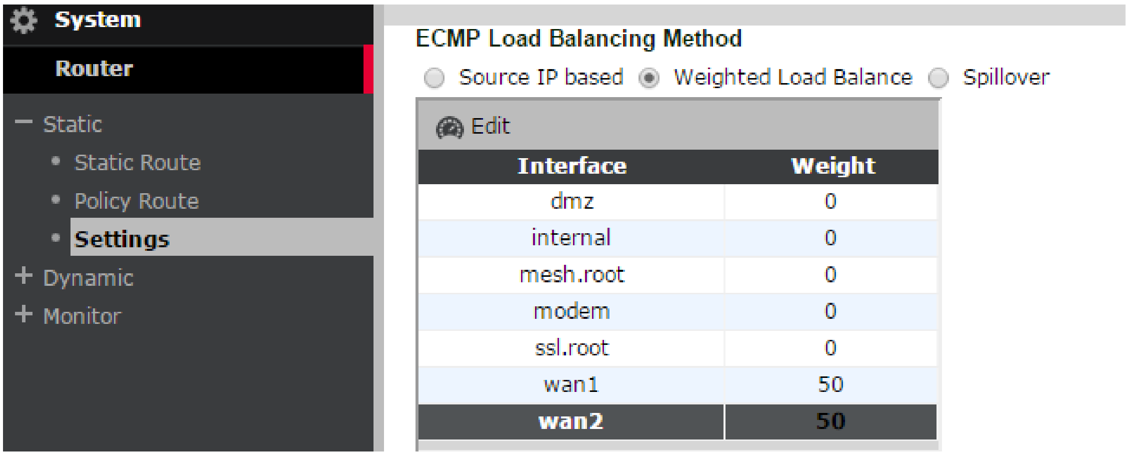


ECMP Load Balancing Method

● Source IP based ○ Weighted Load Balance ○ Spillover

Dead Gateway Detection

Interface	Ping Server



ECMP Load Balancing Method

○ Source IP based ● Weighted Load Balance ○ Spillover

Interface	Weight
dmz	0
internal	0
mesh.root	0
modem	0
ssl.root	0
wan1	50
wan2	50

Source IP based: Choose different routes based on different source IP addresses.

Weighted Load Balance: Choose routes based on weight values. In this example, tick this item.

For example, assume that wan1 interface weight is 50, wan2 interface weight is 50, and weight of other interfaces is 0. In this case, traffic is balanced over two links in 1:1 manner.

Assume that wan1 interface weight is 50 and wan2 interface weight is 100. In this case, traffic is balanced in 1:2 manner.

Spillover: When the traffic over a link exceeds a threshold value, another link is used.

It is recommended to choose **Source IP based**. For example, online banking and online games require source IP address verification. If traffic with different IP addresses interacts, online banking service interaction may fail and games may get offline.

Verification

Check the real-time rates of two interfaces.

3.2.2 Configuring Internet Access via Dual Lines of Different Carriers

Networking Requirements

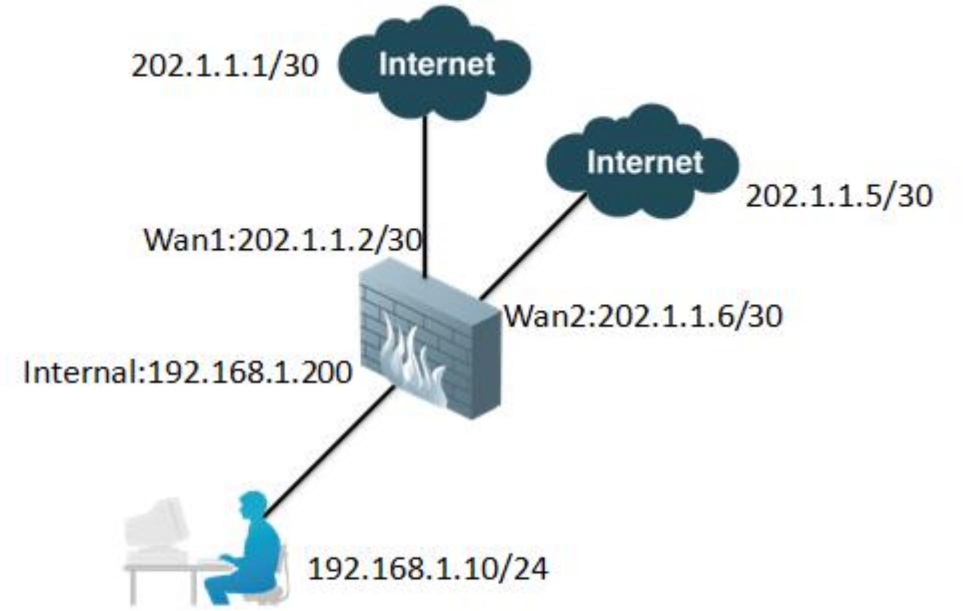
There is one link from the firewall to the Telecom interface and one to Unicom interface. The data transmitted to the IP address of the Telecom interface will pass wan1 interface, while the data transmitted to the IP address of the Unicom interface will pass wan2 interface.

Telecom: wan1 interface, IP address 202.1.1.2/30; gateway address 202.1.1.1; NAT address pool: 100.0.0.1-10

Unicom: wan2 interface, IP address 202.1.1.6/30; gateway address 202.1.1.5; NAT address pool: 200.0.0.1-10

Internal interface: internal 7F51

Network Topology



Configuration Tips

1. Configure IP addresses of interfaces.
2. Configure a route.
3. Configure the address pool.
4. Configure the policy.

Caution

Current routing table entries: The routing table entries for China Telecom reach more than 1,800, while those for China Netcom are more than 400 and those for China Mobile are around 30.

Because the routing tables of the S3100 and S3600 have a limited capacity (100 entries), the S3100 and S3600 are not applied to the multi-line scenario.

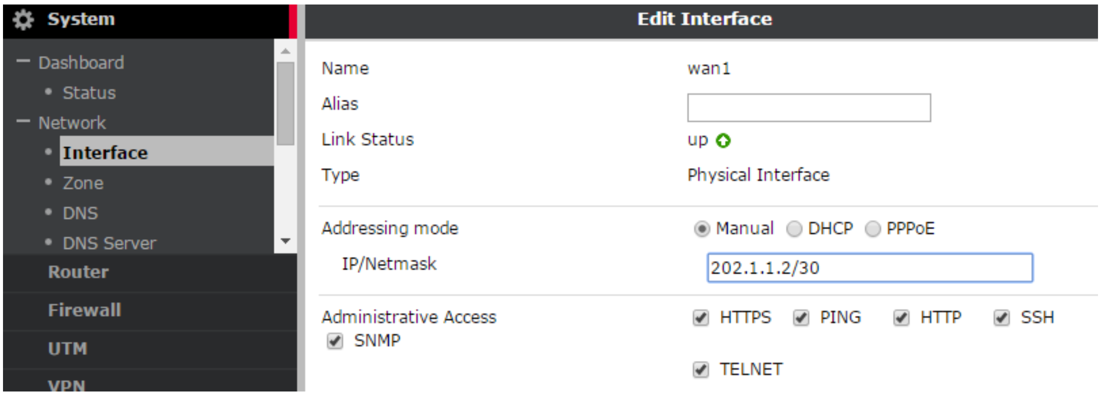
Routing tables of the M5100 and M6600 contain up to 500 entries. When a network involves multiple lines, such as lines of China Telecom and lines of China Netcom, it is recommended to configure a default route for Telecom lines and a static route for Netcom lines.

The X9300 firewalls have sufficient routing table space.

Configuration Steps

1) Configure interface address.

Choose **System**>**Network**>**Interface**. Tick **wan1** and click **Edit** to display the **Edit Interface** page, as shown in the following figure:



Edit Interface

Name: wan1

Alias:

Link Status: up

Type: Physical Interface

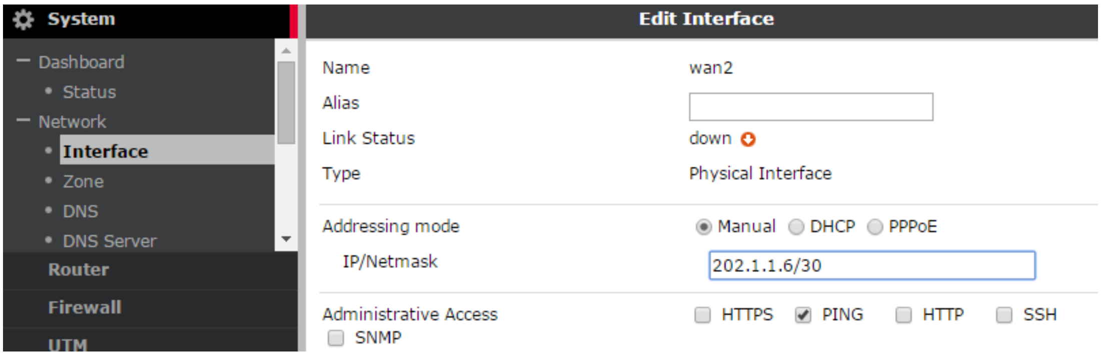
Addressing mode: ● Manual ○ DHCP ○ PPPoE

IP/Netmask: 202.1.1.2/30

Administrative Access: ☑ HTTPS ☑ PING ☑ HTTP ☑ SSH ☑ SNMP ☑ TELNET

Configure IP address and subnet mask to 202.1.1.2/30.

Choose **System**>**Network**>**Interface**. Tick **wan1** and click **Edit** to display the **Edit Interface** page, as shown in the following figure:



Edit Interface

Name: wan2

Alias:

Link Status: down

Type: Physical Interface

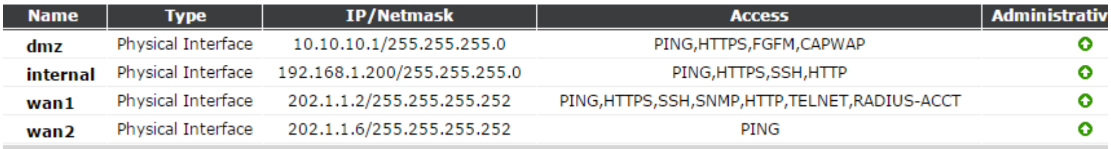
Addressing mode: ● Manual ○ DHCP ○ PPPoE

IP/Netmask: 202.1.1.6/30

Administrative Access: □ HTTPS ☑ PING □ HTTP □ SSH □ SNMP

IP address of wan2 interface is 202.1.1.6/30, while the gateway address is 202.1.1.5.

The configuration is as follows:



Name	Type	IP/Netmask	Access	Administrativ
dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFM,CAPWAP	●
internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP	●
wan1	Physical Interface	202.1.1.2/255.255.255.252	PING,HTTPS,SSH,SNMP,HTTP,TELNET,RADIUS-ACCT	●
wan2	Physical Interface	202.1.1.6/255.255.255.252	PING	●

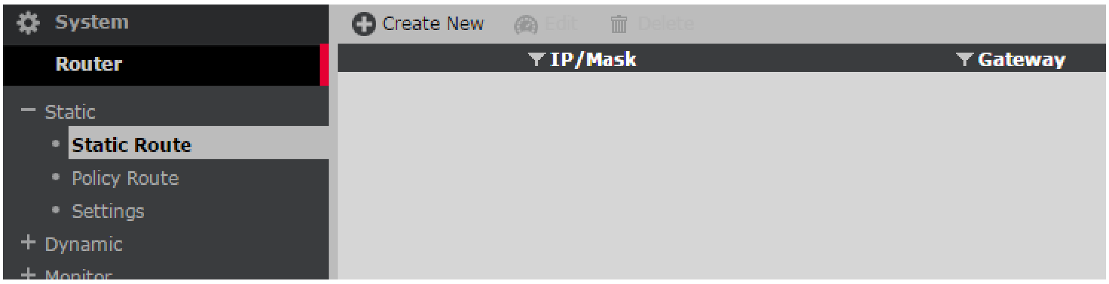
2) Configure a route.

Route for China Telecom: Configure a default route of wan1 interface.

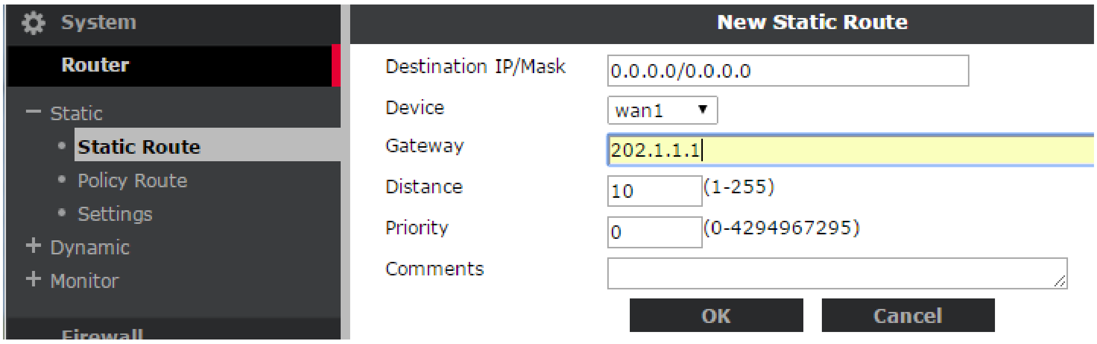
Route for China Unicom: Refer to the tool (attached) for importing routing tables to configure a detailed route. (Recommended)

You can also configure a default route for China Unicom and a detailed route for China Telecom.

Choose **Router**>**Static**>**Static Route**, and then click **Create New**, as shown in the following figure:



Create a default route for China Telecom, as shown in the following figure:



Destination IP/Mask: 0.0.0.0/0.0.0.0

Device: wan1

Gateway: 202.1.1.1

Distance: 10 (1-255)

Priority: 0 (0-4294967295)

Comments:

Destination IP/Mask: Keep the default value **0.0.0.0/0.0.0.0**.

Device: Choose **wan1**, which is connected by this route. It must be set correctly. Otherwise, the route cannot work.

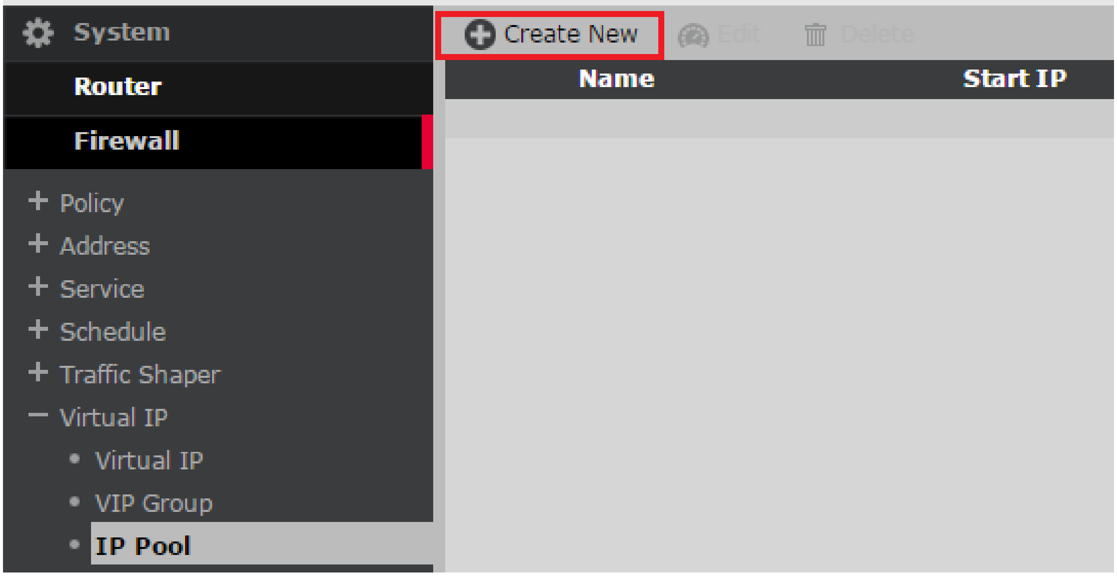
Gateway: The IP address of the next hop, that is, the IP address of the peer device corresponding to wan1 interface.

Distance: The default value is 10. The route with a shorter distance will be put into the routing table.

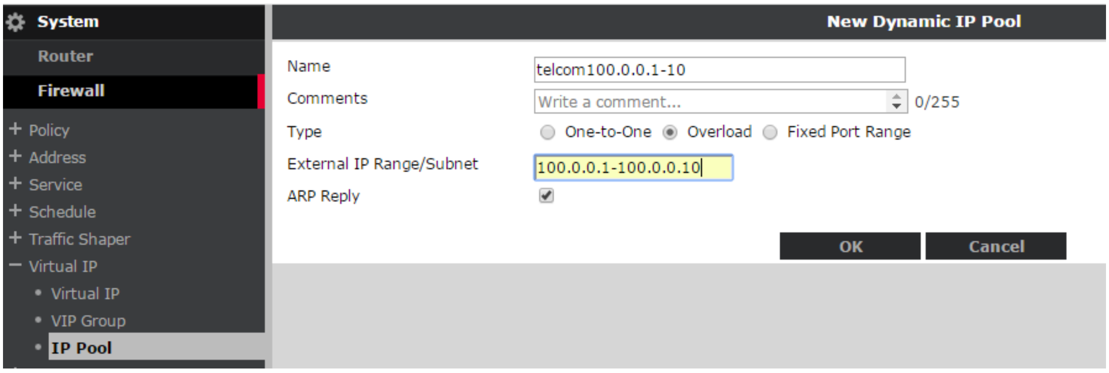
Priority: The default value is 0. The route with a smaller priority is used preferentially.

3) Configure the address pool.

Choose **Firewall**>**Virtual IP**>**IP Pool**, and then click **Create New**, as shown in the following figure:



Create two address pools, as shown in the following figure:



New Dynamic IP Pool

Name: telcom100.0.0.1-10

Comments: Write a comment... 0/255

Type: ○ One-to-One ● Overload ○ Fixed Port Range

External IP Range/Subnet: 100.0.0.1-100.0.0.10

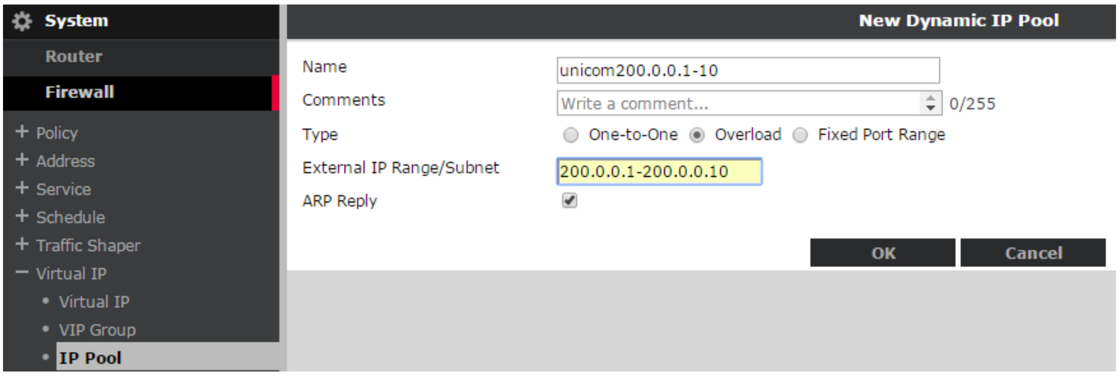
ARP Reply: ☑

Name: Enter **telcom100.0.0.1-10.**

Type: Choose **Overload**. The IP address is dynamically assigned from the address pool.

External IP Range/Subnet: Enter 100.0.0.1-100.0.0.10.

ARP Reply: Tick this item to enable ARP response, which is equivalent to sending gratuitous ARP packets.



New Dynamic IP Pool

Name: unicom200.0.0.1-10

Comments: Write a comment... 0/255

Type: ○ One-to-One ● Overload ○ Fixed Port Range

External IP Range/Subnet: 200.0.0.1-200.0.0.10

ARP Reply: ☑

Name: Enter **unicom200.0.0.1-10.**

Type: Choose **Overload**. The IP address is dynamically assigned from the address pool.

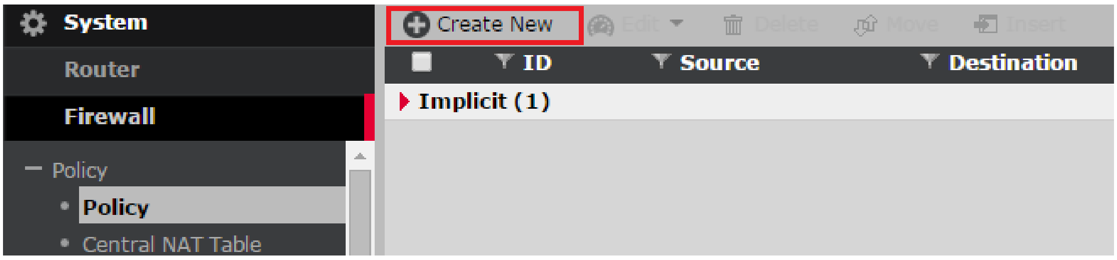
External IP Range/Subnet: Enter 200.0.0.1-200.0.0.10.

ARP Reply: Tick this item to enable ARP response, which is equivalent to sending gratuitous ARP packets.

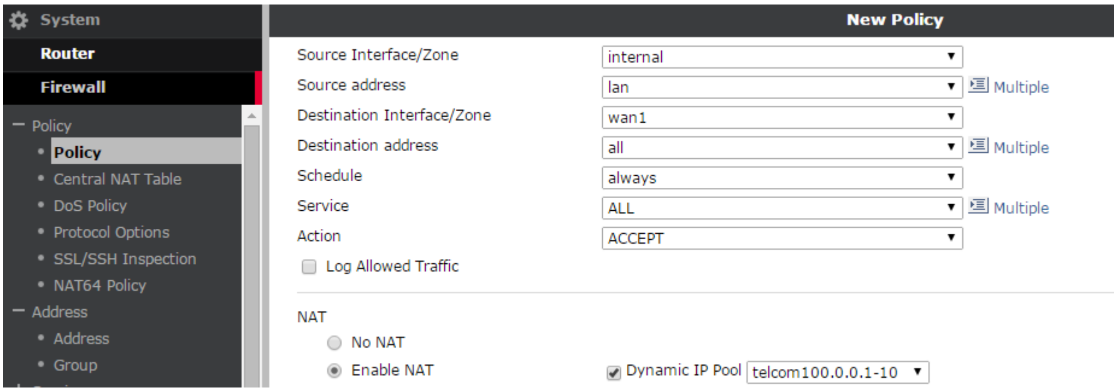
4) Configure the policy.

Configure two policies. One is for the route from the internal interface to wan1 interface, and the other is for the route from the internal interface to wan2 interface.

Choose **Firewall**>**Policy**>**Policy**, and then click **Create New**, as shown in the following figure:



Create a policy for the route from the internal interface to wan1 interface, as shown in the following figure:



New Policy

Source Interface/Zone: internal

Source address: lan (Multiple)

Destination Interface/Zone: wan1

Destination address: all (Multiple)

Schedule: always

Service: ALL (Multiple)

Action: ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT

☑ Dynamic IP Pool: telcom100.0.0.1-10

Source Interface/Zone: Choose **internal**.

Source address: Choose **lan**, which indicates internal network address.

Destination Interface/Zone: Choose **wan1**.

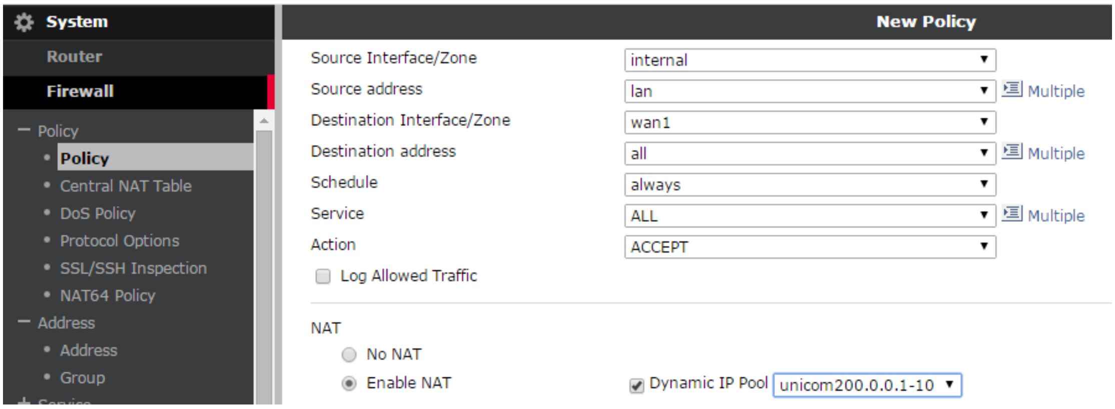
Destination address: Choose **all**, which indicates all the addresses.

Service: Choose **any**.

Log Allowed Traffic: The item is ticked by default. It is recommended to untick it, because many logs will be generated due to excessive data packet traffic and recording normal logs is meaningless.

NAT: Tick **Enable NAT**. Select **Dynamic IP Pool** and choose the corresponding address pool **telecom100.0.0.1-10**.

Create a policy for the route from the internal interface to wan1 interface, as shown in the following figure:



New Policy

Source Interface/Zone: internal

Source address: lan (Multiple)

Destination Interface/Zone: wan1

Destination address: all (Multiple)

Schedule: always

Service: ALL (Multiple)

Action: ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT

☑ Dynamic IP Pool: unicom200.0.0.1-10

Source Interface/Zone: Choose **internal**.

Source address: Choose **lan**, which indicates internal network address.

Destination Interface/Zone: Choose **wan2**.

Destination address: Choose **all**, which indicates all the addresses.

Service: Choose **any**.

Log Allowed Traffic: This item is ticked by default. It is recommended to untick it.

NAT: Tick **Enable NAT**. Select **Dynamic IP Pool** and choose the corresponding address pool **unicom200.0.0.1-10**.

Verification

Access the Internet for testing. Run the **tracert** command to check the path.

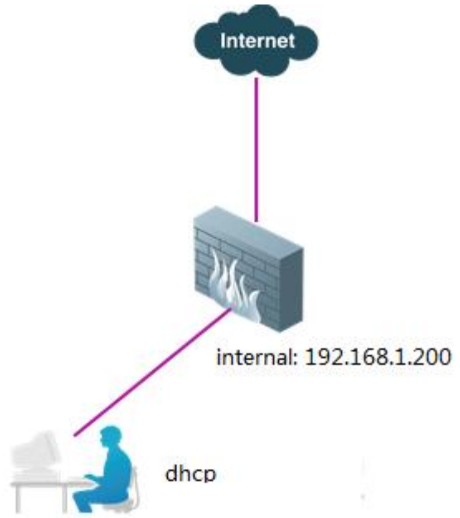
3.3 Configuring DHCP

3.3.1 Configuring the DHCP Server

Networking Requirements

Enable DHCP sever function of the NGFW. The intranet PC can automatically obtain an IP address for Internet access. The intranet segment is 192.168.1.0/24 and the gateway address is 192.168.1.200.

Network Topology



Configuration Tips

1. Basic configuration for Internet access
2. Configure the DHCP server.

Configuration Steps

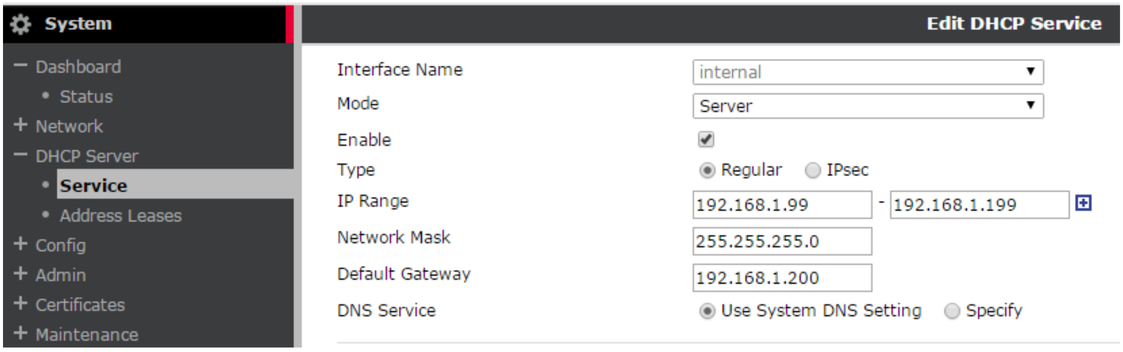
1. Basic configuration for Internet access

For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under section “Internet Access via a Single Line” in “Configuring Routing Mode”.

2. Configure the DHCP service.

   a) Enable the DHCP service.

Choose **System**>**DHCP Server**>**Service**, and then click **Create New**, as shown in the following figure:



Edit DHCP Service

Interface Name	internal ▾
Mode	Server ▾
Enable	☑
Type	● Regular ○ IPsec
IP Range	192.168.1.99 - 192.168.1.199
Network Mask	255.255.255.0
Default Gateway	192.168.1.200
DNS Service	● Use System DNS Setting ○ Specify

Interface Name: Choose the interface where the DHCP server is connected to.

Mode: Choose **Server** or **Relay**.

Enable: This item is ticked by default.

Type: Choose **Regular** or **IPsec**. If you choose **IPsec**, the system assigns IP addresses for IPsec users.

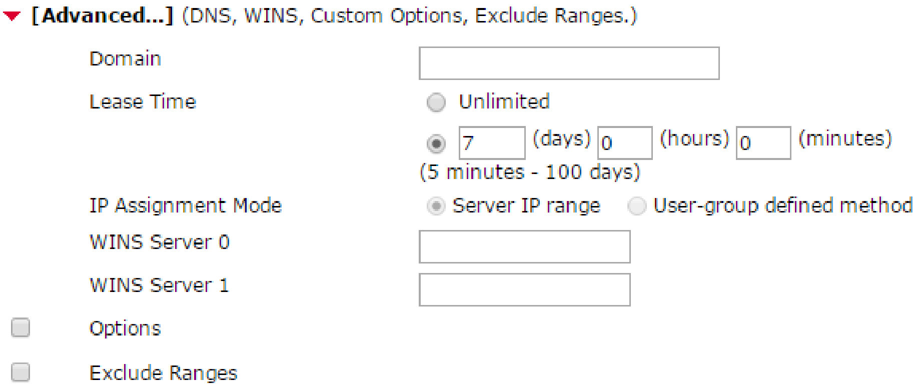
IP Range: It indicates the IP address range assigned to users.

Network Mask: It indicates the subnet mask. Set it to **255.255.255.0**.

Default Gateway: Generally, it indicates the IP address of the interface that the DHCP server is connected to.

DNS Service: You can choose **Specify** or **Use System DNS Setting**.

b) Advanced options. You can set the lease time and excluded range, as shown in the following figure:


[Advanced...] (DNS, WINS, Custom Options, Exclude Ranges.)

Domain	
Lease Time	○ Unlimited ● 7 (days) 0 (hours) 0 (minutes) (5 minutes - 100 days)
IP Assignment Mode	● Server IP range ○ User-group defined method
WINS Server 0	
WINS Server 1	
□ Options	
□ Exclude Ranges	

Lease Time: It is set to **1** day, which can be adjusted according to the actual situations. If you choose **Unlimited**, the assigned IP addresses are not released forever. Therefore, **Unlimited** is not recommended.

Options: It is used to configure the DHCP server options.

Exclude Ranges: Enter the IP address segment to be reserved, such as 192.168.1.120-192.168.1.130.

Verification

Set the PC to automatically obtain an IP address.

Notes

1. **Question: Among DHCP configuration, does the system DNS refer to the DNS settings of the firewall itself?**

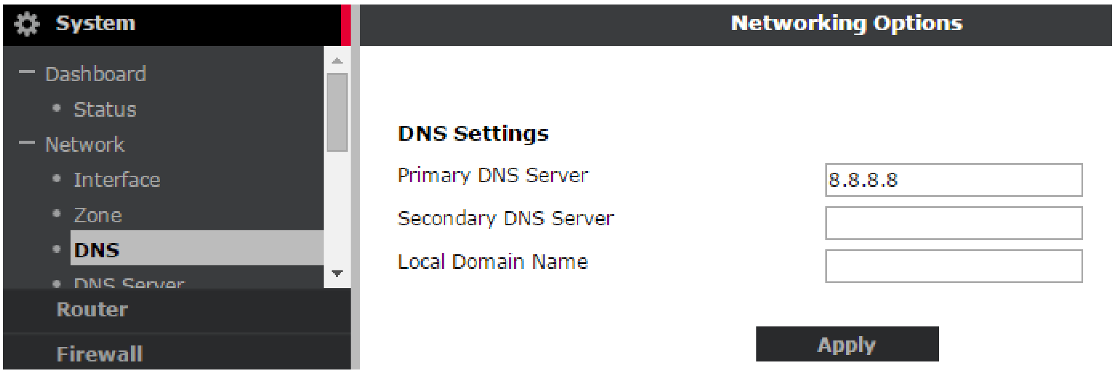
DHCP configuration provides three DNS options:

```
RG-WALL # config system dhcp server
    RG-WALL (server) #edit 1
    RG-WALL (1)#set auto-configuration enable
    RG-WALL (1)#set conflicted-ip-timeout 1800
    RG-WALL (1)#set default-gateway 192.168.1.99
    RG-WALL (1)#set dns-service default        //Default parameter

default    Use system DNS settings.    // DNS server configured on the firewall.
local      Use this RGT as DNS server.   //IP address of the firewall interface.
specify    Specify DNS servers.         //Specify DNS servers.
```

2. **When you run the set dns-service default command, the PC obtains the DNS server configured by the firewall itself.**

Set the DNS server of the firewall itself.

```
RG-WALL #config system dns      //DNS server configured on the firewall.
    RG-WALL (dns) #set primary 8.8.8.8
    RG-WALL (dns) #end
```



DNS Settings

Primary DNS Server 8.8.8.8

Secondary DNS Server

Local Domain Name

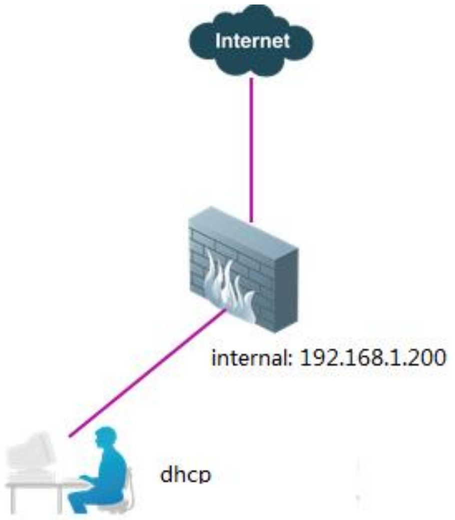
3. **When you run the set dns-service local command, the PC obtains the IP address of the DHCP interface enabled by the firewall.**

3.3.2 DHCP Static Binding

Networking Requirements

Enable DHCP sever function of the NGFW. The intranet PC can automatically obtain an IP address for Internet access. The intranet segment is 192.168.1.0/24 and the gateway address is 192.168.1.200. Reserve IP address 192.168.1.100 for the host with MAC address 04:7d:7b:9b:71:ad.

Network Topology



Configuration Tips

1. Basic configuration for Internet access

2. Configure the DHCP server.

Configuration Steps

1) Basic configuration for Internet access

2) Configure the DHCP service.

See section “Configuring the DHCP Server”.

3) Configure the reserved IP address.

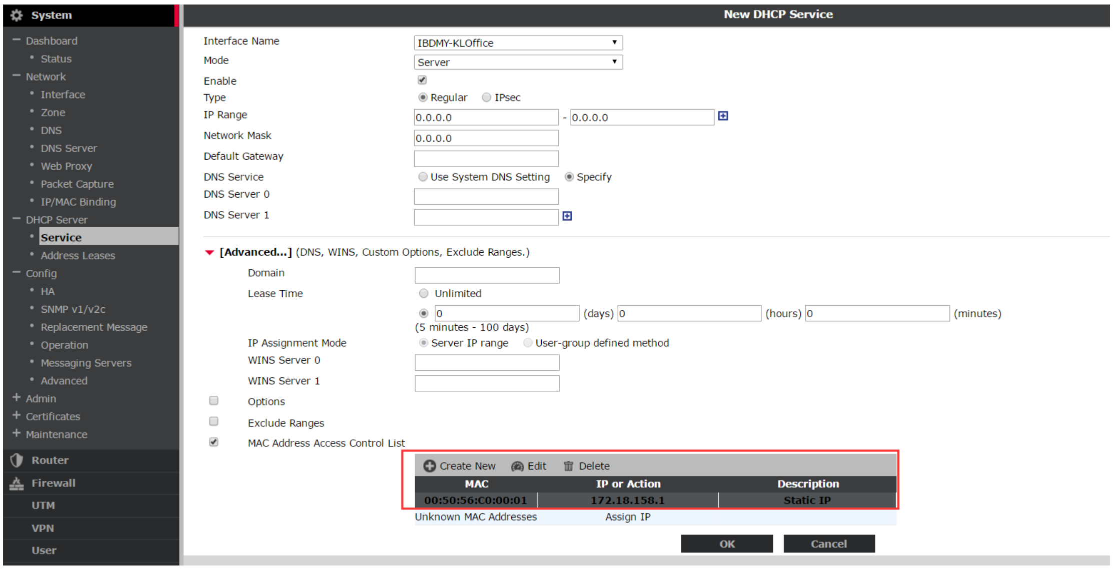
Before operation, it is recommended to upgrade the firewall version to the latest..

Way 1(CLI):

```
RG-WALL # config system dhcp server
        RG-WALL (server) # edit 1
//Basic configuration
        RG-WALL (1)#set dns-service default
        RG-WALL (1)#set default-gateway 192.168.1.200
        RG-WALL (1)#set netmask 255.255.255.0
        RG-WALL (1)#set interface internal
        RG-WALL (1) # config ip-range
        RG-WALL (ip-range) #edit 1
        RG-WALL (1)set start-ip 192.168.1.99
        RG-WALL (1)set end-ip 192.168.1.199
        RG-WALL (1) # next
        RG-WALL (ip-range) # end                          //Basic configuration of
        RG-WALL (1)#config reserved-address                        //Configure the reserved
IP address.
```

```
        RG-WALL (reserved-address)#edit 1                              //Entry 1, 2, or 3,
which is used as identification. You can define multiple entries.
        RG-WALL (1) # set ip 192.168.1.100                    //Assign the IP address to the
specified MAC address.
        RG-WALL (1) # set mac 04:7d:7b:9b:71:ad          //Specify the MAC address.
        RG-WALL (1) # next
        RG-WALL (reserved-address) # end
        RG-WALL (1) # next
        RG-WALL (server) #end
```

Way 2(Web UI):



New DHCP Service

Interface Name	IBDMY-KLOffice
Mode	Server
Enable	☑
Type	● Regular ○ IPsec
IP Range	0.0.0.0 - 0.0.0.0
Network Mask	0.0.0.0
Default Gateway	
DNS Service	○ Use System DNS Setting ● Specify
DNS Server 0	
DNS Server 1	

[Advanced...] (DNS, WINS, Custom Options, Exclude Ranges.)

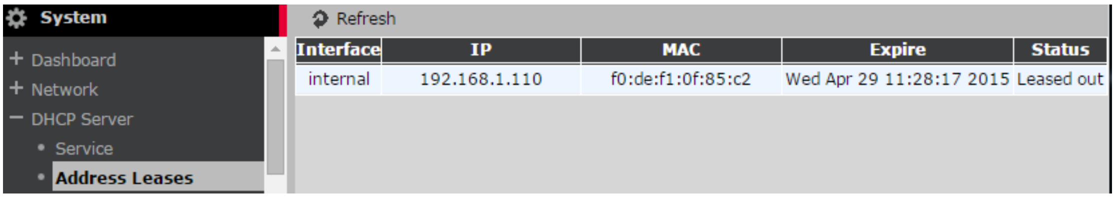
Domain	
Lease Time	○ Unlimited ● 0 (days) 0 (hours) 0 (minutes) (5 minutes - 100 days)
IP Assignment Mode	● Server IP range ○ User-group defined method
WINS Server 0	
WINS Server 1	
□ Options	
□ Exclude Ranges	
☑ MAC Address Access Control List	

MAC	IP or Action	Description
00:50:56:C0:00:01	172.18.158.1	Static IP
Unknown MAC Addresses	Assign IP	

Verification

Set the PC to automatically obtain an IP address. The host with MAC address 04:7d:7b:9b:71:ad will obtain IP address 192.168.1.100.

1. **Check the DHCP address pool assignment on the firewall, as shown in the following figure:**



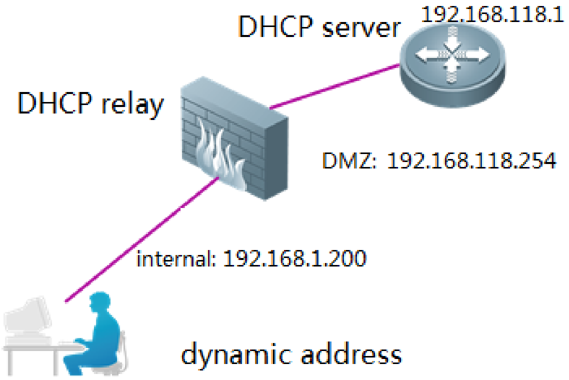
Interface	IP	MAC	Expire	Status
internal	192.168.1.110	f0:de:f1:0f:85:c2	Wed Apr 29 11:28:17 2015	Leased out

3.3.3 DHCP Relay Configuration

I. Networking Requirements

Enable DHCP relay of RG-WALL 1600 Series Next-Generation Firewall (NGFW) to allow the intranet PC to obtain the address assigned to the device by the DHCP server.

II. Network Topology



III. Configuration Tips

1. Basic configuration for Internet access

2. Enable DHCP relay and enter the address of the DHCP server.

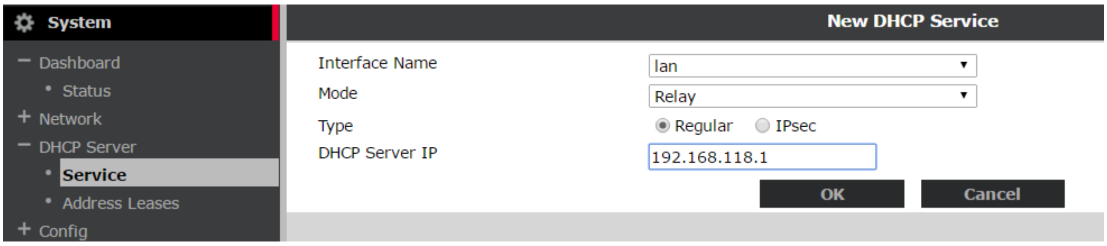
IV. Configuration Steps

1. Basic configuration for Internet access

For the detailed configuration process, see section 1.1.2 "Configuring Internet Access via a Static Link" under section 1.1 "Internet Access via a Single Line" in Chapter 1 "Typical Functions of Routing Mode".

Enable DHCP relay and enter the address of the DHCP server.

Choose **System** > **DHCP Server** > **Service**, and then click Create New.



New DHCP Service

Interface Name: lan

Mode: Relay

Type: ● Regular ○ IPsec

DHCP Server IP: 192.168.118.1

OK Cancel

Interface Name: Choose the interface where the DHCP server is connected to.

Mode: Choose **Server** or **Relay**.

Type: Choose **Regular** or **IPsec**. If you choose **IPsec**, the system assigns IP addresses for IPsec users.

DHCP Server IP: Enter the IP address of the DHCP server.

V. Verification

Set the PC to automatically obtain an IP address.

3.4 Port Mapping

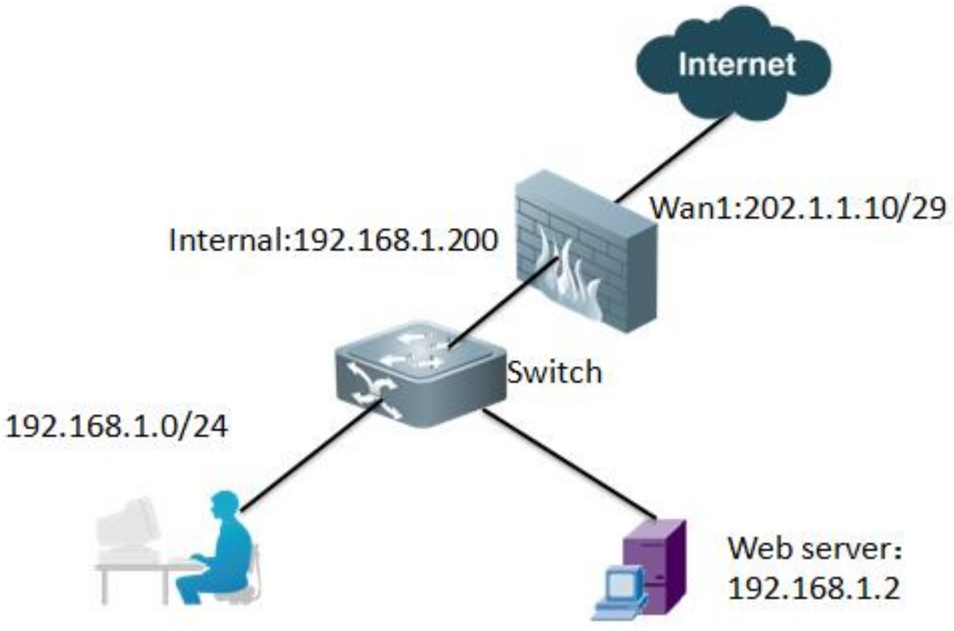
3.4.1 Address Mapping (One-to-One IP Address Mapping)

Networking Requirements

As shown in the following figure, you have completed the basic configuration of the firewall. Now, you need to map one web server address (IP address: 192.168.1.2) on the intranet to the extranet port address (IP address: 202.1.1.11) so that extranet users can access the web server.

Meantime, intranet users can access the web server by using a public network IP address.

Network Topology



Configuration Tips

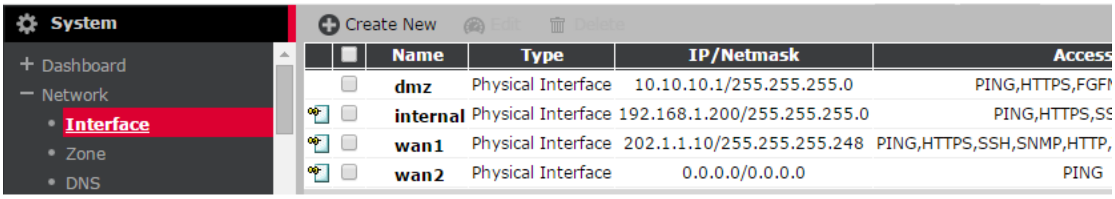
1. Basic configuration for Internet access
2. Configure the virtual IP address (DNAT).
3. Configure the security policy.

Configuration Steps

1. Basic configuration for Internet access

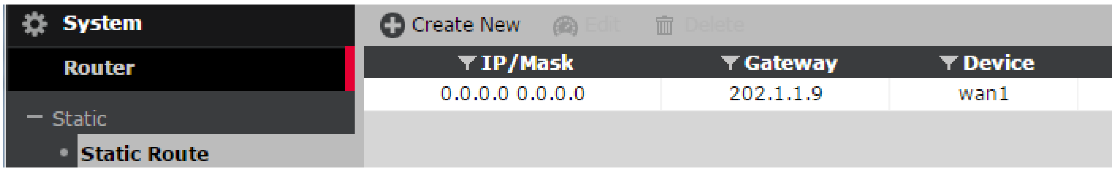
For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under “Internet Access via a Single Line” in “Configuring Routing Mode”.

IP addresses of the interfaces are displayed as shown in the following figure:



	Name	Type	IP/Netmask	Access
	dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFI
	internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SS
	wan1	Physical Interface	202.1.1.10/255.255.255.248	PING,HTTPS,SSH,SNMP,HTTP,
	wan2	Physical Interface	0.0.0.0/0.0.0.0	PING

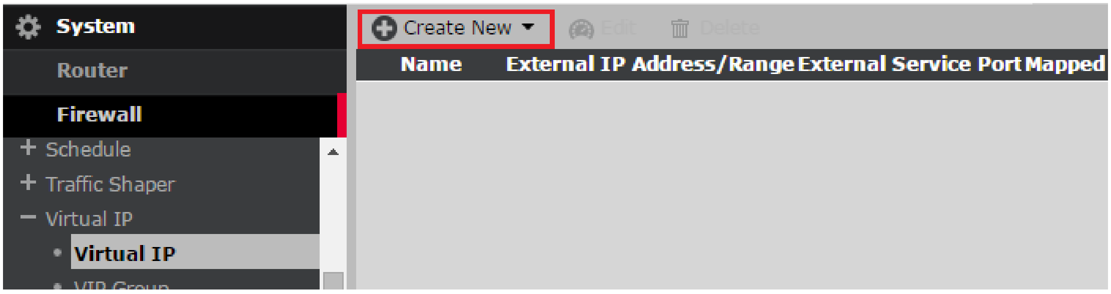
The route configuration is as shown in the following figure:



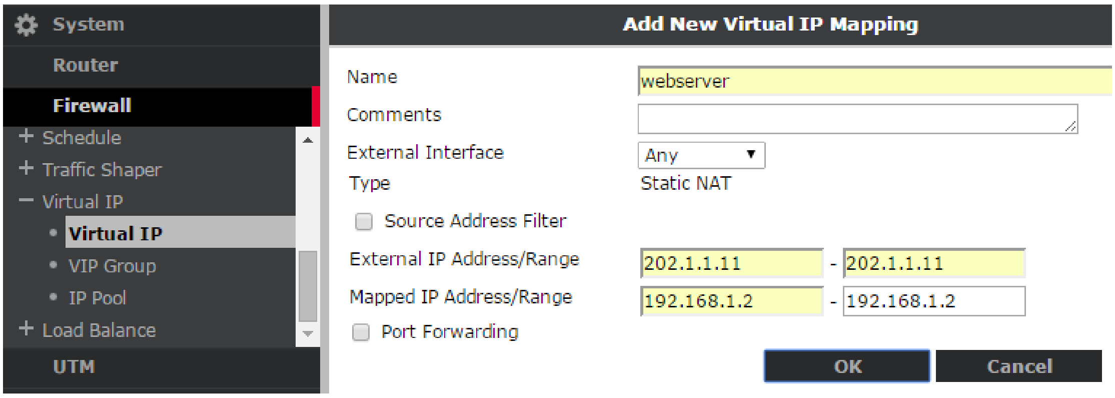
IP/Mask	Gateway	Device
0.0.0.0 0.0.0.0	202.1.1.9	wan1

2. Configure the virtual IP address (DNAT).

Choose **Firewall**>**Virtual IP**>**Virtual IP**, and then click **Create New**, as shown in the following figure:



Configure the virtual IP address. Set the name to **webserver**. The virtual IP address is used for the destination address conversion of wan1 interface.



Add New Virtual IP Mapping

Name: webserver

Comments:

External Interface: Any

Type: Static NAT

□ Source Address Filter

External IP Address/Range: 202.1.1.11 - 202.1.1.11

Mapped IP Address/Range: 192.168.1.2 - 192.168.1.2

□ Port Forwarding

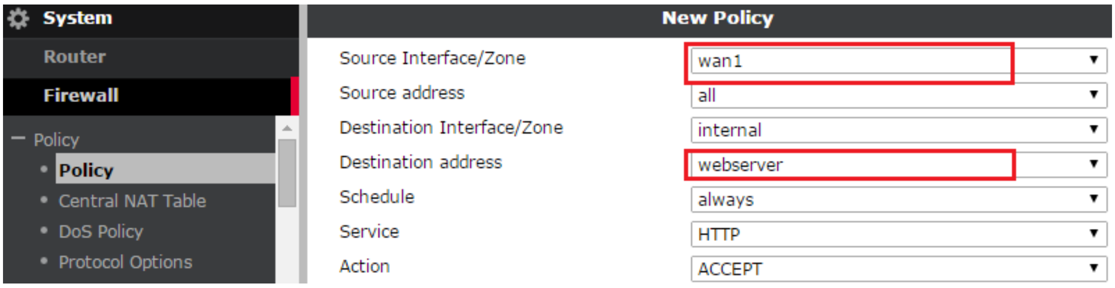
Values of **External IP Address/Range** are mapped to the values of **Mapped IP Address/Range** correspondingly. Enter both the start and end IP addresses of the external IP address range. You just need to enter the start mapped IP address and the system automatically enter the end IP address.

Take the IP address range from 202.1.1.3 to 202.1.1.10 as an example. The start IP address for internal mapping is 192.168.1.2 and the end IP address must be 192.168.1.9 (which is filled in by the system automatically). The IP addresses within the two ranges are mapped correspondingly.

For example, the IP address 202.1.1.3 is mapped to 192.168.1.2, while the IP address 202.1.14 is mapped to 192.168.1.3.

3. Configure the security policy.

Choose **Firewall**>**Policy**>**Policy**, and then click **Create New**, as shown in the following figure:



Source Interface/Zone	wan1
Source address	all
Destination Interface/Zone	internal
Destination address	webserver
Schedule	always
Service	HTTP
Action	ACCEPT

Source Interface/Zone: Choose **wan1**. //If intranet users need to access the Internet by using a virtual IP address, choose **any**.

Source address: Choose **all**.

Destination Interface/Zone: Choose **internal**.

Destination address: Choose **webserver**. //It indicates the defined object mapped by the virtual IP address.

Service: Choose **HTTP**. //The system only allows Internet access via HTTP.

If intranet users need to access the Internet by using a virtual IP address, choose one of the following two methods:

1. Set **Source Interface/Zone** of the original policy to **any**.
2. Add one internal-to-internal policy with the **Source Interface/Zone** value of **internal**.

Source Interface/Zone: Choose **internal**.

Source address: Choose **all**.

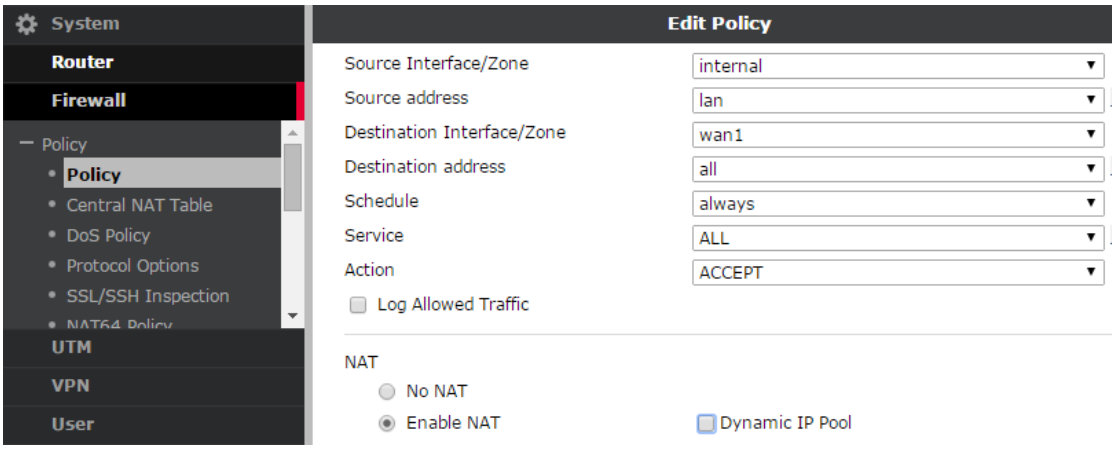
Destination Interface/Zone: Choose **internal**.

Destination address: Choose **webserver**. //It indicates the defined object mapped by the virtual IP address.

Service: Choose **HTTP**. //The system only allows Internet access via HTTP.

4. Intranet users are allowed to access the VIP public network IP address.

Intranet users are allowed to access the internal web server by using the IP address mapped by the public network. You just need to add one policy that allows intranet users to access extranet. Add the policy, as shown in the following figure:



Edit Policy

Source Interface/Zone	internal
Source address	lan
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

Verification

Access http://202.1.1.11 from extranet. To test whether the mapping is valid, temporarily add the ping service .

3.4.2 Port Mapping (One-to-Many Port Mapping)

Networking Requirements

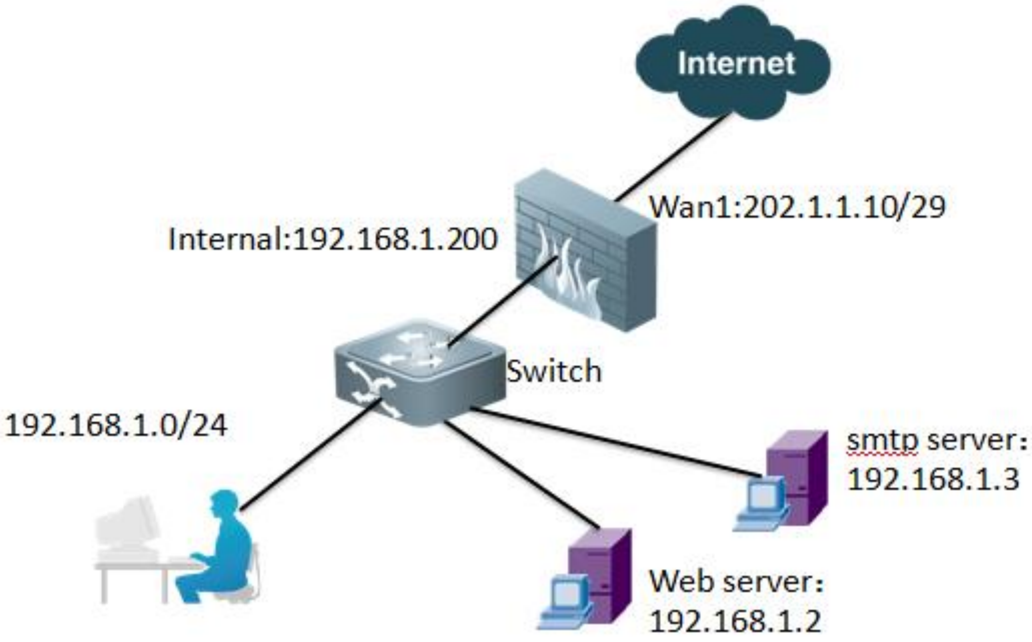
As shown in the following figure, you have completed the basic configuration of the firewall.

Map port 80 of one intranet web server (IP address: 192.168.1.2) to the extranet port 8080 (IP address: 202.1.1.11). (The intranet port is different from the mapped port of the extranet.)

Map port 25 of one intranet SMTP server (IP address: 192.168.1.3) to port 25 of the extranet port (IP address: 202.1.1.11).

Meaning of this case: Master the mapping sequence of the critical function of the new NGFW: DNAT > Route > Security Policy > Source NAT.

Network Topology



Configuration Tips

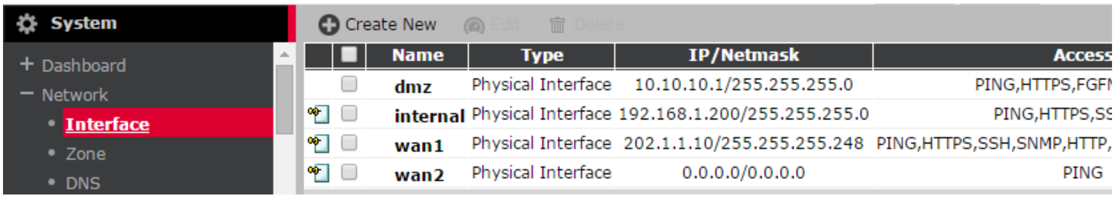
1. Basic configuration for Internet access
2. Configure the virtual IP address (DNAT).
3. Configure the security policy.

Configuration Steps

1. Basic configuration for Internet access

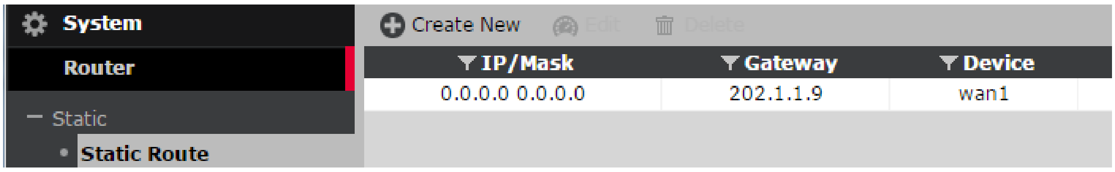
For the detailed configuration process, see section "Configuring Internet Access via a Static Link" section under "Internet Access via a Single Line" in "Configuring Routing Mode".

IP addresses of the interfaces are displayed as shown in the following figure:



Name	Type	IP/Netmask	Access
dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGF
internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SS
wan1	Physical Interface	202.1.1.10/255.255.255.248	PING,HTTPS,SSH,SNMP,HTTP,
wan2	Physical Interface	0.0.0.0/0.0.0.0	PING

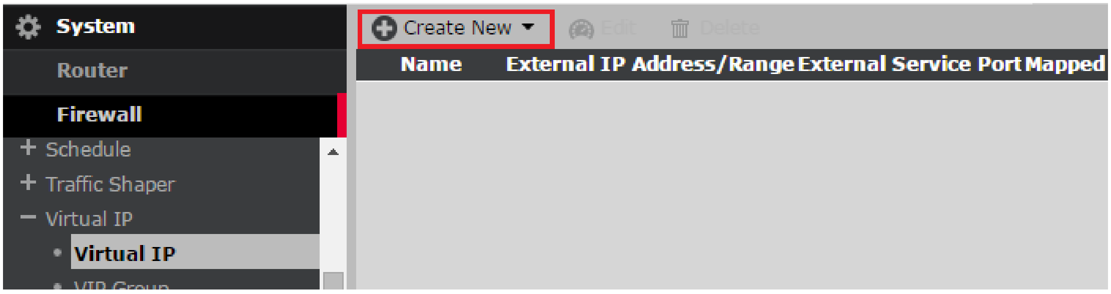
The route configuration is as shown in the following figure:



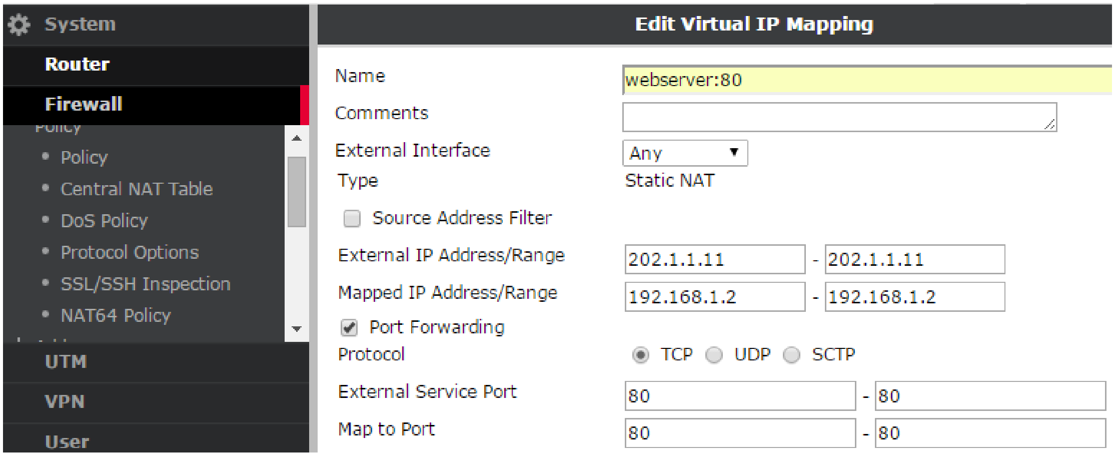
IP/Mask	Gateway	Device
0.0.0.0 0.0.0.0	202.1.1.9	wan1

2. Configure the virtual IP address (DNAT).

Choose **Firewall**>**Virtual IP**>**Virtual IP**, and then click **Create New** to create a new virtual IP address, as shown in the following figure:



Create virtual IP1. Set **Name** to **webserver:80** to map the HTTP server, as shown in the following figure:



Edit Virtual IP Mapping

Name: webserver:80

Comments:

External Interface: Any

Type: Static NAT

□ Source Address Filter

External IP Address/Range: 202.1.1.11 - 202.1.1.11

Mapped IP Address/Range: 192.168.1.2 - 192.168.1.2

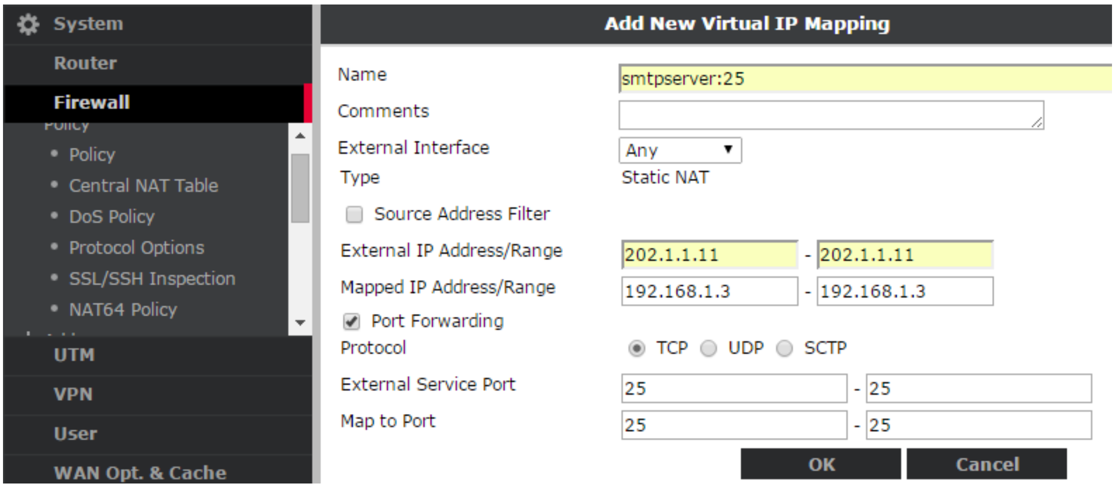
☑ Port Forwarding

Protocol: ● TCP ○ UDP ○ SCTP

External Service Port: 80 - 80

Map to Port: 80 - 80

Create virtual IP2. Set **Name** to **smtpserver:25** to map the SMTP server, as shown in the following figure:



Add New Virtual IP Mapping

Name: smtpserver:25

Comments:

External Interface: Any

Type: Static NAT

□ Source Address Filter

External IP Address/Range: 202.1.1.11 - 202.1.1.11

Mapped IP Address/Range: 192.168.1.3 - 192.168.1.3

☑ Port Forwarding

Protocol: ● TCP ○ UDP ○ SCTP

External Service Port: 25 - 25

Map to Port: 25 - 25

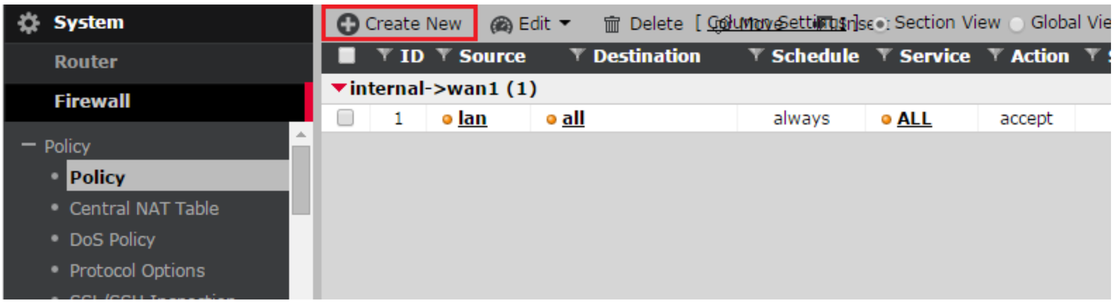
Values of **External IP Address/Range** are mapped to the values of **Mapped IP Address/Range** correspondingly. Enter both the start and end IP addresses of the external IP address range. You just need to enter the start mapped IP address and the system automatically enters the end IP address.

Take the IP address range from 202.1.1.3 to 202.1.1.10 as an example. The start IP address for internal mapping is 192.168.1.2 and the end IP address must be 192.168.1.9 (which is filled in by the system automatically). The IP addresses within the two ranges are mapped correspondingly.

For example, the IP address 202.1.1.3 is mapped to 192.168.1.2, while the IP address 202.1.14 is mapped to 192.168.1.3.

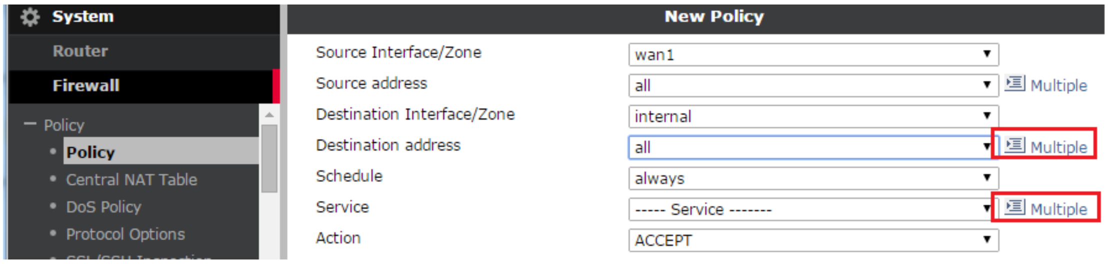
3. Configure the security policy.

Choose **Firewall**>**Policy**>**Policy**, and then click **Create New**, as shown in the following figure:



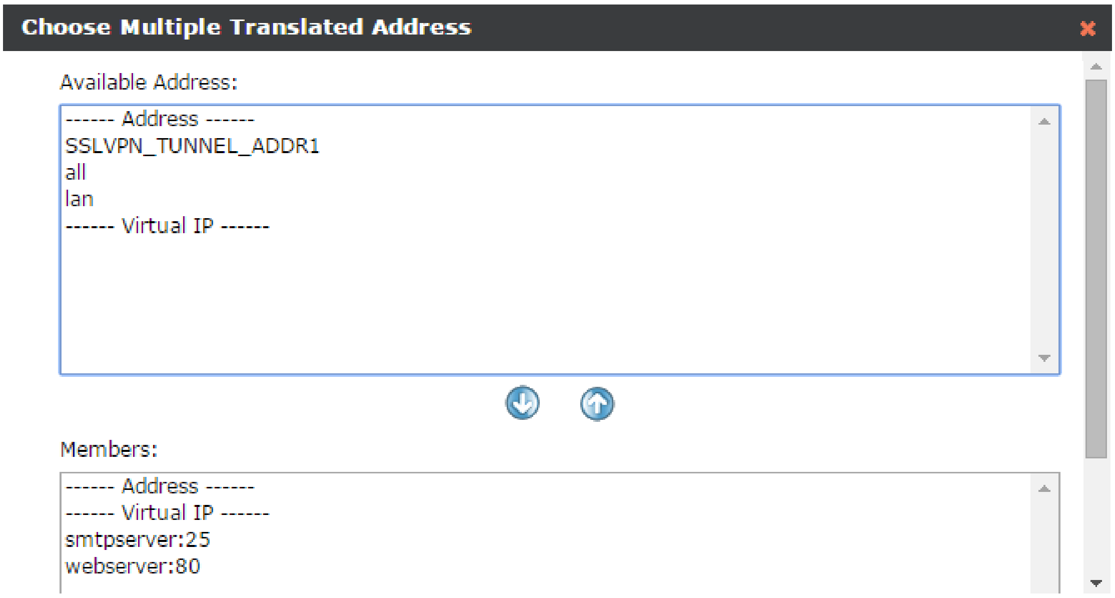
ID	Source	Destination	Schedule	Service	Action
internal->wan1 (1)					
1	lan	all	always	ALL	accept

On the **New Policy** page, add one policy as shown in the following figure:



Source Interface/Zone	wan1
Source address	all
Destination Interface/Zone	internal
Destination address	all
Schedule	always
Service	----- Service -------
Action	ACCEPT

Click **Multiple** next to **Destination Address** to choose two defined virtual IP addresses, as shown in the following figure:



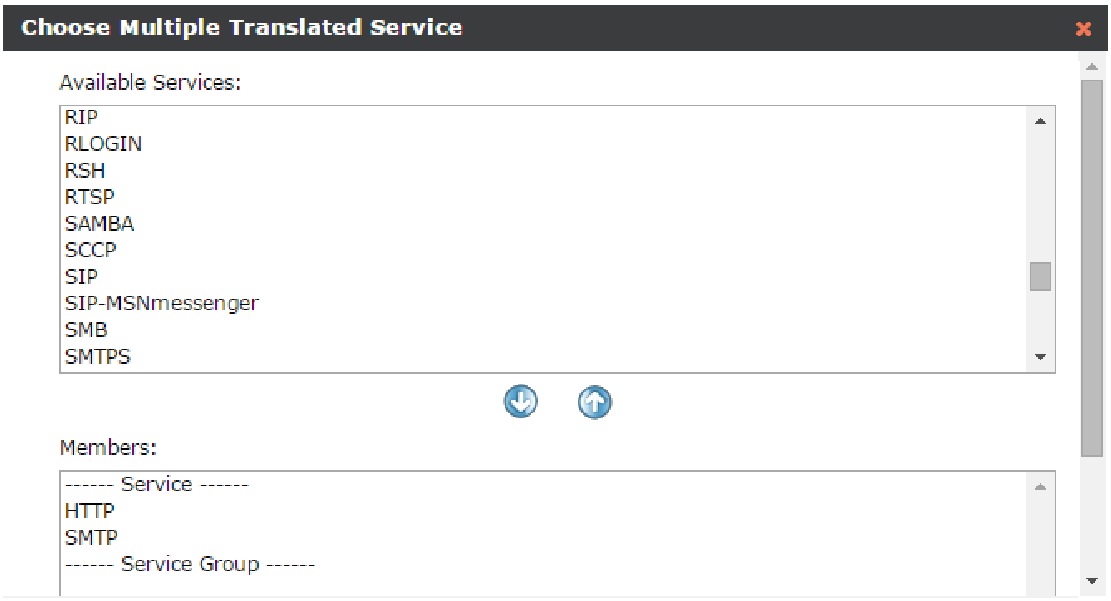
Available Address:

------ Address ------
SSLVPN_TUNNEL_ADDR1
all
lan
------ Virtual IP ------

Members:

------ Address ------
------ Virtual IP ------
smtpserver:25
webserver:80

Click **Multiple** next to **Service** to add HTTP and SMTP services, as shown in the following figure:



Choose Multiple Translated Service

Available Services:

RIP
RLOGIN
RSH
RTSP
SAMBA
SCCP
SIP
SIP-MSNmessenger
SMB
SMTPS

Members:

------ Service ------
HTTP
SMTP
------ Service Group ------

Source Interface/Zone: Choose **wan1**. //If intranet users need to access the Internet by using a virtual IP address, choose **any**.

Source address: Choose **all**.

Destination Interface/Zone: Choose **internal.**

Destination address: Choose **webserver:80 and smtpserver:25.**

Service: Choose **HTTP** and **SMTP**.

If intranet users need to access the Internet by using a virtual IP address, choose one of the following two methods:

1. Set **Source Interface/Zone** of the original policy to **any**.
2. Add one internal-to-internal policy with the **Source Interface/Zone** value of **internal**.

Source Interface/Zone: Choose **internal.**

Source address: Choose **all.**

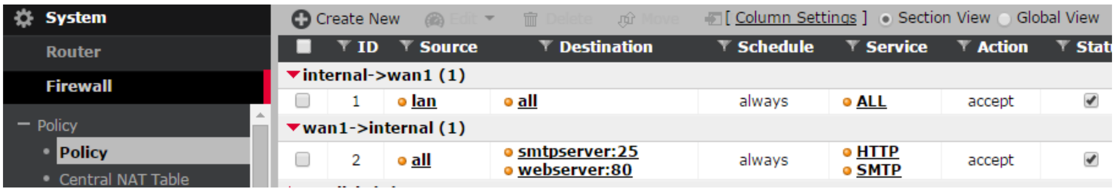
Destination Interface/Zone: Choose **internal.**

Destination address: Choose **webserver:80**and **smtpserver:25.**

Service: Choose **HTTP** and **SMTP**.

Key note: Data traffic of the new NGFW maps the DNAT (virtual IP address), and then the firewall policy. In this case, the extranet port 8080 of the webserver is changed into port 80 after being converted by the DNAT (virtual IP address). Therefore, the HTTP service (port 80) is released by the firewall policy.

The policy configuration is as follows:



□	ID	Source	Destination	Schedule	Service	Action	Stat
internal->wan1 (1)							
□	1	lan	all	always	ALL	accept	☑
wan1->internal (1)							
□	2	all	smtpserver:25 webserver:80	always	HTTP SMTP	accept	☑

Verification

Access http://202.1.1.11 from extranet. To test whether the mapping is valid, temporarily add the ping service.

Do an email test.

3.4.3 Port Mapping for Multiple Lines

Networking Requirements

Respectively map one intranet web server to the public network IP addresses of China Telecom and China Unicom egress ports for Internet access.

Web server address: 192.168.1.2/24; Gateway address: 192.168.1.200

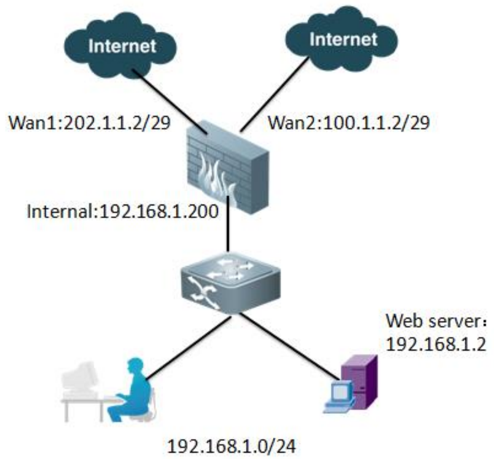
China Telecom egress port address: 202.1.1.2/29; gateway address: 202.1.1.1; public network IP address of the server: 202.1.1.3

China Unicom egress port address: 100.1.1.2/29; gateway: address 100.1.1.1; public network IP address of the server: 100.1.1.3

The PCs in the intranet segment 192.168.1.0/24 need to access the Internet.

Meaning of this case: The new NGFW supports Source In Source Out function of data traffic. The firewall traces sessions. The access from the Telecom port is returned from the Telecom port preferentially, while the access from the Unicom port is returned from the Unicom port preferentially. The precondition is that the routing table of the firewall contains routing entries that can map the returned data traffic. Therefore, you just need to configure default routes to the Telecom port and Unicom port respectively.

Network Topology



Configuration Tips

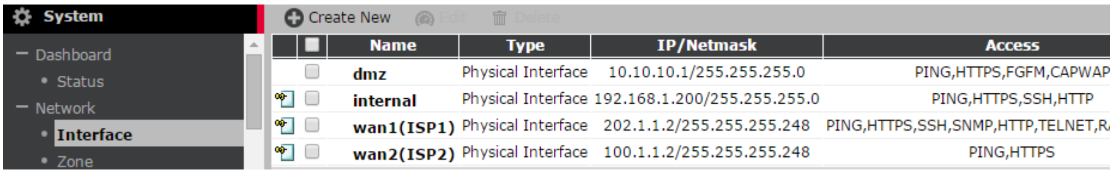
1. Configure the IP addresses of interfaces.
2. Configure a route.
3. Configure the virtual IP address (DNAT).
4. Configure address resources.
5. Configure the policy.

Configuration Steps

1. Configure interface address.

For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under “Internet Access via a Single Line” in “Configuring Routing Mode”.

The following figure shows IP addresses of interfaces:



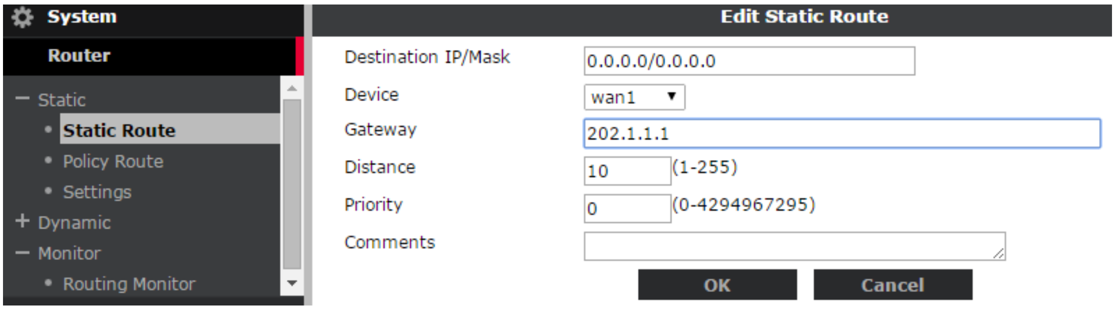
	□	Name	Type	IP/Netmask	Access
	□	dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFM,CAPWAP
	□	internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP
	□	wan1(ISP1)	Physical Interface	202.1.1.2/255.255.255.248	PING,HTTPS,SSH,SNMP,HTTP,TELNET,R
	□	wan2(ISP2)	Physical Interface	100.1.1.2/255.255.255.248	PING,HTTPS

2. Configure a route.

The firewall traces sessions. The access from the Telecom port is returned from the Telecom port preferentially, while the access from the Unicom port is returned from the Unicom port preferentially. The precondition is that the firewall of the firewall contains routing entries that can map the returned data traffic. Therefore, you just need to configure default routes to the Telecom port and Unicom port respectively.

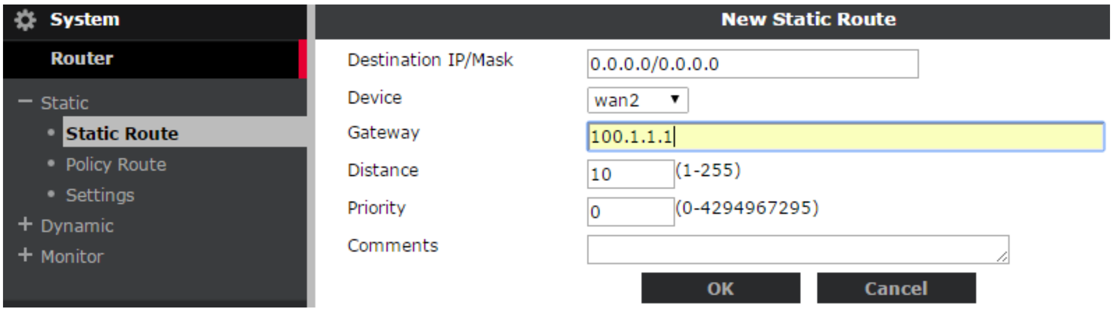
The default route to Telecom port:

The default route to Unicom port:



Edit Static Route

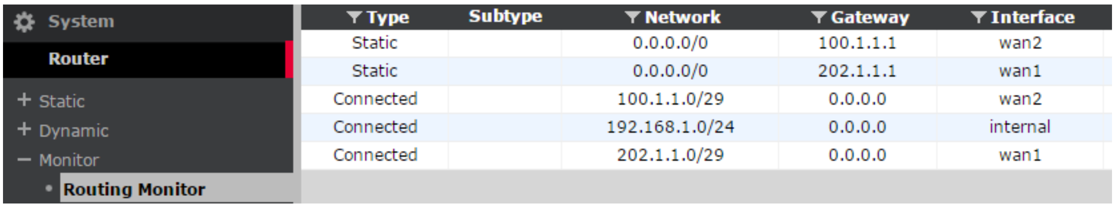
Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan1
Gateway	202.1.1.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	



New Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan2
Gateway	100.1.1.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

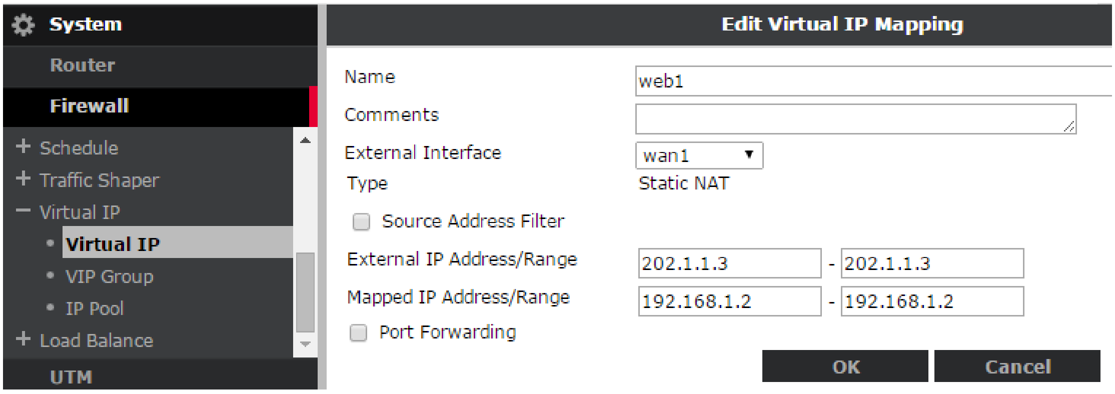
Check the current routes, as shown in the following figure:



Type	Subtype	Network	Gateway	Interface
Static		0.0.0.0/0	100.1.1.1	wan2
Static		0.0.0.0/0	202.1.1.1	wan1
Connected		100.1.1.0/29	0.0.0.0	wan2
Connected		192.168.1.0/24	0.0.0.0	internal
Connected		202.1.1.0/29	0.0.0.0	wan1

3. **Configure the virtual IP address.**

Set **Name** to **web1**, which is used for the IP address mapping of the Telecom interface, as shown in the following figure:



Edit Virtual IP Mapping

Name: web1

Comments:

External Interface: wan1

Type: Static NAT

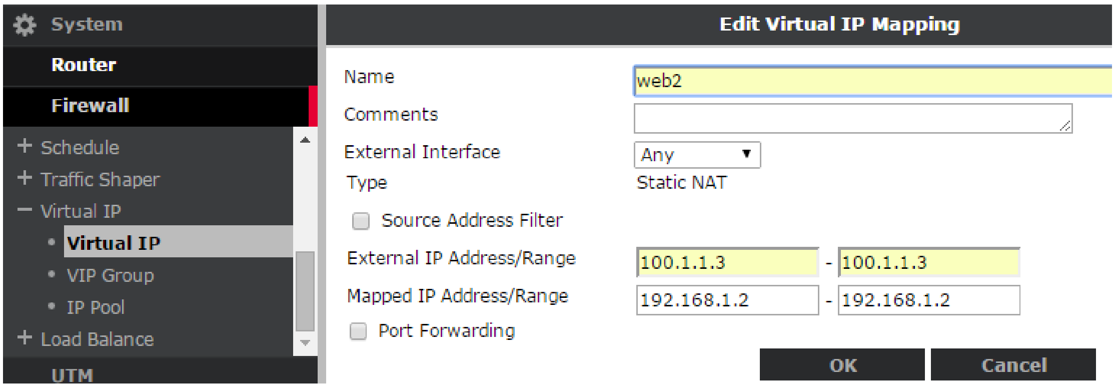
□ Source Address Filter

External IP Address/Range: 202.1.1.3 - 202.1.1.3

Mapped IP Address/Range: 192.168.1.2 - 192.168.1.2

□ Port Forwarding

Set **Name** to **web2**, which is used for the IP address mapping of the Unicom interface, as shown in the following figure:



Edit Virtual IP Mapping

Name: web2

Comments:

External Interface: Any

Type: Static NAT

□ Source Address Filter

External IP Address/Range: 100.1.1.3 - 100.1.1.3

Mapped IP Address/Range: 192.168.1.2 - 192.168.1.2

□ Port Forwarding

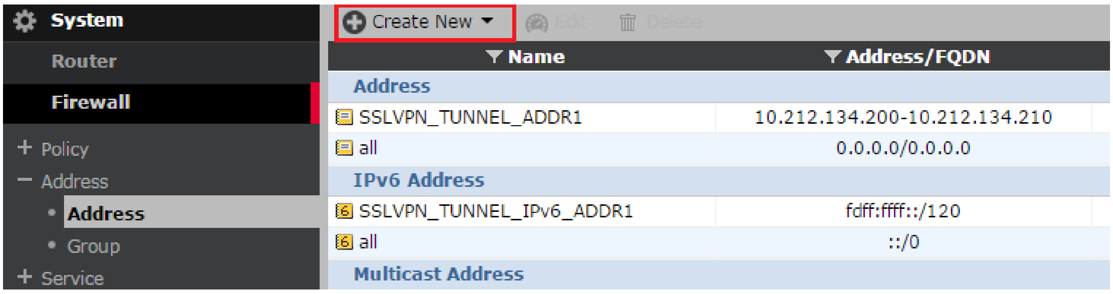
Values of **External IP Address/Range** are mapped to the values of **Mapped IP Address/Range** correspondingly. Enter both the start and end IP addresses of the external IP address range. You just need to Enter the start mapped IP address and the system automatically enters the end IP address.

Take the IP address range from 202.1.1.3 to 202.1.1.10 as an example. The start IP address for internal mapping is 192.168.1.2 and the end IP address must be 192.168.1.9 (which is filled in by the system automatically). The IP addresses within two ranges are mapped correspondingly.

For example, the IP address 202.1.1.3 is mapped to 192.168.1.2, while the IP address 202.1.14 is mapped to 192.168.1.3, and so on.

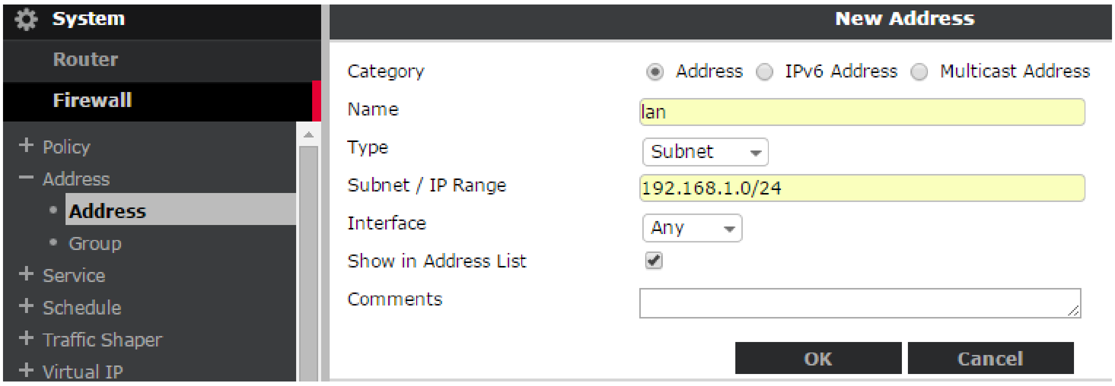
4. Configure address resources.

Choose **Firewall**>**Address**>**Address**, and then click **Create New**, as shown in the following figure:



Name	Address/FQDN
Address	
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210
all	0.0.0.0/0.0.0.0
IPv6 Address	
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120
all	::/0
Multicast Address	

Set **Name** to **lan**. Choose **Subnet** from **Type**. Set **Subnet/IP Range** to **192.168.1.0/24**. Click **OK**. See the following figure:

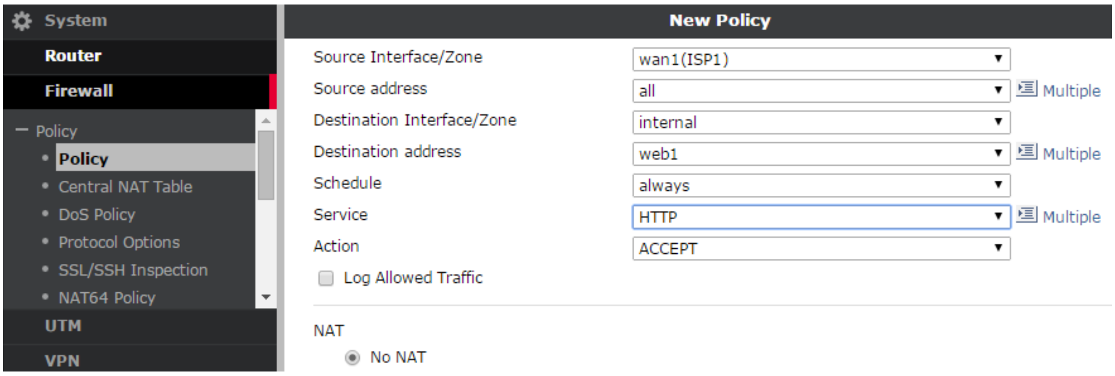


Category	● Address ○ IPv6 Address ○ Multicast Address
Name	lan
Type	Subnet
Subnet / IP Range	192.168.1.0/24
Interface	Any
Show in Address List	☑
Comments	

5. Configure the policy.

You need to configure the following four policies:

a) Configure the virtual IP address policy from wan1 interface to internal interface, as shown in the following figure:



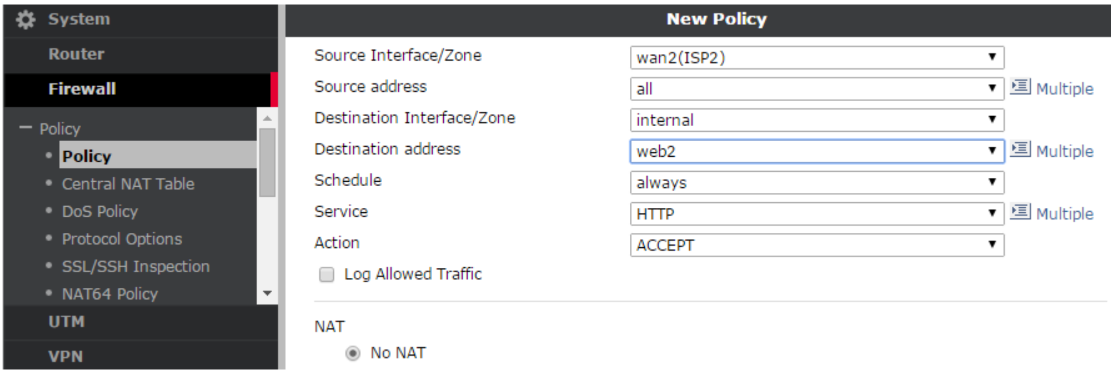
Source Interface/Zone	wan1(ISP1)
Source address	all
Destination Interface/Zone	internal
Destination address	web1
Schedule	always
Service	HTTP
Action	ACCEPT

□ Log Allowed Traffic

NAT

● No NAT

b) Configure the virtual IP address policy from wan2 interface to internal interface, as shown in the following figure:



New Policy

Source Interface/Zone: wan2(ISP2)

Source address: all

Destination Interface/Zone: internal

Destination address: web2

Schedule: always

Service: HTTP

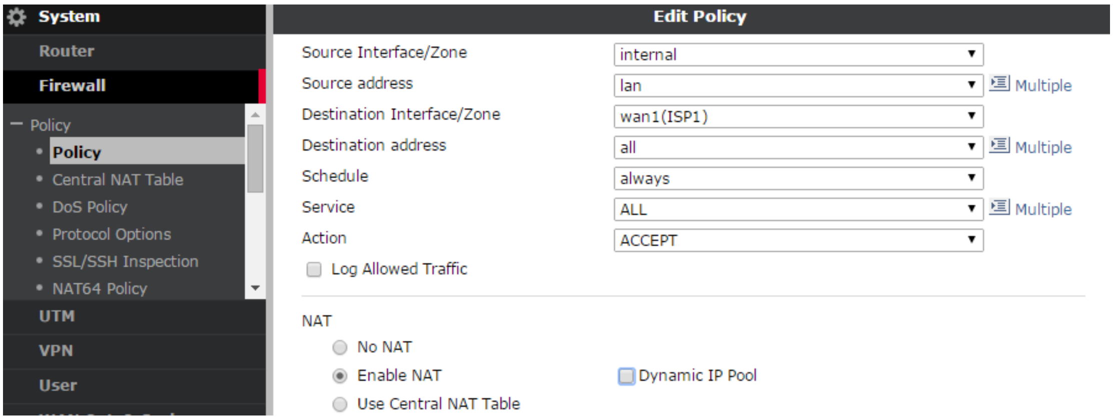
Action: ACCEPT

□ Log Allowed Traffic

NAT

● No NAT

c) Configure the policy from internal interface to wan1 interface to allow the PC with an internal IP address to access the Internet through wan1 interface, as shown in the following figure:



Edit Policy

Source Interface/Zone: internal

Source address: lan

Destination Interface/Zone: wan1(ISP1)

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

□ Log Allowed Traffic

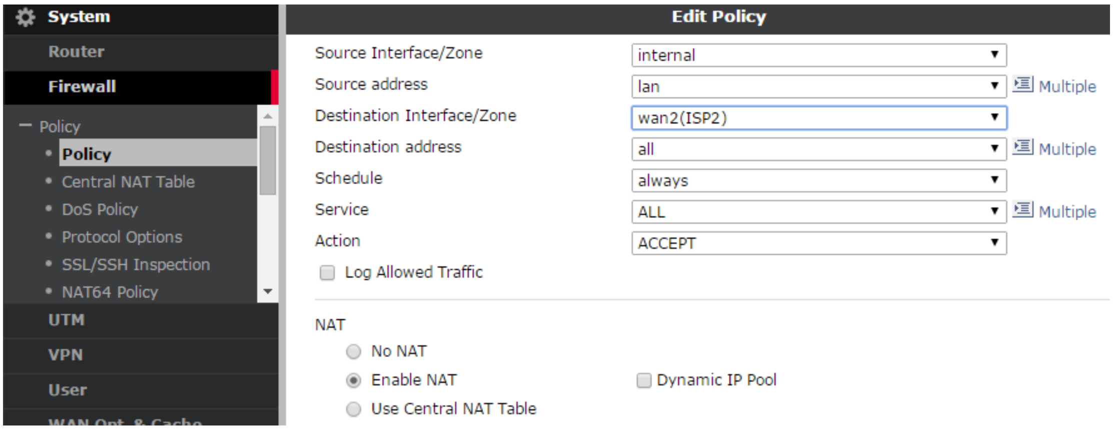
NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

d) Configure the policy from internal interface to wan2 interface to allow the PC with an internal IP address to access the Internet through wan2 interface, as shown in the following figure:



Edit Policy

Source Interface/Zone: internal

Source address: lan

Destination Interface/Zone: wan2(ISP2)

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Verification

Access port 80 at the IP address202.1.1.3 and 100.1.1.3 through two interfaces respectively.

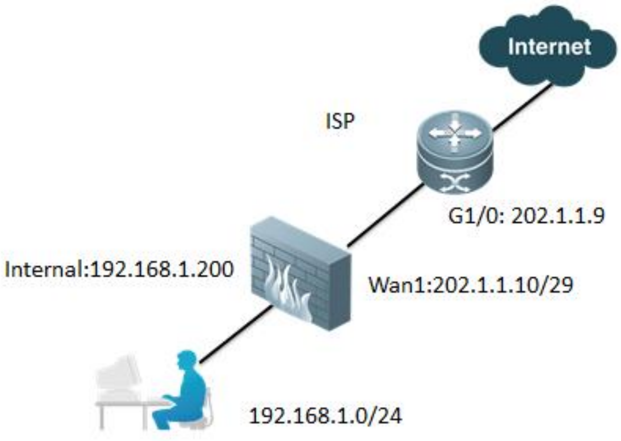
3.5 Configuring Route

3.5.1 Static Routing

Static Routing

Static routing is a routing entry manually added on the firewall by the system administrator according to the network structure. For the firewall, static routing is the most basic manner and is also the most common route configuration.

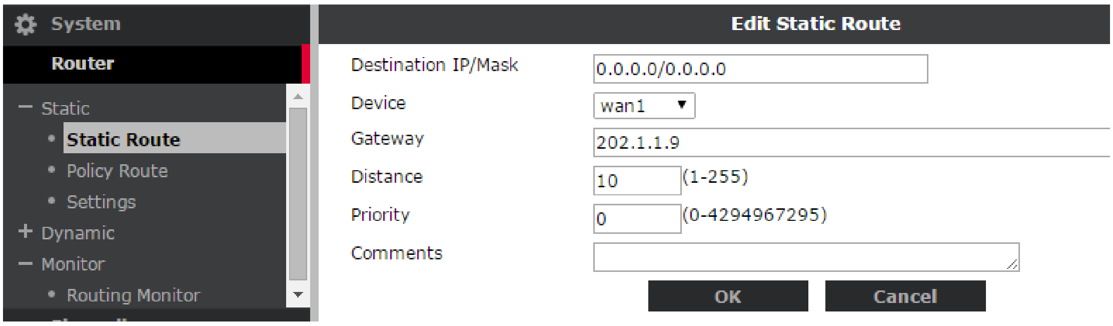
Network Topology



The IP address of wan1 interface of the firewall is 202.1.1.10, while the IP address of G1/0 interface of the peer ISP router is 202.1.1.9.

Configuration Method

Choose **Router**>**Static**>**Static Route**, and then click **Create New**, as shown in the following figure:



Edit Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan1 ▼
Gateway	202.1.1.9
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Destination IP/Mask: Keep the default value **0.0.0.0/0.0.0.0**.

Device: Choose **wan1**, which is related to this route. It must be set correctly. Otherwise, the route cannot work.

Gateway: The IP address of the next hop, that is, the IP address of the peer device corresponding to wan1 interface.

Distance: The default value is **10**. For the same routing entry, the entry with the shorter distance will be put into the routing table. If the distance is the same, both of them will be put into the routing table.

Priority: The default value is 0. For the two routes with the same distance, the firewall chooses the route with a lower priority preferentially.

Configuration Command

1. Configure the default route

```
RG-WALL # config router static
 RG-WALL (static) # edit 1
 RG-WALL (1) # set gateway 202.1.1.9      //This entry does not define the dst destination
network. Therefore, the default value is 0.0.0.0/0.0.0.0.
 RG-WALL (1) # set device wan1
 RG-WALL (1) # next
```

2. Configure the static routing.

```
  RG-WALL # config router static
  RG-WALL (static) # edit 2
  RG-WALL (2) # set dst 1.24.0.0 255.248.0.0
  RG-WALL (2) # set gateway 202.1.1.5
  RG-WALL (2) # set device wan2
  RG-WALL (2) # next
```

Verification

Check the routing table on the graphical page. Choose **Router**>**Monitor**>**Routing Monitor** or run the **get router info routing-table static** command to check whether the route takes effect.

Run **ping 202.1.1.9** to check the link.

3.5.2 Policy-Based Routing

Policy-Based Routing

Both static and dynamic routing are destination routing, which selects a route according to the destination address.

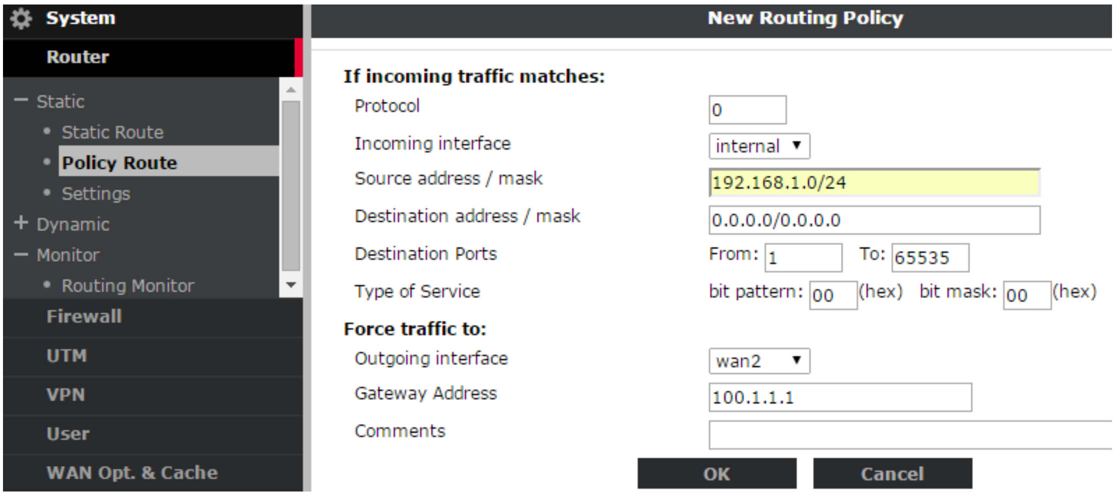
The policy-based routing selects a route according to the original address, protocol type, flow control label, or destination address.

The policy-based routing priority is higher than the static routing priority. The policy-based routing is implemented preferentially.

Application example

Scenario: As described in section “Configuring Internet Access via Dual Lines of Different Carriers” under section “Internet Access via Multiple Links” in “Configuring Routing Mode”, force the PC with IP address 192.168.1.0/29 to access the Internet from wan2 interface.

Choose **Router**>**Static**>**Policy Route**, and then click **Create New**, as shown in the following figure:



New Routing Policy

If incoming traffic matches:

Protocol	0
Incoming interface	internal
Source address / mask	192.168.1.0/24
Destination address / mask	0.0.0.0/0.0.0.0
Destination Ports	From: 1 To: 65535
Type of Service	bit pattern: 00 (hex) bit mask: 00 (hex)

Force traffic to:

Outgoing interface	wan2
Gateway Address	100.1.1.1
Comments	

As defined by this policy-based route, all the data packets from the internal interface with source address 192.168.1.0 255.255.255.248 and destination address 0.0.0.0 0.0.0.0 will be forcibly forwarded by wan2 interface. The gateway address of the next hop is 100.1.1.1.

On the **New Routing Policy** page, the options are as follows:

Protocol: It indicates the protocol type. The value **0** indicates any protocol. You can specify 6 for TCP, 17 for UDP, or 132 for SCTP.

Incoming interface: It indicates the interface through which traffic enters.

Source address/mask: It indicates the source address of the data packet.

Source address/mask: It indicates the source address of the data packet.

Destination Ports: By default, it indicates all the ports, from port 1 to port 65536.

Force traffic to:

Outgoing interface: It indicates the interface through which data is forwarded.

Gateway Address: It indicates the gateway address.

3.5.3 RIP

Application Scenario

If there are many network routing devices and the number does not exceed 16, it is recommended to configure RIP on the NGFW so that the NGFW can dynamically learn the routing to other networks and the routes can automatically age and update.

When the number of routing devices exceeds 16, it is recommended to configure OSPF, because the OSPF enables faster route learning and updating and the OSPF is more suitable for the network with more than 16 routing devices.

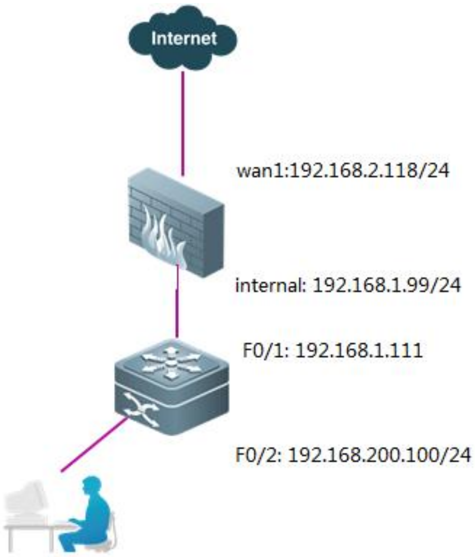
If there are few routing devices, it is recommended to configure the static route. That’s because the static route is easily maintained and does not raise a high requirement for the routers. All the routers support static routes. In general, the low end routers do not support RIP.

Networking Requirements

As shown in the figure, the L3 switch in the intranet and the egress NGFW mutually advertise routes through the dynamic route RIP to enable intranet users to access the Internet.

On the NGFW, manually configure the default route, redistribute the default route into RIP. The L3 switch and NGFW mutually learn routes through RIP to enable intranet users to access the Internet.

Network Topology



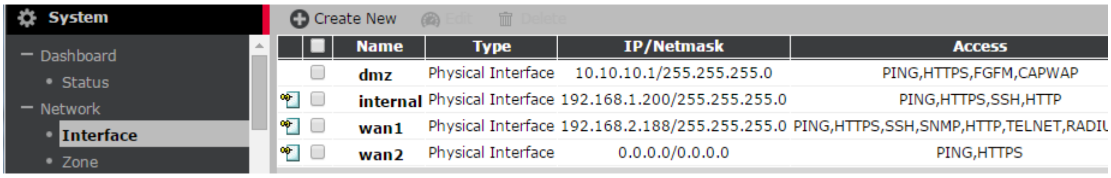
Configuration Tips

1. Configure interface address.
2. Configure the firewall.
3. Configure the router.

Configuration Steps

1. Configure interface address.

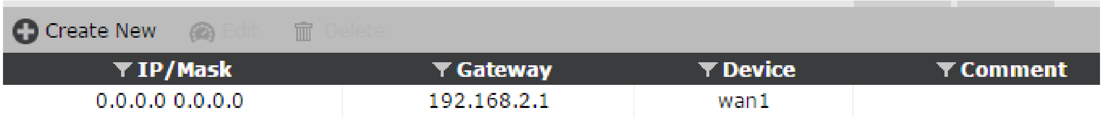
For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under section “Internet Access via a Single Line” in “Configuring Routing Mode”. The configuration is displayed as shown in the following figure:



	□	Name	Type	IP/Netmask	Access
	□	dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFM,CAPWAP
	□	internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP
	□	wan1	Physical Interface	192.168.2.188/255.255.255.0	PING,HTTPS,SSH,SNMP,HTTP,TELNET,RADIU
	□	wan2	Physical Interface	0.0.0.0/0.0.0.0	PING,HTTPS

2. Configure a default route.

For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under section “Internet Access via a Single Line” in “Configuring Routing Mode”. The configuration is displayed as shown in the following figure:

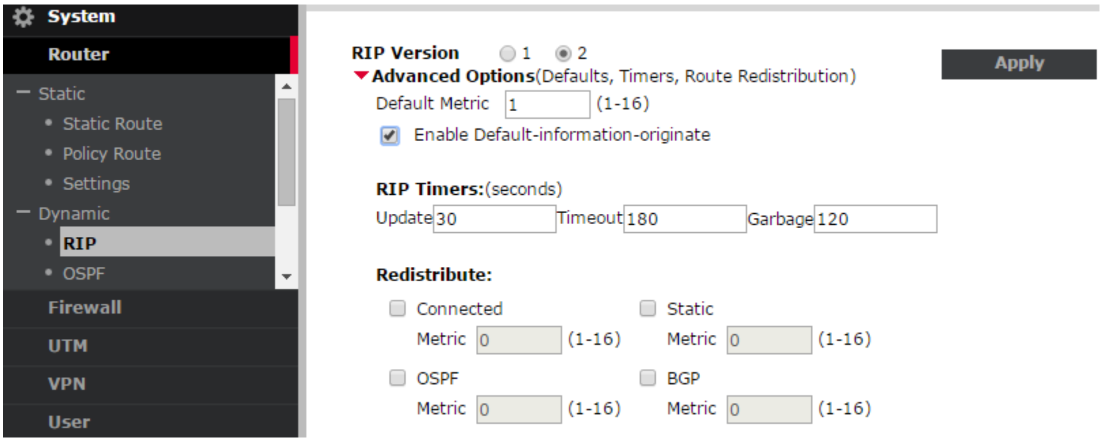


IP/Mask	Gateway	Device	Comment
0.0.0.0 0.0.0.0	192.168.2.1	wan1	

3. Configure RIP.

Choose **Router > Dynamic > RIP.**

a) Configure basic information, as shown in the following figure:



RIP Version ○ 1 ● 2

Advanced Options(Defaults, Timers, Route Redistribution)

Default Metric 1 (1-16)

☑ Enable Default-information-originate

RIP Timers:(seconds)

Update 30 Timeout 180 Garbage 120

Redistribute:

□ Connected Metric 0 (1-16) □ Static Metric 0 (1-16)

□ OSPF Metric 0 (1-16) □ BGP Metric 0 (1-16)

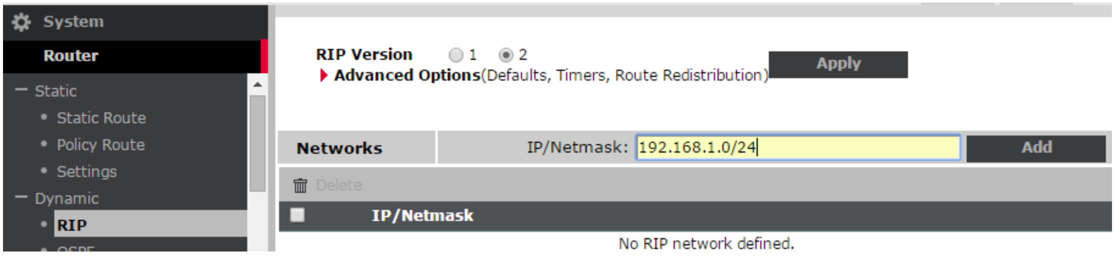
RIP Version: Choose 2.

Enable Default-information-originate: Tick this item to send the default route to the neighbor (router).

Redistribute: It determines whether to distribute other protocol routes.

b) Add the RIP network.

Click Create New. Set IP/Netmask to 192.168.1.0/255.255.255.0, and then click Add, as shown in the following figure:



RIP Version ○ 1 ● 2

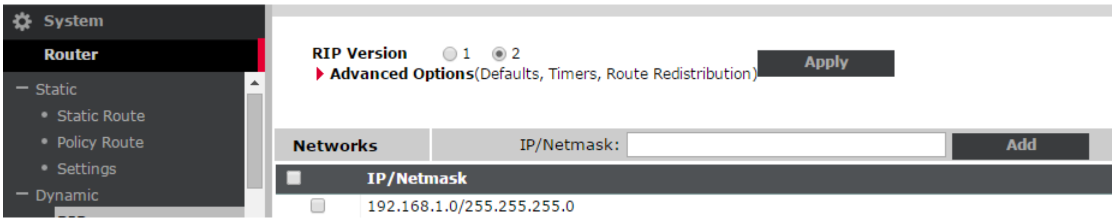
Advanced Options(Defaults, Timers, Route Redistribution)

Networks IP/Netmask: 192.168.1.0/24

□ **IP/Netmask**

No RIP network defined.

After the network segment is added, the configuration is displayed as shown in the following figure:



RIP Version ○ 1 ● 2

Advanced Options(Defaults, Timers, Route Redistribution)

Networks IP/Netmask:

□ **IP/Netmask**

□ 192.168.1.0/255.255.255.0

4. Configure the router.

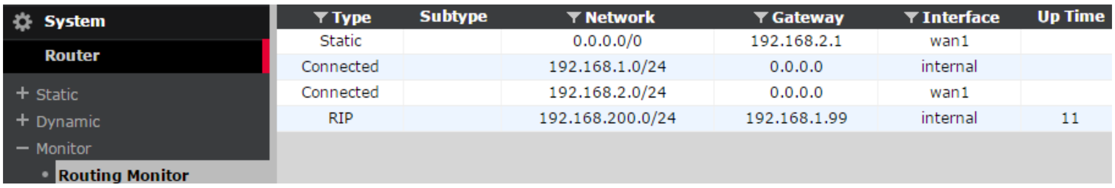
```
interface FastEthernet 0/1
    ip address 192.168.1.111 255.255.255.0
interface FastEthernet 0/2
```

```
    ip address 192.168.200.100 255.255.255.0
    Configure RIP as follows:
    router rip
    version 2
    network 192.168.1.0
    network 192.168.10.0
    no auto-summary
```

Verification

Check the current routes.

Choose **Router**>**Monitor**>**Routing Monitor**, as shown in the following figure:



Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	192.168.2.1	wan1	
Connected		192.168.1.0/24	0.0.0.0	internal	
Connected		192.168.2.0/24	0.0.0.0	wan1	
RIP		192.168.200.0/24	192.168.1.99	internal	11

Run the following command to display the current routes:

```
RG-WALL # get router  info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
S*      0.0.0.0/0 [10/0] via 192.168.2.1, wan1, [0/50]
C       192.168.1.0/24 is directly connected, internal
C       192.168.2.0/24 is directly connected, wan1
R       192.168.200.0/24 [120/2] via 192.168.1.99, internal, 00:00:01
```

3.5.4 OSPF

Application Scenario

When the number of routing devices exceeds 16, it is recommended to configure OSPF, because the OSPF enables faster route learning and updating and the OSPF is more suitable for the network with more than 16 routing devices.

If there are many network routing devices and the number does not exceed 16, it is recommended to configure the RIP on the NGFW so that the NGFW can dynamically learn the routing to other networks and the routes can automatically age and update.

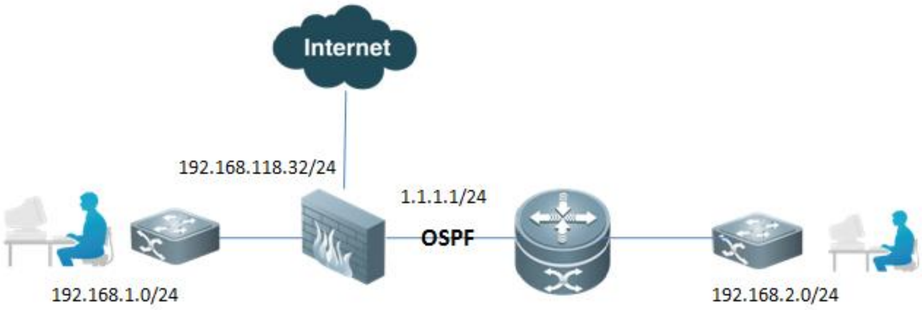
If there are few routing devices, it is recommended to configure the static route. That’s because the static route is easily maintained and does not raise a high requirement for the routers. All the routers support static routes. In general, the low end routers do not support RIP.

Networking Requirements

As shown in the figure, the L3 switch in the intranet and the egress NGFW mutually advertise routes through the dynamic route OSPF to enable intranet users to access the Internet.

On the NGFW, manually configure the default route, redistribute the default route into OSPF. The L3 switch and NGFW mutually learn routes through OSPF to enable intranet users to access the Internet.

Network Topology



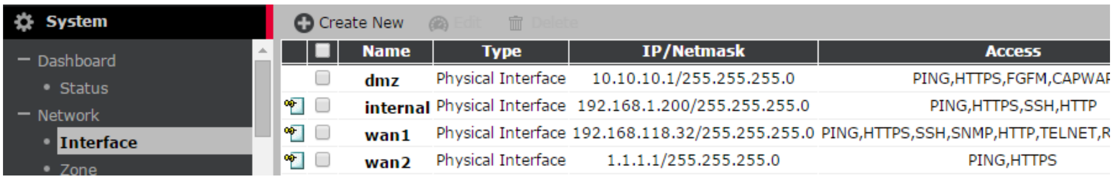
Configuration Tips

1. Configure the IP addresses of interfaces.
2. Configure a default route.
3. Configure OSPF.
   - Configure the router ID.
   - Distribute the default route.
   - Redistribute the default route.
   - Create OSPF areas.
   - Add the OSPF network.
   - Add the interface.
4. Configure the peer router.

Configuration Steps

1. Configure the IP addresses of interfaces.

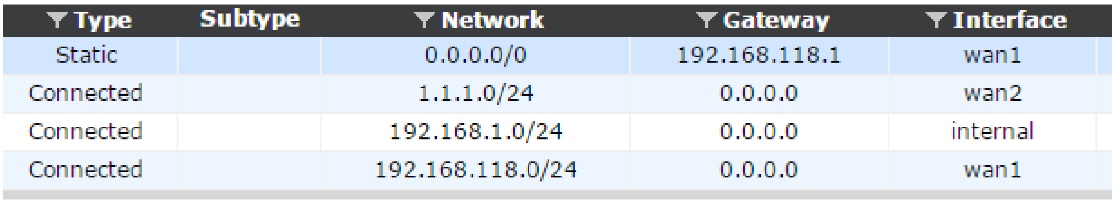
For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under section “Internet Access via a Single Line” in “Configuring Routing Mode”. The configuration is displayed as shown in the following figure:



	□	Name	Type	IP/Netmask	Access
	□	dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFM,CAPWAF
	□	internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP
	□	wan1	Physical Interface	192.168.118.32/255.255.255.0	PING,HTTPS,SSH,SNMP,HTTP,TELNET,R
	□	wan2	Physical Interface	1.1.1.1/255.255.255.0	PING,HTTPS

2. **Configure a default route.**

For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under section “Internet Access via a Single Line” in “Configuring Routing Mode”. The configuration is displayed as shown in the following figure:

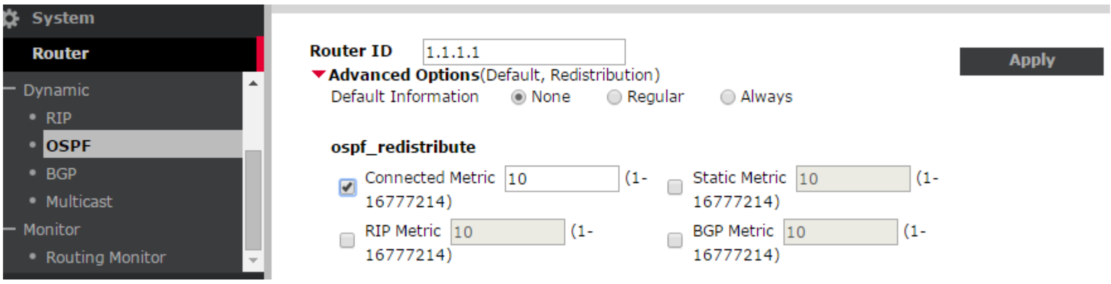


Type	Subtype	Network	Gateway	Interface
Static		0.0.0.0/0	192.168.118.1	wan1
Connected		1.1.1.0/24	0.0.0.0	wan2
Connected		192.168.1.0/24	0.0.0.0	internal
Connected		192.168.118.0/24	0.0.0.0	wan1

3. **Configure OSPF.**

Choose **Router**>**Dynamic**>**OSPF**, as shown in the following figure:

a) Configure basic information, as shown in the following figure:



Router ID 1.1.1.1

Advanced Options(Default, Redistribution)

Default Information ● None ○ Regular ○ Always

ospf_redistribute

☑ Connected Metric 10 (1-16777214) □ Static Metric 10 (1-16777214)

□ RIP Metric 10 (1-16777214) □ BGP Metric 10 (1-16777214)

Set **Router** ID to **1.1.1.1.**

Default Information: Choose **Regular**. The three options are described as follows:

The default route is not distributed.

Regular: If the default route is configured, the system distributes it. If not, the system does not distribute it.

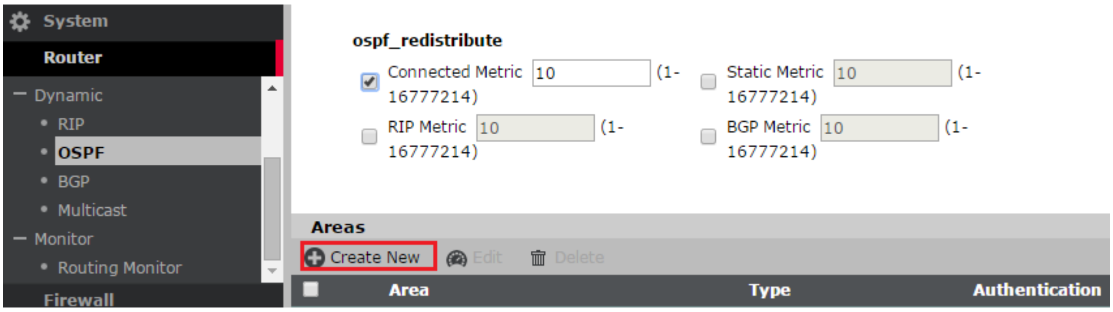
Always: No matter whether the default route is configured, the system distributes a default route.

Ospf_redistribute: Choose **Connected Metric**, which indicates that the routing information at the 192.168.1.0/24 is sent to the OSPF neighbor.

After the above settings are completed, click **Apply** to validate configuration.

b) Create OSPF areas.

Click **Create New**, as shown in the following figure:



ospf_redistribute

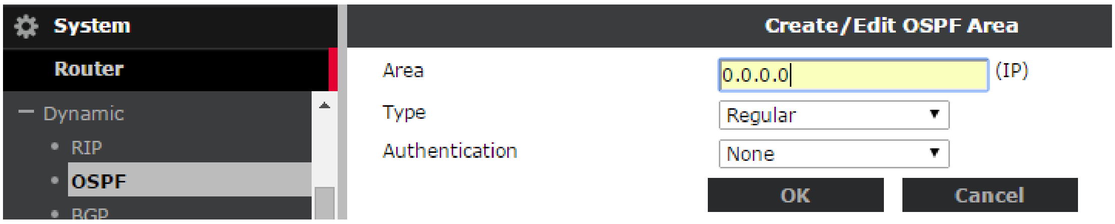
☑ Connected Metric 10 (1-16777214)　□ Static Metric 10 (1-16777214)

□ RIP Metric 10 (1-16777214)　□ BGP Metric 10 (1-16777214)

Areas

□	Area	Type	Authentication

Create root area 0.0.0.0 (area 0), as shown in the following figure:



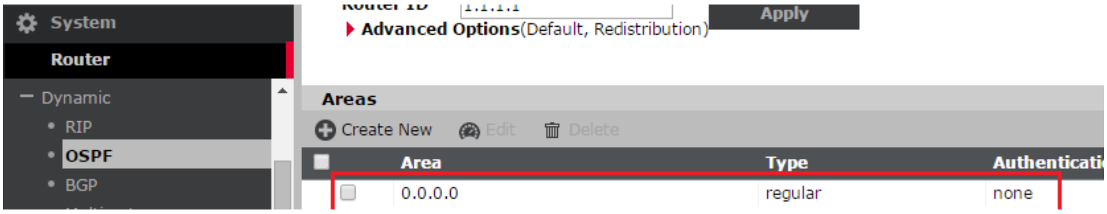
Create/Edit OSPF Area

Area: 0.0.0.0 (IP)

Type: Regular

Authentication: None

The configuration is as follows:



Router ID 1.1.1.1

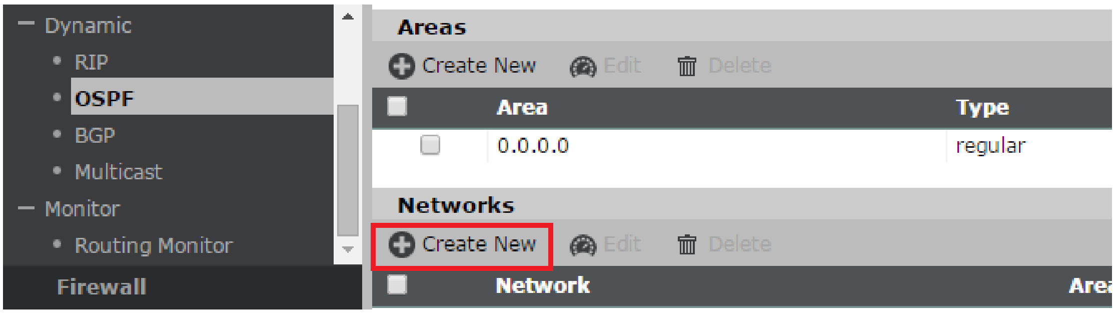
Advanced Options(Default, Redistribution)

Areas

□	Area	Type	Authenticati
□	0.0.0.0	regular	none

c) Add the OSPF network.

Click **Create New**, as shown in the following figure:



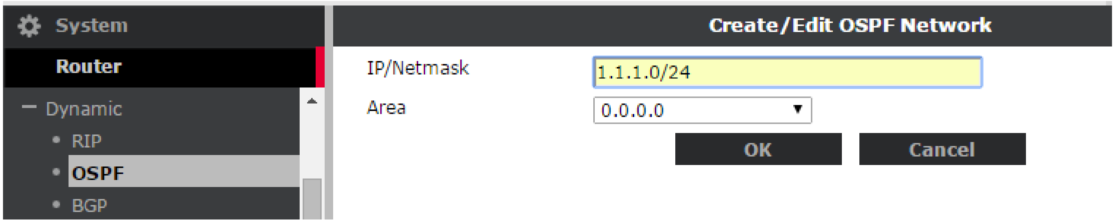
Areas

□	Area	Type
□	0.0.0.0	regular

Networks

□	Network	Are

Add segment 1.1.1.0/24 to the OSPF area 0.0.0.0, as shown in the following figure:



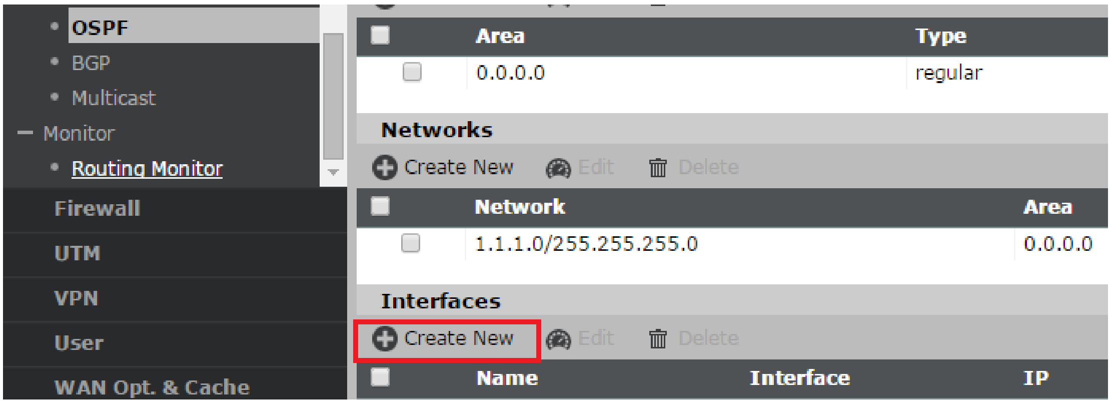
Create/Edit OSPF Network

IP/Netmask: 1.1.1.0/24

Area: 0.0.0.0

d) Add interfaces. (Optional)

Click **Create New**, as shown in the following figure:



□	Area	Type
□	0.0.0.0	regular

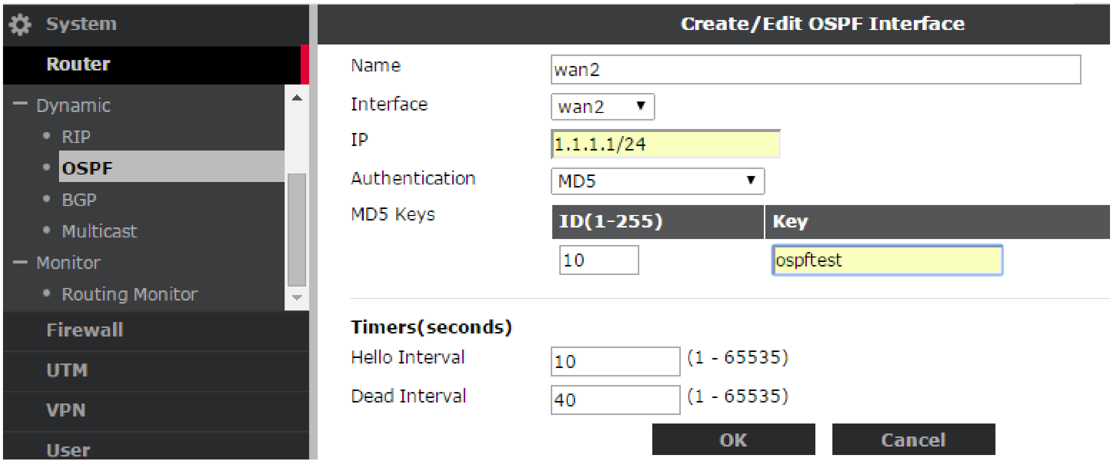
Networks

□	Network	Area
□	1.1.1.0/255.255.255.0	0.0.0.0

Interfaces

□	Name	Interface	IP

You can edit the related parameters of interfaces by using this menu.



Create/Edit OSPF Interface

Name	wan2
Interface	wan2
IP	1.1.1.1/24
Authentication	MD5

MD5 Keys

ID(1-255)	Key
10	ospftest

Timers(seconds)

Hello Interval	10	(1 - 65535)
Dead Interval	40	(1 - 65535)

Name: It is used for identification.

Interface: It indicates the interface to be edited.

IP: It indicates the IP address of the interface.

Authentication: It determines whether to perform OSPF authentication on the interface. The system supports MD5 (MD5 summary), txt (plain text), and none (none).

MD5 keys: Enter key ID and key.

Timers:

Hello Interval: By default, the interval for sending hello packets is 10 seconds, which can be changed as required. In the case of OSPF neighbor negotiation, the value of **Hello Interval** must be the same.

Dead Interval: By default, the value is 40 seconds, which can be changed as required. In the case of OSPF neighbor negotiation, the value of **Dead Interval** must be the same.

4. Configure the switch.

Configure interface address.

```
interface FastEthernet 0/0
ip address 1.1.1.2 255.255.255.0
interface FastEthernet 0/1
ip address 192.168.2.1 255.255.255.0
    Configure OSPF as follows:
    router ospf 10
    network 1.1.1.0 0.0.0.255 area 0
    network 192.168.2.0 0.0.0.255 area 0         //This entry can also be distributed
through direct connection.
```

Verification

```
                  RG-WALL # get router info routing-table all
path=router, objname=info, tablename=(null), size=0
                  Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
                          O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
                          E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
                          * - candidate default
                  S*      0.0.0.0/0 [10/0] via 192.168.118.1, wan1, [0/50]
                  C       1.1.1.0/24 is directly connected, wan2
                  C       192.168.1.0/24 is directly connected, internal
                  O       192.168.2.0/24 [110/11] via 1.1.1.2, wan2, 00:01:49
                  C       192.168.118.0/24 is directly connected, wan1
```

Check the routes of the router:

```
                  Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
                          O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
                          E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
                           * - candidate default

                   O*E2    0.0.0.0/0 [110/10] via 1.1.1.1, wan1, 00:09:34
                   C       1.1.1.0/24 is directly connected, wan1
                   O E2    192.168.1.0/24 [110/10] via 1.1.1.1, wan1, 00:09:34
                   C       192.168.2.0/24 is directly connected, internal
                   O E2    192.168.118.0/24 [110/10] via 1.1.1.1, wan1, 00:09:34
```

3.6 Application Level Gateway (ALG)

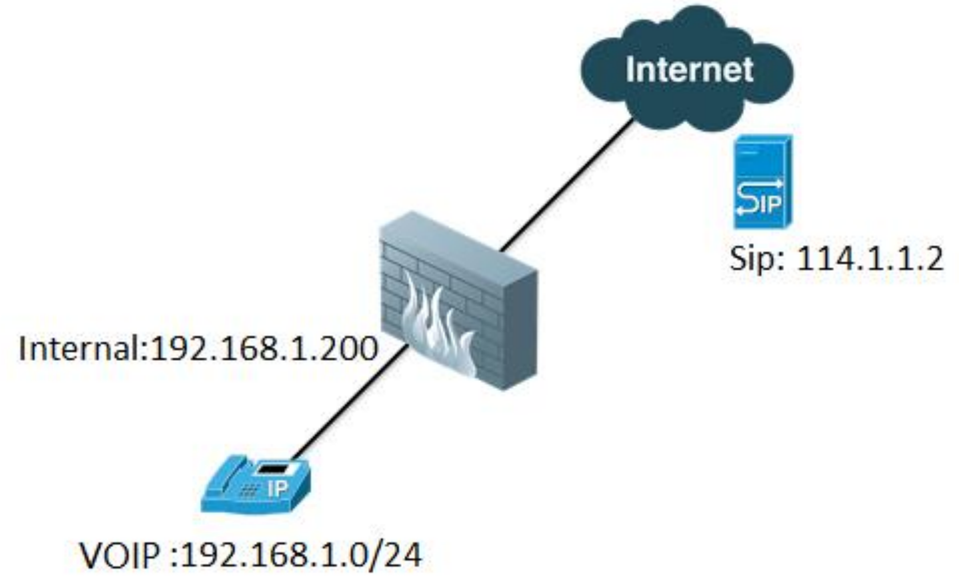
3.6.1 VoIP

I. Networking Requirements

A company uses a voice system based on the Session Initiation Protocol (SIP). The employees use SIP phones in the company. The SIP server is connected to a node outside the firewall.

Because of the particularity of SIP, the firewall should enable SIP ALG to prevent dial-up failure, unidirectional port state, or other problems caused by the firewall policy.

II. Network Topology



III. Configuration Tips

1. Basic configuration for Internet access
2. Configure a VoIP policy.
3. Move policies. (Optional)
4. Configure SIP ports. (Optional)

IV. Configuration Steps

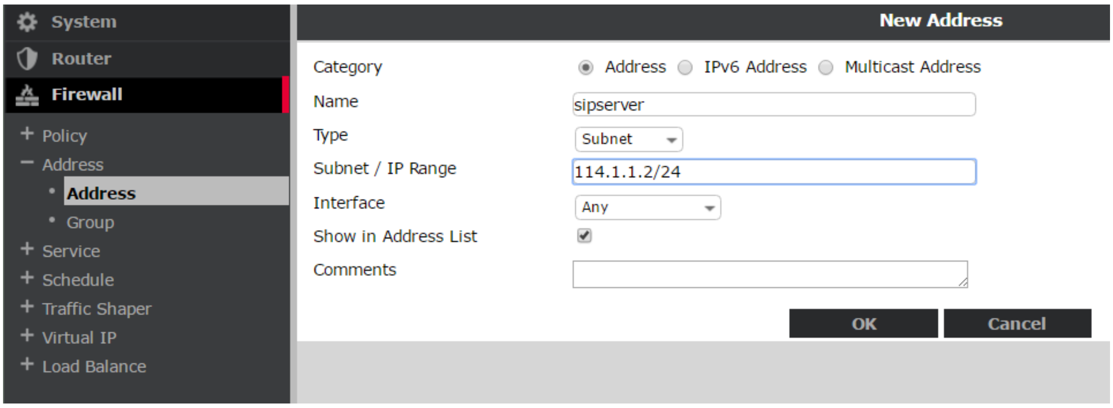
1. Basic configuration for Internet access

See section 1.1 "Internet Access via a Single Line" in Chapter 1 "Typical Functions of Routing Mode".

Configure a VoIP policy.

1) Define the address object.

Choose **Firewall** > **Address** > **Address**.

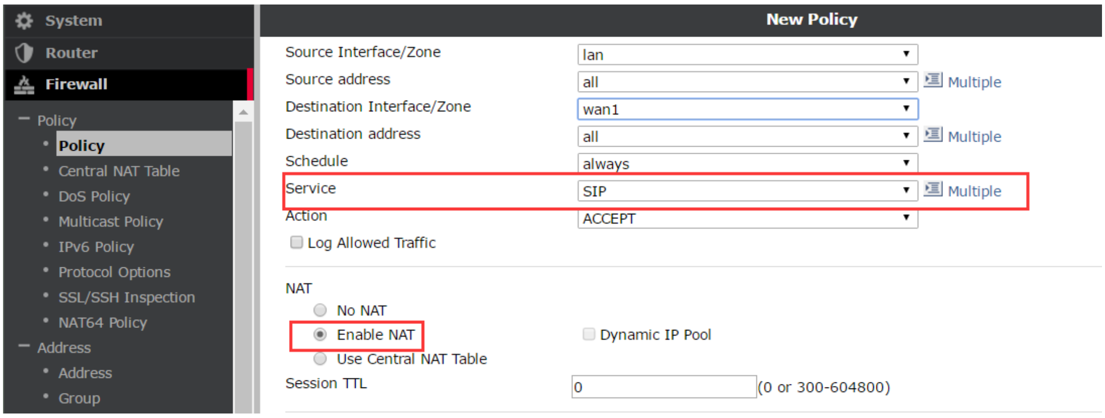


New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	sipserver
Type	Subnet
Subnet / IP Range	114.1.1.2/24
Interface	Any
Show in Address List	☑
Comments	

2) Define a VoIP policy.

Choose **Firewall** > **Policy** > **Policy**.



New Policy

Source Interface/Zone	lan
Source address	all Multiple
Destination Interface/Zone	wan1
Destination address	all Multiple
Schedule	always
Service	SIP Multiple
Action	ACCEPT

□ Log Allowed Traffic

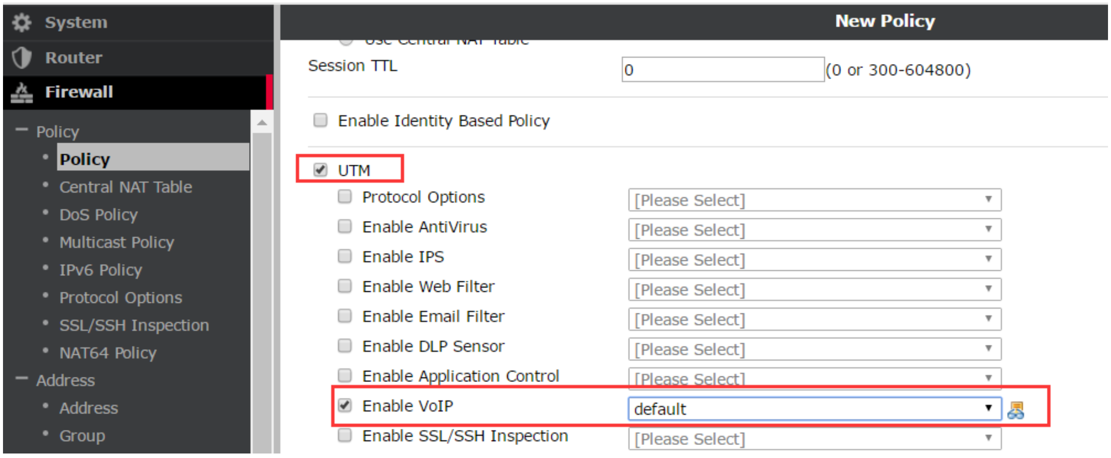
NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Session TTL 0 (0 or 300-604800)



New Policy

Session TTL 0 (0 or 300-604800)

□ Enable Identity Based Policy

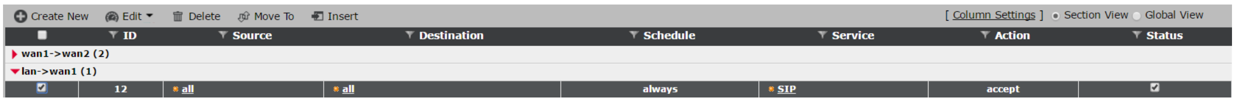
☑ UTM

□ Protocol Options	[Please Select]
□ Enable AntiVirus	[Please Select]
□ Enable IPS	[Please Select]
□ Enable Web Filter	[Please Select]
□ Enable Email Filter	[Please Select]
□ Enable DLP Sensor	[Please Select]
□ Enable Application Control	[Please Select]
☑ Enable VoIP	default
□ Enable SSL/SSH Inspection	[Please Select]

Enable the UTM function, tick **Enable VoIP**, and choose **default**.

Move policies. (Optional)

Move policies to appropriate positions to ensure execution.



□	ID	Source	Destination	Schedule	Service	Action	Status
wan1->wan2 (2)							
lan->wan1 (1)							
☑	12	all	all	always	SIP	accept	☑

Configure SIP ports. (Optional)

In most SIP settings, TCP or UDP port 5060 is used for SIP sessions while port 5061 is used for SIP

SSL sessions. If the SIP network uses other ports for SIP sessions, run the following commands to enable SIP ALG to use other ports of TCP, UDP, or SSL for interception. For example, use TCP port 5064, UDP port 5065, and SSL port 5066 instead.

```
RG-WALL#config system settings
RG-WALL (settings) #set sip-tcp-port 5064
RG-WALL (settings) #set sip-udp-port 5065
RG-WALL (settings) #set sip-ssl-port 5066
RG-WALL (settings) #end
```

SIP ALG can also be set to use two different TCP ports and two different UDP ports for interception of SIP sessions. For example, if ports 5060 and 5064 are used to receive SIP TCP traffic while ports 5061 and 5065 are used to receive SIP UDP traffic, run the following commands to use all these ports to receive SIP traffic.

```
RG-WALL#config system settings
RG-WALL (settings) #set sip-tcp-port 5060 5064
RG-WALL (settings) #set sip-udp-port 5061 5065
RG-WALL (settings) #end
```

V. Verification

Use a SIP phone for testing.

VI. Notes

Q: Why to enable the UTM function of VoIP?

A: Session Helper of the system supports some functions of VoIP ALG but provides simple functions and applies to simple scenarios. As VoIP scenarios become more complicated, VoIP profiles are used now.

VoIP ALG feature can be found on UTM function, which provides a well-developed ALG function and safety protection for VoIP.

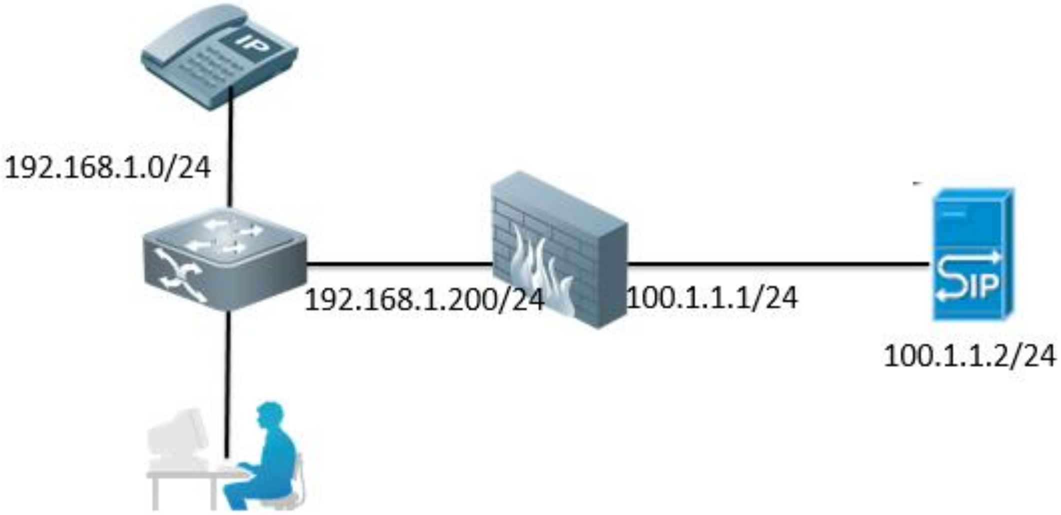
3.6.2 VoIP Destination Address Mapping

I. Networking Requirements

A company uses a SIP-based voice system. The employees use SIP phones in the company. SIP server 100.1.1.2 is connected to a node in the firewall server area. The SIP server needs to be mapped to the intranet 192.168.1.2.

Because of the particularity of SIP, the firewall should enable SIP ALG to prevent dial-up failure, unidirectional port state, or other problems caused by the firewall policy.

II. Network Topology



III. Configuration Tips

1. Basic configuration for Internet access
2. Configure a VoIP policy.
3. Move policies. (Optional)
4. Configure SIP ports. (Optional)

IV. Configuration Steps

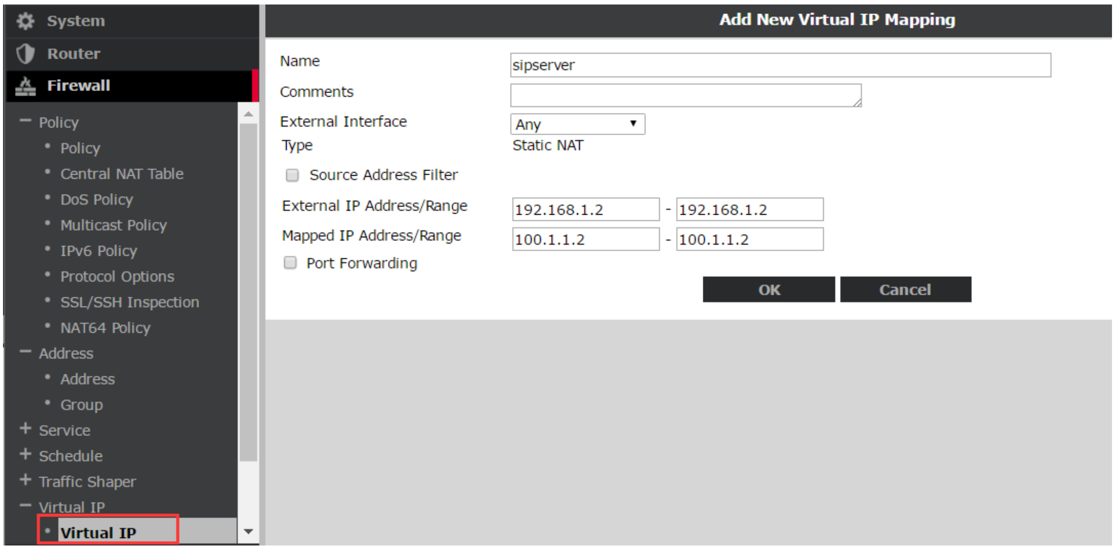
1. Basic configuration for Internet access

See section 1.1 "Internet Access via a Single Line" in Chapter 1 "Typical Functions of Routing Mode"

Configure a VoIP policy.

1) Define a virtual IP address.

Choose **Firewall** > **Virtual IP** > **Virtual IP**.

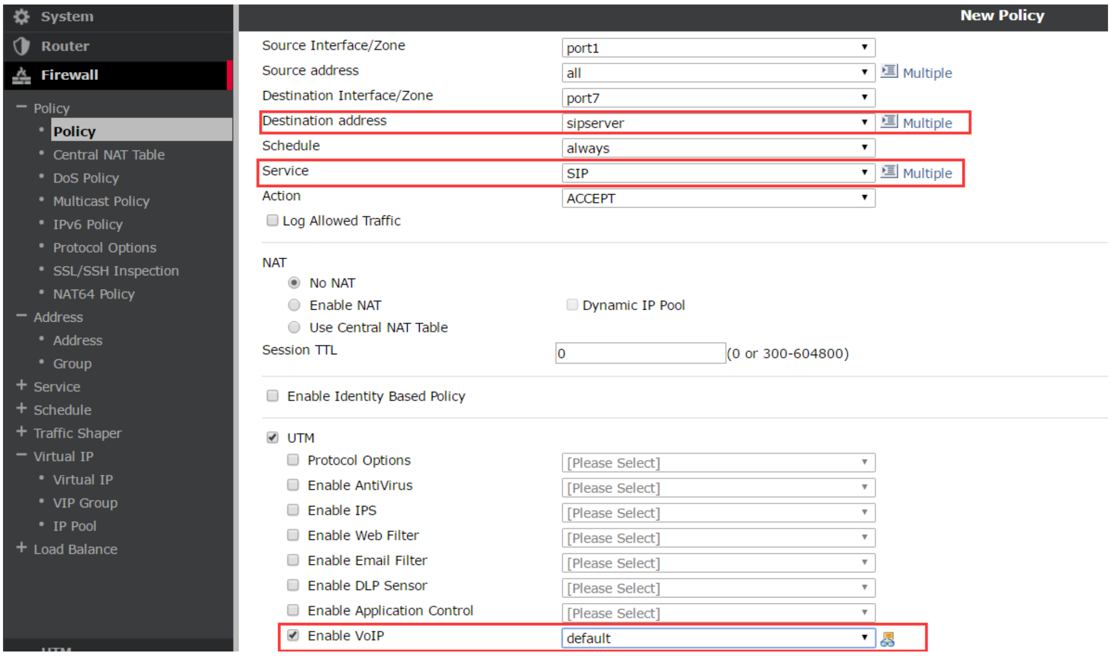


Add New Virtual IP Mapping

Name	sipserver
Comments	
External Interface	Any
Type	Static NAT
□ Source Address Filter	
External IP Address/Range	192.168.1.2 - 192.168.1.2
Mapped IP Address/Range	100.1.1.2 - 100.1.1.2
□ Port Forwarding	

2) Define a VoIP policy.

Choose **Firewall** > **Policy** > **Policy**.



Source Interface/Zone: port1

Source address: all — Multiple

Destination Interface/Zone: port7

Destination address: sipserver — Multiple

Schedule: always

Service: SIP — Multiple

Action: ACCEPT

□ Log Allowed Traffic

NAT

● No NAT

○ Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Session TTL: 0 (0 or 300-604800)

□ Enable Identity Based Policy

☑ UTM

□ Protocol Options [Please Select]

□ Enable AntiVirus [Please Select]

□ Enable IPS [Please Select]

□ Enable Web Filter [Please Select]

□ Enable Email Filter [Please Select]

□ Enable DLP Sensor [Please Select]

□ Enable Application Control [Please Select]

☑ Enable VoIP default

Enable the UTM function, tick **Enable VoIP**, and choose **default**.

3) Configure SIP ports. (Optional)

In most SIP settings, TCP or UDP port 5060 is used for SIP sessions while port 5061 is used for SIP SSL sessions. If the SIP network uses other ports for SIP sessions, run the following commands to enable SIP ALG to use other ports of TCP, UDP, or SSL for interception. For example, use TCP port 5064, UDP port 5065, and SSL port 5066 instead.

```
RG-WALL#config system settings
RG-WALL (settings) #set sip-tcp-port 5064
RG-WALL (settings) #set sip-udp-port 5065
RG-WALL (settings) #set sip-ssl-port 5066
RG-WALL (settings) #end
```

SIP ALG can also be set to use two different TCP ports and two different UDP ports for interception of SIP sessions. For example, if ports 5060 and 5064 are used to receive SIP TCP traffic while ports 5061 and 5065 are used to receive SIP UDP traffic, run the following commands to use all these ports to receive SIP traffic.

```
RG-WALL#config system settings
RG-WALL (settings) #set sip-tcp-port 5060 5064
RG-WALL (settings) #set sip-udp-port 5061 5065
RG-WALL (settings) #end
```

V. Verification

Use a SIP phone for testing.

3.7 Configuring VPN

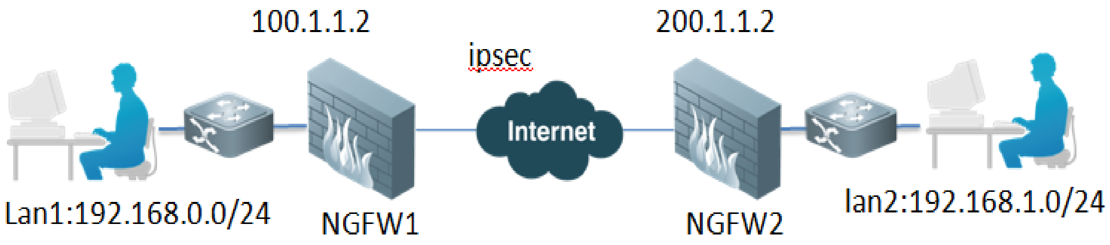
3.7.1 IPSec VPN (Point-to-Point)

3.7.1.1 Interface Mode

Networking Requirements

As shown in the figure, two LANs are connected via VPN, so as to implement the communication between two network segments (including 192.168.0.0/24 and 192.168.1.0/24).

Network Topology



Configuration Tips

1. Configure NGFW1

1. Perform basic configurations of Internet access
2. Configure IKE Phase 1
3. Configure IKE Phase 2
4. Configure the routes
5. Configure the policies

2. Configure NGFW2

1. Perform basic configurations of Internet access
2. Configure IKE Phase 1
3. Configure IKE Phase 2
4. Configure the routes
5. Configure the policies

To delete Phases 1 and 2 of IPSec VPN, you need to delete the invoked route or firewall security policy first.

Configuration Steps

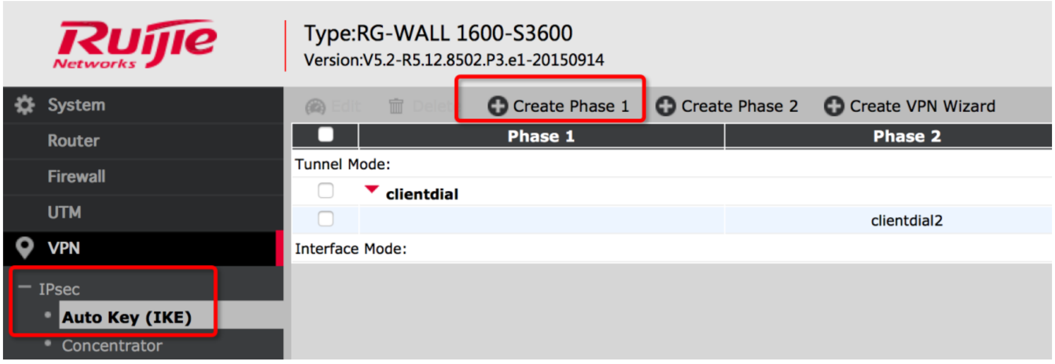
1. Configure NGFW1

1. **Perform basic configurations of Internet access**

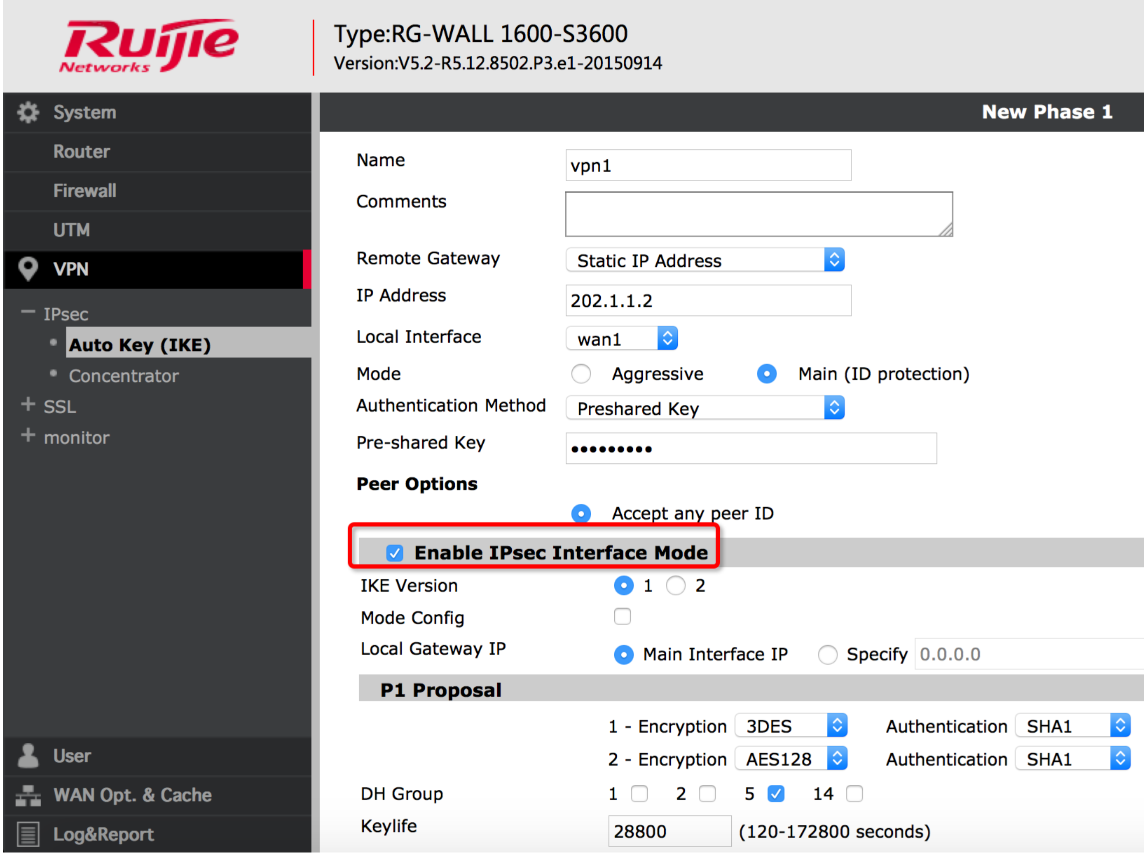
For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Configuring Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

2. **Configure IKE Phase 1**

Choose the **VPN > IPsec > Auto Key (IKE)** menu, and click **Create Phase 1**.



Configure the related parameters of Phase 1, as shown below.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Phase 1

Name: vpn1

Comments:

Remote Gateway: Static IP Address

IP Address: 202.1.1.2

Local Interface: wan1

Mode: ○ Aggressive ● Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key: •••••••••

Peer Options

● Accept any peer ID

☑ **Enable IPsec Interface Mode**

IKE Version: ● 1 ○ 2

Mode Config: □

Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

1 - Encryption 3DES Authentication SHA1

2 - Encryption AES128 Authentication SHA1

DH Group: 1 □ 2 □ 5 ☑ 14 □

Keylife: 28800 (120-172800 seconds)

Name: Set it to **VPN**. In interface mode, it is used to indicate the name of the VPN interface.

Remote Gateway: Set it to **Static IP Address**.

IP Address: The IP address of the extranet interface of the peer firewall is 200.1.1.2.

Local Interface: It refers to the interface via which the firewall builds a VPN connection with the peer device. It is usually an extranet interface.

Authentication Method: It is set to **Pre-shared Key**.

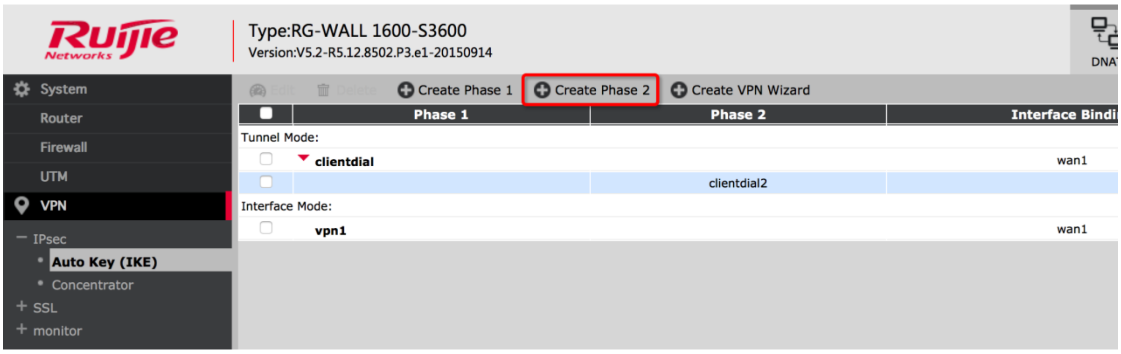
Pre-shared Key: It must be the same at both ends.

Enable IPsec Interface Mode: Ticked.

Other parameters are set to their default values. For details about the parameters, refer to section “Parameters of Phase 1”.

3. Configure IKE Phase 2

Choose the **VPN > IPsec > Auto Key (IKE)** menu, and click **Create Phase 2**.



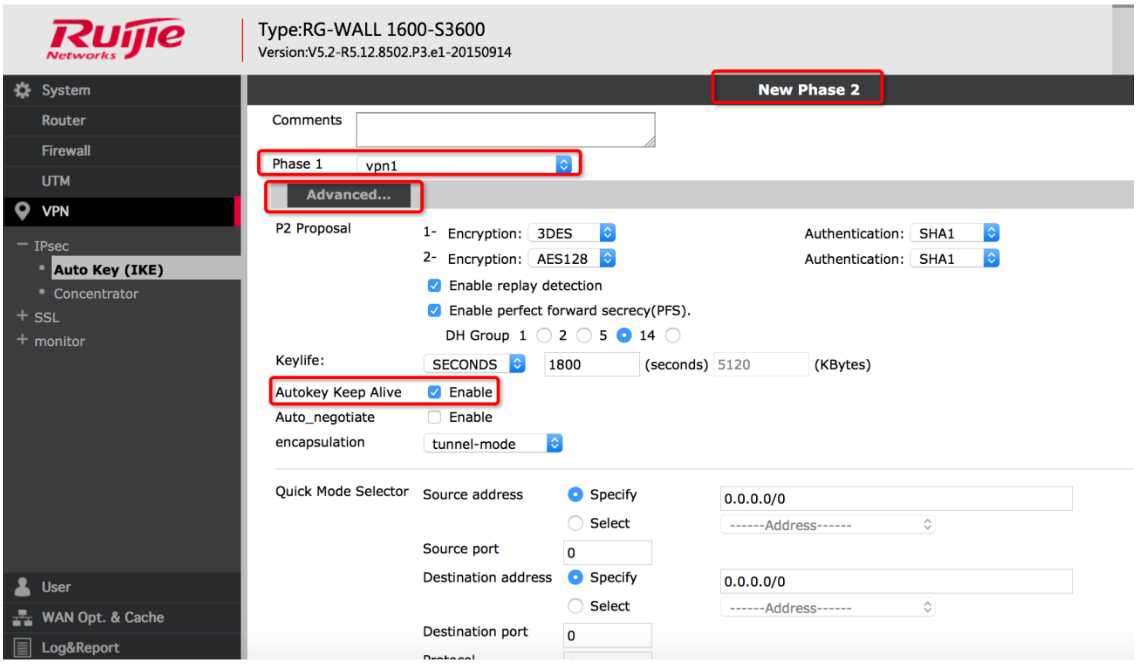
Phase 1	Phase 2	Interface Bindi
Tunnel Mode:		
clientdial		wan1
	clientdial2	
Interface Mode:		
vpn1		wan1

Configure the basic parameters of Phase 2.

Name: It refers to the name of Phase 2, and is here set to **vpn2**.

Phase 1: It is associated with Phase 2, and is here set to **vpn1**.

Click **Advanced**, and the advanced parameter options pop up.



Comments

Phase 1: vpn1

P2 Proposal
1- Encryption: 3DES Authentication: SHA1
2- Encryption: AES128 Authentication: SHA1
☑ Enable replay detection
☑ Enable perfect forward secrecy(PFS).
DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)

Autokey Keep Alive ☑ Enable

Auto_negotiate □ Enable

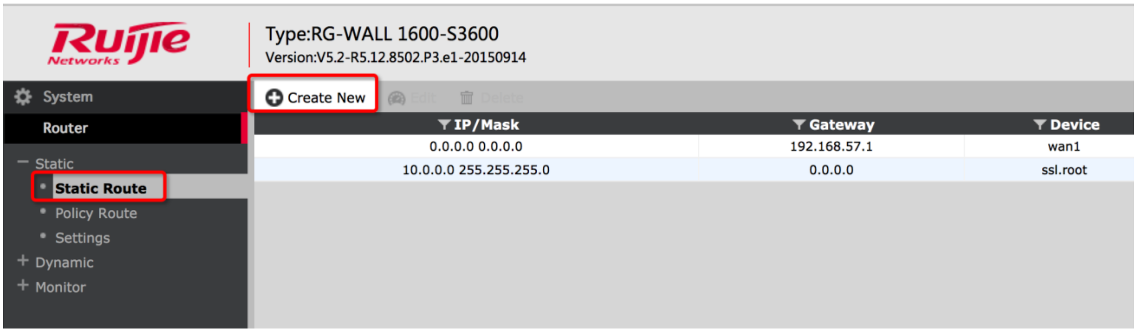
encapsulation: tunnel-mode

Quick Mode Selector
Source address ● Specify 0.0.0.0/0
○ Select ------Address------
Source port 0
Destination address ● Specify 0.0.0.0/0
○ Select ------Address------
Destination port 0
Protocol

Tick **Autokey Keep Alive**, and set other parameters to their default values.

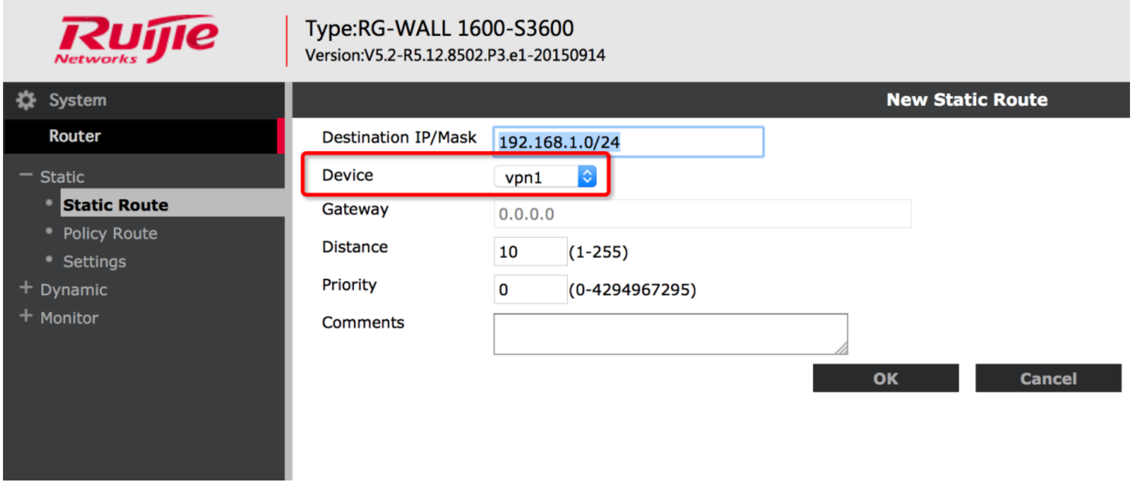
4. Configure the VPN route.

Choose the **Route** > **Static** > **Static Route** menu, and click **Create New**.



IP/Mask	Gateway	Device
0.0.0.0 0.0.0.0	192.168.57.1	wan1
10.0.0.0 255.255.255.0	0.0.0.0	ssl.root

Add the VPN static route of the protected network segment on the peer as follows:



Destination IP/Mask: 192.168.1.0/24

Device: vpn1

Gateway: 0.0.0.0

Distance: 10 (1-255)

Priority: 0 (0-4294967295)

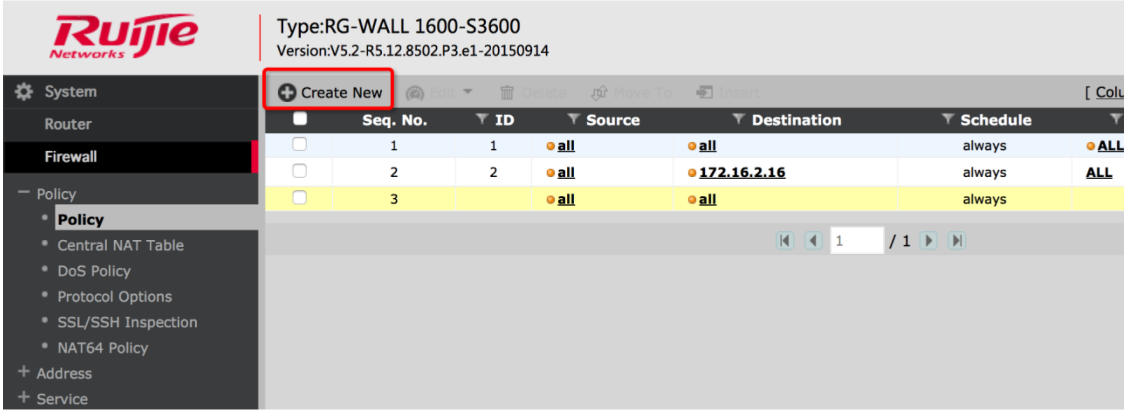
Comments:

Destination IP/Mask: It refers to the subnet protected by the peer firewall; here, it is set to 192.168.1.0.

Device: It refers to the interface generated by the VPN; here, it is set to **vpn1**.

5. Configure the policies

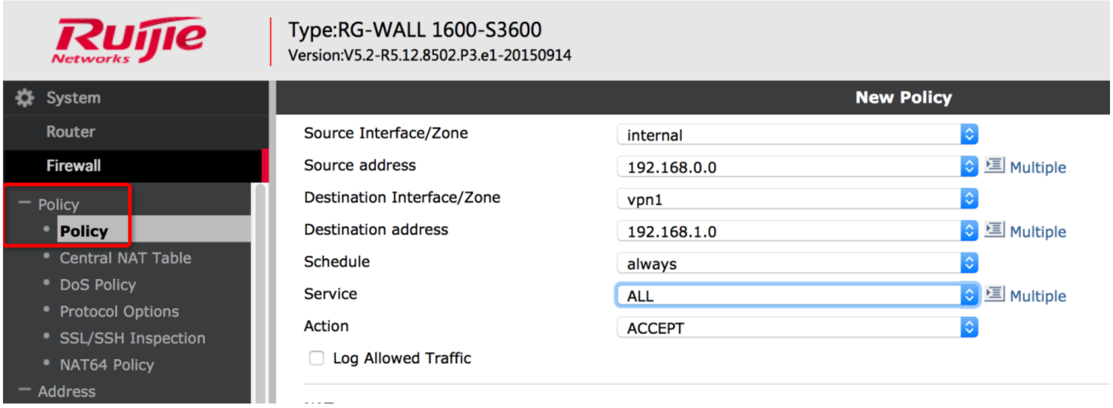
Choose the **Firewall** > **Policy** > **Policy** menu, and click **Create New**.



	Seq. No.	ID	Source	Destination	Schedule	
□	1	1	all	all	always	ALL
□	2	2	all	172.16.2.16	always	ALL
□	3		all	all	always	

Create two policies as shown below. Via the policies, the system controls the access between two subnets at the peer end, and implements NAT and UTM protection.

Policy 1: Allow the local 192.168.0.0 network segment to access the peer 192.168.1.0 network segment.



Source Interface/Zone: internal

Source address: 192.168.0.0

Destination Interface/Zone: vpn1

Destination address: 192.168.1.0

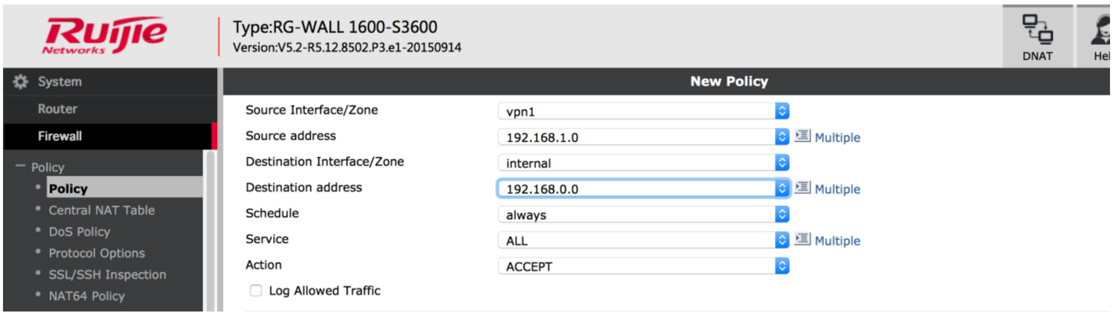
Schedule: always

Service: ALL

Action: ACCEPT

□ Log Allowed Traffic

Policy 2: Allow the peer 192.168.1.0 network segment to access the local 192.168.0.0 network segment.



Source Interface/Zone	vpn1
Source address	192.168.1.0 Multiple
Destination Interface/Zone	internal
Destination address	192.168.0.0 Multiple
Schedule	always
Service	ALL Multiple
Action	ACCEPT

☐ Log Allowed Traffic

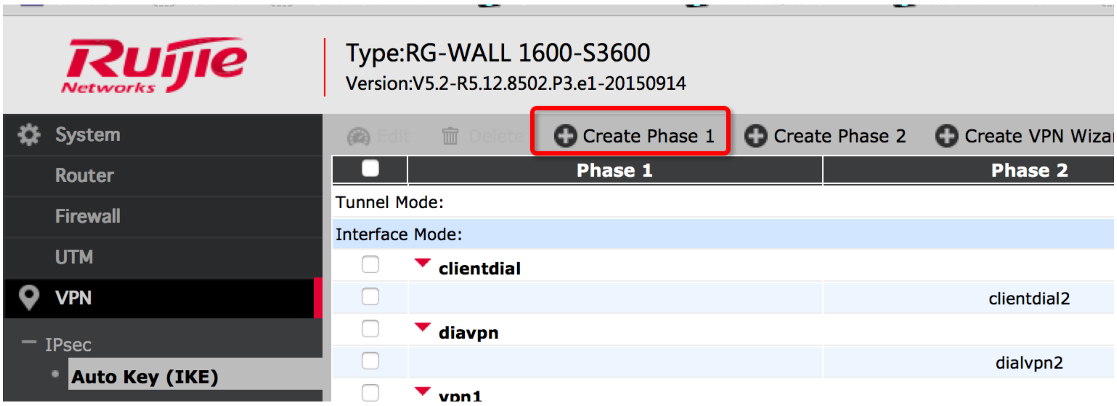
2. Configure NGFW2

1. Perform basic configurations of Internet access

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Configuring Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

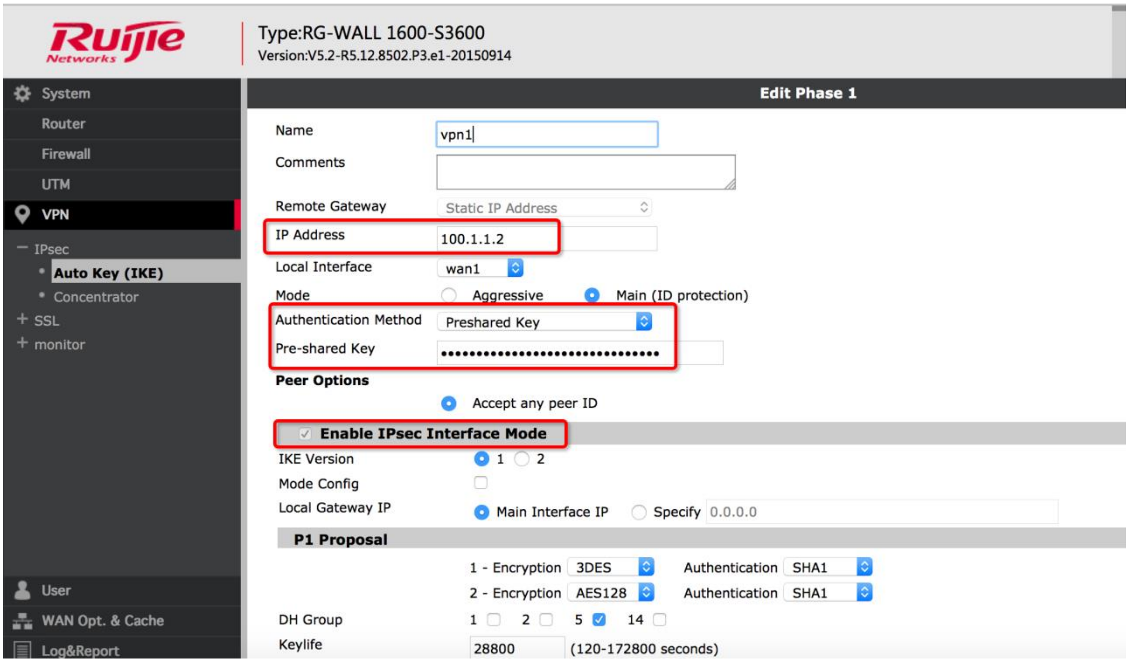
2. Configure IKE Phase 1

Choose the **VPN > IPsec > Auto Key (IKE)** menu, and click **Create Phase 1**.



☐	Phase 1	Phase 2
Tunnel Mode:		
Interface Mode:		
☐	**clientdial**	
☐		clientdial2
☐	**diavpn**	
☐		dialvpn2
☐	**vpn1**	

Configure the related parameters of Phase 1.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Phase 1

Name: vpn1

Comments:

Remote Gateway: Static IP Address

IP Address: 100.1.1.2

Local Interface: wan1

Mode: ○ Aggressive ● Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key: ••••••••••••••••••••••••••••••

Peer Options

● Accept any peer ID

☑ **Enable IPsec Interface Mode**

IKE Version: ● 1 ○ 2

Mode Config: □

Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

1 - Encryption 3DES Authentication SHA1

2 - Encryption AES128 Authentication SHA1

DH Group: 1 □ 2 □ 5 ☑ 14 □

Keylife: 28800 (120-172800 seconds)

Name: Set it to **VPN**. In interface mode, it is used to indicate the name of the VPN interface.

Remote Gateway: Set it to **Static IP Address**.

IP Address: The IP address of the extranet interface of the peer firewall is 100.1.1.2.

Local Interface: It refers to an interface via which the firewall builds a VPN connection with the peer device; it is here set to **wan1**.

Authentication Method: It is set to **Pre-shared Key**.

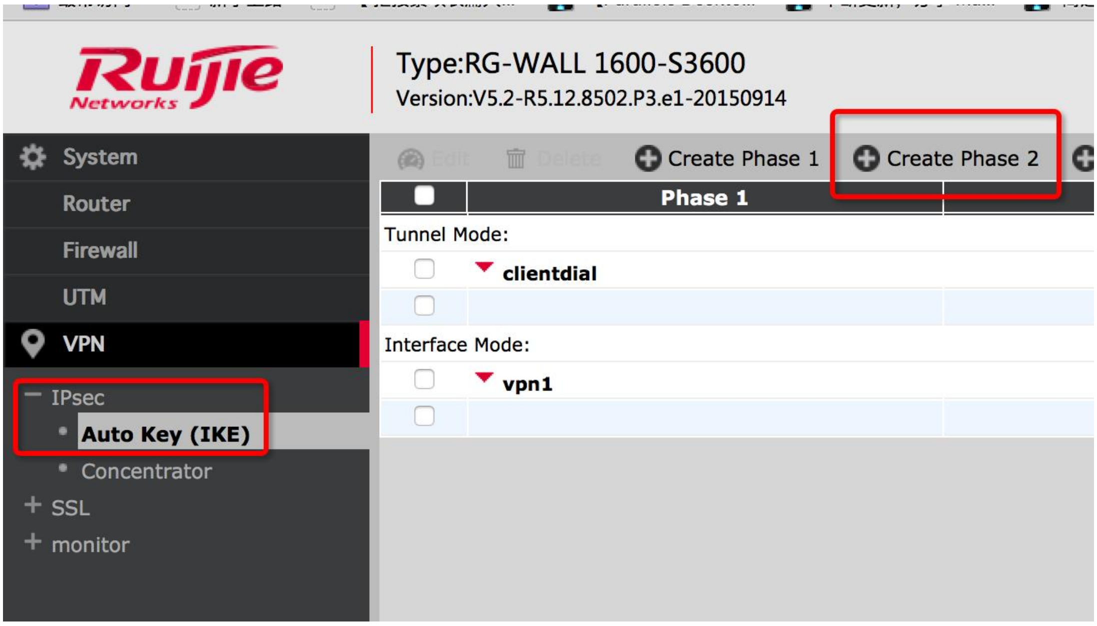
Pre-shared Key: It must be the same at both ends.

Enable IPsec Interface Mode: Ticked.

Other parameters are set to their default values. For details about the parameters, refer to section “Parameters of Phase 1”.

3. Configure IKE Phase 2

Choose the **VPN > IPsec > Auto Key (IKE)** menu, and click **Create Phase 2**.



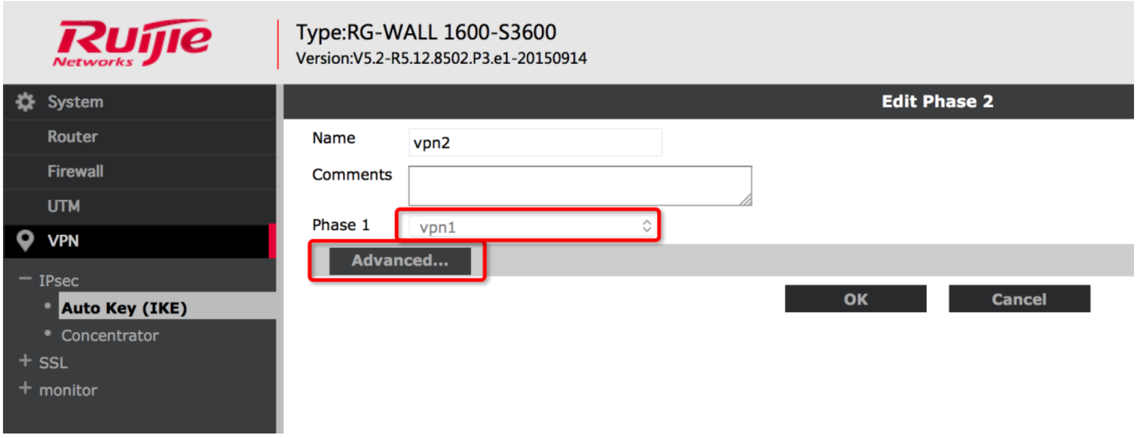
Tunnel Mode:

☐ clientdial

Interface Mode:

☐ vpn1

Configure the basic parameters of Phase 2.



Name: vpn2

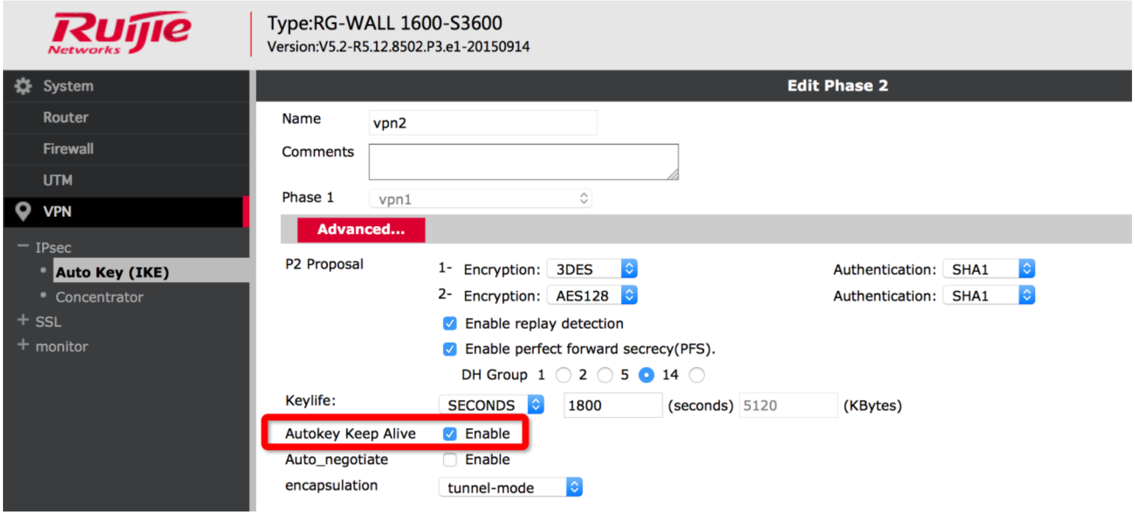
Comments:

Phase 1: vpn1

Name: It refers to the name of Phase 2, and is here set to **vpn2**.

Phase 1: It is associated with Phase 2, and is here set to **vpn**.

Click **Advanced**, and the advanced parameter options pop up.



Name: vpn2

Comments:

Phase 1: vpn1

P2 Proposal
1- Encryption: 3DES Authentication: SHA1
2- Encryption: AES128 Authentication: SHA1
☑ Enable replay detection
☑ Enable perfect forward secrecy(PFS).
DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)

Autokey Keep Alive ☑ Enable

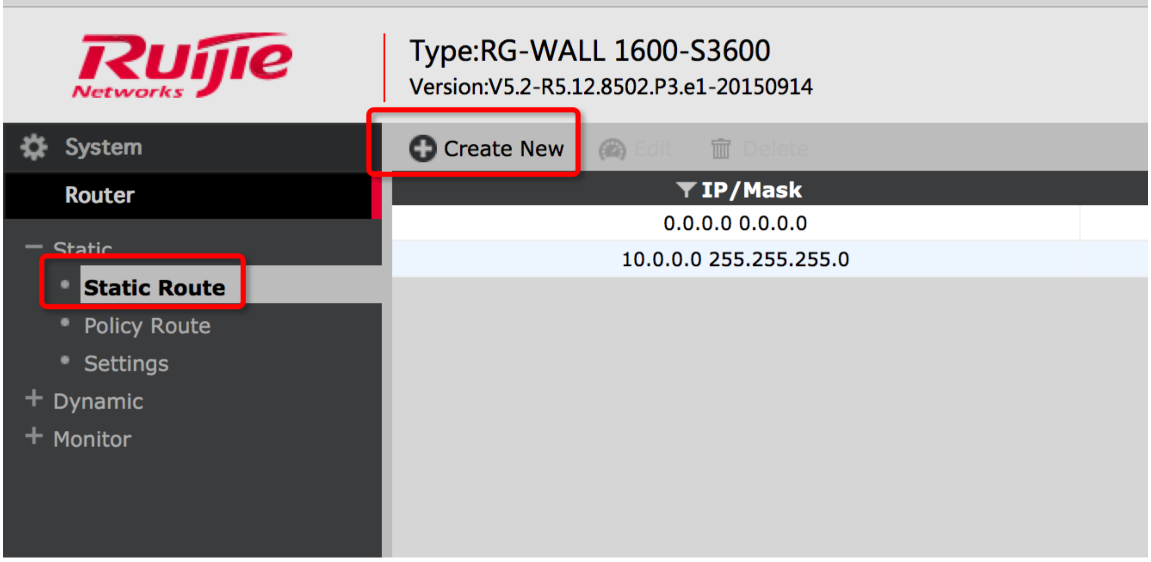
Auto_negotiate ☐ Enable

encapsulation tunnel-mode

Tick **Autokey Keep Alive**, and set other parameters to their default values.

4. Configure the VPN routes.

Choose the **Route** > **Static** > **Static Route** menu, and click **Create New**.

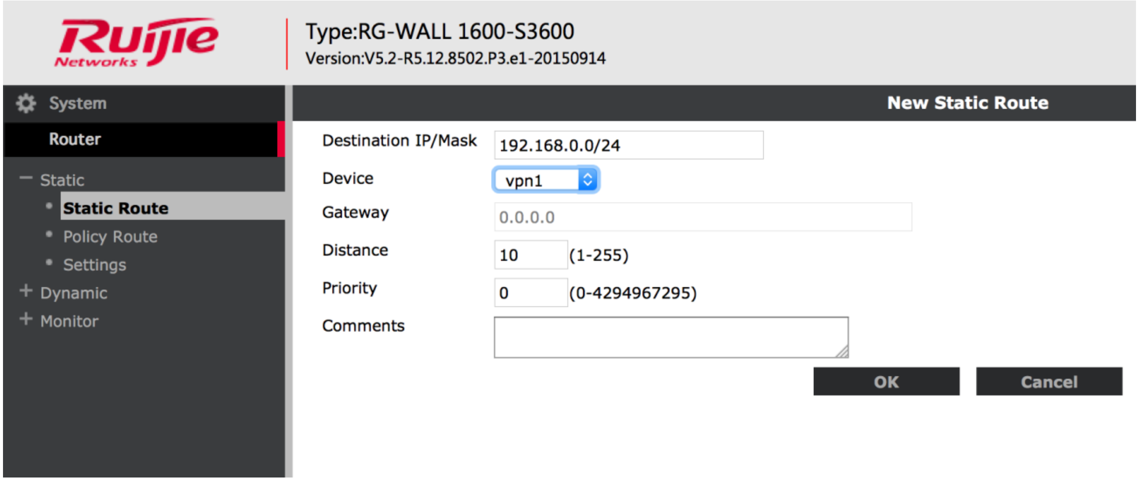


Type:RG-WALL 1600-S3600

Version:V5.2-R5.12.8502.P3.e1-20150914

IP/Mask
0.0.0.0 0.0.0.0
10.0.0.0 255.255.255.0

Add the VPN route of the protected network segment on the peer as shown below:



Type:RG-WALL 1600-S3600

Version:V5.2-R5.12.8502.P3.e1-20150914

New Static Route

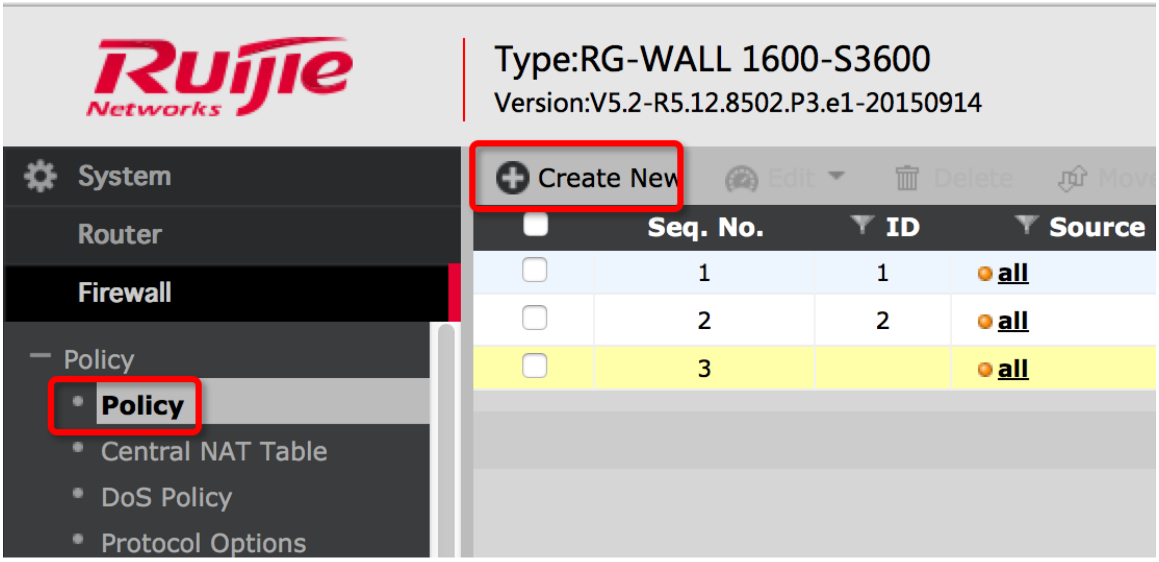
Destination IP/Mask	192.168.0.0/24
Device	vpn1
Gateway	0.0.0.0
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Destination IP/Mask: It refers to the subnet protected by the peer firewall; here, it is set to 192.168.1.0/24.

Device: It refers to the interface generated by the VPN; here, it is set to **vpn**.

5. Configure the policies

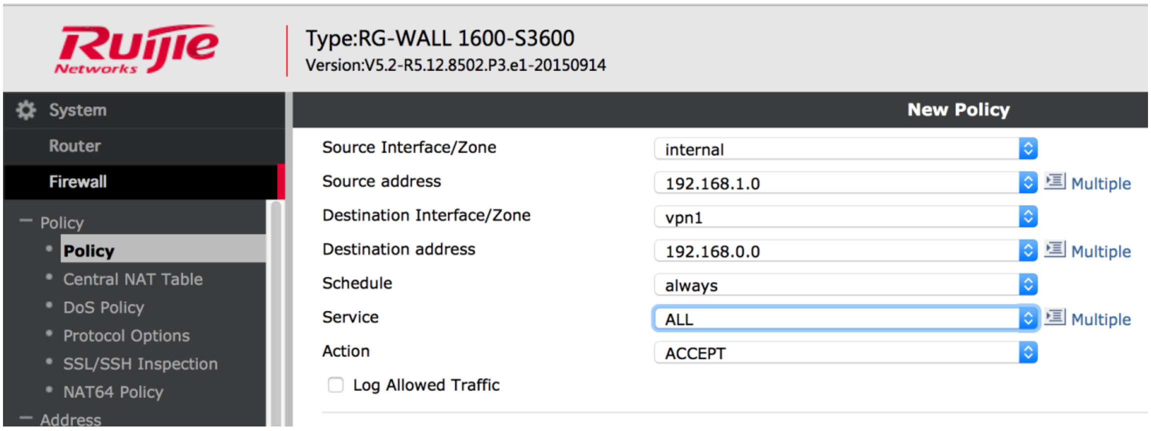
Choose the **Firewall** > **Policy** > **Policy** menu, and click **Create New**.



☐	Seq. No.	ID	Source
☐	1	1	all
☐	2	2	all
☐	3		all

Create two policies as shown below. Via the policies, the system controls the access between two subnets at the peer end, and implements NAT and UTM protection.

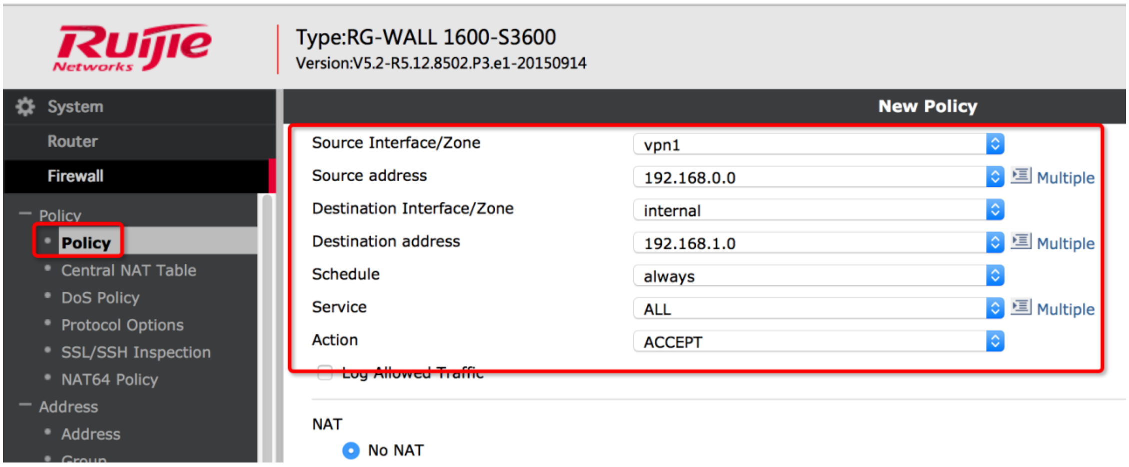
Policy 1: Allow the local 192.168.1.0 network segment to access the peer 192.168.0.0 network segment.



New Policy

Source Interface/Zone: internal
Source address: 192.168.1.0
Destination Interface/Zone: vpn1
Destination address: 192.168.0.0
Schedule: always
Service: ALL
Action: ACCEPT
☐ Log Allowed Traffic

Policy 2: Allow the peer 192.168.0.0 network segment to access the local 192.168.1.0 network segment.



New Policy

Source Interface/Zone: vpn1
Source address: 192.168.0.0
Destination Interface/Zone: internal
Destination address: 192.168.1.0
Schedule: always
Service: ALL
Action: ACCEPT
☐ Log Allowed Traffic

NAT
● No NAT

3.7.1.2 Troubleshooting

Common Negotiation Failures:

1. Inconsistency of pre-shared key;
2. Inconsistency of encryption algorithm and authentication algorithm parameters;
3. Mismatch of quick selector at two ends in Phase 2;
4. Errors of policy configurations or sequence.

Troubleshooting Commands:

```
RG-WALL#diagnose debug enable
RG-WALL#diagnose debug application ike -1
```

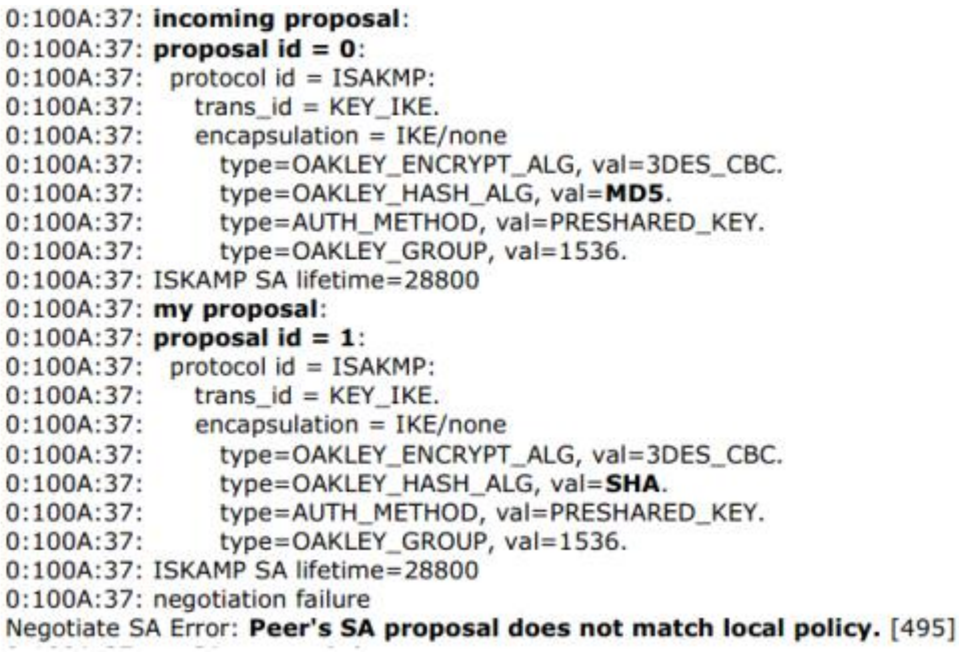
If multiple gateways are available, observe the negotiation process of ike after the gateways are filtered:

```
diagnose vpn ike log-filter dst-addr4 <IP address of peer gateway>
diagnose vpn ike log-filter src-addr4 <IP address of local gateway>
diagnose vpn ike log-filter dst-port  <Peer port of IKE negotiation, for example, 500>
diagnose vpn ike log-filter src-port  <Local port of IKE negotiation, for example, 500>
```

Analysis of Common Faults:

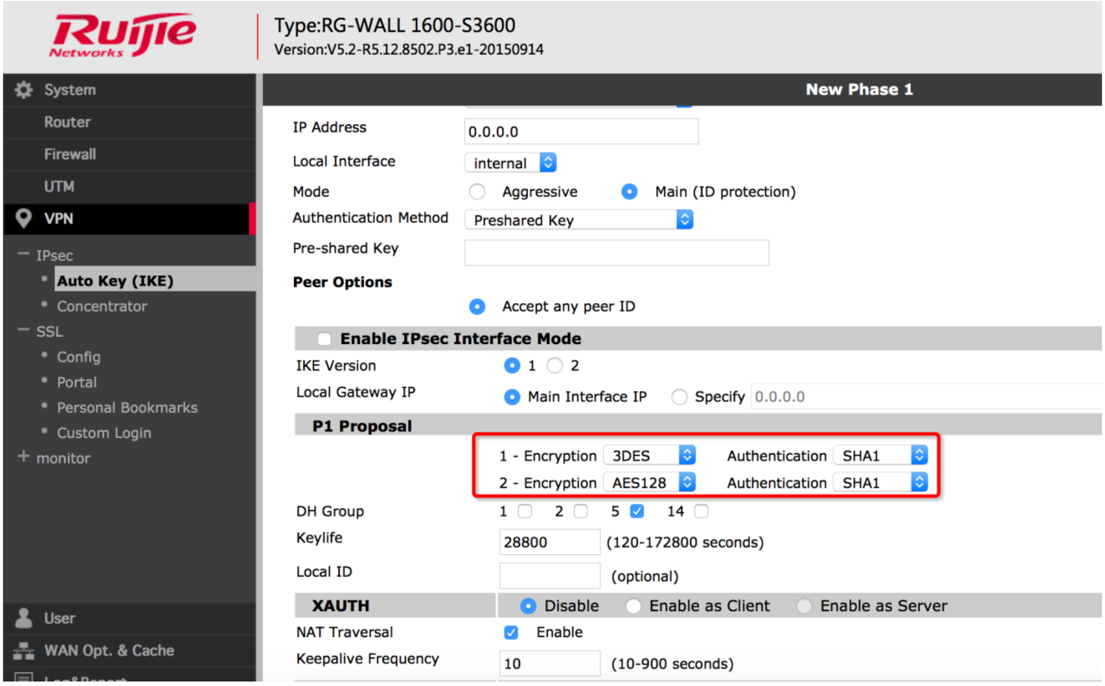
1. Inconsistency of encryption and authentication algorithms: In Phase 1, authentication or encryption algorithms are not consistent. Check the authentication or encryption algorithms on the devices of both ends at the time of IPsec setup for their consistency.

Results of packet capture:



```
0:100A:37: incoming proposal:
0:100A:37: proposal id = 0:
0:100A:37:   protocol id = ISAKMP:
0:100A:37:     trans_id = KEY_IKE.
0:100A:37:     encapsulation = IKE/none
0:100A:37:       type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
0:100A:37:       type=OAKLEY_HASH_ALG, val=MD5.
0:100A:37:       type=AUTH_METHOD, val=PRESHARED_KEY.
0:100A:37:       type=OAKLEY_GROUP, val=1536.
0:100A:37: ISKAMP SA lifetime=28800
0:100A:37: my proposal:
0:100A:37: proposal id = 1:
0:100A:37:   protocol id = ISAKMP:
0:100A:37:     trans_id = KEY_IKE.
0:100A:37:     encapsulation = IKE/none
0:100A:37:       type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
0:100A:37:       type=OAKLEY_HASH_ALG, val=SHA.
0:100A:37:       type=AUTH_METHOD, val=PRESHARED_KEY.
0:100A:37:       type=OAKLEY_GROUP, val=1536.
0:100A:37: ISKAMP SA lifetime=28800
0:100A:37: negotiation failure
Negotiate SA Error: Peer's SA proposal does not match local policy. [495]
```

Troubleshooting position: Check whether the encryption and authentication algorithms in the red frame below match each other at two ends.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Phase 1

IP Address: 0.0.0.0
Local Interface: internal
Mode: ○ Aggressive ● Main (ID protection)
Authentication Method: Preshared Key
Pre-shared Key:

Peer Options

● Accept any peer ID

□ **Enable IPsec Interface Mode**

IKE Version: ● 1 ○ 2
Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

1 - Encryption 3DES Authentication SHA1
2 - Encryption AES128 Authentication SHA1

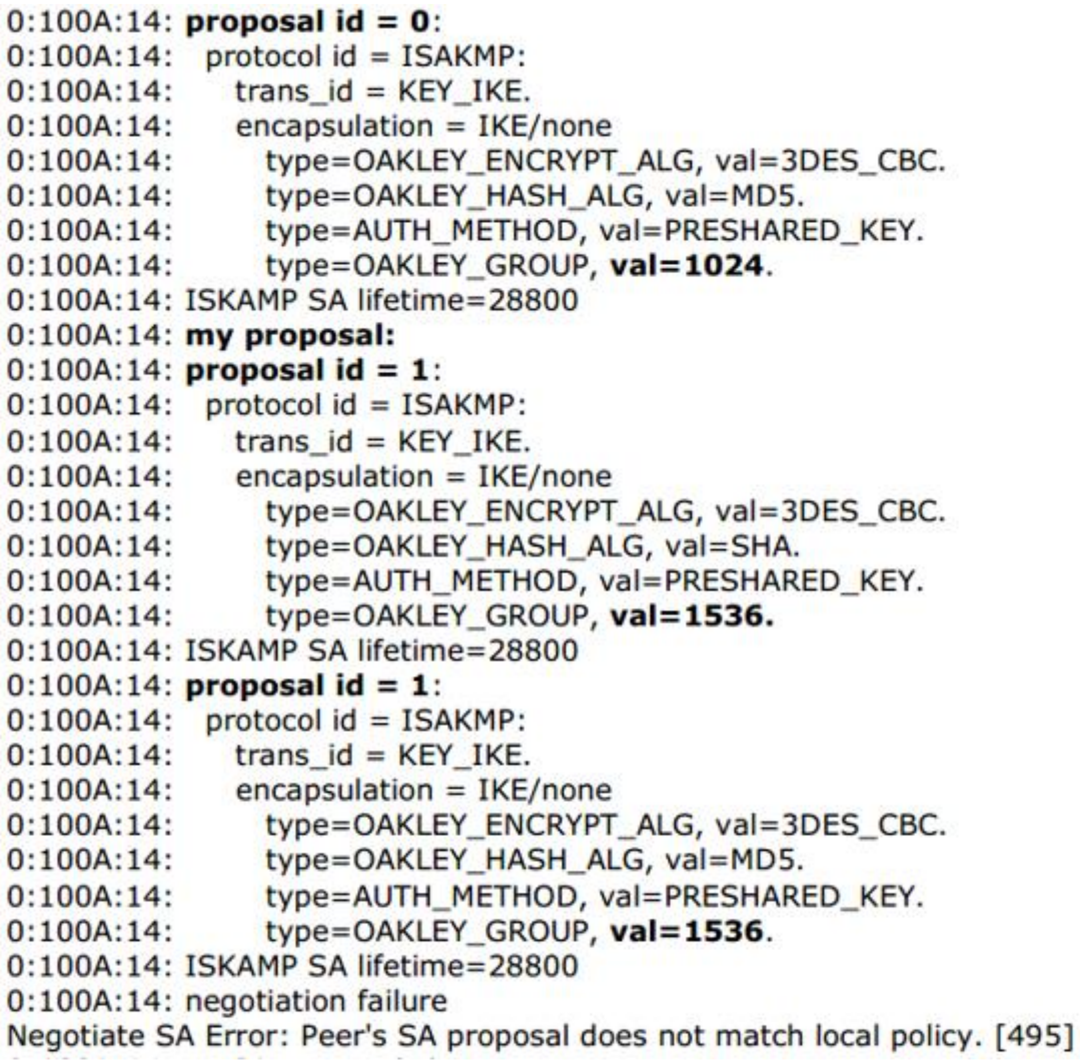
DH Group: 1 □ 2 □ 5 ☑ 14 □
Keylife: 28800 (120-172800 seconds)
Local ID: (optional)

XAUTH ● Disable ○ Enable as Client ○ Enable as Server

NAT Traversal: ☑ Enable
Keepalive Frequency: 10 (10-900 seconds)

2. Inconsistency of DH algorithm: The DH algorithms at two ends are not consistent.

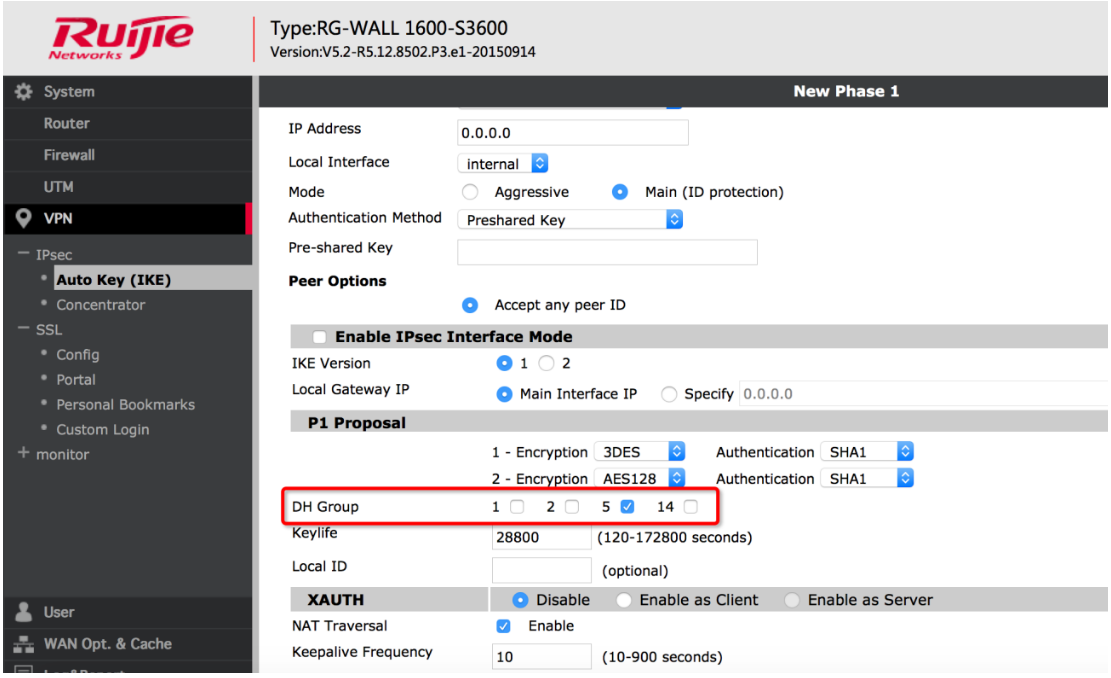
Results of packet capture:



```
0:100A:14: proposal id = 0:
0:100A:14:   protocol id = ISAKMP:
0:100A:14:      trans_id = KEY_IKE.
0:100A:14:      encapsulation = IKE/none
0:100A:14:         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
0:100A:14:         type=OAKLEY_HASH_ALG, val=MD5.
0:100A:14:         type=AUTH_METHOD, val=PRESHARED_KEY.
0:100A:14:         type=OAKLEY_GROUP, val=1024.
0:100A:14: ISKAMP SA lifetime=28800
0:100A:14: my proposal:
0:100A:14: proposal id = 1:
0:100A:14:   protocol id = ISAKMP:
0:100A:14:      trans_id = KEY_IKE.
0:100A:14:      encapsulation = IKE/none
0:100A:14:         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
0:100A:14:         type=OAKLEY_HASH_ALG, val=SHA.
0:100A:14:         type=AUTH_METHOD, val=PRESHARED_KEY.
0:100A:14:         type=OAKLEY_GROUP, val=1536.
0:100A:14: ISKAMP SA lifetime=28800
0:100A:14: proposal id = 1:
0:100A:14:   protocol id = ISAKMP:
0:100A:14:      trans_id = KEY_IKE.
0:100A:14:      encapsulation = IKE/none
0:100A:14:         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
0:100A:14:         type=OAKLEY_HASH_ALG, val=MD5.
0:100A:14:         type=AUTH_METHOD, val=PRESHARED_KEY.
0:100A:14:         type=OAKLEY_GROUP, val=1536.
0:100A:14: ISKAMP SA lifetime=28800
0:100A:14: negotiation failure
Negotiate SA Error: Peer's SA proposal does not match local policy. [495]
```

Troubleshooting position: Check whether the DH Group in the red frame below is consistent at two ends.

(Common packet capture results of DH group: DH group 1 (768-bit), DH group 2 (1024-bit), and DH group 5 (1536-bit))



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Phase 1

IP Address: 0.0.0.0

Local Interface: internal

Mode: ○ Aggressive ● Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key:

Peer Options

● Accept any peer ID

□ **Enable IPsec Interface Mode**

IKE Version: ● 1 ○ 2

Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

1 - Encryption 3DES Authentication SHA1

2 - Encryption AES128 Authentication SHA1

DH Group: 1 □ 2 □ 5 ☑ 14 □

Keylife: 28800 (120-172800 seconds)

Local ID: (optional)

XAUTH ● Disable ○ Enable as Client ○ Enable as Server

NAT Traversal: ☑ Enable

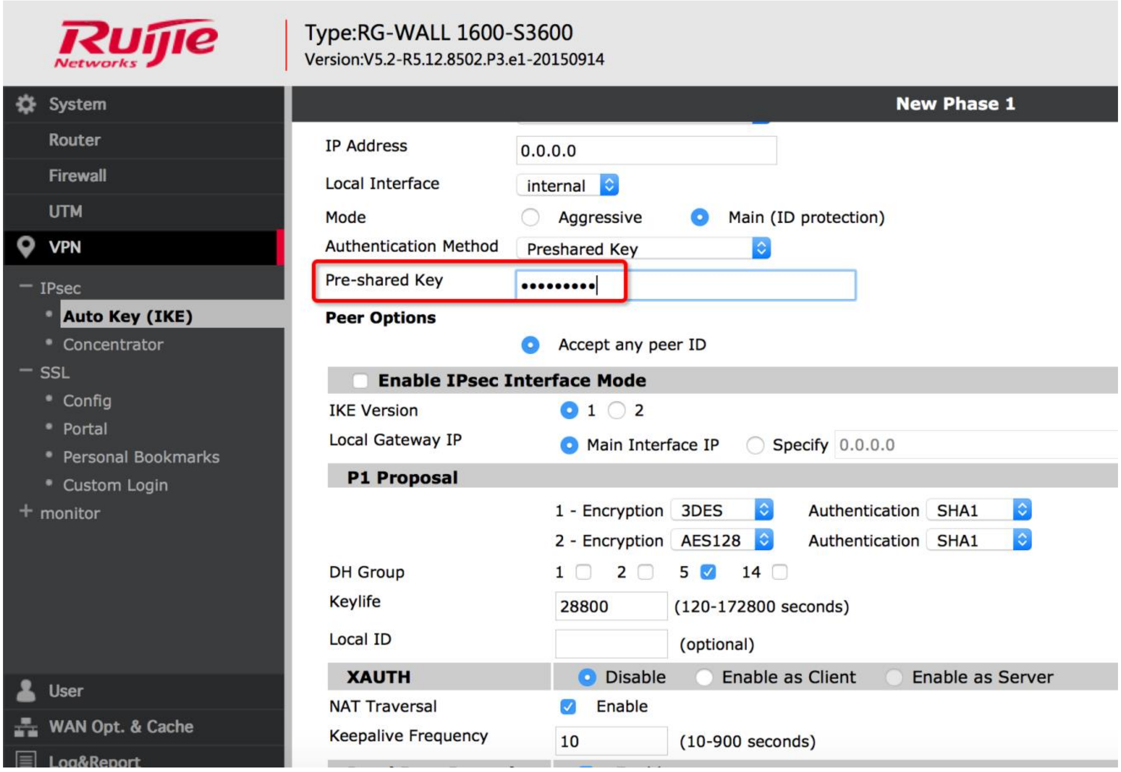
Keepalive Frequency: 10 (10-900 seconds)

3. Inconsistency of pre-shared key;

Results of packet capture:

```
ike 0:mobile:5140: responder: main mode get 3rd message...
ike 0:mobile:5140: dec
A5BF9FFD3412F8CD24C7C54635FA869705100201000000000000005CF50FA936BEFB6D99E76CD6FAA679D778581
60C306FE83B03F7DB8CFB680BB864AB42391BA3C5A5ADCDFB2D6CF1CEEC0A6AC0BAC12DFEABEC25E534580E6EFF
32
ike 0:mobile:5140: probable pre-shared secret mismatch
```

Troubleshooting position: Check the position in the red frame below.



New Phase 1

IP Address: 0.0.0.0

Local Interface: internal

Mode: ○ Aggressive ● Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key: •••••••••

Peer Options

● Accept any peer ID

□ **Enable IPsec Interface Mode**

IKE Version: ● 1 ○ 2

Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

1 - Encryption: 3DES Authentication: SHA1

2 - Encryption: AES128 Authentication: SHA1

DH Group: 1 □ 2 □ 5 ☑ 14 □

Keylife: 28800 (120-172800 seconds)

Local ID: (optional)

XAUTH: ● Disable ○ Enable as Client ○ Enable as Server

NAT Traversal: ☑ Enable

Keepalive Frequency: 10 (10-900 seconds)

Normal packet capture results of pre-shared key:

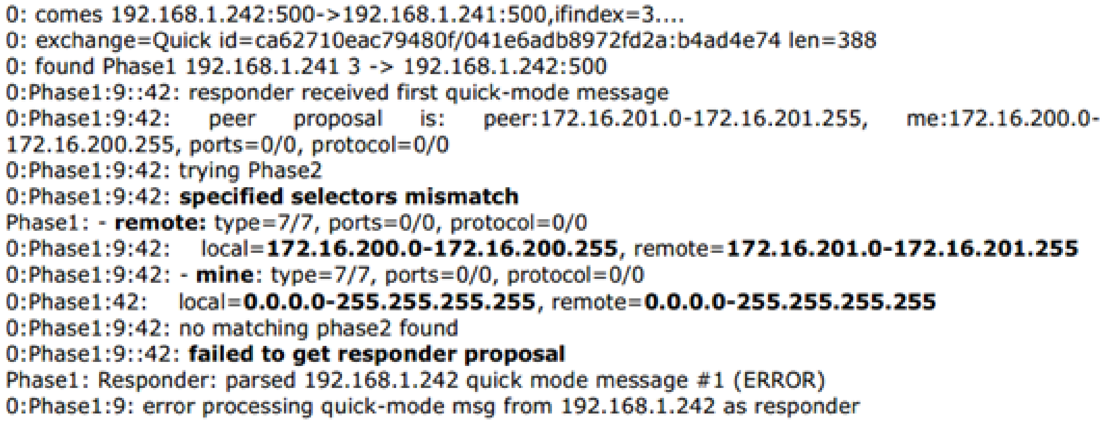
```
ike 0:mobile:5122: responder: main mode get 3rd message...
ike 0:mobile:5122: dec
0AB1AD6CF994A06023E867B8EBB63F45051002010000000000000005C0800000C01000000C0A8FE020B000018608
B589D57388681EC1286989FB775C88FEB66D20000001C00000001011060020AB1AD6CF994A06023E867B8EBB63F
45
ike 0:mobile:5122: received notify type 24578
ike 0:mobile:5122: PSK authentication succeeded
ike 0:mobile:5122: authentication OK
```

4. Normal negotiation prompts of Phase 1

```
ike 0:0ab1ad6cf994a060/0000000000000000:5122: negotiation result
ike 0:0ab1ad6cf994a060/0000000000000000:5122: proposal id = 1:
ike 0:0ab1ad6cf994a060/0000000000000000:5122:   protocol id = ISAKMP:
ike 0:0ab1ad6cf994a060/0000000000000000:5122:      trans_id = KEY_IKE.
ike 0:0ab1ad6cf994a060/0000000000000000:5122:      encapsulation = IKE/none
ike 0:0ab1ad6cf994a060/0000000000000000:5122:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:0ab1ad6cf994a060/0000000000000000:5122:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:0ab1ad6cf994a060/0000000000000000:5122:         type=AUTH_METHOD,
val=PRESHARED_KEY_XAUTH_I.
ike 0:0ab1ad6cf994a060/0000000000000000:5122:         type=OAKLEY_GROUP, val=1536.
ike 0:0ab1ad6cf994a060/0000000000000000:5122: ISAKMP SA lifetime=28800
ike 0:0ab1ad6cf994a060/0000000000000000:5122: SA proposal chosen, matched gateway mobile
```

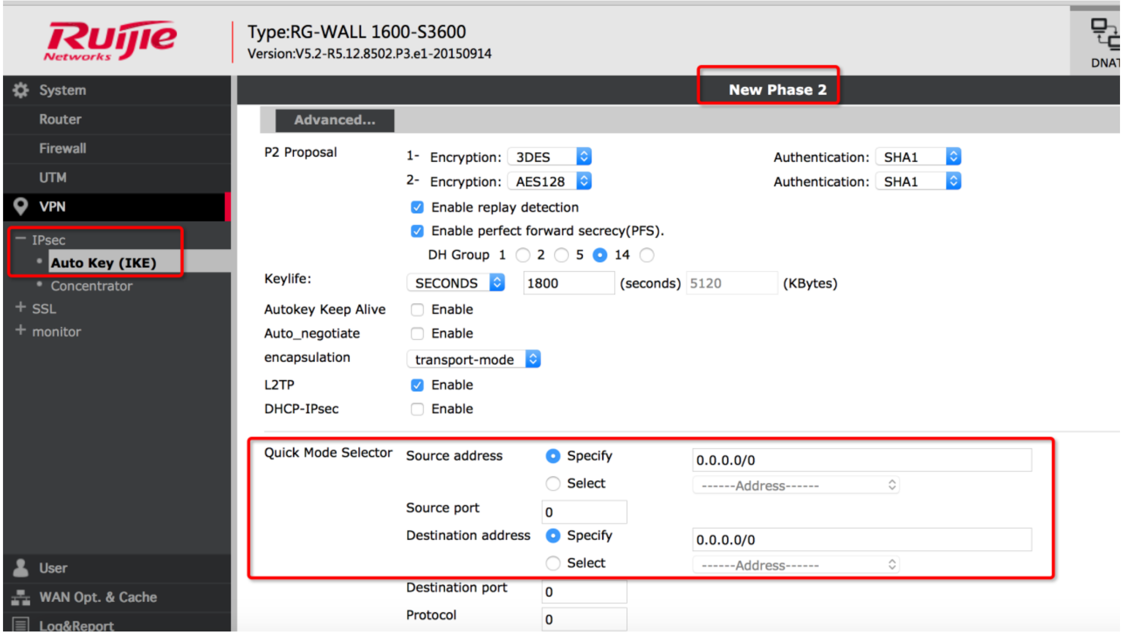
5. Mismatch of quick selector in Phase 2

Results of packet capture



```
0: comes 192.168.1.242:500->192.168.1.241:500,ifindex=3....
0: exchange=Quick id=ca62710eac79480f/041e6adb8972fd2a:b4ad4e74 len=388
0: found Phase1 192.168.1.241 3 -> 192.168.1.242:500
0:Phase1:9::42: responder received first quick-mode message
0:Phase1:9:42:   peer   proposal   is:   peer:172.16.201.0-172.16.201.255,   me:172.16.200.0-
172.16.200.255, ports=0/0, protocol=0/0
0:Phase1:9:42: trying Phase2
0:Phase1:9:42: specified selectors mismatch
Phase1: - remote: type=7/7, ports=0/0, protocol=0/0
0:Phase1:9:42:   local=172.16.200.0-172.16.200.255, remote=172.16.201.0-172.16.201.255
0:Phase1:9:42: - mine: type=7/7, ports=0/0, protocol=0/0
0:Phase1:42:   local=0.0.0.0-255.255.255.255, remote=0.0.0.0-255.255.255.255
0:Phase1:9:42: no matching phase2 found
0:Phase1:9::42: failed to get responder proposal
Phase1: Responder: parsed 192.168.1.242 quick mode message #1 (ERROR)
0:Phase1:9: error processing quick-mode msg from 192.168.1.242 as responder
```

Troubleshooting position: Check whether the network segment settings in the red frame below match each other at two ends.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

P2 Proposal: 1- Encryption: 3DES Authentication: SHA1; 2- Encryption: AES128 Authentication: SHA1

☑ Enable replay detection

☑ Enable perfect forward secrecy(PFS).

DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)

Autokey Keep Alive □ Enable

Auto_negotiate □ Enable

encapsulation transport-mode

L2TP ☑ Enable

DHCP-IPsec □ Enable

Quick Mode Selector

Source address ● Specify 0.0.0.0/0

○ Select ------Address------

Source port 0

Destination address ● Specify 0.0.0.0/0

○ Select ------Address------

Destination port 0

Protocol 0

Other common commands

1) If multiple gateways are available, observe the negotiation process of ike after the gateways are filtered:

diagnose vpn ike log-filter dst-addr4 <IP address of peer gateway>

diagnose vpn ike log-filter src-addr4 <IP address of local gateway>

diagnose vpn ike log-filter dst-port <Peer port of IKE negotiation, for example, 500>

diagnose vpn ike log-filter src-port <Local port of IKE negotiation, for example, 500>

2) View the VPN channels: **diagnose vpn tunnel list**

```
RG-WALL # diagnose  vpn tunnel  list
list all ipsec tunnel in vd 0
```

```
------------------------------------------------------
name=mobile_0 ver=1 serial=4 192.168.118.25:4500->192.168.118.151:10954 lgwy=static
tun=intf mode=dial_inst bound_if=5
parent=mobile index=0
proxyid_num=1 child_num=0 refcnt=7 ilast=3 olast=3
stat: rxp=10 txp=0 rxb=1280 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=22
natt: mode=silent draft=32 interval=10 remote_port=10954
proxyid=mobile proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.0.0.10-10.0.0.10:0
  SA: ref=4 options=00000006 type=00 soft=0 mtu=1280 expire=1671 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1790/1800
  dec: spi=b2ad0f87 esp=aes key=16 046a1e666f7ae7b2aaf6197a13ea5818
       ah=sha1 key=20 6f607decd4416c203911070d960cd5f26e2061bf
  enc: spi=dfe610a1 esp=aes key=16 453e333a15416cfdb6ab95d324fa3ffe
       ah=sha1 key=20 2a2d1cee5da51a1503ddb18599a265d5dce51e5a
  dec:pkts/bytes=10/608, enc:pkts/bytes=0/0
  npu_flag=02 npu_rgwy=192.168.118.151 npu_lgwy=192.168.118.25 npu_selid=2
------------------------------------------------------
name=mobile ver=1 serial=1 192.168.118.25:0->0.0.0.0:0 lgwy=static tun=intf mode=dialup
bound_if=5
proxyid_num=0 child_num=1 refcnt=5 ilast=29 olast=29
stat: rxp=0 txp=0 rxb=0 txb=0
```

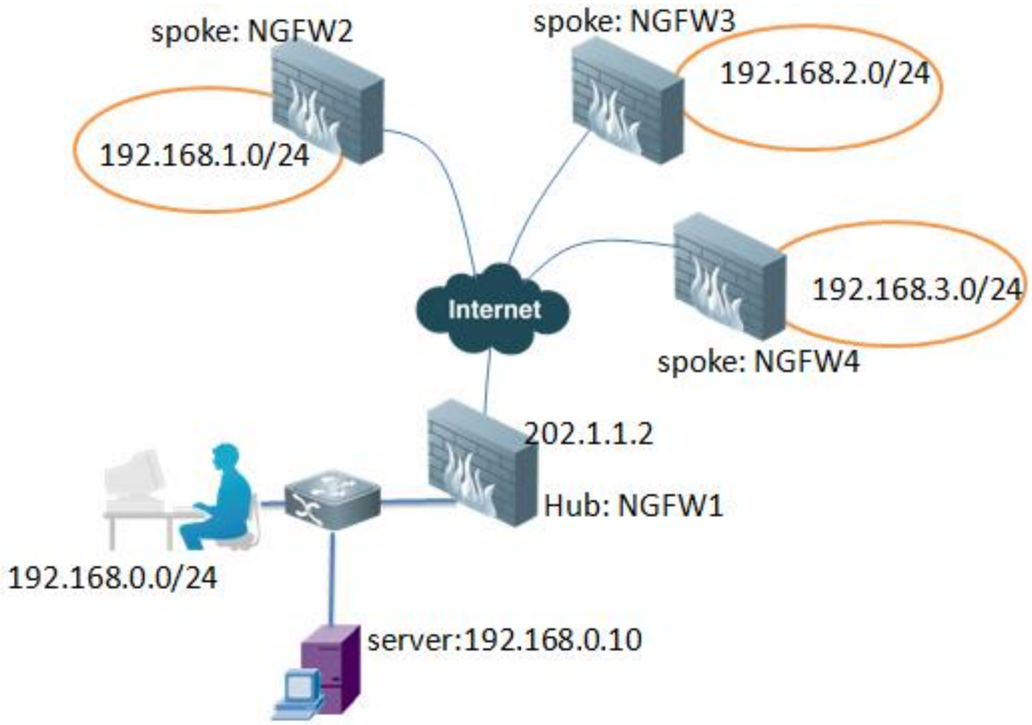
3.7.2 IPSec VPN (Dial-up)

3.7.2.1 HUB-SPOKE Mode

Networking Requirements

As shown in the figure, the headquarters of a company is internally fitted with an OA server and the three branch offices of the company need to log in to the headquarters' intranet by VPN dial-up first and then access the OA server. To facilitate the configurations, the headquarters wants to build only one VPN tunnel to implement the communications between all branch offices and the headquarters.

Network Topology



Configuration Tips

1. Configure NGFW-1

1. Perform basic configurations of Internet access;
2. Configure IKE Stage 1;
3. Configure IKE Stage 2;
4. Configure the IPsec policy;
5. Configure the route.

2. Configure NGFW-2

1. Perform basic configurations of Internet access;
2. Configure IKE Stage 1;
3. Configure IKE Stage 2;
4. Configure the route;
5. Configure the IPSec policy;

3. Configure other spoke node devices.

To delete Stages 1 and 2 of IPSec VPN, you need to delete the invoked route or firewall security policy first.

Configuration Steps

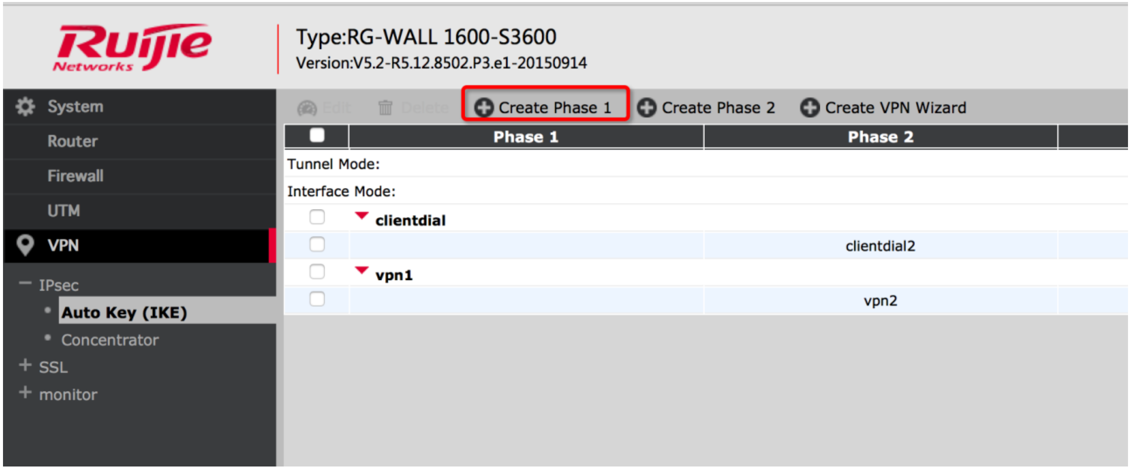
1. Configure NGFW-1

1) Perform basic configurations of Internet access

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

2) Configure IKE Stage 1

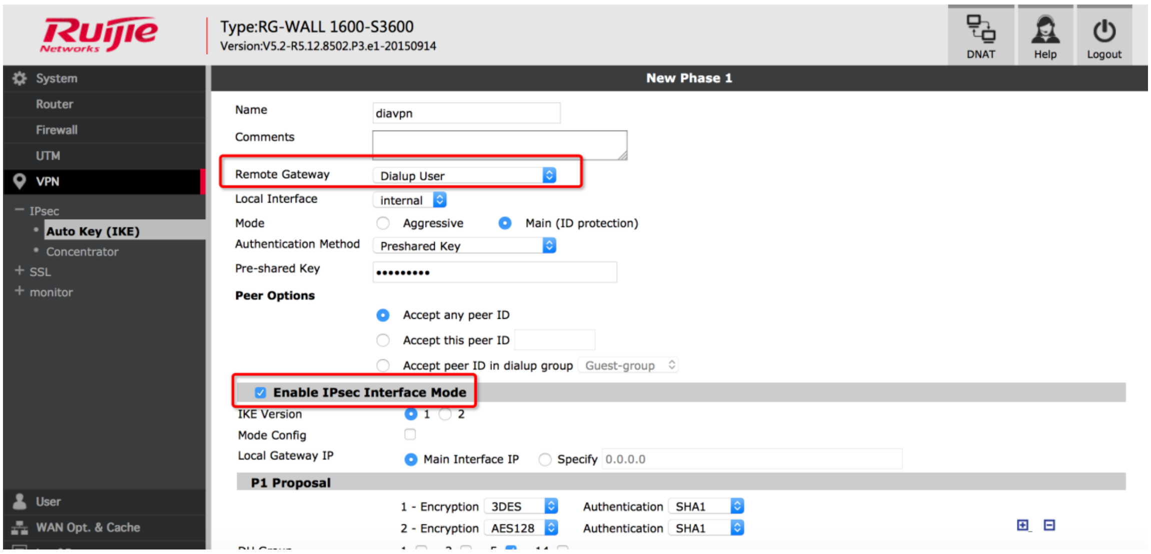
Choose the **VPN > IPsec > Auto Key (IKE)** menu, and click **Create Phase 1**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

□	Phase 1	Phase 2
Tunnel Mode:		
Interface Mode:		
□	clientdial	
□		clientdial2
□	vpn1	
□		vpn2

Configure the related parameters of Phase 1.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Phase 1

Name: diavpn
Comments:
Remote Gateway: Dialup User
Local Interface: internal
Mode: ○ Aggressive ● Main (ID protection)
Authentication Method: Preshared Key
Pre-shared Key: •••••••••

Peer Options

● Accept any peer ID
○ Accept this peer ID
○ Accept peer ID in dialup group Guest-group

☑ **Enable IPsec Interface Mode**

IKE Version: ● 1 ○ 2
Mode Config: □
Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

1 - Encryption 3DES Authentication SHA1
2 - Encryption AES128 Authentication SHA1

Name: Set it to **dialvpn**. In interface mode, it is used to indicate the name of the VPN interface.

Remote Gateway: It is used to connect the dialup user.

Local Interface: It refers to the interface via which the firewall builds a VPN connection with the peer device. It is usually an extranet interface. Here, it is set to **wan1**.

Authentication Method: It is set to **Pre-shared Key**.

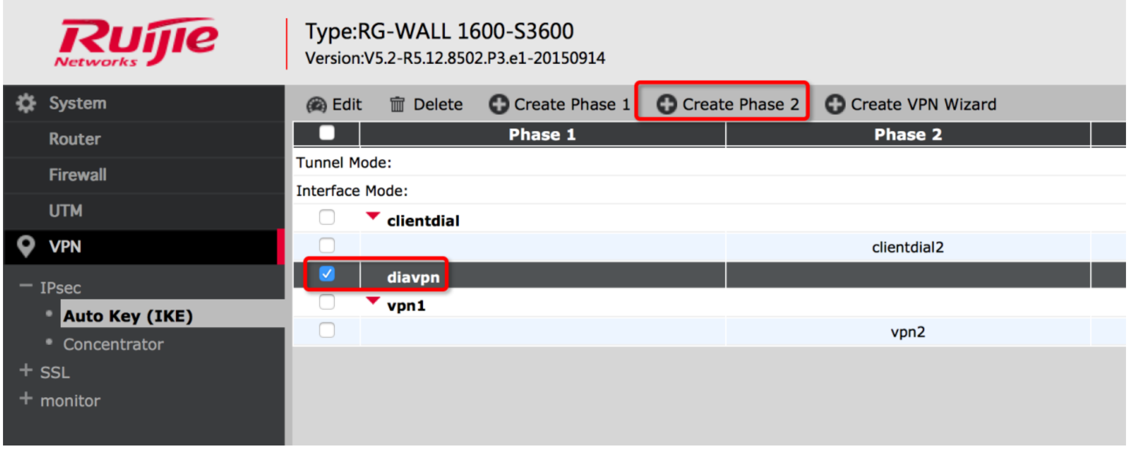
Pre-shared Key: It must be the same at both ends.

Enable IPsec Interface Mode: Ticked.

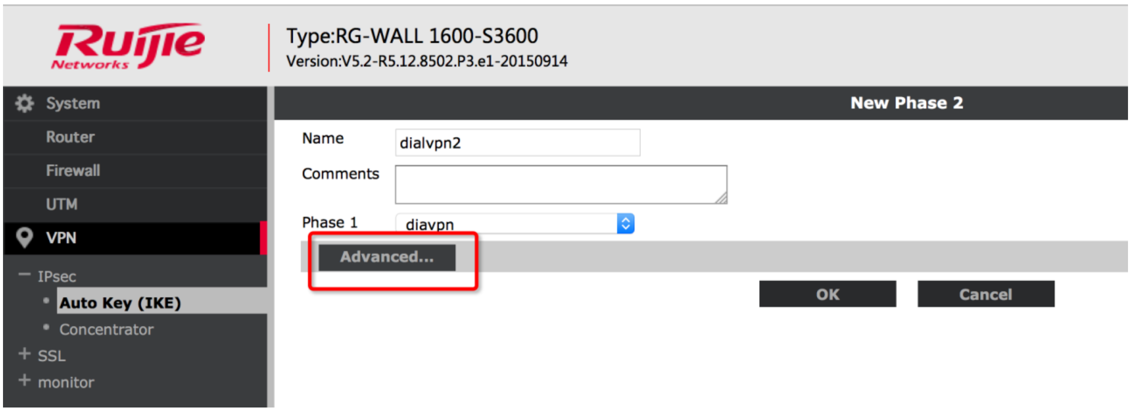
Other parameters are set to their default values. For details about the parameters, refer to section "Parameters of Phase 1".

3) Configure IKE Phase 2

Choose the **VPN > IPsec > Auto Key (IKE)** menu, and click **Create Phase 2**.



Configure the basic parameters of Phase 2.



Name: dialvpn2

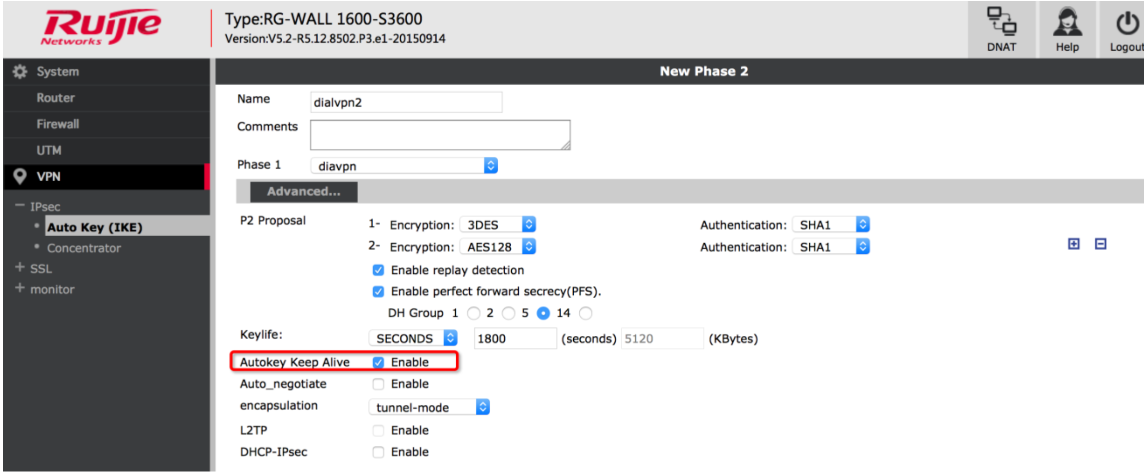
Comments:

Phase 1: diavpn

Name: It refers to the name of Phase 2, and is here set to **dialvpn2**.

Phase 1: It is associated with Phase 2, and is here set to **dialvpn**.

Click **Advanced**, and the advanced parameter options pop up.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Phase 2

Name: dialvpn2

Comments:

Phase 1: diavpn

P2 Proposal
1- Encryption: 3DES Authentication: SHA1
2- Encryption: AES128 Authentication: SHA1
☑ Enable replay detection
☑ Enable perfect forward secrecy(PFS).
DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)

Autokey Keep Alive ☑ Enable

Auto_negotiate □ Enable

encapsulation: tunnel-mode

L2TP □ Enable

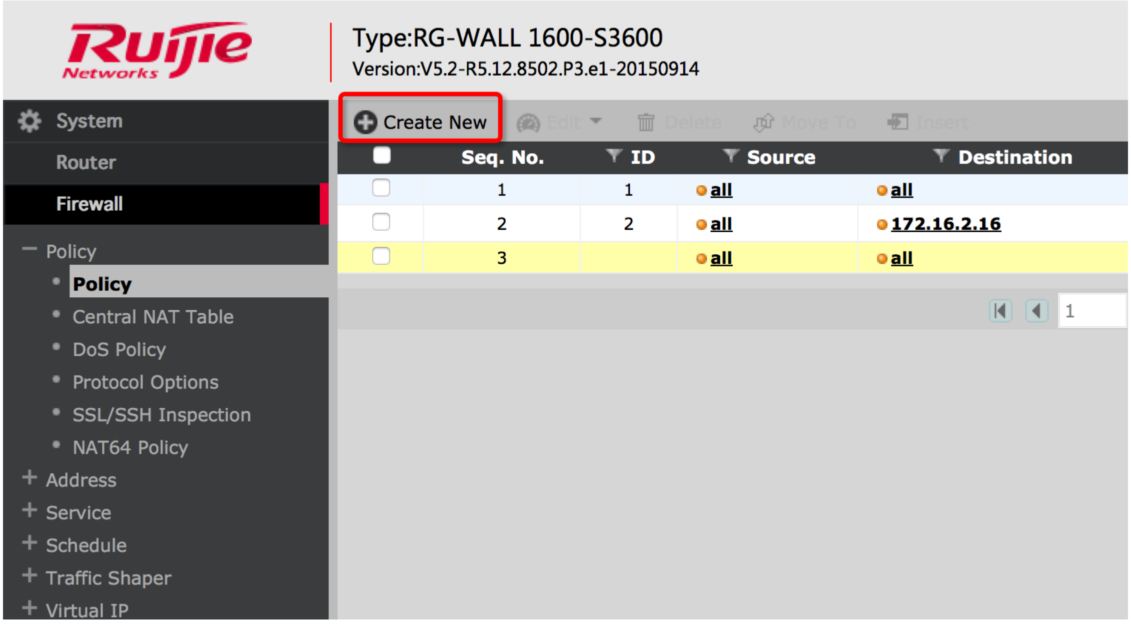
DHCP-IPsec □ Enable

Tick **Autokey Keep Alive**, and set other parameters to their default values.

Quick Mode Selector: Both the source address and destination address are set to their default values **0.0.0.0 0.0.0.0**.

4) Configure the IPSec policy

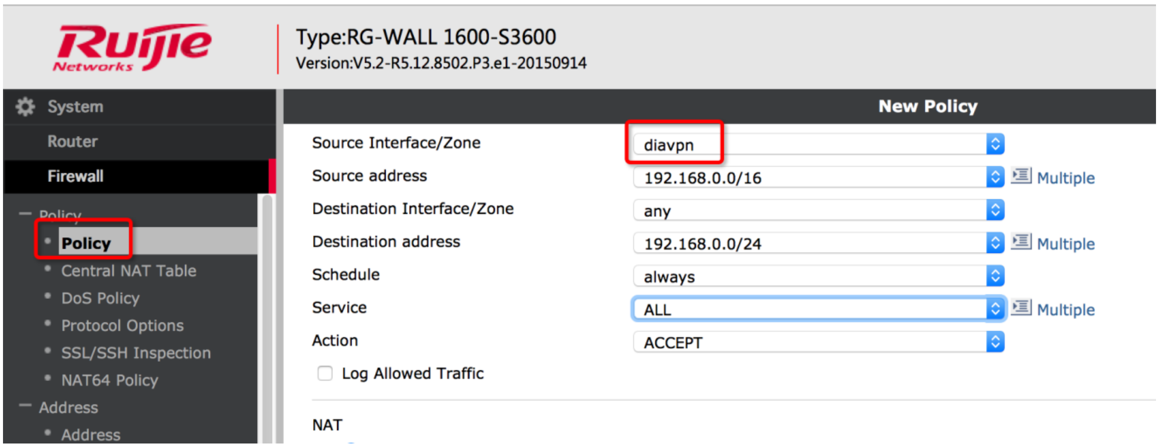
Choose the **Firewall** > **Policy** > **Policy** menu, and click **Create New**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

□	Seq. No.	ID	Source	Destination
□	1	1	all	all
□	2	2	all	172.16.2.16
□	3		all	all

Add an IPSec policy as shown below, allowing the external user 192.168.0.0/16 to access the network segment 192.168.0.0/24.



Source Interface/Zone: diavpn

Source address: 192.168.0.0/16

Destination Interface/Zone: any

Destination address: 192.168.0.0/24

Schedule: always

Service: ALL

Action: ACCEPT

□ Log Allowed Traffic

NAT

Source Interface/Zone: Select the new dialup VPN interface **dialvpn**.

5) Configure the route

You do not need to configure the hub-end firewall into the routing table of each branch office; instead, the system will generate the hub-end firewall automatically.

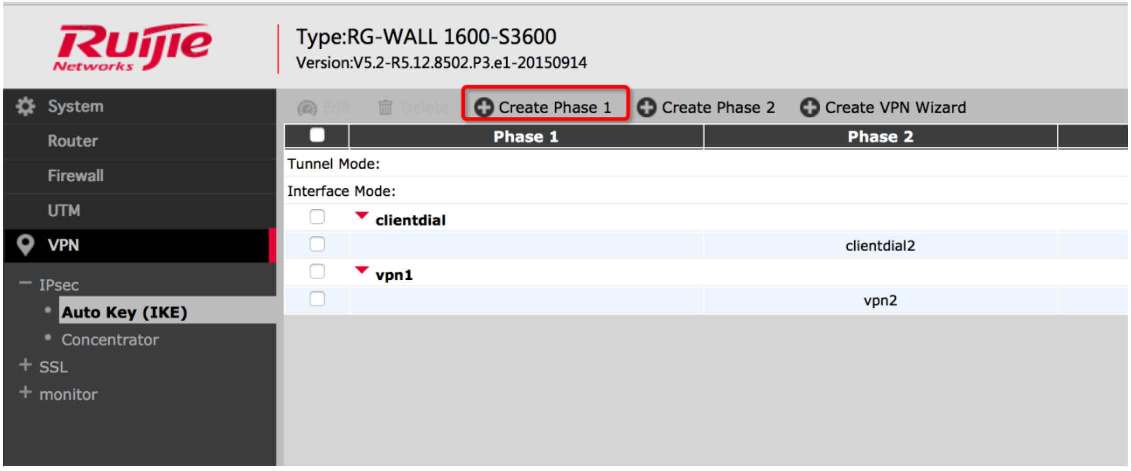
2. Configure NGFW-2

1) Perform basic configurations of Internet access

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

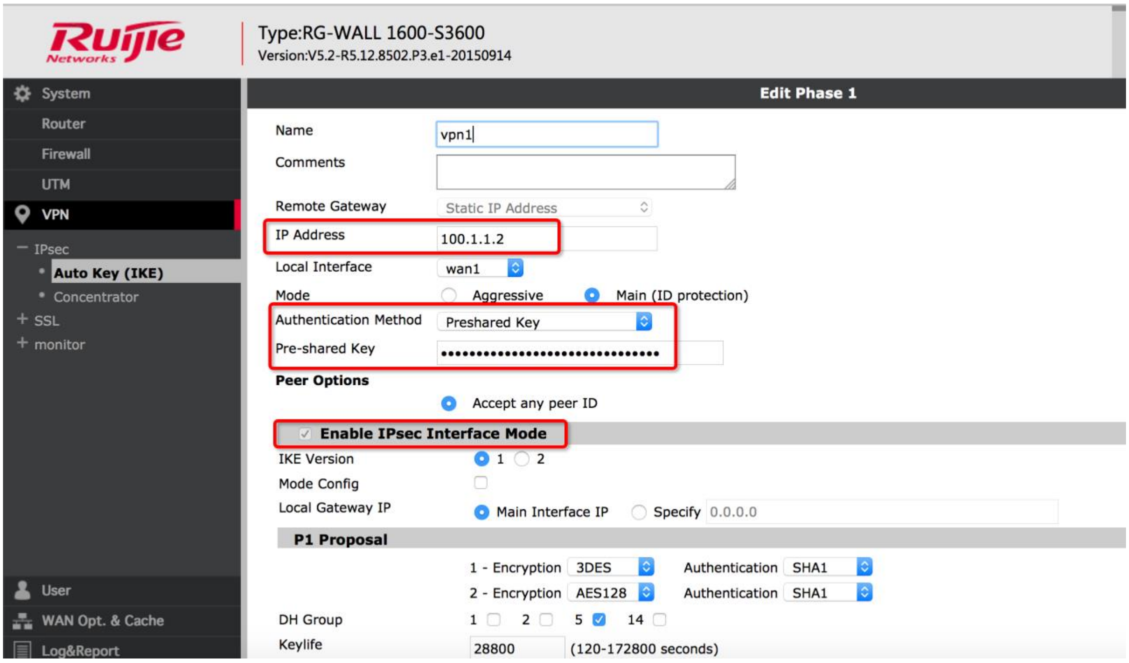
2) Configure IKE Phase 1

Choose the **VPN > IPsec > Auto Key (IKE)** menu, and click **Create Phase 1**.



□	Phase 1	Phase 2
Tunnel Mode:		
Interface Mode:		
□	clientdial	
□		clientdial2
□	vpn1	
□		vpn2

Configure the related parameters of Phase 1.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Phase 1

Name	vpn1
Comments	
Remote Gateway	Static IP Address
IP Address	100.1.1.2
Local Interface	wan1
Mode	○ Aggressive ● Main (ID protection)
Authentication Method	Preshared Key
Pre-shared Key	••••••••••••••••••••••••••••••

Peer Options

● Accept any peer ID

☑ Enable IPsec Interface Mode

IKE Version	● 1 ○ 2
Mode Config	□
Local Gateway IP	● Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

	1 - Encryption	3DES	Authentication	SHA1
	2 - Encryption	AES128	Authentication	SHA1
DH Group	1 □ 2 □ 5 ☑ 14 □			
Keylife	28800	(120-172800 seconds)		

Name: Set it to **VPN**. In interface mode, it is used to indicate the name of the VPN interface.

Remote Gateway: Set it to **Static IP Address**.

IP Address: The IP address of the extranet interface of the peer firewall is 100.1.1.2.

Local Interface: It refers to an interface via which the firewall builds a VPN connection with the peer device; it is here set to **wan1**.

Authentication Method: It is set to **Pre-shared Key**.

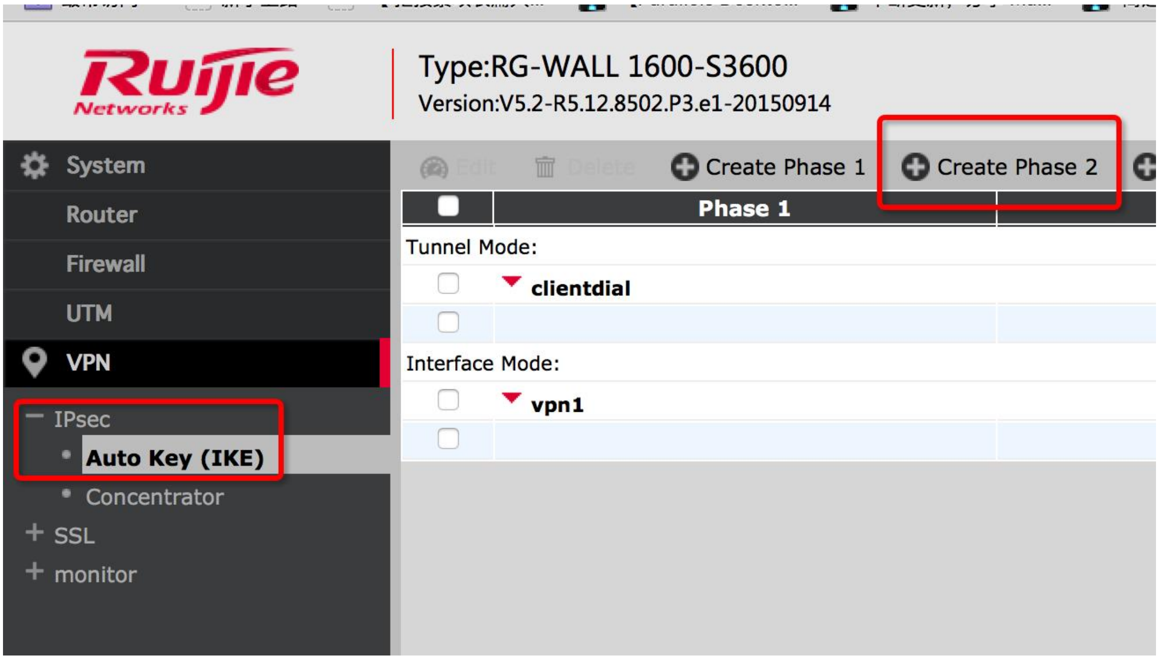
Pre-shared Key: It must be the same at both ends.

Enable IPsec Interface Mode: Ticked.

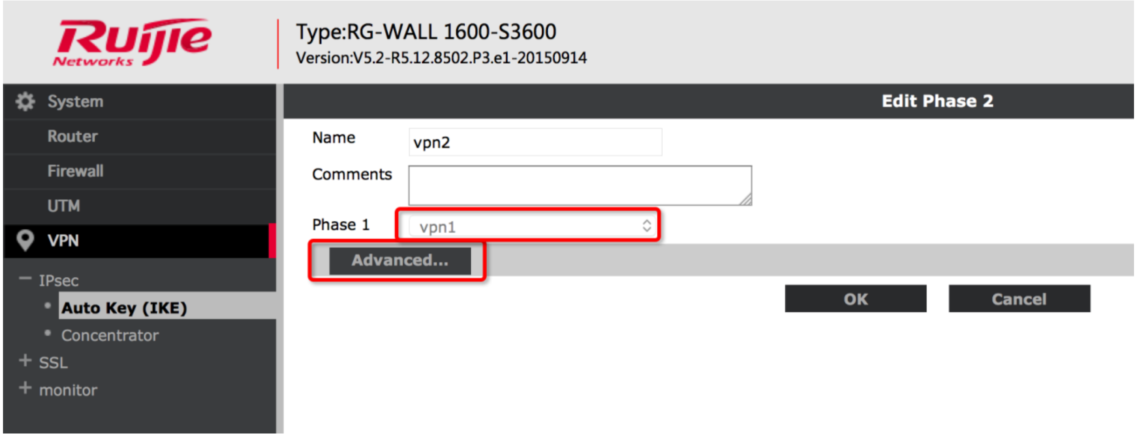
Other parameters are set to their default values. For details about the parameters, refer to section “Parameters of Phase 1”.

3) IKE Phase 2

Choose the **VPN** > **IPsec** > **Auto Key (IKE)** menu, and click Create Phase 2.



Configure the basic parameters of Phase 2.



Name: vpn2

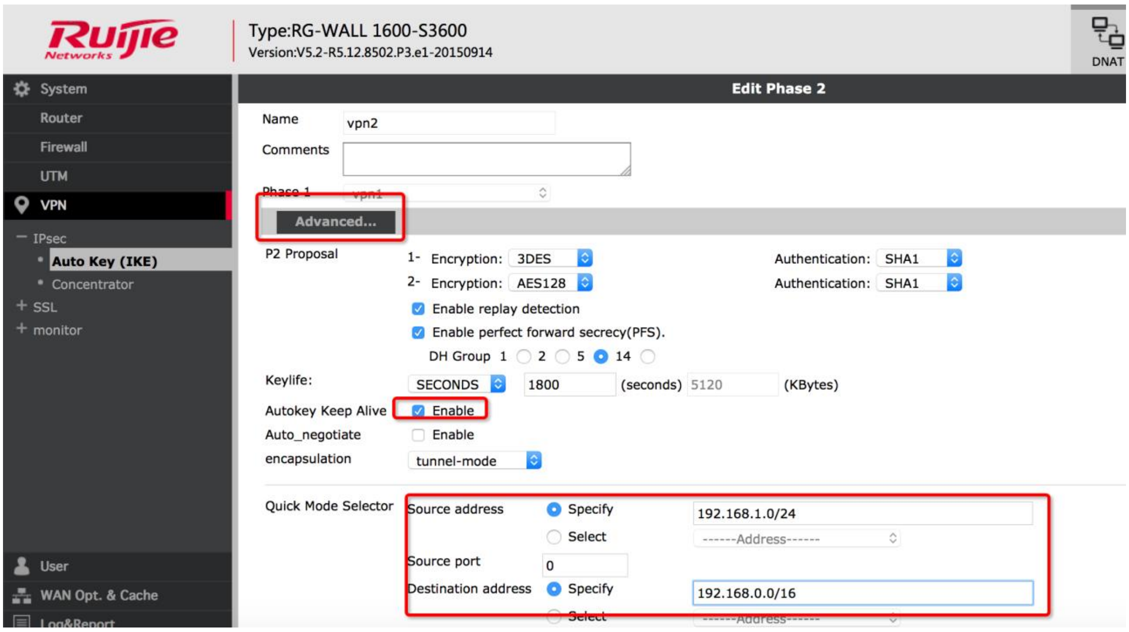
Comments:

Phase 1: vpn1

Name: It refers to the name of Phase 2, and is here set to **vpn2**.

Phase 1: It is associated with Phase 2, and is here set to **vpn**.

Click **Advanced**, and the advanced parameter options pop up.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Phase 2

Name: vpn2
Comments:
Phase 1: vpn1
Advanced...

P2 Proposal
1- Encryption: 3DES Authentication: SHA1
2- Encryption: AES128 Authentication: SHA1
☑ Enable replay detection
☑ Enable perfect forward secrecy(PFS).
DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)
Autokey Keep Alive ☑ Enable
Auto_negotiate □ Enable
encapsulation tunnel-mode

Quick Mode Selector
Source address ● Specify 192.168.1.0/24
○ Select ------Address------
Source port 0
Destination address ● Specify 192.168.0.0/16
○ Select ------Address------

Tick **Autokey Keep Alive**, and set other parameters to their default values.

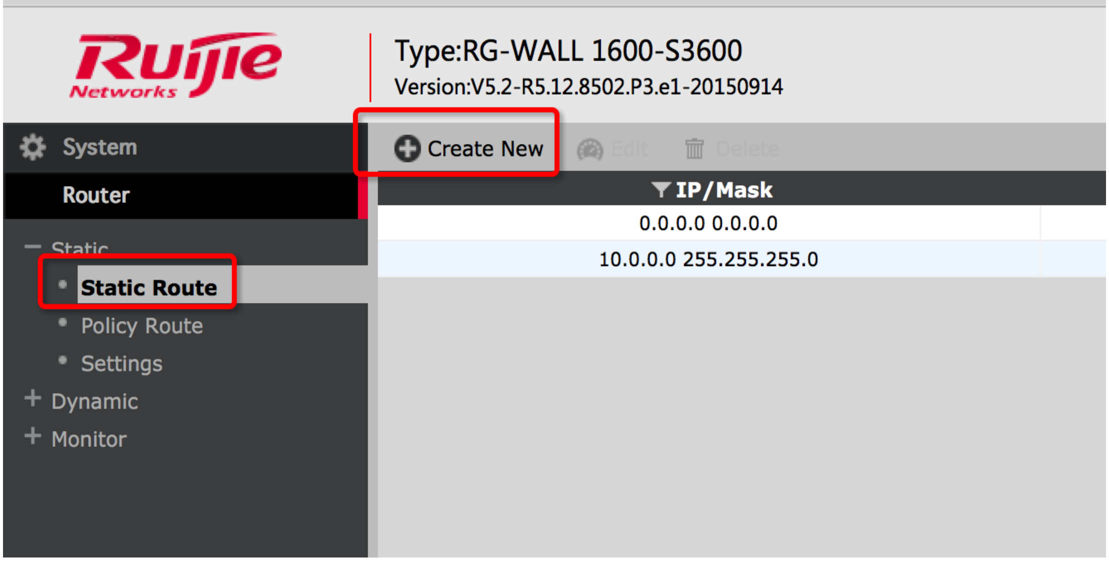
Source Address: It refers to the locally protected subnet.

Destination address: It refers to the network segment accessed via the VPN.

The destination IP address mask of the static route can comprise 16 or 24 bits; in this scenario, the branch offices can communicate with each other if it comprises 16 bits; the branch offices can access the network segment 0 of the headquarters if it comprises 24 bits.

4) Configure the route

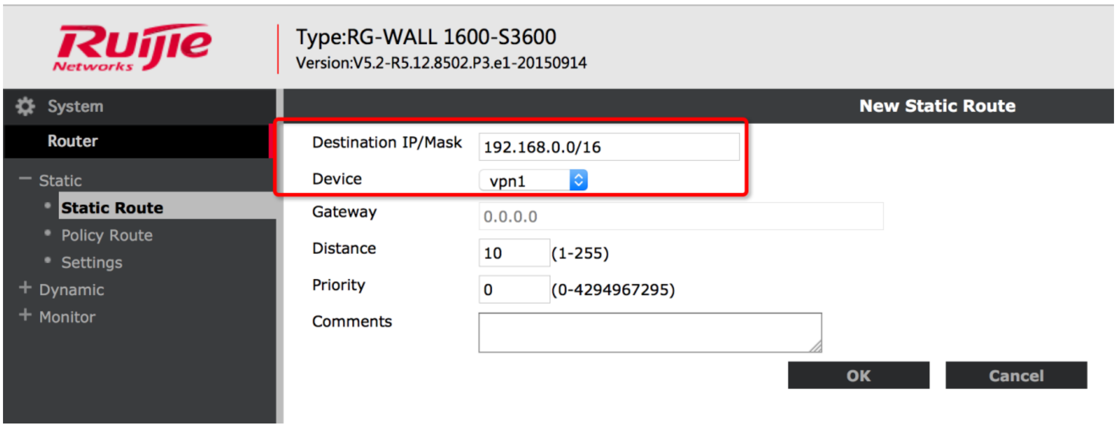
Choose the **Route** > **Static** > **Static Route** menu, and click **Create New**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

IP/Mask
0.0.0.0 0.0.0.0
10.0.0.0 255.255.255.0

Add the VPN route of the protected network segment on the peer as follows:



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Static Route

Destination IP/Mask: 192.168.0.0/16
Device: vpn1
Gateway: 0.0.0.0
Distance: 10 (1-255)
Priority: 0 (0-4294967295)
Comments:

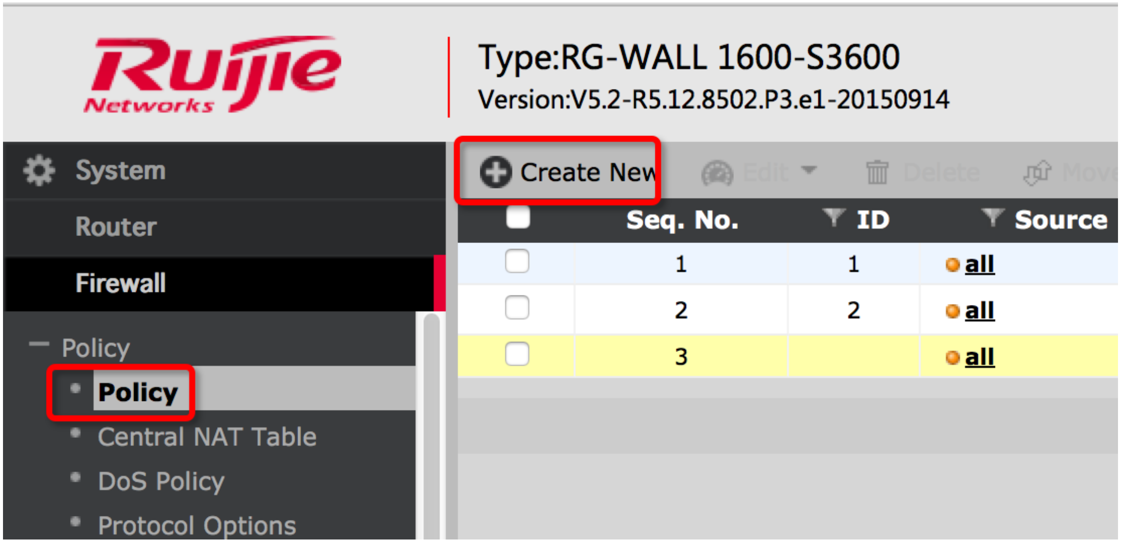
Destination IP/Mask: It refers to the subnet protected by the peer firewall; here, it is set to 192.168.1.0/16.

Device: It refers to the interface generated by the VPN; here, it is set to **vpn**.

The destination IP address mask of the static route can comprise 16 or 24 bits; in this scenario, the branch offices can communicate with each other if it comprises 16 bits; the branch offices can access the network segment 0 of the headquarters if it comprises 24 bits.

5) **Configure the IPSec policy**

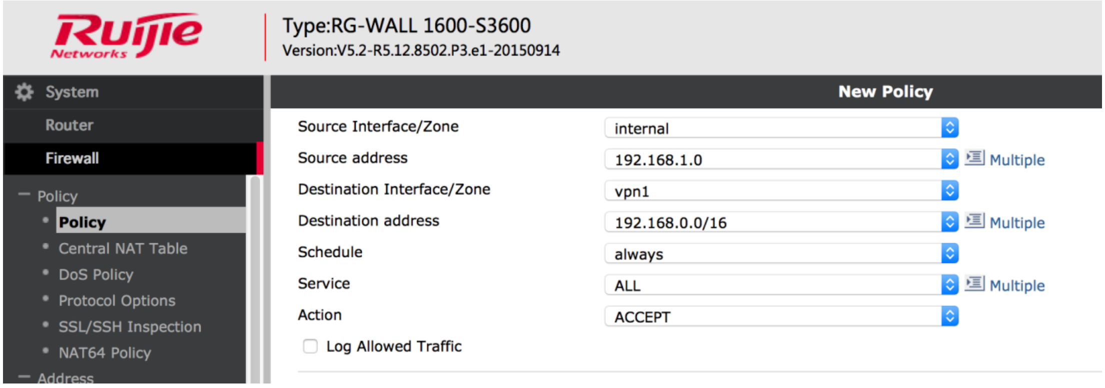
Choose the **Firewall** > **Policy** > **Policy** menu, and click **Create New**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

□	Seq. No.	ID	Source
□	1	1	all
□	2	2	all
□	3		all

Create a security policy as follows:



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Policy

Source Interface/Zone	internal
Source address	192.168.1.0
Destination Interface/Zone	vpn1
Destination address	192.168.0.0/16
Schedule	always
Service	ALL
Action	ACCEPT

□ Log Allowed Traffic

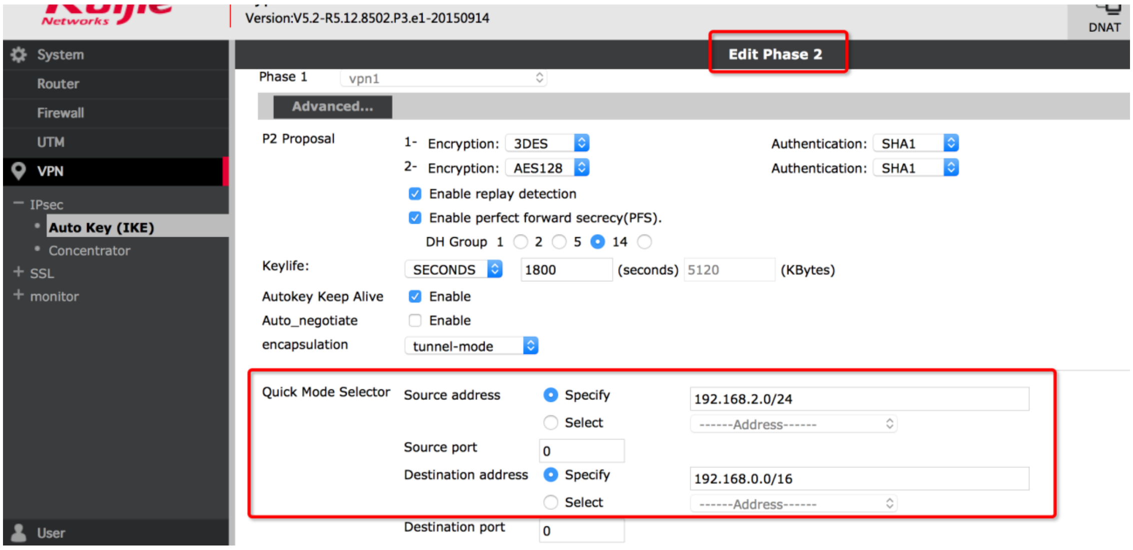
Source Address: 192.168.1.0/24 can access other network segments.

Destination Address: It can be **192.168.0.0/16** or **192.168.0.0/24**. Then, the user is allowed to access only the network segment protected by NGFW1, but not the network segments of other branch offices, for example, 192.168.2.0/24.

3. Configure other spoke node devices.

By reference to the configurations of NGFW2, adjust the related parameters according to the local private network segment.

When editing Phase 2 of IPsec, modify the Source Address of the quick mode selector. For example, the related configurations of NGFW3 are as follows:



Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Phase 2

Phase 1: vpn1

P2 Proposal
1- Encryption: 3DES Authentication: SHA1
2- Encryption: AES128 Authentication: SHA1
☑ Enable replay detection
☑ Enable perfect forward secrecy(PFS).
DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)

Autokey Keep Alive ☑ Enable

Auto_negotiate □ Enable

encapsulation: tunnel-mode

Quick Mode Selector
Source address ● Specify 192.168.2.0/24
○ Select ------Address------
Source port 0
Destination address ● Specify 192.168.0.0/16
○ Select ------Address------
Destination port 0

3.7.3 SSL VPN

3.7.3.1 Configuration Tips

I. Configuration Steps

1. Configure SSL: a. Define SSL VPN server port. b. Define the address pool of the SSL VPN client.

2. Configure SSL Portal: Define the SSL VPN access mode: tunnel or Web proxy (which can be enabled at the same time). Choose "**Enable Split Tunneling**" in tunnel mode, and the client will obtain the detailed route; otherwise, the client will obtain the default route.

3. Set the action to SSL VPN firewall policy, no matter it is in tunnel mode or Web proxy mode.

a. Source interface and address of the policy: Check the traffic of SSL VPN. Only the traffic matching the source interface and address can pass SSL VPN authentication.

b. Destination interface and address of the policy: Specify the destination address that SSL VPN users can access and the route available to the client (when enabling tunnel splitting, do not set the destination address to all).

c. SSL VPN user: Enable user authentication. Users who pass authentication can access destination resources. When there are multiple SSL VPN policies, match these policies from top to down (match only the source interface, source address, and user). Different SSL VPN policies can be applied to different users.

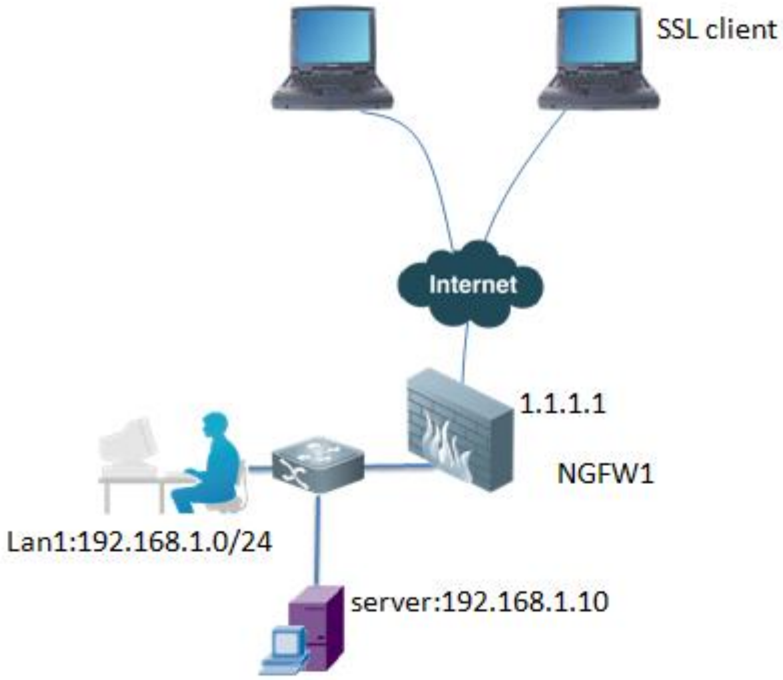
d. When there are two or more SSL VPN policies, for example, one in tunnel mode and the other in Web proxy mode, if they have the same source interface, source address, and SSL VPN user, the SSL VPN user can log in only one of the two modes, which depends on the priority. First match the policy prior to the other, and stop further matching if it succeeds.

3.7.3.2 SSL VPN Client Mode

Networking Requirements

As shown in the figure, a company is internally fitted with an OA server, and to access the OA server, the employees outside the company need to first log in to its intranet via a SSL VPN client.

Network Topology



Configuration Tips

1. Perform basic configurations of Internet access;
2. Configure the users;
3. Configure the SSL VPN;
4. Configure the policies;
5. Configure the PC SSL client.

Configuration Steps

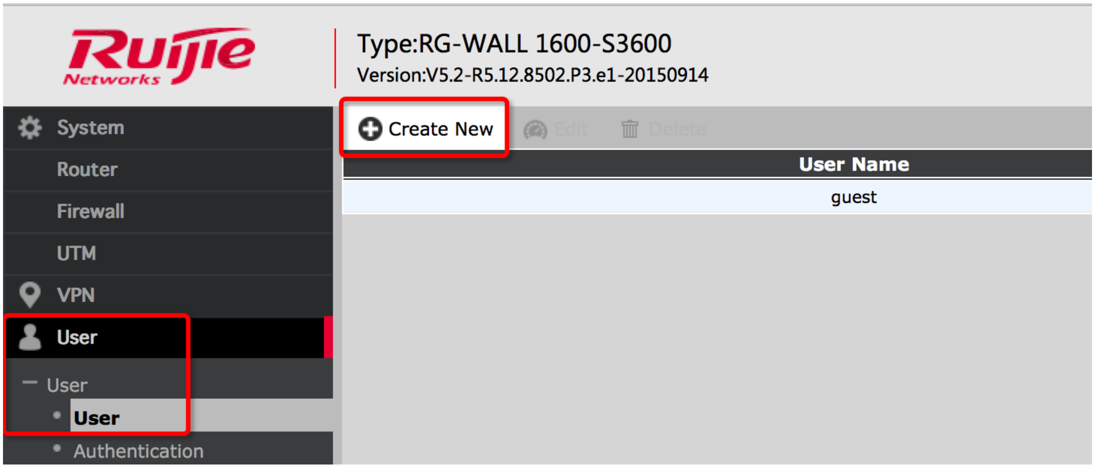
1. Perform basic configurations of Internet access

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

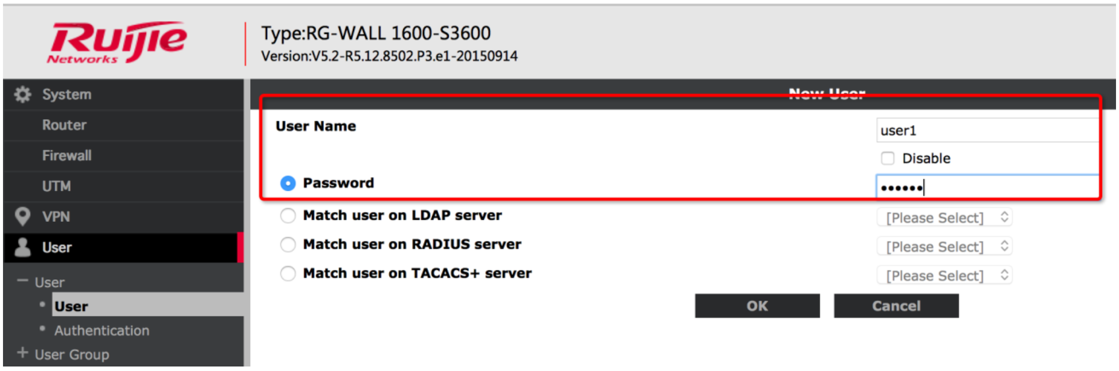
2. Configure the user

1) Define the user

Choose the **User** > **User** > **User** menu, and click **Create New**.



Add the user name **user1** and password **11111111**.



User Name: user1

□ Disable

● Password: ••••••

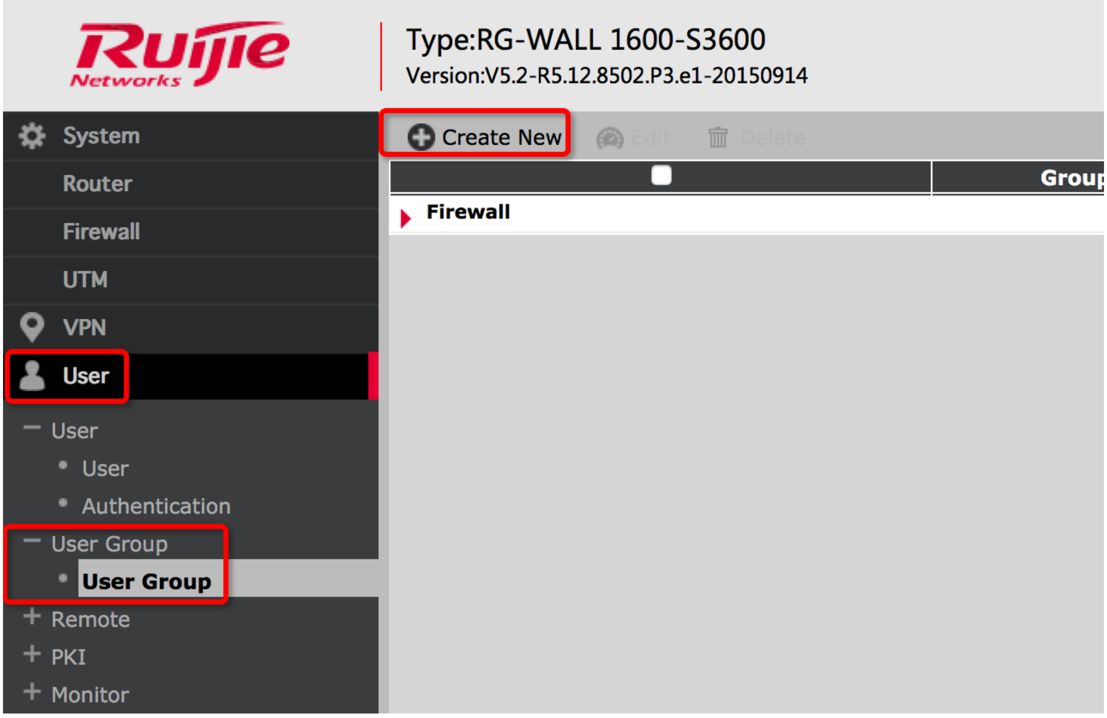
○ Match user on LDAP server [Please Select]

○ Match user on RADIUS server [Please Select]

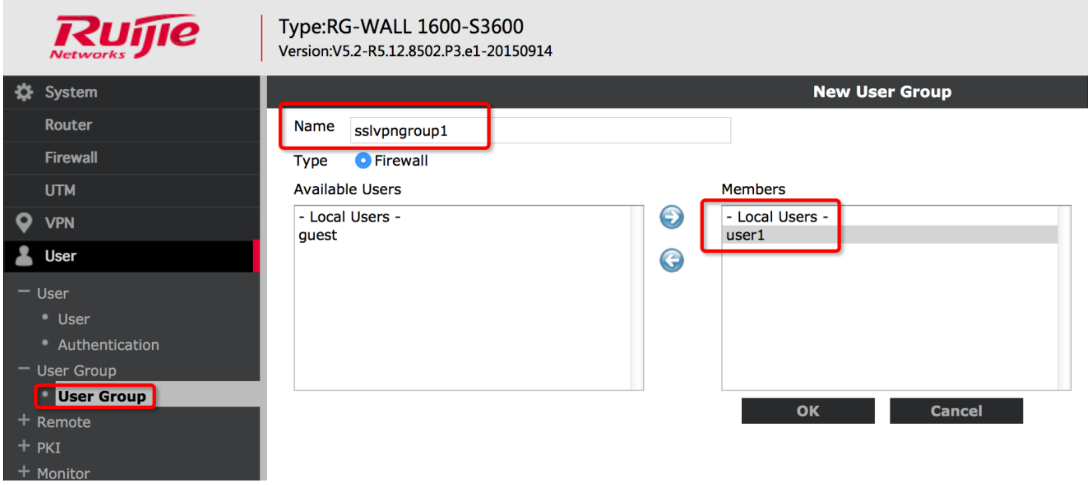
○ Match user on TACACS+ server [Please Select]

2) Define the user group

Choose the **User** > **User Group** > **User Group** menu, and click **Create New**.



Add the user group **sslvpngroup1**, and add the user **user1** to the user group.



Name sslvpngroup1

Type ● Firewall

Available Users

- Local Users -
guest

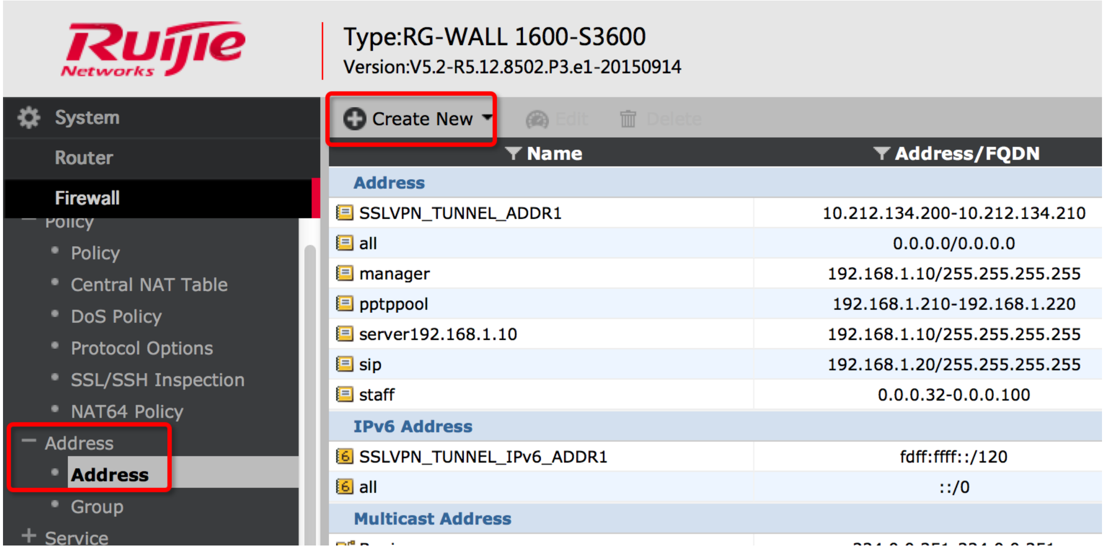
Members

- Local Users -
user1

3. Configure the SSL VPN

1) Create the SSL VPN user address pool;

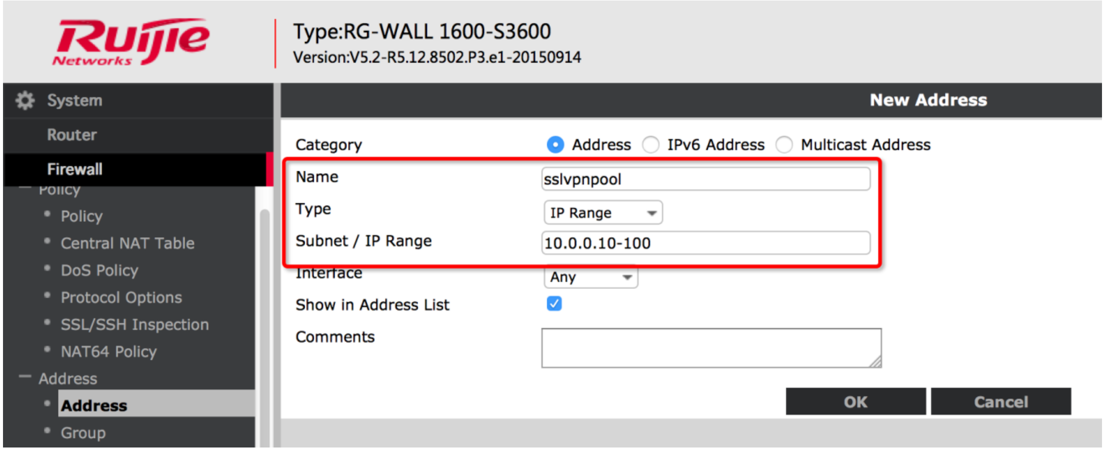
Choose the **Firewall** > **Address** > **Address** menu, and click **Create New**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Name	Address/FQDN
Address	
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210
all	0.0.0.0/0.0.0.0
manager	192.168.1.10/255.255.255.255
pptppool	192.168.1.210-192.168.1.220
server192.168.1.10	192.168.1.10/255.255.255.255
sip	192.168.1.20/255.255.255.255
staff	0.0.0.32-0.0.0.100
IPv6 Address	
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120
all	::/0
Multicast Address	

Add the SSL VPN address pool as shown below:



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	sslvpnpool
Type	IP Range
Subnet / IP Range	10.0.0.10-100
Interface	Any
Show in Address List	☑
Comments	

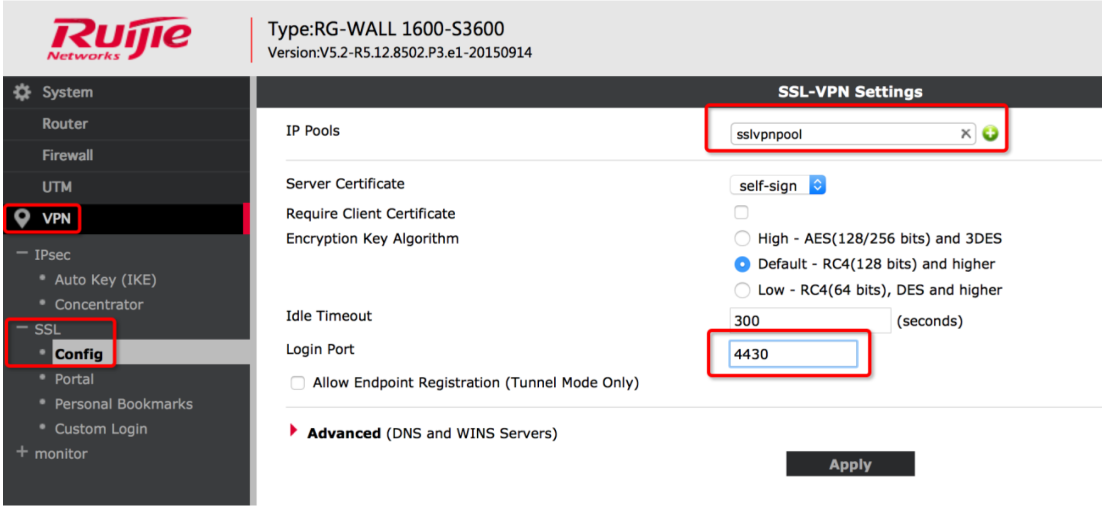
Type: Select **IP Range** (you must select **IP Range** rather than **Subnet**).

Subnet / IP Range: Set it to **10.0.0.10** to **10.0.0.100**.

2) Configure the SSL parameters;

Choose the **VPN** > **SSL** > **Config** menu.

Configure the SSL parameters as shown below.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

SSL-VPN Settings

IP Pools: sslvpnpool

Server Certificate: self-sign

Require Client Certificate: □

Encryption Key Algorithm:
○ High - AES(128/256 bits) and 3DES
● Default - RC4(128 bits) and higher
○ Low - RC4(64 bits), DES and higher

Idle Timeout: 300 (seconds)

Login Port: 4430

□ Allow Endpoint Registration (Tunnel Mode Only)

Advanced (DNS and WINS Servers)

IP Pools: It refers to the address range allocated to the user. IP Pools is usually defined on the SSL interface.

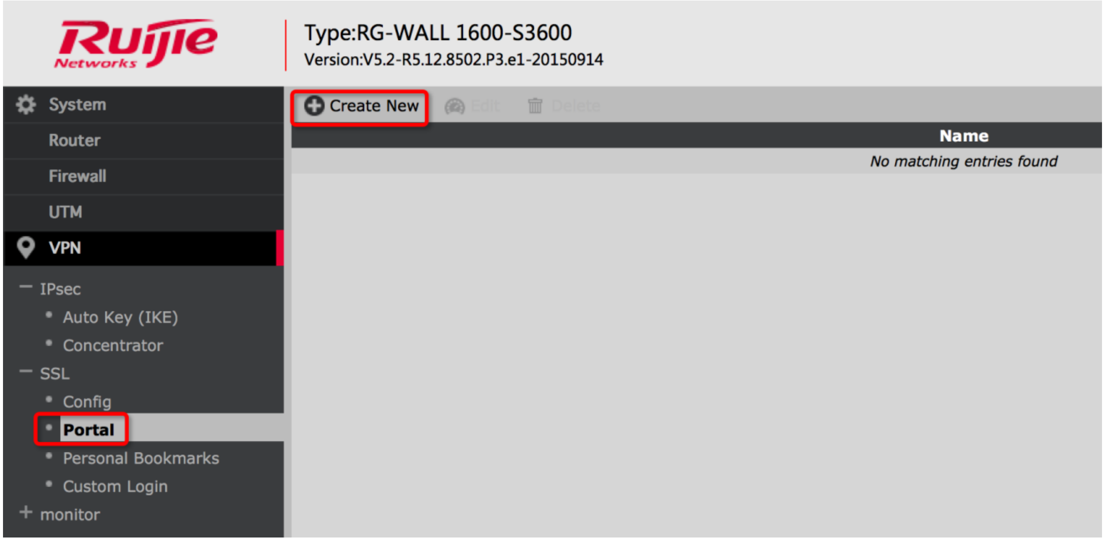
Server Certificate: It is usually set to **Self-sign**. Enterprises can also set it to their proprietary **Local Certificate**.

Login Port: It refers to the port for accessing the SSL VPN. The default value is **443**. If the HTTPS service is enabled for interfaces, this port will conflict with the login port. Then, you can modify the management port of the HTTPS service or modify the login port as another port, for example, **4430**.

DNS Server and WINS Server: If you need to use a domain name to access internal resources, you need to configure an internal DNS.

3) Configure the SSL interface.

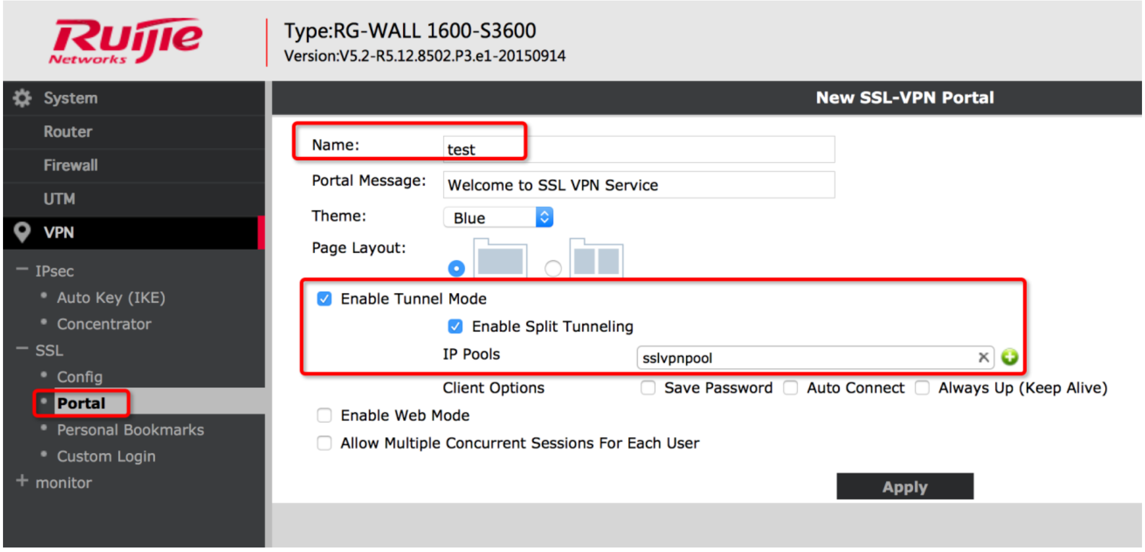
Choose the **VPN** > **SSL** > **Interface** menu, and **Create New**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Name
No matching entries found

You can define the SSL interface specific to the user group, and define whether the address pool allocated to each user group supports the channel mode, thus facilitating policy control.



Name: test

Portal Message: Welcome to SSL VPN Service

Theme: Blue

Page Layout: ● ○

☑ Enable Tunnel Mode

☑ Enable Split Tunneling

IP Pools sslvpnpool

Client Options □ Save Password □ Auto Connect □ Always Up (Keep Alive)

□ Enable Web Mode

□ Allow Multiple Concurrent Sessions For Each User

Name: It is self-defined, and is here set to **test**.

Theme: It refers to the style of the login page.

Page Layout: It refers to the layout of the page.

Enable Tunnel Mode: If it is ticked, the client obtains an IP address from the firewall, and builds a secure VPN channel with the firewall, so as to access internal network resources.

Enable Split Tunneling: Traffic is sent to the SSL VPN channel only when the client accesses internal resources; other network traffic is still transmitted through the local connection. After the client dials into the VPN, the client still accesses Internet resources via the local network.

The internal network segment needs to be configured when you configure the SSL VPN policy.

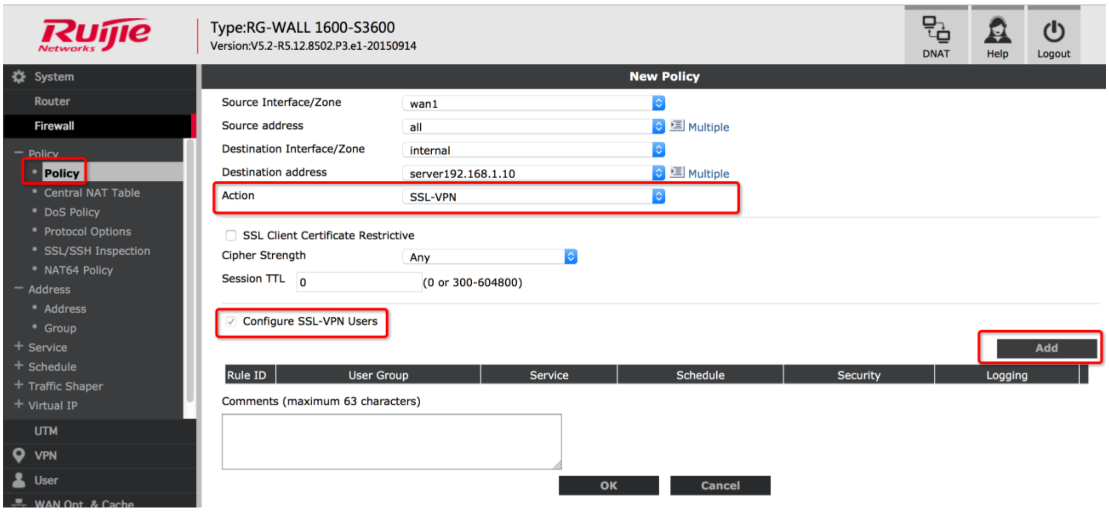
IP Pools: It refers to the IP address range allocated to each client; it is here set to **sslvpnpool**.

4. Configure the SSL policy

1) Configure the allowing policies

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

The policy is configured as follows:



New Policy

Source Interface/Zone: wan1
Source address: all
Destination Interface/Zone: internal
Destination address: server192.168.1.10
Action: SSL-VPN
□ SSL Client Certificate Restrictive
Cipher Strength: Any
Session TTL: 0 (0 or 300-604800)
☑ Configure SSL-VPN Users
Comments (maximum 63 characters)

Source Interface: It is used to receive a SSL request.

Source Address: It is here set to **all**, indicating that all IP addresses are allowed to perform the SSL connection.

Destination Interface / Zone: It refers to an intranet interface accessed via the SSL VPN.

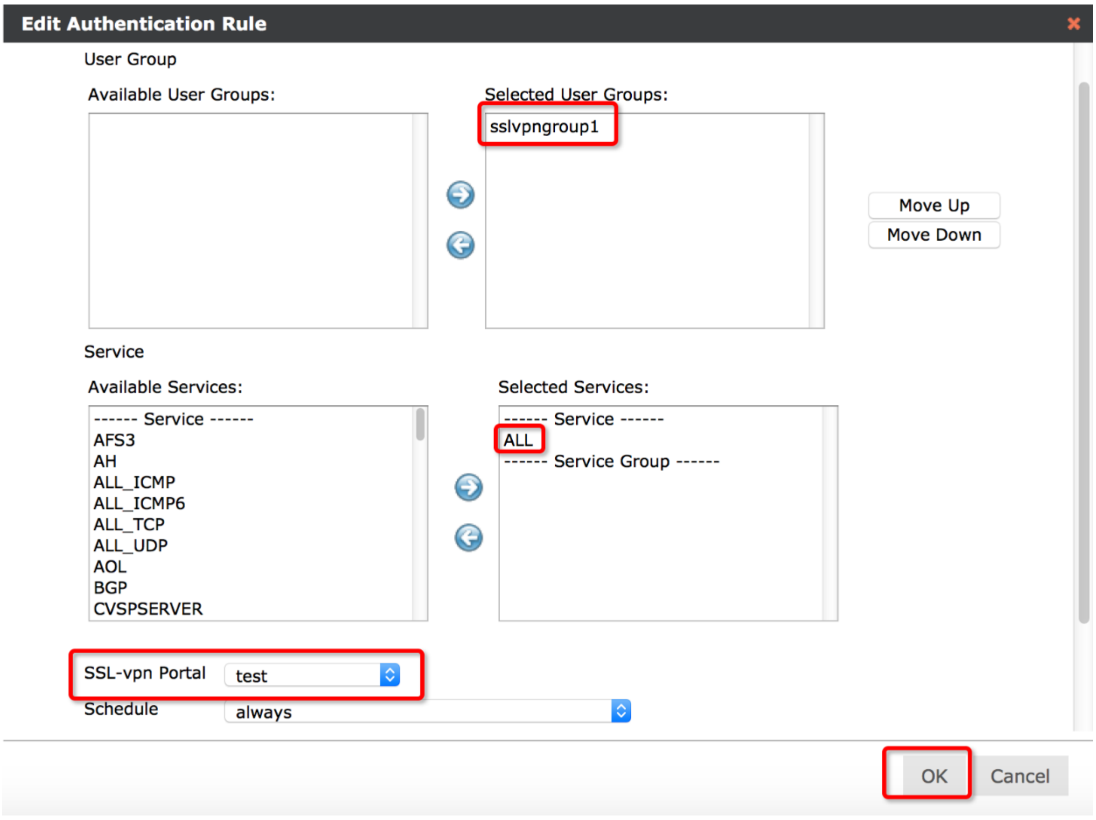
Destination Address: It refers to an internal address that is accessed.

Action: It is here set to **SSLVPN**.

Configure SSL-VPN Users: Tick it to add a user group and interface.

2) Add users to the SSL policy. Click **Add**, and the following box pops up.

Add the related user group, services and interface portal for the SSL VPN.



Edit Authentication Rule

User Group

Available User Groups:

Selected User Groups: sslvpngroup1

Service

Available Services:
------ Service ------
AFS3
AH
ALL_ICMP
ALL_ICMP6
ALL_TCP
ALL_UDP
AOL
BGP
CVSPSERVER

Selected Services:
------ Service ------
ALL
------ Service Group ------

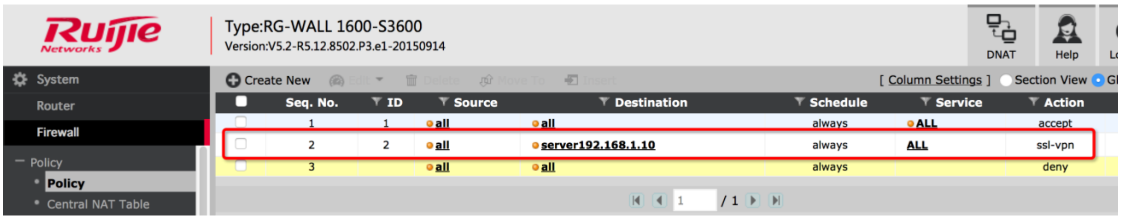
SSL-vpn Portal: test
Schedule: always

User Group: It refers to the user group who is allowed to log in to the VPN. Here, select **sslvpngroup1**.

Service: Select **ALL**.

SSL-vpn Portal: It refers to an SSL interface allocated to the user group. Here, select **test**.

Click **OK** to complete the policy configurations.

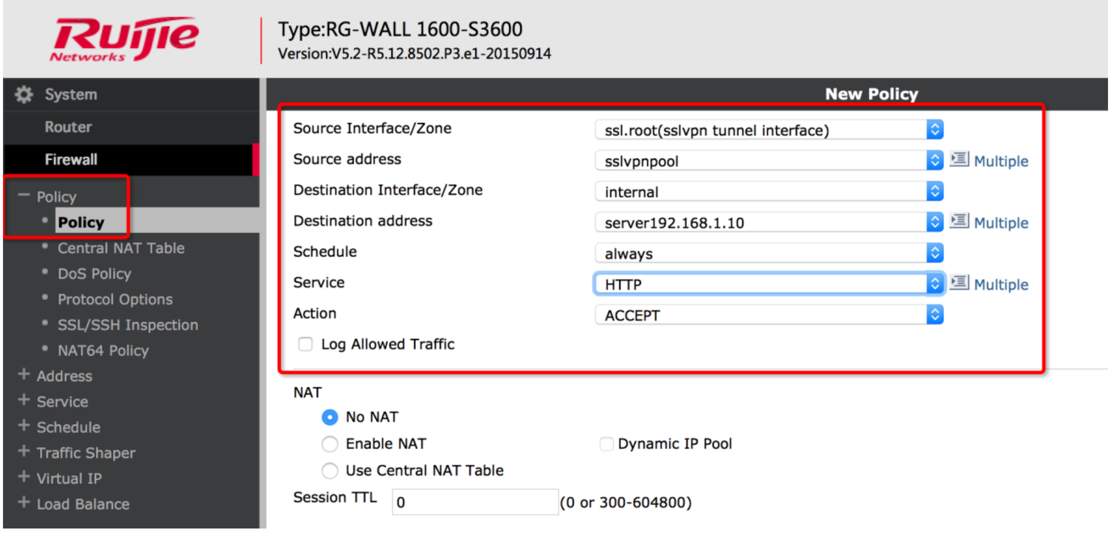


Seq. No.	ID	Source	Destination	Schedule	Service	Action
1	1	all	all	always	ALL	accept
2	2	all	server192.168.1.10	always	ALL	ssl-vpn
3		all	all	always		deny

3) Add the OA server address

For details about the configuration procedure, refer to section 1) under 3. The name is **OAserver192.168.1.10** and the address is 192.168.1.10/32.

4) Configure the access policy for the users in channel mode



Source Interface/Zone	ssl.root(sslvpn tunnel interface)
Source address	sslvpnpool
Destination Interface/Zone	internal
Destination address	server192.168.1.10
Schedule	always
Service	HTTP
Action	ACCEPT

□ Log Allowed Traffic

NAT

● No NAT

○ Enable NAT　　□ Dynamic IP Pool

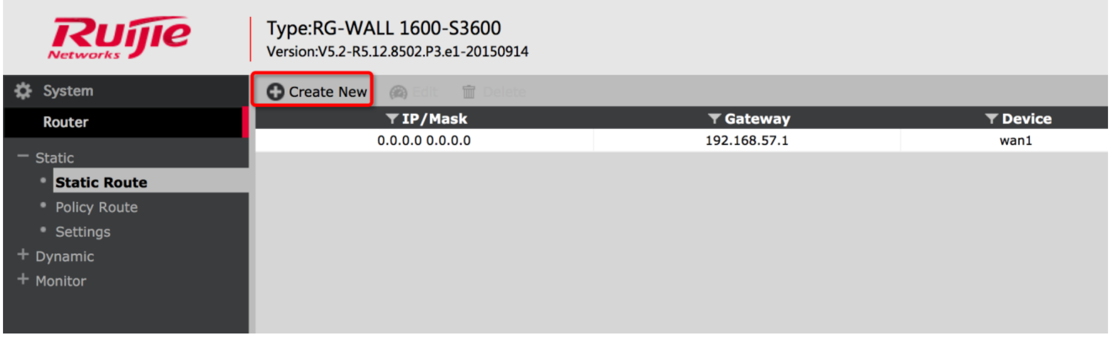
○ Use Central NAT Table

Session TTL 0 (0 or 300-604800)

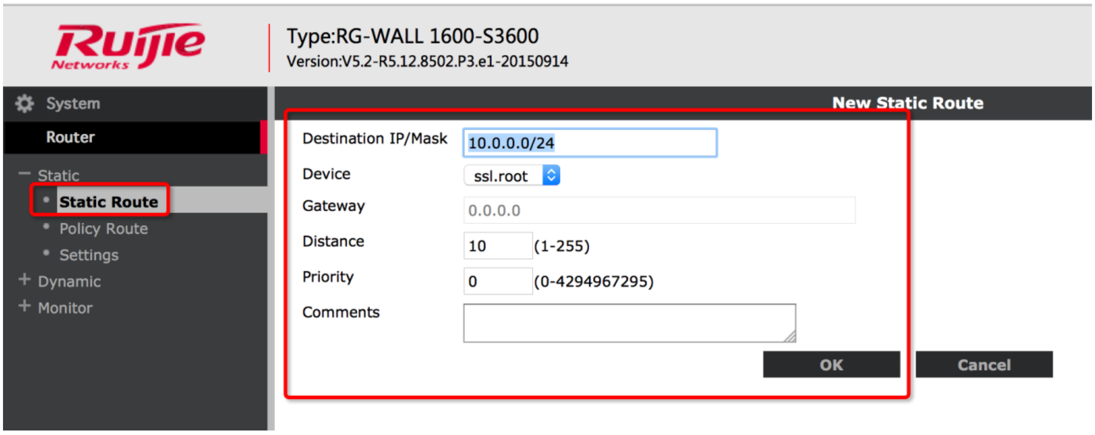
Only the SSL users are allowed to access the OAserver192.168.1.10 in the intranet via tunnels.

5. Configure the routes

Direct the routing table of the SSL user address pools to the ssl.root interface.



IP/Mask	Gateway	Device
0.0.0.0 0.0.0.0	192.168.57.1	wan1



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Static Route

Destination IP/Mask: 10.0.0.0/24
Device: ssl.root
Gateway: 0.0.0.0
Distance: 10 (1-255)
Priority: 0 (0-4294967295)
Comments:

Destination IP / Mask: It refers to the network segment of the SSL user address pools. Here, it is set to **10.0.0.0/24**.

Device: Select the **ssl.root** interface.

Set other parameters to their default values. Click **OK**.

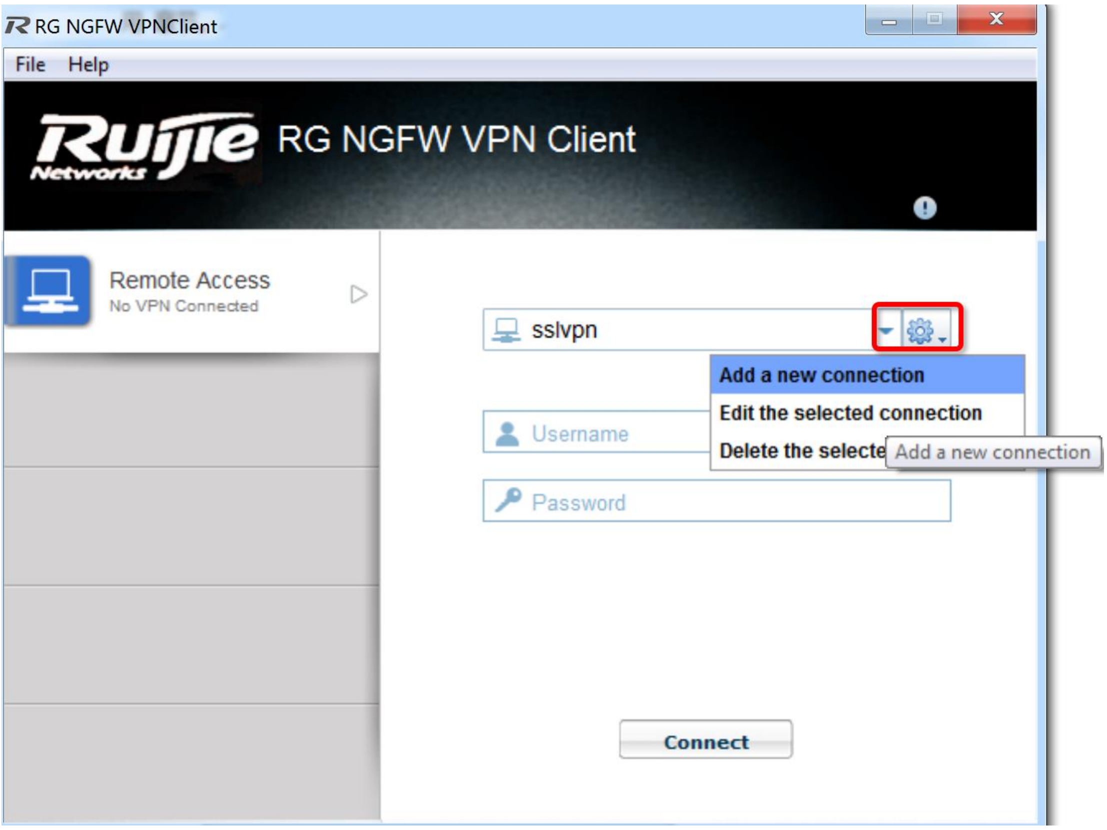
V. Configuring the SSL Client

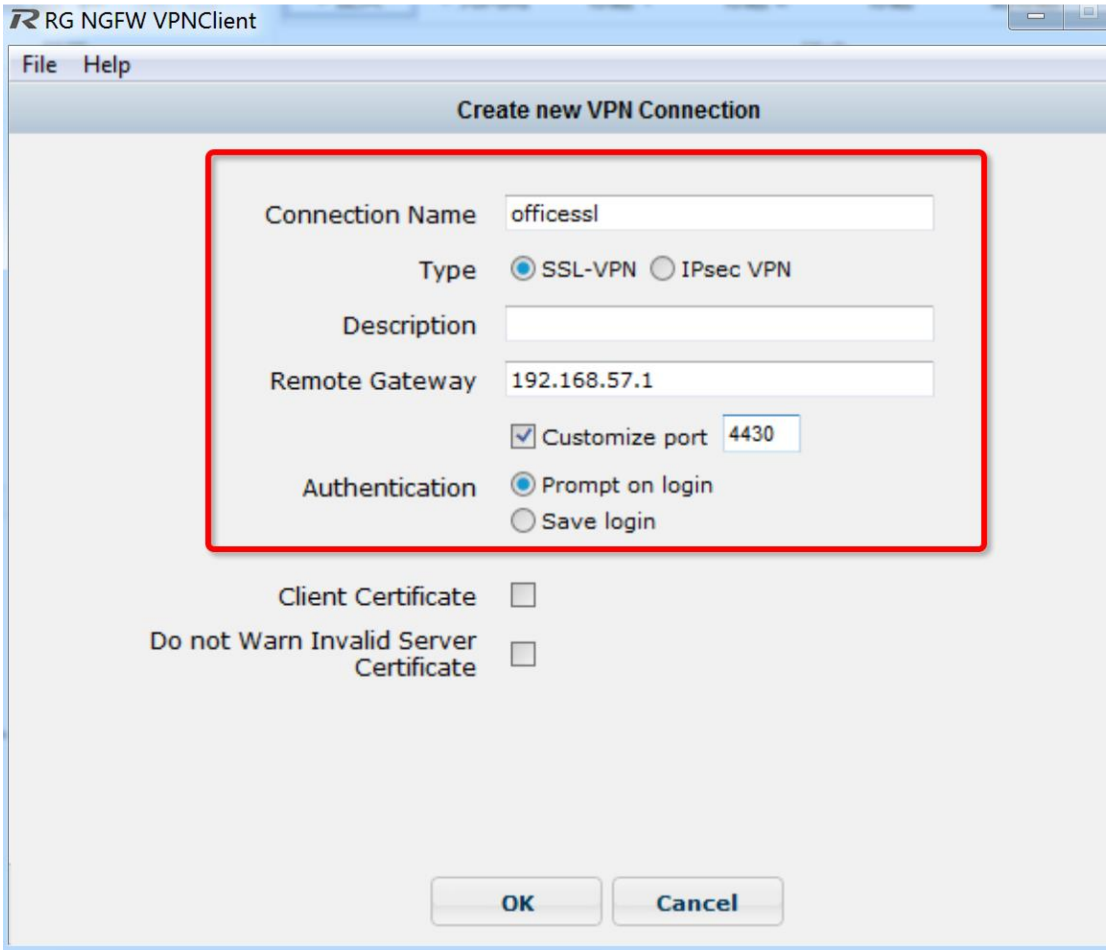
a) Install the SSL VPN client

The current client supports the 32/64-bit Windows system. For details, refer to the sections “Release Note” and “Installation and Use” under “VPN Client”.

b) Create a SSL-VPN connection

Select a type of new SSL VPN.

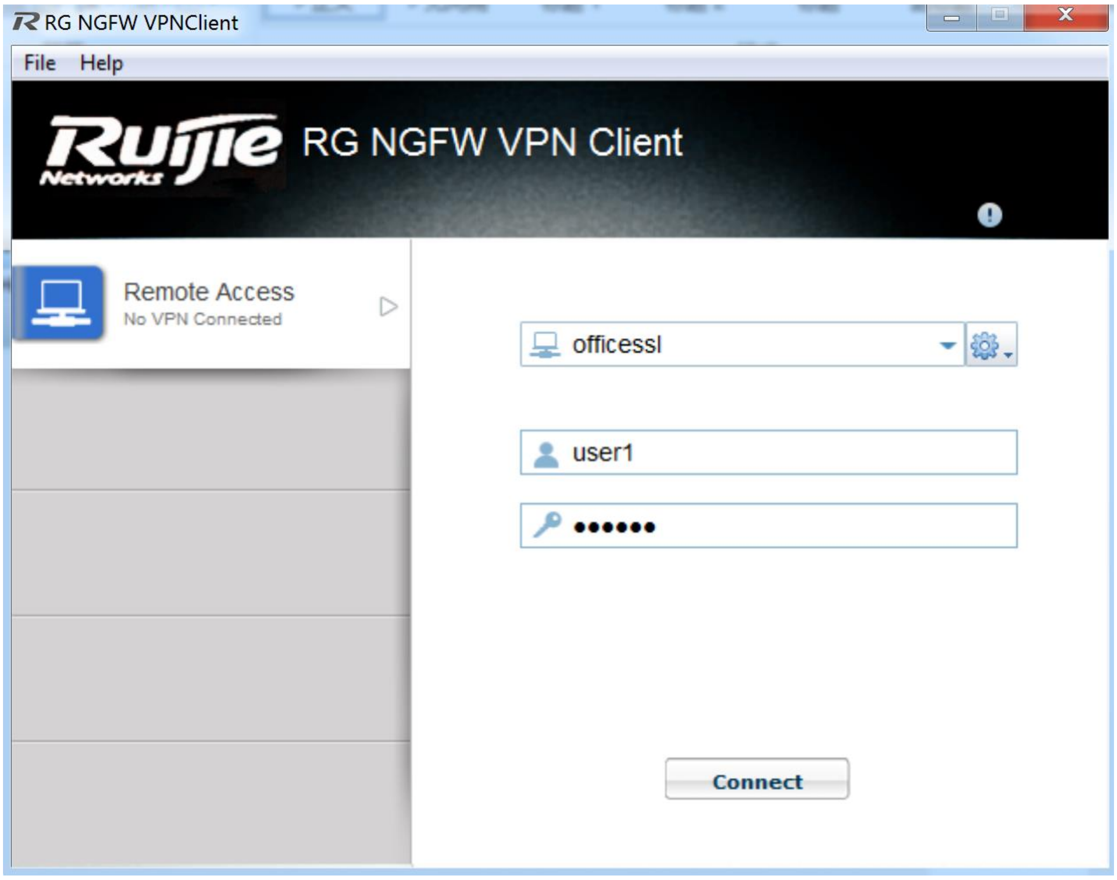




Create new VPN Connection

Connection Name	officessl
Type	● SSL-VPN ○ IPsec VPN
Description	
Remote Gateway	192.168.57.1
	☑ Customize port 4430
Authentication	● Prompt on login ○ Save login
Client Certificate	□
Do not Warn Invalid Server Certificate	□

c) Enter the user name and password to log in to the client.



officessl

user1

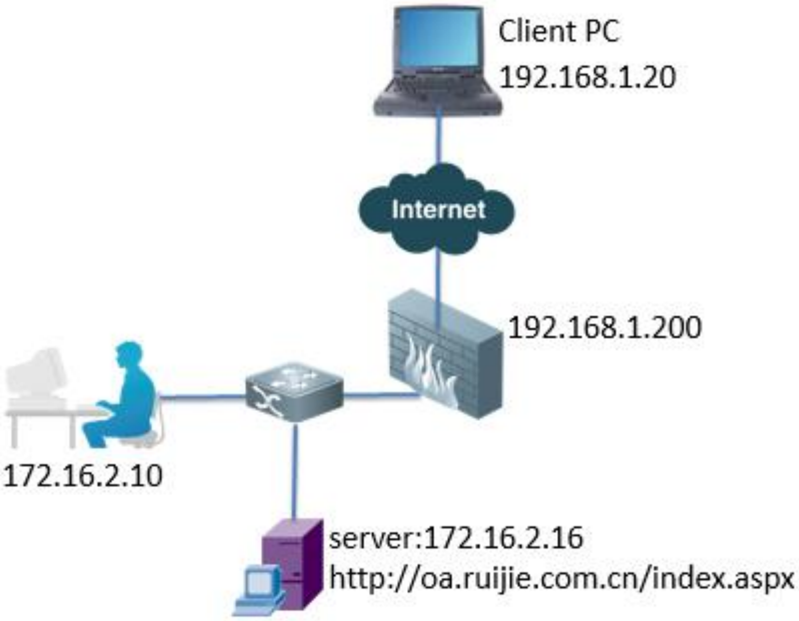
••••••

3.7.3.3 SSL VPN Agent Mode

Networking Requirements

As shown in the figure, a company is internally fitted with an OA server, and to access the OA server, the employees outside the company need to first log in to its intranet via web-based SSL VPN dial-up.

Network Topology



Configuration Tips

1. Perform basic configurations of Internet access;
2. Configure the users;
3. Configure the SSL VPN;
4. Configure the policies;

Configuring the Firewall

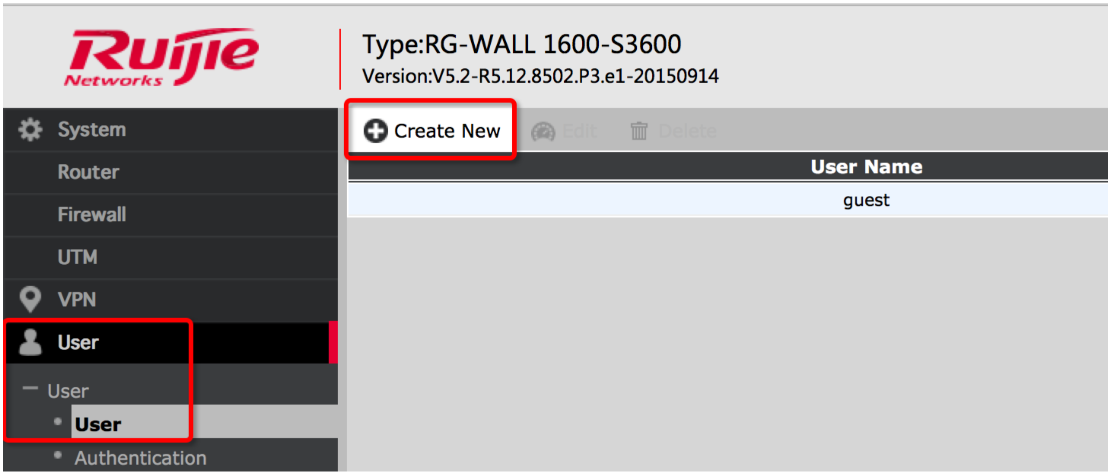
1. Perform basic configurations of Internet access

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

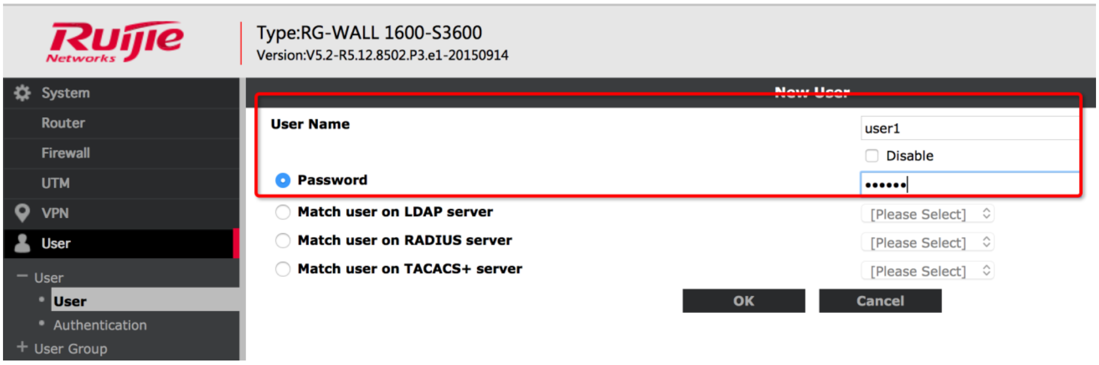
3. Configure the users

1) Define the user.

Choose the **User** > **User** > **User** menu, and click **Create New**.



Add the user name **user1** and password **11111111**.



User Name: user1

□ Disable

● Password: ••••••

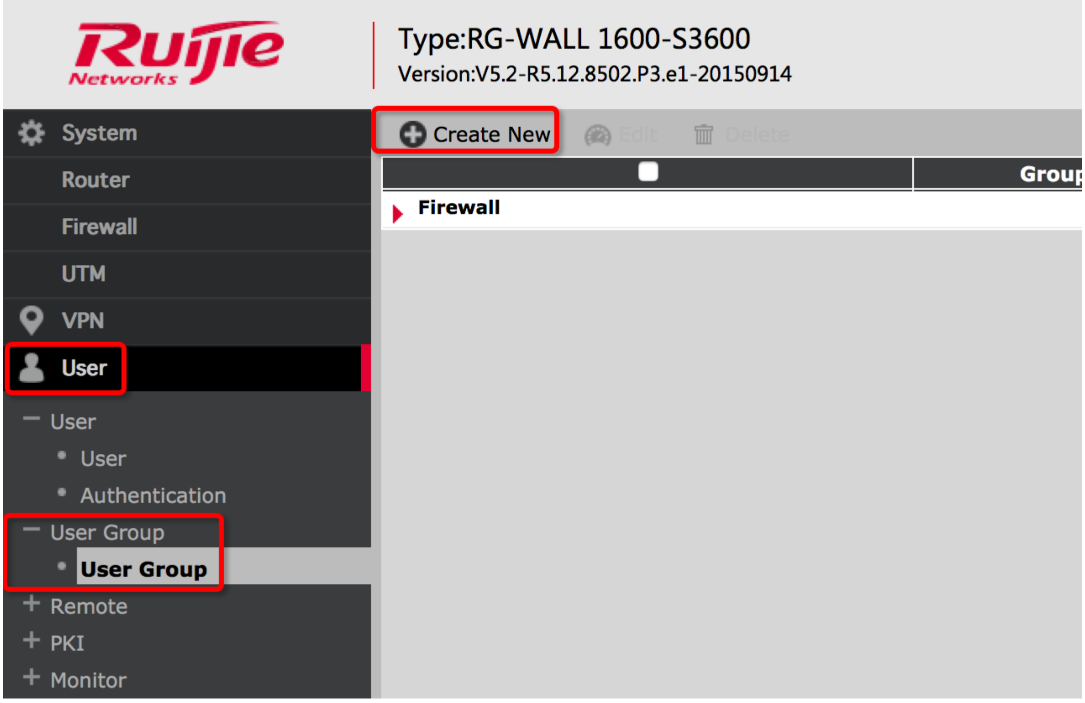
○ Match user on LDAP server [Please Select]

○ Match user on RADIUS server [Please Select]

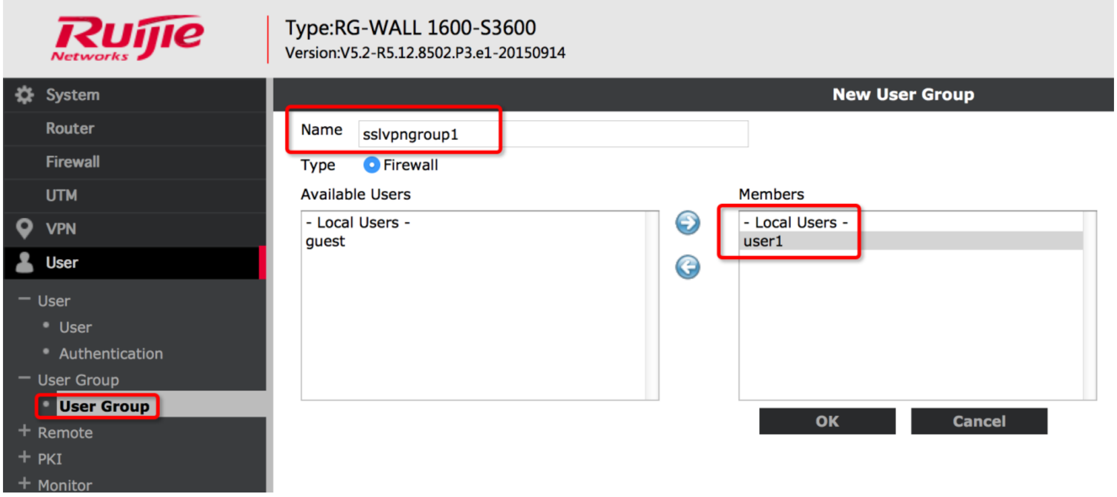
○ Match user on TACACS+ server [Please Select]

2) Define the user group

Choose the **User** > **User Group** > **User Group** menu, and click **Create New**.



Add the user group **sslvpngroup1**, and add the user **user1** to the user group.



Name sslvpngroup1

Type ● Firewall

Available Users: - Local Users - guest

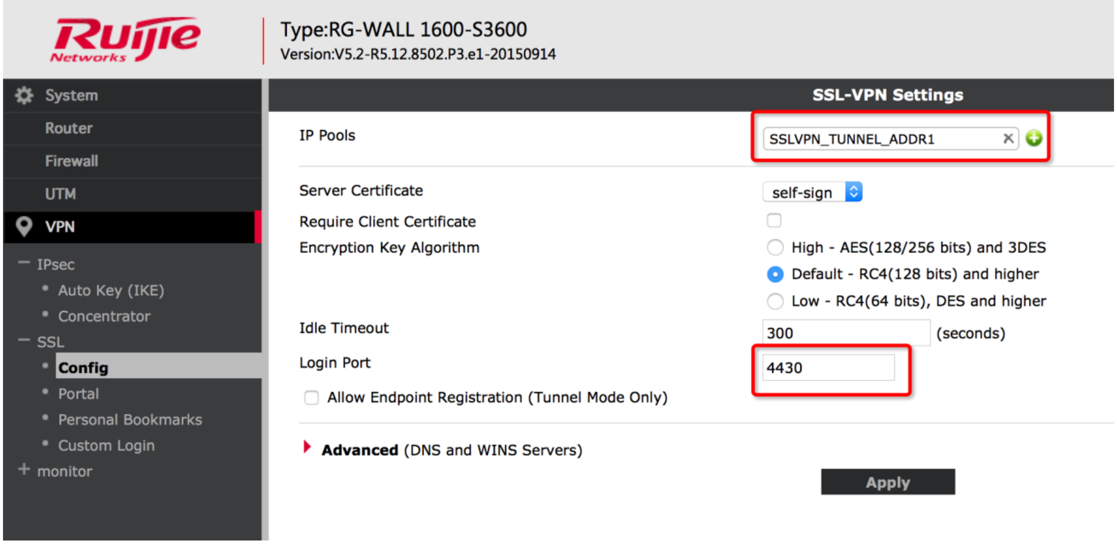
Members: - Local Users - user1

4. Configure the SSL VPN

1) Set SSL VPN

Choose the **VPN** > **SSL** > **Config** menu.

Configure the related parameters as shown below.



IP Pools: SSLVPN_TUNNEL_ADDR1

Server Certificate: self-sign

Require Client Certificate: □

Encryption Key Algorithm:
○ High - AES(128/256 bits) and 3DES
● Default - RC4(128 bits) and higher
○ Low - RC4(64 bits), DES and higher

Idle Timeout: 300 (seconds)

Login Port: 4430

□ Allow Endpoint Registration (Tunnel Mode Only)

▸ **Advanced** (DNS and WINS Servers)

IP Pools: In proxy mode, it does not need to be configured.

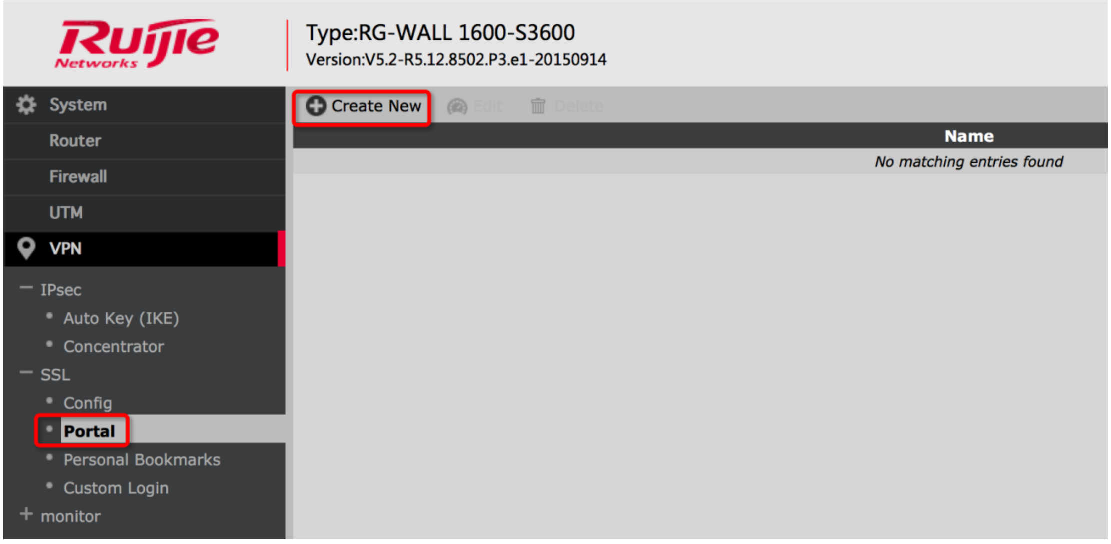
Server Certificate: It is usually set to **Self-sign**. Enterprises can also set it to their proprietary **Local Certificate**.

Login Port: It refers to the port for accessing the SSL VPN. The default value is **443**. If the HTTPS service is enabled for interfaces, this port will conflict with the login port. Then, you can modify the management port of the HTTPS service or modify the login port as another port, for example, **4430**.

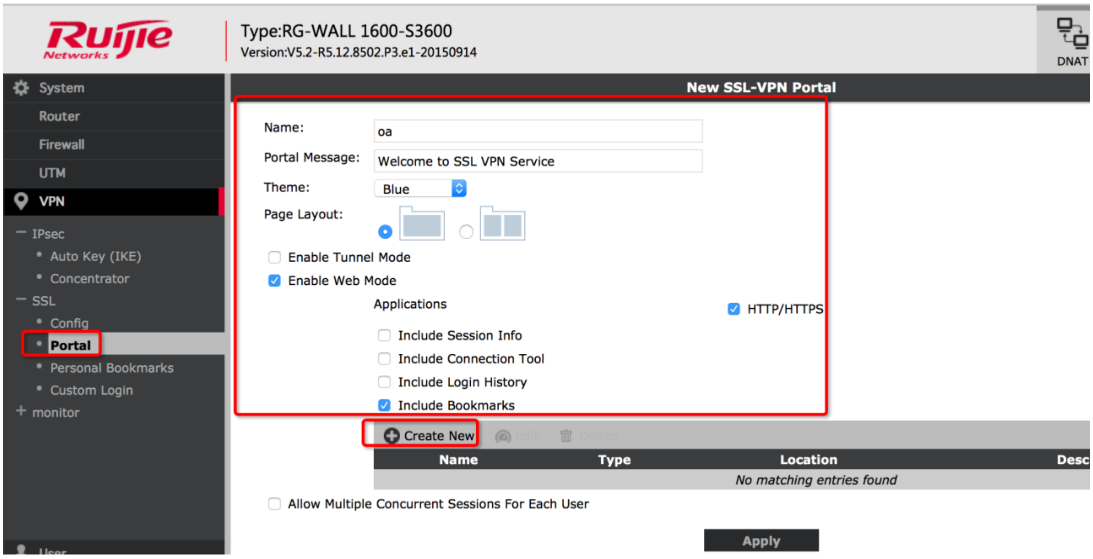
DNS Server and WINS Server: If you need to use a domain name to access internal resources, you need to configure an internal DNS.

2) Configure the SSL interface

Choose the **VPN** > **SSL** > **Interface** menu, and **Create New**.



You can configure the SSL interface specific to the user group.



Name: oa

Portal Message: Welcome to SSL VPN Service

Theme: Blue

Page Layout: ● ○

□ Enable Tunnel Mode

☑ Enable Web Mode

Applications ☑ HTTP/HTTPS

□ Include Session Info

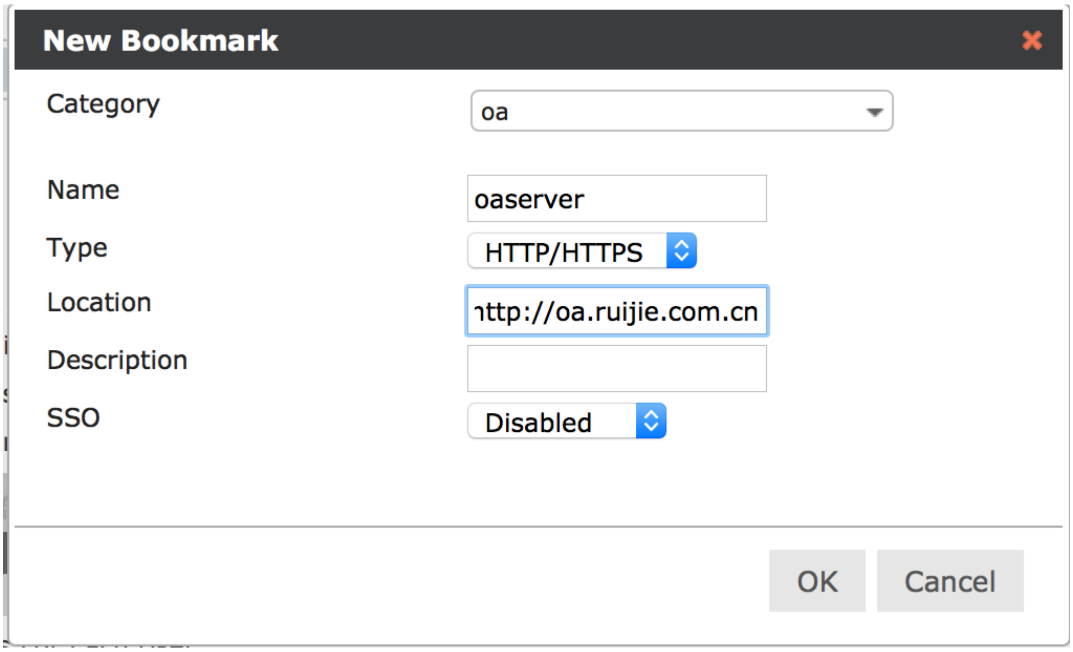
□ Include Connection Tool

□ Include Login History

☑ Include Bookmarks

□ Allow Multiple Concurrent Sessions For Each User

Create a new bookmark:


New Bookmark

Category: oa

Name: oaserver

Type: HTTP/HTTPS

Location: ıttp://oa.ruijie.com.cn

Description:

SSO: Disabled

Category: It refers to the category name.

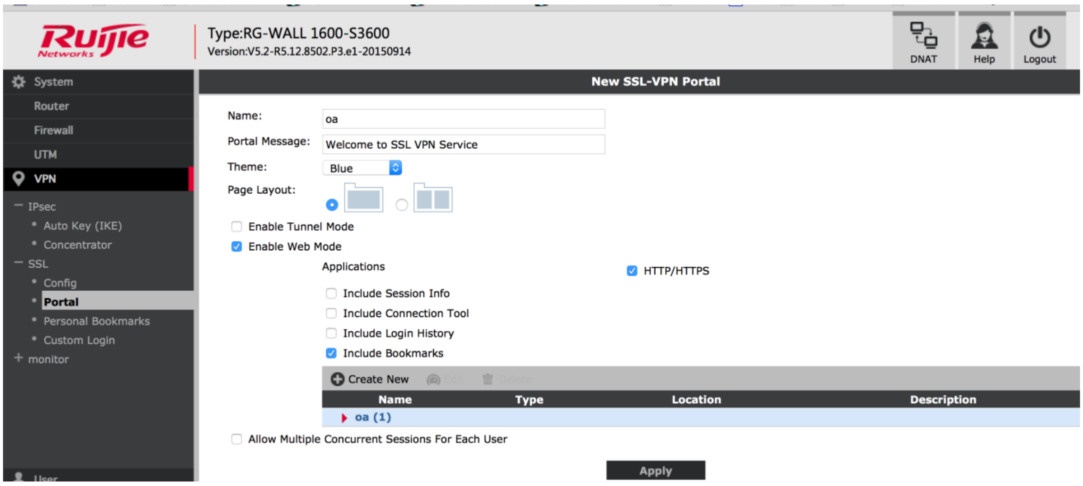
Name: It refers to the server name.

Type: Here, select **HTTP/HTTPS**.

Location: It refers to the login address. Here, enter **http://oa.ruijie.com.cn/index.aspx**.

SSO: It indicates that whether Single Sign On (SSO) is enabled.

After setting the parameters, the following interface pops up.


Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New SSL-VPN Portal

Name: oa

Portal Message: Welcome to SSL VPN Service

Theme: Blue

Page Layout: ● ○

□ Enable Tunnel Mode

☑ Enable Web Mode

Applications ☑ HTTP/HTTPS

□ Include Session Info

□ Include Connection Tool

□ Include Login History

☑ Include Bookmarks

Name	Type	Location	Description
oa (1)			

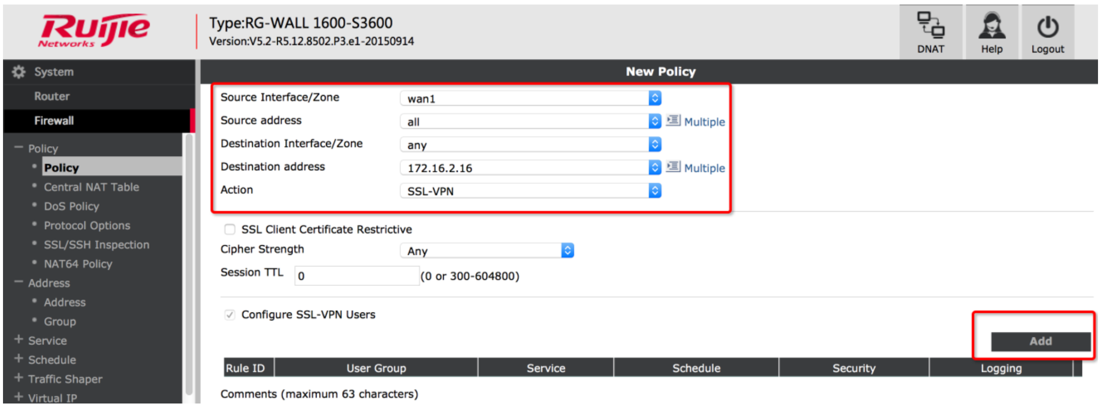
□ Allow Multiple Concurrent Sessions For Each User

5. Configure the SSL policy

1) Configure the allowing policies

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.

The policy is configured as follows:



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Policy

Source Interface/Zone: wan1
Source address: all
Destination Interface/Zone: any
Destination address: 172.16.2.16
Action: SSL-VPN

□ SSL Client Certificate Restrictive
Cipher Strength: Any
Session TTL: 0 (0 or 300-604800)

☑ Configure SSL-VPN Users

Rule ID	User Group	Service	Schedule	Security	Logging

Comments (maximum 63 characters)

Source Interface: It is used to receive a SSL request.

Source Address: It is here set to **all**, indicating that all IP addresses are allowed to perform the SSL connection.

Destination Interface / Zone: It refers to an intranet interface accessed via the SSL VPN.

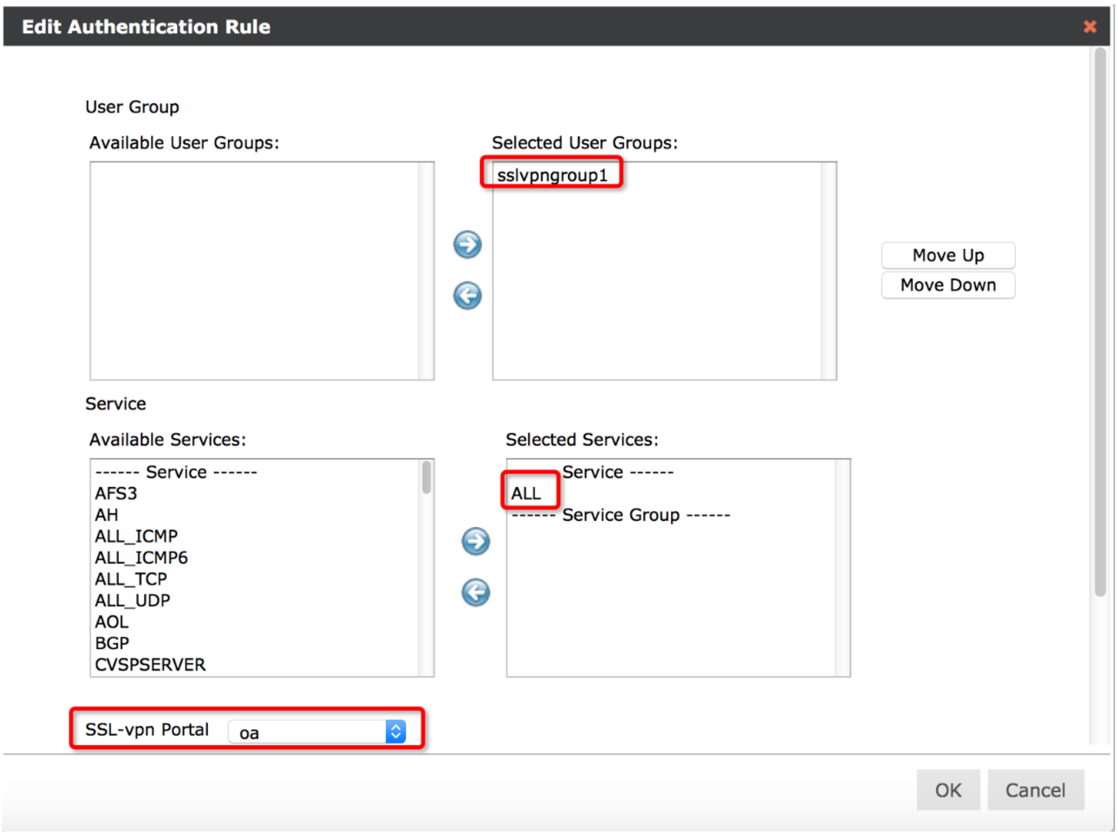
Destination Address: It refers to an internal address that is accessed.

Action: Here, select **SSLVPN**.

Configure SSL-VPN Users: Tick it to add a user group and interface.

2) Add users to the SSL policy. Click **Add**, and the following box pops up.

Add the related user group, services and interface portal for the SSL VPN.



Edit Authentication Rule

User Group

Available User Groups:

Selected User Groups: sslvpngroup1

Service

Available Services:
------ Service ------
AFS3
AH
ALL_ICMP
ALL_ICMP6
ALL_TCP
ALL_UDP
AOL
BGP
CVSPSERVER

Selected Services:
------ Service ------
ALL
------ Service Group ------

SSL-vpn Portal: oa

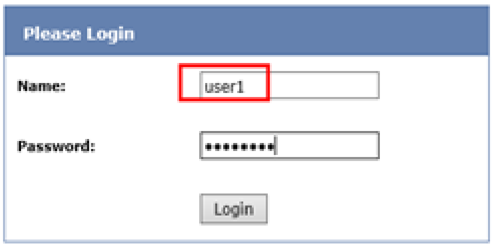
User Group: It refers to the user group who is allowed to log in to the VPN. It is here set to **sslvpngroup1**.

Service: Select **ALL**.

SSL-vpn Portal: It refers to an SSL interface allocated to the user group. Here, select **oa**.

Verification

In the browser, enter **https://192.168.1.200:4430**, the user name **user1** and password **11111111**.

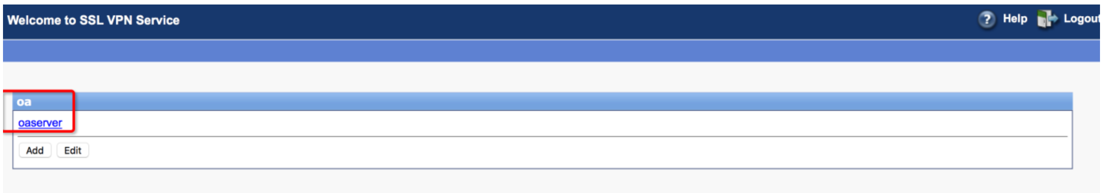


Please Login

Name: user1

Password: ••••••••

After the login is successful, a bookmark page pops up.



Welcome to SSL VPN Service

Click **oaserver**, and access the OA server successfully.

3.7.4 L2TP/PPTP

Overview

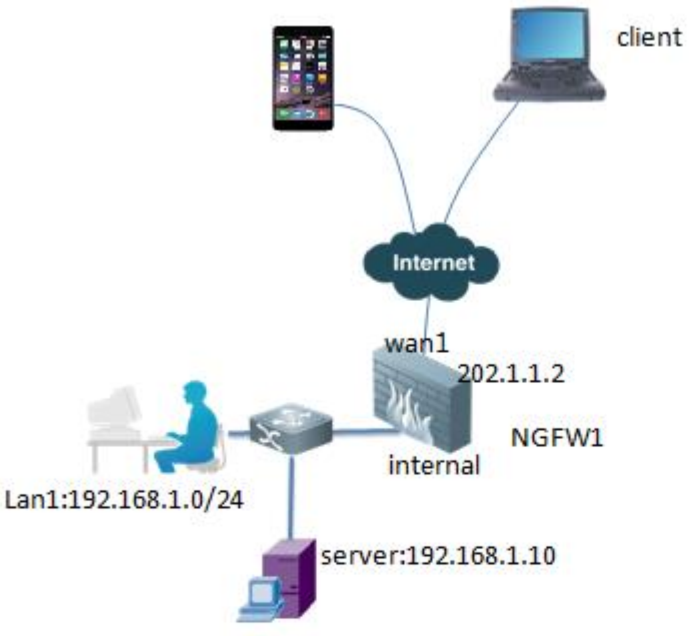
The PPTP VPN allows a PC client or mobile client to dial up.

Networking Requirements

As shown in the figure, a company is internally fitted with an OA server, and to access the OA server, the employees outside the company need to first log in to its intranet via PPT VPN.

The configurations of L2TP VPN are the same as those of PPTP VPN.

Network Topology



Configuration Tips

1. Perform basic configurations of Internet access;
2. Configure the users;
3. Perform PPTP/L2TP configurations for the NGFW;
4. Define the policy;
5. Configure the PC client;
6. If PPTP dialup is successful, the DNS is not issued; if LSTP dialup is successful, the DNS of the firewall system is issued.

Configuration Steps

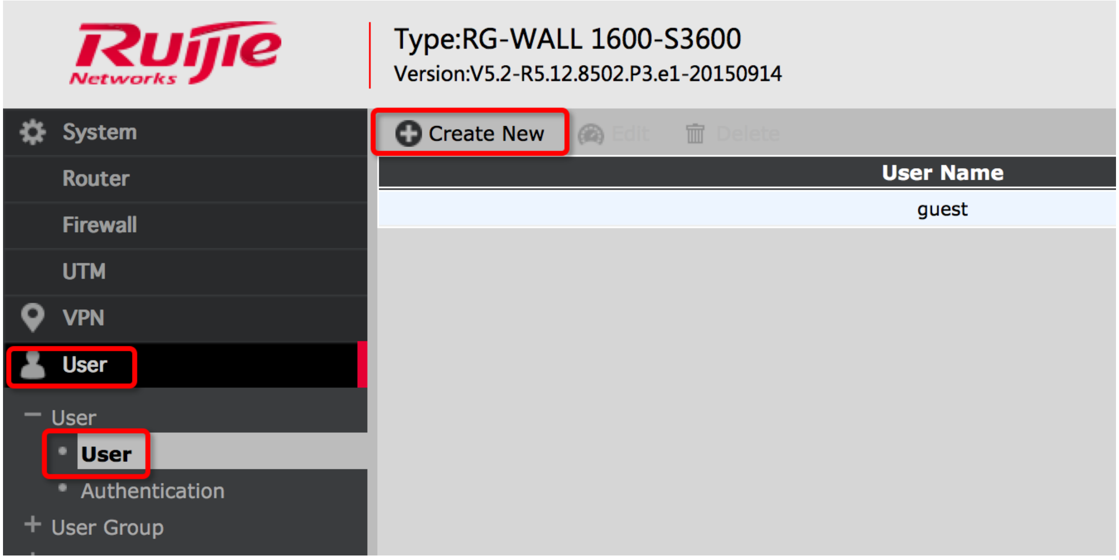
Step 1. Perform basic configurations of Internet access

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” or “Internet Access via a Multiple Links”.

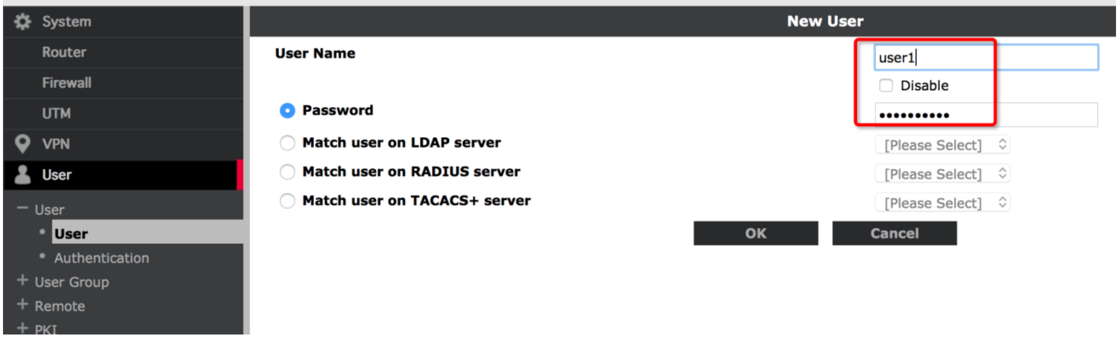
Step 2. Configure the users

1) Define the users

Choose the **User** > **User** > **User** menu, and click **Create New**.



Add the user name **user1** and password **11111111**.



User Name: user1

□ Disable

● Password: ••••••••••

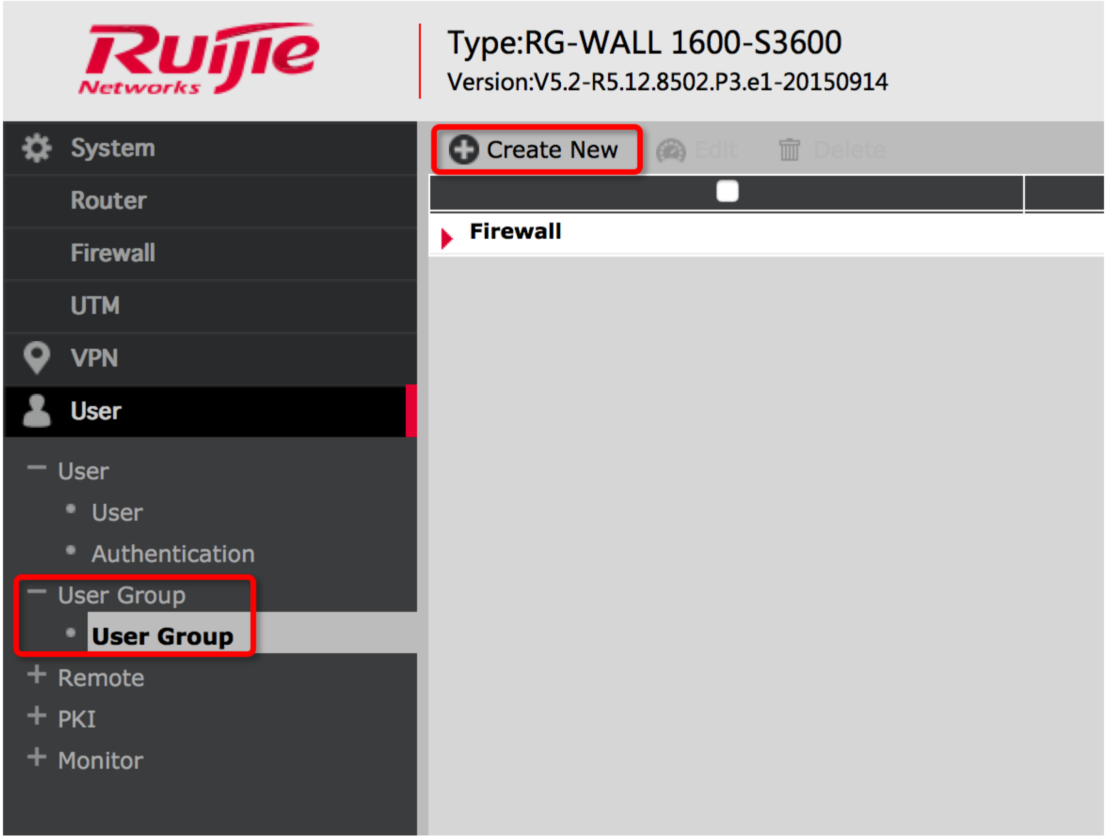
○ Match user on LDAP server [Please Select]

○ Match user on RADIUS server [Please Select]

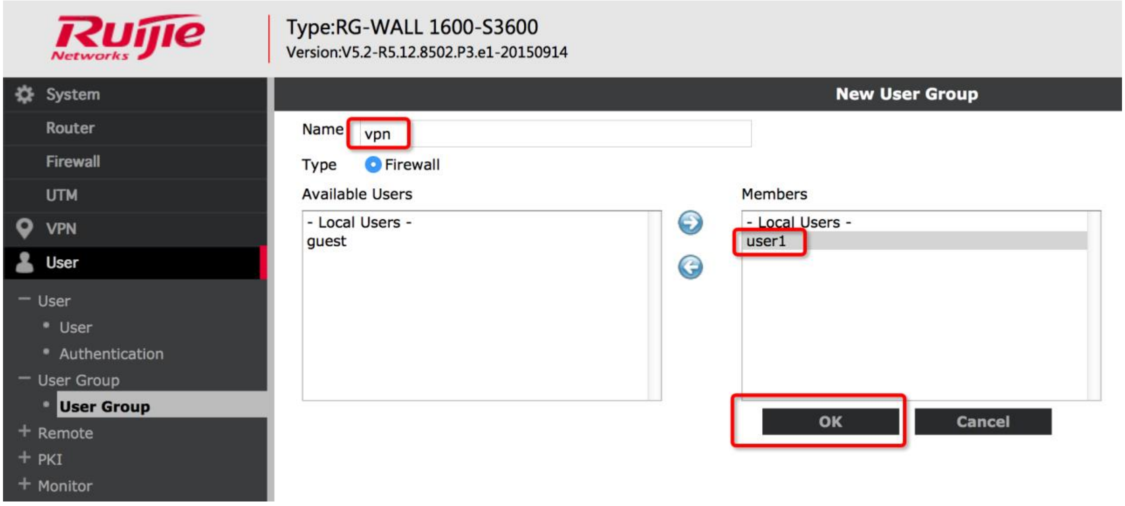
○ Match user on TACACS+ server [Please Select]

2) Define the user group

Choose the **User** > **User Group** > **User Group** menu, and click **Create New**.



Add the user group **vpn**, and add the user **user1** to the user group.



Name: vpn

Type: ● Firewall

Available Users: - Local Users - guest

Members: - Local Users - user1

Step 3. Perform PPTP/L2TP VPN configurations for the NGFW (on the CLI)

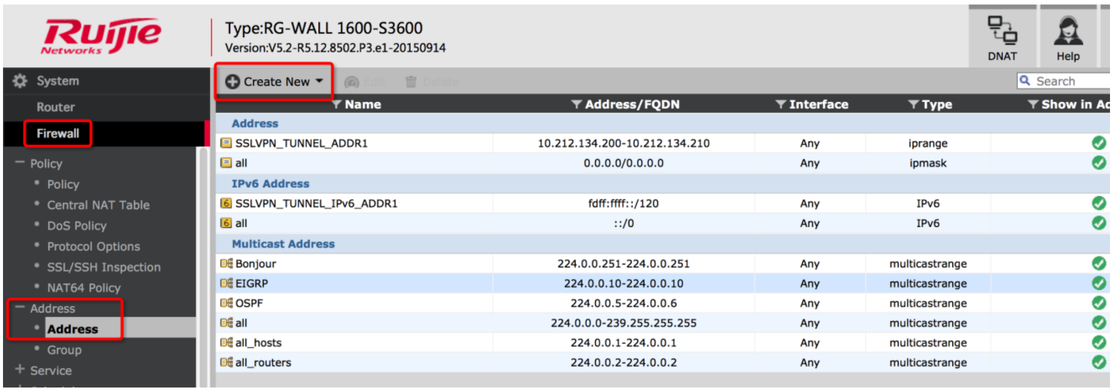
```
RG-WALL #config vpn pptp                                         // config vpn l2tp
The configurations of pptp are the same as the configurations of l2TP; take pptp as an
example.
RG-WALL (pptp) #set status enable                                  //  Enable the VPN
function
```

```
RG-WALL (pptp) #set eip 192.168.1.220                    //  Configure the range of
IP addresses allocated to the client: End IP address
RG-WALL (pptp) #set sip 192.168.1.210                    // Configure the range of
IP addresses allocated to the client: Start IP address
RG-WALL (pptp) #set usrgrp vpn                           //  Invoke the VPN user
group
RG-WALL (pptp) #end
```

The address range allocated to the VPN user can be a segment of intranet addresses or an independent network segment.

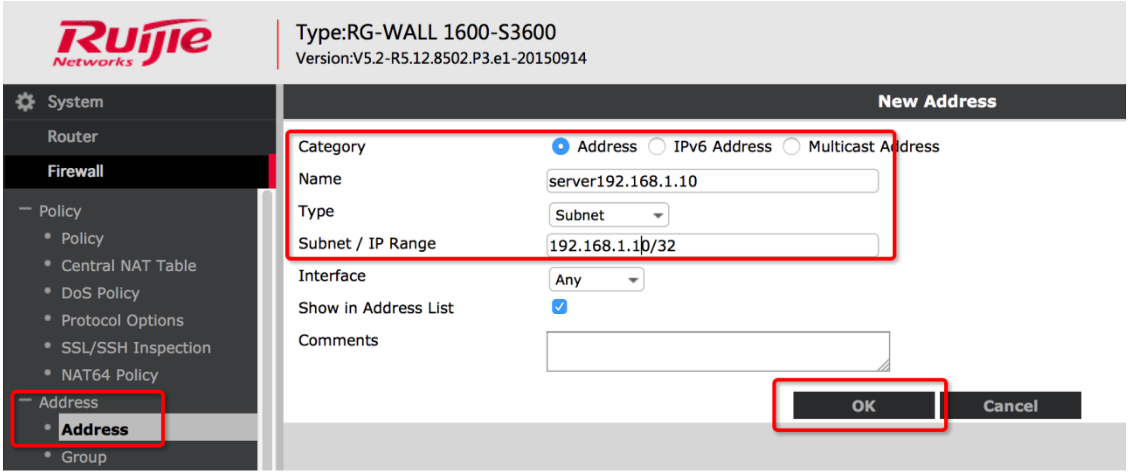
Step 4. Define the policy

1) Configure an address object



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

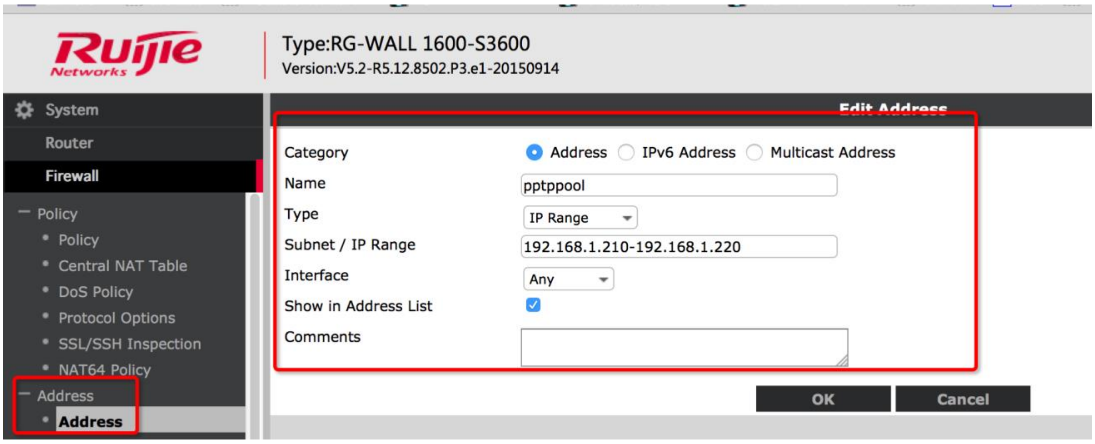
Name	Address/FQDN	Interface	Type	Show in Ad
Address				
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any	iprange	✓
all	0.0.0.0/0.0.0.0	Any	ipmask	✓
IPv6 Address				
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120	Any	IPv6	✓
all	::/0	Any	IPv6	✓
Multicast Address				
Bonjour	224.0.0.251-224.0.0.251	Any	multicastrange	✓
EIGRP	224.0.0.10-224.0.0.10	Any	multicastrange	✓
OSPF	224.0.0.5-224.0.0.6	Any	multicastrange	✓
all	224.0.0.0-239.255.255.255	Any	multicastrange	✓
all_hosts	224.0.0.1-224.0.0.1	Any	multicastrange	✓
all_routers	224.0.0.2-224.0.0.2	Any	multicastrange	✓



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	server192.168.1.10
Type	Subnet
Subnet / IP Range	192.168.1.10/32
Interface	Any
Show in Address List	☑
Comments	



Category: ● Address ○ IPv6 Address ○ Multicast Address

Name: pptppool

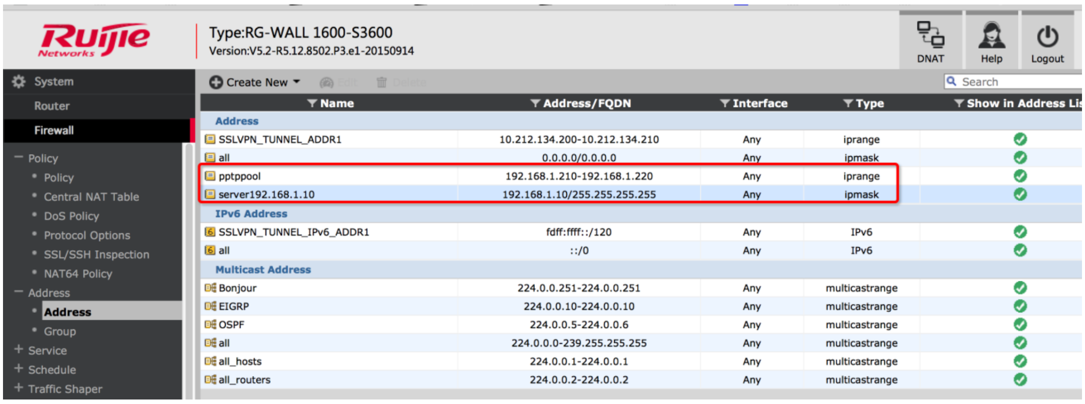
Type: IP Range

Subnet / IP Range: 192.168.1.210-192.168.1.220

Interface: Any

Show in Address List: ☑

Comments:

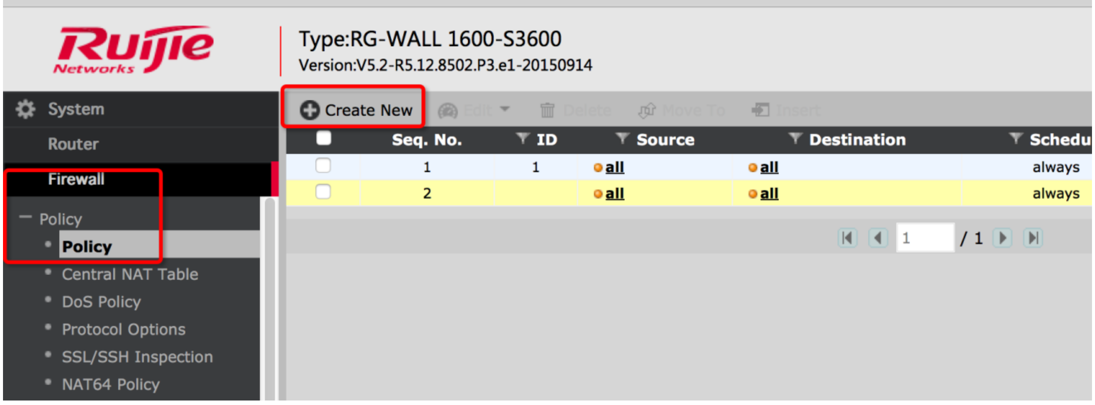


Name	Address/FQDN	Interface	Type	Show in Address Lis
Address				
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any	iprange	✓
all	0.0.0.0/0.0.0.0	Any	ipmask	✓
pptppool	192.168.1.210-192.168.1.220	Any	iprange	✓
server192.168.1.10	192.168.1.10/255.255.255.255	Any	ipmask	✓
IPv6 Address				
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120	Any	IPv6	✓
all	::/0	Any	IPv6	✓
Multicast Address				
Bonjour	224.0.0.251-224.0.0.251	Any	multicastrange	✓
EIGRP	224.0.0.10-224.0.0.10	Any	multicastrange	✓
OSPF	224.0.0.5-224.0.0.6	Any	multicastrange	✓
all	224.0.0.0-239.255.255.255	Any	multicastrange	✓
all_hosts	224.0.0.1-224.0.0.1	Any	multicastrange	✓
all_routers	224.0.0.2-224.0.0.2	Any	multicastrange	✓

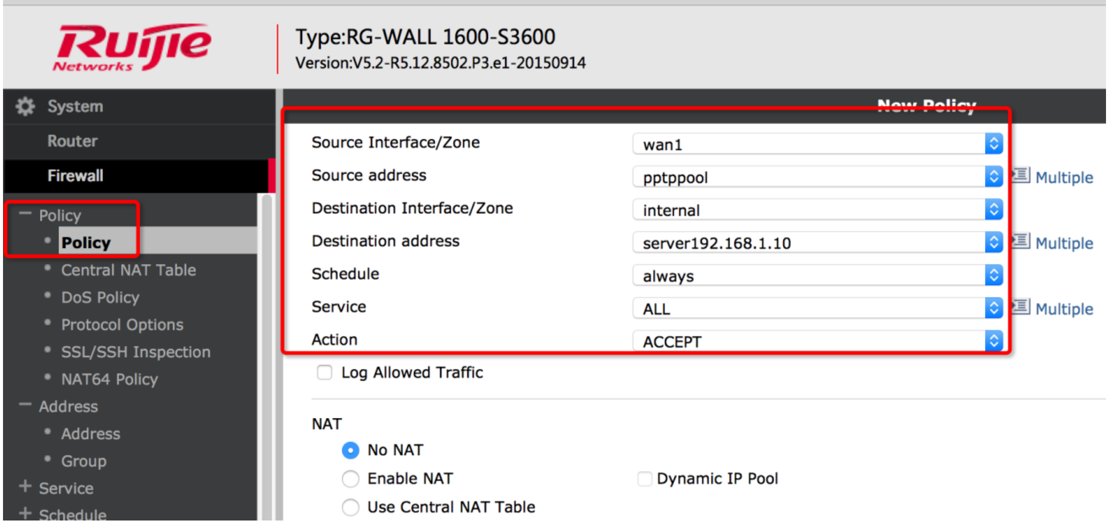
2) Create the policy

Choose the **Firewall** > **Policy** > **Policy** menu, and click **Create New**.

The policy is configured as shown below:



□	Seq. No.	ID	Source	Destination	Schedu
□	1	1	all	all	always
□	2		all	all	always



Source Interface/Zone: wan1

Source address: pptppool

Destination Interface/Zone: internal

Destination address: server192.168.1.10

Schedule: always

Service: ALL

Action: ACCEPT

□ Log Allowed Traffic

NAT

● No NAT

○ Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Source interface/zone: wan1, extranet interface

Source address: Select the previously created **pptppool**.

Destination Interface/Zone: Select **internal**.

Destination Address: Enter **192.168.1.10/32**.

Service: Select **ALL**.

Other parameters: Select the default settings.

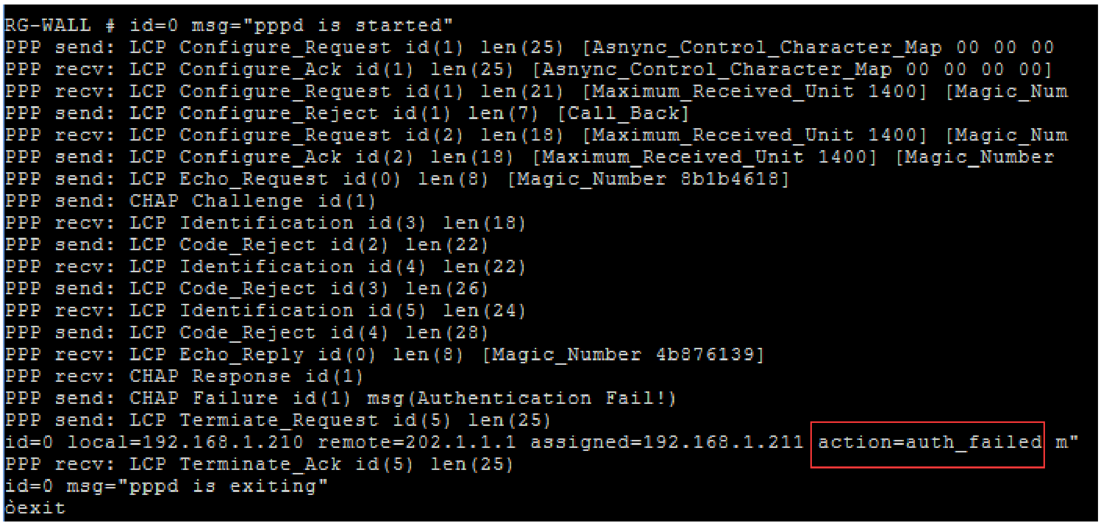
Verification

Note: If the VPN is not established successfully, run the diagnosis command below:

dia debug enable

dia deb app ppp -1

For example, the entered user name or password is incorrect; the system displays the following prompt:



```
RG-WALL # id=0 msg="pppd is started"
PPP send: LCP Configure_Request id(1) len(25) [Asnync_Control_Character_Map 00 00 00
PPP recv: LCP Configure_Ack id(1) len(25) [Asnync_Control_Character_Map 00 00 00 00]
PPP recv: LCP Configure_Request id(1) len(21) [Maximum_Received_Unit 1400] [Magic_Num
PPP send: LCP Configure_Reject id(1) len(7) [Call_Back]
PPP recv: LCP Configure_Request id(2) len(18) [Maximum_Received_Unit 1400] [Magic_Num
PPP send: LCP Configure_Ack id(2) len(18) [Maximum_Received_Unit 1400] [Magic_Number
PPP send: LCP Echo_Request id(0) len(8) [Magic_Number 8b1b4618]
PPP send: CHAP Challenge id(1)
PPP recv: LCP Identification id(3) len(18)
PPP send: LCP Code_Reject id(2) len(22)
PPP recv: LCP Identification id(4) len(22)
PPP send: LCP Code_Reject id(3) len(26)
PPP recv: LCP Identification id(5) len(24)
PPP send: LCP Code_Reject id(4) len(28)
PPP recv: LCP Echo_Reply id(0) len(8) [Magic_Number 4b876139]
PPP recv: CHAP Response id(1)
PPP send: CHAP Failure id(1) msg(Authentication Fail!)
PPP send: LCP Termiate_Request id(5) len(25)
id=0 local=192.168.1.210 remote=202.1.1.1 assigned=192.168.1.211 action=auth_failed m"
PPP recv: LCP Terminate_Ack id(5) len(25)
id=0 msg="pppd is exiting"
òexit
```

Should you have any query, collect the related information and then call the technical support hotline (400-111-000) to seek help.

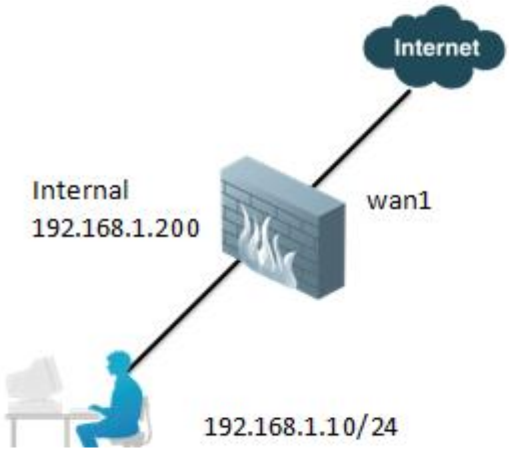
3.8 WAN Optimization

3.8.1 Standalone Mode

I. Networking Requirements

Configure basic functions for Internet access and enable Web cache.

II. Network Topology



Assume that the ISP assigns the following addresses:

Network segment: 202.1.1.8/29; IP address: 202.1.1.10; gateway address: 202.1.1.9; DNS: 202.106.196.115.

III. Configuration Tips

1. Basic Configuration for Internet Access (Omitted. See section 1.1 "Internet Access via a Single Line" in Chapter 1 "Typical Functions of Routing Mode".)
   a. Configure an interface.
   b. Configure a static routing table.
   c. Set the address object to **InternalIP** and the address to 192.168.1.0/24.
   d. Configure the policy from LAN to wan1, and enable NAT.
2. Enable Web cache.
3. Configure Web cache parameters.

IV. Configuration Steps

1. Basic Configuration for Internet Access (Omitted. See section 1.1 "Internet Access via a Single Line" in Chapter 1 "Typical Functions of Routing Mode".)

   a) Configure an interface.

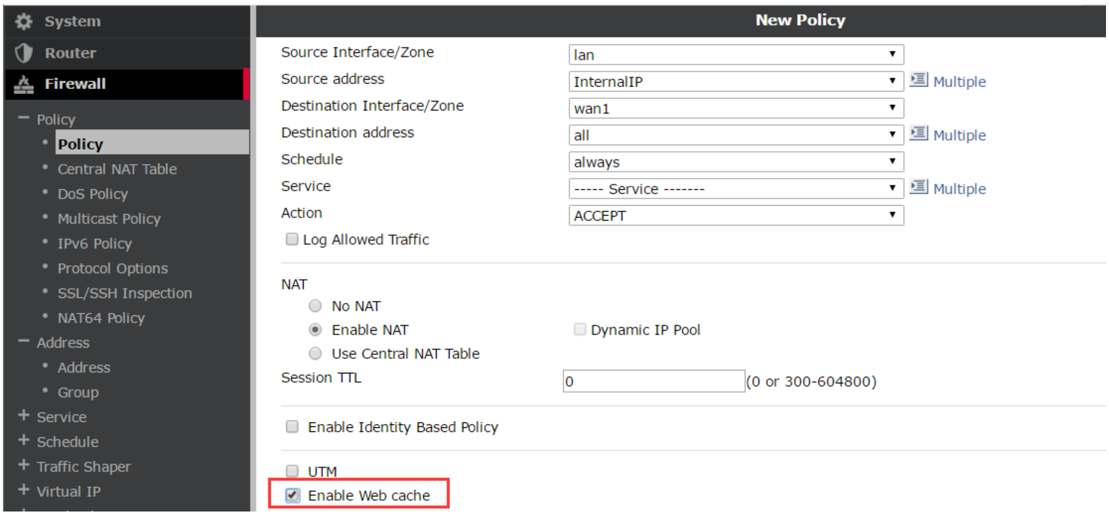
   b) Configure a static routing table.

   c) Set the address object to **InternalIP** and the address to 192.168.1.0/24.

   d) Configure the policy from LAN to wan1, and enable NAT.

For some low-end models, the system configures an NAT policy from internal to wan1 by default.

In the **New Policy** window, create a policy as follows:



Source Interface/Zone: lan

Source address: InternalIP

Destination Interface/Zone: wan1

Destination address: all

Schedule: always

Service: ----- Service -------

Action: ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

Session TTL: 0 (0 or 300-604800)

□ Enable Identity Based Policy

□ UTM

☑ Enable Web cache

Source Interface/Zone: Choose **lan**.

Source address: Choose **InternalIP**.

Destination Interface/Zone: Choose **wan1**.

Destination address: Choose **all**, which indicates all addresses.

Service: Choose **ALL**.

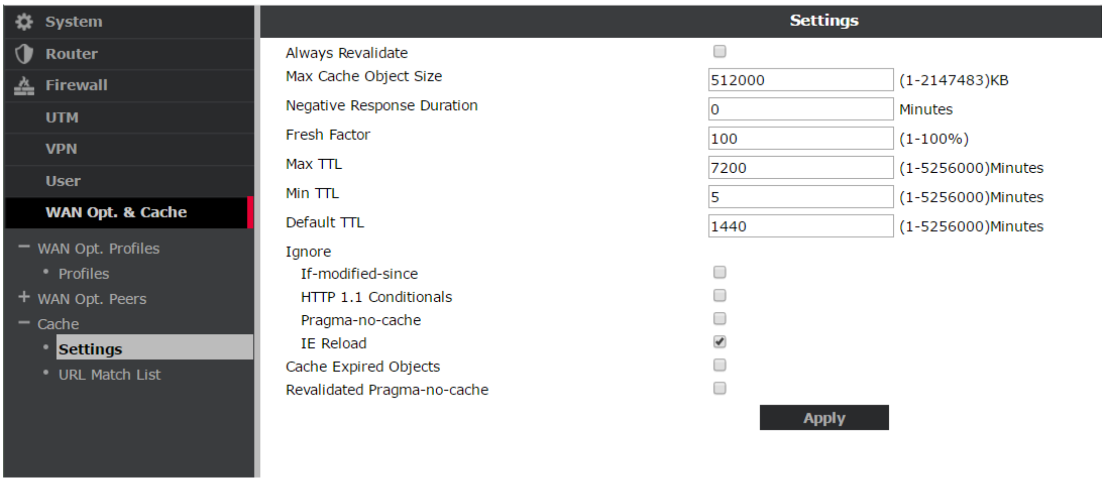
NAT: Tick **Enable NAT**. The system automatically converts the IP address of the intranet lan to the IP address of wan1 interface 202.1.1.10 for Internet access.

Click **Enable Web cache**.

Click **OK**. The system automatically saves configuration and the policy takes effect.

Configure Web cache parameters.

Choose **WAN Opt. & Cache** > **Cache** >**Settings**. Default settings are used generally.



Settings

Always Revalidate	☐	
Max Cache Object Size	512000	(1-2147483)KB
Negative Response Duration	0	Minutes
Fresh Factor	100	(1-100%)
Max TTL	7200	(1-5256000)Minutes
Min TTL	5	(1-5256000)Minutes
Default TTL	1440	(1-5256000)Minutes
Ignore		
If-modified-since	☐	
HTTP 1.1 Conditionals	☐	
Pragma-no-cache	☐	
IE Reload	☑	
Cache Expired Objects	☐	
Revalidated Pragma-no-cache	☐	

Always Revalidate:

Max Cache Object Size: It indicates the maximum size of the cache object, which is 512 MB by default. Larger files are directly sent to clients without caches.

Negation Response Duration: It indicates whether to cache error messages returned by the server. The default value is 0.

Fresh Factor: It is used to set the check frequency of cache update by the firewall. If it is set to 100%, check caches once before expiration (TTL timeout). If it is set to 20%, check caches five times.

Max TTL: It indicates the maximum alive time of caches when the expiration is not checked.

Min TTL: It indicates the minimum alive time of caches before the expiration is checked.

Default TTL: It indicates the default alive time of caches.

Ignore: It indicates that caches are ignored.

V. Verification

```
RGFW # diagnose  wacs stats
Disk 0 /var/storage/FLASH1-68B85ACE134E6A3A/wa_cs
        Current number of open connections: 2
        Number of terminated connections: 21 //
        Number of requests -- Adds: 6547 (0 repetitive keys), Lookups: 12780, Conflict
incidents: 0
        Percentage of missed lookups: 96.39
        Communication is blocked for 0 client(s)
        wa_cs disk space: 4278 MB
        Disk usage: 93861 KB (2%)           //Indicates the space occupied by caches.
```

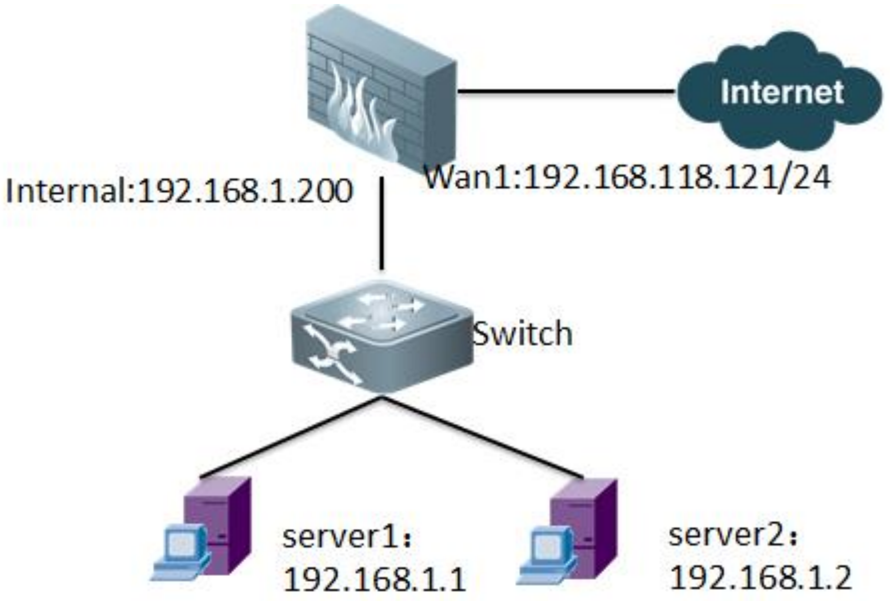
3.9 Load Balancing

3.9.1 HTTP Traffic-based Server Load Balancing

I. Networking Requirements

As shown in the following figure, the company has two Web servers. Load balancing is configured on the servers and loads Web services to the server 192.168.1.1 and the server 192.168.1.2.

II. Network Topology



III. Configuration Tips

1. Basic configuration for Internet access

Configure the load balancing server.

a) Configure health check.

b) Configure the load balancing server.

c) Configure a real server.

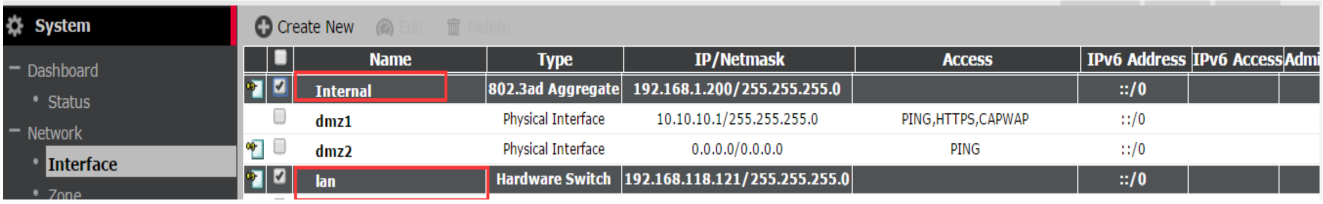
d) Configure a safety policy.

IV. Configuration Steps

1. Basic configuration for Internet access

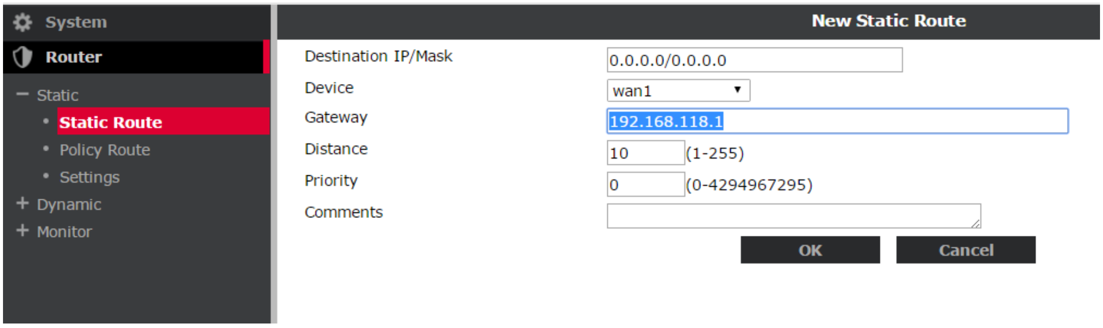
For the detailed configuration process, see section 1.1.2 "Configuring Internet Access via a Static Link" under section 1.1 "Internet Access via a Single Line" in Chapter 1 "Typical Functions of Routing Mode".

IP addresses of interfaces are as follows:



	☐	Name	Type	IP/Netmask	Access	IPv6 Address	IPv6 Access	Admi
	☑	Internal	802.3ad Aggregate	192.168.1.200/255.255.255.0		::/0		
	☐	dmz1	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,CAPWAP	::/0		
	☐	dmz2	Physical Interface	0.0.0.0/0.0.0.0	PING	::/0		
	☑	lan	Hardware Switch	192.168.118.121/255.255.255.0		::/0		

The routing configuration is as follows:



New Static Route

Destination IP/Mask 0.0.0.0/0.0.0.0

Device wan1

Gateway 192.168.118.1

Distance 10 (1-255)

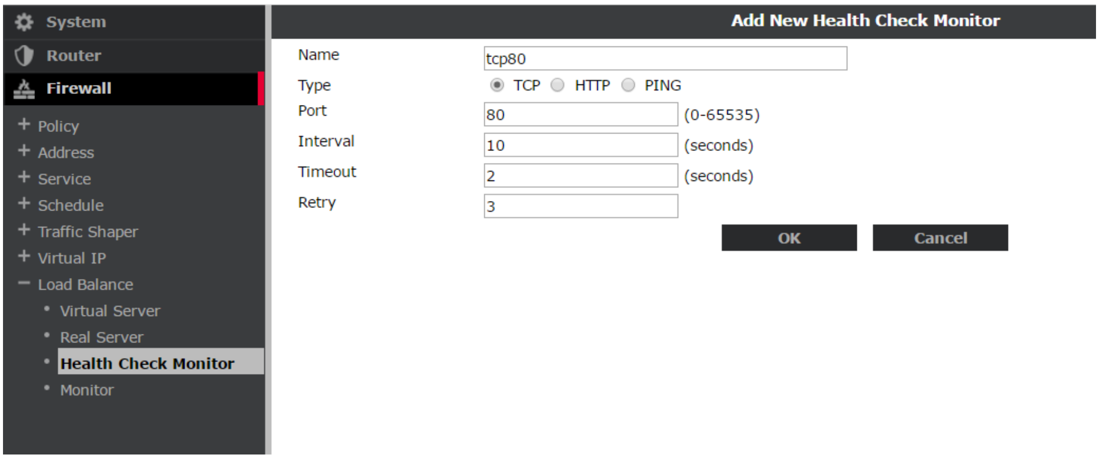
Priority 0 (0-4294967295)

Comments

2. Configure the load balancing server.

(1) health check.

Choose **Firewall** > **Load Balance** > **Health Check Monitor**. Set health check methods to check the health condition of the real server. The following takes TCP as an example.



Add New Health Check Monitor

Name tcp80

Type ● TCP ○ HTTP ○ PING

Port 80 (0-65535)

Interval 10 (seconds)

Timeout 2 (seconds)

Retry 3

Name: Enter tcp80. This item is user-defined.

Type: **TCP**, **HTTP**, and **PING** are supported. Tick **TCP** to check the service port 80, or tick **HTTP** to check whether the HTTP service process is normal and whether Web pages can be accessed, or tick **PING** to check whether the host is online.

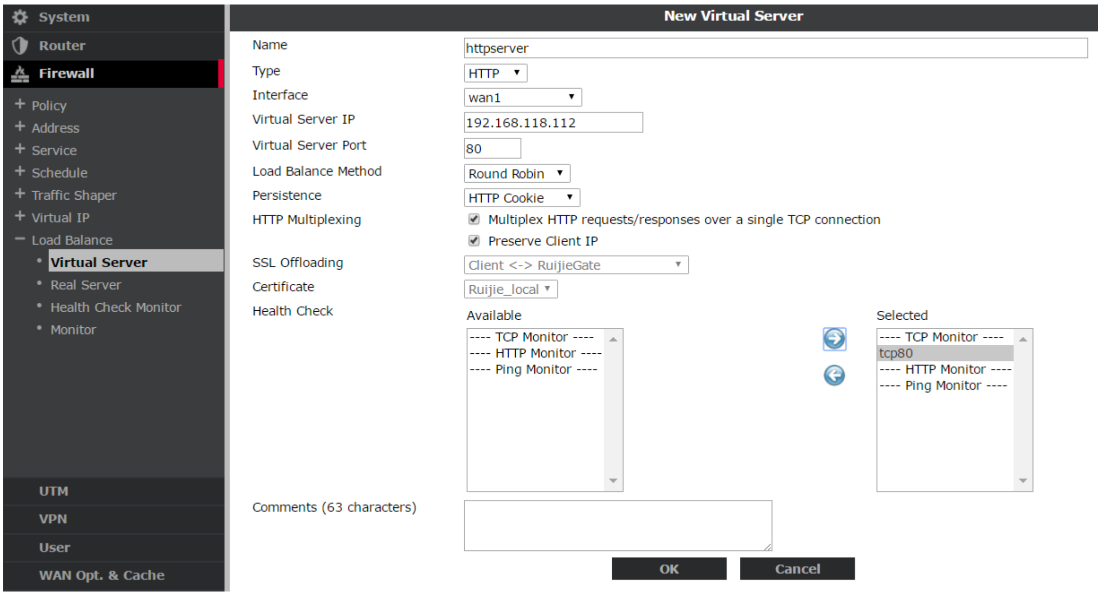
Interval: Enter **10**, which indicates check every 10 seconds.

Timeout: Enter **2**. If no response is received from the server within 2 seconds, it indicates exceptions on the server.

Retry: If the server still fails to give any response after retry for three consecutive times, it indicates that the server is out of service and will not assign load to the device.

(2) Configure the load balancing server.

Choose **Firewall** > **Load Balance** > **Virtual Server**, and then click **Create New** to create a virtual server, as shown in the following figure.



New Virtual Server

Name: httpserver

Type: HTTP

Interface: wan1

Virtual Server IP: 192.168.118.112

Virtual Server Port: 80

Load Balance Method: Round Robin

Persistence: HTTP Cookie

HTTP Multiplexing: ☑ Multiplex HTTP requests/responses over a single TCP connection

☑ Preserve Client IP

SSL Offloading: Client <-> RuijieGate

Certificate: Ruijie_local

Health Check:

Available: ---- TCP Monitor ---- / ---- HTTP Monitor ---- / ---- Ping Monitor ----

Selected: ---- TCP Monitor ---- / tcp80 / ---- HTTP Monitor ---- / ---- Ping Monitor ----

Comments (63 characters)

Name: Enter **httpserver**. This item is user-defined.

Type: HTTP, TCP, UDP, and IP are supported. **HTTP** is chosen in this example. For the DNS server, choose UDP.

Interface: Choose **wan1**. It indicates the port where the server is connected to external servers.

Virtual Server IP: It indicates the IP address where the server provides external services.

Load Balance Method: Static, Round-Robin, Weighted, First Alive, Least RTT, Least-conn, and HTTP Host are supported. For the difference between these methods, see the *Firewall Configuration Guide*.

Persistence: Choose **http cookie**.

HTTP Multiplexing: This item is optional. Multiple links requested by a customer can be merged into one request to reduce the server load.

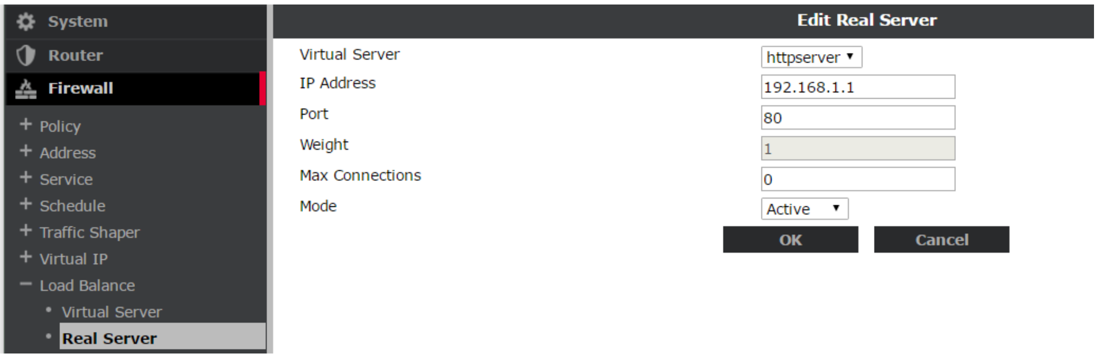
SSL: It indicates the load applicable to HTTPS service.

Certificate: It indicates the certificate that enables HTTP proxy.

Health Check: Select **tcp80**.

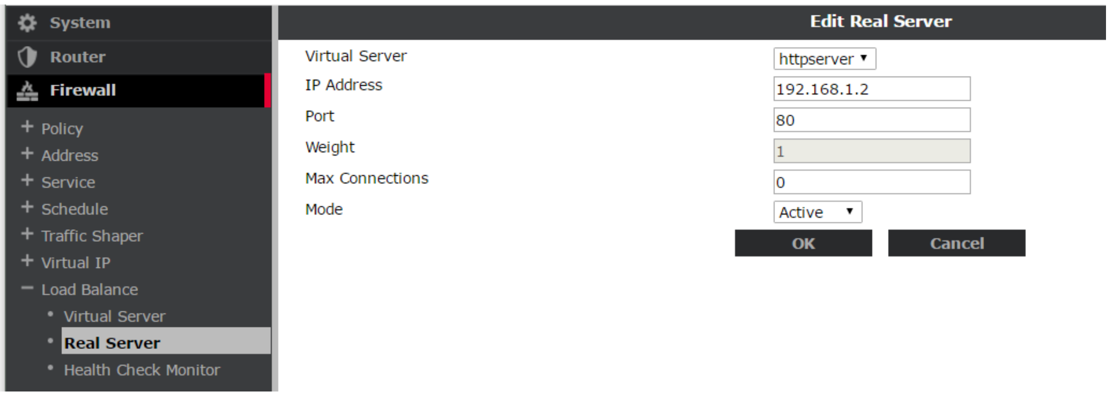
(3) Configure a real server.

Choose **Firewall** > **Load Balance** > **Real Server**, and then click **Create New** to create two real servers, as shown in the following figure.



Edit Real Server

Virtual Server	httpserver
IP Address	192.168.1.1
Port	80
Weight	1
Max Connections	0
Mode	Active



Edit Real Server

Virtual Server	httpserver
IP Address	192.168.1.2
Port	80
Weight	1
Max Connections	0
Mode	Active

Virtual Server: Choose **httpserver**. It indicates the virtual server for which a real server is configured.

IP Address: It indicates IP address of the real server.

Port: It indicates the HTTP service port of the real server, which may be different from the server port of the virtual server.

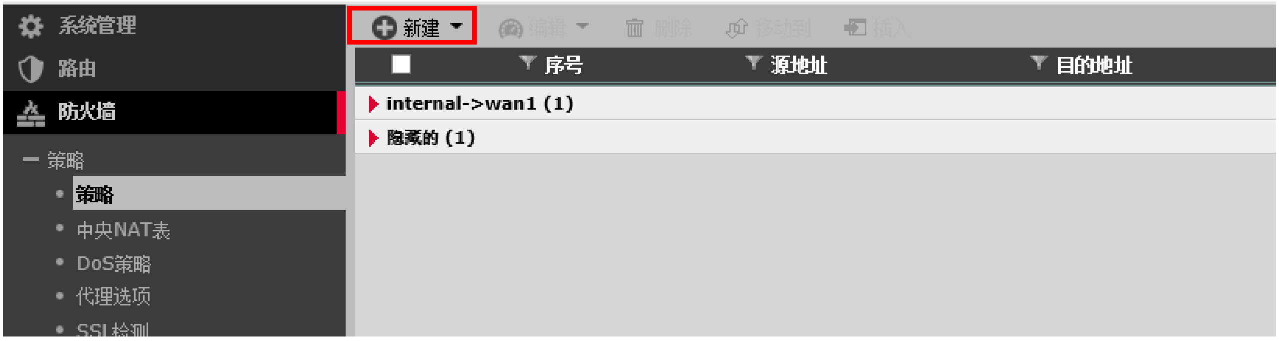
Weight: It is disabled in this example. If the load balance method is set to **weighted**, specify the percentage, such as 10:10.

Max Connections: The value **0** indicates no restriction.

Mode: Choose **Active**. Three options are available: active, inactive, and standby.

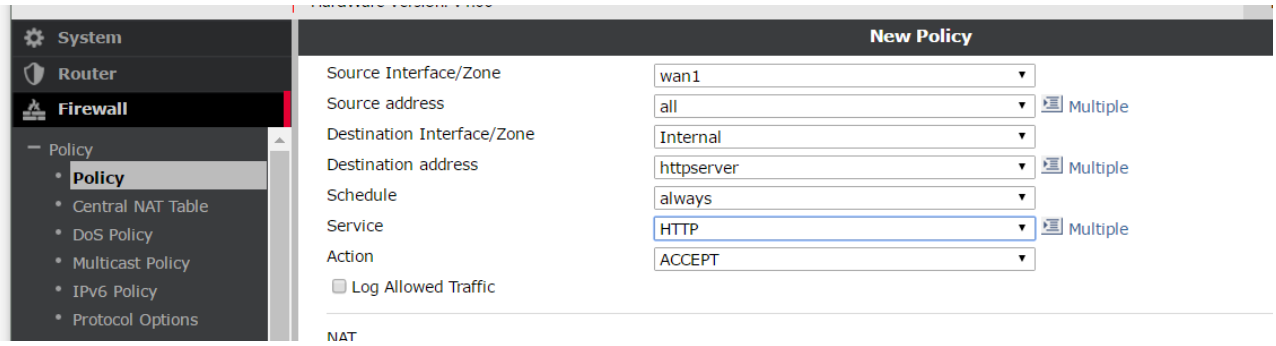
Configure a safety policy.

Choose **Firewall** > **Policy** > **Policy**, and then click **Create New**.



□	序号	源地址	目的地址
internal->wan1 (1)			
隐藏的 (1)			

In the **New Policy** window, create a policy as follows:



New Policy

Source Interface/Zone: wan1
Source address: all Multiple
Destination Interface/Zone: Internal
Destination address: httpserver Multiple
Schedule: always
Service: HTTP Multiple
Action: ACCEPT
□ Log Allowed Traffic
NAT

Click **Multiple** behind **Destination address**, and choose two virtual IP addresses that have been defined.

Source Interface/Zone: Choose **wan1**.

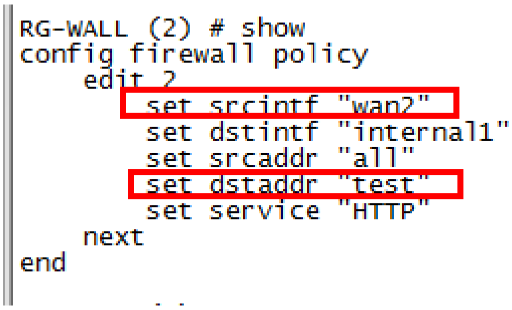
Source address: Choose **all**.

Destination Interface/Zone: Choose **internal**.

Destination address: Choose **httpserver**.

Service: Choose **HTTP**.

Note: Virtual IP addresses defined with earlier versions than P4 cannot be called on the Web page but can be called from the command line. Choose the interface defined by the virtual server as the source interface, and run the following commands:



```
RG-WALL (2) # show
config firewall policy
    edit 2
        set srcintf "wan2"
        set dstintf "internal1"
        set srcaddr "all"
        set dstaddr "test"
        set service "HTTP"
    next
end
```

V. Verification

Access http://192.168.118.122 from an external address.

Common Diagnosis Commands:

1. Check the status of a real server.

```
    RG-WALL # diagnose  firewall  vip realserver  list

alloc=4

------------------------------

vf=0 name=httpserver/1 type=3 192.168.118.122:(80-80), protocol=6

total=2 alive=2 power=2 ptr=197676

ip=192.168.1.1-192.168.1.1:80 adm_status=0 holddown_interval=300 max_connections

=0 weight=1 option=01

alive=1 total=1 enable=00000001 alive=00000001 power=1
```

```
src_sz=0

id=0 status=up ks=12 us=0 events=1 bytes=2078892 rtt=0

ip=192.168.1.2-192.168.1.2:80 adm_status=0 holddown_interval=300 max_connections

=0 weight=1 option=01

alive=1 total=1 enable=00000001 alive=00000001 power=1

src_sz=0

id=0 status=up ks=9 us=0 events=1 bytes=50450 rtt=0
```

Check the status of a real server configured for a virtual server.

```
RG-WALL # diagnose  firewallvip  virtual-server  real-server

vd root/0  vs httpserver/1  addr 192.168.1.1:80  status 2/1 (process 193)

conn: max 0  active 5  attempts 1440success 165  drop  0  fail 3

http: available 4  total 5


vd root/0  vs httpserver/1  addr 192.168.1.2:80  status 2/1 (process 193)

conn: max 0  active 1  attempts 37success 11  drop  0  fail 2

http: available 0  total 1
```

Collect statistics on the sessions of a virtual server.

```
RG-WALL # diagnose  firewallvip  virtual-server  stats

summary

c2p_connections: now 21  max 31total 140

embryonics: now 0  max 6total 140

close_during_connect: 0

........
```

Collect statistics on the sessions of a virtual server.

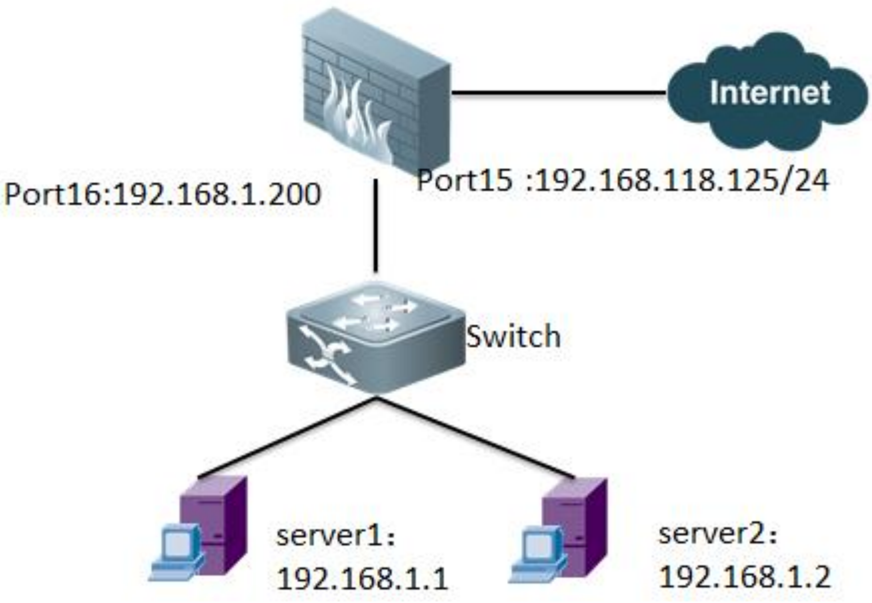
```
RG-WALL # diagnose  firewallvip  virtual-server  stats

summary

c2p_connections: now 21  max 31total 140
```

3.9.2 HTTPS Traffic-based Server Load Balancing

I. Networking Requirements

As shown in the following figure, the company has two Web servers with the domain name www.test.com, which can be accessed via HTTPS. Load balancing is configured on the firewall and loads Web services to the server 192.168.1.1 and the server 192.168.1.2.

II. Network Topology



III. Configuration Tips

2. Basic configuration for Internet access

Configure the load balancing server.

(1) Configure health check.

(2) Configure the load balancing server.

(3) Configure a real server.

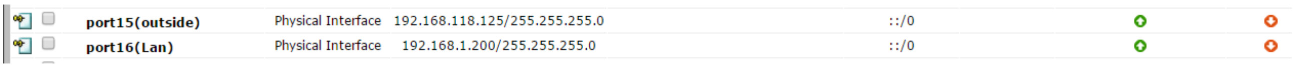
(4) Configure a safety policy.

IV. Configuration Steps

1. Basic configuration for Internet access

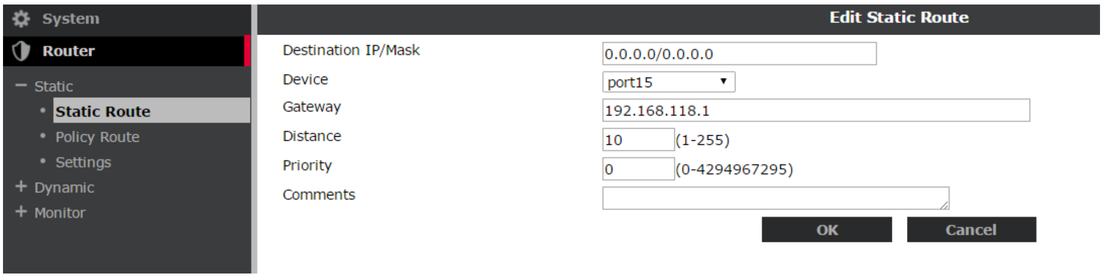
For the detailed configuration process, see section 1.1.2 "Configuring Internet Access via a Static Link" under section 1.1 "Internet Access via a Single Line" in Chapter 1 "Typical Functions of Routing Mode".

IP addresses of interfaces are as follows:



□	port15(outside)	Physical Interface	192.168.118.125/255.255.255.0	::/0
□	port16(Lan)	Physical Interface	192.168.1.200/255.255.255.0	::/0

The routing configuration is as follows:



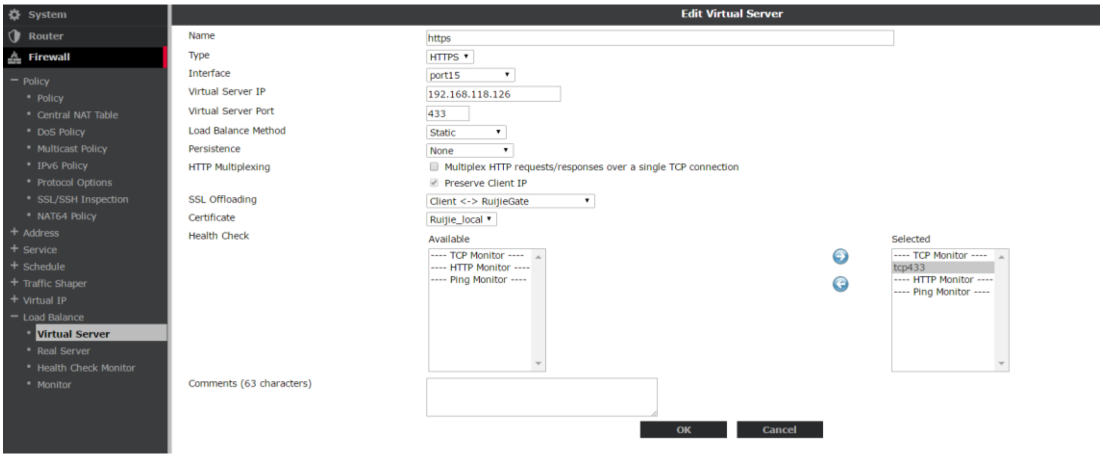
Edit Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port15
Gateway	192.168.118.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Configure the load balancing server.

(1) Configure the load balancing server.

Choose **Firewall** > **Load Balance** > **Virtual Server**, and then click **Create New** to create a virtual server, as shown in the following figure.



Edit Virtual Server

Name	https
Type	HTTPS
Interface	port15
Virtual Server IP	192.168.118.126
Virtual Server Port	433
Load Balance Method	Static
Persistence	None
HTTP Multiplexing	□ Multiplex HTTP requests/responses over a single TCP connection ☑ Preserve Client IP
SSL Offloading	Client <-> RuijieGate
Certificate	Ruijie_local
Health Check	Available: ---- TCP Monitor ---- ---- HTTP Monitor ---- ---- Ping Monitor ---- Selected: ---- TCP Monitor ---- tcp433 ---- HTTP Monitor ---- ---- Ping Monitor ----
Comments (63 characters)	

Name: Enter **https**. This item is user-defined and can be modified as required.

Type: HTTP, TCP, UDP, and IP are supported. **HTTP** is chosen in this example. For the DNS server, choose UDP.

Interface: Choose **port15**. It indicates the port where the firewall is connected to the Internet.

Virtual Server IP: Enter **192.168.118.126**. It indicates the IP address where the server provides external services.

Load Balance Method: Static, Round-Robin, Weighted, First Alive, Least RTT, Least-conn, and HTTP Host are supported.

Persistence: Choose **http cookie**.

HTTP Multiplexing: This item is optional. Multiple links requested by a customer can be merged into one request to reduce the server load.

SSL Offloading: **client--RuijieGate** indicates that a client and the firewall are connected via SSL, and the firewall and a server are connected via a plaintext password to reduce the server load.

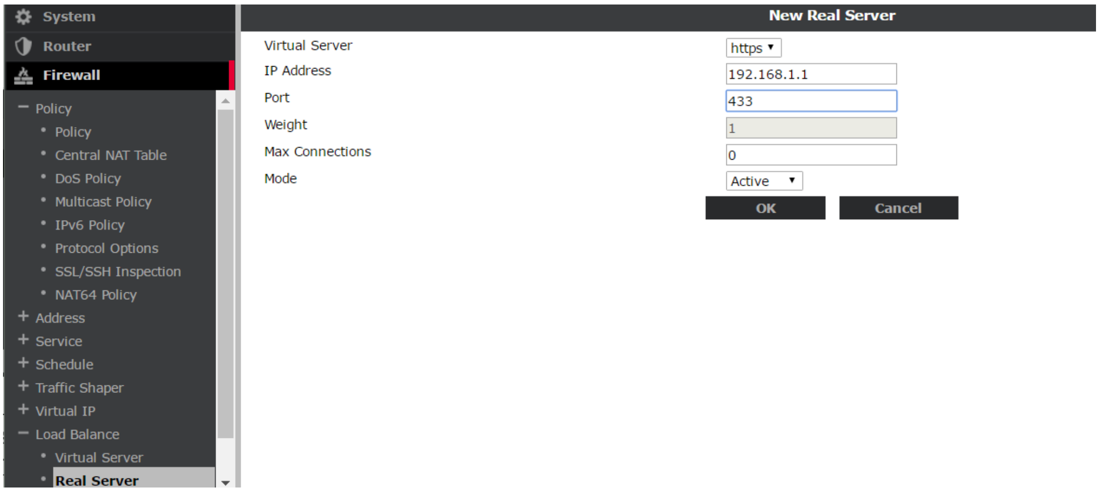
client--RuijieGate--server indicates that a client and the firewall are connected via SSL, and the firewall and a server are connected also via SSL.

Certificate: Choose the certificate that is applied for the server. In this example, the valid certificate of the website is web.

Health check: This item is optional. If there is only one real server, it is set by default. (The configuration is similar to HTTP.)

(2) Configure a real server.

Choose **Firewall** > **Load Balance** > **Real Server**, and then click **Create New** to create two real servers, as shown in the following figure.



New Real Server

Virtual Server	https
IP Address	192.168.1.1
Port	433
Weight	1
Max Connections	0
Mode	Active

Virtual Server: Choose **https**. It indicates the virtual server for which a real server is configured.

IP Address: It indicates IP address of the real server.

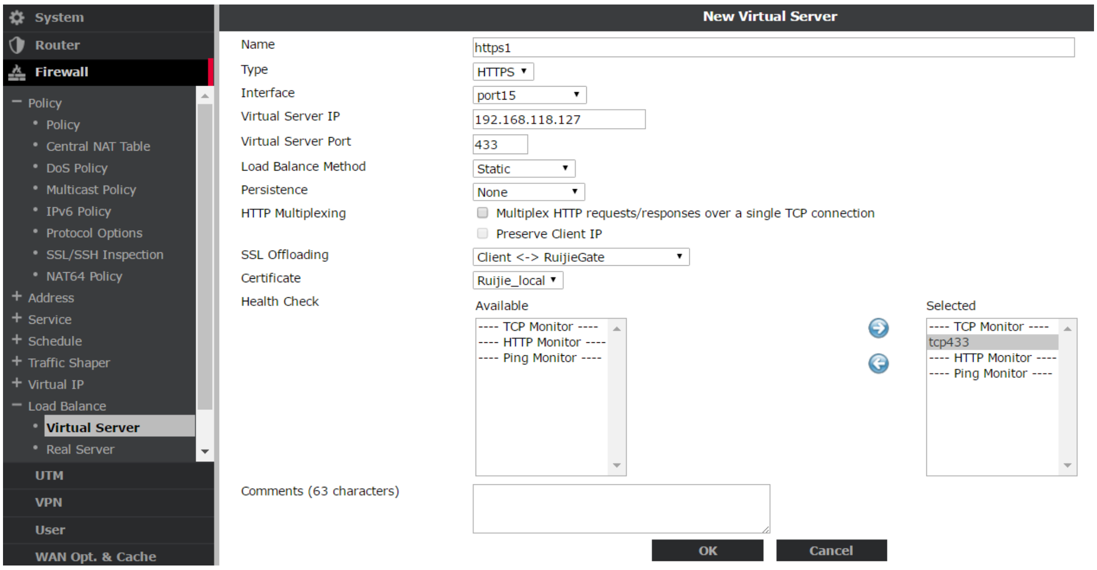
Port: It indicates the HTTP service port of the real server, which may be different from the server port of the virtual server.

Weight: It is disabled in this example. If the load balance method is set to weighted, specify the percentage, such as 10:10.

Max Connections: The value **0** indicates no restriction.

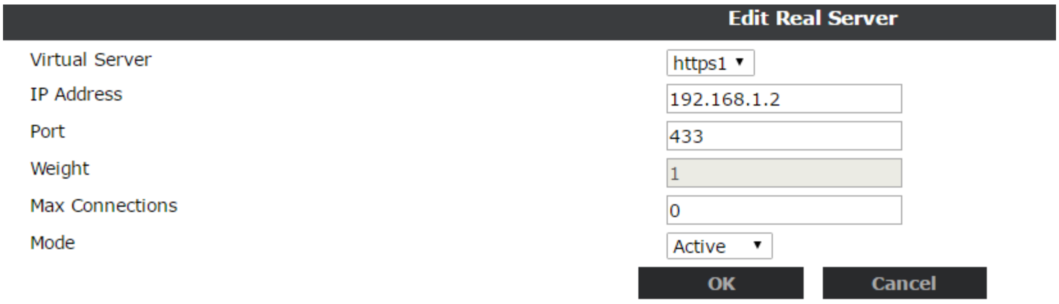
Mode: Choose **Active**. Three options are available: active, inactive, and standby are optional.

(3) Configure the second server in the above way.



New Virtual Server

Name	https1
Type	HTTPS
Interface	port15
Virtual Server IP	192.168.118.127
Virtual Server Port	433
Load Balance Method	Static
Persistence	None
HTTP Multiplexing	□ Multiplex HTTP requests/responses over a single TCP connection □ Preserve Client IP
SSL Offloading	Client <-> RuijieGate
Certificate	Ruijie_local
Health Check	Available: ---- TCP Monitor ----, ---- HTTP Monitor ----, ---- Ping Monitor ---- Selected: ---- TCP Monitor ----, tcp433, ---- HTTP Monitor ----, ---- Ping Monitor ----
Comments (63 characters)	

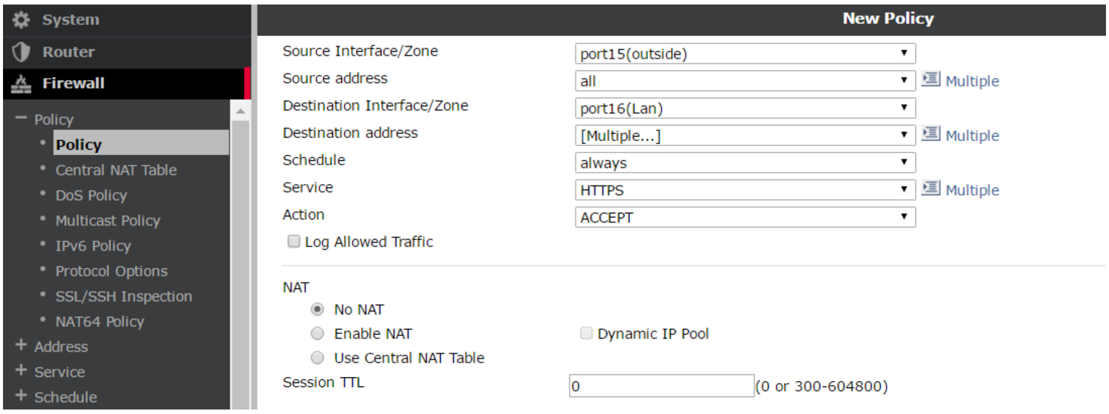


Edit Real Server

Virtual Server	https1 ▾
IP Address	192.168.1.2
Port	433
Weight	1
Max Connections	0
Mode	Active ▾

(4) Configure a safety policy.

Choose **Firewall** > **Policy** > **Policy**, and then click **Create New**. In the **New Policy** window, create a policy.



New Policy

Source Interface/Zone	port15(outside) ▾
Source address	all ▾ Multiple
Destination Interface/Zone	port16(Lan) ▾
Destination address	[Multiple...] ▾ Multiple
Schedule	always ▾
Service	HTTPS ▾ Multiple
Action	ACCEPT ▾

□ Log Allowed Traffic

NAT
● No NAT
○ Enable NAT   □ Dynamic IP Pool
○ Use Central NAT Table

Session TTL 0 (0 or 300-604800)

Click **Multiple** behind **Destination address**, and choose two virtual IP addresses that have been defined.

Source Interface/Zone: Choose **wan1**.

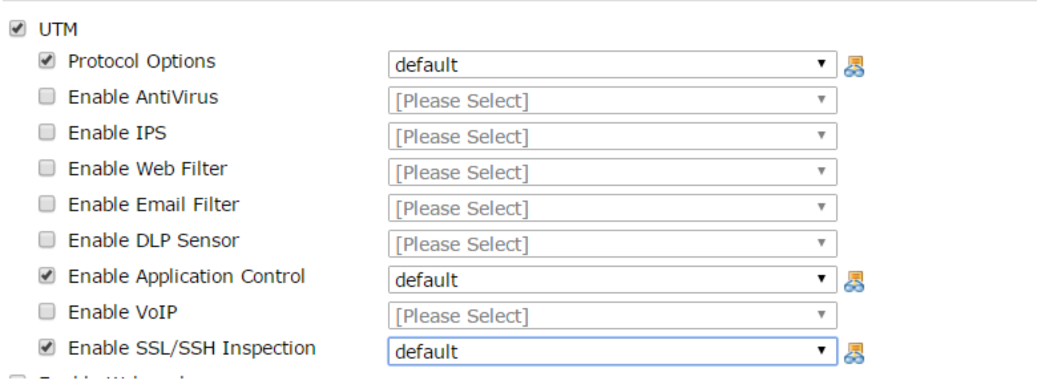
Source address: Choose **all**.

Destination Interface/Zone: Choose **internal**.

Destination address: Click **Multiple** to choose **https** and **https 1**.

Service: Choose **HTTPS**.

In the policy, enable the HTTP archiving function of DLP, and tick **Enable SSL/SSH Inspection**.



☑ UTM

☑ Protocol Options	default ▾
□ Enable AntiVirus	[Please Select] ▾
□ Enable IPS	[Please Select] ▾
□ Enable Web Filter	[Please Select] ▾
□ Enable Email Filter	[Please Select] ▾
□ Enable DLP Sensor	[Please Select] ▾
☑ Enable Application Control	default ▾
□ Enable VoIP	[Please Select] ▾
☑ Enable SSL/SSH Inspection	default ▾

V. Verification

Access http://www.test.com from an external address to view logs.

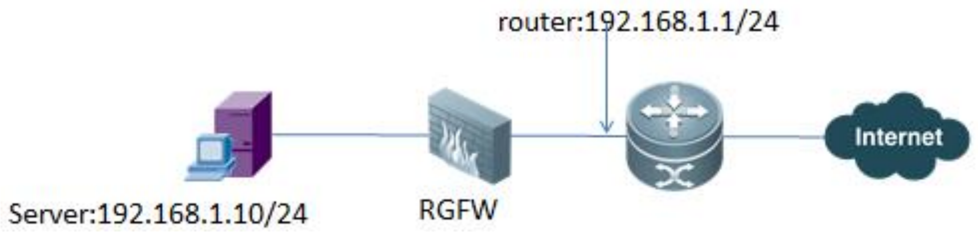
4 Configuring Transparent Mode

4.1 Enabling Transparent Mode

Networking Requirements

Without changing the current network topology, deploy the firewall NGFW in transparent mode between the router and server. The firewall works in transparent mode to protect server 192.168.1.10.

Network Topology



Configuration Tips

- Set the firewall to work in transparent mode.
- Add the server address.
- Configure the policy.

Configuration Steps

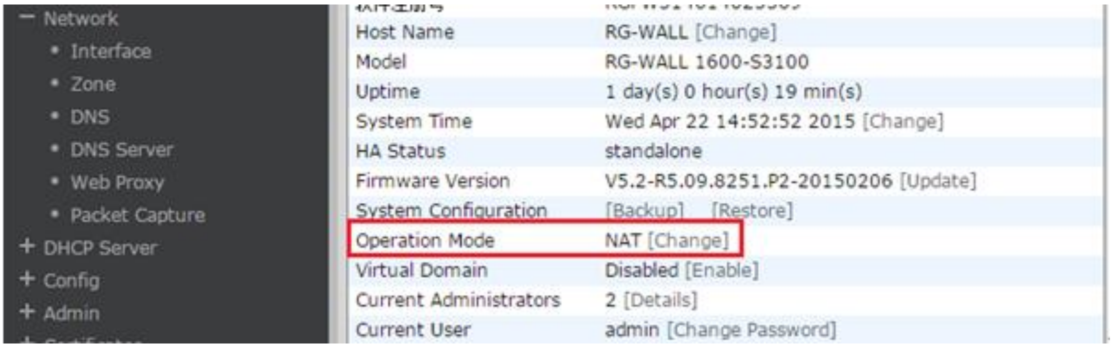
For the M5100, take the following steps to convert the LAN port into the routing port, and then switch to the transparent mode. For other modes, such operation is not required. Delete the policy, route, and DHCP configuration related to the LAN port.

```
RG-WALL#config system virtual-switch
     RG-WALL# (virtual-switch)#delete lan
     RG-WALL# end
```

Before operation, it is recommended to upgrade the firewall version to the latest.

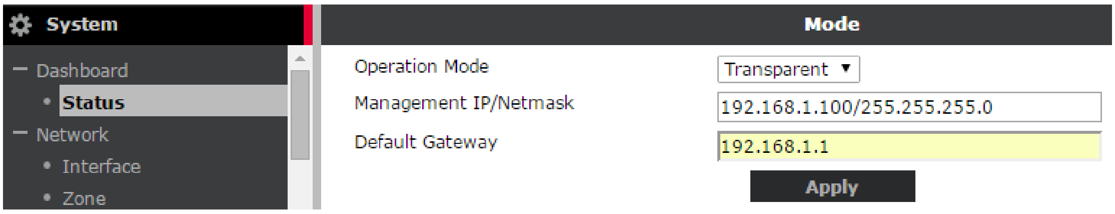
1. **Set the firewall to work in transparent mode.**

Choose **System** > **Dashboard** > **Status**. The information on the home page is as follows:



Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	1 day(s) 0 hour(s) 19 min(s)
System Time	Wed Apr 22 14:52:52 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	2 [Details]
Current User	admin [Change Password]

Click **Change** in the **Operation Mode** field. Change the value of **Operation Mode** into **Transparent**. Set the management IP address and gateway for the device. See the following figure:

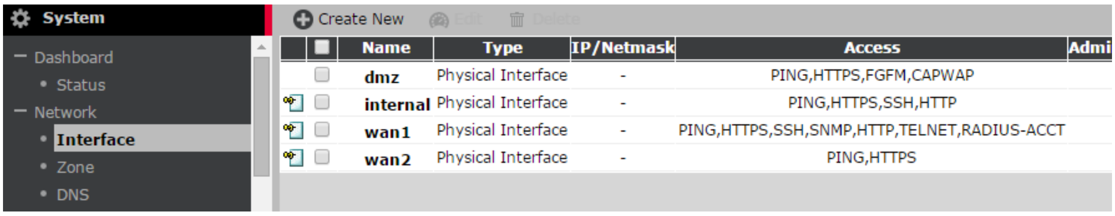


Operation Mode	Transparent ▼
Management IP/Netmask	192.168.1.100/255.255.255.0
Default Gateway	192.168.1.1

In transparent mode, the interface address cannot be written. There is only one user-managed device IP address. To manage the device through an interface, run the following command to enable management via the interface (mgmt or mgmt1 interface by default). The following takes port1 as an example:

```
RG-WALL#config system interface
           RG-WALL (interface)#edit port1
           RG-WALL (port1)#set allowaccess ping https ssh telnet
           RG-WALL (port1)#end
```

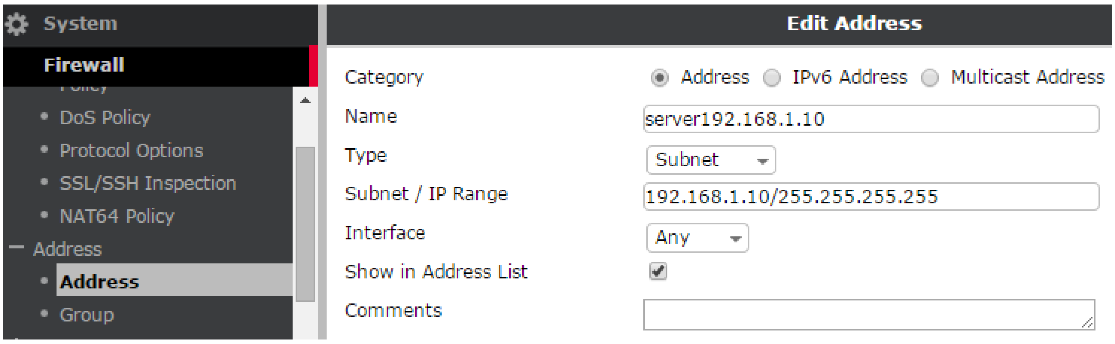
The following figure shows interfaces:



□	Name	Type	IP/Netmask	Access	Admi
□	dmz	Physical Interface	-	PING,HTTPS,FGFM,CAPWAP	
□	internal	Physical Interface	-	PING,HTTPS,SSH,HTTP	
□	wan1	Physical Interface	-	PING,HTTPS,SSH,SNMP,HTTP,TELNET,RADIUS-ACCT	
□	wan2	Physical Interface	-	PING,HTTPS	

2. Add the server address.

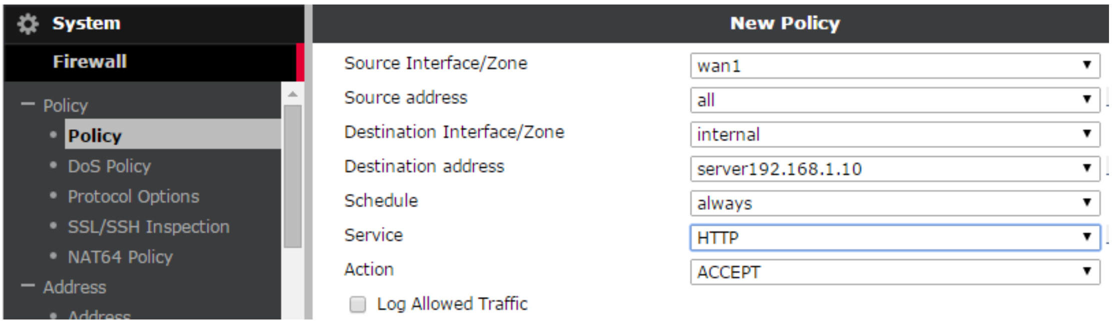
Choose **Firewall** > **Address** > **Address**, and then click **Create New** to add the server address, as shown in the following figure:



Category	● Address ○ IPv6 Address ○ Multicast Address
Name	server192.168.1.10
Type	Subnet
Subnet / IP Range	192.168.1.10/255.255.255.255
Interface	Any
Show in Address List	☑
Comments	

3. Add the policy.

Choose **Firewall** > **Policy** > **Policy**, and then click **Create New**. Add the policy, as shown in the following figure to allow extranet users to access the HTTP service of server 192.168.1.10.



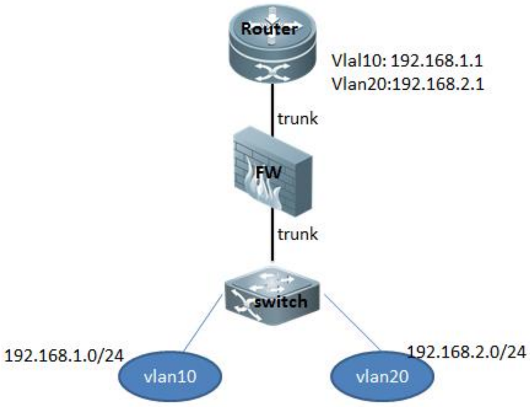
Source Interface/Zone: wan1
Source address: all
Destination Interface/Zone: internal
Destination address: server192.168.1.10
Schedule: always
Service: HTTP
Action: ACCEPT
□ Log Allowed Traffic

4.2 VLAN and Transparent Mode

Networking Requirements

There are two VLANs (in trunk environment) established on the intranet. The gateway is deployed on the router. The firewall works in transparent mode between the core switch and core router. Two VLANs, enabled with virus filtering, are allowed to access the extranet under protection.

Network Topology



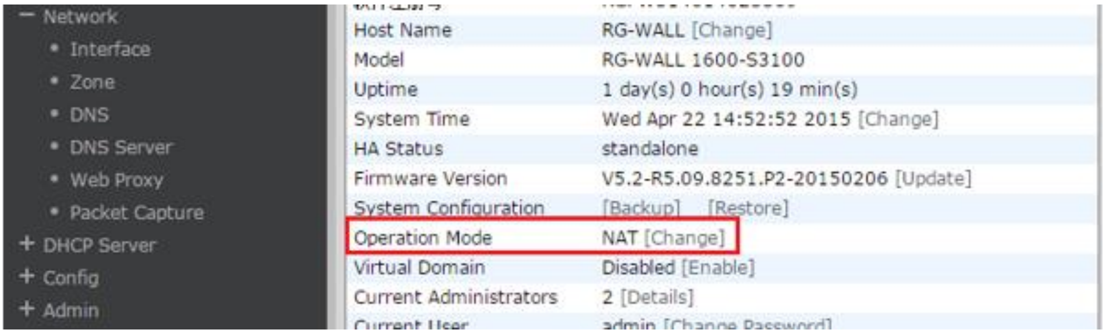
Configuration Tips

- Configure the transparent mode.
- Create VLAN sub-interfaces.
- Configure the forwarding domain.
- Configure the policy.

Configuration Steps

1. Configure the transparent mode.

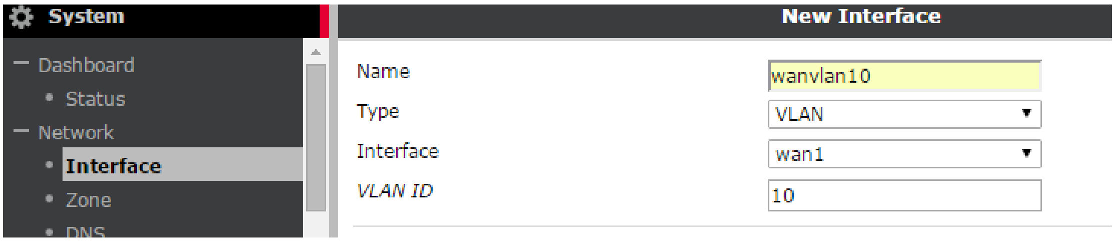
For the detailed configuration steps, see section 2.1 “How to Enable Transparent Mode”. Click **Change** in the **Operation Mode** field. Change the value of **Operation Mode** into **Transparent**. Configure the management address and gateway for the firewall. See the following figure:



Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	1 day(s) 0 hour(s) 19 min(s)
System Time	Wed Apr 22 14:52:52 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	2 [Details]
Current User	admin [Change Password]

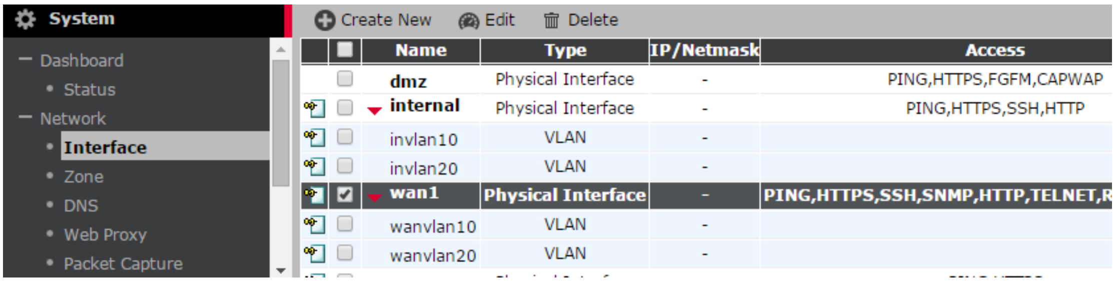
2. Establish VLAN sub-interfaces.

Choose **System** > **Network** > **Interface**, and then click **Create New**. Create a VLAN interface, as shown in the following figure:



Name	wanvlan10
Type	VLAN
Interface	wan1
VLAN ID	10

Create four VLAN interfaces in the same way. Respectively create VLAN10 and VLAN20 sub-interfaces on wan1 and internal interfaces. The configured VLAN interfaces are displayed as shown in the following figure:



	Name	Type	IP/Netmask	Access
□	dmz	Physical Interface	-	PING,HTTPS,FGFM,CAPWAP
□	internal	Physical Interface	-	PING,HTTPS,SSH,HTTP
□	invlan10	VLAN	-	
□	invlan20	VLAN	-	
☑	wan1	Physical Interface	-	PING,HTTPS,SSH,SNMP,HTTP,TELNET,R
□	wanvlan10	VLAN	-	
□	wanvlan20	VLAN	-	

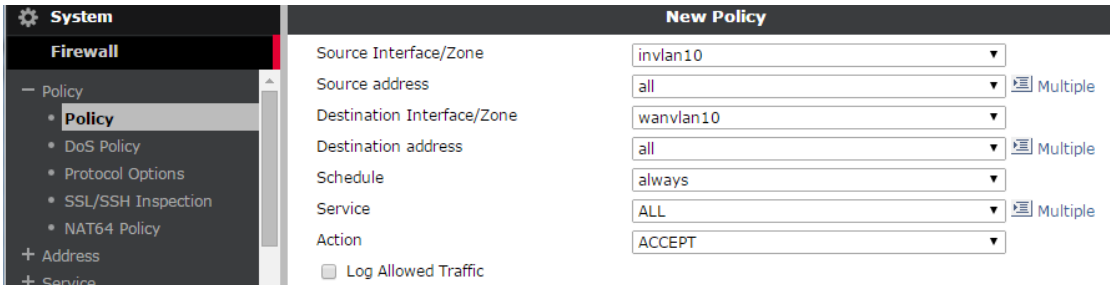
3. Configure the forwarding domain. (CLI is mandatory.)

```
RG-WALL #config system interface
        RG-WALL (interface) #edit wanvlan10
        RG-WALL (wanvlan10)#set forward-domain 10
        RG-WALL (wanvlan10)#next
        RG-WALL (interface) #edit invlan10
        RG-WALL (invlan10)#set forward-domain 10                                     //Put the
uplink interfaces wanvlan10 and invlan10 into one forwarding domain. Only within one
forwarding domain can they communicate.
        RG-WALL (invlan10)#next
        RG-WALL (interface) #edit wanvlan20
        RG-WALL (wanvlan20)#set forward-domain 20
        RG-WALL (wanvlan20)#next
        RG-WALL (interface) #edit invlan20
        RG-WALL (invlan20)#set forward-domain 20
        RG-WALL (invlan20)#end
```

4. Configure the policy.

1) Configure the policy for VLAN10.

For the detailed configuration steps, see section "Configuring Internet Access via a Static Link" under section 1.1 "Internet Access via a Single Line" in "Configuring Routing Mode". The policy configuration is as follows:



New Policy

Source Interface/Zone: invlan10

Source address: all

Destination Interface/Zone: wanvlan10

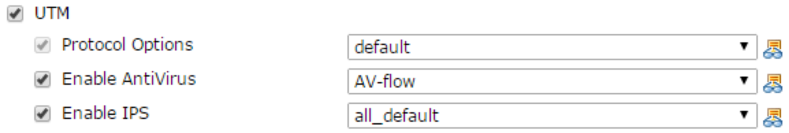
Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

☐ Log Allowed Traffic



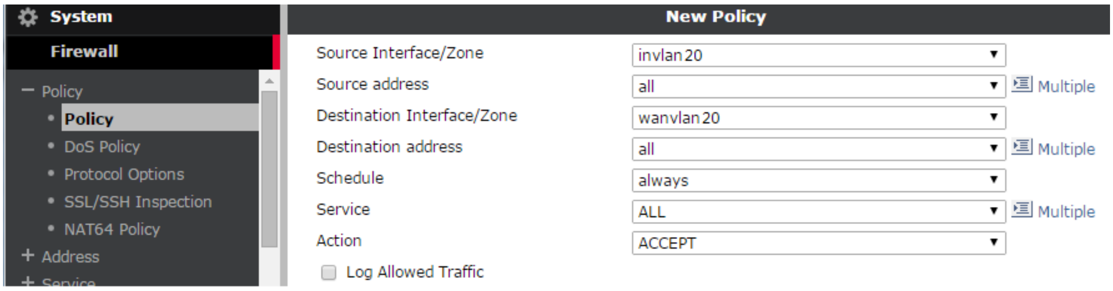
☑ UTM

☑ Protocol Options: default

☑ Enable AntiVirus: AV-flow

☑ Enable IPS: all_default

2) Configure the policy for vlan20, as shown in the following figure:



New Policy

Source Interface/Zone: invlan20

Source address: all

Destination Interface/Zone: wanvlan20

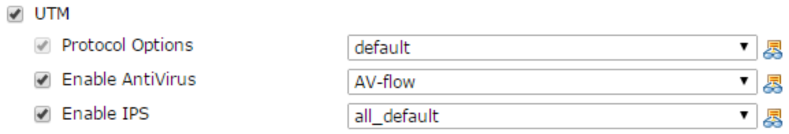
Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

☐ Log Allowed Traffic



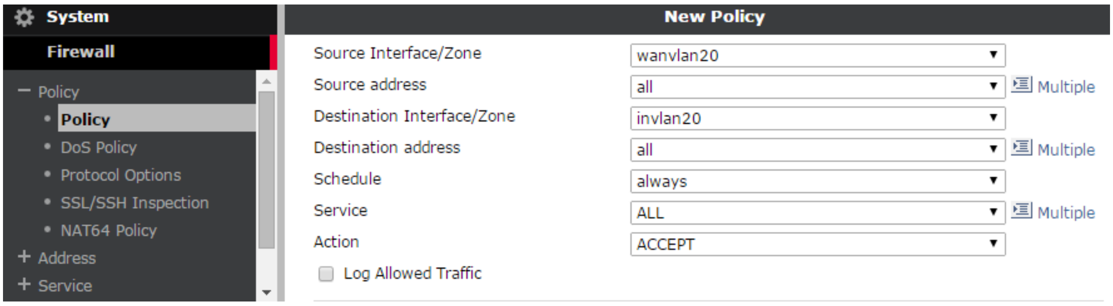
☑ UTM

☑ Protocol Options: default

☑ Enable AntiVirus: AV-flow

☑ Enable IPS: all_default

3) When VLAN10 and VLAN20 access each other, configure the policy for the access from wanvlan10 to invlan10 and another policy from wanvlan20 to invlan20. See the following figure:



New Policy

Source Interface/Zone: wanvlan20

Source address: all

Destination Interface/Zone: invlan20

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

☐ Log Allowed Traffic

Verification

Test Internet access and virus detection respectively on vlan10 and vlan20.

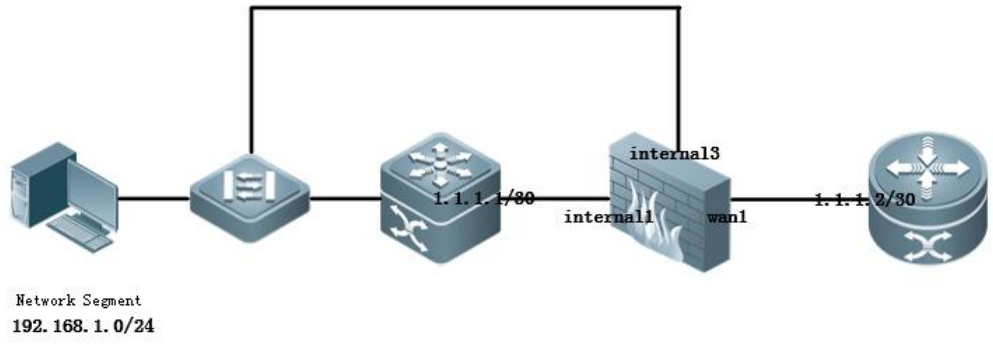
4.3 Out-of-Band Management in Transparent Mode

Networking Requirements

The firewall deployed in transparent mode requires out-of-band management.

- On the firewall, configure an IP address the same as that of the management network segment.
- The local route generated by the management IP address does not come into conflict with the regular business data, such as asynchronous route.

Network Topology



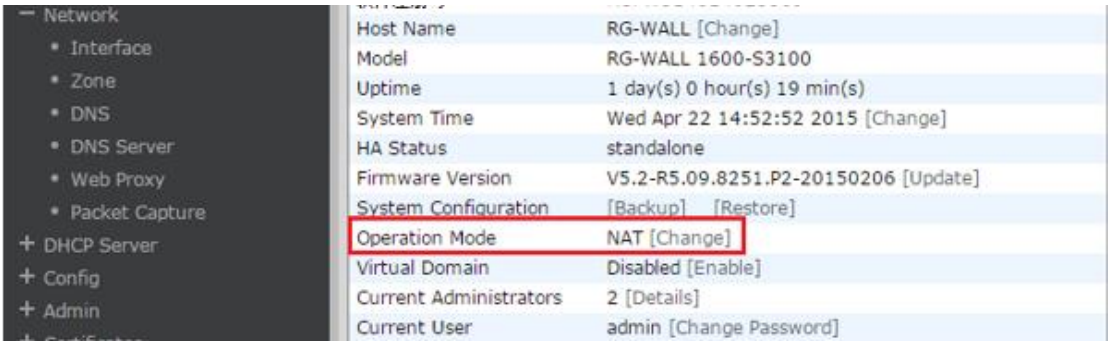
Configuration Tips

- Enable VDOM.
- Assign the interface connected to the management network segment to one VDOM. (**internal3** interface in this example)
- Configure the management IP address and management access mode for **internal3** interface.

Configuration Steps

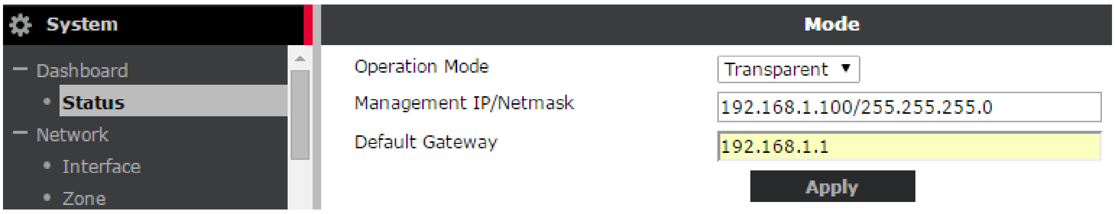
1. **Enable the transparent mode.**

Choose **System** > **Dashboard** > **Status**. The information on the home page is displayed as follows:



Host Name RG-WALL [Change]
Model RG-WALL 1600-S3100
Uptime 1 day(s) 0 hour(s) 19 min(s)
System Time Wed Apr 22 14:52:52 2015 [Change]
HA Status standalone
Firmware Version V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration [Backup] [Restore]
Operation Mode NAT [Change]
Virtual Domain Disabled [Enable]
Current Administrators 2 [Details]
Current User admin [Change Password]

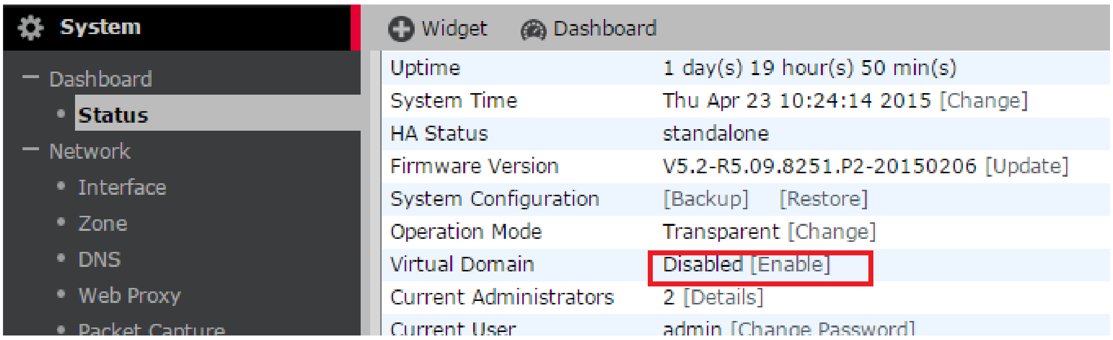
Click **Change** in the **Operation Mode** field. Change the value of **Operation Mode** into **Transparent**, as shown in the following figure:



Operation Mode Transparent
Management IP/Netmask 192.168.1.100/255.255.255.0
Default Gateway 192.168.1.1

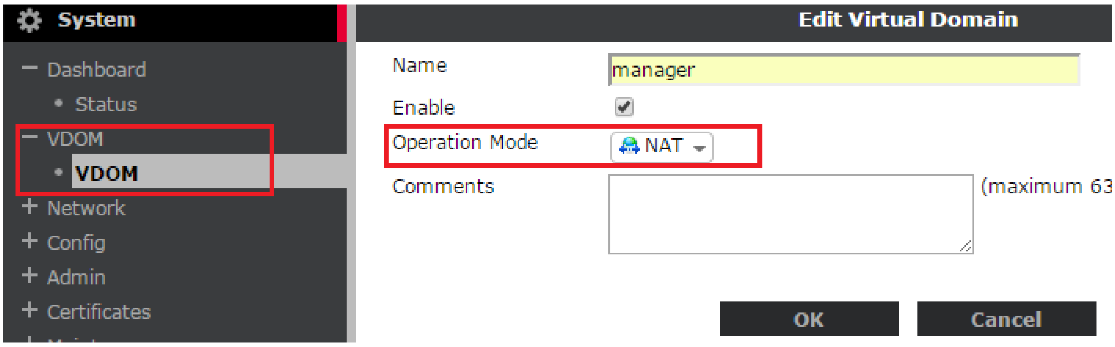
2. **Configure the VDOM.**

Choose **System** > **Dashboard** > **Status**. Find the **Virtual Domain** value, as shown in the following figure:



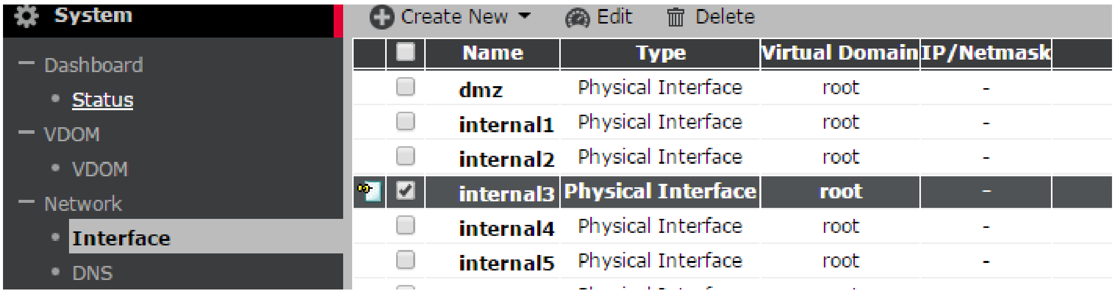
Uptime 1 day(s) 19 hour(s) 50 min(s)
System Time Thu Apr 23 10:24:14 2015 [Change]
HA Status standalone
Firmware Version V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration [Backup] [Restore]
Operation Mode Transparent [Change]
Virtual Domain Disabled [Enable]
Current Administrators 2 [Details]
Current User admin [Change Password]

Create a VDOM named **manager**, as shown in the following figure:



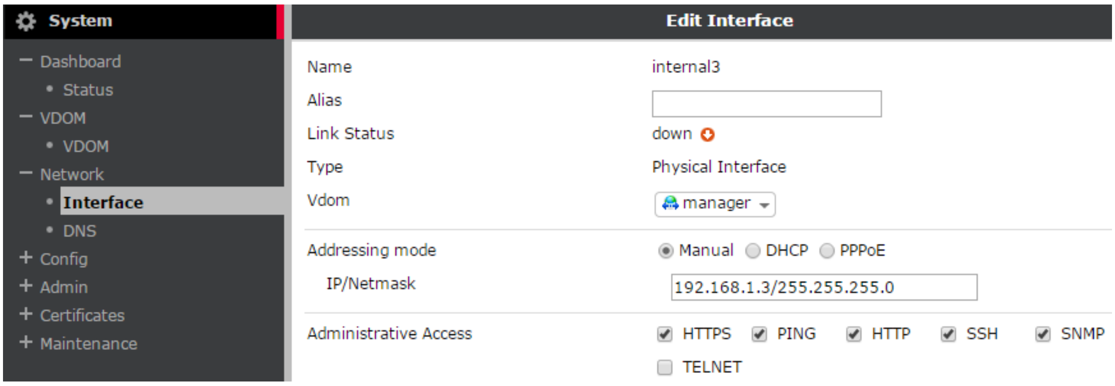
Name manager
Enable ☑
Operation Mode NAT
Comments (maximum 63

3. **Assign management interface internal3 to VDOM manager. Choose System > Network > Interface and then click Edit, as shown in the following figure:**



☐	Name	Type	Virtual Domain	IP/Netmask
☐	dmz	Physical Interface	root	-
☐	internal1	Physical Interface	root	-
☐	internal2	Physical Interface	root	-
☑	internal3	Physical Interface	root	-
☐	internal4	Physical Interface	root	-
☐	internal5	Physical Interface	root	-

Edit **internal3** interface, as shown in the following figure:



Edit Interface

Name: internal3

Alias:

Link Status: down

Type: Physical Interface

Vdom: manager

Addressing mode: ● Manual ○ DHCP ○ PPPoE

IP/Netmask: 192.168.1.3/255.255.255.0

Administrative Access: ☑ HTTPS ☑ PING ☑ HTTP ☑ SSH ☑ SNMP ☐ TELNET

Vdom: Choose **manager**.

IP/Netmask: Set it to **192.168.1.3/24** (in the management network segment).

Administrative Access: Tick **HTTPS**, **PING**, and **SSH**.

Verification

Set the IP address of the PC to 192.168.1.1/24. Access the web management page of the firewall by https://192.168.1.3.

- The firewall can be managed.
- The PC in the management network segment can access the Internet.

Notes

If the out-of-band management port is not required and the firewall in bridge mode is directly managed (**internal1** or **wan1** interface in this example), pay attention to the following notes:

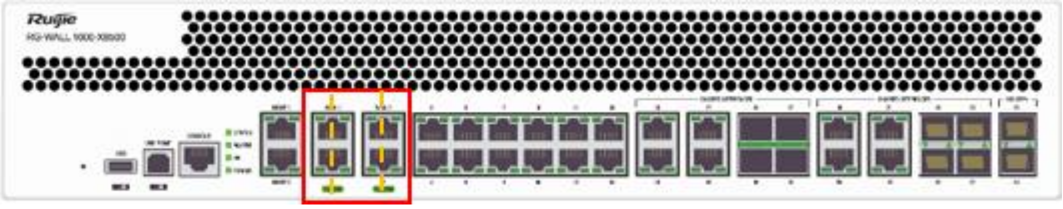
- The bridge IP address is the IP address of the entire firewall instead of the IP address of an interface.
- To manage the firewall in bridge mode through an interface, enable management functions on the corresponding interface, for example, ping, HTTPS, and SSH functions.

In this example, to manage the firewall through **internal1** or **wan1** interface, enable Ping, HTTPS, and SSH management functions of internal1 or wan1 interfaces.

4.4 Bypass Deployment

Bypass Mode

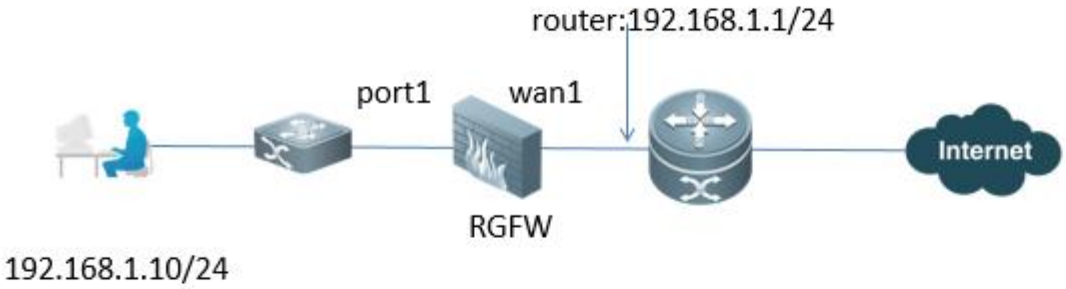
Among the RG-WALL 1600 series new next-generation firewalls, only the X8500 supports two groups of electrical bypass interfaces. That is, after the device is powered off or restarted, communication still proceeds. The two groups of interfaces are wan1---port1 and wan2---port2. The indicators below port1 and port2 are bypass indicators, as shown in the following figure:



For the new NGFW products, only the X8500 supports two groups of electrical bypass interfaces. All the NGFW products do not support optical bypass interfaces.

Network Topology

The firewall works in transparent mode, enabled with the anti-virus function. The bypass interface is used. After the firewall fails, enabling the bypass interface ensures that links work.



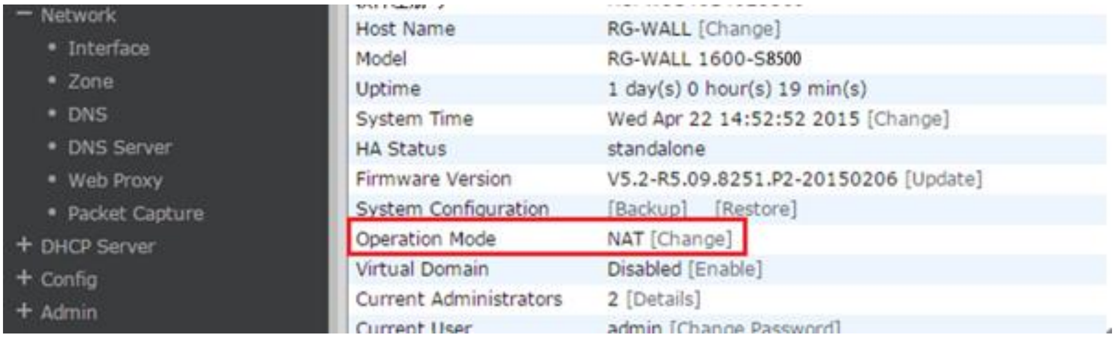
Configuration Tips

- Set the firewall to work in transparent mode.
- Configure a firewall policy.
- Enable bypass mode.

Configuration Steps

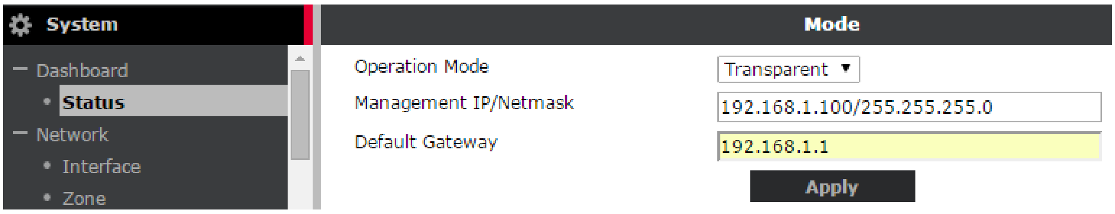
1. **Set the firewall to work in transparent mode.**

Choose **System** > **Dashboard** > **Status**. The information on the home page is as follows:



Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S8500
Uptime	1 day(s) 0 hour(s) 19 min(s)
System Time	Wed Apr 22 14:52:52 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	2 [Details]
Current User	admin [Change Password]

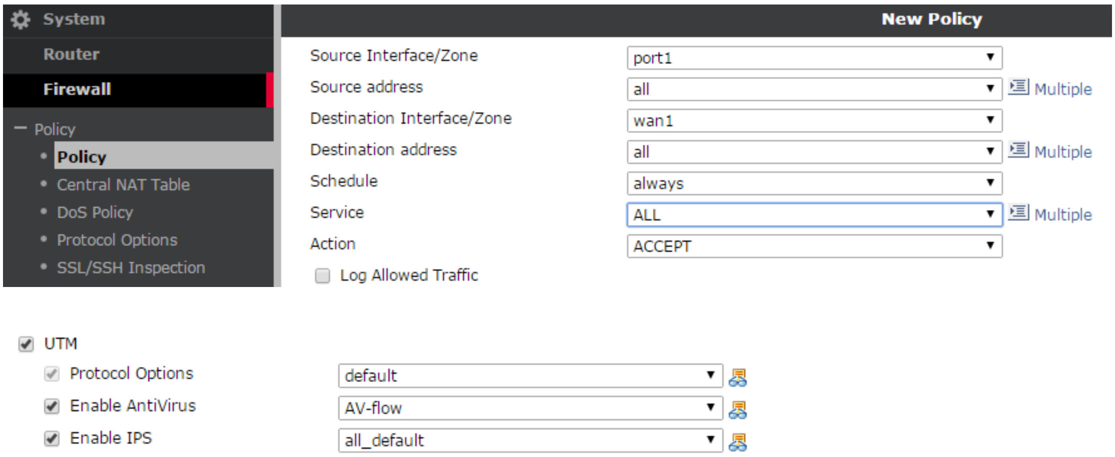
Click **Change** in the **Operation Mode** field. Change the value of **Operation Mode** into **Transparent**. Set the management IP address and gateway for the device. See the following figure:



Operation Mode	Transparent
Management IP/Netmask	192.168.1.100/255.255.255.0
Default Gateway	192.168.1.1

2. Configure a firewall policy.

Choose **Firewall** > **Policy** > **Policy**. Add a policy for Internet access and enable the anti-virus function, as shown in the following figure:



Source Interface/Zone	port1
Source address	all
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT
□ Log Allowed Traffic	
☑ UTM	
☑ Protocol Options	default
☑ Enable AntiVirus	AV-flow
☑ Enable IPS	all_default

3. Enable bypass mode.

```
config system bypass
set bypass-watchdog enable
set poweroff-bypass enable
end
```

Verification

Power off the system or restart the device, but business of customers is not interrupted.

4.5 Notes in Transparent Mode

Notes in Transparent

Mode

1. By default, the new NGFW does not forward BPDU packets. This may cause L2 loops due to STP problems. You can log in to the CLI of the new NGFW and enter the Edit Interface page. Run the following command to enable BPDU forwarding: **set stpforward enable**.

```
   RG-WALL # config system interface
   RG-WALL (interface) #edit port1
   RG-WALL (port1) #set stpforwad enable        #By default, it is disabled.
   RG-WALL (port1) #next
```

Log in to each interface in turns to enable stpforward.

2. You can use forward domain to control the data forwarding among the specified interfaces. The data packets can be forwarded among interfaces with the same forward domain ID.

```
RG-WALL # config system interface
RG-WALL (interface) # edit wan1
RG-WALL (wan1) # set forward-domain 10
RG-WALL (wan1) # next
RG-WALL (interface) # edit wan2
RG-WALL (wan2) # set forward-domain 10
RG-WALL (wan2) # end
```

There is no need to define forward-domain in advance. The forward-domain takes effect immediately after being configured. The broadcast packets can be only broadcast within one forward-domain.

3. Only the Ethernet II frames can be forwarded. By default, the other L2 protocol frames cannot be forwarded. To forward these frames, enable the L2 forward function on the interface.

```
 RG-WALL # config system interface
 RG-WALL (interface) #edit port1
 RG-WALL (port1) #set l2forward enable       #By default, it is disabled.
 RG-WALL (port1) #next
```

Log in to each interface in turns to enable l2forward.

4. By default, multicast packets are not forwarded. To deploy the firewall in transparent mode in the multicast environment, configure the corresponding multicast policy to allow the related multicast data flow to pass the new NGFW. For example, to deploy the firewall in the OSPF or RIP V2 environment, configure a firewall policy to allow data transmitted to 224.0.0.5 and 224.0.0.6/224.0.0.9, or from 224.0.0.5 and 224.0.0.6/224.0.0.9.

```
 RG-WALL # config system settings
 RG-WALL (settings)set multicast-skip-policy enable    #By default, it is disabled.
 RG-WALL (settings)end
```

5. To enable out-of-band management, set multiple VDOMs. VDOM root is only used to manage other

related transparent VDOMs.

6. If you want to deploy the new NGFW in transparent mode between router and host, ensure that MAC addresses of the data flow in this line with the same source and destination IP addresses are the same in different directions on the firewall. For the simple applications, such as VRRP, HSRP and other host route backup protocols, set the static IP/MAC addresses on the firewall to enable the new NGFW to learn the VRRP group or HSRP group to which the specified virtual MAC address belongs . Note: Only one identical MAC address pair is specified for one forward_domain.

7. Check the MAC table in transparent mode.

```
Run diag netlink brctl name host <VDOM_name>.b to check the MAC table in transparent mode.
The following example takes VDOM root as an example.
RGFW# diag netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table
port no device devname mac addr ttl attributes
2 7 wan2 02:09:0f:78:69:00 0 Local Static
5 6 trunk_1 02:09:0f:78:69:01 0 Local Static
3 8 dmz 02:09:0f:78:69:01 0 Local Static
4 9 internal 02:09:0f:78:69:02 0 Local Static
3 8 dmz 00:80:c8:39:87:5a 194
4 9 internal 02:09:0f:78:67:68 8
1 3 wan1 00:09:0f:78:69:fe 0 Local Static
```

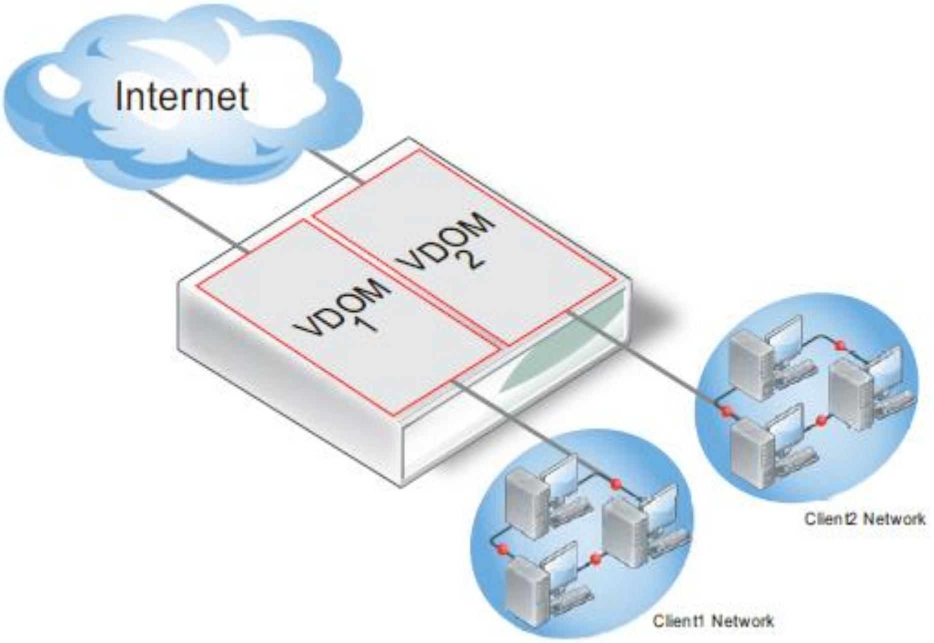
8. Limitation of the transparent mode.

- Only IPSec VPN in policy mode is supported. User authentication is supported.
- The interface mode, SSL VPN, dynamic routing, policy-based routing or DHCP is not supported.

5 Configuring VDOM

5.1 Enabling VDOM

Overview



A virtual domain (VDOM) can be regarded as a virtual firewall. The VDOM technique can divide one RG-WALL device into two or more virtual devices with different firewall policies which function independently. In NAT or routing mode, VDOMs can be configured separately and accessed mutually, providing routing or VPN services for connected networks or organizations. Different VDOMs can be assigned manually with differentiated system resources, which generally adapts to multiple networks that should be split like cloud network. Because the next-generation firewall (NGFW) can work in NAT or transparent mode, VDOMs must be adopted in the hybrid mode.

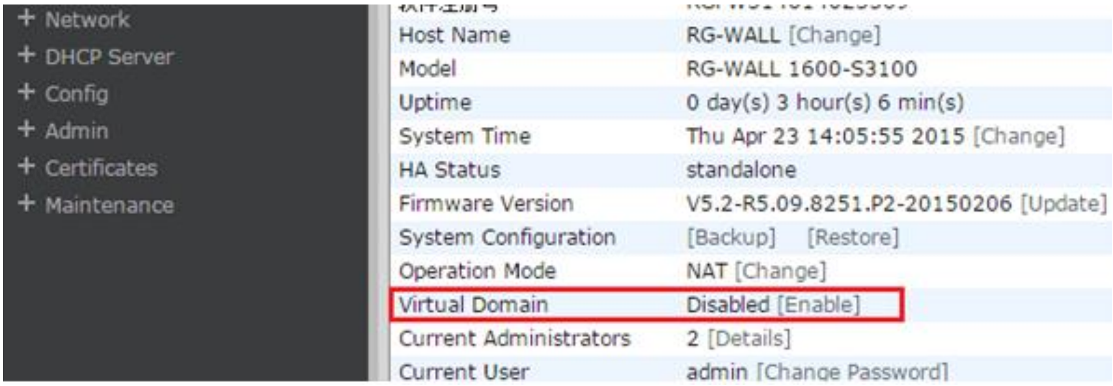
Configuration Tips

- Enable VDOM.
- Add a VDOM.
- Add interfaces to the VDOM.
- Assign resources to the VDOM. (Optional)
- Assign the administrator account to the VDOM. (Optional)

Configuration Steps

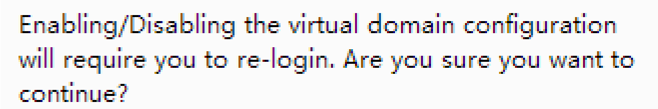
1. Enable VDOM.

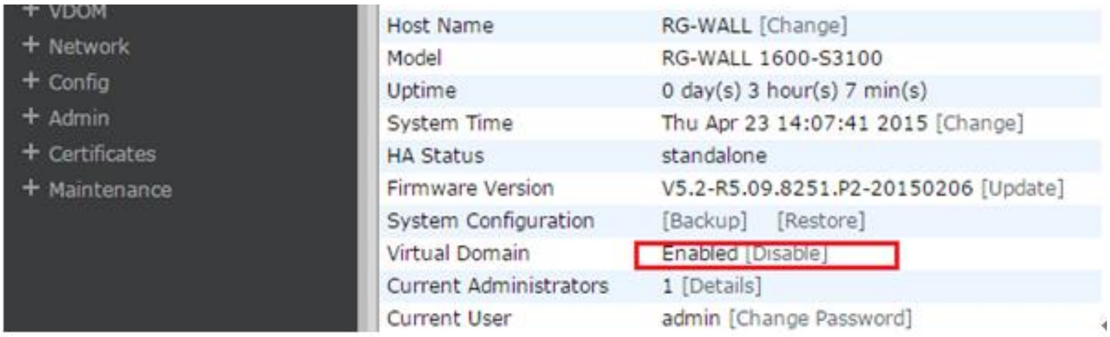
Choose **System** > **Dashboard** > **Status**. Locate the **Virtual Domain** value among system information, as shown in the following figure:



Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 3 hour(s) 6 min(s)
System Time	Thu Apr 23 14:05:55 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	2 [Details]
Current User	admin [Change Password]

Click **Enable** corresponding to **Virtual Domain**. The system requires you to re-login. After re-login, VDOM is enabled. See the following figure:

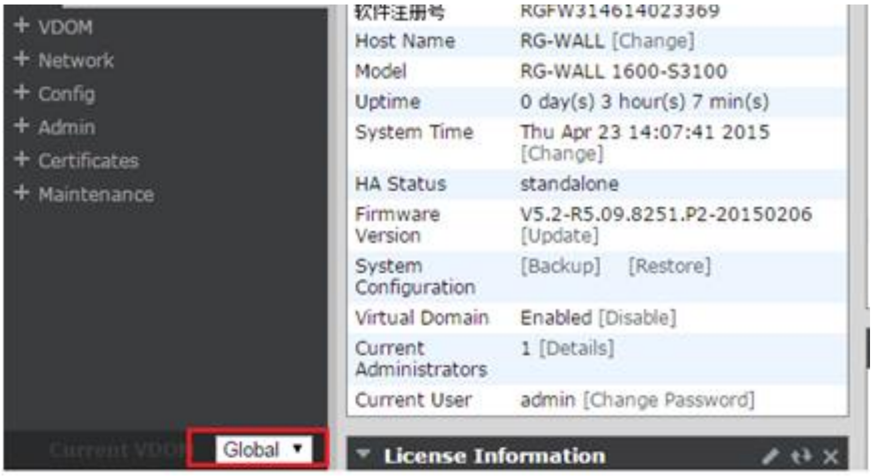

Enabling/Disabling the virtual domain configuration will require you to re-login. Are you sure you want to continue?



Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 3 hour(s) 7 min(s)
System Time	Thu Apr 23 14:07:41 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Virtual Domain	Enabled [Disable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

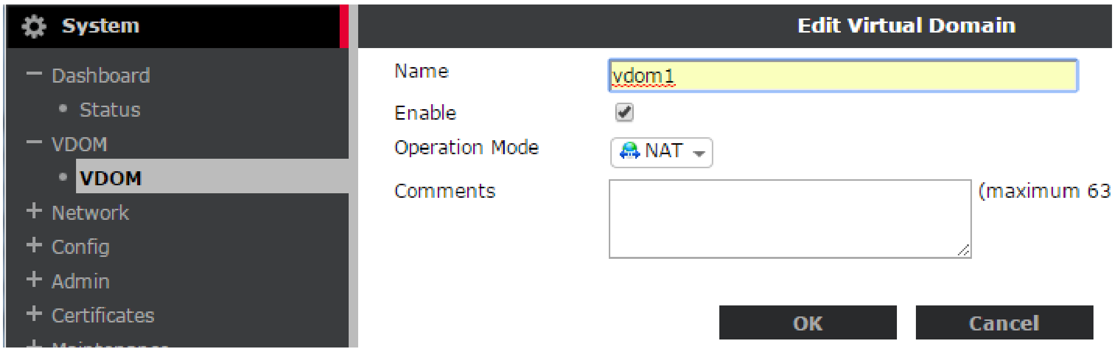
2. Add a VDOM.

Adding a VDOM is completed in global configuration mode. After step 1, the system runs in global configuration mode by default. See the following figure:



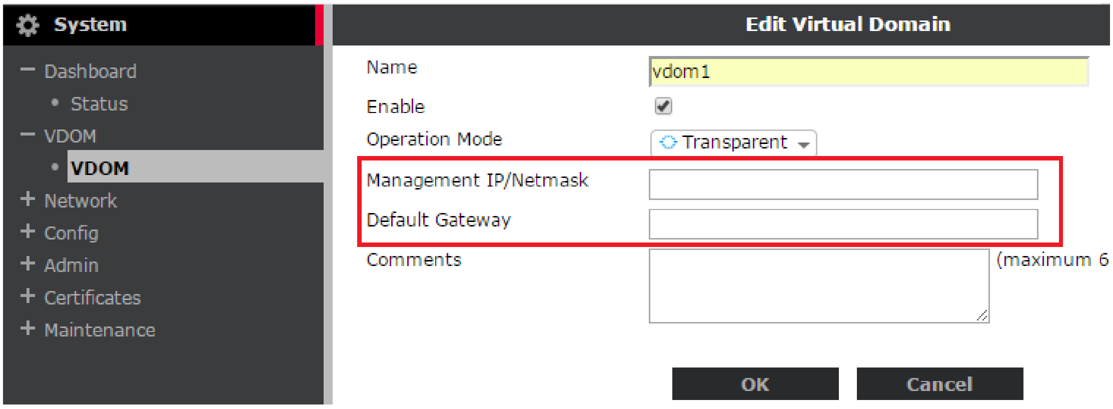
软件注册号	RGFW314614023369
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 3 hour(s) 7 min(s)
System Time	Thu Apr 23 14:07:41 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Virtual Domain	Enabled [Disable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

Choose **System** > **VDOM** > **VDOM**. The default vdom root is displayed. Click **Create New**. Enter a VDOM name in the displayed **Edit Virtual Domain** dialog box, and then click **OK**.



Edit Virtual Domain

Name	vdom1
Enable	☑
Operation Mode	NAT
Comments	(maximum 63



Edit Virtual Domain

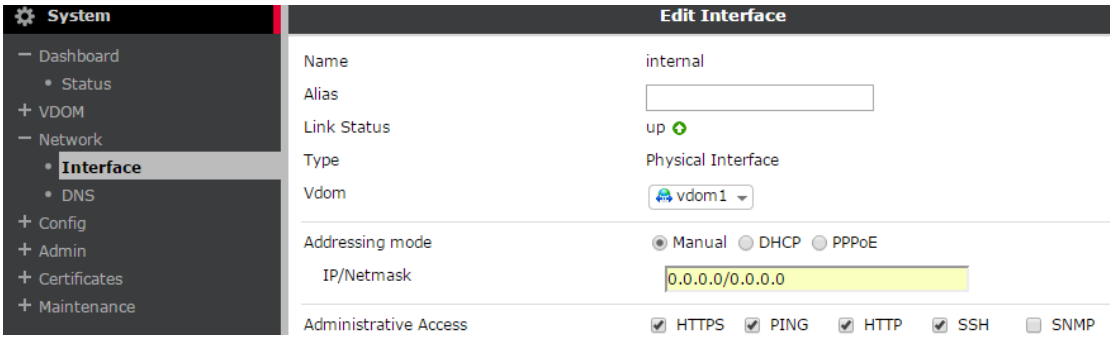
Name	vdom1
Enable	☑
Operation Mode	Transparent
Management IP/Netmask	
Default Gateway	
Comments	(maximum 6

If **Operation Mode** is set to **Transparent**, you need to configure the management IP address and default gateway.

3. Add interfaces to the VDOM.

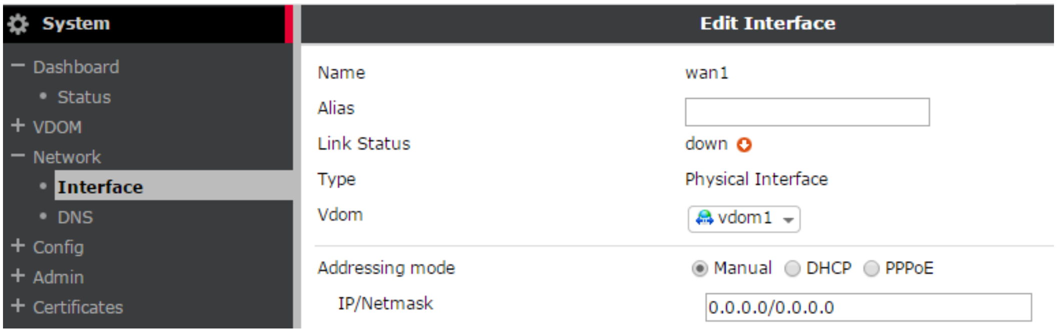
For the newly created VDOM, add interfaces to it. The interfaces can be physical or virtual.

Choose **System** > **Network** > **Interface** to edit the interfaces. The following figure shows that internal and wan1 are added to the VDOM:



Edit Interface

Name	internal
Alias	
Link Status	up
Type	Physical Interface
Vdom	vdom1
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	0.0.0.0/0.0.0.0
Administrative Access	☑ HTTPS ☑ PING ☑ HTTP ☑ SSH □ SNMP



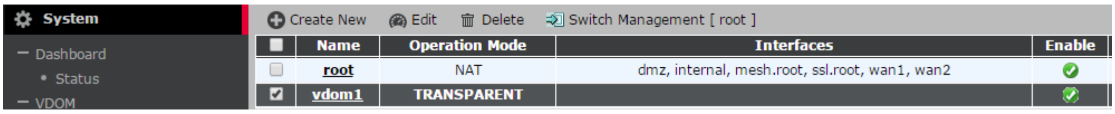
Edit Interface

Name	wan1
Alias	
Link Status	down
Type	Physical Interface
Vdom	vdom1
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	0.0.0.0/0.0.0.0

4. Assign resources to the VDOM.

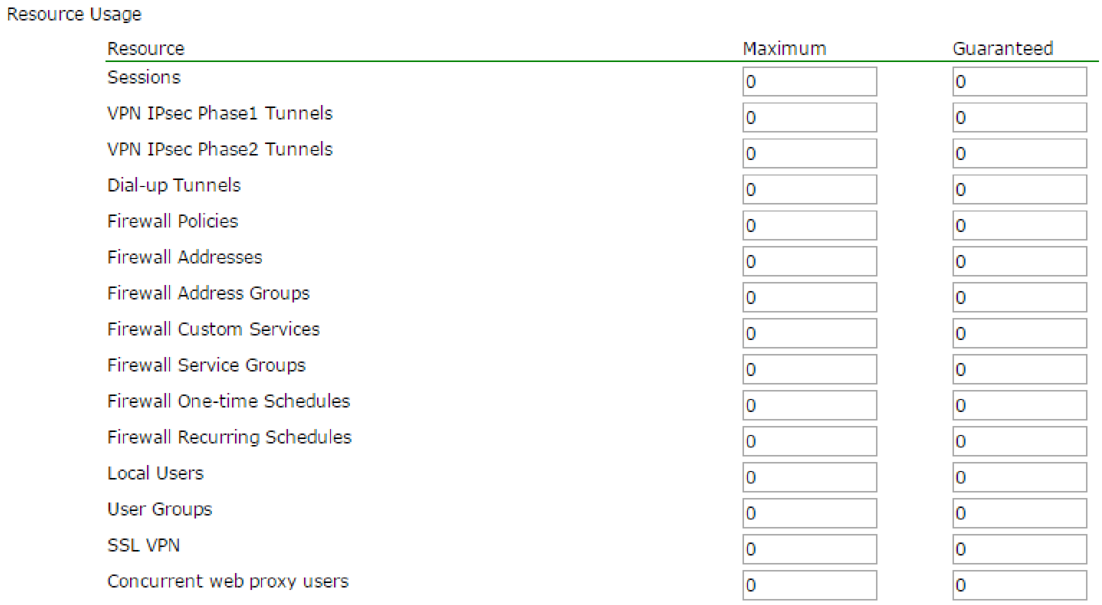
(Optional) Assign system resources to each VDOM, such as session quantity and VPN channel quantity.

Choose **System** > **VDOM** > **VDOM**. Double-click vdom1 to which resources should be assigned, as shown in the following figure:



□	Name	Operation Mode	Interfaces	Enable
□	root	NAT	dmz, internal, mesh.root, ssl.root, wan1, wan2	✓
☑	vdom1	TRANSPARENT		✓

The **Resource Usage** page is as shown in the following figure. The value 0 indicates no restriction and guarantee. Set the maximum value and guaranteed value of each item.


Resource Usage

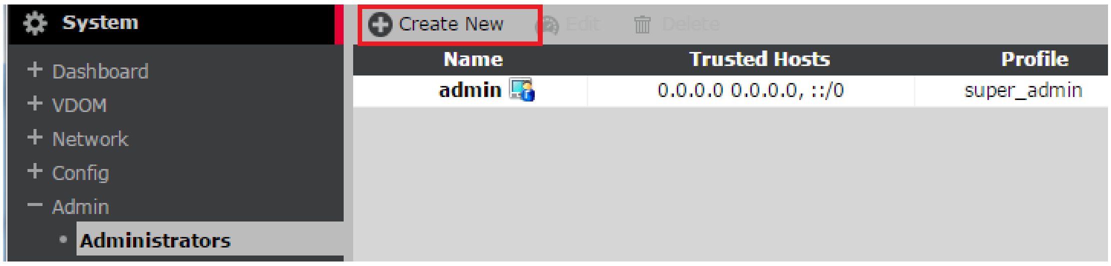
Resource	Maximum	Guaranteed
Sessions	0	0
VPN IPsec Phase1 Tunnels	0	0
VPN IPsec Phase2 Tunnels	0	0
Dial-up Tunnels	0	0
Firewall Policies	0	0
Firewall Addresses	0	0
Firewall Address Groups	0	0
Firewall Custom Services	0	0
Firewall Service Groups	0	0
Firewall One-time Schedules	0	0
Firewall Recurring Schedules	0	0
Local Users	0	0
User Groups	0	0
SSL VPN	0	0
Concurrent web proxy users	0	0

Maximum: It indicates the maximum value of the device resources that can be used by a VDOM. For example, set **Maximum** under **Local Users** to **10**, which indicates that up to 10 users can be created in this VDOM.

Guaranteed: It indicates the value of the device resources that can be used at least by a VDOM. For example, set **Maximum** under **Local Users** to **10**, which indicates that at least 10 users can be created in this VDOM.

5. Assign the administrator account to the VDOM.

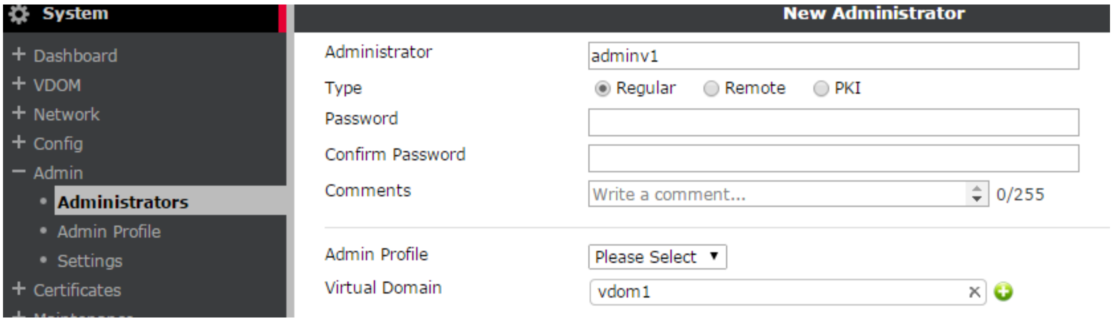
Choose **System** > **Admin** > **Administrators**, and then click **Create New**, as shown in the following figure:



Name	Trusted Hosts	Profile
admin	0.0.0.0 0.0.0.0, ::/0	super_admin

If the administrator does not have the management authority over a VDOM, he/she cannot login to a VDOM through IP addresses of its interfaces. A super administrator has the authority over all the VDOMs and therefore can login to any VDOM.

In the displayed **New Administrator** page, fill in the information, and then choose **vdom1** in the **Virtual Domain** drop list, as shown in the following figure:

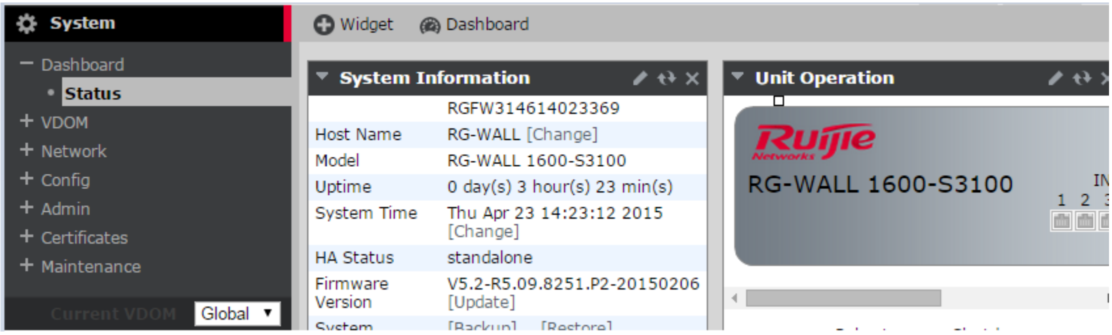


New Administrator

Administrator	adminv1
Type	● Regular ○ Remote ○ PKI
Password	
Confirm Password	
Comments	Write a comment... 0/255
Admin Profile	Please Select ▼
Virtual Domain	vdom1

Enter the VDOM.

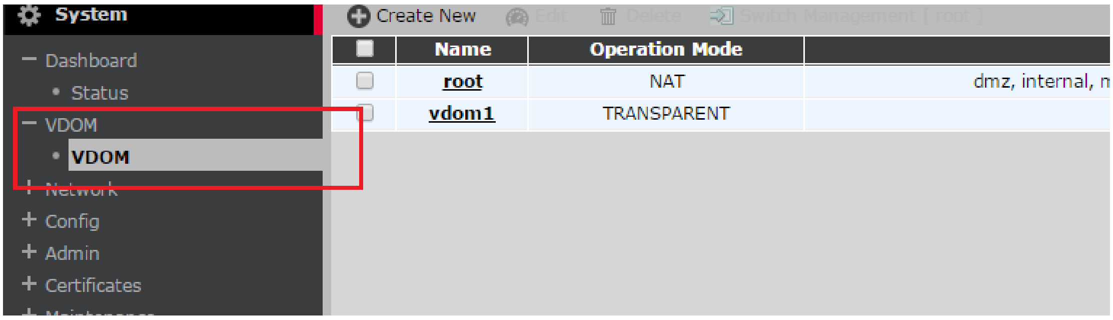
On the bottom of the navigation bar, current VDOM options are added. Choose **vdom1** to which you want to login, so that you can configure the interfaces and firewall policies.



System Information

	RGFW314614023369
Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 3 hour(s) 23 min(s)
System Time	Thu Apr 23 14:23:12 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System	[Backup] [Restore]

Choose **System** > **VDOM** > **VDOM** to add a new VDOM. Before that, switch the mode to global configuration mode.



☐	Name	Operation Mode	
☐	root	NAT	dmz, internal, m
☐	vdom1	TRANSPARENT	

Command Notes

To configure a VDOM in the CLI, for example, configure the interface IP address and firewall policy for a VDOM or enable the UTM logging function, enter a specific VDOM by running the **edit** command and then make configuration.

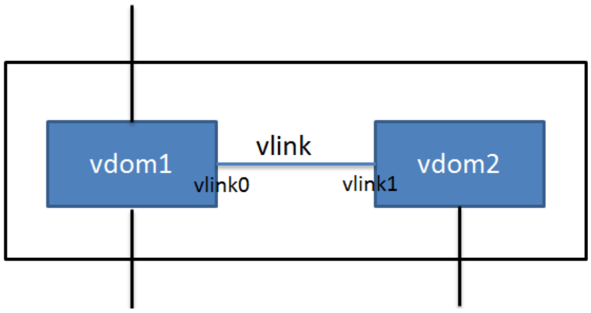
```
RG-WALL # config vdom
         RG-WALL (vdom) # edit nattest  //”nattest” is a VDOM name.
         current vf=nattest:3
RG-WALL (nattest) # config ips senso
```

To display the global running status, CPU, memory usage or perform global operations like restarting the firewall system or restoring factory settings, please run the corresponding commands:

```
RG-WALL # config global
          RG-WALL (global) # get system performance status
          CPU states: 0% user 0% system 0% nice 100% idle
```

5.2 Configuring Vlink

Overview

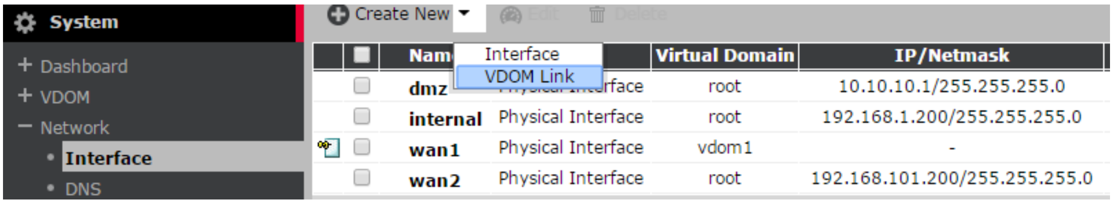


As shown in the preceding figure, to enable communication between vdom1 (port1-port10) and vdom2 (port11-port20), use a network cable to connect one port of vdom1 and one port of vdom2. Another method is to set up a logical virtual link (Vlink) in the firewall to connect two VDOMs. The high-end firewalls support the VDOM connection through the hardware NPU-Vlink.

Vlink Type

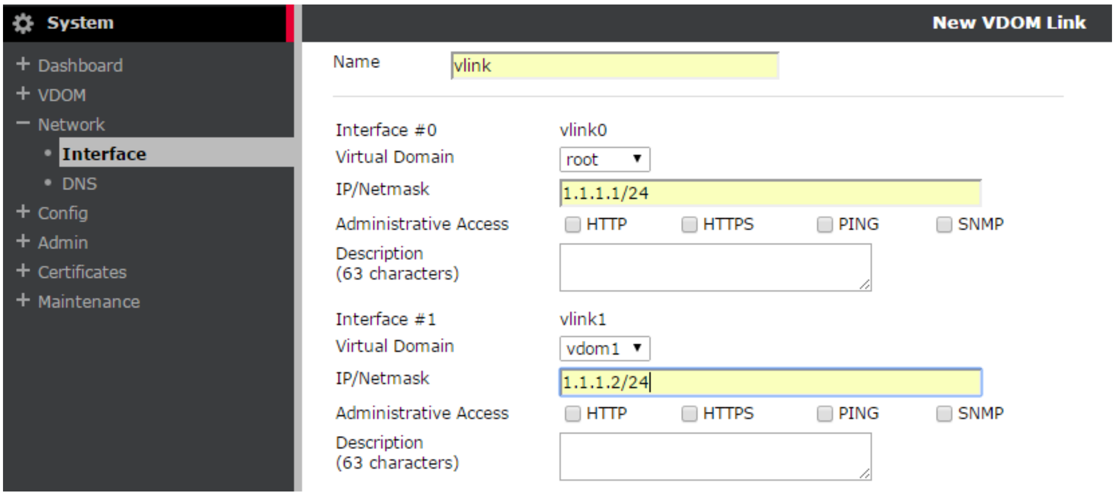
- Manually Configured Vlink

Choose **System** > **Network** > **Interface**. Click ▼ next to **Create New**, and then choose **VDOM Link**, as shown in the following figure:



☐	Name	Type	Virtual Domain	IP/Netmask
☐	dmz	Physical Interface	root	10.10.10.1/255.255.255.0
☐	internal	Physical Interface	root	192.168.1.200/255.255.255.0
☐	wan1	Physical Interface	vdom1	-
☐	wan2	Physical Interface	root	192.168.101.200/255.255.255.0

In the displayed **New VDOM Link** page, add a Vlink. The Vlink consists of two interfaces. For example, if the Vlink is named vlink, the two interfaces of the link are vlink0 and vlink1.



New VDOM Link

Name: vlink

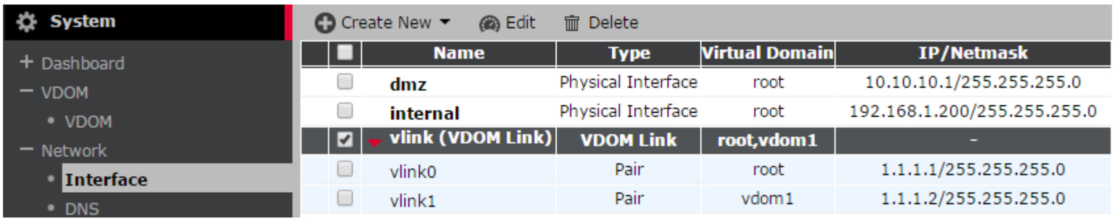
Interface #0: vlink0
Virtual Domain: root ▼
IP/Netmask: 1.1.1.1/24
Administrative Access: ☐ HTTP ☐ HTTPS ☐ PING ☐ SNMP
Description (63 characters):

Interface #1: vlink1
Virtual Domain: vdom1 ▼
IP/Netmask: 1.1.1.2/24
Administrative Access: ☐ HTTP ☐ HTTPS ☐ PING ☐ SNMP
Description (63 characters):

Name: It can be any string for identification.

Virtual Domain: It indicates the VDOM to which the Vlink interface belongs. It is meaningful only when two interfaces belong to two different VDOMs.

After configuration, the two new network interfaces will be displayed in the **Interface** page, as shown in the following figure:



☐	Name	Type	Virtual Domain	IP/Netmask
☐	dmz	Physical Interface	root	10.10.10.1/255.255.255.0
☐	internal	Physical Interface	root	192.168.1.200/255.255.255.0
☑	vlink (VDOM Link)	VDOM Link	root,vdom1	-
☐	vlink0	Pair	root	1.1.1.1/255.255.255.0
☐	vlink1	Pair	vdom1	1.1.1.2/255.255.255.0

- NPU Vlink (Preferred)

For the integrated npu0-vlink and npu1-vlink, each link has two interfaces, such as npu0-vlink0 and npu0-vlink1. You can add these two interfaces to different VDOMs to enable communication between VDOMs.

The NP chip speeds up NPU-Vlink. The manually configured Vlink is processed by the CPU. Therefore, NPU-Vlink should be used preferably. Only the high-end models support this function.

5.3 Configuring VDOM in Hybrid Mode

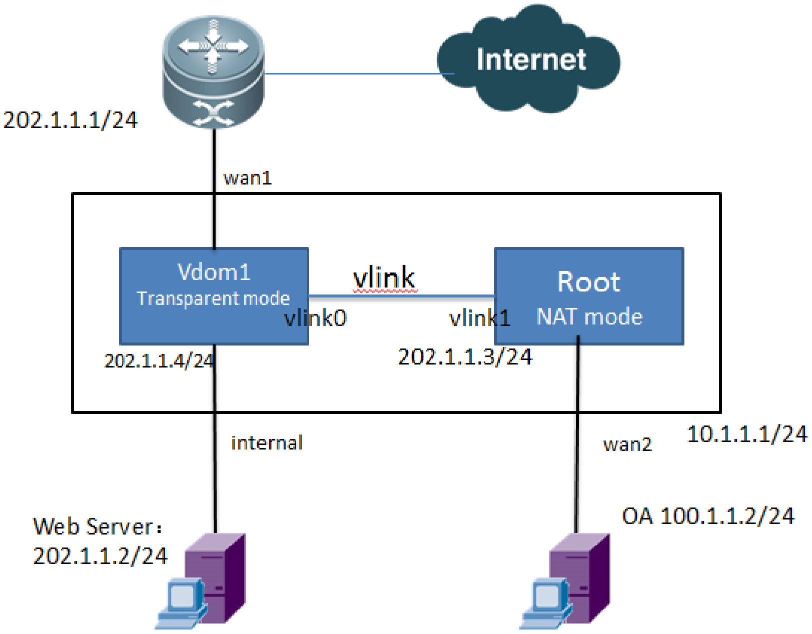
Networking

Requirements

By VDOM, configure a firewall to work in hybrid mode. That is, some VDOMs work in NAT mode, while others work in transparent mode to meet the following requirements:

- Configure the firewall as two VDOMs. One is vdom1 in transparent mode. The other is vdom root in NAT mode.
- The transparent mode is serially established between the Internet egress router and Intranet Web server. The vdom1 is used to protect the server and allow the Extranet and vdom root to access the Web server.
- The OA server at 100.1.1.2 should be mapped to the public network at 202.1.1.3 to enable public network access.

Network Topology



As shown in the preceding figure, the Vlink between VDOMs can be manually configured Vlink, NPU-Vlink or connected physically (the latter two preferred). The following takes manually configured Vlink as an example.

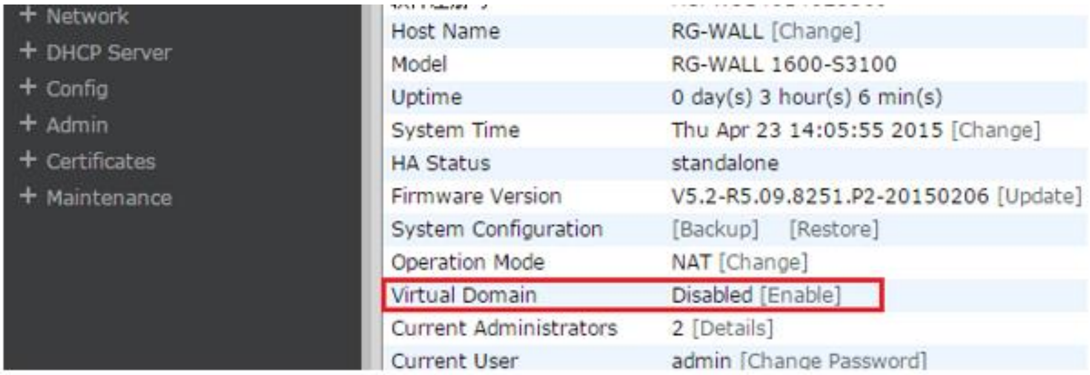
Configuration Tips

- Enable VDOM.
- Add vdom1.
- Establish Vlink.
- Add interfaces to vdom1.
- Configure vdom1.
- Configure vdom root.

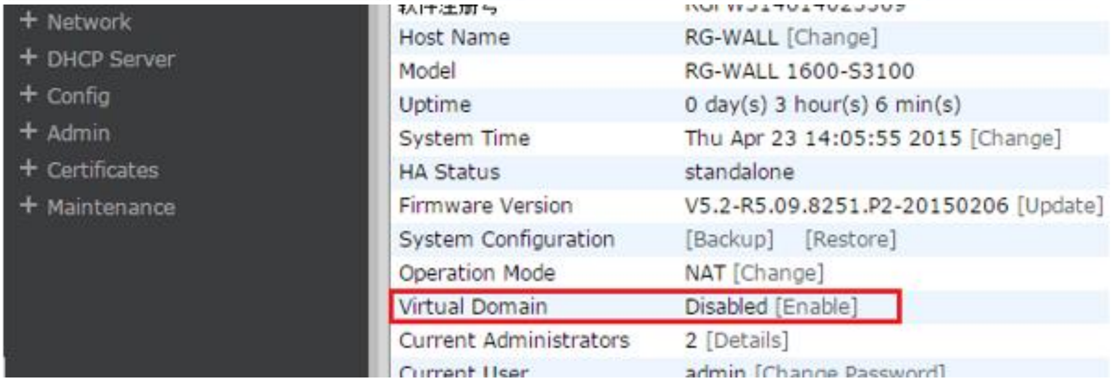
Configuration Steps

1. **Enable VDOM.**

Choose **System** > **Dashboard** > **Status**. Locate the **Virtual Domain** value among system information, as shown in the following figure:

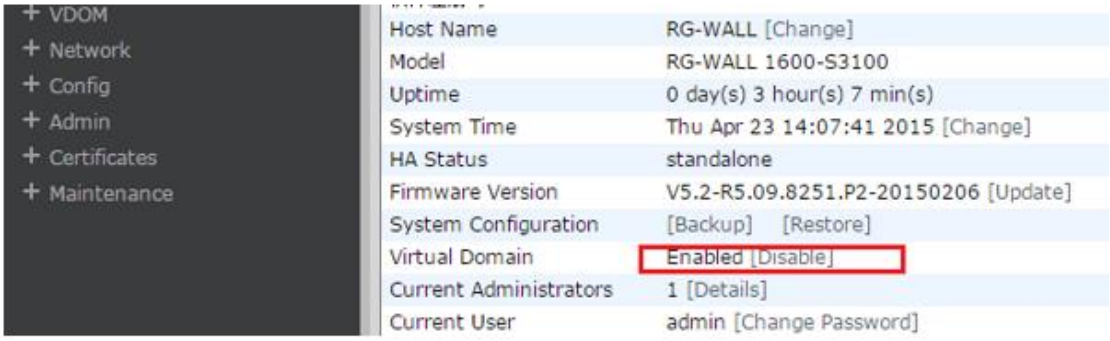


Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 3 hour(s) 6 min(s)
System Time	Thu Apr 23 14:05:55 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	2 [Details]
Current User	admin [Change Password]



Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 3 hour(s) 6 min(s)
System Time	Thu Apr 23 14:05:55 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	2 [Details]
Current User	admin [Change Password]

Click **Enable** corresponding to **Virtual Domain**. The system requires you to re-login. After re-login, VDOM is enabled. See the following figure:

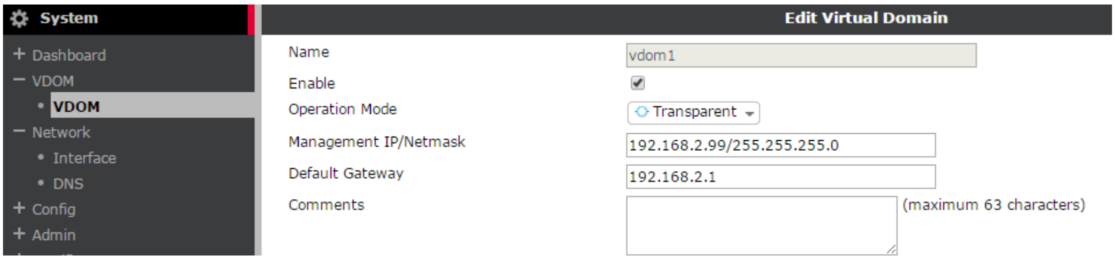


Host Name	RG-WALL [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 3 hour(s) 7 min(s)
System Time	Thu Apr 23 14:07:41 2015 [Change]
HA Status	standalone
Firmware Version	V5.2-R5.09.8251.P2-20150206 [Update]
System Configuration	[Backup] [Restore]
Virtual Domain	Enabled [Disable]
Current Administrators	1 [Details]
Current User	admin [Change Password]

2. **Add vdom1.**

Choose **System** > **VDOM** > **VDOM**. The default vdom root is displayed. Click **Create New**. Enter the VDOM name **vdom1** in the displayed **Edit Virtual Domain** dialog box, and choose **Transparent** as **Operation Mode**.

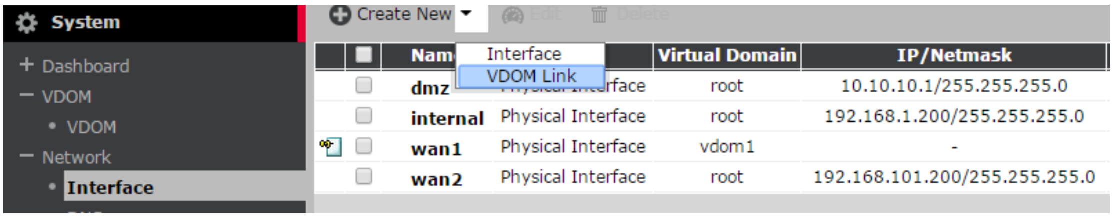
Set **Management IP/Netmask** and **Default Gateway**, and then click **OK**, as shown in the following figure:



Name	vdom1
Enable	☑
Operation Mode	Transparent
Management IP/Netmask	192.168.2.99/255.255.255.0
Default Gateway	192.168.2.1
Comments	(maximum 63 characters)

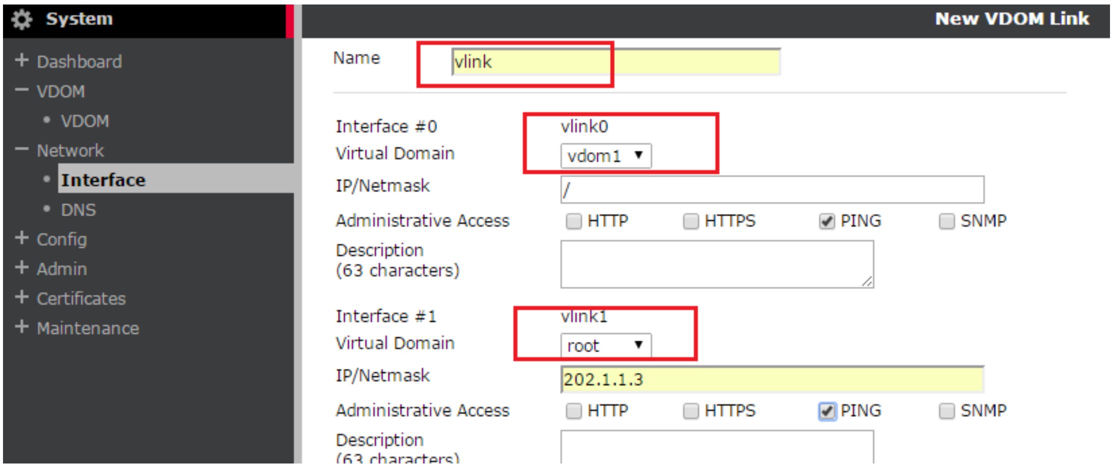
3. Establish the Vlink.

Choose **System** > **Network** > **Interface**, and then click ▼ next to **Create New**. Choose **VDOM Link**, as shown in the following figure:



Name		Virtual Domain	IP/Netmask
dmz	Physical Interface	root	10.10.10.1/255.255.255.0
internal	Physical Interface	root	192.168.1.200/255.255.255.0
wan1	Physical Interface	vdom1	-
wan2	Physical Interface	root	192.168.101.200/255.255.255.0

In the displayed **New VDOM Link** page, enter Vlink name in the **Name** text box and set the VDOM and IP address of Vlink interface, as shown in the following figure:



Name	vlink
Interface #0	vlink0
Virtual Domain	vdom1
IP/Netmask	/
Administrative Access	□ HTTP □ HTTPS ☑ PING □ SNMP
Description (63 characters)	
Interface #1	vlink1
Virtual Domain	root
IP/Netmask	202.1.1.3
Administrative Access	□ HTTP □ HTTPS ☑ PING □ SNMP
Description (63 characters)	

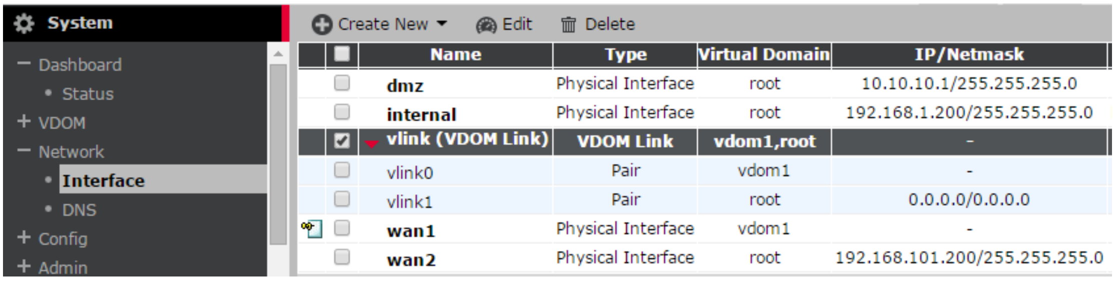
The vlink1 is connected to vdom root and the IP address is set to 202.1.1.3.

If you cannot add a Vlink interface to vdom1on the Web, you can run commands in the CLI. See the following:

```
RG-WALL #config system global
RG-WALL (global) # config sys int
RG-WALL (interface) # edit vlink0
RG-WALL (vlink0) # set vdom vdom1
Warning: "vdom1" is a Transparent Mode VDOM. VDOM link type for "vlink" must bechanged from
the default PPP to Ethernet so that NAT mode and transparent mode VDOMs can communicate.
//When the interface works in PPPoE mode, the system will alert you to change the interface
mode to the Ethernet mode so that you can add an interface to the VDOM.
```

```
By choosing to continue, type of VDOM link "vlink" will be changed from PPP to Ethernet.
Do you want to continue? (y/n)y
RG-WALL (vlink0) #
```

Choose **System** > **Network** > **Interface** to view the new Vlink interface, as shown in the following figure:

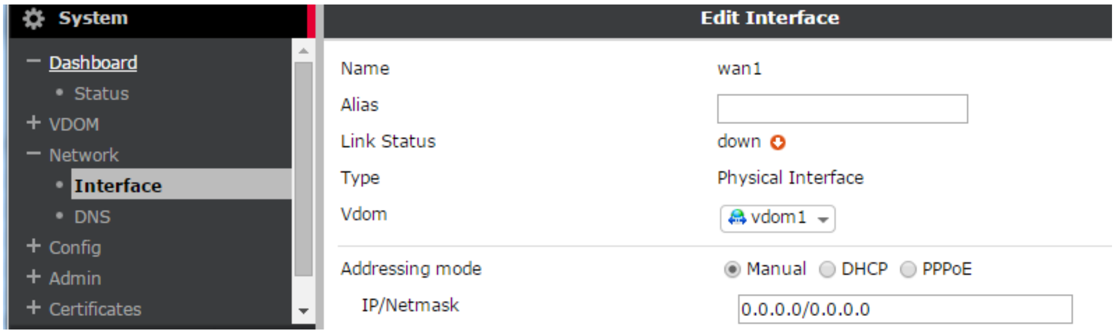


□	Name	Type	Virtual Domain	IP/Netmask
□	dmz	Physical Interface	root	10.10.10.1/255.255.255.0
□	internal	Physical Interface	root	192.168.1.200/255.255.255.0
☑	vlink (VDOM Link)	VDOM Link	vdom1,root	-
□	vlink0	Pair	vdom1	-
□	vlink1	Pair	root	0.0.0.0/0.0.0.0
□	wan1	Physical Interface	vdom1	-
□	wan2	Physical Interface	root	192.168.101.200/255.255.255.0

4. Add interfaces to VDOM.

1) Add interfaces to vdom1.

In global configuration mode, choose **System** > **Network** > **Interface**. Add internal and wan1 interfaces to vdom1, as shown in the following figure:



Edit Interface

Name: wan1

Alias:

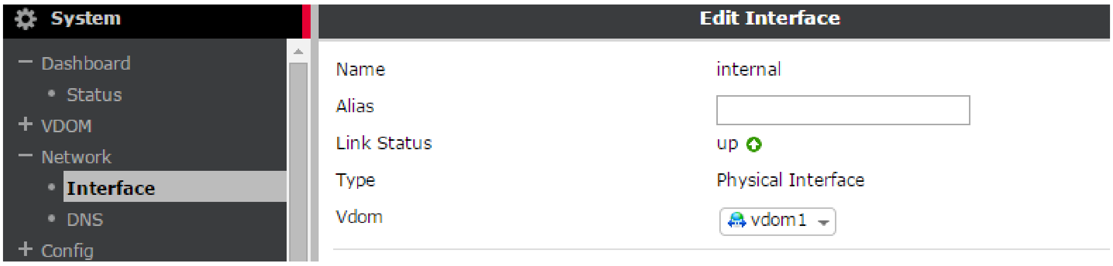
Link Status: down

Type: Physical Interface

Vdom: vdom1

Addressing mode: ● Manual ○ DHCP ○ PPPoE

IP/Netmask: 0.0.0.0/0.0.0.0



Edit Interface

Name: internal

Alias:

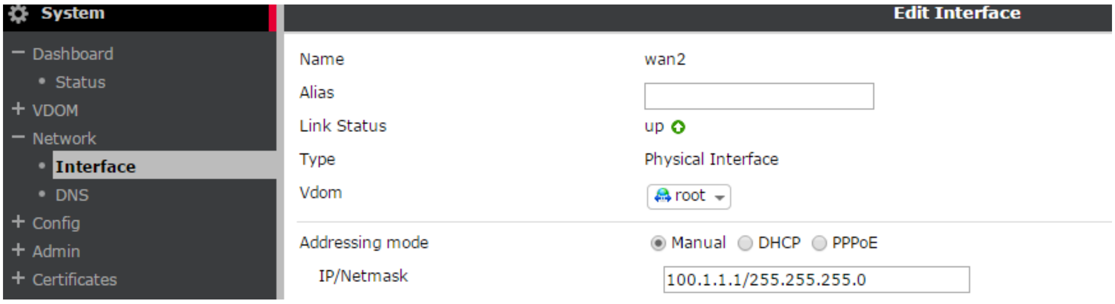
Link Status: up

Type: Physical Interface

Vdom: vdom1

2) Add interfaces to vdom root.

After you add wan2 interface to vdom root, all the interfaces belong to vdom root by default.



Edit Interface

Name: wan2

Alias:

Link Status: up

Type: Physical Interface

Vdom: root

Addressing mode: ● Manual ○ DHCP ○ PPPoE

IP/Netmask: 100.1.1.1/255.255.255.0

5. Configure vdom1.

Choose vdom1 to enter vdom1.

1) Configure server IP addresses.

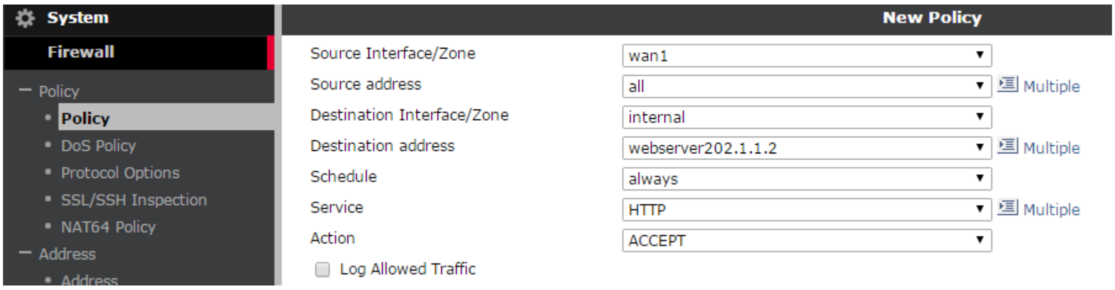
Web server: name is webserver202.1.1.2; IP address is 202.1.1.2

OA server: name is OAserver100.1.1.2; IP address is 202.1.1.3 (mapped to public network IP address)

For detailed configuration, see the section “Configuring Internet Access via a Static Link” in “Configuring Routing Mode”.

2) Configure the policies.

a) Allow the Extranet to access webserver202.1.1.2.

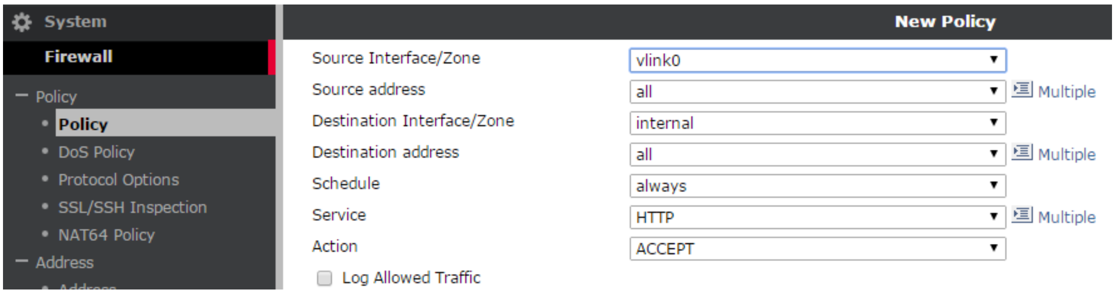


New Policy

Source Interface/Zone	wan1
Source address	all
Destination Interface/Zone	internal
Destination address	webserver202.1.1.2
Schedule	always
Service	HTTP
Action	ACCEPT

□ Log Allowed Traffic

b. Allow vdom root to access webserver202.1.1.2.

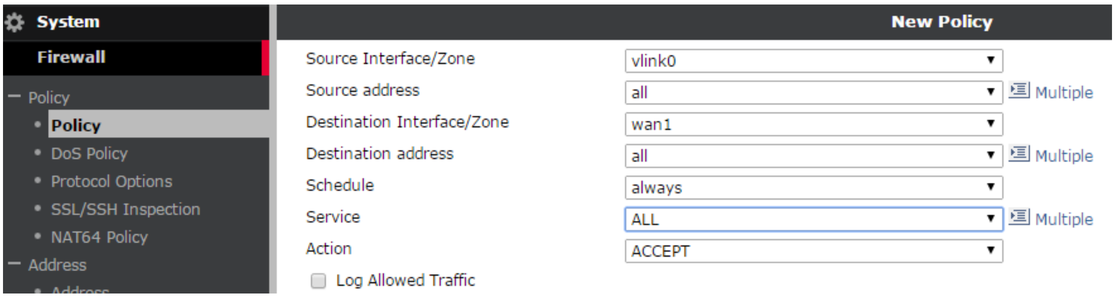


New Policy

Source Interface/Zone	vlink0
Source address	all
Destination Interface/Zone	internal
Destination address	all
Schedule	always
Service	HTTP
Action	ACCEPT

□ Log Allowed Traffic

c. Allow vdom root to access the Internet.

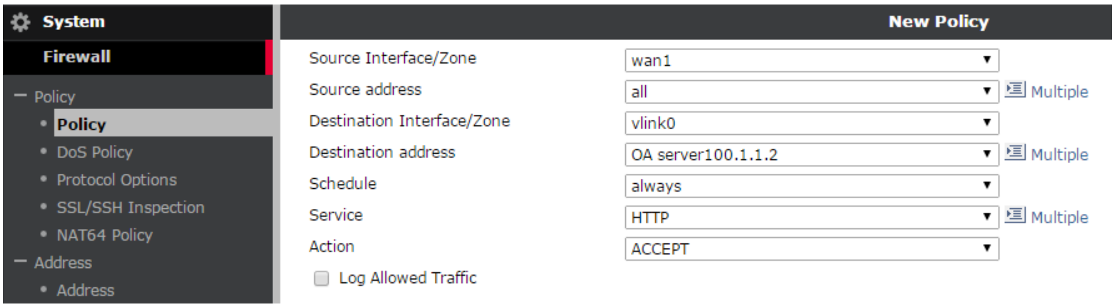


New Policy

Source Interface/Zone	vlink0
Source address	all
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT

□ Log Allowed Traffic

d. Allow the Internet to access mapped IP address 202.1.1.3 of the OA server in vdom root.

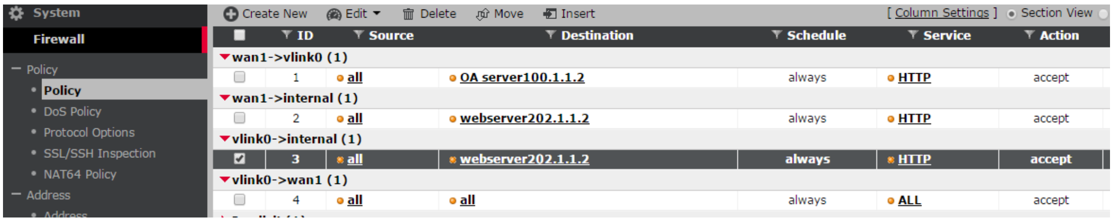


New Policy

Source Interface/Zone	wan1
Source address	all
Destination Interface/Zone	vlink0
Destination address	OA server100.1.1.2
Schedule	always
Service	HTTP
Action	ACCEPT

□ Log Allowed Traffic

The policy configuration is displayed as follows:



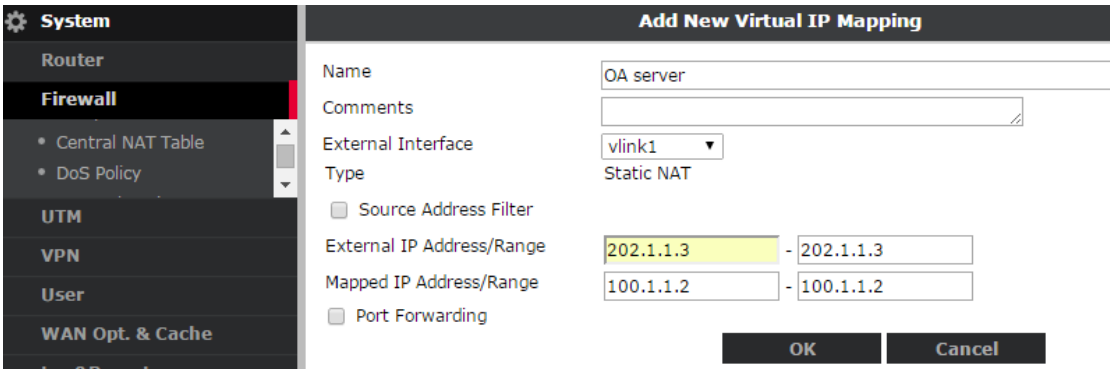
	ID	Source	Destination	Schedule	Service	Action
wan1->vlink0 (1)						
□	1	all	OA server100.1.1.2	always	HTTP	accept
wan1->internal (1)						
□	2	all	webserver202.1.1.2	always	HTTP	accept
vlink0->internal (1)						
☑	3	all	webserver202.1.1.2	always	HTTP	accept
vlink0->wan1 (1)						
□	4	all	all	always	ALL	accept

6. Configure vdom root.

Choose **root** to enter vdom root.

1) Configure the virtual IP address.

Choose **Firewall** > **Virtual IP** > **Virtual IP**, and then click **Create New**. Add the **Mapped IP Address** of the OA server, as shown in the following figure:

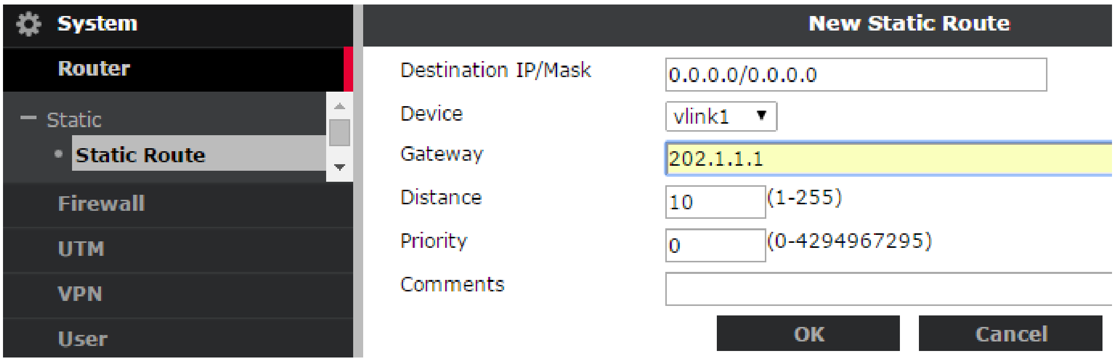


Add New Virtual IP Mapping

Name: OA server
Comments:
External Interface: vlink1
Type: Static NAT
□ Source Address Filter
External IP Address/Range: 202.1.1.3 - 202.1.1.3
Mapped IP Address/Range: 100.1.1.2 - 100.1.1.2
□ Port Forwarding

Choose **vlink1** from **External Interface** drop-down list.

2) Configure a route.



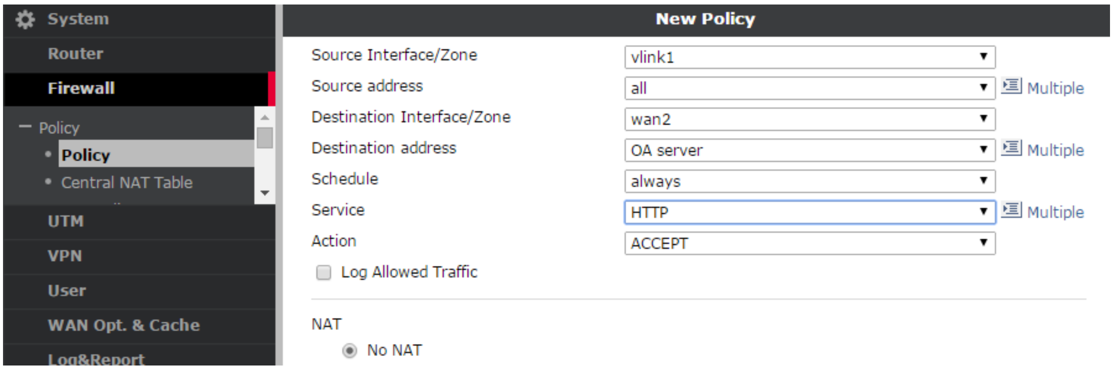
New Static Route

Destination IP/Mask: 0.0.0.0/0.0.0.0
Device: vlink1
Gateway: 202.1.1.1
Distance: 10 (1-255)
Priority: 0 (0-4294967295)
Comments:

Choose **vlink1** from **Device** drop-down list.

3) Configure policies.

a) Allow the Extranet to access OA server.



New Policy

Source Interface/Zone: vlink1

Source address: all

Destination Interface/Zone: wan2

Destination address: OA server

Schedule: always

Service: HTTP

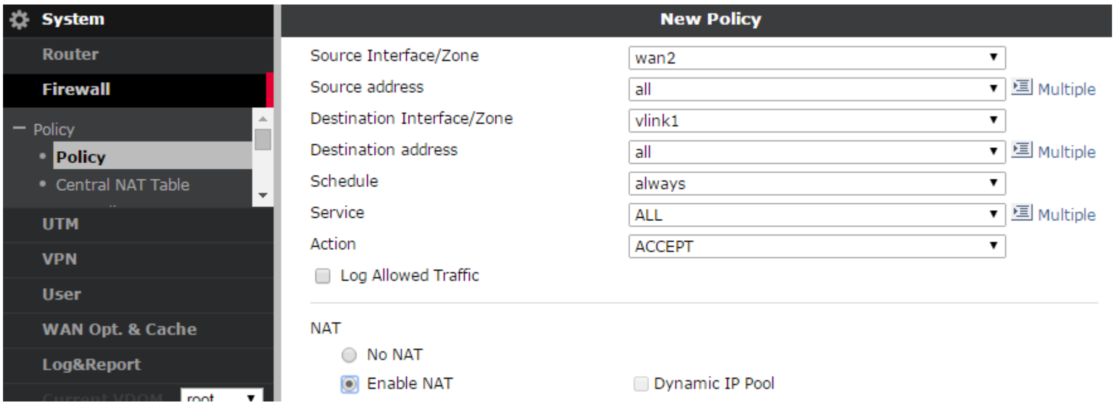
Action: ACCEPT

□ Log Allowed Traffic

NAT

● No NAT

b) Allow wan2 interface to access the Internet.



New Policy

Source Interface/Zone: wan2

Source address: all

Destination Interface/Zone: vlink1

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT

□ Dynamic IP Pool

Verification

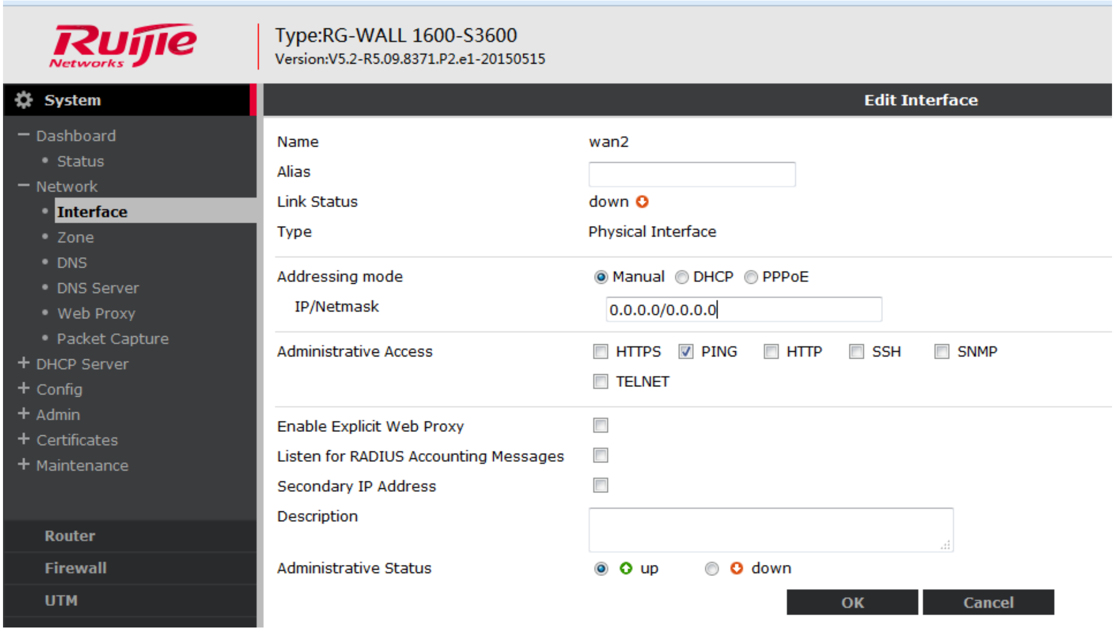
1. Normally Access the webserver202.1.1.2 and OAserver202.1.1.3 from the Extranet.
2. In vdom root, Intranet users can normally access http://202.1.1.2.
3. The webserver202.1.1.2 can normally access OAserver202.1.1.3.

6 Configuring HA

6.1 Networking Requirements

Hardware and software versions should meet the following requirements:

1. Hardware models of the firewalls are the same.
2. The same model requires the same hardware version, memory capacity, CPU model, and hard disk capacity.
3. The software versions are the same.
4. All the interfaces of the device cannot work in DHCP or PPPoE mode. For the interface IP address mode that is not used, choose **Manual**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.09.8371.P2.e1-20150515

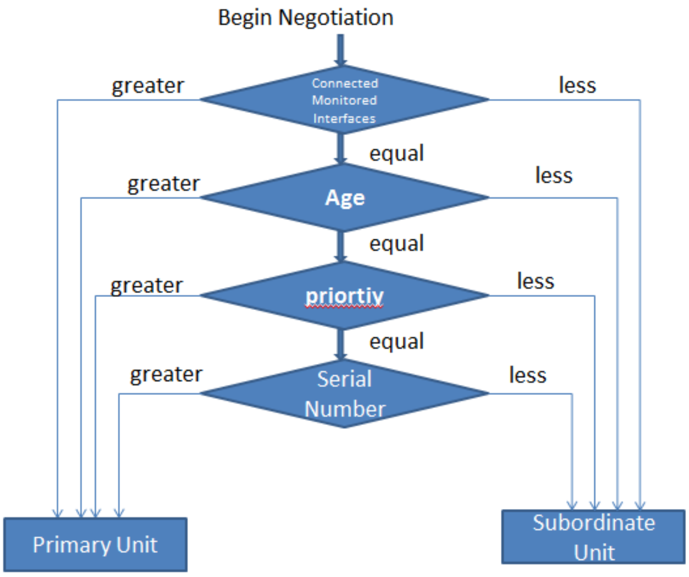
Edit Interface

Name	wan2
Alias	
Link Status	down
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	0.0.0.0/0.0.0.0
Administrative Access	□ HTTPS ☑ PING □ HTTP □ SSH □ SNMP □ TELNET
Enable Explicit Web Proxy	□
Listen for RADIUS Accounting Messages	□
Secondary IP Address	□
Description	
Administrative Status	● up ○ down

6.2 Master Election

Election Rule

When firewalls form a cluster, one master needs to be elected. Other devices except the master are slaves. Master election is carried out according to the rule shown as the following figure. If there is any failure with hardware or links, the master will be re-elected. Firewalls make comparison in the following factors orderly to elect the master: valid-monitored port quantity, device runtime, HA priority, and device sequence number (SN).



Valid-Monitored Port Quantity

After the business ports to be monitored are configured, the firewall with the maximum valid-monitored ports will become the master. In general, when an HA cluster is set up, all the monitored ports are connected and work normally. In this case, the number of the monitored ports will not affect master election. When one monitored port fails or one link fails, master election is re-performed by negotiation. When the faulty port or link recovers, re-negotiation will be triggered. For example, port 3 and port 4 are monitored ports on a master firewall. When port 3 is down, its valid-monitored port quantity decreases. In this case, the number of the valid interfaces of the slave device is not changed and the slave device will become a primary device to continue running. If this happens to slaves, election restarts but the master is unchanged, because the number of monitored ports on slaves is smaller. Every time when a port on a device fails, the master is re-elected.

```
RG-WALL#config system ha
RG-WALL(ha)#set monitor ″port3″ ″port4″
RG-WALL(ha)#end
```

Link failover aims to guarantee the maximum valid ports. The device with the least failure points will become a master device.

Device Runtime

The device with the longest runtime will become the master. Runtime indicates the normal running time since the last device failure. After the device is restarted, the runtime is reset to 0. When the devices in a cluster start up at the same time, the runtime of each device is the same. When one monitored port on one firewall fails, the runtime will be reset and its port number decreases. After the faulty monitored port is restored, although its monitored port quantity may be the same as that of other firewalls, the firewall cannot become the master because of its runtime.

In most of cases, the cluster reduces the election time by adjusting the **age** parameter to stabilize the cluster in case of transmission interruption during election.

The runtime is reset to 0 after devices are restarted or ports fail.

Startup Time Difference

Sometimes, some firewalls in the cluster require more startup time than others. Different startup time results in a series of problems. To reduce the influence of time difference, RG-WALL Cluster Protocol (RGCP) neglects 5-minute difference by default. In most of cases, RGCP can help users realize their expected configuration easier. In the following cases, the runtime difference will result in unexpected results:

1. When the firmware version is upgraded, **uninterruptable-upgrade enable** is run by default. The cluster will re-elect the master after all the firewalls are upgraded. If he runtime difference caused by the upgrade is less than 5 minutes, it will be neglected.
2. When link failover is being tested repeatedly, the runtime difference of devices in the cluster occurs. In general, failed devices re-join the cluster after failover and the runtime of these hosts is shorter than other devices. Therefore, they will not be elected as the master. If the failed firewalls join the cluster and the runtime difference with others is smaller than 5 minutes, the failed may be elected as new master.

Changing Runtime Difference

Use the following command to change runtime difference:

```
RG-WALL#config system ha
RG-WALL(ha)#set ha-uptime-diff-margin 60
RG-WALL(ha)#end
```

The runtime difference is set to 60 seconds. The runtime ranges from 1 to 65535 seconds. By default, the runtime is 300 seconds. You can reduce the runtime difference manually, if you cannot wait for five minutes to test or when the firewall OS is upgraded without being interrupted. You can increase runtime difference when the startup time difference of the devices in the cluster increases.

HA Priority

With the same number of monitored ports and runtime, the device with a higher priority becomes the master. By default, the HA priority is 128. You can set the priority manually to prioritize a device as the master. The priority will not be synchronized between HA members as the device name. When a new device with a higher priority joins one cluster, it will not trigger negotiation until the cluster re-negotiates. You can modify the priority on the graphical interface or by running the following commands:

```
RG-WALL#config system ha
RG-WALL(ha)#Set priority 200
RG-WALL(ha)#end
```

Use the **execute ha manage** command to change the priority of the slaves in a cluster. The master is re-elected after priority change.

SN

Different device has different SN. When the devices in a cluster have the same number of valid interfaces, runtime, and HA priority, the SN determines the master. The one with the greatest SN will become the master.

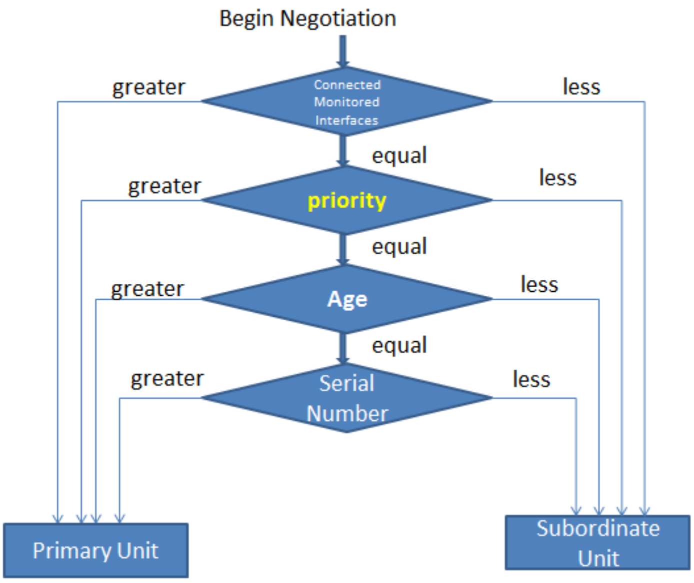
Override

During HA configuration, the **override** parameter will affect the master election.

```
RG-WALL#config system ha
RG-WALL(ha)#set override disable/enable
RG-WALL(ha)#end
```

The **override** parameter should be set in the CLI. The default value is **disable**.

After the **override** parameter is set, the method of master election changes. The **priority** parameter takes precedence over runtime.



If the priority of a device is the highest with **override** enabled, it runs as the master when it shares the same number of valid ports as others. Due to the feature of the **override** parameter, device configuration may be lost due to mis-operation. See the following example:

1. The priority of device A is 200 with the **override** parameter set to **enable**. The priority of device B is 100 with the **override** parameter set to **disable**.
2. Device A fails, and device B becomes the master.
3. Change device A with a new one. The HA priority is set to 200, while the **override** parameter is set to **enable**. Business is not set.
4. After all the lines of the new device are connected, enable the new device. Though the new device and device B have the same number of valid interfaces, the new device has higher priority and thus acts as the master.

5. The null configuration file of the new device is synchronized to device B. Data of device B will be lost.

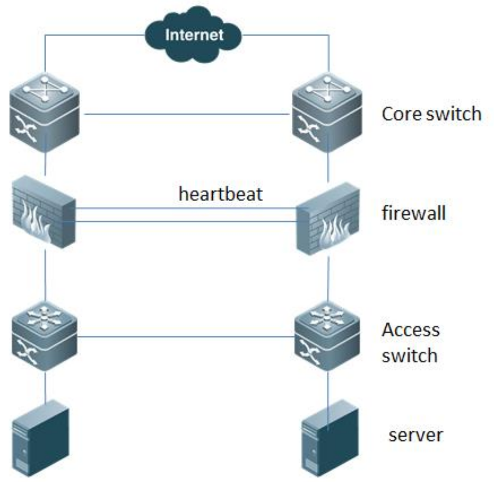
Avoidance method: Check whether the **override** parameter is set to **enable**. Check the **priority** parameter. Another method is not to connect the cable of any monitored port when a new device accesses, which minimizes the number of valid ports.

When virtual cluster2 is enabled in the firewall, the **override** parameter is set to **enable** by default to facilitate control.

```
RG-WALL#config system ha
RG-WALL(ha)#set vcluster2 enable
config secondary-vcluster
        set override disable              // The default is disable.
set vdom "ts"
end
```

6.3 Basic Configuration

Network Topology



Hardware and software need to meet the following requirements so that you can configure HA:

1. Hardware models of the firewalls are the same.
2. The same hardware model requires the same hardware version, memory capacity, CPU model, and hard disk capacity.
3. The software versions are the same.
4. All the interfaces of the device should not work in DHCP or PPPoE mode. For the interface IP address mode that is not used, choose **self-defined**.

Configuration Steps

Step 1: Configure HA for device 1.

Step 2: Configure HA for device 2.

Step 3: Establish HA.

Step 4: Display HA cluster.

Configuration Tips

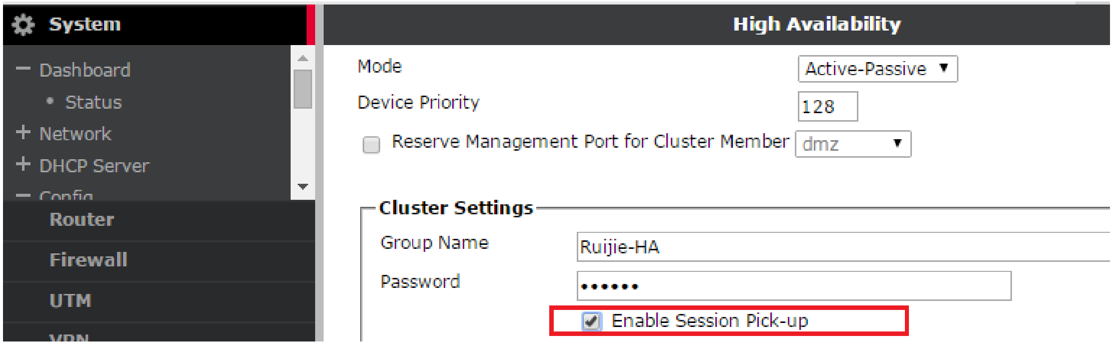
1. Before device change in the HA environment, back up configuration to prevent configuration loss caused by mis-operation.
2. It is recommend to configure more than two heartbeat cables to prevent HA cluster breakdown caused by the failure of a single heartbeat cable. Use an independent heartbeat interface to avoid the mixed usage of business ports.
3. Preferably use the fiber interface.
4. Enable session synchronization. Execute the **session-pickup enable** command or enable “session pickup” on the Web. (By default, **session-pickup** is set to **disable**.)
5. Use the override function with caution. After override is enabled, HA priority is prior to the runtime during election. In this case, the device expected to be a slave device is elected to be the master, thus resulting in reversely configuration synchronization.
6. Change the ID of the default HA group to prevent that multiple HA clusters exist in one broadcast domain which avoids virtual MAC address conflict of interfaces.
7. Choose proper monitored port and heartbeat port. When the virtual cluster in VDOM is enabled, each cluster should be independently configured.
8. If ping server is enabled, configure it by using the corresponding HA commands.
9. It is recommend to set the interface of the switch connected to the firewall to fastport mode. In the case of failover, the interface of the switch will be changed into forwarding status at once.

HA Basic Configuration

Use the following method to configure the two firewalls to run in HA mode:

1. Configure the master.

Choose **System** > **Config** > **HA**. Choose **Active-Passive** from **Mode** drop-down list. Set **Device Priority** to **200** (the master priority is higher than that of the slave). Keep the default group name and password. Select **Enable Session Pick-up**. See the following figure:



High Availability

Mode: Active-Passive

Device Priority: 128

□ Reserve Management Port for Cluster Member: dmz

Cluster Settings

Group Name: Ruijie-HA

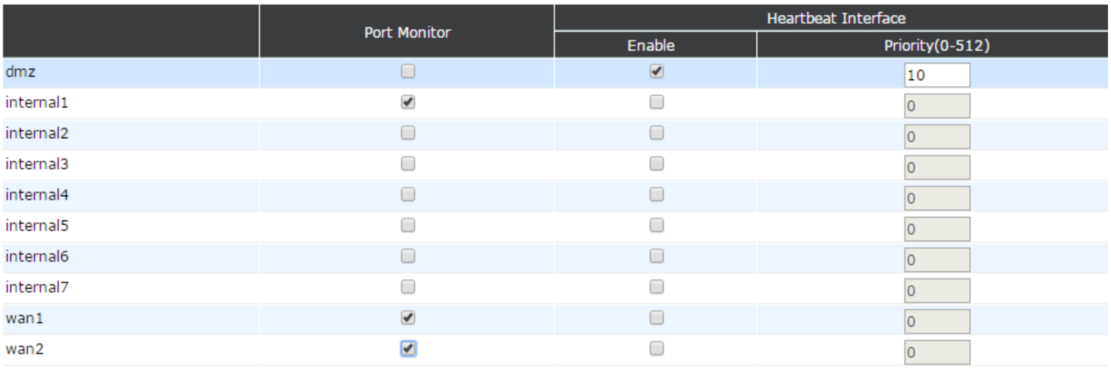
Password: ••••••

☑ Enable Session Pick-up

HA interface configuration:

2. **Port Monitor: monitored port in HA mode, which is a basis for HA switchover. In this case, wan1 (extranet port), wan2 (extranet port) and internal1 (intranet port) are monitored.**

3. **Heartbeat Port: Enable two heartbeat ports: internal13 and internal14.**



	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
dmz	□	☑	10
internal1	☑	□	0
internal2	□	□	0
internal3	□	□	0
internal4	□	□	0
internal5	□	□	0
internal6	□	□	0
internal7	□	□	0
wan1	☑	□	0
wan2	☑	□	0

The following describes the steps for basic HA configuration of the firewalls:

1) Define the working mode. Choose **Active-Passive** or **Active-Active**. In most of networks, choose **Active-Passive**, which indicates that the master deals with service, while the slave is in standby state. When the master fails or the interface link of the master fails, the slave continues service handling.

2) Define the device priority. The device with the highest priority is elected as the master preferably.

3) Group name and password: Keep the default group name and password. If you change the group name and password, the two devices in one HA cluster should be configured with the same group name and password.

4) Enable session pick-up. Sessions are synchronized between the master firewall and standby firewall in real time. In the case of switchover, the standby firewall has the same session information and the original session will be processed without interrupting sessions.

5) Define two heartbeat ports: internal6 and internal7. These two ports are used for special purposes such as configuring session synchronization and detecting the alive heartbeat of the peer party. To keep cluster stable, it is recommended to configure two or more lines.

6) When multiple heartbeat lines exist, the heartbeat priority of the heartbeat port determines the line used preferably for heartbeat synchronization. (The line connected to the port with a higher priority is preferably used.)

7) Define monitored ports: internal1 and wan1. Business ports need to be monitored by the firewall.

When a port fails, failover proceeds. The device with more valid monitored ports will work as a master firewall for data processing.

8) Enter a new device name (optional), which facilitates identification and operation.

4. Configure the slave device.

Except that the priority is different (priority of the slave device is lower than that of the master device), other parameters are the same as those of device 1.

5. Establish HA.

1) Connect the heartbeat line. Internal13 and internal14 ports of the master NGFW are connected to internal13 and internal14 ports of the slave NGFW.

2) The firewall begins negotiation about HA cluster establishment. At this time, the connection to the firewall will be lost at the moment. That’s because the MAC address of the firewall interface will be changed during negotiation. You can run the arp-d command to update the ARP table of the PC to restore the connection.

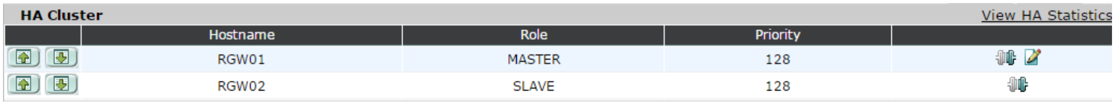
3) Connect the link of the business port.

4) After HA is established, two firewalls synchronize configuration. The two firewalls are equipped with the same configuration. Business is configured by accessing the master firewall, such as IP address and policy. The new configuration will be automatically synchronized.

After HA is established, access and management can only be done by the master device. To log in to the slave device for management, see section 4.6 “Out-of-Band Management of HA Cluster”.

6. Display HA cluster.

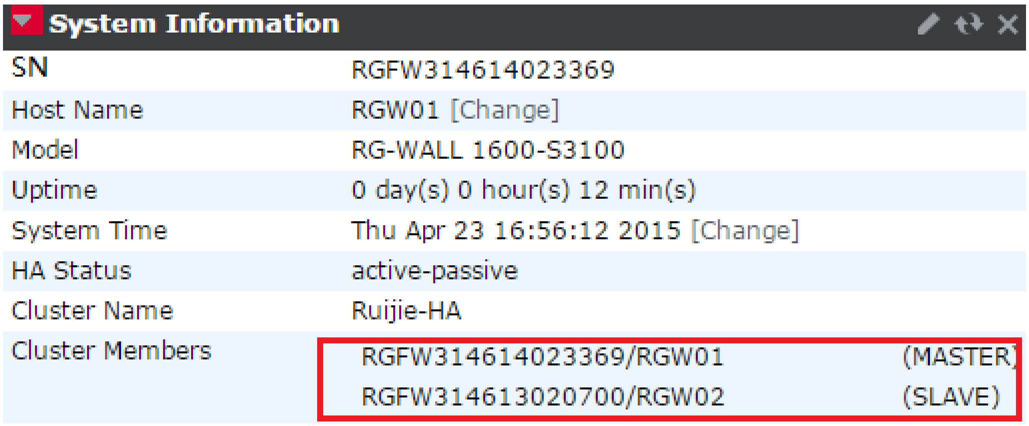
Choose **System** > **Config** > **High Availability** to display HA establishment, as shown in the following figure:



HA Cluster View HA Statistics

	Hostname	Role	Priority	
	RGW01	MASTER	128	
	RGW02	SLAVE	128	

The status panel on the home page also shows group members, as shown in the following figure:



System Information

SN	RGFW314614023369
Host Name	RGW01 [Change]
Model	RG-WALL 1600-S3100
Uptime	0 day(s) 0 hour(s) 12 min(s)
System Time	Thu Apr 23 16:56:12 2015 [Change]
HA Status	active-passive
Cluster Name	Ruijie-HA
Cluster Members	RGFW314614023369/RGW01 (MASTER) RGFW314613020700/RGW02 (SLAVE)

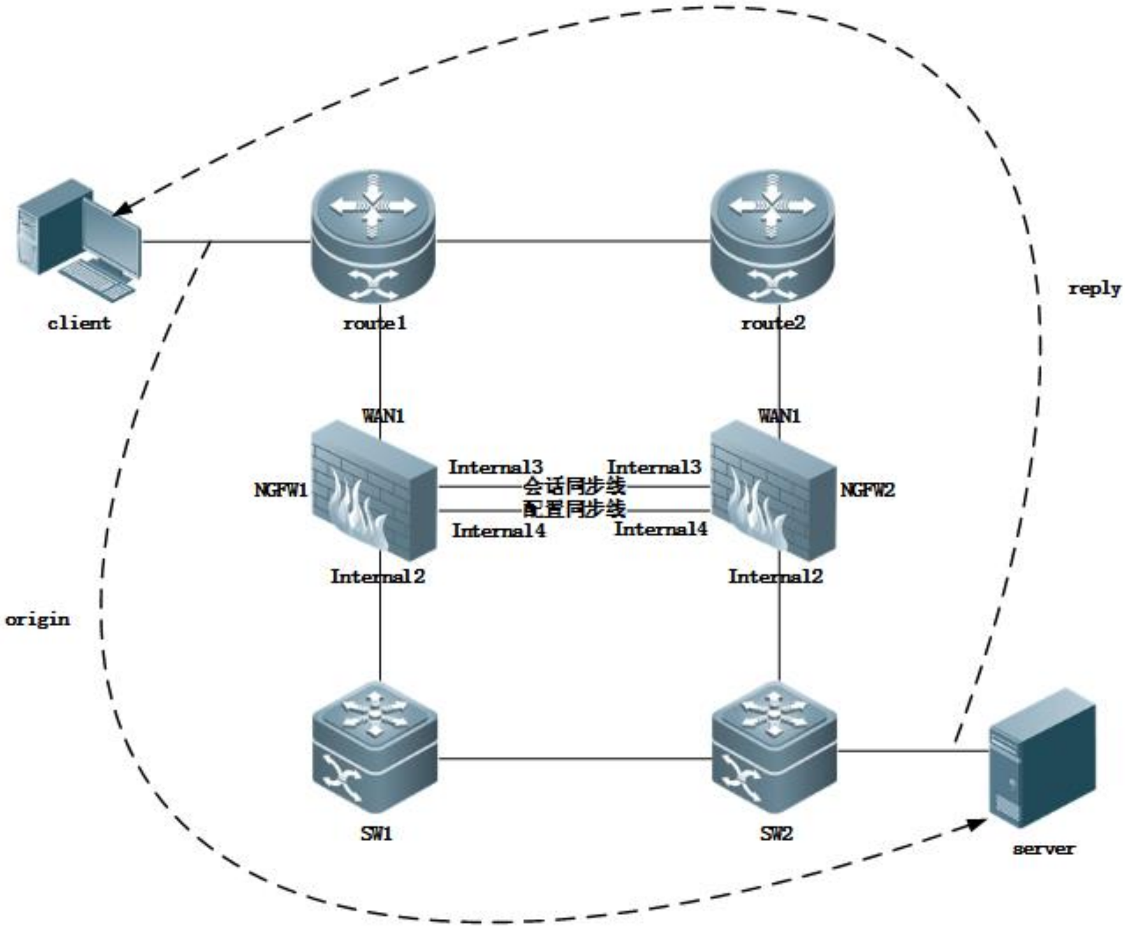
6.4 Configuring Synchronization of Standalone Device Configuration and Sessions

Overview

Since version 5.0, NGFW supports synchronizing standalone device configuration and sessions. In some application scenarios, NGFW can replace HA function enabled by two devices to control asynchronous traffic.

Network Topology

1. In the network topology, OSPF routing protocol is enabled between router1 and router2 and between SW1 and SW2.
2. NGFW1 and NGFW2 access the network transparently. (TP mode; enabling VDOM)
3. Asynchronous traffic exists in the communication between the client and server. Herein, internal4 is the HA heartbeat interface for synchronizing configuration. Internal3 is used to synchronize sessions, which should be configured with an interconnection IP address.



NGFW1

internal1: 192.168.1.21/24

internal3: 10.1.1.1/24

NGFW2

internal1: 192.168.1.22/24

internal3: 10.1.1.2/24

Configuration Steps

Step 1: Configure synchronization of NGFW configuration in HA mode.

Step 2: On NGFW1, establish a VDOM to divide interfaces and configure policies. (Configuration will be automatically synchronized to NGFW2.)

Step 3: Enables session pickup.

Step 4: Enable session synchronization.

Step 5: Verification.

Step 6: Notes.

Basic Configuration

Use the following method to configure the two firewalls to run in HA mode:

Step 1: Respectively configure IP addresses of two firewalls and enable configuration synchronization.

NGFW1

```
RG-WALL #config system interface
RG-WALL (interface) # edit internal1
RG-WALL( internal1) # set ip 192.168.1.21 255.255.255.0 //Set the management interface and IP address.
RG-WALL( internal1)# set allowaccess ping https ssh snmp http telnet
RG-WALL( internal1) #next
RG-WALL (interface) #edit internal3
RG-WALL( internal3) #set ip 10.1.1.1 255.255.255.0
RG-WALL( internal3) #set allowaccess ping https ssh http telnet
RG-WALL( internal3) #next
RG-WALL (interface) # end
RG-WALL #config system ha
RG-WALL (ha) #set hbdev internal4 0   //Set internal4 interface, which is used for configuration synchronization.
RG-WALL (ha) #set standalone-config-sync enable
RG-WALL (ha) #set priority 200    //Set priority.
RG-WALL (ha) #end
```

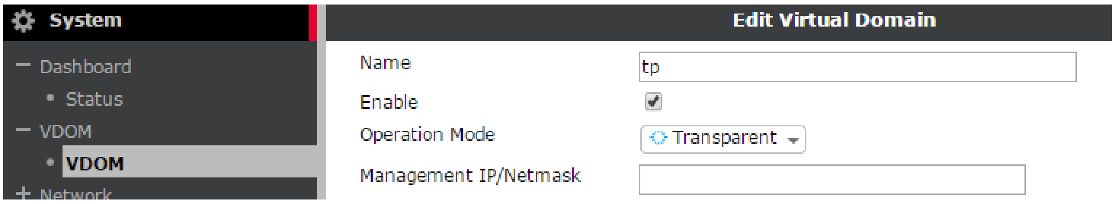
NGFW2

```
RG-WALL #config system interface
RG-WALL (interface)#edit internal1
RG-WALL( internal1) #set ip 192.168.1.22 255.255.255.0
RG-WALL( internal1) #set allowaccess ping https ssh snmp http telnet
RG-WALL( internal1) #next
RG-WALL (interface)#edit internal3                   //Configure the IP address of internal3 interface, which is used to synchronize sessions.
RG-WALL( internal3) #set ip 10.1.1.2 255.255.255.0
RG-WALL( internal3) #set allowaccess ping https ssh http telnet fgfm
RG-WALL( internal3) #next
RG-WALL (interface)#end
RG-WALL #config system ha
RG-WALL (ha) #set hbdev internal4 0//Configure internal4, which is used for configuration synchronization.
RG-WALL (ha) #set standalone-config-sync enable
RG-WALL (ha) #set priority 100    //Set priority.
RG-WALL (ha) #end
```

Configuration of new NGFW1 will be synchronized to NGFW2.

Step 2: On the web interface, add a VDOM in transparent mode to NGFW1. Enable policies. (Configuration will be synchronized to NGFW2.)

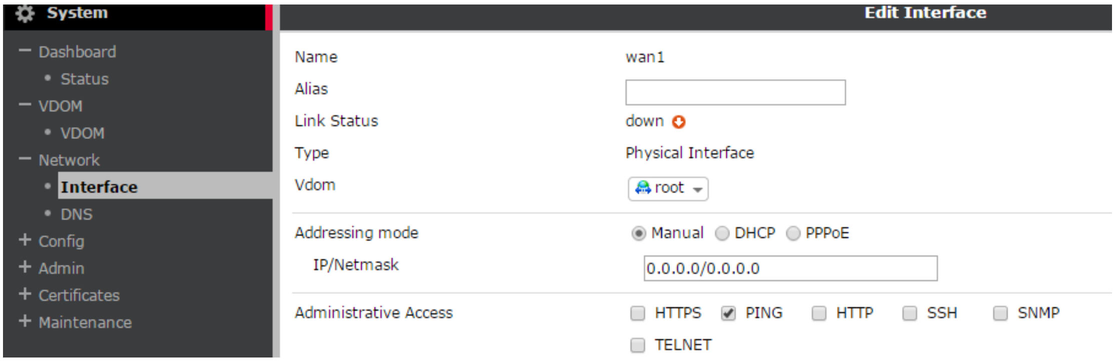
1. Add a VDOM in transparent mode.



Edit Virtual Domain

Name	tp
Enable	☑
Operation Mode	Transparent
Management IP/Netmask	

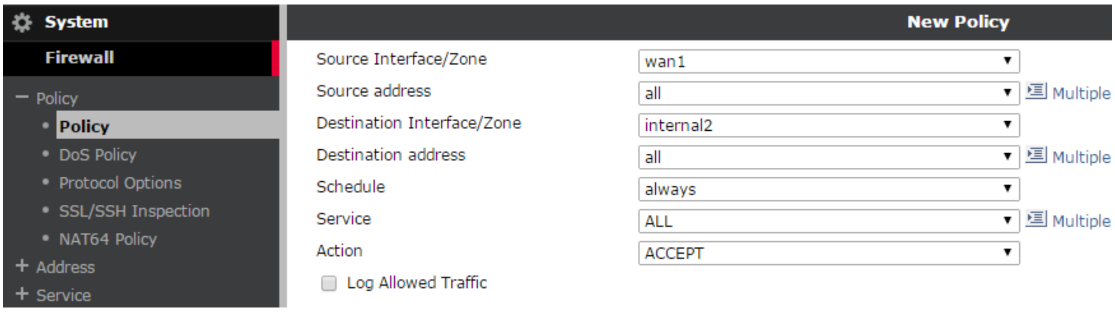
2. Add wan1 and internal2 to VDOM tp.



Edit Interface

Name	wan1
Alias	
Link Status	down
Type	Physical Interface
Vdom	root
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	0.0.0.0/0.0.0.0
Administrative Access	□ HTTPS ☑ PING □ HTTP □ SSH □ SNMP □ TELNET

3. Set the policy to allow the client to access the server.



New Policy

Source Interface/Zone	wan1
Source address	all (Multiple)
Destination Interface/Zone	internal2
Destination address	all (Multiple)
Schedule	always
Service	ALL (Multiple)
Action	ACCEPT
□ Log Allowed Traffic	

Step 3: NGFW1 enables session pickup. (Configured in CLI)

NGFW1

```
RG-WALL #config global
RG-WALL(global) #config system ha
RG-WALL(ha) #set session-sync-dev internal3
RG-WALL(ha) set session-pickup enable
RG-WALL(ha) set session-pickup-connectionless enable
```

```
RG-WALL(ha) set session-pickup-expectation enable
RG-WALL(ha) set session-pickup-nat enable
RG-WALL(ha) end
```

Step 4: Two NGFWs respectively enable session synchronization. (Configured in CLI)

NGFW1

```
RG-WALL #config global
RG-WALL(global) #config system session-sync
RG-WALL (session-sync)#edit 1
RG-WALL (1) # set peerip 10.1.1.2
RG-WALL (1) # set syncvd tp
RG-WALL (1) # next
RG-WALL (session-sync)#end
```

NGFW2

```
RG-WALL #config global
RG-WALL(global) #config system session-sync
RG-WALL (session-sync)#edit 1
RG-WALL (1) # set peerip 10.1.1.1
RG-WALL (1) # set syncvd tp
RG-WALL (1) # next
RG-WALL (session-sync)#end
```

Verification

After configuration synchronization is enabled, run **dia sys ha status** to display synchronization status. Run **dia sys ha showcsum** to compare the details of configuration synchronization.

NGFW1

```
RG-WALL #config global
RG-WALL(global) # dia sys ha showcsum
is_manage_master()=1, is_root_master()=1
debugzone
global: 8e fe 7b be 34 43 5e cc 3e 0c 6b 31 02 f9 d5 d1
tp: 9f 05 b8 6e f2 12 e8 f7 a1 58 9b b0 ad 60 1b 09
root: 45 73 10 c7 19 9d a2 8f d9 20 71 6c 98 48 e4 30
all: 26 60 34 e7 7d 0e 6e 1f cc 73 96 c4 1b 17 ee 53

checksum
global: 8e fe 7b be 34 43 5e cc 3e 0c 6b 31 02 f9 d5 d1
tp: 9f 05 b8 6e f2 12 e8 f7 a1 58 9b b0 ad 60 1b 09
root: 45 73 10 c7 19 9d a2 8f d9 20 71 6c 98 48 e4 30
all: 26 60 34 e7 7d 0e 6e 1f cc 73 96 c4 1b 17 ee 53
```

NGFW2

```
RG-WALL #Config global
```

```
RG-WALL(global) # dia sys ha showcsum
is_manage_master()=1, is_root_master()=1
debugzone
global: 8e fe 7b be 34 43 5e cc 3e 0c 6b 31 02 f9 d5 d1
tp: 9f 05 b8 6e f2 12 e8 f7 a1 58 9b b0 ad 60 1b 09
root: 45 73 10 c7 19 9d a2 8f d9 20 71 6c 98 48 e4 30
all: 26 60 34 e7 7d 0e 6e 1f cc 73 96 c4 1b 17 ee 53

checksum
global: 8e fe 7b be 34 43 5e cc 3e 0c 6b 31 02 f9 d5 d1
tp: 9f 05 b8 6e f2 12 e8 f7 a1 58 9b b0 ad 60 1b 09
root: 45 73 10 c7 19 9d a2 8f d9 20 71 6c 98 48 e4 30
all: 26 60 34 e7 7d 0e 6e 1f cc 73 96 c4 1b 17 ee 53
```

In the preceding results of running commands, the highlighted characters indicate that synchronization status is consistent.

View session status.

NGFW1

```
RG-WALL#config vdom
RG-WALL(vdom)#edit tp
RG-WALL(tp) # di sys session list
session info: proto=6 proto_state=01 duration=5 expire=3595 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty br npu synced
statistic(bytes/packets/allow_err): org=92/2/1 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=15->16/16->15 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.1.11:1493->10.30.1.3:23(0.0.0.0:0)
hook=post dir=reply act=noop 10.30.1.3:23->192.168.1.11:1493(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=3
serial=0001572b tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x81/0x00, offload=4/0, ips_offload=0/0, epid=11/0, ipid=10/0, vlan=0/0
```

NGFW2

```
RG-WALL#config vdom
RG-WALL(vdom)#tp
RG-WALL(tp) # dia sys session list
```

```
session info: proto=6 proto_state=01 duration=23 expire=3576 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty br npu
statistic(bytes/packets/allow_err): org=0/0/0 reply=104/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=15->16/16->15 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.1.11:1493->10.30.1.3:23(0.0.0.0:0)
hook=post dir=reply act=noop 10.30.1.3:23->192.168.1.11:1493(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=3
serial=0001572b tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x81, offload=0/4, ips_offload=0/0, epid=0/10, ipid=0/11, vlan=0/0
```

NGFW1

```
RG-WALL#config vdom
RG-WALL(vdom)#edit tp
RG-WALL(tp) # dia sni packet any ’port 23’ 4
interfaces=[any]
filters=[port 23]
24.976627 wan1 in 192.168.1.11.2323 -> 10.30.1.3.23: syn 408581540
24.976641 internal2 out 192.168.1.11.2323 -> 10.30.1.3.23: syn 408581540
24.987196 wan1 in 192.168.1.11.2323 -> 10.30.1.3.23: ack 129336467
24.987205 internal2 out 192.168.1.11.2323 -> 10.30.1.3.23: ack 129336467
29.252381 wan1 in 192.168.1.11.2323 -> 10.30.1.3.23: fin 408581616 ack 129336688
29.252386 internal2 out 192.168.1.11.2323 -> 10.30.1.3.23: fin 408581616 ack 129336688
```

NGFW2

```
RG-WALL#config vdom
RG-WALL(vdom)#edit tp
RG-WALL(tp) # dia sni packet any ’port 23’ 4
interfaces=[any]
filters=[port 23]
9.044384 internal2 in 10.30.1.3.23 -> 192.168.1.11.2323: syn 129336466 ack 408581541
9.044396 wan1 out 10.30.1.3.23 -> 192.168.1.11.2323: syn 129336466 ack 408581541
9.049790 internal2 in 10.30.1.3.23 -> 192.168.1.11.2323: psh 129336467 ack 408581541
9.049800 wan1 out 10.30.1.3.23 -> 192.168.1.11.2323: psh 129336467 ack 408581541
13.309659 internal2 in 10.30.1.3.23 -> 192.168.1.11.2323: fin 129336687 ack 408581616
13.309665 wan1 out 10.30.1.3.23 -> 192.168.1.11.2323: fin 129336687 ack 408581616
```

Notes

1. MAC Address Timeout (critical)

By default, the MAC address timeout of the NGFW is 300 seconds. If the upstream and downstream devices of the NGFW do not send new ARP messages to request the MAC table of the NGFW after 300 seconds, timeout occurs and the forwarding traffic is interrupted.

a) Solution 1: Bind the MAC addresses of the upstream and downstream interfaces of the NGFW.

```
NGFW1 (global) # dia netlink brctl name host tp.b
show bridge control interface tp.b host.
fdb: size=2048, used=9, num=9, depth=1
Bridge tp.b host table
port no device  devname mac addr                ttl     attributes
  1     15      wan1   0a:9e:01:b3:dc:0a       0        Static Hit(254423)
  2     16      internal2  00:1b:8f:61:08:c3       0        Static Hit(423913)

RG-WALL # config vdom
RG-WALL (vdom) # edit tp
RG-WALL(tp)#config system mac-address-table   //Note: Enter print cliovrd enabl4e, and then
press Enter. You can run the following commands after log out, and then log in.
RG-WALL (mac-address-table) # edit 0a:9e:01:b3:dc:0a
RG-WALL (0a:9e:01:b3:dc:0a) #set interface wan1
RG-WALL (0a:9e:01:b3:dc:0a) #next
 RG-WALL (mac-address-table) #edit 00:1b:8f:61:08:c3
 RG-WALL (00:1b:8f:61:08:c3) #set interface internal2
 RG-WALL (00:1b:8f:61:08:c3) #next
 RG-WALL (mac-address-table) #end
```

b) Solution 2: Set the MAC address timeout time of the NGFW to the maximum value (100 days).

```
RG-WALL # config vdom
RG-WALL (vdom) # edit tp
RG-WALL#config system settings
RG-WALL(settings)#set mac-ttl 8640000
RG-WALL(settings)#end

Disable anti-replay.
RG-WALL #config system global
RG-WALL (global) #set anti-replay disable
RG-WALL (global) #end
```

2. The following configuration can be synchronized between two NGFWs:

1) router

```
access-list
as-path
community-list
prefix-list
route-map
```

```
bgp (*exclude* neighbor, router-id, as)
```

2) firewall

```
address
addgrp
interface-policy
policy
service custom
service group
shaper
schedule
vip
vipgrp
```

3) log

```
all items
```

4) system

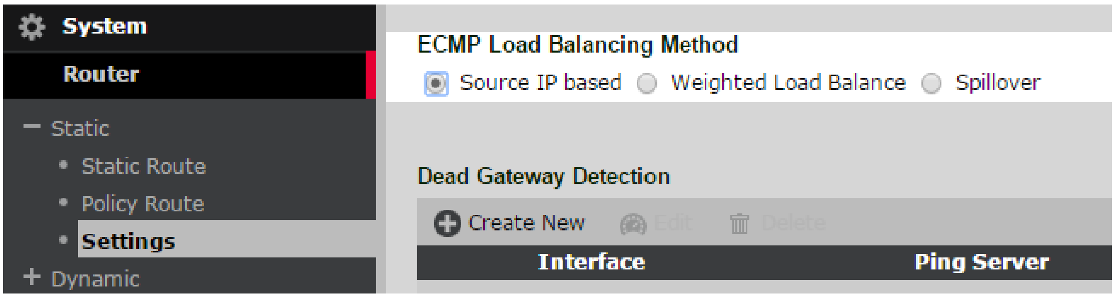
```
accprofile
admin
console
global
ha
ntp
settings (*exclude* ip/gateway/manageip)
zone
      [interface] --*name (16)
               |- vdom (12)
               |- vlanid (0,0)
               |- interface (16)
               |- type
```

6.5 Configuring the Ping Server

Overview

Ping server serves to prevent "feign death" of ports. The link status is normal, but links cannot work. The firewall can send ping packets to determine whether the port link is available according to the response from the peer device.

Choose **System** > **Router** > **Static** > **Settings** > **Dead Gateway Detection**, as shown in the following figure:

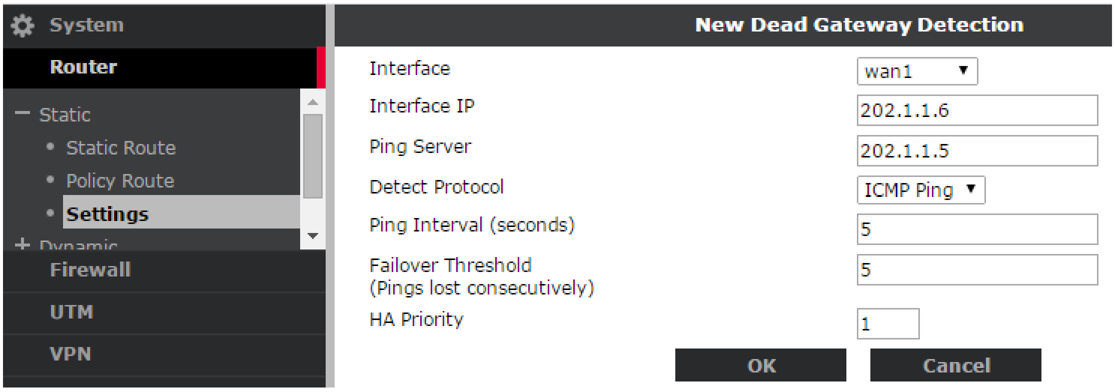


ECMP Load Balancing Method

● Source IP based ○ Weighted Load Balance ○ Spillover

Dead Gateway Detection

Click **Create New**. Set ping server detection as shown in the following figure:



New Dead Gateway Detection

Interface	wan1
Interface IP	202.1.1.6
Ping Server	202.1.1.5
Detect Protocol	ICMP Ping
Ping Interval (seconds)	5
Failover Threshold (Pings lost consecutively)	5
HA Priority	1

Interface: It indicates the interface to be monitored. Here, choose **wan1**.

Interface IP: It indicates the IP address of the interface and the source IP address of the detection data packet.

Ping Server: Enter the IP address of the server for detection. In general, it is defined as the IP address of the next-hop gateway.

Detect Protocol: Options are **ICMP Ping**, **TCP echo**, and **UDP echo**.

Ping Interval (seconds): Enter **5**. One detection data packet is sent every five seconds.

Failover Threshold: If detection fails for five times, it indicates that the interface cannot be used.

HA Priority: Set it to **1**. After interface detection fails, the values of users and the variable (initial value is 0) for determining HA switchover in the HA protocol increase by 1.

Configuration commands:

config router gwdetect edit "wan1"	Specifies the monitored interface.
set failtime 3	If three detection data packets are lost continuously, it indicates that the interface fails.
set ha-priority 5	After ping detection of the interface fails, HA association parameter value increases by 5.
set interval 2	Second one ping packet every two seconds.
set server 202.1.1.5	More than two detected gateways can be configured. As long as one gateway responds, it indicates that the interface works normally.

end	

Related HA Configuration

If only the preceding configuration is done, HA switchover is not carried out in the case of ping detection failure. The route to this interface is not valid again. HA configuration should tell wan1 interface of the firewall that ping server will be used as the condition of triggering HA switchover.

```
RG-WALL #config system ha
RG-WALL (ha)#Set pingserver-monitor-interface wan2     //Set ping server of wan2
interface.
RG-WALL (ha)#Set pingserver-failover-threshold 0       //It indicates the threshold of HA
switchover. By default, the value is 0.
RG-WALL (ha)#set pingserver-flip-timeout 60            //It indicates the interval at
which HA switchover continuously triggered by ping server twice.
```

Related HA Configuration

The command **set ha-priority 1** is related to **pingserver-failover-threshold 0**. When ping server detection of wan1 interface fails, **pingserver-failover-threshold** value increases by 1, which reaches the threshold (0) and HA switchover is triggered.

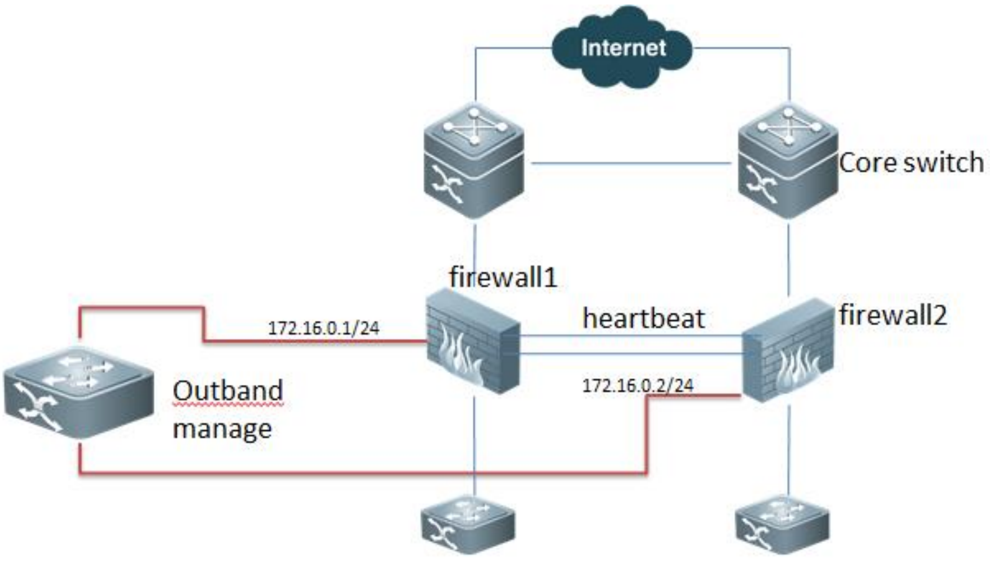
In the case of **pingserver-failover-threshold 2**, even if pingserver detection of wan1 interface fails, **set ha-prioirty 1** is smaller than **pingserver-failover-threshold 2**, which does not reach the threshold, HA switchover is not triggered.

6.6 Configuring the Out-of-Band Management Interface

Management Requirements

In an HA cluster, the configuration of all the cluster members is the same. The master device can be managed only through its IP address. Each slave device cannot be separately managed through its IP address. To ensure business security, it is essential to separate the management network from the business network. To realize the aim, configure a specialized out-of band management interface for HA. The configuration will not be synchronized.

Network Topology



Configuration Tips

1. Basic configuration.
2. Configure the reserved management port.
3. Configure the IP address for the out-of-band management port.
4. Configure the gateway for the out-of-band management port.
5. Configure SNMP.

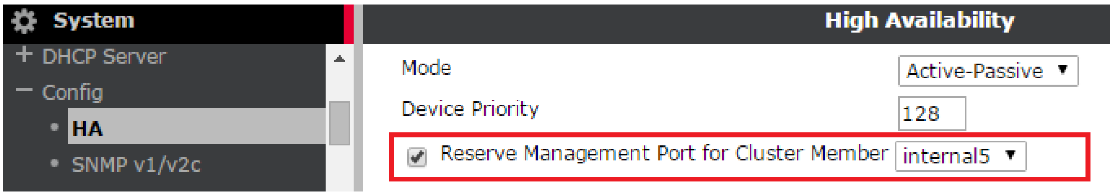
Configuration Steps

1. Basic configuration.

Complete HA basic configuration according to the section “Basic Configuration” in this chapter.

2. Configure the reserved management port.

Choose **System** > **Config** > **HA**. Select **Reserve Management Port for Cluster Member**. Choose an interface as an independent management interface. Here, choose **internal5**. See the following figure:



Mode: Active-Passive ▼

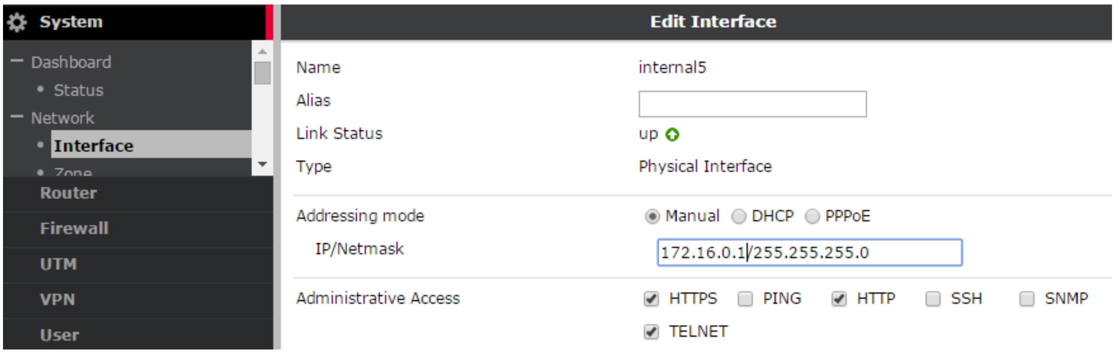
Device Priority: 128

☑ Reserve Management Port for Cluster Member: internal5 ▼

3. Configure the IP address for the out-of-band management port.

1) Configure the IP address for the out-of-band management port on the master device.

Choose **System** > **Network** > **Interface** > **internal5**, as shown in the following figure:



Edit Interface

Name	internal5
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	172.16.0.1/255.255.255.0
Administrative Access	☑ HTTPS □ PING ☑ HTTP □ SSH □ SNMP ☑ TELNET

Configure the IP address of internal5. Set **Administrative Access**.

2) Configure the management IP address for the slave device.

At the beginning, when HA is not established, set internal5 interface of the slave device through the web interface to be a management interface. If HA has been established and has started running, the slave device cannot be managed on the web interface at the beginning.

You can set the IP address of internal5 interface of the slave device to be the out-of-band management address by using the following methods:

A. Manage the slave device on the master device.

Run the following command on the master device to enter the slave device. Run the following command to enter the slave device.

```
RG-WALL # exec ha  manage  ?
<id>    please input peer box index.
<1>     xxxxxxxx SN
           RG-WALL # exec ha  manage   1   //Jump to the slave device.
```

Run the following command to set the IP address of internal5 interface.

```
RG-WALL #config system interface
RG-WALL(interface)#edit internal5
RG-WALL(internal5)#set ip 172.16.0.2/24
RG-WALL(internal5)#set allowaccess  https ping snmp
RG-WALL(internal5)#end
```

B. The slave device can also be managed through the console interface.

Run the following command to set the IP address of internal5 interface.

```
RG-WALL#config system interface
RG-WALL(interface)#edit internal5
RG-WALL(internal5)#set ip 172.16.0.2/24
RG-WALL(internal5)#set allowaccess  https ping snmp
RG-WALL(internal5)#end
```

4. Configure the gateway for the out-of-band management port.

Run the following commands respectively on two firewalls:

```
RG-WALL#config system ha
```

```
RG-WALL(ha)#set ha-mgmt-interface-gateway 172.16.0.254

RG-WALL(ha)#end
```

5. **Configure SNMP.**

```
RG-WALL#config system snmp  community
RG-WALL (community)#edit 1
RG-WALL (1)#config hosts
RG-WALL (hosts)#edit 1
RG-WALL (1)#set ha-direct enable                / /This command is used to access the
independent management port only.
RG-WALL (1)#set ip 10.0.0.100 255.255.255.255
RG-WALL (1)#next
RG-WALL (hosts)#end
RG-WALL (community)#set name readfornm
RG-WALL (community)#next
```

Verification

Perform HTTPS management and SNMP monitor of two devices through the independent management interface.

6.7 Related Commands

Use the **config system ha** command to enter HA configuration mode. The following lists common configuration commands:

1) set group-id *ID*

This command is used to configure the group ID of an HA cluster. The members in one cluster must have the same group ID. The group ID is a component element of the virtual MAC address of the firewall interface. When one broadcast domain contains more than two HA clusters, their group IDs should be different to prevent MAC address conflict.

2) set group-name "Ruijie-HA"

The members in one cluster must have the same group name.

3) set mode standalone/a-a/a-p

In HA, generally set it to **a-p**. In AA mode, HA roles contain master and slave devices. Generally, they are regarded to work in active-active mode. Actually, although the master and slave devices are working, one device will act as the master device to control and assign traffic and sessions to other devices in the cluster. In AA mode, by default, only the UTM traffic is balanced. Therefore, when the UTM function is not used, recommend using AP mode.

4) set password

The members in one cluster must have the same password.

5) **set hbdev port_number priority**

Use this command to configure the heartbeat interface. The port with a higher priority is preferably used.

6) **unset session-sync-dev**

You can configure a dedicated heartbeat interface for synchronizing session information. By default, the heartbeat interface for synchronizing session information and the heartbeat interface for synchronizing control information are the same.

7) **set route-ttl *time***

It indicates the alive time of the route forwarding table. Between HA devices, only the forwarding table is synchronized instead of the routing table. After one slave device is elected to be the master device, the alive time of the original forwarding table is set to 10 seconds by default. Later, the forwarding table is generated by the static or dynamic routing protocol and the device continues working.

8) **set route-wait *time***

Use this command to set the waiting time for configuration synchronization to slaves after the master device receives a new routing entry.

9) **set route-hold *time***

Use this command to set the routing synchronization interval for the master device to avoid repeated route update caused by route flapping.

10) **set sync-config enable**

Use this command to enable automatic synchronization of configuration files.

11) **set encryption {enable | disable}**

Use this command to enable or disable AES-128 and SHA1 to encrypt and verify heartbeat information.

12) **set authentication {enable | disable}**

Use this command to enable or disable SHA1 algorithm to verify heartbeat information.

13) **set hb-interval *time***

Use this command to set the interval at which heartbeat packets are sent in the unit of 100 ms. If the interval is set to 2, it indicates that one heartbeat message is sent every 200 ms.

14) **set hb-lost-threshold *number***

Use this command to set the threshold for heartbeat packet loss. If six heartbeat messages are lost continuously, the peer device is thought to die.

15) **set helo-holddown *number***

Use this command to set the hello interval. It is the waiting time before a device joins an HA cluster to prevent HA repeated negotiation caused by the member discovering failure.

16) **set arps *number***

Use this command to configure the update number. After a device becomes the master, it shall send a gratuitous ARP packet to announce its MAC address, so that the connected switches can timely update the MAC address table.

17) **set arps-interval *time***

Use this command to set the interval at which gratuitous ARP packets are sent in the unit of seconds.

18) **set session-pickup {enable | disable}**

Use this command to enable or disable session synchronization. The default is **disable**. Generally, it is set to **enable**.

19) **set session-pickup-delay {enable | disable}**

Use this command to synchronize the sessions that keep alive for more than 30 seconds. After it is set to **enable**, the performance is optimized. The sessions that keep alive for less than 30 seconds will be lost during HA failover. By default, it is set to **disable**. Use this command with caution.

20) **set link-failed-signal disable**

Use this command to shut down all the interfaces except the heartbeat interface for one second when the HA failover is triggered by the port failure, so that the connected switch can timely update the MAC address table.

21) **set uninterruptable-upgrade enable**

Use this command to enable uninterrupted OS upgrade. The system automatically upgrades the devices in the cluster and the devices in the cluster automatically switch over without business interruption.

22) **set ha-uptime-diff-margin *time***

Use this command to set the interval of startup difference neglection. During HA master election, startup time is factor. When the startup time difference between two devices is less than 300, it will be ignored.

23) **set override disable**

By default, it is set to **disable**. During HA election, elements are compared in the following order: valid interface quantity > runtime > HA priority > device SN. When it is set to **enable**, the order is changed into: valid interface quantity > HA priority > Runtime > device SN. Every time when a device joins or leaves from the cluster, the entire cluster is forced to begin the election of the master device again.

24) **set priority *number***

Use this command to set the HA priority to facilitate management. It is recommend to set the HA priority of the master device to 200, while that of slave devices to 100.

25) **set monitor *port_number***

Use this command to configure the port to be monitored. The device with the maximum number of valid ports becomes the master device.

26) **unset pingserver-monitor-interface**

Use this command to unset the pingserver monitored port.

27) **set pingserver-failover-threshold 0**

Use this command to set the failover threshold for pingserver. If the threshold is 0, it indicates that any pingserver failure will trigger HA failover.

28) **set pingserver-flip-timeout *time***

Use this command to set the failover interval for the pingserver. If A fails, pingserver is switched over to

B. If B also fails, it waits for 60 minutes to switch back to A.

29) **set ha-mgmt-status enable**

Use this command to configure out-of-band management. Use the following two commands to respectively set the out-of-band management interface and gateway IP address.

set ha-mgmt-interface port_number

set ha-mgmt-interface-gateway x.x.x.x

7 Universal Typical Functions

7.1 UTM Security Applications

7.1.1 Intrusion Prevention

7.1.1.1 Protecting the Intranet Server

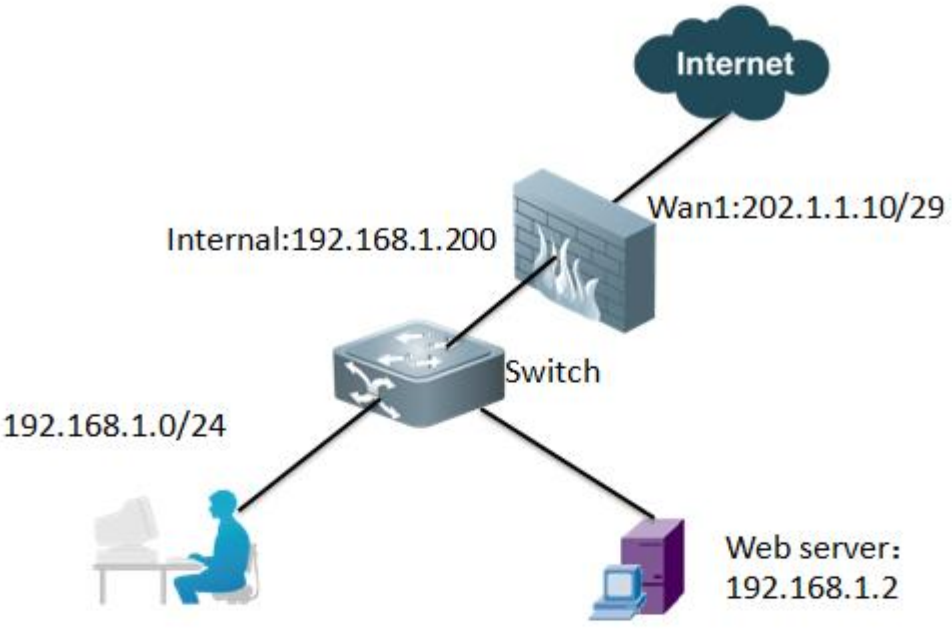
Application Scenario:

One Web server (IP address: 192.168.1.2) is deployed inside the company, which is mapped to the extranet IP address 202.1.1.11. Open the HTTP service to the extranet.

Networking Requirements

The Web server opens HTTP service to the Internet, thus increasing the risk in attacking the server. The IPS function should be used for protection against the access from the Internet.

Network Topology



Configuration Tips

1) Initialize Internet access configuration.

2) Configure the virtual IP (DNAT).

3) Define the IPS sensor.

4) Configure policies and enable IPS.

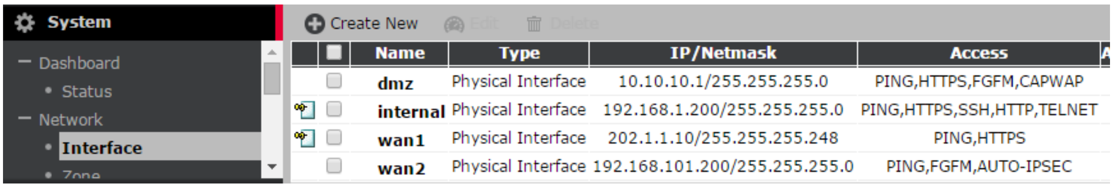
5) Enable the logging function.

Configuration Steps

1. Basic configuration for Internet access

For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under section “Internet Access via a Single Line” in “Configuring Routing Mode”.

IP address configuration of the interfaces is as shown in the following figure:

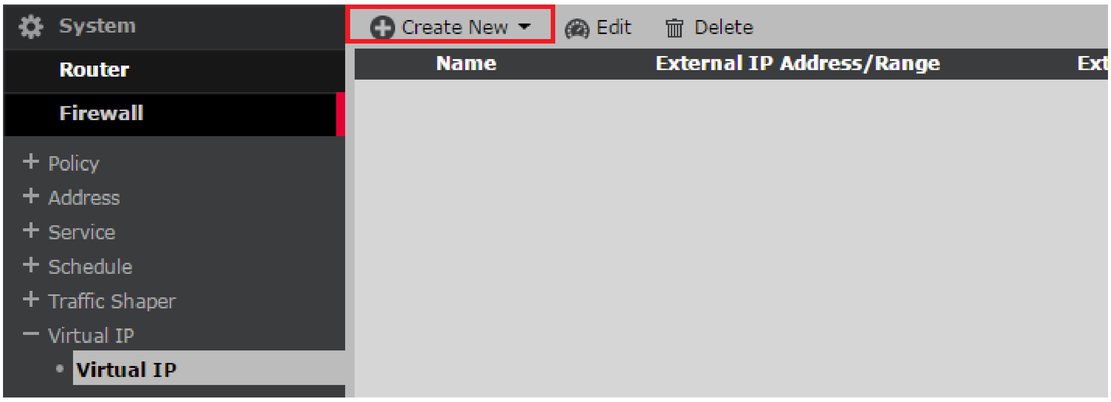


Name	Type	IP/Netmask	Access
dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFM,CAPWAP
internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP,TELNET
wan1	Physical Interface	202.1.1.10/255.255.255.248	PING,HTTPS
wan2	Physical Interface	192.168.101.200/255.255.255.0	PING,FGFM,AUTO-IPSEC

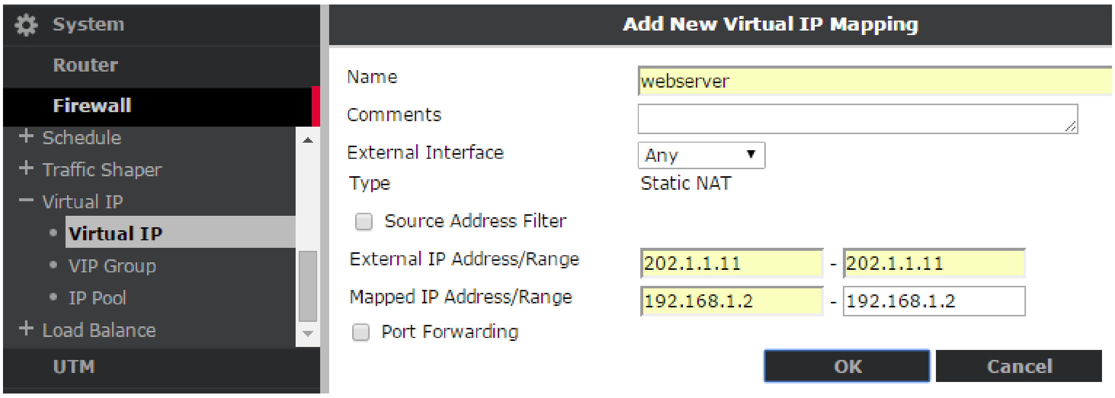
The route configuration is as shown in the following figure:

2. Configure the virtual IP address (DNAT).

Choose **Firewall** > **Virtual IP** > **Virtual IP**, and then click **Create New**, as shown in the following figure:



Configure the virtual IP address. Enter the name: **webserver**. The virtual IP address is used for the destination address translation of wan1 interface.



Add New Virtual IP Mapping

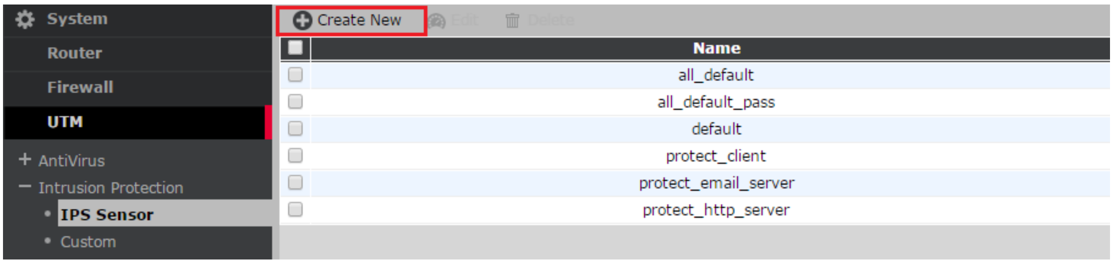
Name	webserver	
Comments		
External Interface	Any ▾	
Type	Static NAT	
□ Source Address Filter		
External IP Address/Range	202.1.1.11	- 202.1.1.11
Mapped IP Address/Range	192.168.1.2	- 192.168.1.2
□ Port Forwarding		

3. Define the IPS sensor.

Customize the signature database of the IPS for the system and programs of the server. Suppose that the system is installed with Windows and enables HTTP service.

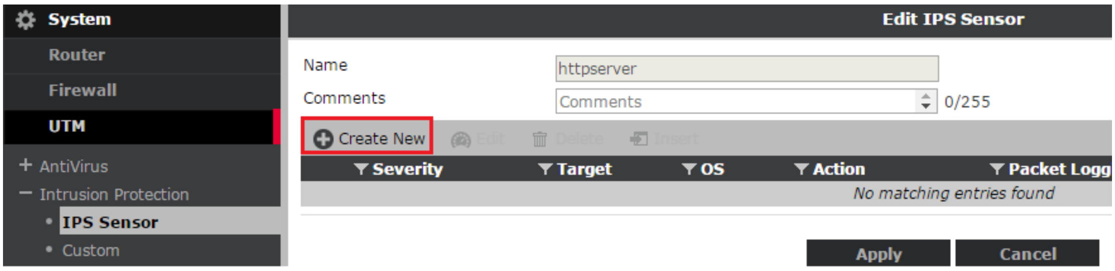
a) Choose **System** > **Intrusion Protection** > **IPS Sensor**. The pre-defined sensor has been embedded. Click **Create New**.

Enter the sensor name **httpserver**, and then click **OK**.



□	Name
□	all_default
□	all_default_pass
□	default
□	protect_client
□	protect_email_server
□	protect_http_server

b) Add the IPS filter (multiple IPS filters can be added) to the sensor. On the **Edit IPS Sensor** page, click **Create New**, as shown in the following figure:



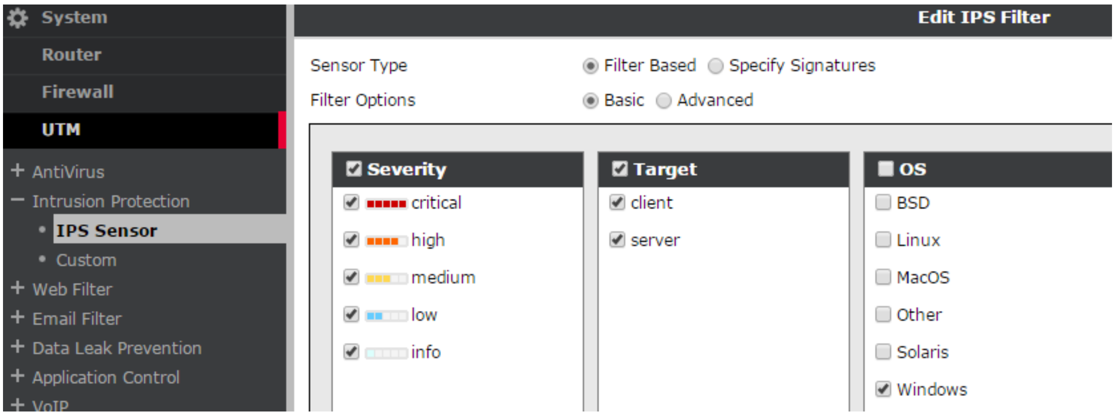
Edit IPS Sensor

Name	httpserver	
Comments	Comments	0/255

Severity	Target	OS	Action	Packet Logg
No matching entries found				

The IPS signature configuration page is displayed. Signatures are filtered in the following two manners:

A. Basic mode



Edit IPS Filter

Sensor Type ● Filter Based ○ Specify Signatures

Filter Options ● Basic ○ Advanced

☑ Severity: ☑ critical, ☑ high, ☑ medium, ☑ low, ☑ info

☑ Target: ☑ client, ☑ server

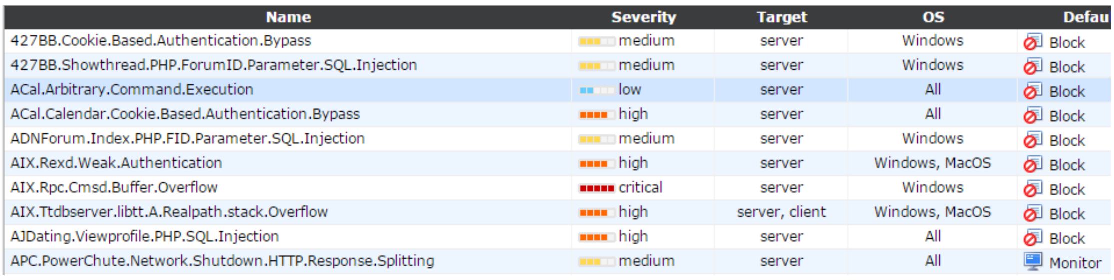
□ OS: □ BSD, □ Linux, □ MacOS, □ Other, □ Solaris, ☑ Windows

Severity: Classified according to severity. Choose all the options.

Target: In this example, it is a Web server. For the attack against the server, choose **server**.

OS: Choose the OS type of the system to be protected.

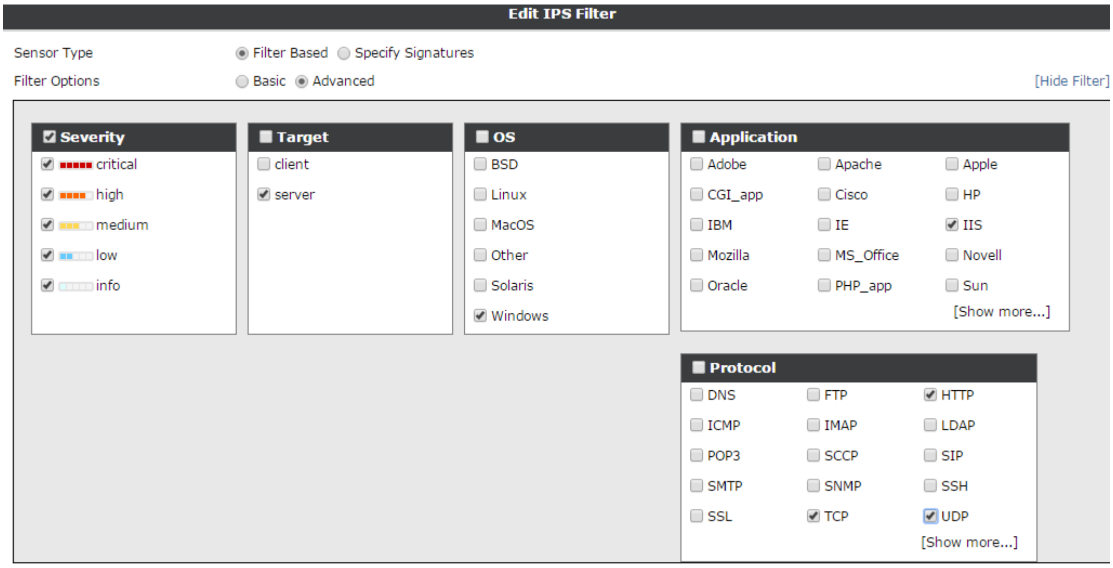
The following page lists the IPS attack types to be filtered:



Name	Severity	Target	OS	Defau
427BB.Cookie.Based.Authentication.Bypass	medium	server	Windows	Block
427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection	medium	server	Windows	Block
ACal.Arbitrary.Command.Execution	low	server	All	Block
ACal.Calendar.Cookie.Based.Authentication.Bypass	high	server	All	Block
ADNForum.Index.PHP.FID.Parameter.SQL.Injection	medium	server	Windows	Block
AIX.Rexd.Weak.Authentication	high	server	Windows, MacOS	Block
AIX.Rpc.Cmsd.Buffer.Overflow	critical	server	Windows	Block
AIX.Ttdbserver.libtt.A.Realpath.stack.Overflow	high	server, client	Windows, MacOS	Block
AJDating.Viewprofile.PHP.SQL.Injection	high	server	All	Block
APC.PowerChute.Network.Shutdown.HTTP.Response.Splitting	medium	server	All	Monitor

B. Advanced mode (Recommended)

In this mode, more accurate matching can be done to improve system efficiency. Choose **IIS**, **HTTP**, **TCP**, and **UDP** as prompted.



Edit IPS Filter

Sensor Type ● Filter Based ○ Specify Signatures

Filter Options ○ Basic ● Advanced [Hide Filter]

☑ Severity: ☑ critical, ☑ high, ☑ medium, ☑ low, ☑ info

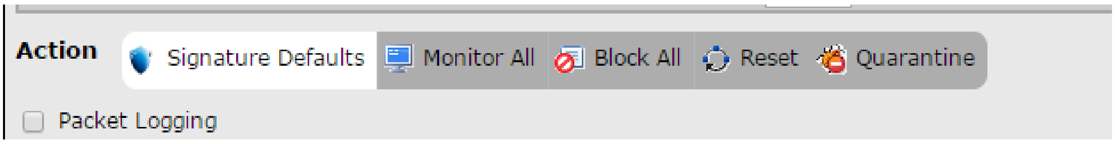
□ Target: □ client, ☑ server

□ OS: □ BSD, □ Linux, □ MacOS, □ Other, □ Solaris, ☑ Windows

□ Application: □ Adobe, □ Apache, □ Apple, □ CGI_app, □ Cisco, □ HP, □ IBM, □ IE, ☑ IIS, □ Mozilla, □ MS_Office, □ Novell, □ Oracle, □ PHP_app, □ Sun [Show more...]

□ Protocol: □ DNS, □ FTP, ☑ HTTP, □ ICMP, □ IMAP, □ LDAP, □ POP3, □ SCCP, □ SIP, □ SMTP, □ SNMP, □ SSH, □ SSL, ☑ TCP, ☑ UDP [Show more...]

After the IPS signature is chosen, choose the actions for handling these attack signatures:



Action ● Signature Defaults | Monitor All | Block All | Reset | Quarantine

□ Packet Logging

Signature Defaults: By default, each IPS signature defines the action against the attack. The firewall is processed according to the pre-defined action.

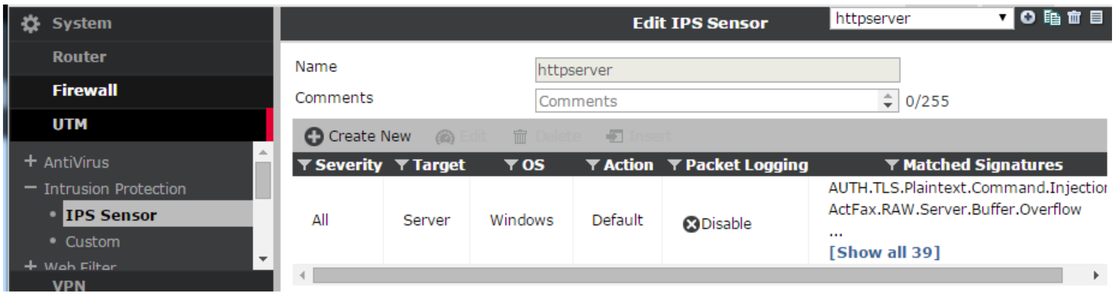
Monitor All: Only monitor applications and generate logs without interrupting service.

Block All: Block and discard data packets.

Reset: Reset sessions.

Quarantine: Quarantining manners are classified into the attacked IP address, attacker IP address and attacked device IP address, and quarantining interfaces. After quarantining proceeds for a period of time, disable service communication of the quarantined device. Use this function with caution.

c) Click **OK** to finish the filter configuration. To add more filters, repeat the preceding method.



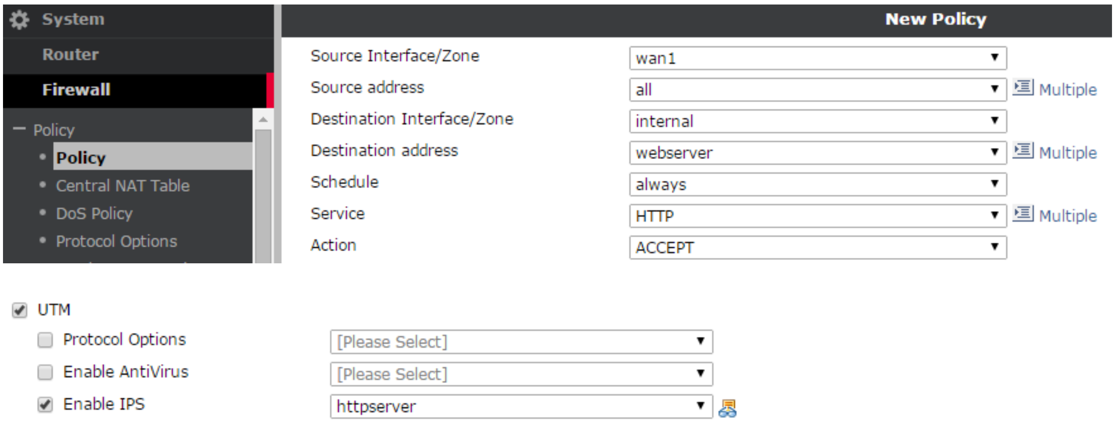
Name: httpserver

Comments: Comments 0/255

Severity	Target	OS	Action	Packet Logging	Matched Signatures
All	Server	Windows	Default	Disable	AUTH.TLS.Plaintext.Command.Injectior ActFax.RAW.Server.Buffer.Overflow ... [Show all 39]

As shown in the above figure, there are 39 IPS signatures matching the filter.

4. Configure policies and enable IPS.



Source Interface/Zone: wan1

Source address: all

Destination Interface/Zone: internal

Destination address: webserver

Schedule: always

Service: HTTP

Action: ACCEPT

☑ UTM

□ Protocol Options [Please Select]

□ Enable AntiVirus [Please Select]

☑ Enable IPS httpserver

Source Interface/Zone: Choose wan1.

Source address: Choose all.

Destination Interface/Zone: Choose internal.

Destination address: Choose webserver. It indicates the defined object mapped by the virtual IP address.

Service: Choose HTTP. The system allows Internet access only by HTTP.

UTM: Select it.

Enable IPS: Choose the defined IPS sensor httpserver.

5. Enable packet logging.

```
RG-WALL # config ips sensor
RG-WALL (sensor) # edit httpserver
new entry ’httpserver’ added
RG-WALL (httpserver) # set log enable
RG-WALL (httpserver) # config entries
RG-WALL (entries) # edit 1
new entry ’1’ added
RG-WALL (1) # set log enable
RG-WALL (1) # set log-packet enable
RW-WALL (1) # end
```

7.1.1.2 Preventing DoS Attacks

Application Scenario:

DoS focuses on initiating attacks by using the specific vulnerabilities of the host, resulting in network stack failure, system breakdown, and host breakdown. Therefore, the host fails to provide normal network service functions, which results in denial of service. Common DoS attacks include TearDrop, Land, Jolt, IGMP Nuker, Boink, Smurf, Bonk, and OOB. Scanning is also a kind of network attack. Before initiating network attacks, attackers generally try to determine the open TCP/UDP ports on the target device. An open port indicates an application.

DoS has two manners: traffic attack and resource exhaustion attack. Traffic attack is the attack against network bandwidth. Large number of attack packets block network bandwidth and legal packets cannot reach the host. Resource exhaustion attack is the attack against servers. The attackers send a large number of attack packets to exhaust host memory or the CPU, resulting in disrupt network service.

The NGFW anti-SYN Flood attack function employs the latest SYN cookie technology, which occupies few system resources and effectively prevents DoS attacks against servers.

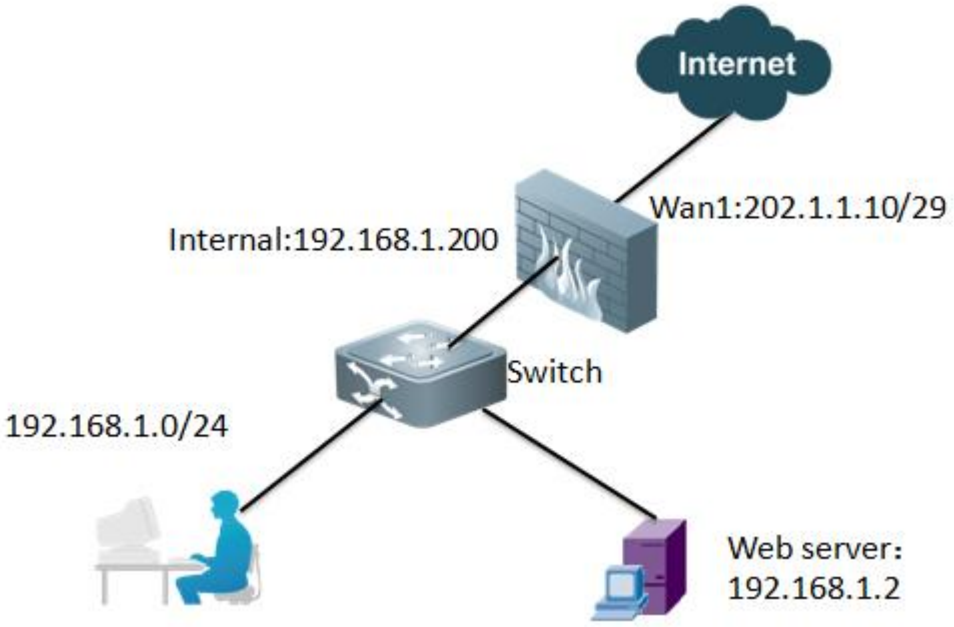
The anti-SYN Flood function can prevent external malicious attacks and protect devices and intranet. An alarm is reported when such attacks are detected..

In the preceding example “protecting intranet servers”, apart from IPS protection, DoS protection is required.

Networking Requirements

The Web server IP address is 192.168.1.2, mapped to the extranet IP address 202.1.1.11. The Web server opens HTTP service to the Internet, thus increasing the server attack risk. DoS prevention should be enabled to ensure Internet access security.

Network Topology



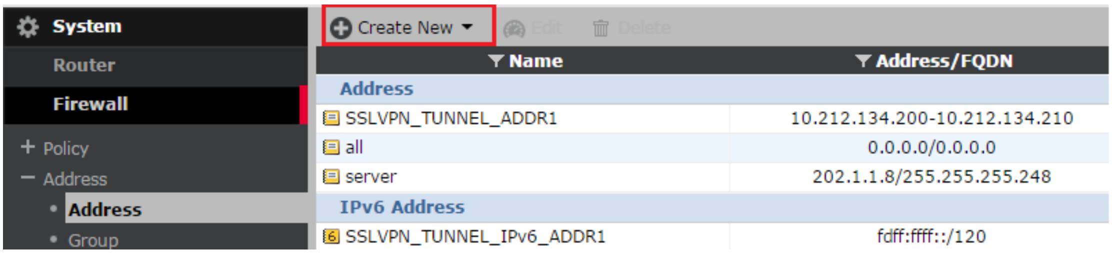
Configuration Tips

1. Configure the server IP address.
2. Define the DoS policy.

Configuration Steps

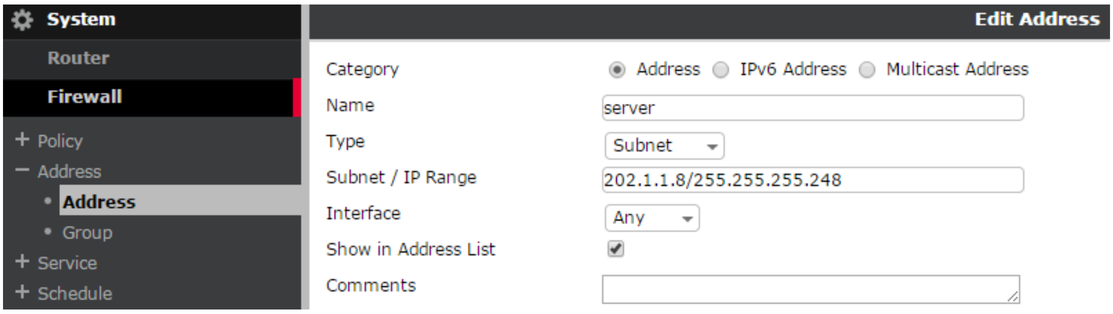
1. Configure the server IP address.

Choose **Firewall** > **Address** > **Address**, and then click **Create New**, as shown in the following figure:



Name	Address/FQDN
Address	
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210
all	0.0.0.0/0.0.0.0
server	202.1.1.8/255.255.255.248
IPv6 Address	
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120

Set **Name** to **server**. Choose **Subnet** as **Type**. Set **Subnet/IP Range** to **202.1.1.8/29**. Click **OK**. See the following figure:



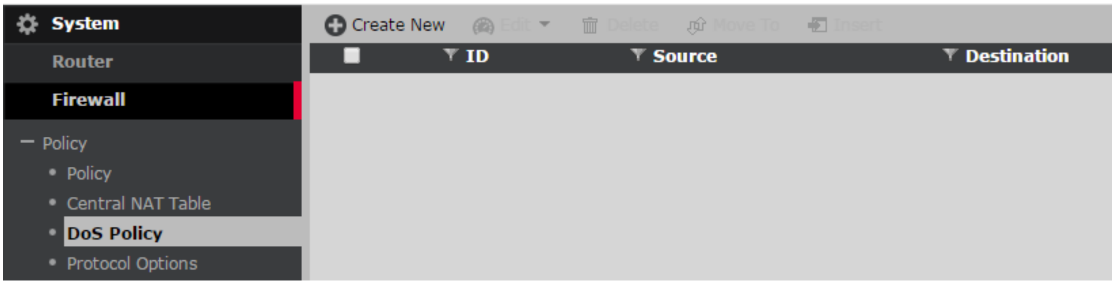
Edit Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	server
Type	Subnet
Subnet / IP Range	202.1.1.8/255.255.255.248
Interface	Any
Show in Address List	☑
Comments	

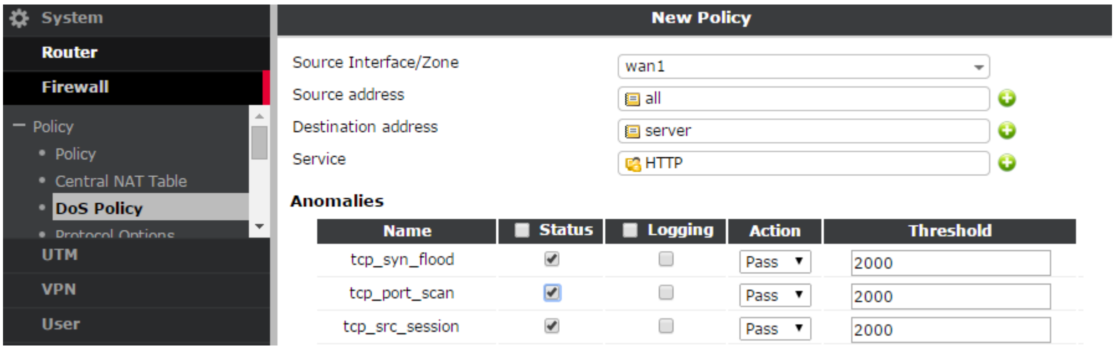
The IP range includes the server IP address (202.1.1.11) and the extranet port IP address (202.1.1.10) of the firewall.

2. **Define the DoS policy.**

Choose **Firewall** > **Policy** > **DoS Policy**, and then click **Create New**, as shown in the following figure:



Configure DoS policy parameters, as shown in the following figure:



New Policy

Source Interface/Zone	wan1
Source address	all
Destination address	server
Service	HTTP

Anomalies

Name	□ Status	□ Logging	Action	Threshold
tcp_syn_flood	☑	□	Pass	2000
tcp_port_scan	☑	□	Pass	2000
tcp_src_session	☑	□	Pass	2000

Source Interface/Zone: Choose **wan1**. Wan1 interface is the extranet interface. Apply the DoS policy on the wan1 interface.

Source address: Choose **all**.

Destination address: The protected IP address.

Service: It indicates the protected service, such as HTTP80 in this example.

Anomalies: It indicates the DoS protection type.

tcp_sysn_flood: It is a DoS attack name.

Status: It indicates whether to enable the protection.

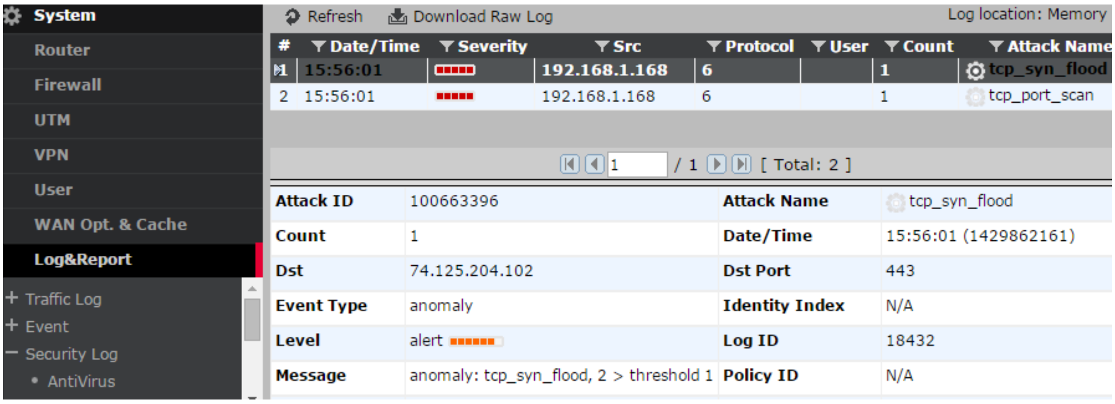
Logging: It indicates whether to enable logging. DoS logging can be enabled without the need of running the command in the CLI. You just need to select **Logging**.

Action: It indicates the action upon detecting an attack. There are two options: **Block** and **Pass**.

Threshold: It indicates the number of attacks detected every second that will trigger the corresponding action.

Click **OK** to finish configuration.

3. **View DOS protection logs.**



#	Date/Time	Severity	Src	Protocol	User	Count	Attack Name
1	15:56:01	■■■■■	192.168.1.168	6		1	tcp_syn_flood
2	15:56:01	■■■■■	192.168.1.168	6		1	tcp_port_scan

1 / 1 [Total: 2]

Attack ID	100663396	Attack Name	tcp_syn_flood
Count	1	Date/Time	15:56:01 (1429862161)
Dst	74.125.204.102	Dst Port	443
Event Type	anomaly	Identity Index	N/A
Level	alert ■■■■■■	Log ID	18432
Message	anomaly: tcp_syn_flood, 2 > threshold 1	Policy ID	N/A

7.1.2 Anti-Virus

7.1.2.1 Enabling Anti-Virus Function

Application Scenario:

As the Internet rapidly develops, the network environment becomes more and more complicated. A mix of malicious attacks, Trojan horse viruses, and worms increase. Enterprises need to protect the network deeply at multiple layers, thus effectively protecting network security. IPS provides deep protection against the network. If vulnerabilities in the intranet server are not timely repaired, these vulnerabilities may be used by attackers to cause the consequences that cannot be avoided. In this case, enable virus, vulnerability, and Trojan horse filter functions on the egress firewall.

Principles:

The protocol analysis module identifies protocols of the data packets, including TCP, UDP, and ICMP and common protocols, such as HTTP, FTP, SMTP, POP3 and IMAP. After protocol identification, the alarm information is reported.

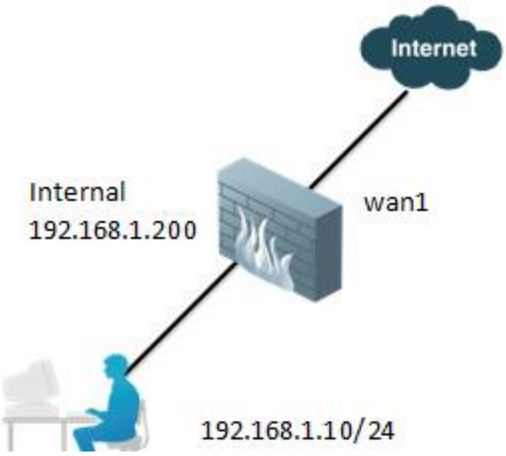
Note:

The intrusion prevention, anti-virus, and application control functions of the NGFW can be used only when the corresponding signature databases are imported. By default, the NGFW is equipped with the latest signature database version. To keep the ideal effects of these functions, you need to update the signature feature in real time. If you do not purchase the formal license, the signature database cannot be updated and functions are not ideal. If you purchase the formal license and import the license to the device, the system automatically updates the signature database to the latest version.

Networking Requirements

When intranet users view Web pages and receive/send emails, the system needs to detect viruses in the files transmitted via the related protocols to prevent viruses from spreading to the intranet.

Network Topology



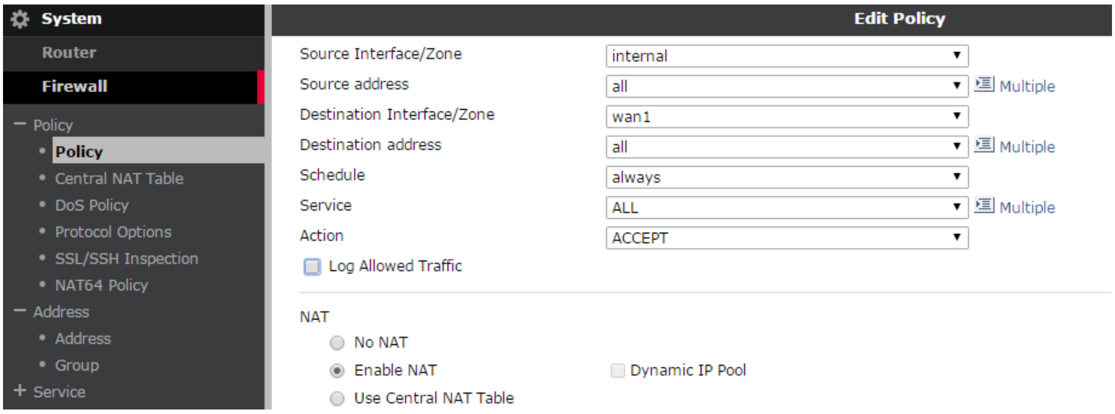
Configuration Tips

1. Initialize Internet access configuration.
2. Configure anti-virus function.
3. Configure the proxy options.
4. Enable anti-virus function in the policy.

Configuration Steps

1. Initialize Internet access configuration.

For the detailed configuration process, see section "Configuring Internet Access via a Static Link" under section "Internet Access via a Single Line" in "Configuring Routing Mode".



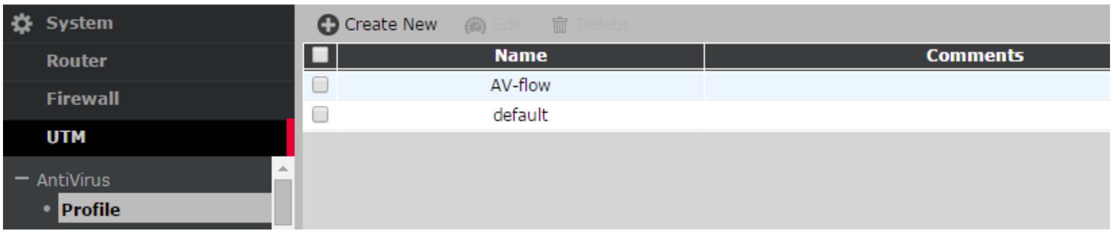
Source Interface/Zone	internal
Source address	all (Multiple)
Destination Interface/Zone	wan1
Destination address	all (Multiple)
Schedule	always
Service	ALL (Multiple)
Action	ACCEPT

□ Log Allowed Traffic

NAT
○ No NAT
● Enable NAT □ Dynamic IP Pool
○ Use Central NAT Table

2. Configure anti-virus function.

Choose **UTM** > **AntiVirus** > **Profile**, as shown in the following figure:



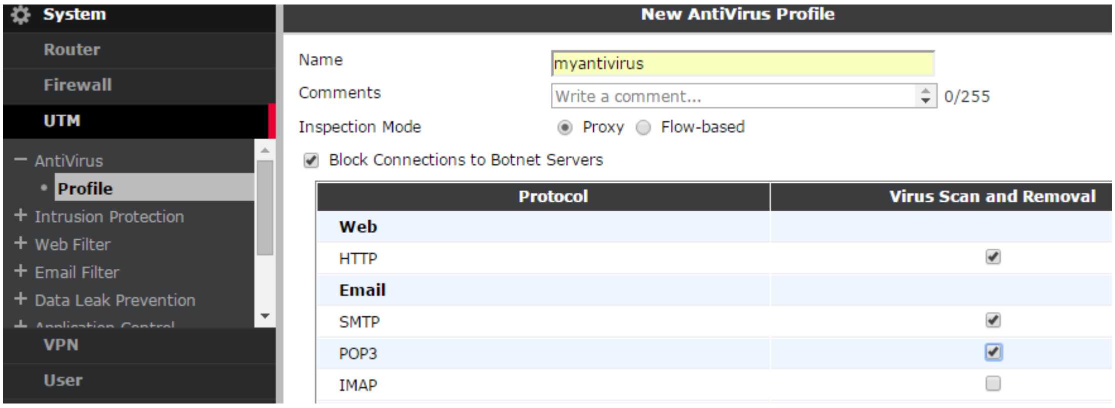
□	Name	Comments
□	AV-flow	
□	default	

You can view two embedded anti-virus profiles:

AV-flow: It is the script for flow-based inspection mode. In this mode, virus scanning is fast and accuracy is lower than the proxy mode.

default: It is the script for proxy inspection mode. In this mode, files are buffered in the memory for scanning. The accuracy is high, but scanning is slow.

You can directly use the default profiles and edit the profile script (if needed), or create a new anti-virus profile. The following takes creating a new anti-virus profile as an example. Click **Create New**, then fill in the following parameters:



New AntiVirus Profile

Name: myantivirus

Comments: Write a comment... 0/255

Inspection Mode: ● Proxy ○ Flow-based

☑ Block Connections to Botnet Servers

Protocol	Virus Scan and Removal
Web	
HTTP	☑
Email	
SMTP	☑
POP3	☑
IMAP	□

Name: Configure the anti-virus profile name. Here, set it to **myantivirus**.

Comments: Add the description of the script.

Inspection Mode: Choose the virus scanning mode. Consider the current network traffic and the device type. Here, choose **Proxy**.

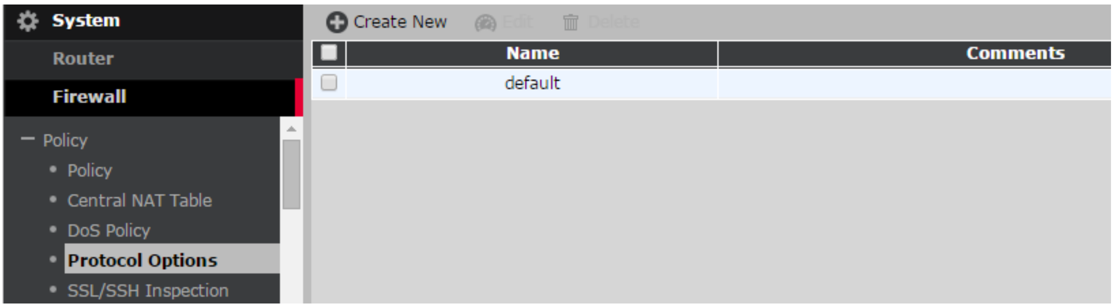
Block Connections to Botnet Servers: Choose this option. It indicates that the system blocks the connections to Botnet servers and therefore enables protection against Botnets and phishing attacks.

Protocol: Select the protocol types for virus scanning. Here, select HTTP, SMTP, and POP3.

3. Configure the proxy options. (Optional)

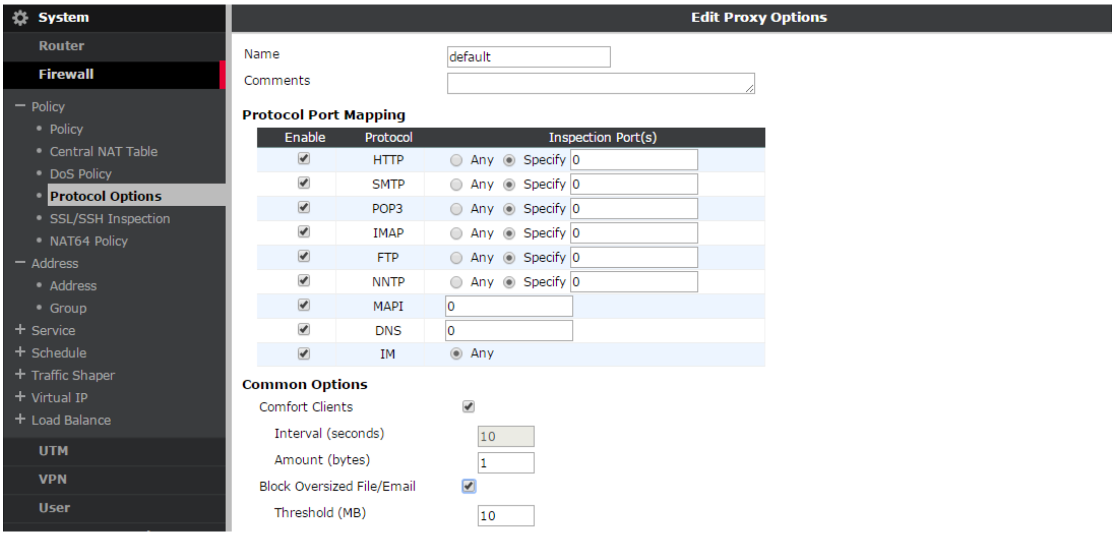
Generally, keep the default proxy options.

Choose **Firewall** > **Policy** > **Protocol Options**, as shown in the following figure:



□	Name	Comments
□	default	

Edit the default file, as shown in the following figure:



Edit Proxy Options

Name: default

Comments:

Protocol Port Mapping

Enable	Protocol	Inspection Port(s)
☑	HTTP	○ Any ● Specify 0
☑	SMTP	○ Any ● Specify 0
☑	POP3	○ Any ● Specify 0
☑	IMAP	○ Any ● Specify 0
☑	FTP	○ Any ● Specify 0
☑	NNTP	○ Any ● Specify 0
☑	MAPI	0
☑	DNS	0
☑	IM	● Any

Common Options

Comfort Clients ☑

Interval (seconds) 10

Amount (bytes) 1

Block Oversized File/Email ☑

Threshold (MB) 10

4. Protocol Port Mapping:

Enable, Protocol, Inspection Port(s): Configure the proxy options of different protocols, for example, enable HTTP port scanning. To scan multiple ports, ports should be separated with space, for example, 80 80 80 .

Common Options (Taking effect only for proxy inspection mode)

Comfort Clients: When viruses are scanned in proxy mode, files should be buffered in the firewall. After the files are scanned and the system ensures that the files are safe, the system sends them to users. In this process, users do not receive any data file. If file size is large, users need to wait for a longer time. To refine such poor user experience, the firewall is enabled to send files at a slow speed during scanning, while users are informed that the file requests have been responded and handled.

Interval (seconds): Set it to **10**. It indicates that data is sent once every 10 seconds.

Amount (bytes): Set it to **1**. It indicates the number of bytes sent every time.

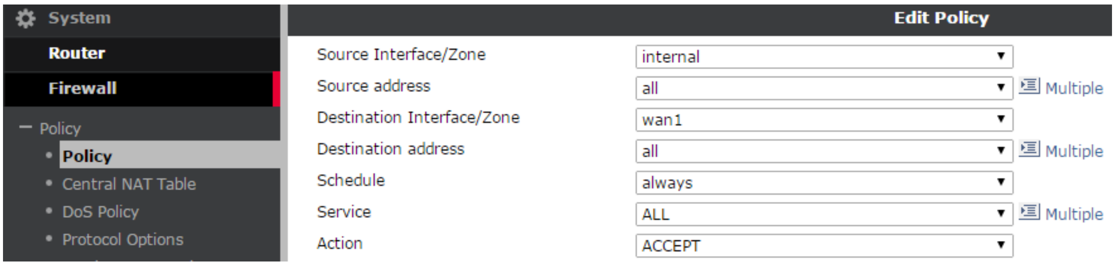
Block Oversized File/Email: It indicates that the file that exceeds the virus scanning buffer size (10 MB) is blocked. If **Black Oversized File/Email** is not chosen, the oversized file is permitted without virus scanning.

If Block Oversized File/Email is enabled, the file that exceeds the threshold will be deleted directly, which may affect user services. Confirm with the users about whether to choose this option.

Click **OK** to validate configuration.

5. Enable anti-virus function in the policy.

Edit the policy for Internet access in step 1.



Edit Policy

Source Interface/Zone: internal

Source address: all (Multiple)

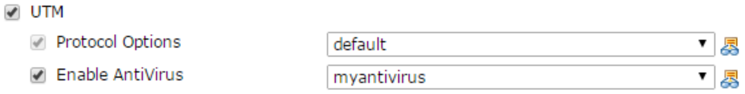
Destination Interface/Zone: wan1

Destination address: all (Multiple)

Schedule: always

Service: ALL (Multiple)

Action: ACCEPT



☑ UTM

☑ Protocol Options: default

☑ Enable AntiVirus: myantivirus

Choose **UTM** and **Enable AntiVirus**. Choose **default** from **Protocol Options** drop-down list and **myantivirus** from **Enable AntiVirus** drop-down list. Click **OK** to finish the configuration.

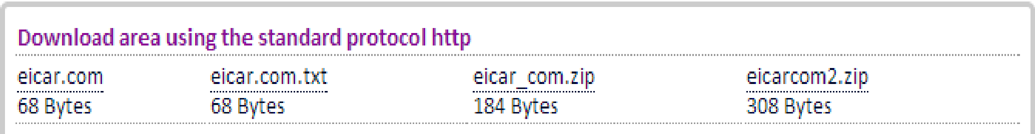
6. Enable anti-virus logging.

```
RG-WALL # config antivirus profile
RG-WALL (profile) # edit myantirus
RG-WALL (default) # set extended-utm-log enable
RG-WALL (default) # set av-virus-log enable
RG-WALL (default) # set av-block-log enable
RG-WALL (default) # end
```

Verification

1. Intercept HTTP Web page viruses.

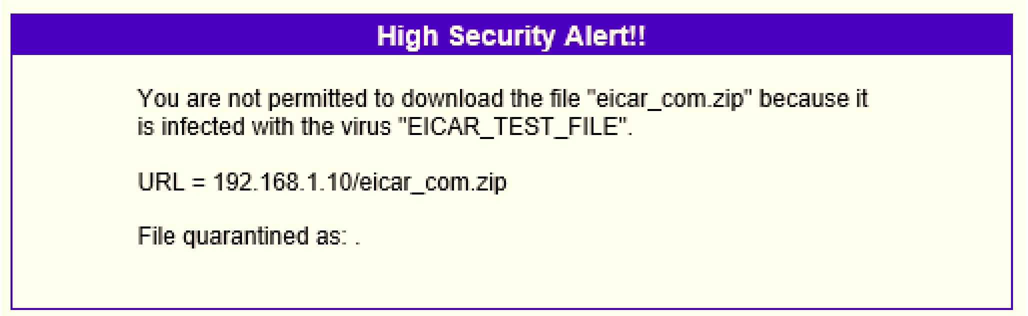
Access http://www.eicar.org/85-0-Download.html. Download the virus testing file.



Download area using the standard protocol http

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

The virus file is successfully intercepted.



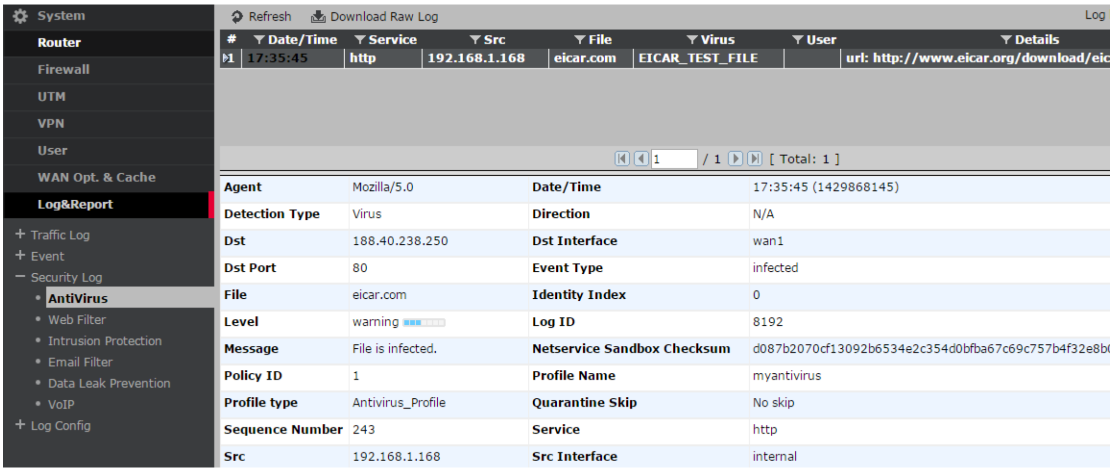
High Security Alert!!

You are not permitted to download the file "eicar_com.zip" because it is infected with the virus "EICAR_TEST_FILE".

URL = 192.168.1.10/eicar_com.zip

File quarantined as: .

Virus interception log is as follows:



#	Date/Time	Service	Src	File	Virus	User	Details
1	17:35:45	http	192.168.1.168	eicar.com	EICAR_TEST_FILE		url: http://www.eicar.org/download/eic

Agent	Mozilla/5.0	Date/Time	17:35:45 (1429868145)
Detection Type	Virus	Direction	N/A
Dst	188.40.238.250	Dst Interface	wan1
Dst Port	80	Event Type	infected
File	eicar.com	Identity Index	0
Level	warning	Log ID	8192
Message	File is infected.	Netservice Sandbox Checksum	d087b2070cf13092b6534e2c354d0bfba67c69c757b4f32e8b
Policy ID	1	Profile Name	myantivirus
Profile type	Antivirus_Profile	Quarantine Skip	No skip
Sequence Number	243	Service	http
Src	192.168.1.168	Src Interface	internal

7.1.3 Web Filter

7.1.3.1 URL Filter

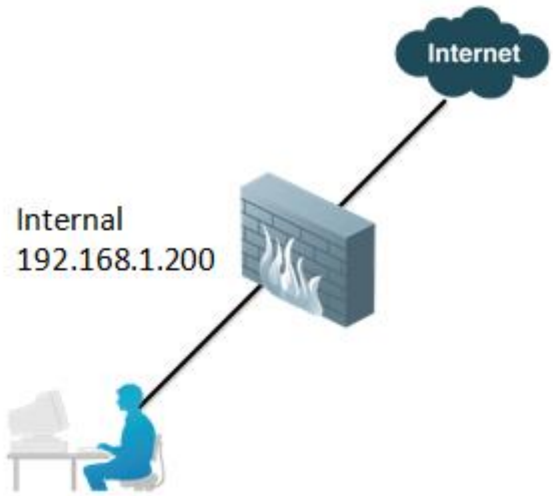
Application Scenario:

Restrict the behavior of the specific Internet users according to the specific URL.

Networking Requirements

Intranet users are only allowed to access the websites of 163.com and Baidu.com.

Network Topology



Intranet users access the Internet through firewalls.

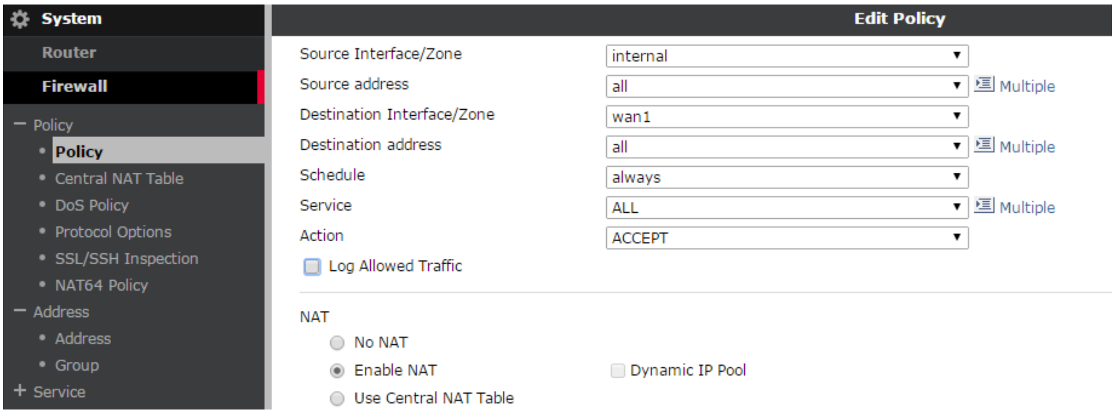
Configuration Tips

1. Initialize Internet access configuration.
2. Configure the Web filter.
3. Enable Web filter function in the policy.

Configuration Steps

1. **Initialize Internet access configuration.**

For the detailed configuration process, see section "Configuring Internet Access via a Static Link" under section "Internet Access via a Single Line" in "Configuring Routing Mode".



Edit Policy

Source Interface/Zone	internal
Source address	all
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT

□ Log Allowed Traffic

NAT

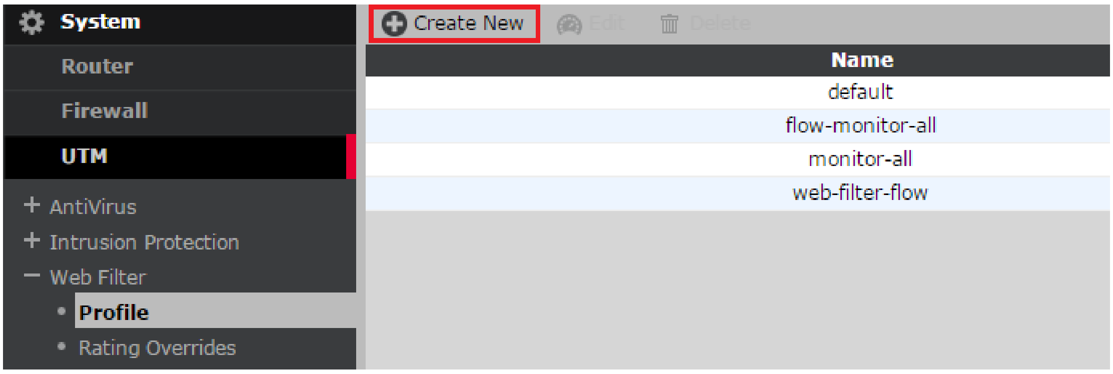
○ No NAT

● Enable NAT □ Dynamic IP Pool

○ Use Central NAT Table

2. **Define Web filter configuration.**

Choose **UTM** > **Web Filter** > **Profile**. Some Web filters are embedded, such as default and flow-monitor-all, as shown in the following figure. You can modify the embedded filter configuration, or self-define filters. Click **Create New**.

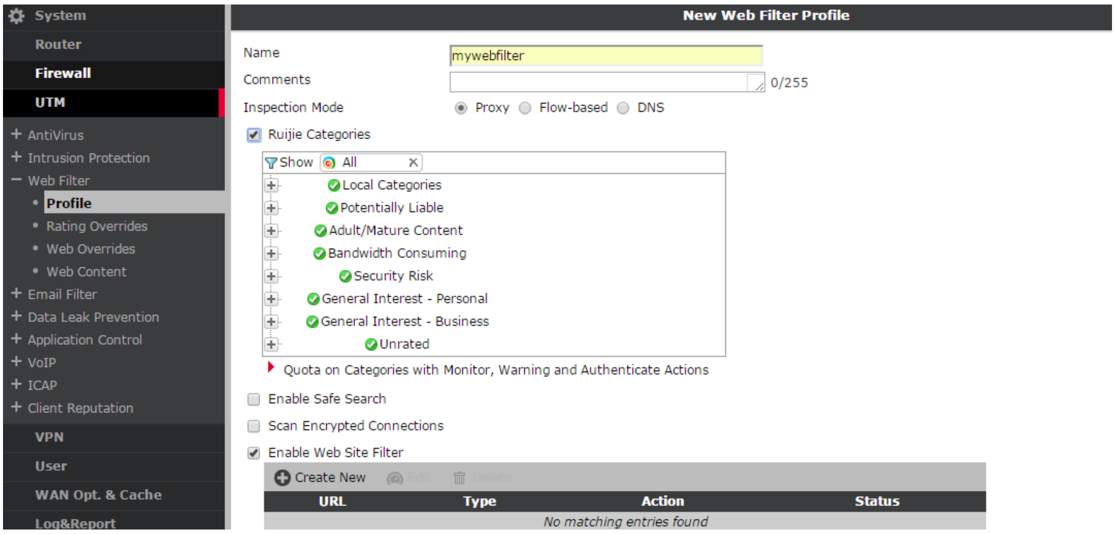


Name
default
flow-monitor-all
monitor-all
web-filter-flow

On the **New Web Filter Profile** page, fill in the following parameters:

Name: Enter the name: **mywebfilter**.

Inspection Mode: Choose **Flow-based**.



New Web Filter Profile

Name mywebfilter

Comments 0/255

Inspection Mode ● Proxy ○ Flow-based ○ DNS

☑ Ruijie Categories

Show All

- Local Categories
- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
- Security Risk
- General Interest - Personal
- General Interest - Business
- Unrated

Quota on Categories with Monitor, Warning and Authenticate Actions

□ Enable Safe Search

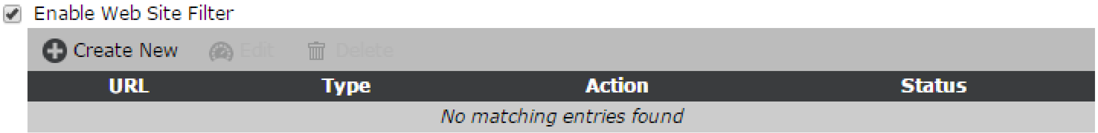
□ Scan Encrypted Connections

☑ Enable Web Site Filter

Create New Edit Delete

URL	Type	Action	Status
No matching entries found			

Choose Enable Web Site Filter.



☑ Enable Web Site Filter

Create New Edit Delete

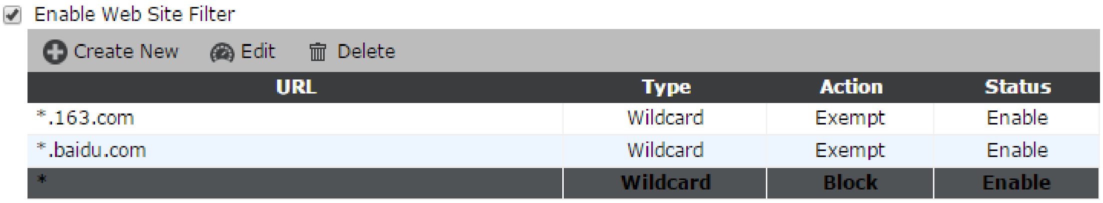
URL	Type	Action	Status
No matching entries found			

You can edit the URL filter or create new filters..

*.baidu.com: It indicates that all Baidu websites are allowed.

*.163.com: It indicates that all NetEase websites are allowed.

*: It indicates that other websites are rejected. The following figure shows the configuration after URLs are added:



☑ Enable Web Site Filter

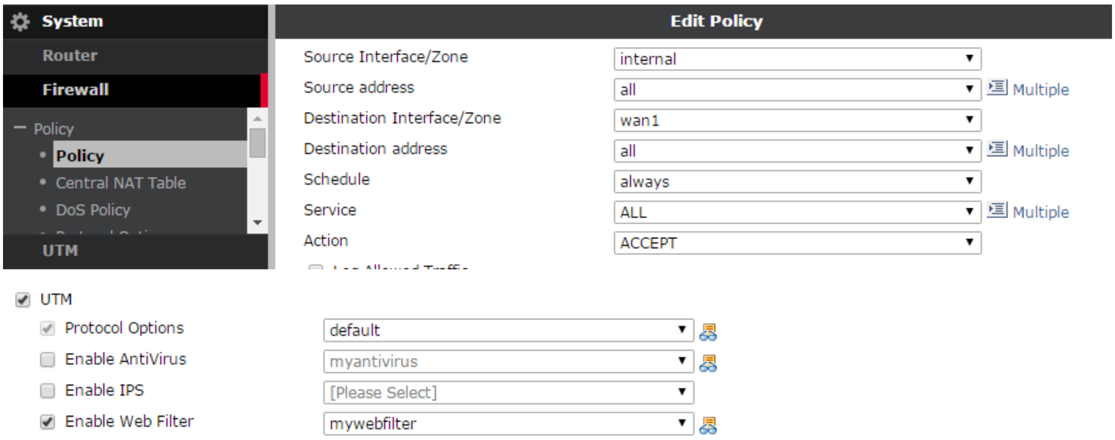
Create New Edit Delete

URL	Type	Action	Status
*.163.com	Wildcard	Exempt	Enable
*.baidu.com	Wildcard	Exempt	Enable
*	Wildcard	Block	Enable

The URL filters in this list are executed from top to bottom. To adjust the sequence, click the item, and then drag it.

3. Enable Web filter in the policy.

On the **Edit Policy** page, choose **UTM** and **Enable Web Filter**. Choose **mywebfilter** from **Enable Web Filter** drop-down list. See the following figure:



Edit Policy

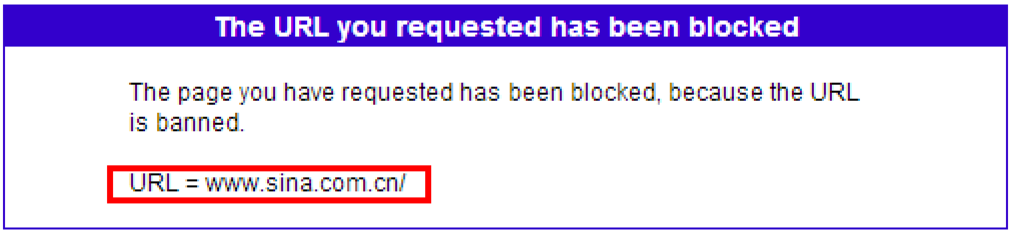
Source Interface/Zone	internal
Source address	all
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT

☑ UTM

☑ Protocol Options	default
□ Enable AntiVirus	myantivirus
□ Enable IPS	[Please Select]
☑ Enable Web Filter	mywebfilter

Verification

The URL of www.baidu.com can be accessed. The URL of www.sina.com.cn is blocked.

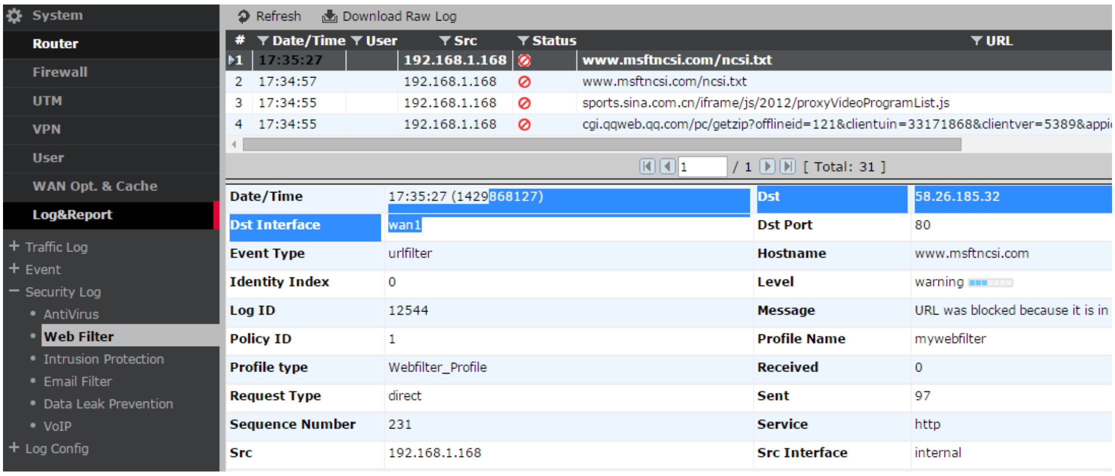


The URL you requested has been blocked

The page you have requested has been blocked, because the URL is banned.

URL = www.sina.com.cn/

The log is as follows:



#	Date/Time	User	Src	Status	URL
1	17:35:27		192.168.1.168	⊘	www.msftncsi.com/ncsi.txt
2	17:34:57		192.168.1.168	⊘	www.msftncsi.com/ncsi.txt
3	17:34:55		192.168.1.168	⊘	sports.sina.com.cn/iframe/js/2012/proxyVideoProgramList.js
4	17:34:55		192.168.1.168	⊘	cgi.qqweb.qq.com/pc/getzip?offlineid=121&clientuin=33171868&clientver=5389&appi

1 / 1 [Total: 31]

Date/Time	17:35:27 (1429868127)	Dst	58.26.185.32
Dst Interface	wan1	Dst Port	80
Event Type	urlfilter	Hostname	www.msftncsi.com
Identity Index	0	Level	warning
Log ID	12544	Message	URL was blocked because it is in
Policy ID	1	Profile Name	mywebfilter
Profile type	Webfilter_Profile	Received	0
Request Type	direct	Sent	97
Sequence Number	231	Service	http
Src	192.168.1.168	Src Interface	internal

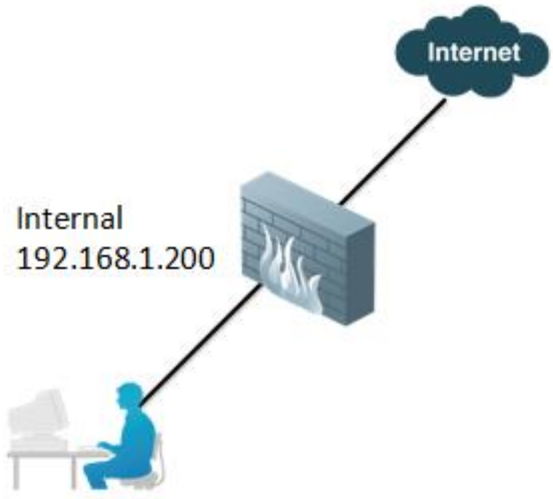
7.1.4 Mail Filter

7.1.4.1 Mail Filter

Networking Requirements

The emails received/transmitted by the intranet are filtered via a firewall, and the emails sent by @qq.com are marked as spam emails.

Network Topology



The intranet users access the Internet via a firewall.

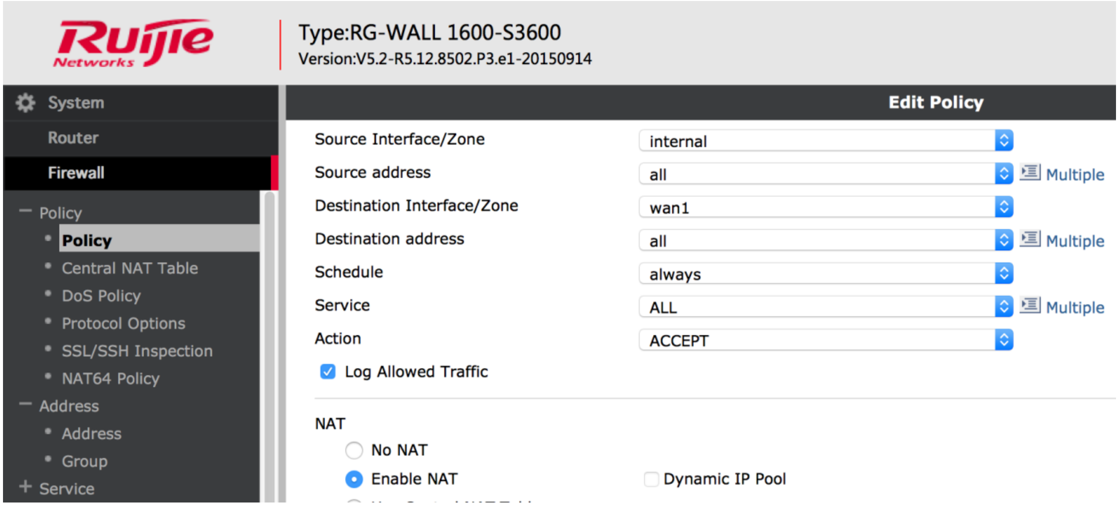
Configuration Tips

1. Initialize the configurations on Internet access
2. Define the anti-spam configurations
3. Configure the proxy options
4. Enable the Web filtering function in the policy

Configuration Steps

1) Initialize the configurations on Internet access

For details about the configuration procedure, refer to the section “Configuring Routing Mode” > “Internet Access via a Single Line” > “Configuring Internet Access via a Static Link”.



Source Interface/Zone: internal

Source address: all Multiple

Destination Interface/Zone: wan1

Destination address: all Multiple

Schedule: always

Service: ALL Multiple

Action: ACCEPT

☑ Log Allowed Traffic

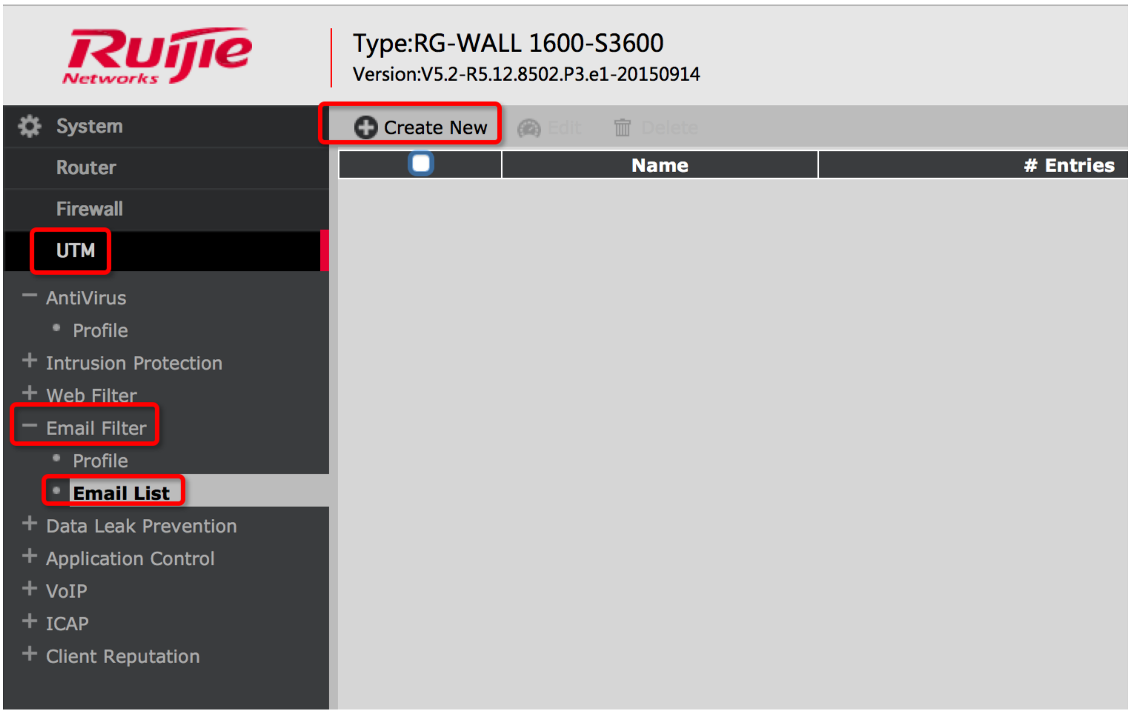
NAT

○ No NAT

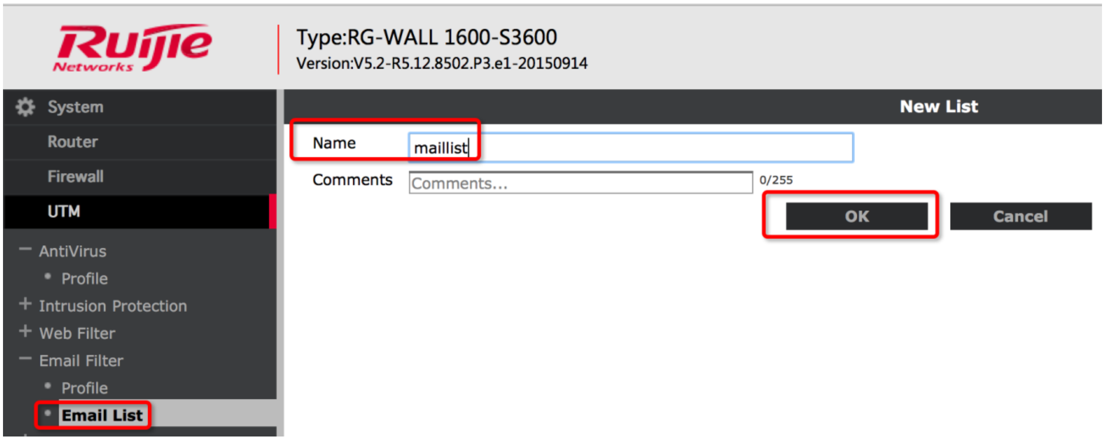
● Enable NAT □ Dynamic IP Pool

2) Define the anti-spam configurations

Choose the **UTM** > **Email Filter** > **Email List** menu.



Click **Create New**, and define the name as **maillist**.



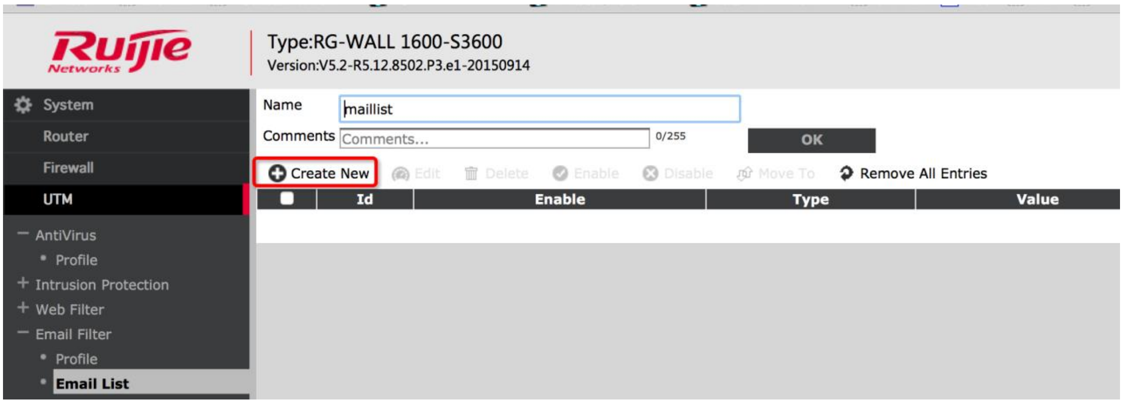
Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New List

Name: maillist

Comments: Comments... 0/255

Click **Create New** to create specific maillist entries:

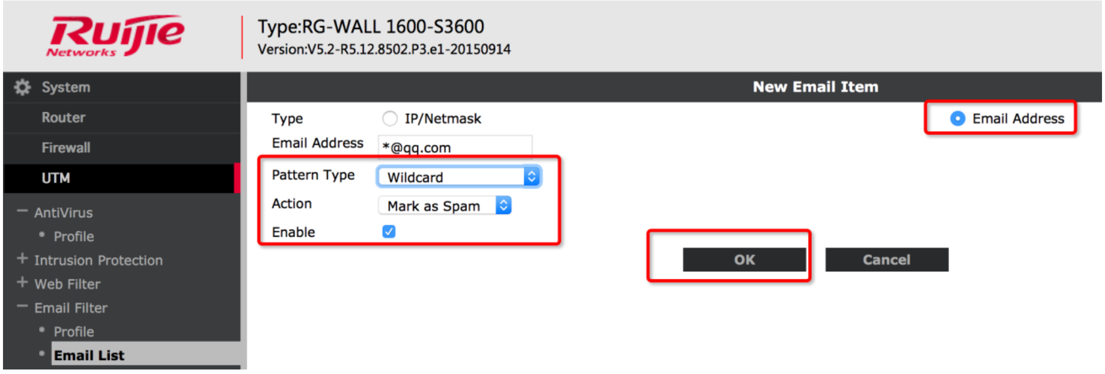


Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Name: maillist

Comments: Comments... 0/255

□	Id	Enable	Type	Value



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

New Email Item

Type: ○ IP/Netmask ● Email Address

Email Address: *@qq.com

Pattern Type: Wildcard

Action: Mark as Spam

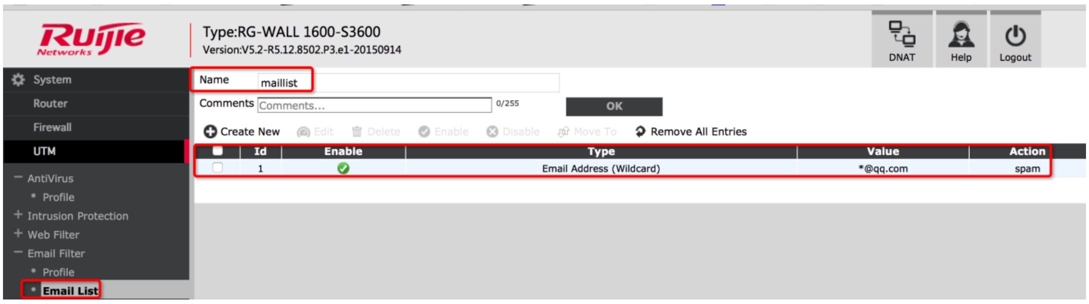
Enable: ☑

Type: Select **Email Address**.

Email Address: Enter ***@qq.com**.

Action: Select **Mark as Spam**.

Click **OK**. Then, the maillist is displayed as follows:

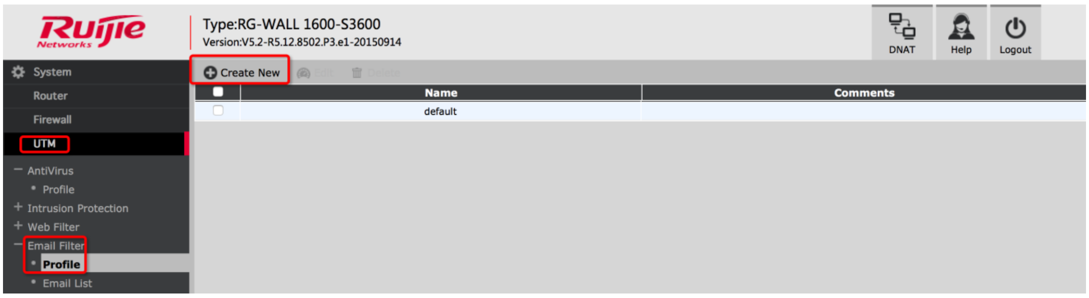


Name: maillist

Comments: Comments... 0/255

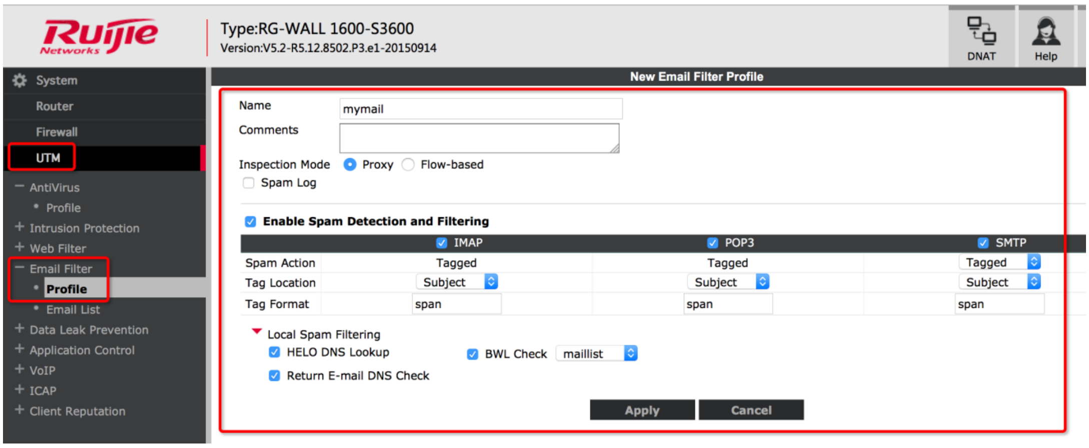
	Id	Enable	Type	Value	Action
□	1	✓	Email Address (Wildcard)	*@qq.com	spam

Choose the **UTM** > **Email Filter** > **Config** menu, and click **Create New**.



	Name	Comments
□	default	

You can directly edit the default configuration file. You can also create a new configuration file, for example:



Name: mymail

Comments:

Inspection Mode: ● Proxy ○ Flow-based

□ Spam Log

☑ Enable Spam Detection and Filtering

	☑ IMAP	☑ POP3	☑ SMTP
Spam Action	Tagged	Tagged	Tagged
Tag Location	Subject	Subject	Subject
Tag Format	span	span	span

Local Spam Filtering

☑ HELO DNS Lookup ☑ BWL Check maillist

☑ Return E-mail DNS Check

Name: Enter the name of the configuration file, here, **mymail**.

Comments: Add the descriptions of the script.

Inspection Mode: Select **Proxy**.

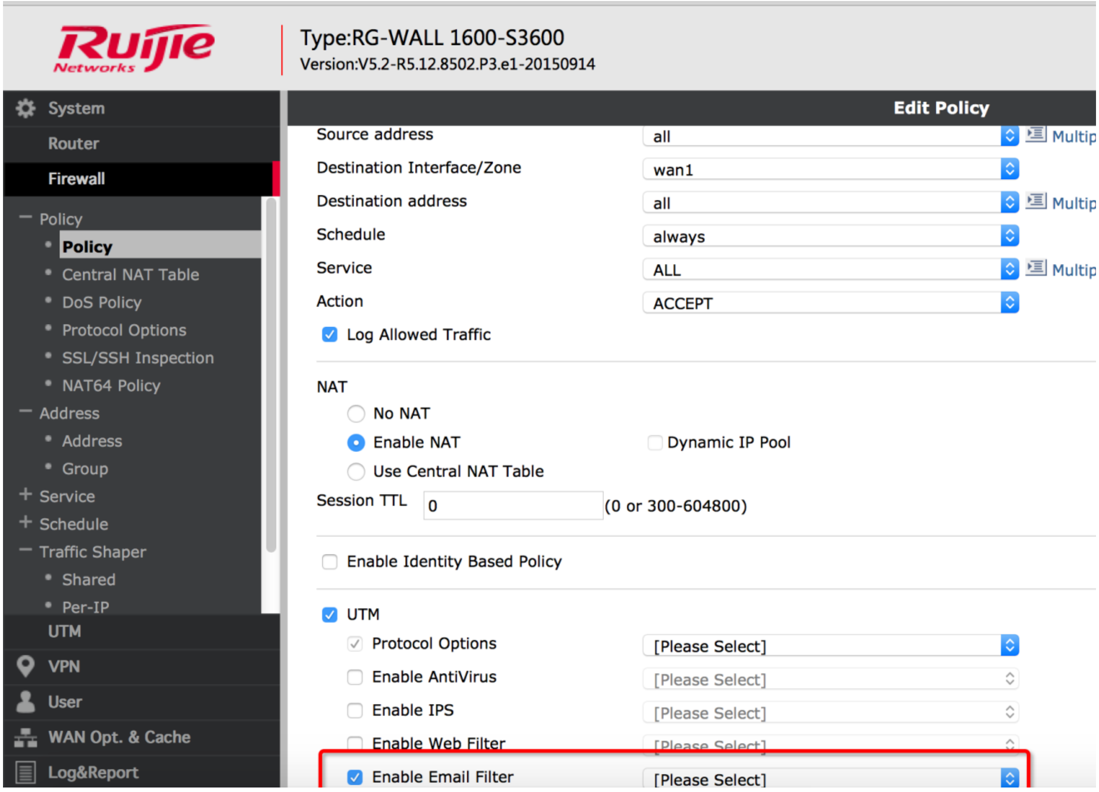
Enable Spam Detection and Filtering: Select **IAMP**, **POP3**, and **SMTP**.

Local Spam Filtering: Select HELO DNS Lookup and Remain E-mail DNS Check.

BWL Check: Select **maillist**. Use local blacklist and whitelist, which need to be manually configured as follows:

3) Enable the anti-spam function in the policy

In the firewall policy for Internet access, enable UTM and select **Enable Email Filter**.



Type:RG-WALL 1600-S3600
Version:V5.2-R5.12.8502.P3.e1-20150914

Edit Policy

Source address: all
Destination Interface/Zone: wan1
Destination address: all
Schedule: always
Service: ALL
Action: ACCEPT
☑ Log Allowed Traffic

NAT
○ No NAT
● Enable NAT   □ Dynamic IP Pool
○ Use Central NAT Table
Session TTL: 0 (0 or 300-604800)

□ Enable Identity Based Policy

☑ UTM
☑ Protocol Options: [Please Select]
□ Enable AntiVirus: [Please Select]
□ Enable IPS: [Please Select]
□ Enable Web Filter: [Please Select]
☑ Enable Email Filter: [Please Select]

4) Enable log display

If the log is not displayed, you can enable log display via a CLI.

Before performing the operations, it is recommended that you upgrade the current version to P2. If you perform the operations under the P1 version, you need to enter **print cliovrd enabl4e** and press **Enter**; after logging in and then logging out, execute the following command.

```
RG-WALL # config spamfilter profile
RG-WALL (profile) # edit mymail
RG-WALL (mymail) # set extended-utm-log enable
RG-WALL (mymail) # end
```

Verification

For each email originated from qq, the **spam** characters are inserted into its header, indicating that the email is a spam email.

For each email destined for qq, the **spam** characters are inserted into its header, indicating that the email is a spam email. Therefore, it is recommended that POP3 and SMTP are processed respectively.

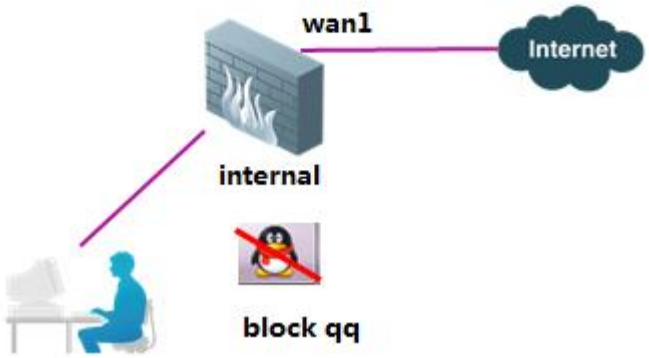
7.1.5 Network Application Control

7.1.5.1 Configuring Application Control

Networking Requirements

The employees in a company can access Internet. The company forbids employees to use instant messaging (IM) applications, or allows only the specified employees to use the IM applications.

Network Topology



Configuration Tips

1. Initialize Internet access configuration.
2. Configure application control sensors.
   - Block IM applications.
   - Configure flow control for P2P applications.
3. Enable application control in the policy.

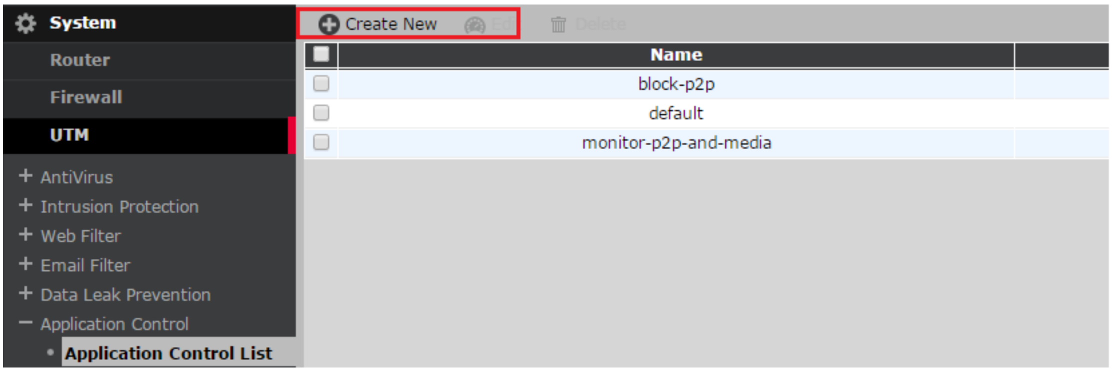
Configuration Steps

1. Initialize Internet access configuration.

For the detailed configuration process, see section “Configuring Internet Access via a Static Link under section “Internet Access via a Single Line” in “Configuring Routing Mode”.

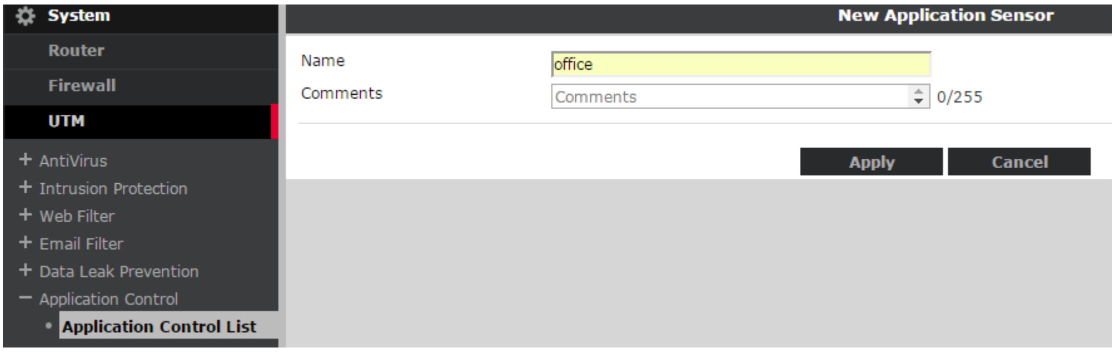
2. Define the application control sensor.

Choose **UTM** > **Application Control** > **Application Control List**. Click **Create New**, as shown in the following figure:



□	Name
□	block-p2p
□	default
□	monitor-p2p-and-media

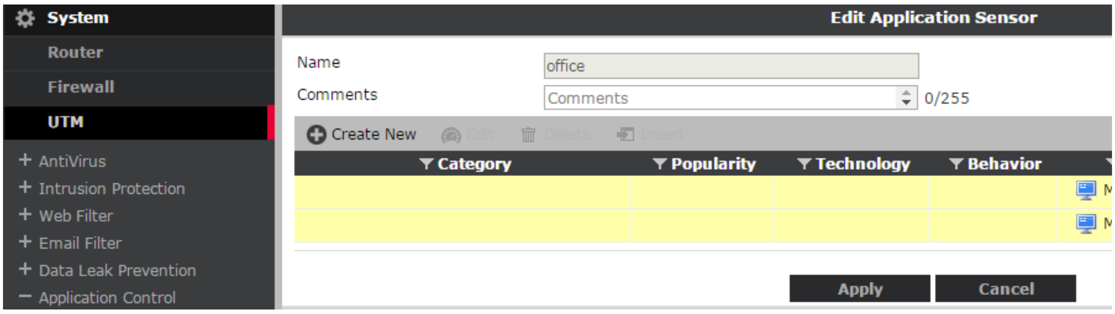
a) Create a sensor. Enter the name: **office**, then click **Apply**. See the following figure:



Name: office

Comments: Comments 0/255

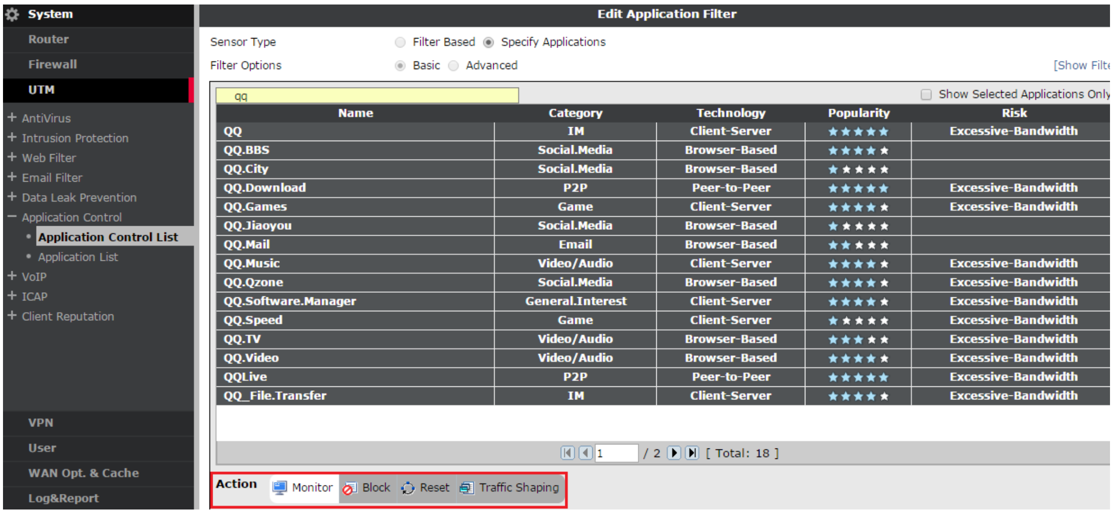
b) Choose the office sensor, then click **Create New**. Add the application control filter entry to the sensor, as shown in the following figure:



Name: office

Comments: Comments 0/255

c) Block QQ and related software, as shown in the following figure:



Sensor Type ○ Filter Based ● Specify Applications

Filter Options ● Basic ○ Advanced

qq

Name	Category	Technology	Popularity	Risk
QQ	IM	Client-Server	★★★★★	Excessive-Bandwidth
QQ.BBS	Social.Media	Browser-Based	★★★★★	
QQ.City	Social.Media	Browser-Based	★★★★★	
QQ.Download	P2P	Peer-to-Peer	★★★★★	Excessive-Bandwidth
QQ.Games	Game	Client-Server	★★★★★	Excessive-Bandwidth
QQ.Jiaoyou	Social.Media	Browser-Based	★★★★★	
QQ.Mail	Email	Browser-Based	★★★★★	
QQ.Music	Video/Audio	Client-Server	★★★★★	Excessive-Bandwidth
QQ.Qzone	Social.Media	Browser-Based	★★★★★	Excessive-Bandwidth
QQ.Software.Manager	General.Interest	Client-Server	★★★★★	Excessive-Bandwidth
QQ.Speed	Game	Client-Server	★★★★★	Excessive-Bandwidth
QQ.TV	Video/Audio	Browser-Based	★★★★★	Excessive-Bandwidth
QQ.Video	Video/Audio	Browser-Based	★★★★★	Excessive-Bandwidth
QQLive	P2P	Peer-to-Peer	★★★★★	Excessive-Bandwidth
QQ_File.Transfer	IM	Client-Server	★★★★★	Excessive-Bandwidth

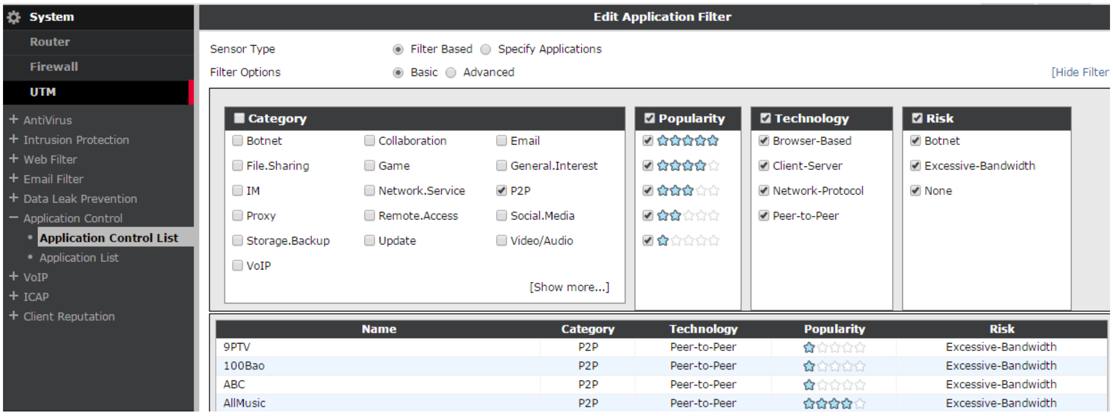
1 / 2 [Total: 18]

Sensor Type: Choose **Specify Applications**. Then enter qq.

The all the QQ-related applications are displayed. Click the target application.

Action: Click **Block**.

d) Configure flow control for P2P applications, as shown in the following figure:



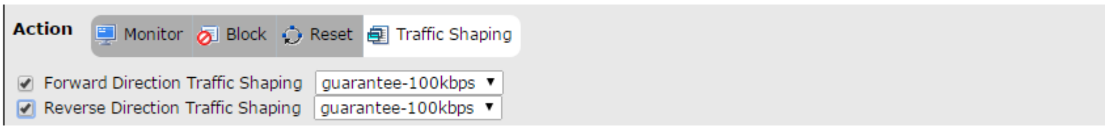
Edit Application Filter

Sensor Type ● Filter Based ○ Specify Applications

Filter Options ● Basic ○ Advanced

□ Category			☑ Popularity	☑ Technology	☑ Risk
□ Botnet	□ Collaboration	□ Email	☑ ★★★★★	☑ Browser-Based	☑ Botnet
□ File.Sharing	□ Game	□ General.Interest	☑ ★★★★☆	☑ Client-Server	☑ Excessive-Bandwidth
□ IM	□ Network.Service	☑ P2P	☑ ★★★☆☆	☑ Network-Protocol	☑ None
□ Proxy	□ Remote.Access	□ Social.Media	☑ ★★☆☆☆	☑ Peer-to-Peer	
□ Storage.Backup	□ Update	□ Video/Audio	☑ ★☆☆☆☆		
□ VoIP					

Name	Category	Technology	Popularity	Risk
9PTV	P2P	Peer-to-Peer	★☆☆☆☆	Excessive-Bandwidth
100Bao	P2P	Peer-to-Peer	★☆☆☆☆	Excessive-Bandwidth
ABC	P2P	Peer-to-Peer	★☆☆☆☆	Excessive-Bandwidth
AllMusic	P2P	Peer-to-Peer	★★★★☆	Excessive-Bandwidth



Action: Traffic Shaping

☑ Forward Direction Traffic Shaping guarantee-100kbps

☑ Reverse Direction Traffic Shaping guarantee-100kbps

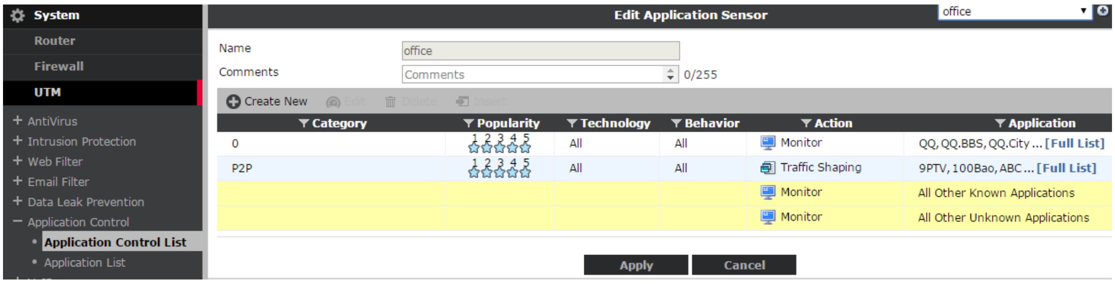
Sensor Type: Choose **Filter Based**.

Category: Choose **P2P**.

Action: Click **Traffic Shaping**.

Forward Direction Traffic Shaping: Set it to 1M.

e) The application control sensor configuration is as follows:



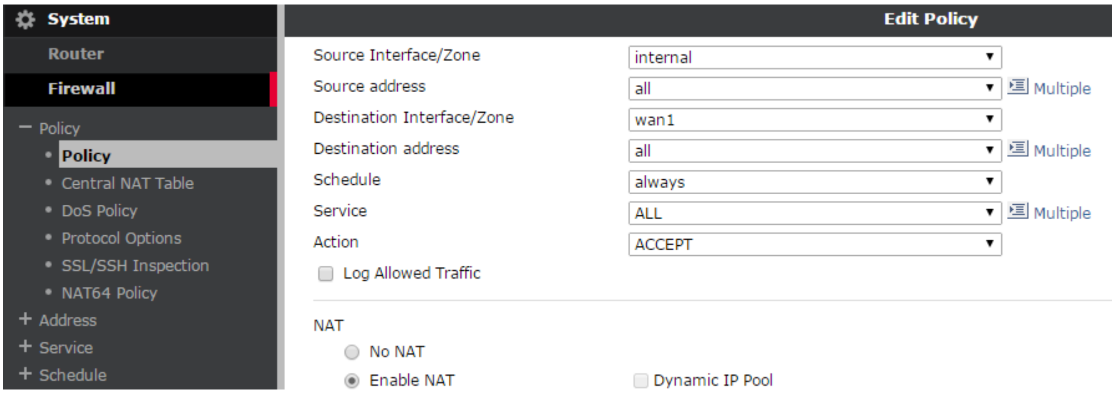
Edit Application Sensor

Name: office

Comments: Comments 0/255

Category	Popularity	Technology	Behavior	Action	Application
0	1 2 3 4 5	All	All	Monitor	QQ, QQ.BBS, QQ.City ... [Full List]
P2P	1 2 3 4 5	All	All	Traffic Shaping	9PTV, 100Bao, ABC ... [Full List]
				Monitor	All Other Known Applications
				Monitor	All Other Unknown Applications

3. Enable application control in the policy.



Edit Policy

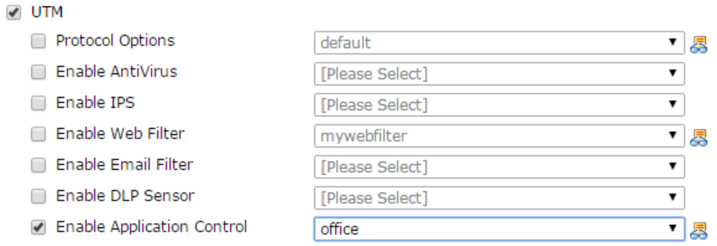
Source Interface/Zone	internal
Source address	all
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool



☑ UTM

□ Protocol Options	default
□ Enable AntiVirus	[Please Select]
□ Enable IPS	[Please Select]
□ Enable Web Filter	mywebfilter
□ Enable Email Filter	[Please Select]
□ Enable DLP Sensor	[Please Select]
☑ Enable Application Control	office

Choose **Enable Application Control**, and select office from Enable **Application Control** drop-down list.

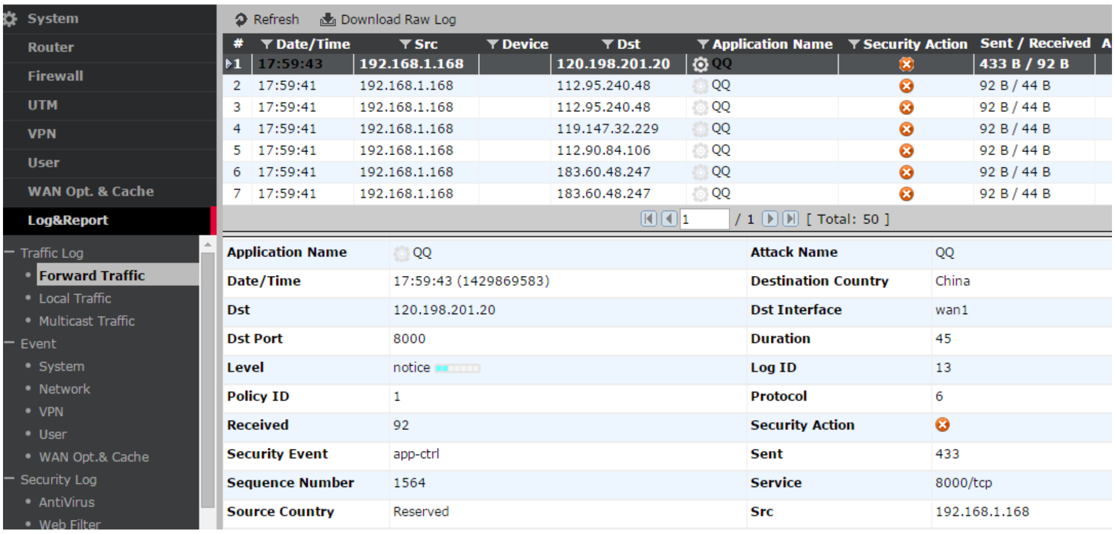
4. Enable log display.

If logs are not displayed, run a command to enable log display.

```
RG-WALL # config application list
RG-WALL (list) # edit office
new entry 'office' added
RG-WALL (office) # set extended-utm-log  enable
RG-WALL (office) # end
```

Verification

Use an application for testing.



#	Date/Time	Src	Device	Dst	Application Name	Security Action	Sent / Received	A
1	17:59:43	192.168.1.168		120.198.201.20	QQ	⊗	433 B / 92 B	
2	17:59:41	192.168.1.168		112.95.240.48	QQ	⊗	92 B / 44 B	
3	17:59:41	192.168.1.168		112.95.240.48	QQ	⊗	92 B / 44 B	
4	17:59:41	192.168.1.168		119.147.32.229	QQ	⊗	92 B / 44 B	
5	17:59:41	192.168.1.168		112.90.84.106	QQ	⊗	92 B / 44 B	
6	17:59:41	192.168.1.168		183.60.48.247	QQ	⊗	92 B / 44 B	
7	17:59:41	192.168.1.168		183.60.48.247	QQ	⊗	92 B / 44 B	

1 / 1 [Total: 50]

Application Name	QQ	**Attack Name**	QQ
Date/Time	17:59:43 (1429869583)	**Destination Country**	China
Dst	120.198.201.20	**Dst Interface**	wan1
Dst Port	8000	**Duration**	45
Level	notice	**Log ID**	13
Policy ID	1	**Protocol**	6
Received	92	**Security Action**	⊗
Security Event	app-ctrl	**Sent**	433
Sequence Number	1564	**Service**	8000/tcp
Source Country	Reserved	**Src**	192.168.1.168

7.1.5.2 Traffic Rate Limit

Networking Requirements

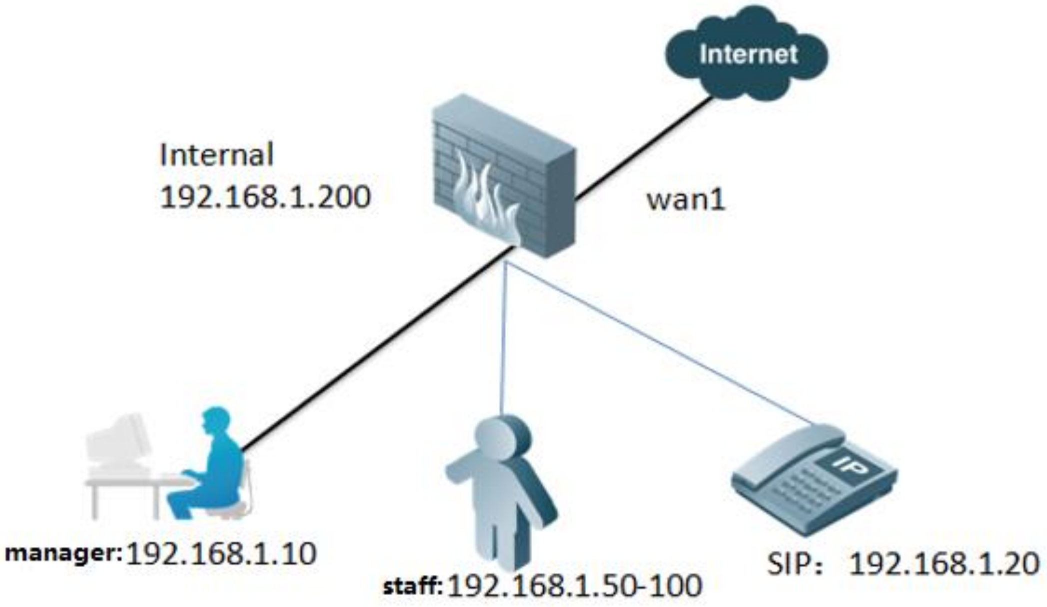
A company performs traffic management over intranet users. The egress bandwidth is restricted to 20 Mbps.

Manager: Traffic for 192.168.1.10 is not restricted.

Staff: The total bandwidth for 192.168.1.50-100 is restricted to 15 Mbps. Traffic of each employee cannot exceed 1 Mbps.

IP phone and video: The bandwidth for 192.168.1.20 is 3 Mbps to guarantee smooth video playing.

Network Topology



Configuration Tips

1) Basic configuration of the interfaces and routes for Internet access.

2) Define the address object according to the IP address segments to be restricted.

3) Define the traffic shaper.

4) Configure the policy and enable flow control.

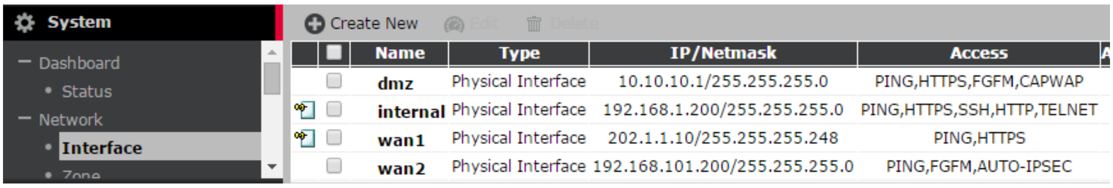
To control upload and download traffic, enable reverse flow control. **Reverse flow control** refers to control the flow in the downloading direction. After reverse flow control is enable, upload and download traffic is separately controlled.

Configuration Steps

1. **Basic configuration of the interfaces and routes for Internet access.**

For the detailed configuration process, see section “Configuring Internet Access via a Static Link” section under “Internet Access via a Single Line” in “Configuring Routing Mode”.

IP address configuration of the interfaces is as shown in the following figure:



Name	Type	IP/Netmask	Access
dmz	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,FGFM,CAPWAP
internal	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS,SSH,HTTP,TELNET
wan1	Physical Interface	202.1.1.10/255.255.255.248	PING,HTTPS
wan2	Physical Interface	192.168.101.200/255.255.255.0	PING,FGFM,AUTO-IPSEC

2. **Define the address object according to the IP address segments to be restricted.**

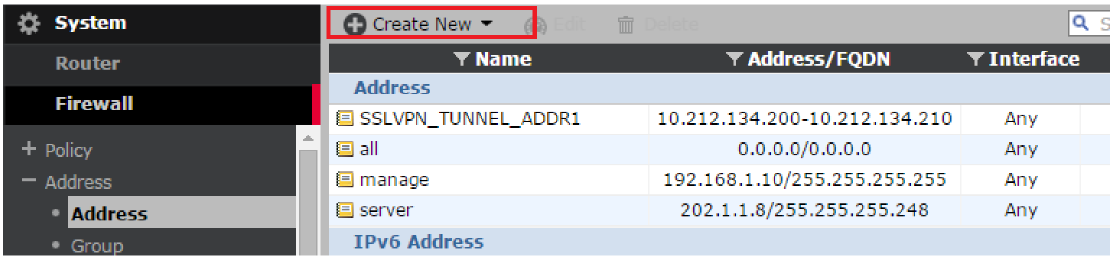
Define three address objects:

manager: 192.168.1.10

sip: 192.168.1.20

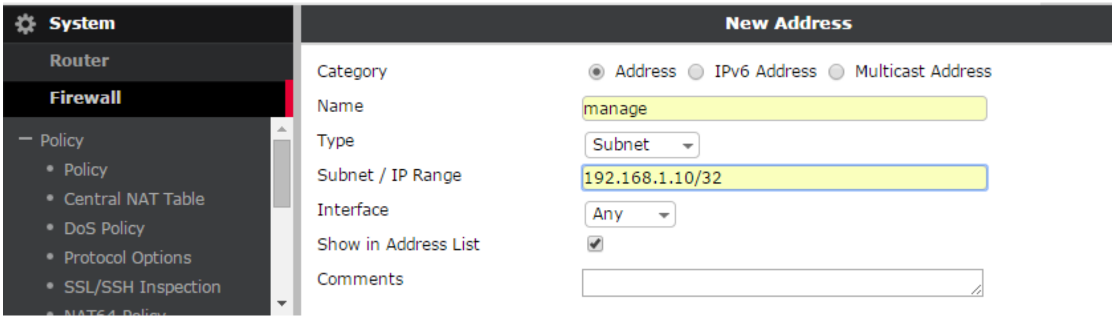
staff:192.168.1.50-100

Choose **Firewall** > **Address** > **Address**, and then click **Create New**, as shown in the following figure:



Name	Address/FQDN	Interface
Address		
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any
all	0.0.0.0/0.0.0.0	Any
manage	192.168.1.10/255.255.255.255	Any
server	202.1.1.8/255.255.255.248	Any
IPv6 Address		

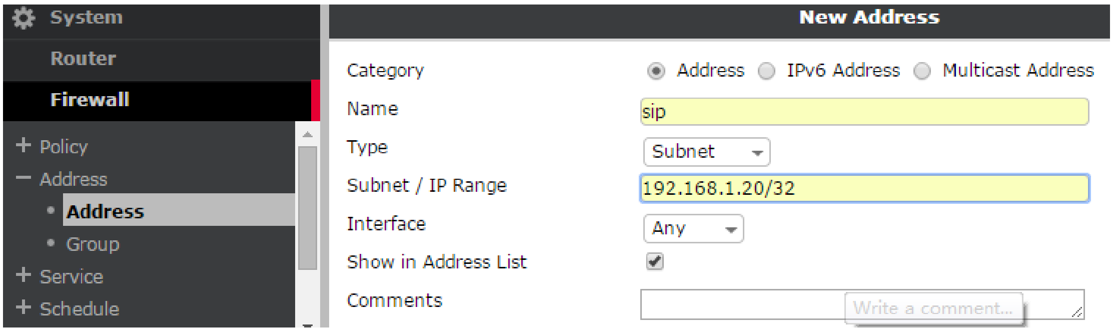
1) Define the IP address of the leader’s PC. Set **Name** to **manage** and set **Subnet/IP Range** to **192.168.1.10**, as shown in the following figure:



New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	manage
Type	Subnet
Subnet / IP Range	192.168.1.10/32
Interface	Any
Show in Address List	☑
Comments	

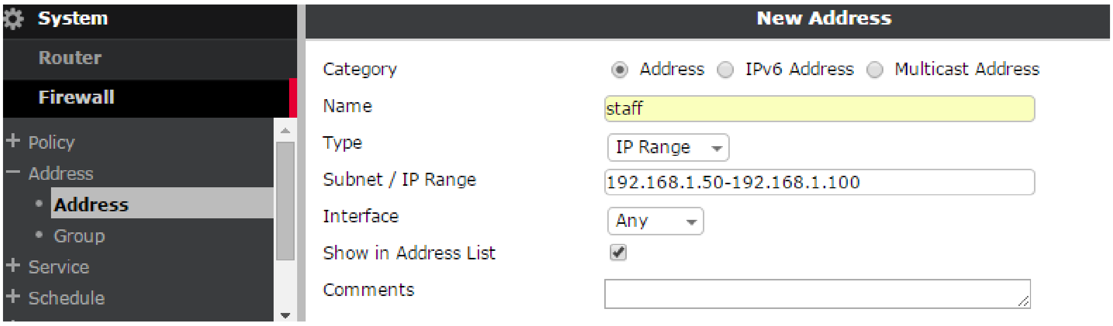
2) Define the IP address of SIP. Set **Name** to **sip** and set **Subnet/IP Range** to **192.168.1.20**, as shown in the following figure:



New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	sip
Type	Subnet
Subnet / IP Range	192.168.1.20/32
Interface	Any
Show in Address List	☑
Comments	Write a comment...

3) Define the IP address of the staff's PC. Set **Name** to **staff** and set **Subnet/IP Range** to **192.168.1.50-100** as shown in the following figure:

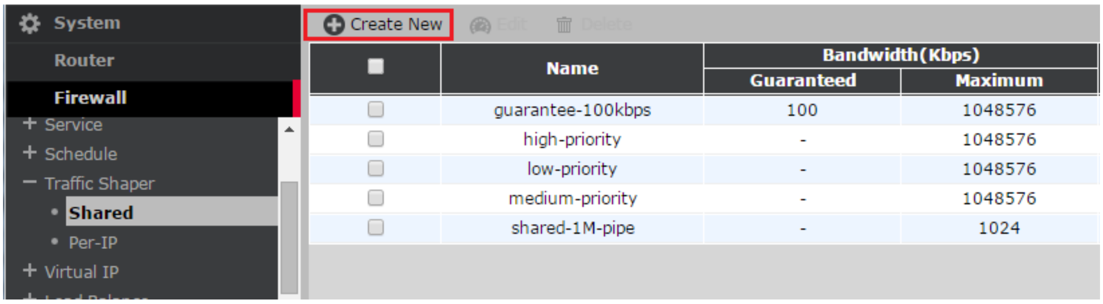


New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	staff
Type	IP Range
Subnet / IP Range	192.168.1.50-192.168.1.100
Interface	Any
Show in Address List	☑
Comments	

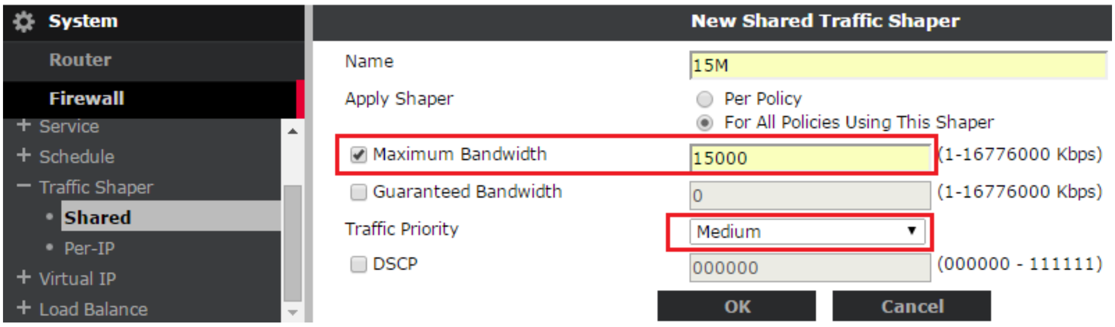
3. Define the traffic shaper.

Choose **Firewall** > **Traffic Shaper** > **Shared**, and then click **Create New**, as shown in the following figure:



□	Name	Bandwidth(Kbps)	
		Guaranteed	Maximum
□	guarantee-100kbps	100	1048576
□	high-priority	-	1048576
□	low-priority	-	1048576
□	medium-priority	-	1048576
□	shared-1M-pipe	-	1024

a) Create a 15 Mbps shared traffic shaper, as shown in the following figure:



New Shared Traffic Shaper

Name	15M	
Apply Shaper	○ Per Policy ● For All Policies Using This Shaper	
☑ Maximum Bandwidth	15000	(1-16776000 Kbps)
□ Guaranteed Bandwidth	0	(1-16776000 Kbps)
Traffic Priority	Medium	
□ DSCP	000000	(000000 - 111111)

Name: Configure the shaper name.

Apply Shaper: Set how the flow control script is applied by the policy.

Per Policy: Each policy that uses the traffic shaper to control flow independently. For example, if 10 policies use the 15Mbps flow control script, each policy can use 15 Mbps bandwidth.

For All Policies Using This Shaper: All the policies that use this script control flows together. For example, if 10 policies use the 15 Mbps flow control script, all the users of the policy share 15 Mbps bandwidth.

That is, the maximum traffic used by the 10 policies is 15 Mbps.

Traffic Priority: The firewall interface defines 6 FIFO queues, among which queue 0 has the highest priority, while queue 5 has the lowest priority. Queue 0 is used for firewall management and VPN negotiation. All the traffic sent or received by the firewall is automatically put into queue 0 and forwarded first.

For the traffic enabled with the traffic shaper in the policy and forwarded by the firewall, its priority is classified into high, medium, and low levels. The traffic with high level is forwarded by the firewall first. High, medium, and low priority levels are corresponding to queues 1, 2, and 3:

High (queue 1), medium (queue 2), low (queue 3).

Traffic priorities can be classified according to service type. Set priorities of services such as VoIP to high priority. Set priorities of HTTP, POP3, SNTP, and OA services to medium priority. Set priorities of other services to low priority.

If the priority level is not specified in the policy, by default, the priority is high.

Maximum Bandwidth: It indicates the maximum bandwidth that is allowed by the policy, and the unit is Kbps. When the traffic exceeds the threshold, the data packets that exceed traffic will be discarded. Setting this value to **0** indicates that the maximum bandwidth is not restricted.

Guaranteed Bandwidth: It indicates the bandwidth guaranteed by the policy. When the traffic is lower than the guaranteed bandwidth, data packets will be put into queue 0. That is, data packets will be forwarded first, thus ensuring that the service occupies the lowest bandwidth. Setting the parameter for non-critical business is not recommended.

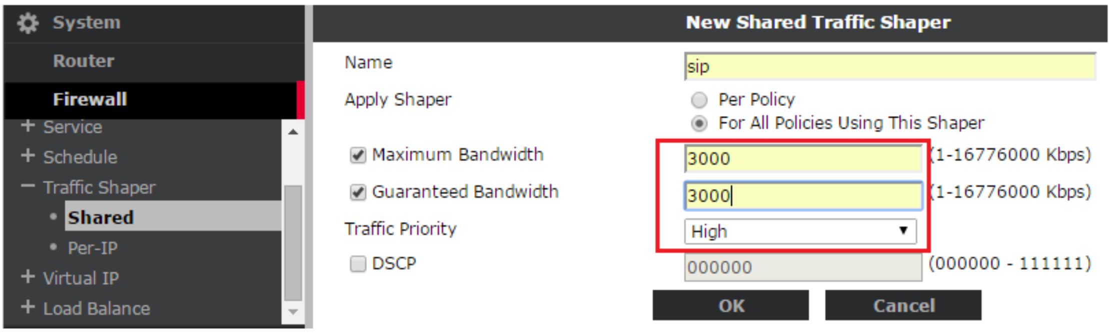
When the policy bandwidth is between the maximum bandwidth and guaranteed bandwidth, data packets are forwarded according to the priority defined in the policy.

DSCP: It determines whether to use differentiated services code point (DSCP) , which is used to configure point-to-point QoS services on the entire network.

b) Create a 3Mbps traffic shaper for voice and video.

c) Create a 1 Mbps per-IP traffic shaper.

Choose **Firewall** > **Traffic Shaper** > **Per-IP**, as shown in the following figure:



New Shared Traffic Shaper

Name: sip

Apply Shaper: ○ Per Policy ● For All Policies Using This Shaper

☑ Maximum Bandwidth: 3000 (1-16776000 Kbps)

☑ Guaranteed Bandwidth: 3000 (1-16776000 Kbps)

Traffic Priority: High

□ DSCP: 000000 (000000 - 111111)

Name: configure the traffic shaper.

Maximum Bandwidth: It indicates the maximum bandwidth used by each IP address. It is the sum of the upstream and downstream traffic. Set it to **1000 Kbps**.

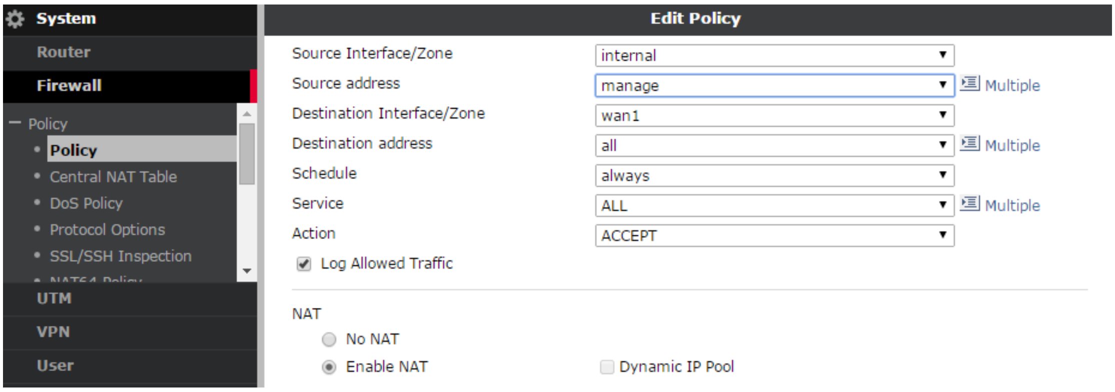
Maximum Concurrent Connections: The maximum number of connections that can be initiated by each user in the policy. If the maximum number of connections is exceeded, users cannot create a new connection. Set this option as required.

Forward DSCP: It determines whether to use DSCP, which is used to configure point-to-point QoS services on the entire network.

Reverse DSCP: It determines whether to use DSCP, which is used to configure point-to-point QoS services on the entire network.

4. **Configure the policy and enable traffic control.**

   a) Add the policy for leaders to access the Internet without any restriction, as shown in the following figure:



Edit Policy

Source Interface/Zone: internal

Source address: manage

Destination Interface/Zone: wan1

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

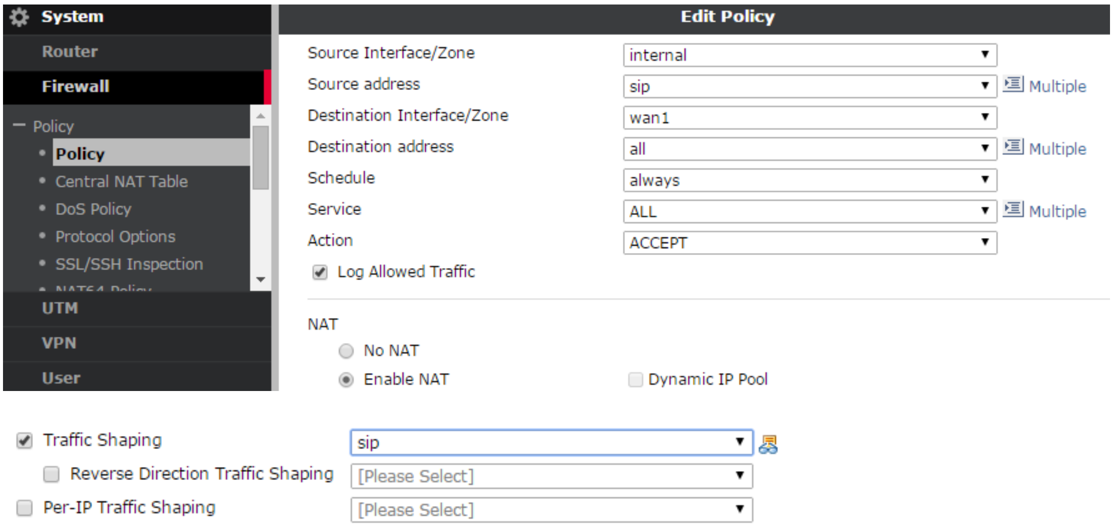
☑ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT □ Dynamic IP Pool

   b) Add the policy for SIP to use the traffic shaping policy, as shown in the following figure:



Edit Policy

Source Interface/Zone: internal

Source address: sip

Destination Interface/Zone: wan1

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

☑ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT

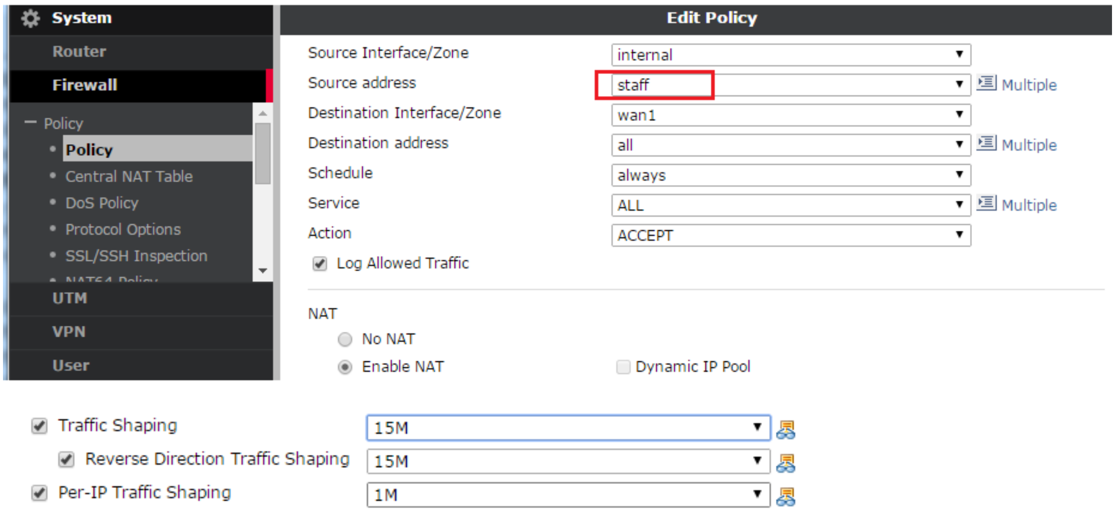
□ Dynamic IP Pool

☑ Traffic Shaping: sip

□ Reverse Direction Traffic Shaping: [Please Select]

□ Per-IP Traffic Shaping: [Please Select]

c) Add the policy for the staffs to access the Internet, as shown in the following figure:



Edit Policy

Source Interface/Zone: internal

Source address: staff

Destination Interface/Zone: wan1

Destination address: all

Schedule: always

Service: ALL

Action: ACCEPT

☑ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT

□ Dynamic IP Pool

☑ Traffic Shaping: 15M

☑ Reverse Direction Traffic Shaping: 15M

☑ Per-IP Traffic Shaping: 1M

Reverse Direction Traffic Shaping: This option is used to control the download traffic. After you enable it, the upload and download traffic is separately controlled. The upload and download rates are respectively 15 Mbps. If you do not choose this option, the sum of upload and download rates is 15 Mbps.

Verification

Use the FTP tool for downloading to observe rate.

If you choose **Per-IP Traffic Shaping**, the sessions that exceed the limit are blocked and you cannot accessing the Internet.

FAQs

Ask: Because per-IP does not respectively restrict upload and download rates, is there any problem during actual application?

Answer: Generally, there is no problem. In the preceding example, upload and download rates are not restricted separately.

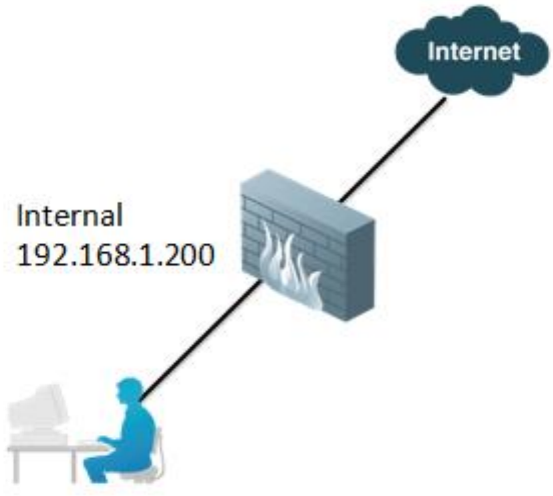
7.1.6 Data Leakage Prevention (DLP)

7.1.6.1 File Blocking - Non-Blocking List

I. Networking Requirements

The system needs to directly transmit executable files, and filter executable files from Web pages and emails.

II. Network Topology



Intranet users access the Internet through the firewall.

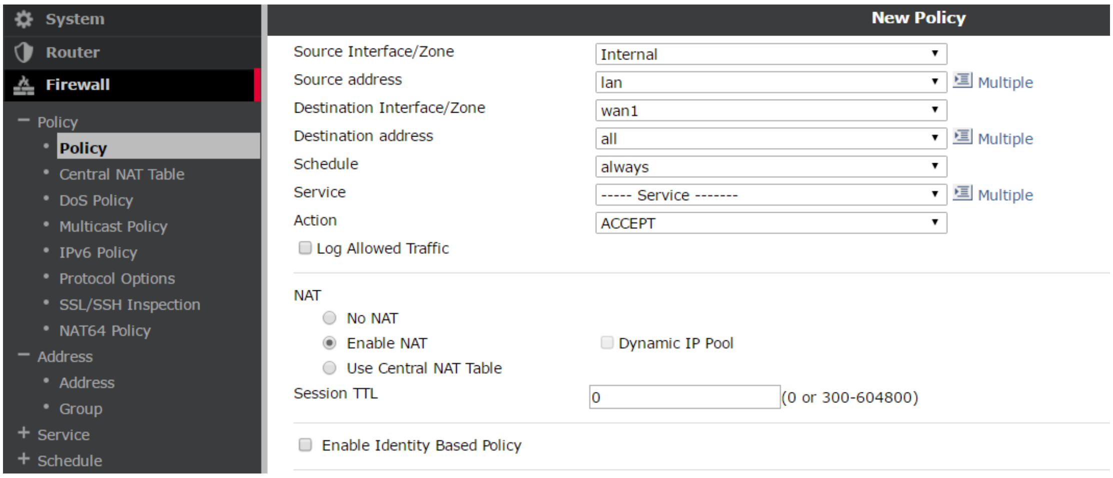
III. Configuration Tips

1. Initialize Internet access configuration.
2. Define DLP configuration.
3. Configure the proxy options.
4. Enable the DLP sensor in the policy.

IV. Configuration Steps

1. Initialize Internet access configuration.

Configure an access policy from **Internal** to **wan1**, set **Destination address** to **all**, and tick **Enable NAT**.



New Policy

Source Interface/Zone	Internal
Source address	lan
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	----- Service -------
Action	ACCEPT

□ Log Allowed Traffic

NAT
○ No NAT
● Enable NAT □ Dynamic IP Pool
○ Use Central NAT Table

Session TTL 0 (0 or 300-604800)

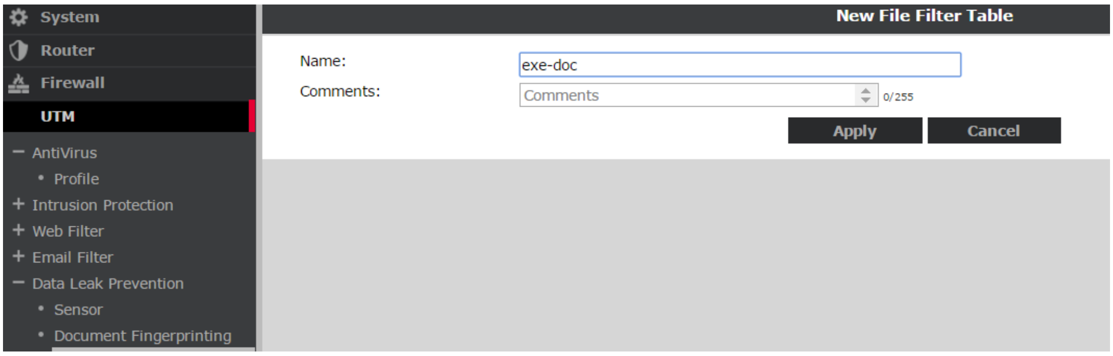
□ Enable Identity Based Policy

Define configuration for DLP sensor.

(1) File filter

a. A file filter is used to define the type of filtered files. Directly use the built-in all_executables file filter or define a new one.

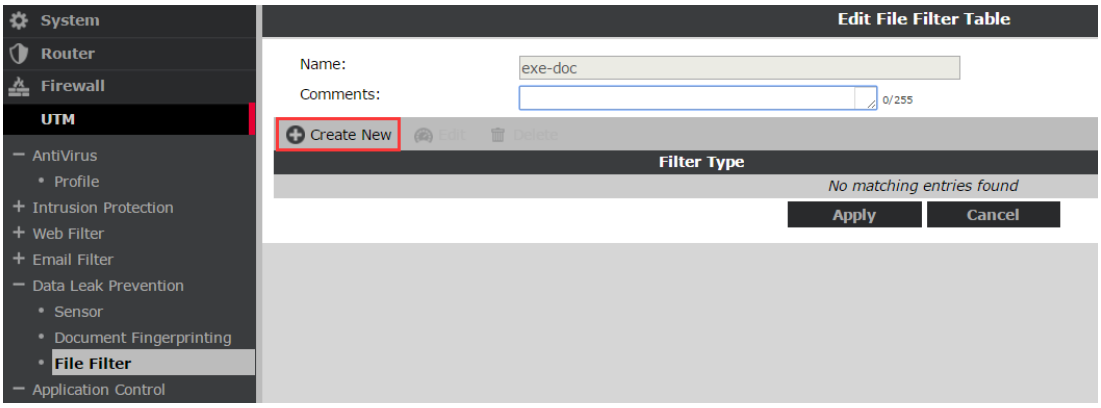
Choose **UTM** > **Data Leakage Prevention** > **File Filter**, and then click **Create New**.



New File Filter Table

Name: exe-doc
Comments: Comments 0/255

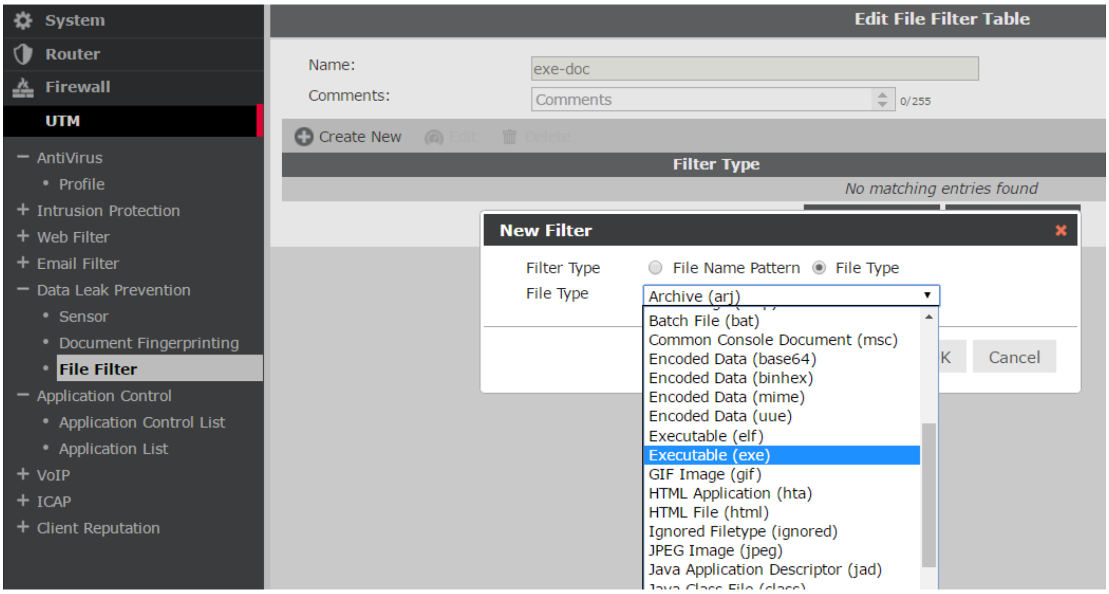
b. Create file types for the file filter table. Click **Create New**.



Edit File Filter Table

Name: exe-doc
Comments: 0/255

Filter Type
No matching entries found



Edit File Filter Table

Name: exe-doc

Comments: Comments 0/255

Filter Type
No matching entries found

New Filter

Filter Type ○ File Name Pattern ● File Type

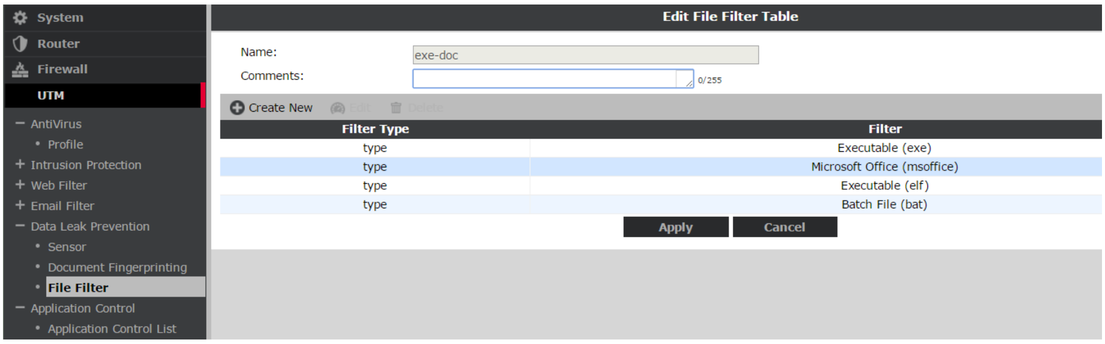
File Type: Archive (arj)

Batch File (bat)
Common Console Document (msc)
Encoded Data (base64)
Encoded Data (binhex)
Encoded Data (mime)
Encoded Data (uue)
Executable (elf)
Executable (exe)
GIF Image (gif)
HTML Application (hta)
HTML File (html)
Ignored Filetype (ignored)
JPEG Image (jpeg)
Java Application Descriptor (jad)
Java Class File (class)

Filter Type: Choose **File Type**.

File Type: Choose **Executable (exe)**.

c. Create all file types in the above way. The result is displayed as follows:



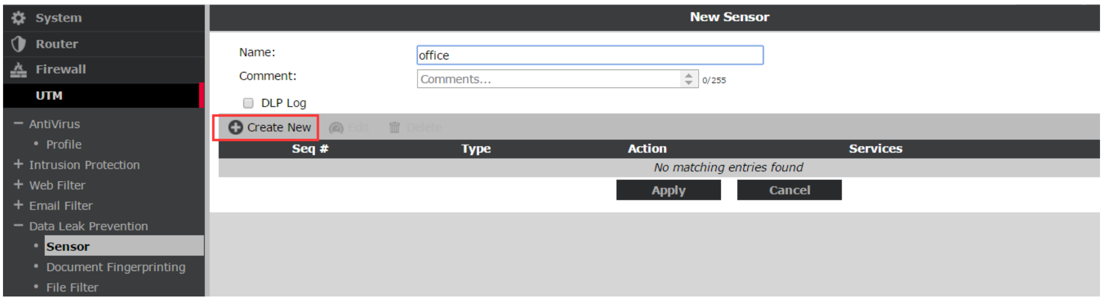
Edit File Filter Table

Name: exe-doc

Comments: 0/255

Filter Type	Filter
type	Executable (exe)
type	Microsoft Office (msoffice)
type	Executable (elf)
type	Batch File (bat)

(2) Choose UTM > Data Leakage Prevention > Sensor, and then click Create New.



New Sensor

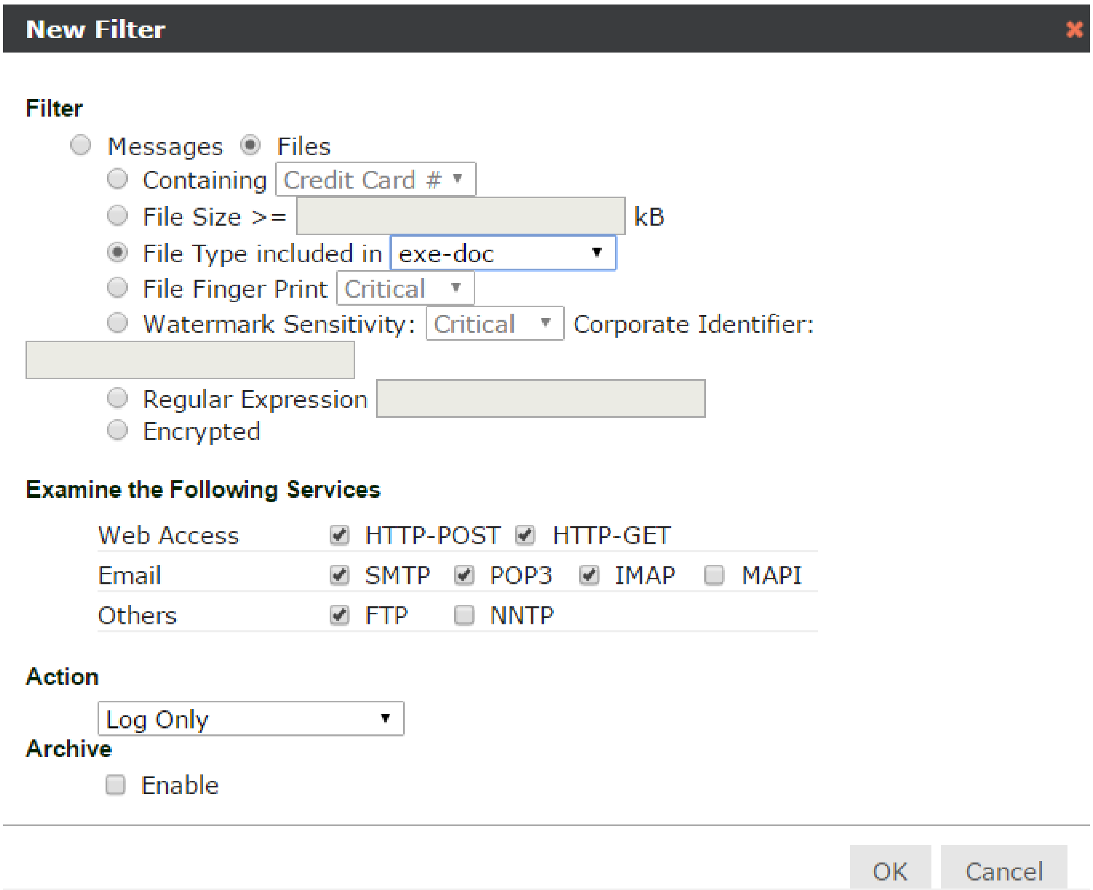
Name: office

Comment: Comments... 0/255

□ DLP Log

Seq #	Type	Action	Services
No matching entries found			

Enter the name **office**, and then click **Create New** to create the file filter.



New Filter

Filter

○ Messages ● Files

○ Containing Credit Card #

○ File Size >= kB

● File Type included in exe-doc

○ File Finger Print Critical

○ Watermark Sensitivity: Critical Corporate Identifier:

○ Regular Expression

○ Encrypted

Examine the Following Services

Web Access	☑ HTTP-POST	☑ HTTP-GET		
Email	☑ SMTP	☑ POP3	☑ IMAP	□ MAPI
Others	☑ FTP	□ NNTP		

Action

Log Only

Archive

□ Enable

Filter: Tick **Files**.

File Type included in: Choose **exe-doc**.

Examine the Following Services: It indicates files to be filtered.

Action: Choose **Log Only** to isolate this IP address and the source interface (use it with caution because it may lead to communication failure on the interface).

Configure the proxy options. (Optional)

Generally, retain the default proxy options and some advanced parameters. For modification, see the section "Anti-Virus".

Protocol Port Mapping:

Enable, Protocol, Inspection Port(s): Configure the proxy options of different protocols, for example, enable scanning on HTTP port 80. To scan multiple ports, ports should be separated with space, for example, 80 80 80 .

Common Options (Taking effect only for proxy inspection mode)

Comfort Clients: When viruses are scanned in proxy mode, files should be buffered in the firewall. After the files are scanned and ensured safe, the system sends them to users. In this process, users do not receive any data files. If the file size is large, users need to wait for a longer time. To refine such poor user experience, the firewall is enabled to send files at a slow speed during scanning, while users are informed that the file requests have been responded and handled.

Interval (seconds): Set it to 10. It indicates that data is sent once every 10 seconds.

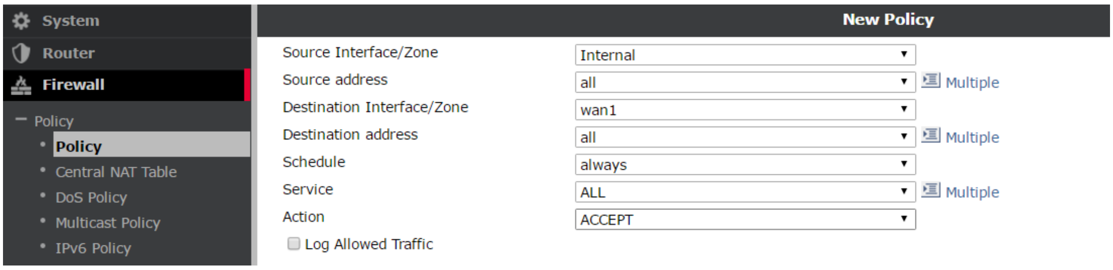
Amount (bytes): Set it to 1. It indicates the number of bytes sent every time.

Block Oversized File/Email: It indicates that the file exceeding the virus scanning buffer size (10 MB) is blocked. If **Block Oversized File/Email** is not chosen, the oversized file is permitted without virus scanning.

Click **OK** to validate the configuration.

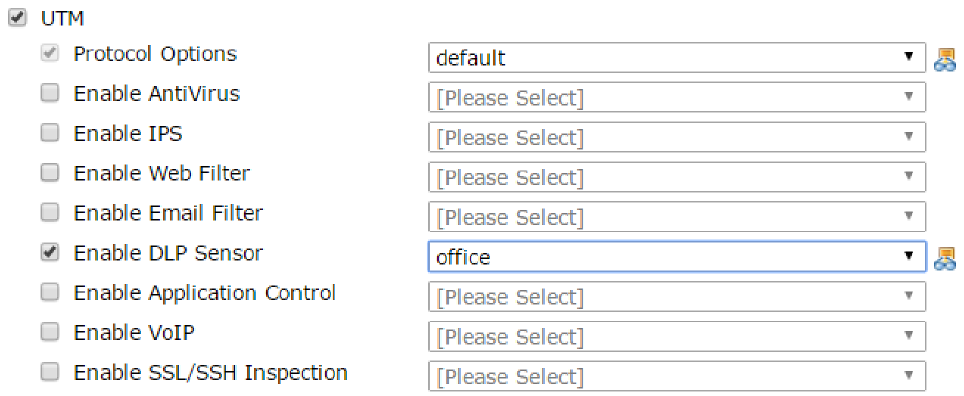
Enable the DLP sensor in the policy.

Edit the policy for Internet access. Choose **UTM**. Choose **default** from **Protocol Options** drop-down list. Choose **office** from **Enable DLP Sensor** drop-down list.



New Policy

Source Interface/Zone: Internal
Source address: all
Destination Interface/Zone: wan1
Destination address: all
Schedule: always
Service: ALL
Action: ACCEPT
☐ Log Allowed Traffic



☑ UTM
☑ Protocol Options: default
☐ Enable AntiVirus: [Please Select]
☐ Enable IPS: [Please Select]
☐ Enable Web Filter: [Please Select]
☐ Enable Email Filter: [Please Select]
☑ Enable DLP Sensor: office
☐ Enable Application Control: [Please Select]
☐ Enable VoIP: [Please Select]
☐ Enable SSL/SSH Inspection: [Please Select]

Tick **UTM**, choose **default** from the **Protocol Options** drop-down list, and lick **OK** to finish the configuration.

Enable log display.

If logs are not displayed, run a command to enable log display.

Note: Before operation, it is recommended to update the version to P2. Under P1 version, a user can run the following commands only after entering **print cliovrd enabl4e**, pressing **Enter**, logging out, and then logging in.

```
RG-WALL # config dlp sensor
RG-WALL (sensor) # edit office
RG-WALL (office) # set extended-utm-log enable
RG-WALL (office) # end
```

V. Verification

Send, download, or upload **exe** and **bat** files via email or FTP. The files are intercepted.

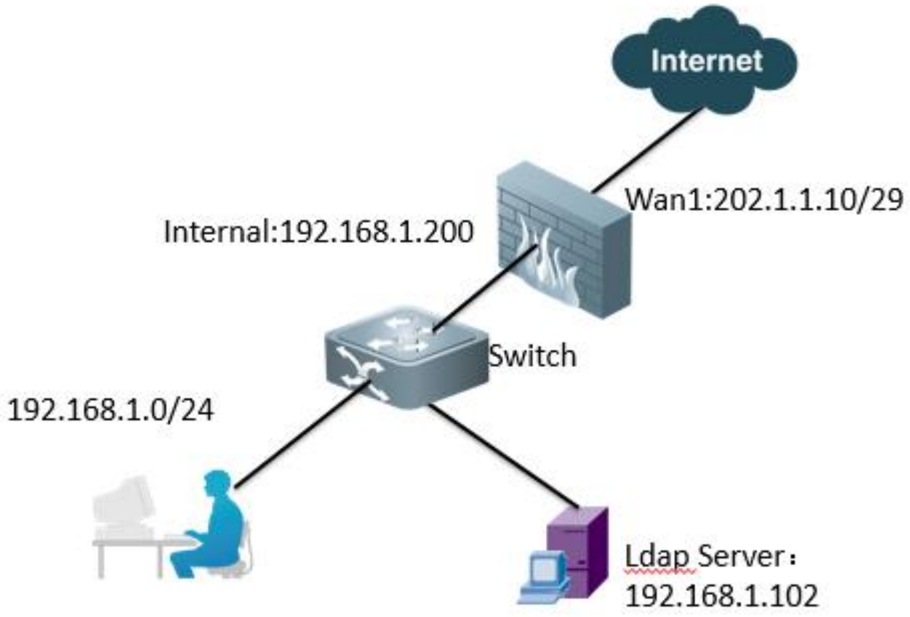
7.1.7 User Authentication

7.1.7.1 LDAP User Authentication

I. Requirements

Only authenticated users can access the Internet. For Internet access, user authentication information should be provided by users in the LDAP server.

II. Topology



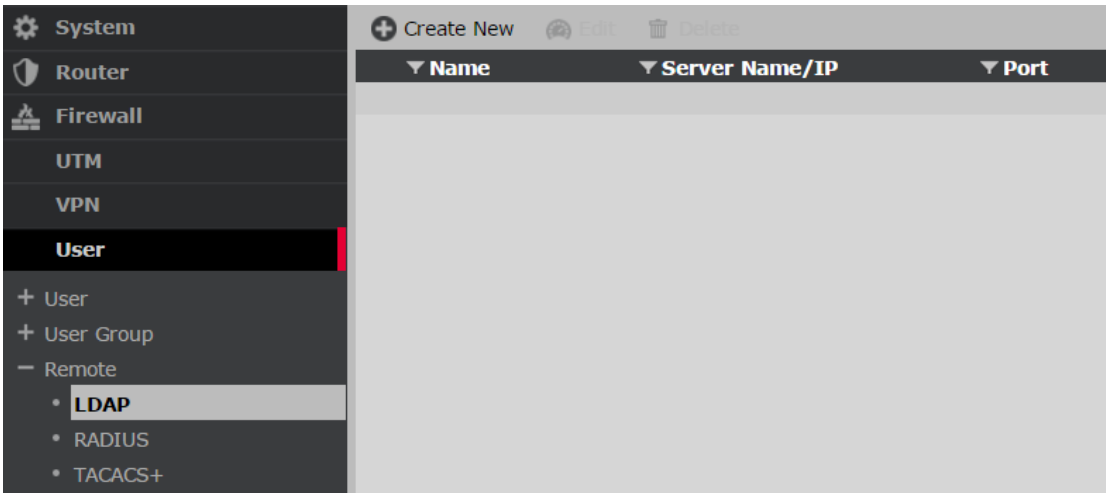
III. Configuration Tips

1. Create a LDAP server.
2. Create a user group.
3. Configure an identity-based Internet access policy.

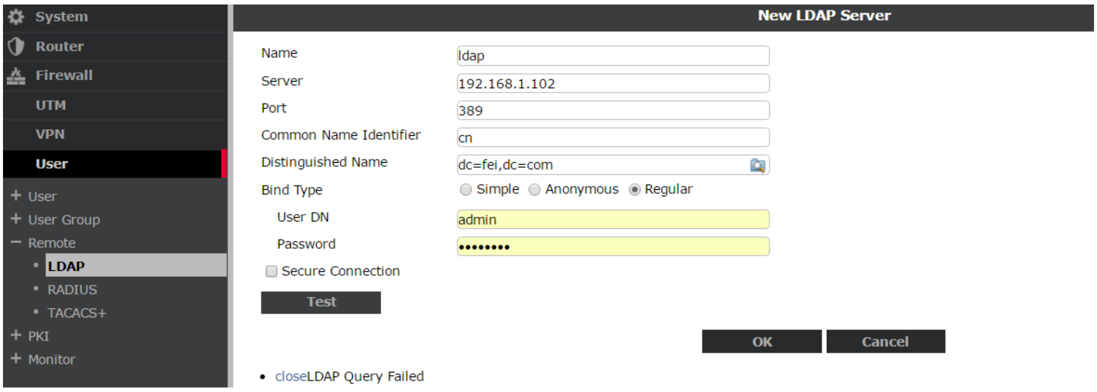
IV. Configuration Steps

1. Create a LDAP server.

Choose **User** > **Remote** > **LDAP**.



Click **Create New**.



New LDAP Server

Name	ldap
Server	192.168.1.102
Port	389
Common Name Identifier	cn
Distinguished Name	dc=fei,dc=com
Bind Type	○ Simple ○ Anonymous ● Regular
User DN	admin
Password	••••••••
□ Secure Connection	

- closeLDAP Query Failed

Name: Enter a name. This item is user-defined.

Server/IP: Set it to 192.168.1.102. It indicates IP address of the LDAP server.

Port: The default value is **389**.

Common Name Identifier: Set it to **cn**. It is set to **uid** in some systems.

Distinguished Name: Set it to **dc=fei,dc=com**. This item is based on the LDAP database.

Bind Type: Tick **Regular**.

User DN and **Password**: The items indicate an account of the LDAP server.

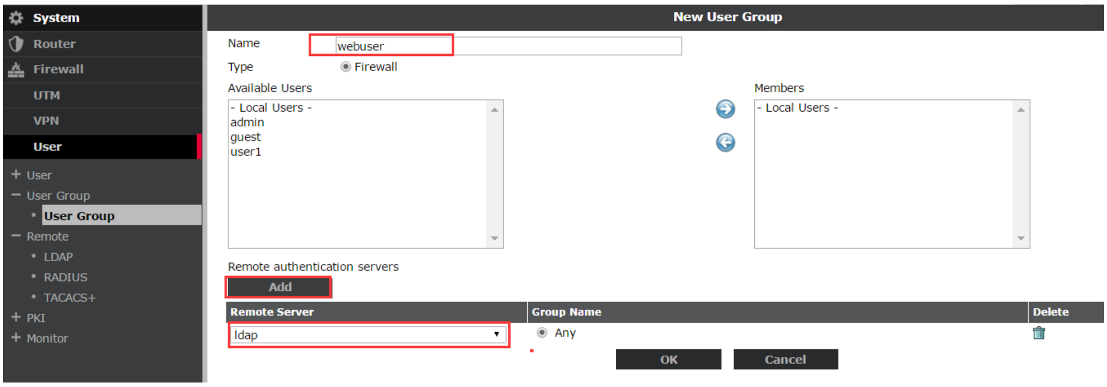
Click **Test** to check the configuration.

Run the following commands to check the server:

```
NGFW # diagnose  test  authserver  ldap ldap test fei!@#

 authenticate 'test' against 'ldap' succeeded!

 Group membership(s) - CN=rj,OU=rj,DC=fei,DC=com
```

2. Create a user group.

Choose **System** > **User** > **User Group**, and then click **Create New**.



New User Group

Name: webuser

Type: ● Firewall

Available Users: - Local Users - admin guest user1

Members: - Local Users -

Remote authentication servers

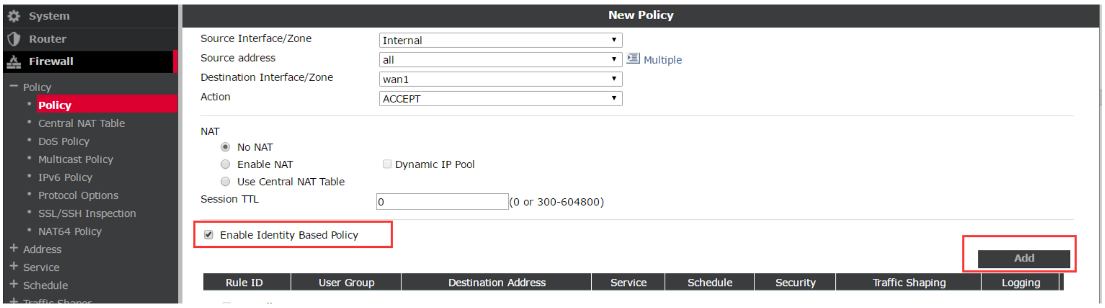
Remote Server	Group Name	Delete
ldap	● Any	🗑

Name: Set it to **webuser**. This item can be set optionally.

Remote Server: Set it to **ldap**.

3. **Configure an identity-based Internet access policy.**

Choose **Firewall** > **Policy** > **Policy**, and then click **Create New**. Configure an Internet access policy as follows:



New Policy

Source Interface/Zone: Internal

Source address: all

Destination Interface/Zone: wan1

Action: ACCEPT

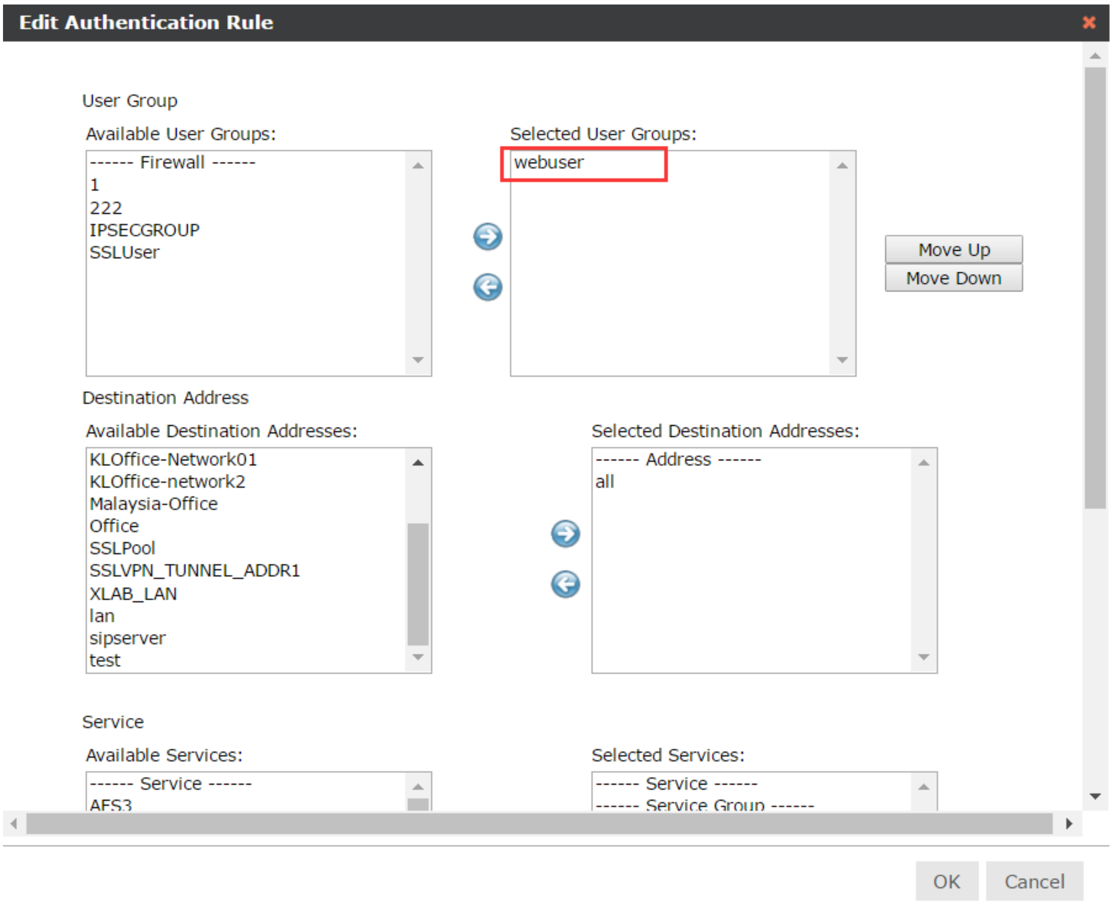
NAT
- ● No NAT
- ○ Enable NAT □ Dynamic IP Pool
- ○ Use Central NAT Table

Session TTL: 0 (0 or 300-604800)

☑ Enable Identity Based Policy

Rule ID	User Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging

Tick **Enable Identity Based Policy** and click **Add**. In the **Edit Authentication Rule**, select the user group **webuser**, and configure **Available Destination Addresses** and **Available Services**.



Edit Authentication Rule

User Group

Available User Groups:

------ Firewall ------
1
222
IPSECGROUP
SSLUser

Selected User Groups:

webuser

Destination Address

Available Destination Addresses:

KLOffice-Network01
KLOffice-network2
Malaysia-Office
Office
SSLPool
SSLVPN_TUNNEL_ADDR1
XLAB_LAN
lan
sipserver
test

Selected Destination Addresses:

------ Address ------
all

Service

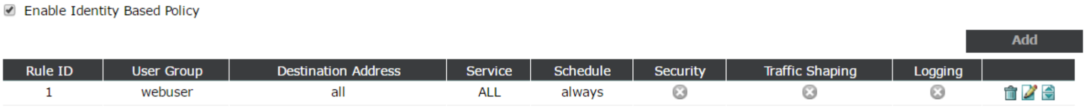
Available Services:

------ Service ------
AFS3

Selected Services:

------ Service ------
------ Service Group ------

The policy is displayed as follows:

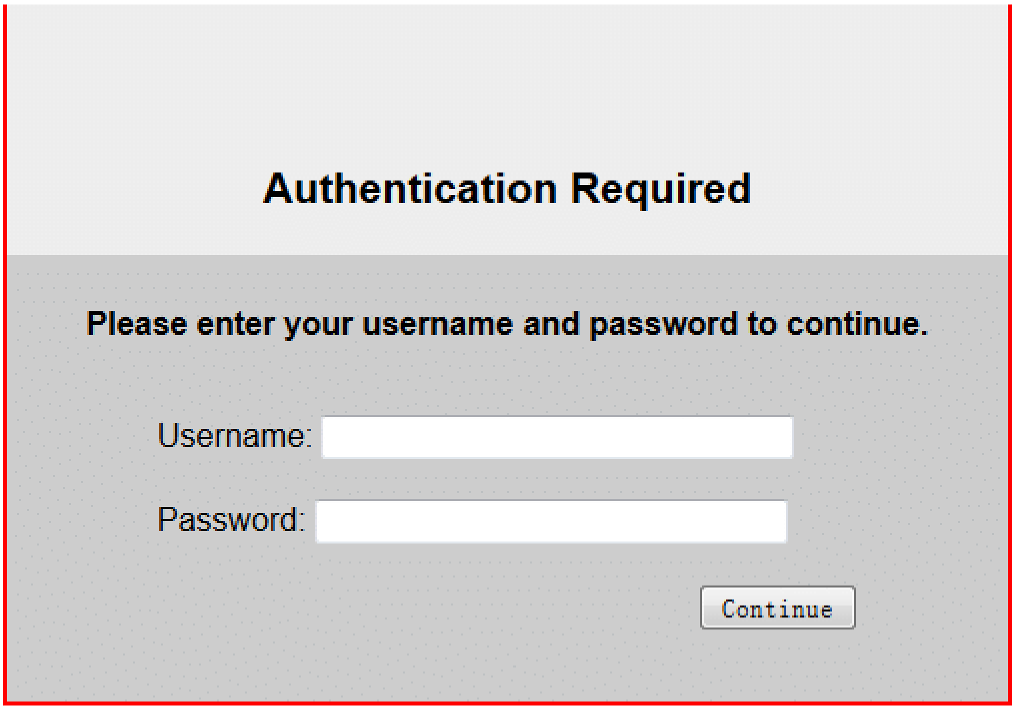


☑ Enable Identity Based Policy

Rule ID	User Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging	
1	webuser	all	ALL	always	⊗	⊗	⊗	

V. Verification

Choose **Firewall** > **Policy** > **Policy**. In the browser window, the **Authentication Required** page is displayed. Enter the user name and password of the LDAP account to access the Internet.



Authentication Required

Please enter your username and password to continue.

Username:

Password:

Choose **Firewall** > **User** > **Monitor** to view authenticated users.

Troubleshooting commands:

RG-WALL #diagnose deb enable

RG-WALL #diagnose debug application fnbamd -1//**Note:** Before operation, it is recommended to update the version to P2. Under P1 version, a user can run the following command only after entering **print cliovrd enabl4e**, pressing **Enter**, logging out, and then logging in.

Run the following command to check whether the account is valid.

```
RG-FW # diagnose  test  authserver  ldap ldap test   fei!@#        //The authentication type is ldap, server name is ldap, user name is test, and password is fei!@#.
```

7.2 Configuring Log

7.2.1 Log Storage Manner

Setting Log Storage Manner

Currently, firewall logs can be stored in three manners: 1) hard disk; 2) memory; 3) the third-party server (sending syslog).

On the **Log Settings** page, you can set the log storage manner.

Disk: If you choose **Disk**, logs will be stored in the hard disk.

Syslog Server: It indicates the third-party syslog storage server. You can set three Syslog Servers.

Event Logging: Choose the event log type.

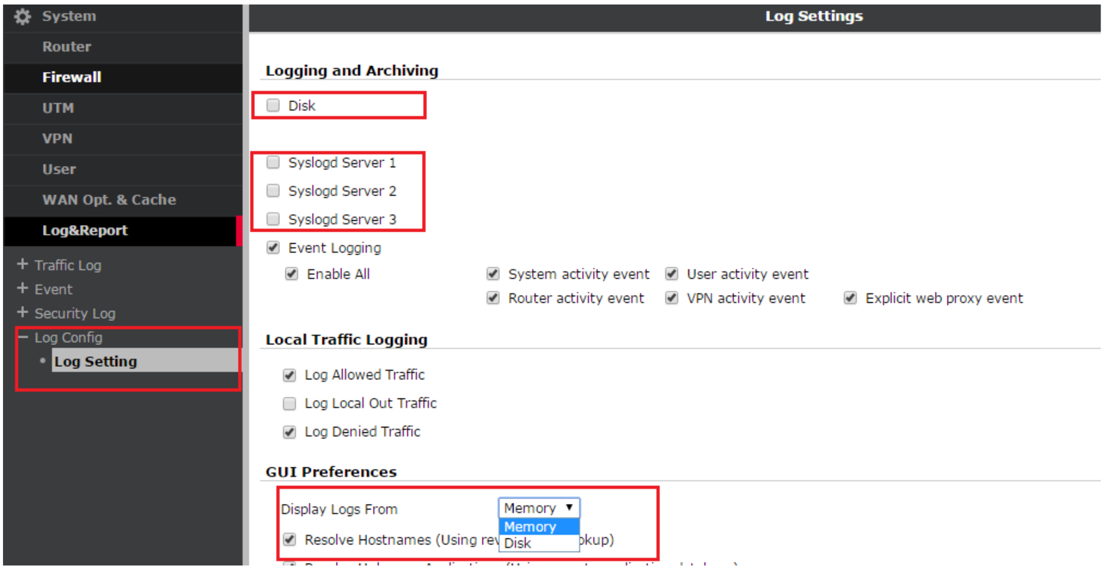
Local Traffic Logging: Choose the local traffic log type. Local traffic refers to the traffic for accessing the firewall.

GUI Preferences: Choose the source of the logs: hard disk or memory.

1. By default, logs are stored in the hard disk.

2. The S3100 and M6600 are not installed with hard disks. Therefore, you cannot choose **Disk**.

3. Choosing **Resolve Hostnames** and **Resolve Unknown Applications** is not recommended.



Log Settings

Logging and Archiving

☐ Disk

☐ Syslogd Server 1
☐ Syslogd Server 2
☐ Syslogd Server 3

☑ Event Logging

☑ Enable All ☑ System activity event ☑ User activity event
☑ Router activity event ☑ VPN activity event ☑ Explicit web proxy event

Local Traffic Logging

☑ Log Allowed Traffic
☐ Log Local Out Traffic
☑ Log Denied Traffic

GUI Preferences

Display Logs From: Memory ▼ (Memory, Disk)

☑ Resolve Hostnames (Using rev okup)

7.2.2 Storing Logs in the Hard Disk

Requirements

All the logs generated on the firewall are stored in the hard disk, such as traffic logs, event logs, and security logs. In this example, configure the local traffic logging to log allowed traffic and enable event loggings, and store logs in the hard disk.

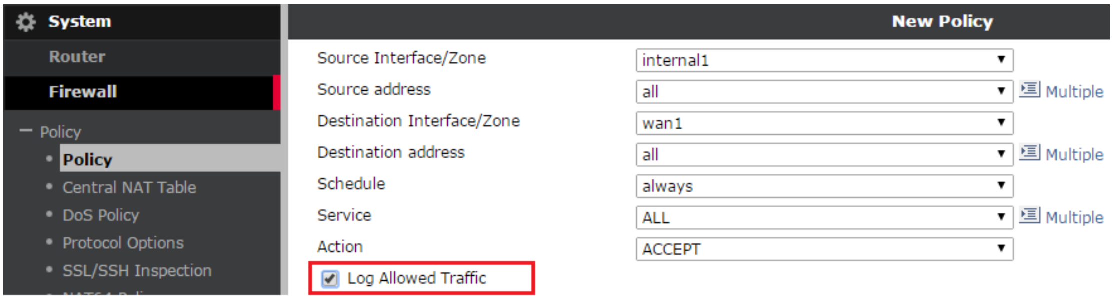
The S3100 and M6600 are not installed with hard disks. Therefore, they do not support log storage in the hard disk. Refer to section 5.2.3 “Storing Logs in the Memory”.

Caution

Because there is a great number of allowed traffic logs, performance of the device will be consumed and hard disk lifecycle is reduced when logs are stored in the hard disk. It is recommended to send logs to the third-party server. For details, see section 5.2.4 “Sending Syslog”.

Configuration Tips

1. **Choose Firewall > Policy, and edit the specific policy. Choose Log Allowed Traffic. See the following figure:**



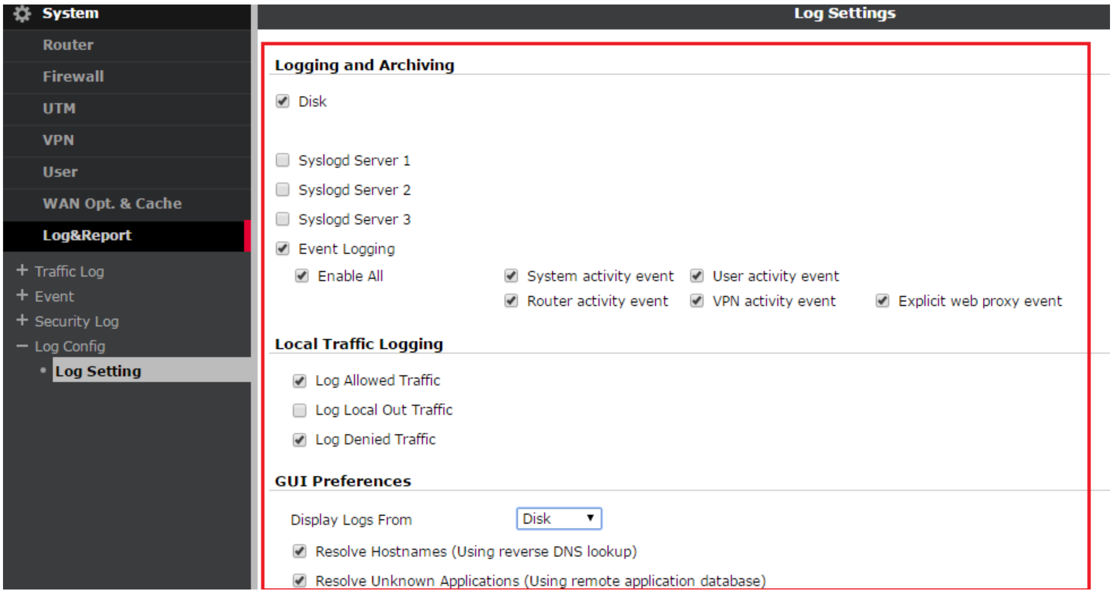
New Policy

Source Interface/Zone: internal1
Source address: all
Destination Interface/Zone: wan1
Destination address: all
Schedule: always
Service: ALL
Action: ACCEPT
☑ Log Allowed Traffic

2. **Choose Log&Report > Log Config > Log Setting.**

Choose **Disk** in the **Logging and Archiving** pane. Choose **Disk** from **Display Logs From** drop-down list in the **GUI Preferences** pane. Choose the event log and local traffic log types to be recorded.

For how to enable logs of each UTM function, (By default, such logs are not enabled.), see section “UTM Log Configuration” in “Universal Typical Functions”.



Log Settings

Logging and Archiving

☑ Disk

☐ Syslogd Server 1
☐ Syslogd Server 2
☐ Syslogd Server 3
☑ Event Logging
☑ Enable All ☑ System activity event ☑ User activity event
☑ Router activity event ☑ VPN activity event ☑ Explicit web proxy event

Local Traffic Logging

☑ Log Allowed Traffic
☐ Log Local Out Traffic
☑ Log Denied Traffic

GUI Preferences

Display Logs From: Disk
☑ Resolve Hostnames (Using reverse DNS lookup)
☑ Resolve Unknown Applications (Using remote application database)

3. Set the parameters for storing logs in the hard disk. (Only configured through CLI)

```
RG-WALL # config log disk setting
RG-WALL (setting) # set maximum-log-age 30   //Set the log storage period to 30
days.
RG-WALL (setting) # end

RG-WALL # config log disk filter
RG-WALL (filter) # set forward-traffic disable      //Disable forward-traffic.
RG-WALL (filter) # end
```

Forward-traffic refers to enabling **Log Allowed Traffic**. It is strongly recommended to disable it.

4. View the parameters for storing logs in the hard disk. (Only configured through CLI)

a) View the parameters for recording logs in the hard disk.

```
RG-WALL # get log disk setting
status              : enable
ips-archive         : enable
max-policy-packet-capture-size: 10
log-quota           : 0                         //By default, it is not restricted. Enter the
hard disk space size assigned for hard disk logs.
dlp-archive-quota   : 0
report-quota        : 0
maximum-log-age     : 30                   //Set it to 30. By default, logs are kept for 7
days.
upload              : disable
drive-standby-time  : 0
full-first-warning-threshold: 75         //Enter the value before the threshold reaches 75%
to configure the first warning.
full-second-warning-threshold: 90          //Enter the value before the threshold reaches 90%
to configure the second warning.
full-final-warning-threshold: 95          //Enter the value before the threshold reaches 95%
to configure the last warning.
  : 100
storage             :
roll-schedule       : daily                //It indicates the log rolling frequency. By
default, logs are rolled every day.
roll-time           : 00:00                //By default, logs are rolled at 00:00.
diskfull            : overwrite           //By default, set it to overwrite. When you enter
nolog, the RG-WALL device stops logging. When you enter overwrite and the hard disk is
full, the file with the longest time will be immediately overwritten.
```

```
report              : enable
```

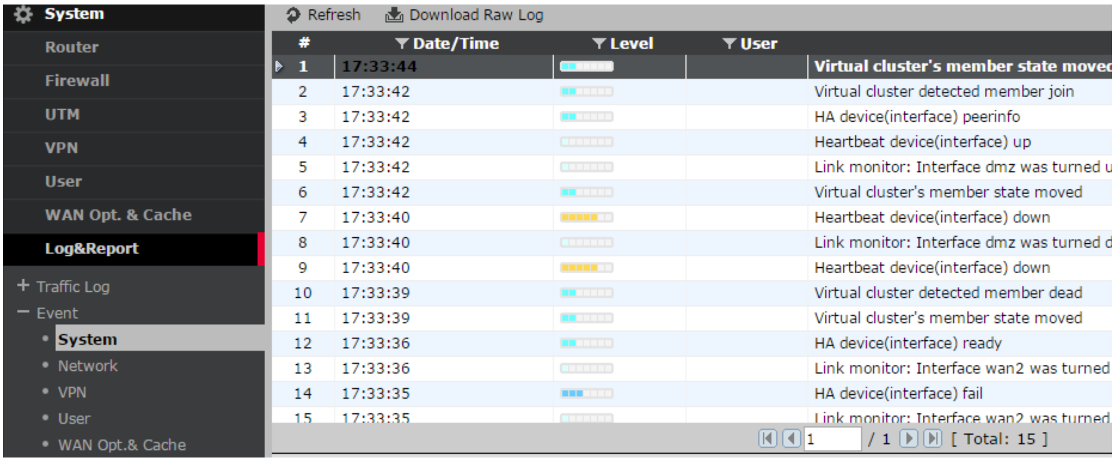
b) View the options for recording logs in the hard disk.

```
RG-WALL # get log disk filter
severity            : information
traffic             : enable
forward-traffic     : disable
local-traffic       : enable
attack              : enable
web                 : enable
netscan             : enable
dlp                 : enable
virus               : enable
email               : enable
voip                : enable
app-ctrl            : enable
dlp-archive         : enable
multicast-traffic   : enable
signature           : enable
anomaly             : enable
web-content         : enable
url-filter          : enable
ftgd-wf-block       : enable
ftgd-wf-errors      : enable
web-filter-activex  : enable
web-filter-cookie   : enable
web-filter-applet   : enable
web-filter-script-other: enable
web-filter-ftgd-quota-counting: enable
web-filter-ftgd-quota-expired: enable
web-filter-ftgd-quota: enable
web-filter-command-block: enable
discovery           : enable
vulnerability       : enable
dlp-all             : enable
dlp-docsource       : enable
infected            : enable
blocked             : enable
scanerror           : enable
suspicious          : enable
analytics           : enable
oversized           : enable
```

```
switching-protocols : enable
email-log-smtp      : enable
email-log-pop3      : enable
email-log-imap      : enable
email-log-msn       : enable
email-log-yahoo     : enable
email-log-google    : enable
app-ctrl-all        : enable
```

Verification

After the preceding configuration is completed, choose **Log&Report** > **Traffic Log** or **Event** or **Security Log** to view specific logs, as shown in the following figure:



#	Date/Time	Level	User	
1	17:33:44			Virtual cluster's member state movec
2	17:33:42			Virtual cluster detected member join
3	17:33:42			HA device(interface) peerinfo
4	17:33:42			Heartbeat device(interface) up
5	17:33:42			Link monitor: Interface dmz was turned u
6	17:33:42			Virtual cluster's member state moved
7	17:33:40			Heartbeat device(interface) down
8	17:33:40			Link monitor: Interface dmz was turned d
9	17:33:40			Heartbeat device(interface) down
10	17:33:39			Virtual cluster detected member dead
11	17:33:39			Virtual cluster's member state moved
12	17:33:36			HA device(interface) ready
13	17:33:36			Link monitor: Interface wan2 was turned
14	17:33:35			HA device(interface) fail
15	17:33:35			Link monitor: Interface wan2 was turned

1 / 1 [Total: 15]

7.2.3 Storing Logs in the Memory

Requirements

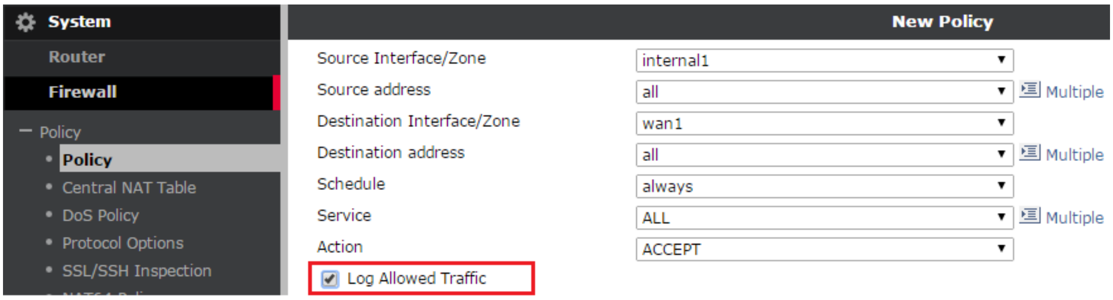
For the devices that are not installed with hard disks, such as the S3100 and M6600, you can store the logs generated on the firewall in the memory, such as traffic logs, event logs, and security logs. In this example, configure the local traffic logging to log allowed traffic and enable event loggings, and store logs in the memory.

⚠ Caution

Because there is a great number of allowed traffic logs, performance of the device will be consumed and memory lifecycle is reduced when logs are stored in the memory. It is recommended to send logs to the third-party server. For details, see section 5.2.4 “Sending Syslog”.

Configuration Tips

1. **Choose Firewall > Policy, and edit the specific policy. Choose Log Allowed Traffic. See the following** figure:



New Policy

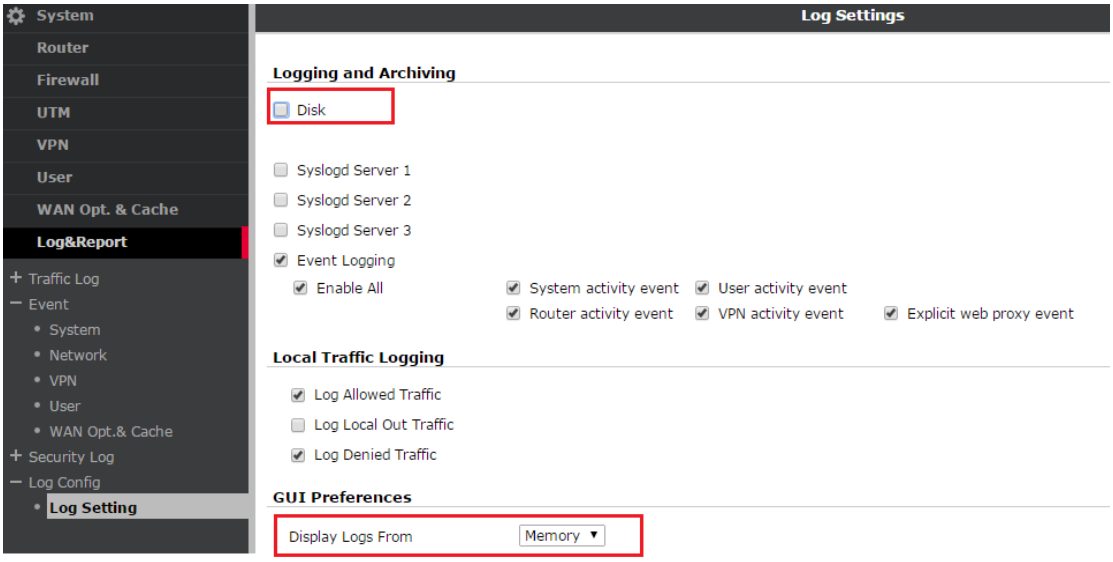
Source Interface/Zone	internal1
Source address	all
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT

☑ Log Allowed Traffic

2. Choose Log&Report > Log Config > Log Setting.

Choose **Disk** in the **Logging and Archiving** pane. Choose **Memory** from **Display Logs** From drop-down list in the **GUI Preferences** pane. Choose the event log and local traffic log types to be recorded.

For how to enable logs of each UTM function (By default, such logs are not enabled.), see section “UTM Log Configuration” in “Universal Typical Functions”.



Log Settings

Logging and Archiving

□ Disk

□ Syslogd Server 1

□ Syslogd Server 2

□ Syslogd Server 3

☑ Event Logging

☑ Enable All ☑ System activity event ☑ User activity event

☑ Router activity event ☑ VPN activity event ☑ Explicit web proxy event

Local Traffic Logging

☑ Log Allowed Traffic

□ Log Local Out Traffic

☑ Log Denied Traffic

GUI Preferences

Display Logs From Memory

3. Set the parameters for storing logs in the memory. (Only configured through CLI)

```
RG-WALL # config log memory setting
RG-WALL (setting) # set status enable   //Enable log storage in the memory.
RG-WALL (setting) # end

RG-WALL # config log memory filter
RG-WALL (filter) # set forward-traffic disable        //Disable forward-traffic.
RG-WALL (filter) # end
```

Forward-traffic refers to enabling **Log Allowed Traffic**. It is strongly recommended to disable it.

4. **View the parameters for storing logs in the memory. (Only configured through CLI)**

   a) View the parameters for recording logs in the memory.

```
RG-WALL # get log memory setting
status              : enable
diskfull            : overwrite
```

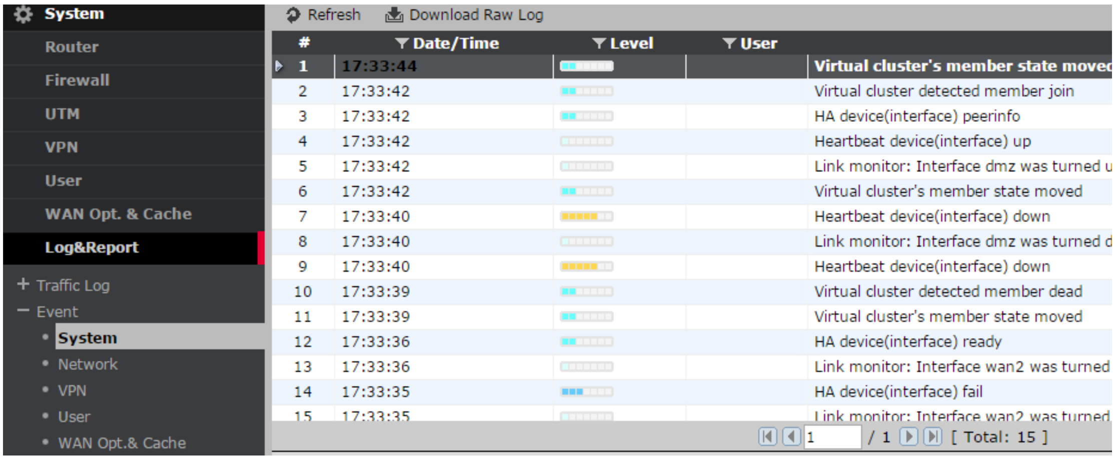
   b) View the options for recording logs in the memory.

```
RG-WALL # get log memory filter
severity            : information
traffic             : enable
forward-traffic     :disable
local-traffic       : enable
attack              : enable
web                 : enable
netscan             : enable
dlp                 : enable
virus               : enable
email               : enable
voip                : enable
app-ctrl            : enable
multicast-traffic   : enable
signature           : enable
anomaly             : enable
web-content         : enable
url-filter          : enable
ftgd-wf-block       : enable
ftgd-wf-errors      : enable
web-filter-activex  : enable
web-filter-cookie   : enable
web-filter-applet   : enable
web-filter-script-other: enable
web-filter-ftgd-quota-counting: enable
web-filter-ftgd-quota-expired: enable
web-filter-ftgd-quota: enable
web-filter-command-block: enable
discovery           : enable
vulnerability       : enable
dlp-all             : enable
```

```
dlp-docsource       : enable
infected            : enable
blocked             : enable
scanerror           : enable
suspicious          : enable
analytics           : enable
oversized           : enable
switching-protocols : enable
email-log-smtp      : enable
email-log-pop3      : enable
email-log-imap      : enable
email-log-msn       : enable
email-log-yahoo     : enable
email-log-google    : enable
app-ctrl-all        : enable
```

Verification

After the preceding configuration is completed, choose **Log&Report** > **Traffic Log** or **Event** or **Security Log** to view specific logs, as shown in the following figure:



#	Date/Time	Level	User	
1	17:33:44			Virtual cluster's member state movec
2	17:33:42			Virtual cluster detected member join
3	17:33:42			HA device(interface) peerinfo
4	17:33:42			Heartbeat device(interface) up
5	17:33:42			Link monitor: Interface dmz was turned u
6	17:33:42			Virtual cluster's member state moved
7	17:33:40			Heartbeat device(interface) down
8	17:33:40			Link monitor: Interface dmz was turned d
9	17:33:40			Heartbeat device(interface) down
10	17:33:39			Virtual cluster detected member dead
11	17:33:39			Virtual cluster's member state moved
12	17:33:36			HA device(interface) ready
13	17:33:36			Link monitor: Interface wan2 was turned
14	17:33:35			HA device(interface) fail
15	17:33:35			Link monitor: Interface wan2 was turned

1 / 1 [Total: 15]

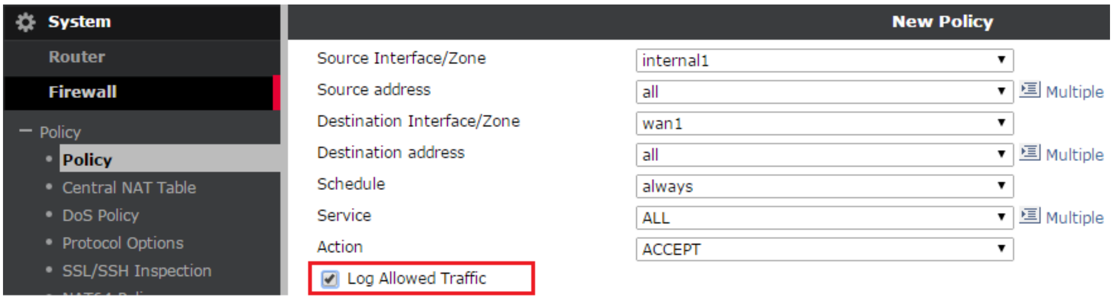
7.2.4 Sending Syslog

Requirements

For the devices that are not installed with hard disks, such as the S3100 and M6600, you can send the logs, such as traffic logs, event logs, and security logs, which are generated on the firewall to a third-party server. (This storage manner is recommended.) In this example, configure the local traffic logging to log allowed traffic and enable event loggings, and send logs to a syslog server.

Configuration Tips

1. **Choose Firewall > Policy, and edit the specific policy. Choose Log Allowed Traffic. See the following figure:**

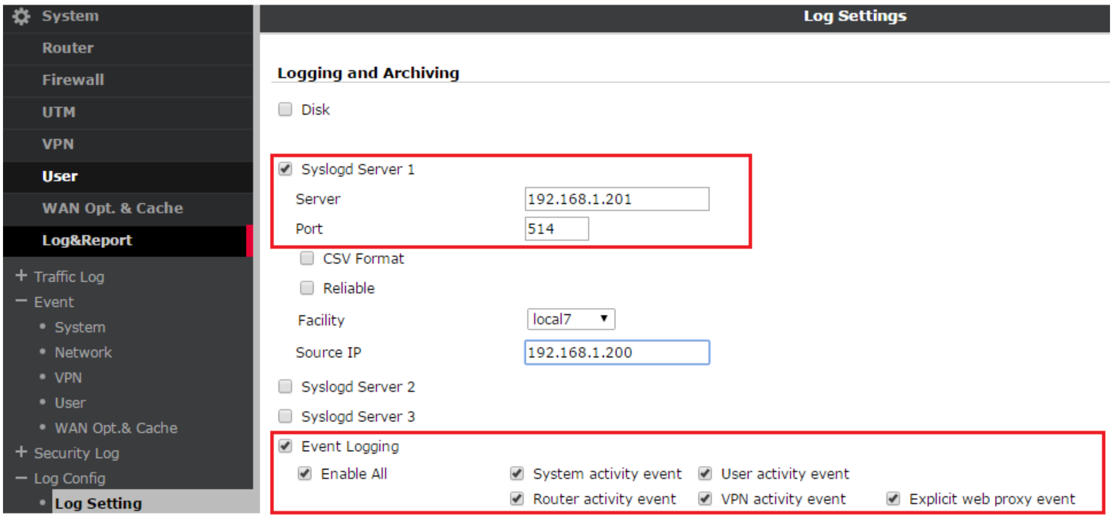


New Policy

Source Interface/Zone	internal1	
Source address	all	Multiple
Destination Interface/Zone	wan1	
Destination address	all	Multiple
Schedule	always	
Service	ALL	Multiple
Action	ACCEPT	

☑ Log Allowed Traffic

2. **Choose Log&Report > Log Config > Log Setting.**



Log Settings

Logging and Archiving

☐ Disk

☑ Syslogd Server 1

Server	192.168.1.201
Port	514

☐ CSV Format

☐ Reliable

Facility	local7
Source IP	192.168.1.200

☐ Syslogd Server 2

☐ Syslogd Server 3

☑ Event Logging

☑ Enable All ☑ System activity event ☑ User activity event

☑ Router activity event ☑ VPN activity event ☑ Explicit web proxy event

Logging and Archiving: Clear **Disk**.

Syslog Server 1: Set the IP address of the log server.

Facility: Set the level to define the emergency of messages.

Source IP: Set the IP address of the firewall that can interwork with the log server. Here, enter the internal port IP address.

Event Logging: Choose the events logs to be recorded.

3. **On the third-party server, install software to receive syslog from the firewall, such as Syslog watcher.**

4. View the parameters for storing syslogs. (Only configured through CLI)

a) View the parameters for recording syslogs.

```
RG-WALL # get log syslogd setting
status               : enable
```

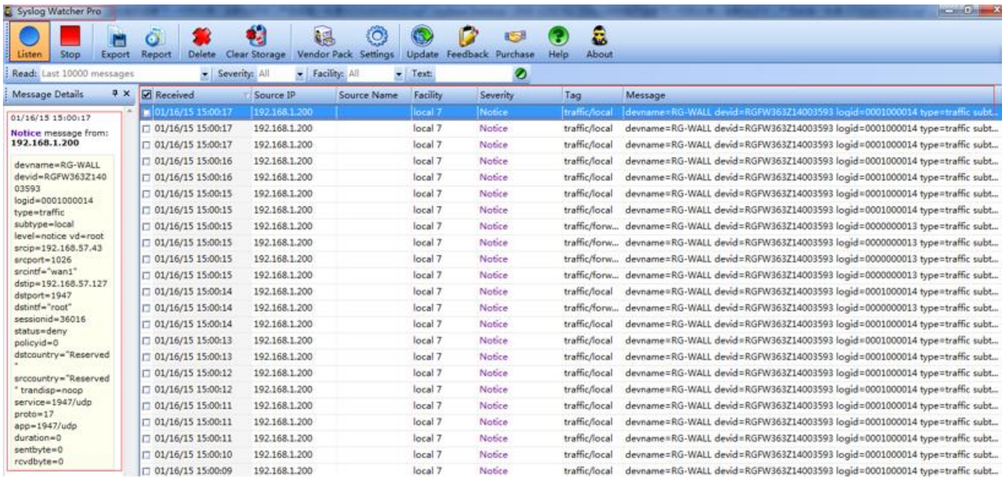
b) View the options for recording syslogs.

```
RG-WALL # get log syslogd filter
severity             : information
traffic              : enable
forward-traffic      : enable
local-traffic        : enable
attack               : enable
web                  : enable
netscan              : enable
dlp                  : enable
virus                : enable
email                : enable
voip                 : enable
app-ctrl             : enable
multicast-traffic    : enable
signature            : enable
anomaly              : enable
web-content          : enable
url-filter           : enable
ftgd-wf-block        : enable
ftgd-wf-errors       : enable
web-filter-activex   : enable
web-filter-cookie    : enable
web-filter-applet    : enable
web-filter-script-other: enable
web-filter-ftgd-quota-counting: enable
web-filter-ftgd-quota-expired: enable
web-filter-ftgd-quota: enable
web-filter-command-block: enable
discovery            : enable
vulnerability        : enable
dlp-all              : enable
dlp-docsource        : enable
infected             : enable
blocked              : enable
scanerror            : enable
suspicious           : enable
analytics            : enable
oversized            : enable
```

```
switching-protocols : enable
email-log-smtp      : enable
email-log-pop3      : enable
email-log-imap      : enable
email-log-msn       : enable
email-log-yahoo     : enable
email-log-google    : enable
app-ctrl-all        : enable
```

Verification

After the preceding configuration is completed, open Syslog watcher on the log server for viewing logs. See the following figure.



Read: Last 10000 messages   Severity: All   Facility: All   Text:

01/16/15 15:00:17

Notice message from:
192.168.1.200

```
devname=RG-WALL
devid=RGFW363Z140
03593
logid=0001000014
type=traffic
subtype=local
level=notice vd=root
srcip=192.168.57.43
srcport=1026
srcintf="wan1"
dstip=192.168.57.127
dstport=1947
dstintf="root"
sessionid=36016
status=deny
policyid=0
dstcountry="Reserved
"
srccountry="Reserved
" trandisp=noop
service=1947/udp
proto=17
app=1947/udp
duration=0
sentbyte=0
rcvdbyte=0
```

☑ Received	Source IP	Source Name	Facility	Severity	Tag	Message
■ 01/16/15 15:00:17	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:17	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:17	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:16	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:16	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:15	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:15	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:15	192.168.1.200		local 7	Notice	traffic/forw...	devname=RG-WALL devid=RGFW363Z14003593 logid=0000000013 type=traffic subt...
□ 01/16/15 15:00:15	192.168.1.200		local 7	Notice	traffic/forw...	devname=RG-WALL devid=RGFW363Z14003593 logid=0000000013 type=traffic subt...
□ 01/16/15 15:00:15	192.168.1.200		local 7	Notice	traffic/forw...	devname=RG-WALL devid=RGFW363Z14003593 logid=0000000013 type=traffic subt...
□ 01/16/15 15:00:15	192.168.1.200		local 7	Notice	traffic/forw...	devname=RG-WALL devid=RGFW363Z14003593 logid=0000000013 type=traffic subt...
□ 01/16/15 15:00:14	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:14	192.168.1.200		local 7	Notice	traffic/forw...	devname=RG-WALL devid=RGFW363Z14003593 logid=0000000013 type=traffic subt...
□ 01/16/15 15:00:14	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:13	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:13	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:12	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:12	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:11	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:11	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:11	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:10	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...
□ 01/16/15 15:00:09	192.168.1.200		local 7	Notice	traffic/local	devname=RG-WALL devid=RGFW363Z14003593 logid=0001000014 type=traffic subt...

7.2.5 Configuring UTM Logging

7.2.5.1 Enabling UTM Logging

UTM logging including IPS and anti-virus logs should be enabled through CLI.

1. Enable IPS logging.

```
RG-WALL # config ips sensor
RG-WALL (sensor) # edit httpserver
new entry 'httpserver' added
RG-WALL (httpserver) # set log enable
RG-WALL (httpserver) # config entries
RG-WALL (entries) # edit 1
new entry '1' added
RG-WALL (1) # set log enable
RG-WALL (1) # set log-packet enable
```

```
RW-WALL (1) # end
```

2. Enable anti-virus logging.

```
RG-WALL # config antivirus profile
RG-WALL (profile) # edit default
RG-WALL (default) # set extended-utm-log enable
RG-WALL (default) # set av-virus-log enable
RG-WALL (default) # set av-block-log enable
             RG-WALL (default) # end
```

3. Enable email filter logging.

```
RG-WALL # config spamfilter profile
RG-WALL (profile) # edit mymail
RG-WALL (mymail) # set extended-utm-log enable
RG-WALL (mymail) # end
```

4. Enable application control logging.

```
RG-WALL # config application list
RG-WALL (list) # edit office
new entry ’office’ added
RG-WALL (office) # set extended-utm-log  enable
RG-WALL (office) # end
```

5. Enable anti-data-leakage logging.

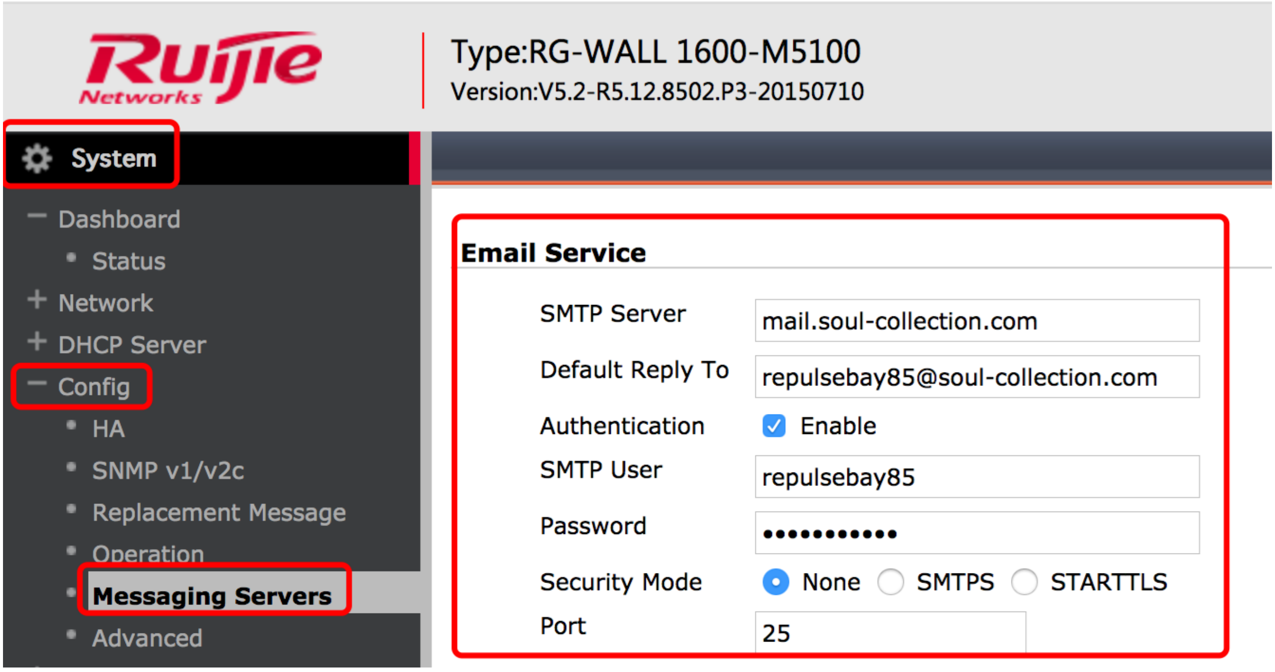
```
RG-WALL # config dlp sensor
RG-WALL (sensor) # edit office
RG-WALL (office) # set extended-utm-log enable
RG-WALL (office) # end
```

7.2.6 Email Configuration

Alert Email Configuration:

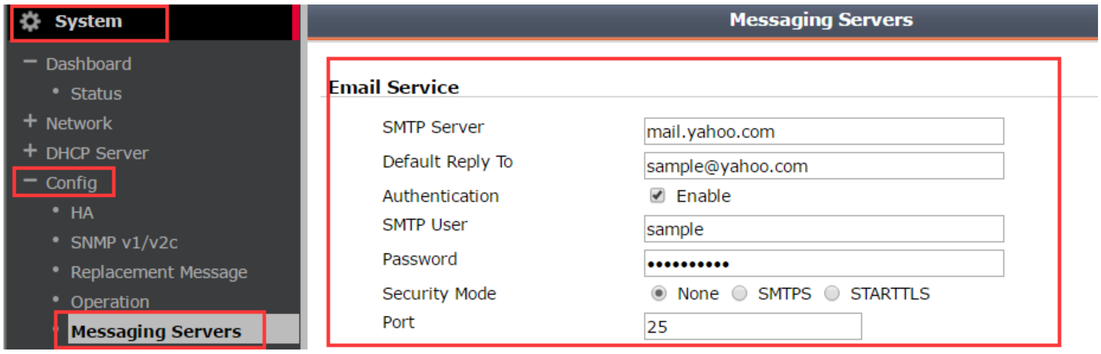
(1) Configuration of the incoming mailbox and outgoing mailbox (on the Web or on the command line)

Method 1: Configuration on the Web (as shown in the following screenshot)



Email Service

SMTP Server	mail.soul-collection.com
Default Reply To	repulsebay85@soul-collection.com
Authentication	☑ Enable
SMTP User	repulsebay85
Password	●●●●●●●●●●●
Security Mode	● None ○ SMTPS ○ STARTTLS
Port	25



Messaging Servers

Email Service

SMTP Server	mail.yahoo.com
Default Reply To	sample@yahoo.com
Authentication	☑ Enable
SMTP User	sample
Password	●●●●●●●●●●
Security Mode	● None ○ SMTPS ○ STARTTLS
Port	25

Method 2: Configuration on the command line

```
config system email-server   //Enters the email server configuration.
    set reply-to "sample@yahoo.com"     //Indicates the incoming mailbox.
    set server "mail.yahoo.com"       //Indicates the outgoing mailbox.
    set authenticate enable    //Enables outgoing mailbox authentication.
    set username "sample"     //Indicates the user name for sending emails.
set password xxxxxx    //Indicates the password for sending emails.
```

(2) Configuration of the mailbox associated with alert messages (on the command line only)

```
config alertemail setting  //Configures alert email sending settings.
    set username "sample@yahoo.com"
    set mailto1 "sample_receive@yahoo.com"    //Sets the incoming mailbox of alert emails.
    set filter-mode threshold //Sets the message threshold for email 1 to critical.
    set filter-mode threshold //Sets the message threshold for email 2 to critical.
```

7.2.7 Traffic Rate Limit

I. Networking Requirements

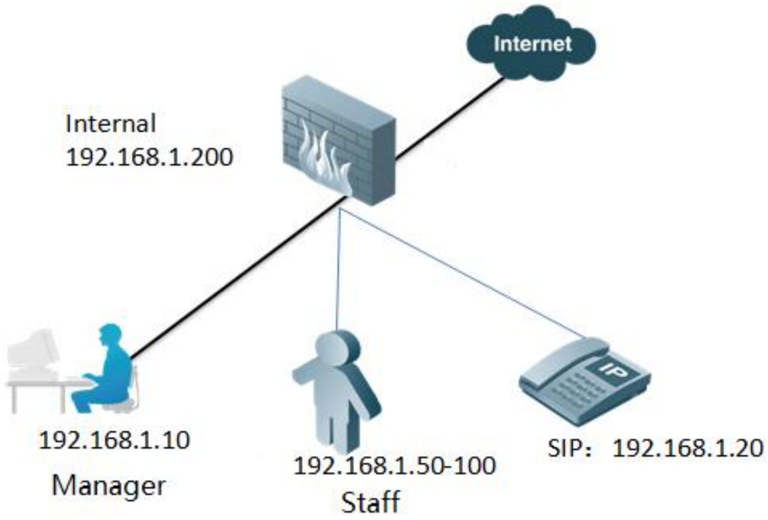
A company performs traffic management over intranet users. The egress bandwidth is restricted to 20 Mbps.

Manager: Traffic for 192.168.1.10 is not restricted.

Staff: The total bandwidth for 192.168.1.50-100 is restricted to 15 Mbps. Traffic of each employee cannot exceed 1 Mbps.

IP phone and video: The bandwidth for 192.168.1.20 is 3 Mbps to guarantee smooth video playing.

II. Network Topology



III. Configuration Tips

1. Basic configuration of the interfaces and routes for Internet access
2. Define the address object according to the IP address segments to be restricted.
3. Define the traffic shaper.
4. Configure the policy and enable traffic control.

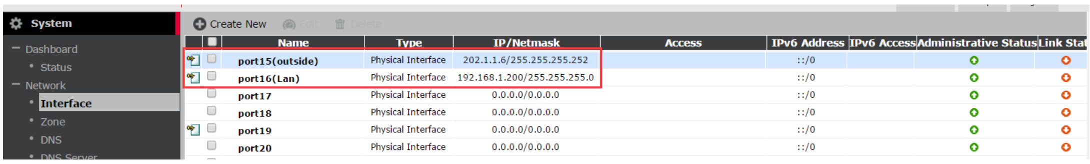
Note: To control upload and download traffic, enable reverse flow control. Reverse flow control refers to controlling the flow in the downloading direction. After reverse flow control is enabled, upload and download traffic is separately controlled.

IV. Configuration Steps

1. Basic configuration of the interfaces and routes for Internet access

For the detailed configuration process, see "Configuring Internet Access via a Static Link" under "Internet Access via a Single Line" in "Functions of Firewall".

IP address configuration of the interfaces is shown in the following figure:



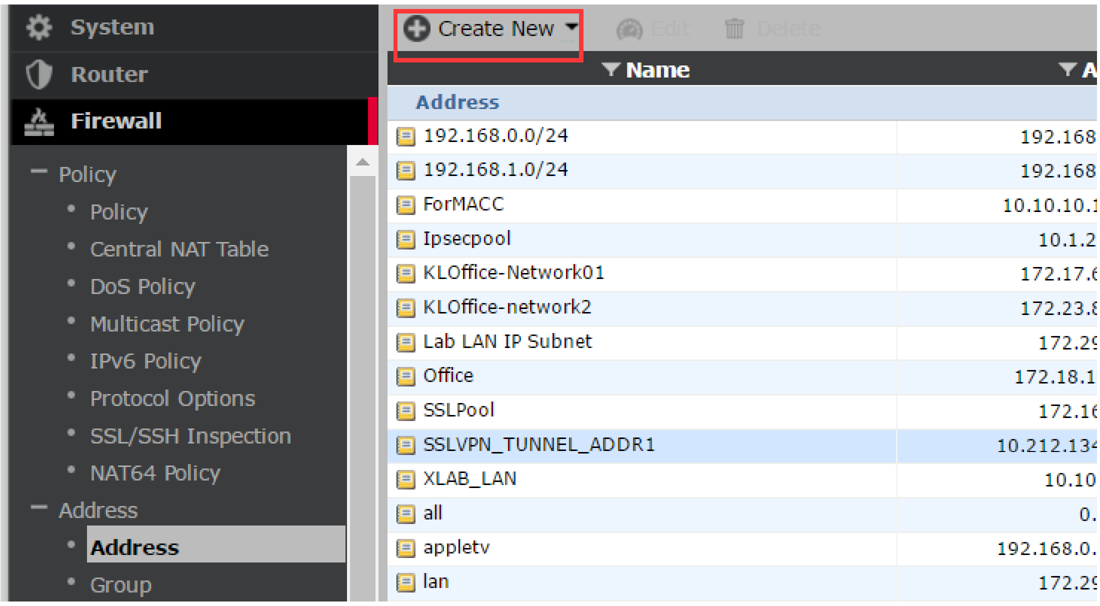
Name	Type	IP/Netmask	Access	IPv6 Address	IPv6 Access	Administrative Status	Link Stat
port15(outside)	Physical Interface	202.1.1.6/255.255.255.252		::/0		↑	↓
port16(Lan)	Physical Interface	192.168.1.200/255.255.255.0		::/0		↑	↓
port17	Physical Interface	0.0.0.0/0.0.0.0		::/0		↑	↓
port18	Physical Interface	0.0.0.0/0.0.0.0		::/0		↑	↓
port19	Physical Interface	0.0.0.0/0.0.0.0		::/0		↑	↓
port20	Physical Interface	0.0.0.0/0.0.0.0		::/0		↑	↓

2. **Define the address object according to the IP address segments to be restricted.**

Define three address objects:

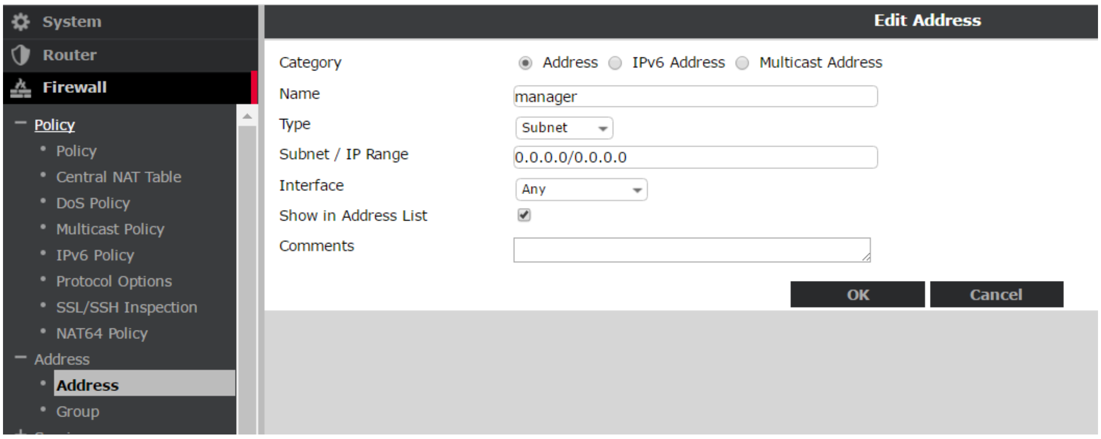
```
manager: 192.168.1.10

sip: 192.168.1.20

staff: 192.168.1.50-100
```

Choose **Firewall** > **Address** > **Address**, and then click **Create New**.



Name	A
Address	
192.168.0.0/24	192.168
192.168.1.0/24	192.168
ForMACC	10.10.10.1
Ipsecpool	10.1.2
KLOffice-Network01	172.17.6
KLOffice-network2	172.23.8
Lab LAN IP Subnet	172.29
Office	172.18.1
SSLPool	172.16
SSLVPN_TUNNEL_ADDR1	10.212.134
XLAB_LAN	10.10
all	0.
appletv	192.168.0.
lan	172.29

a) Define the IP address of the leader's PC. Set **Name** to **manager** and set **Subnet/IP Range** to **192.168.1.10**.



Category ● Address ○ IPv6 Address ○ Multicast Address

Name: manager

Type: Subnet

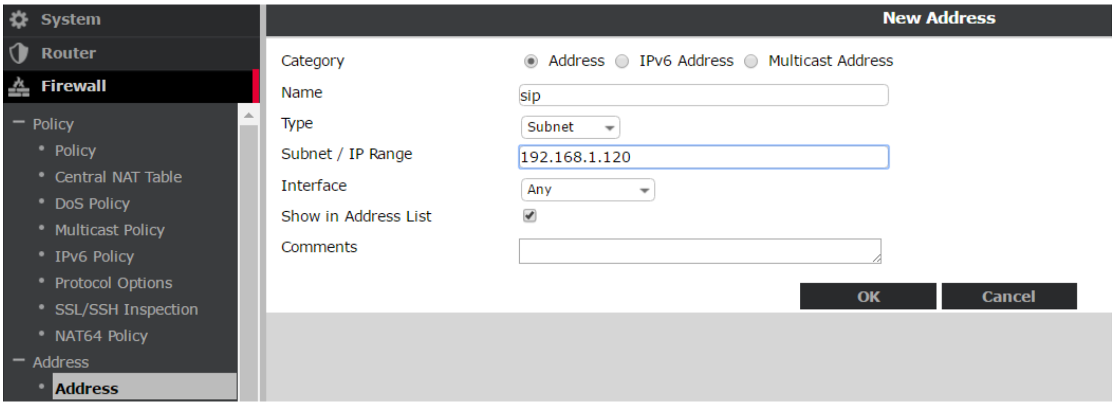
Subnet / IP Range: 0.0.0.0/0.0.0.0

Interface: Any

Show in Address List ☑

Comments

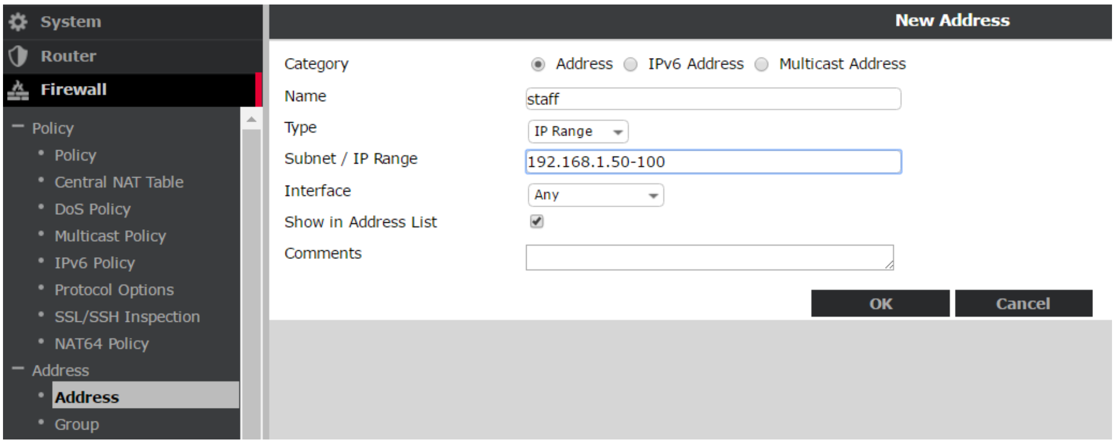
b) Define the IP address of SIP. Set **Name** to **sip** and set **Subnet/IP Range** to **192.168.1.20**.



New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	sip
Type	Subnet
Subnet / IP Range	192.168.1.120
Interface	Any
Show in Address List	☑
Comments	

c) Define the IP address of the staff's PC. Set **Name** to **staff** and set **Subnet/IP Range** to **192.168.1.50-100**.

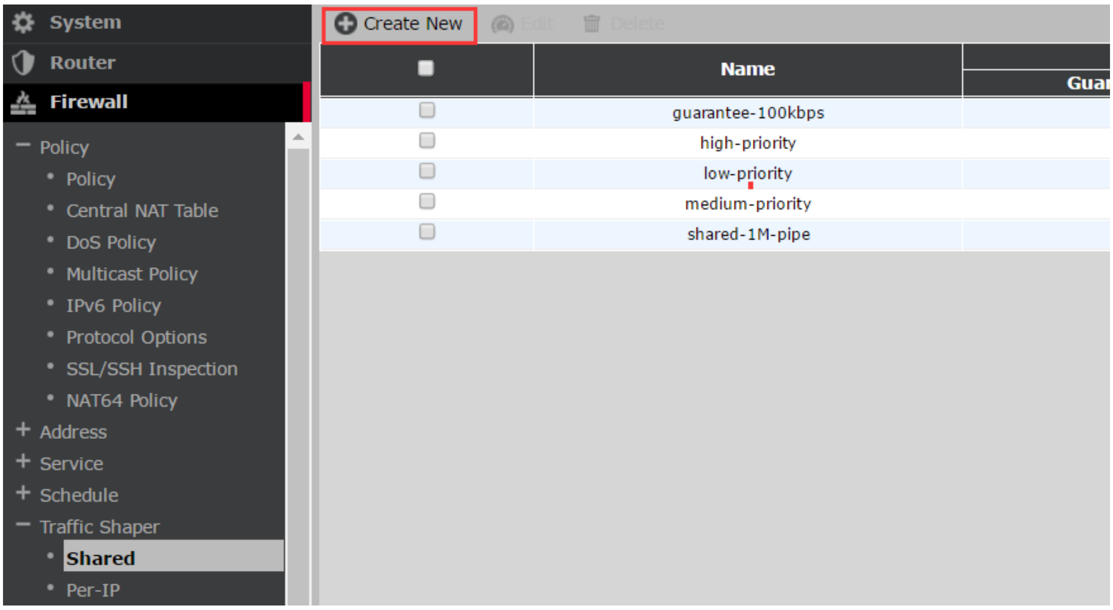


New Address

Category	● Address ○ IPv6 Address ○ Multicast Address
Name	staff
Type	IP Range
Subnet / IP Range	192.168.1.50-100
Interface	Any
Show in Address List	☑
Comments	

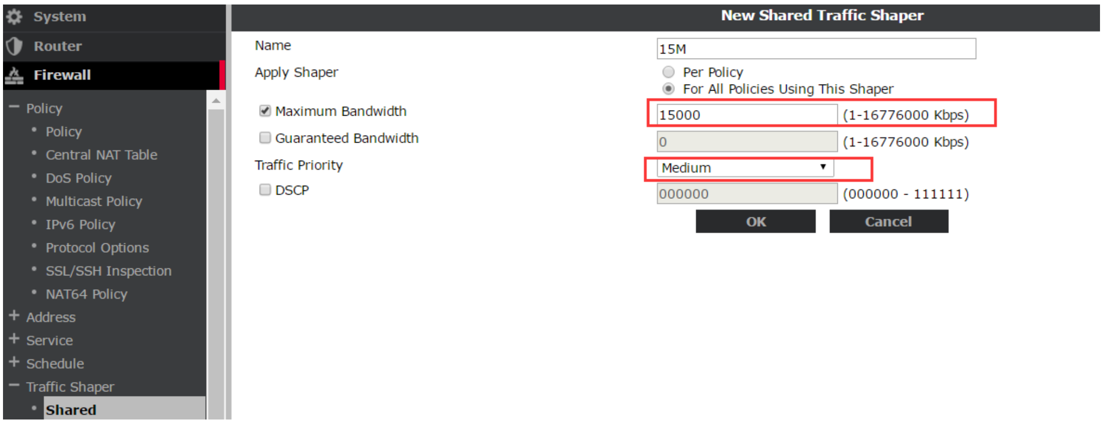
3. Define the traffic shaper.

Choose **Firewall** > **Traffic Shaper** > **Shared**, and then click **Create New**.



□	Name	Guar
□	guarantee-100kbps	
□	high-priority	
□	low-priority	
□	medium-priority	
□	shared-1M-pipe	

a) Create a 15 Mbps shared traffic shaper.



New Shared Traffic Shaper

Name: 15M

Apply Shaper: ○ Per Policy ● For All Policies Using This Shaper

☑ Maximum Bandwidth: 15000 (1-16776000 Kbps)

□ Guaranteed Bandwidth: 0 (1-16776000 Kbps)

Traffic Priority: Medium

□ DSCP: 000000 (000000 - 111111)

OK Cancel

Name: It is user-defined for identification.

Apply Shaper: Set how the flow control script is applied by the policy.

Per Policy: Each policy that uses the traffic shaper to control flow independently. For example, if 10 policies use the 15 Mbps flow control script, each policy can use 15 Mbps bandwidth.

For All Policies Using This Shaper: All the policies using this script control flows together. For example, if 10 policies use the 15 Mbps flow control script, all the users of the policy share 15 Mbps bandwidth.

That is, the maximum traffic used by the 10 policies is 15 Mbps.

Traffic Priority:

The firewall interface defines six FIFO queues, among which queue 0 has the highest priority while queue 5 has the lowest priority.

Queue 0 is used for firewall management and VPN negotiation. All the traffic sent or received by the firewall is automatically put into queue 0 and forwarded first.

For the traffic enabled with the traffic shaper in the policy and forwarded by the firewall, its priority is classified into high, medium, and low levels. The traffic with high level is forwarded by the firewall first. High, medium, and low priority levels are corresponding to queues 1, 2, and 3:

High (queue 1), medium (queue 2), low (queue 3).

Traffic priorities can be classified by service type. Set priorities of services such as VoIP to **high**, priorities of HTTP, POP3, SNTP, and OA services to **medium**, and priorities of other services to **low**.

If the priority level is not specified in the policy, the priority is high by default.

Maximum Bandwidth:

It indicates the maximum bandwidth that is allowed by the policy, and the unit is Kbps. When the traffic exceeds the threshold, the data packets that exceed the threshold will be discarded. Setting this value to 0 indicates that the maximum bandwidth is not restricted.

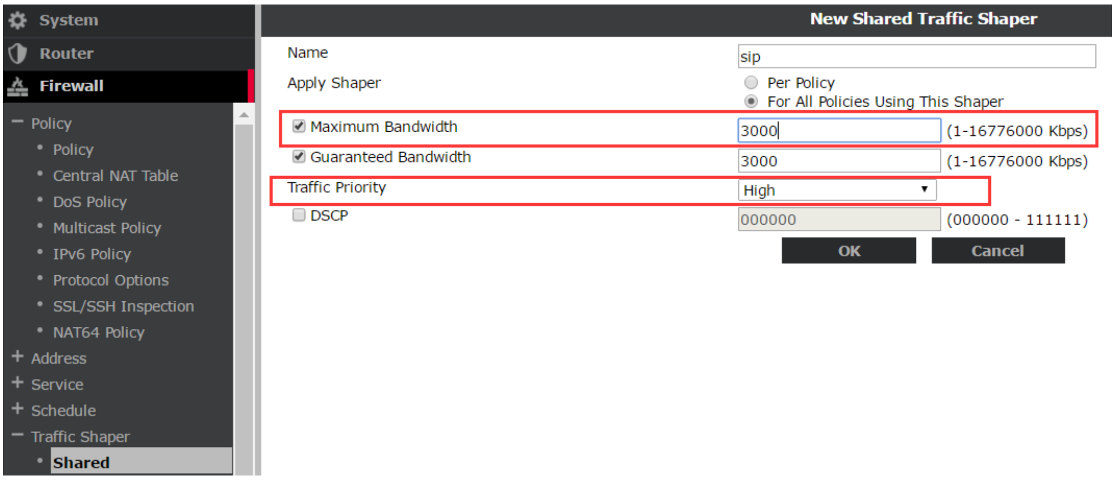
Guaranteed Bandwidth:

It indicates the bandwidth guaranteed by the policy. When the traffic is lower than the guaranteed bandwidth, data packets will be put into queue 0. That is, data packets will be forwarded first, thus ensuring that the service occupies the lowest bandwidth. Setting the parameter for non-critical business is not recommended.

When the policy bandwidth is between the maximum bandwidth and guaranteed bandwidth, data packets are forwarded according to the priority defined in the policy.

DSCP: It determines whether to use differentiated services code point (DSCP), which is used to configure point-to-point QoS services on the entire network.

b) Create a 3 Mbps traffic shaper for voice and video.

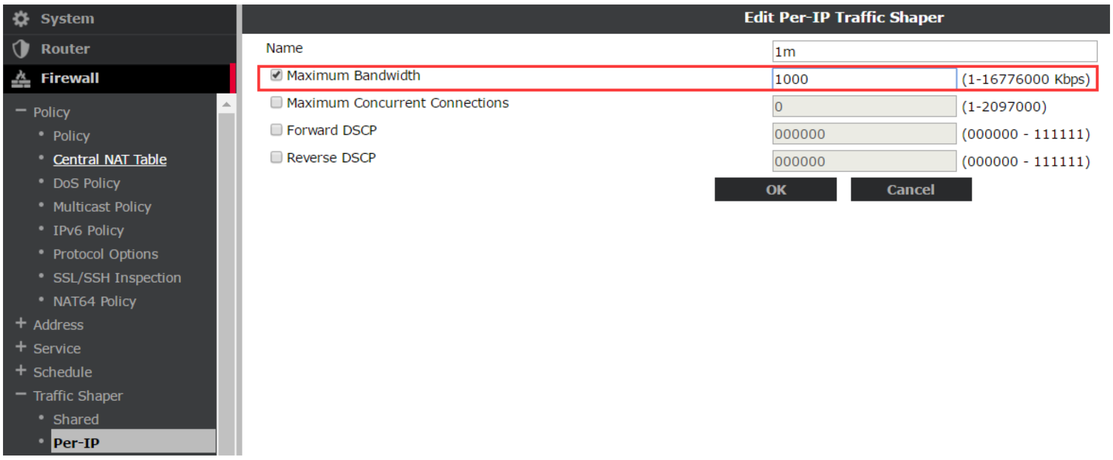


New Shared Traffic Shaper

Name	sip	
Apply Shaper	○ Per Policy ● For All Policies Using This Shaper	
☑ Maximum Bandwidth	3000	(1-16776000 Kbps)
☑ Guaranteed Bandwidth	3000	(1-16776000 Kbps)
Traffic Priority	High	
□ DSCP	000000	(000000 - 111111)

c) Create a 1 Mbps per-IP traffic shaper.

Choose **Firewall** > **Traffic Shaper** > **Per-IP**.



Edit Per-IP Traffic Shaper

Name	1m	
☑ Maximum Bandwidth	1000	(1-16776000 Kbps)
□ Maximum Concurrent Connections	0	(1-2097000)
□ Forward DSCP	000000	(000000 - 111111)
□ Reverse DSCP	000000	(000000 - 111111)

Name: It is user-defined.

Maximum Bandwidth: It indicates the maximum bandwidth used by each IP address. It is the sum of the upstream and downstream traffic. Set it to 1000 Kbps.

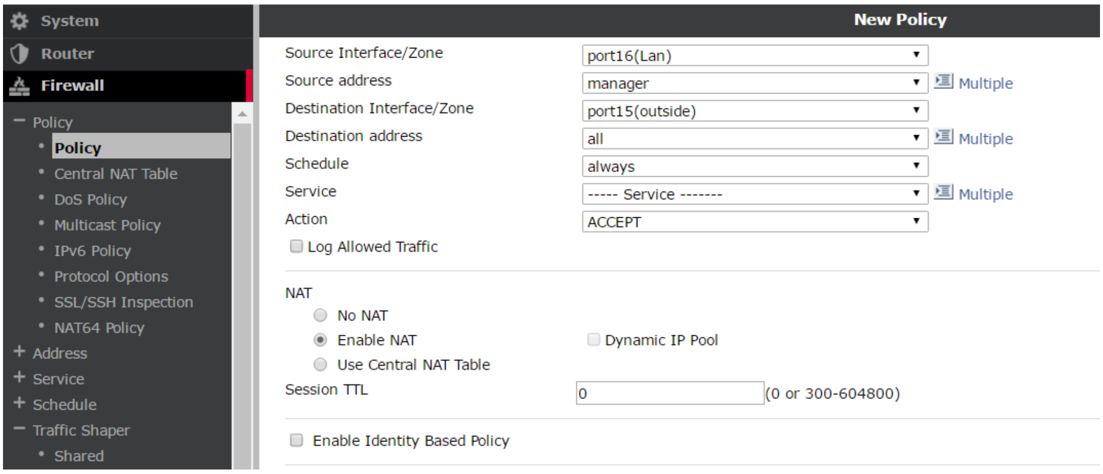
Maximum Concurrent Connections: It indicates the maximum number of connections that can be initiated by each user in the policy. If the maximum number of connections is exceeded, users cannot create a new connection.

Forward DSCP: It determines whether to use DSCP, which is used to configure point-to-point QoS services on the entire network.

Reverse DSCP: It determines whether to use DSCP, which is used to configure point-to-point QoS services on the entire network.

4. Configure policies and enable traffic control.

a) Add a policy for leaders to access the Internet without any restriction.



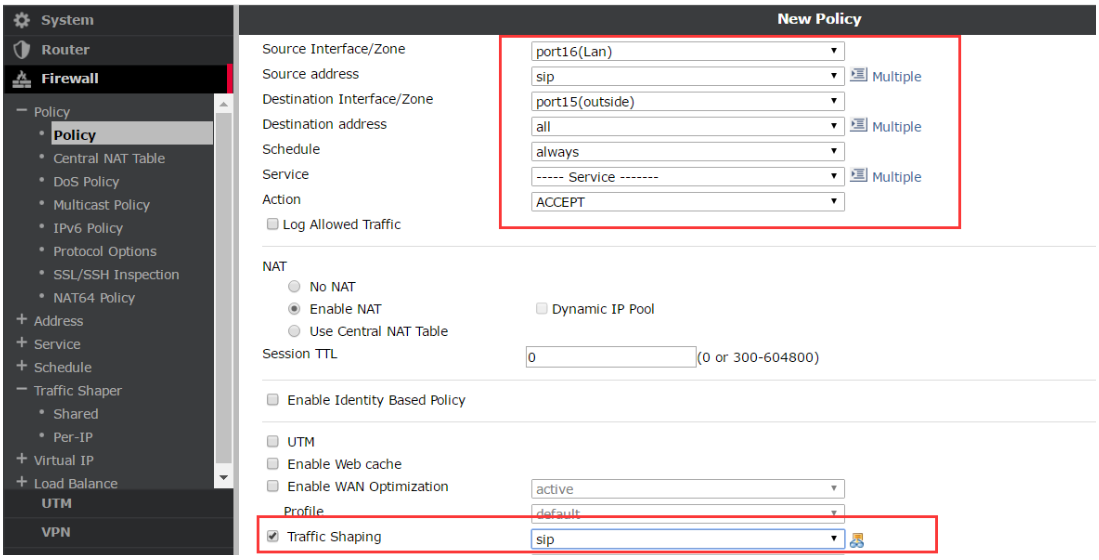
New Policy

Source Interface/Zone: port16(Lan)
Source address: manager — Multiple
Destination Interface/Zone: port15(outside)
Destination address: all — Multiple
Schedule: always
Service: ----- Service ------- — Multiple
Action: ACCEPT
□ Log Allowed Traffic

NAT
○ No NAT
● Enable NAT — □ Dynamic IP Pool
○ Use Central NAT Table
Session TTL: 0 (0 or 300-604800)

□ Enable Identity Based Policy

b) Add a policy for SIP to use the traffic shaping policy.



New Policy

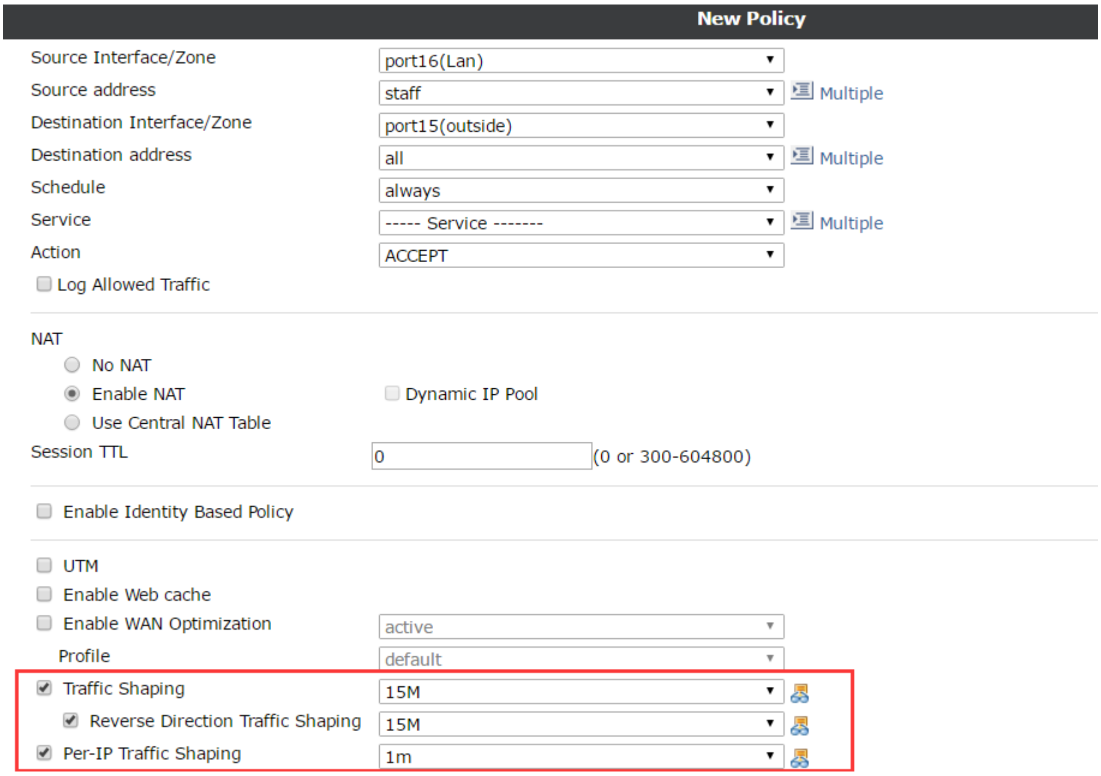
Source Interface/Zone: port16(Lan)
Source address: sip — Multiple
Destination Interface/Zone: port15(outside)
Destination address: all — Multiple
Schedule: always
Service: ----- Service ------- — Multiple
Action: ACCEPT
□ Log Allowed Traffic

NAT
○ No NAT
● Enable NAT — □ Dynamic IP Pool
○ Use Central NAT Table
Session TTL: 0 (0 or 300-604800)

□ Enable Identity Based Policy

□ UTM
□ Enable Web cache
□ Enable WAN Optimization: active
Profile: default
☑ Traffic Shaping: sip

c) Add a policy for the staff to access the Internet.



New Policy

Source Interface/Zone	port16(Lan)
Source address	staff (Multiple)
Destination Interface/Zone	port15(outside)
Destination address	all (Multiple)
Schedule	always
Service	----- Service ------- (Multiple)
Action	ACCEPT

□ Log Allowed Traffic

NAT

○ No NAT

● Enable NAT — □ Dynamic IP Pool

○ Use Central NAT Table

Session TTL: 0 (0 or 300-604800)

□ Enable Identity Based Policy

□ UTM

□ Enable Web cache

□ Enable WAN Optimization: active

Profile: default

☑ Traffic Shaping: 15M

☑ Reverse Direction Traffic Shaping: 15M

☑ Per-IP Traffic Shaping: 1m

Note: Reverse Direction Traffic Shaping: This option is used to control the download traffic. After you enable it, the upload and download traffic is separately controlled. The upload and download rates are respectively 15 Mbps. If you disable this option, the sum of upload and download rates is 15 Mbps.

V. Verification

Download via FTP or observe rate via speedtest. If you choose Per-IP Traffic Shaping, the sessions that exceed the limit are blocked and you cannot access the Internet. According to a test, the rate is 4-6 Mbps when Per-IP Traffic Shaping is disabled; the rate is lowered to around 1 Mbps when Per-IP Traffic Shaping is enabled.

VI. Notes

Q: Because per-IP does not respectively restrict upload and download rates, is there any problem during actual application?

A: Generally, there is no problem. In the preceding example, upload and download rates are not restricted separately.

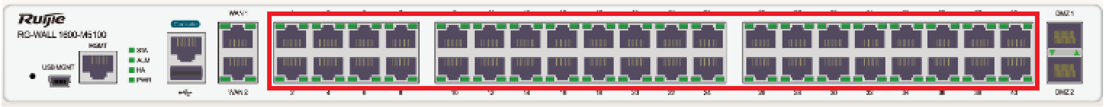
7.3 Converting Interface Attribute

7.3.1.1 Converting the Interface Attribution for M5100

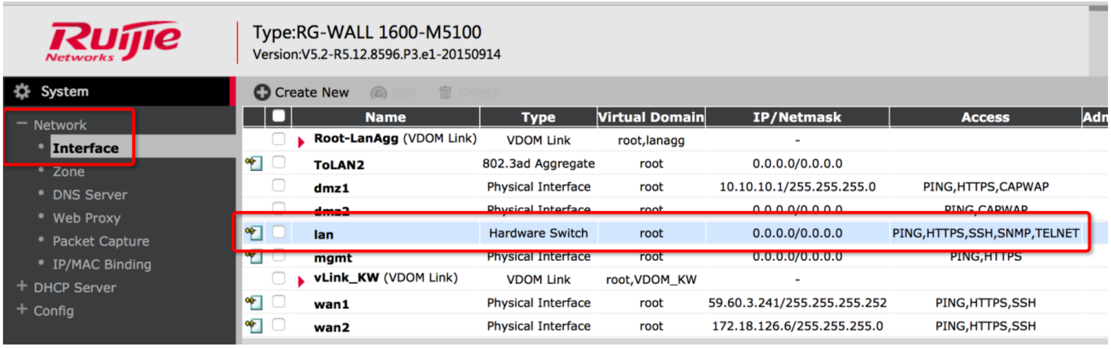
M5100 Switching Interface

The M5100 has 48 switching interfaces. One or more of the LAN interfaces can be split into independent routing interfaces as needed. As compared with the S3100 and S3600, the M5100 is used more flexibly.

You can split the switching interfaces of the M5100 on a Web interface or CLI. It is recommended that you perform the configurations on a Web interface.



After logging in to the M5100, you can only view LAN interfaces, but not specific switching interfaces.



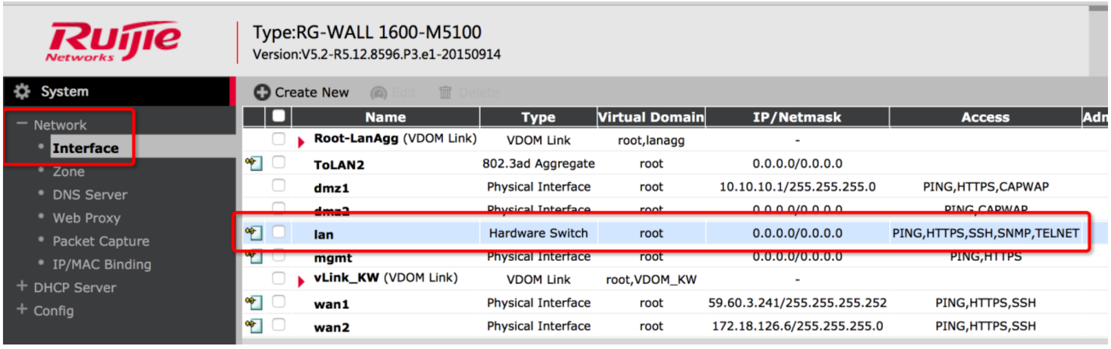
Type:RG-WALL 1600-M5100
Version:V5.2-R5.12.8596.P3.e1-20150914

Name	Type	Virtual Domain	IP/Netmask	Access	Adr
Root-LanAgg (VDOM Link)	VDOM Link	root,lanagg	-		
ToLAN2	802.3ad Aggregate	root	0.0.0.0/0.0.0.0		
dmz1	Physical Interface	root	10.10.10.1/255.255.255.0	PING,HTTPS,CAPWAP	
dmz2	Physical Interface	root	0.0.0.0/0.0.0.0	PING,CAPWAP	
lan	Hardware Switch	root	0.0.0.0/0.0.0.0	PING,HTTPS,SSH,SNMP,TELNET	
mgmt	Physical Interface	root	0.0.0.0/0.0.0.0	PING,HTTPS	
vLink_KW (VDOM Link)	VDOM Link	root,VDOM_KW	-		
wan1	Physical Interface	root	59.60.3.241/255.255.255.252	PING,HTTPS,SSH	
wan2	Physical Interface	root	172.18.126.6/255.255.255.0	PING,HTTPS,SSH	

Method 1: Configuration via Web Interface

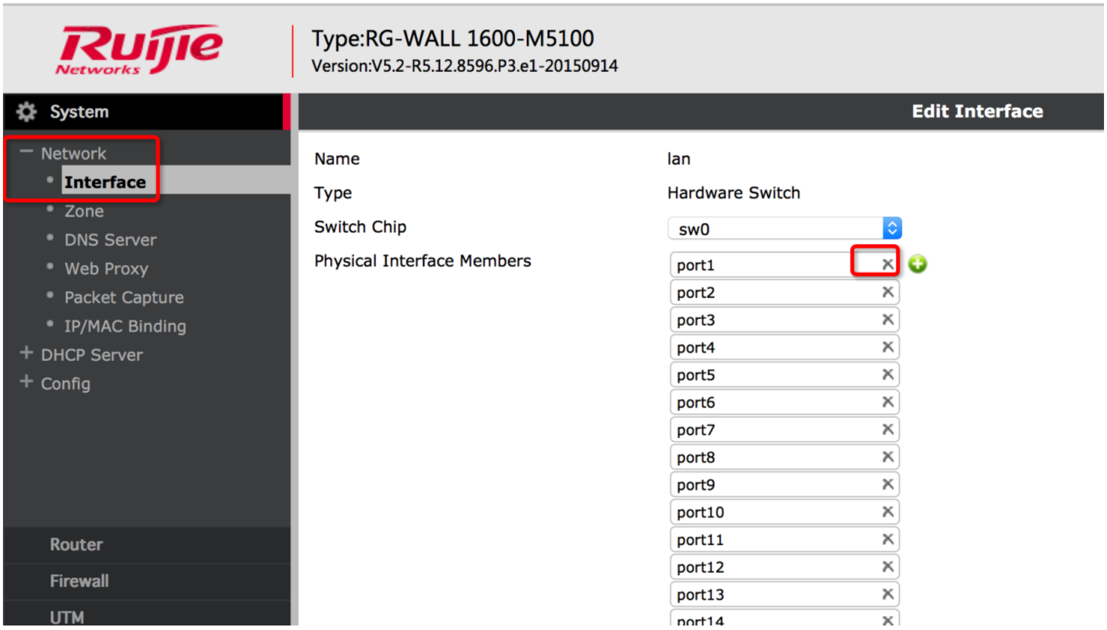
1) Set the routing interface

Step 1: Choose the **System** > **Network** > **Interface** menu, click **Edit Interface**.


Type:RG-WALL 1600-M5100
Version:V5.2-R5.12.8596.P3.e1-20150914

Name	Type	Virtual Domain	IP/Netmask	Access	Adr
Root-LanAgg (VDOM Link)	VDOM Link	root,lanagg	-		
ToLAN2	802.3ad Aggregate	root	0.0.0.0/0.0.0.0		
dmz1	Physical Interface	root	10.10.10.1/255.255.255.0	PING,HTTPS,CAPWAP	
dmz2	Physical Interface	root	0.0.0.0/0.0.0.0	PING,CAPWAP	
lan	Hardware Switch	root	0.0.0.0/0.0.0.0	PING,HTTPS,SSH,SNMP,TELNET	
mgmt	Physical Interface	root	0.0.0.0/0.0.0.0	PING,HTTPS	
vLink_KW (VDOM Link)	VDOM Link	root,VDOM_KW	-		
wan1	Physical Interface	root	59.60.3.241/255.255.255.252	PING,HTTPS,SSH	
wan2	Physical Interface	root	172.18.126.6/255.255.255.0	PING,HTTPS,SSH	

Step 2: For an interface that will be split into independent routing interfaces, click the small **X** after it, and click **OK**.

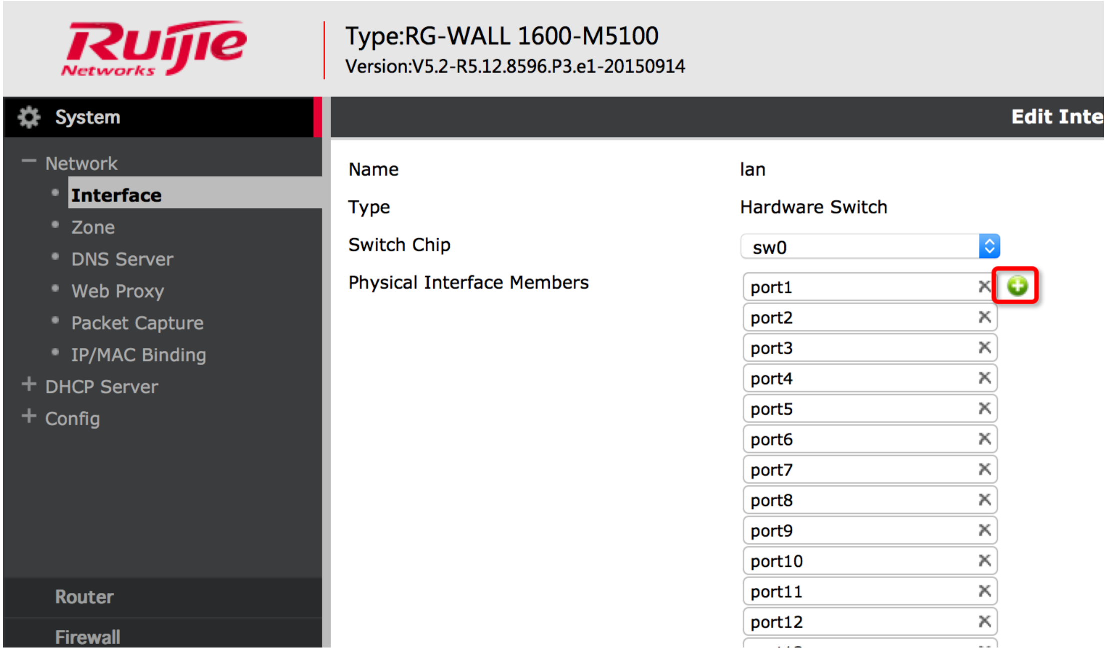


Type:RG-WALL 1600-M5100
Version:V5.2-R5.12.8596.P3.e1-20150914

Name	lan
Type	Hardware Switch
Switch Chip	sw0
Physical Interface Members	port1 port2 port3 port4 port5 port6 port7 port8 port9 port10 port11 port12 port13 port14

2) Cancel routing interfaces, and return them to the lan switching interface

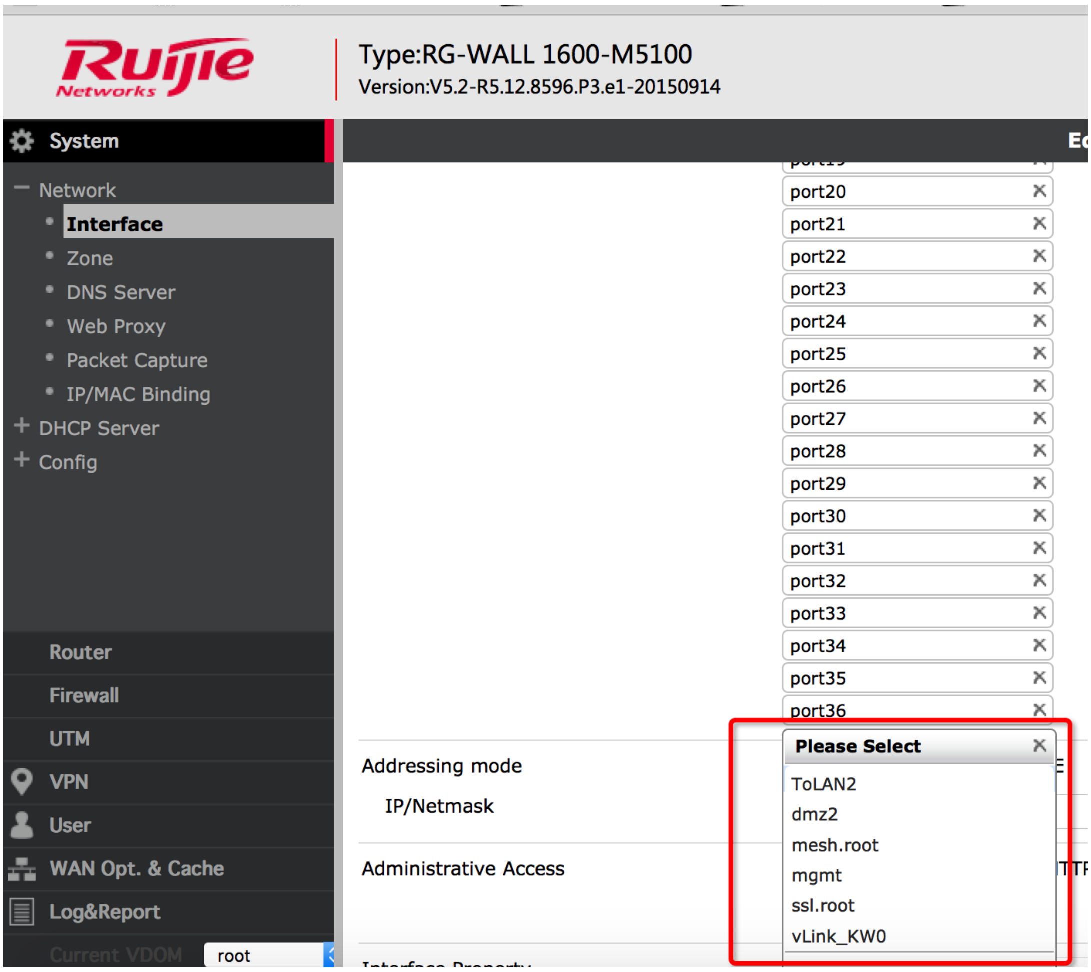
Step 1: Choose the **System** > **Network** > **Interface** > **Edit Interface** menu, and click the ⊕ .



Type:RG-WALL 1600-M5100
Version:V5.2-R5.12.8596.P3.e1-20150914

Name	lan
Type	Hardware Switch
Switch Chip	sw0
Physical Interface Members	port1 port2 port3 port4 port5 port6 port7 port8 port9 port10 port11 port12

Step 2: Select the interfaces that will be returned to the switching interface, and click **OK**.



A lan interface cannot be deleted on a Web interface, and it comprises at least two physical interface (as an integral part of the lan interface, the remaining two interfaces cannot be removed).

Method 2: Configurations via CLI

Step 1. Delete the internal associated interfaces

To split an internal interface into multiple independent routing interfaces, you need to delete all configurations associated with the internal interface. Otherwise, the system displays the following error prompt:

```
intf lan is used
```

The associated configurations to be deleted include the following content:

(1) Firewall policy: For example, the internal interface is configured as a source or destination interface.

(2) Static route: Delete the route entries related to the internal interface.

(3) DHCP service.

(4) IPsec and VIP.

(5) address objects.

Check command:

```
RG-WALL # diagnose sys checkused system.interface.name lan    // Check the use of the
internal interface in the configurations.
entry used by table system.dhcp.server:id ’1’
entry used by child table srcintf:name ’lan’ of table firewall.policy:policyid ’1’
```

Delete the associated configurations one by one according to the above results.

Step 2: Switch the working mode of the internal interface

Before performing the switching operation, it is recommended that you upgrade the current version to P2. If you perform the switching operation under the P1 version, you need to enter **print cliovrd enabl4e** and press **Enter**; after logging in and then logging out, execute the following command.

You can execute the following command to switch the working mode of the internal interface:

```
RG-WALL # config system virtual-switch
RG-WALL (virtual-switch) #delete lan
RG-WALL (virtual-switch) #end
```

Step 3. Verification

After interface switching is complete, log in to the network interface configuration page. Then, you can see that all lan interface are split into routing interfaces.

7.4 Configuring LACP

Application Scenarios

Port aggregation is supported by high-end devices, but not supported by the S3100 and S3600.

1. When bandwidths are limited, bandwidths can be expanded to be n times as much as the original links via logical aggregation;

2. If links need to be backed up dynamically, link aggregation can be configured to ensure that the member ports in the same aggregation group are dynamically backed up by each other.

LACP Modes

LACP ports support the following modes: static, passive and active.

Static: The aggregation group is configured manually; the system is not allowed to automatically add or delete any manual or static aggregated port.

Passive: A port in passive mode will not actively send LACPDU packets, and enters a protocol computation state after receiving the LACP packets sent by the peer.

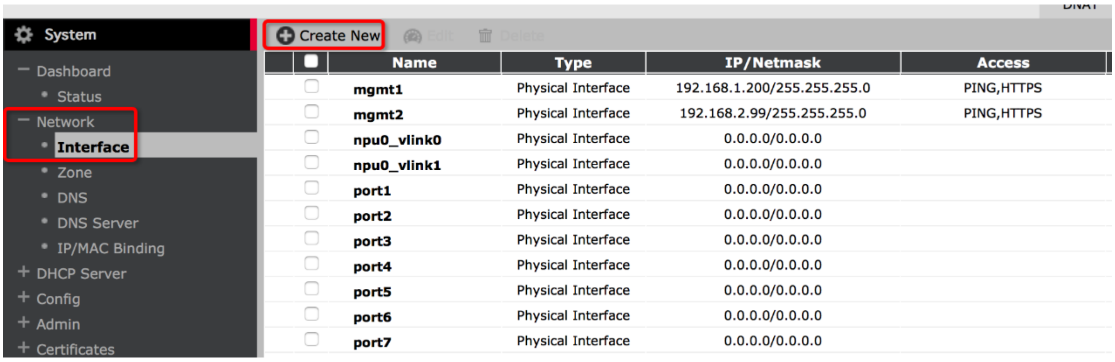
Active: A port in active mode will actively send LACPDU packets to the peer to perform PACP computation.

It is recommended that one of the interconnected two devices should be active and the other of them should be passive.

Configuration Steps

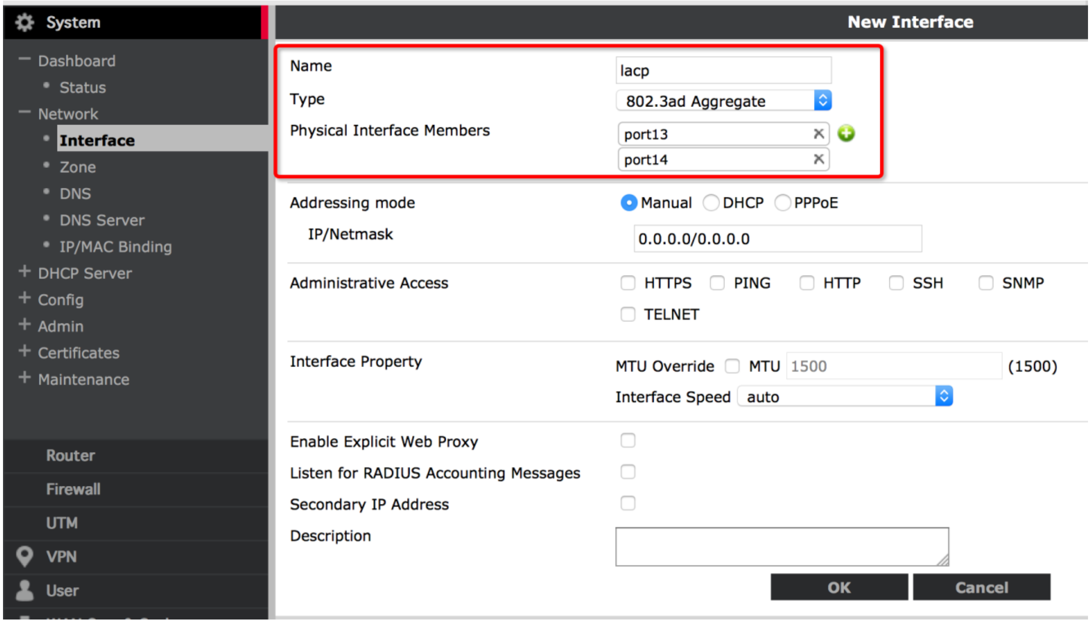
Step 1: Add aggregated ports

In the configuration page, choose the **System** > **Network** > **Interface** > **Create New** menu.



☐	Name	Type	IP/Netmask	Access
☐	mgmt1	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS
☐	mgmt2	Physical Interface	192.168.2.99/255.255.255.0	PING,HTTPS
☐	npu0_vlink0	Physical Interface	0.0.0.0/0.0.0.0	
☐	npu0_vlink1	Physical Interface	0.0.0.0/0.0.0.0	
☐	port1	Physical Interface	0.0.0.0/0.0.0.0	
☐	port2	Physical Interface	0.0.0.0/0.0.0.0	
☐	port3	Physical Interface	0.0.0.0/0.0.0.0	
☐	port4	Physical Interface	0.0.0.0/0.0.0.0	
☐	port5	Physical Interface	0.0.0.0/0.0.0.0	
☐	port6	Physical Interface	0.0.0.0/0.0.0.0	
☐	port7	Physical Interface	0.0.0.0/0.0.0.0	

Type: 802.3ad aggregation; select **Physical Interface**;



New Interface

Name	lacp
Type	802.3ad Aggregate
Physical Interface Members	port13 port14
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	0.0.0.0/0.0.0.0
Administrative Access	☐ HTTPS ☐ PING ☐ HTTP ☐ SSH ☐ SNMP ☐ TELNET
Interface Property	MTU Override ☐ MTU 1500 (1500) Interface Speed auto
Enable Explicit Web Proxy	☐
Listen for RADIUS Accounting Messages	☐
Secondary IP Address	☐
Description	

Step 2: Modify the LACP

```
RG-WALL # config system interface
RG-WALL (interface) # edit lacp
RG-WALL (lacp) # set lacp-mode static           // Configure the mode of LACP negotiation:
active, passive or static (dynamic by default)
RG-WALL (lacp) # set algorithm L3               // Load balancing algorithm L3: Hash
algorithm based on IP addresses; L4: Hash algorithm based on Layer 4
RG-WALL (lacp) # end

After the configurations are complete, check the configurations of the aggregated ports,
and check the established soft switching interface on the interface configuration page.
Note: The corresponding physical ports will disappear on the Web interface or CLI, and are
not configurable.

Execute the command below to check the configurations:
RG-WALL # show system interface lacp
config system interface
    edit "lacp"
        set vdom "root"
        set type aggregate
        set member "port13" "port14"
        set description "    "
        set snmp-index 51
        set lacp-mode static
        set algorithm L3
    next
end
```

The commands above are the logics and references configured on the CLI.

Verification

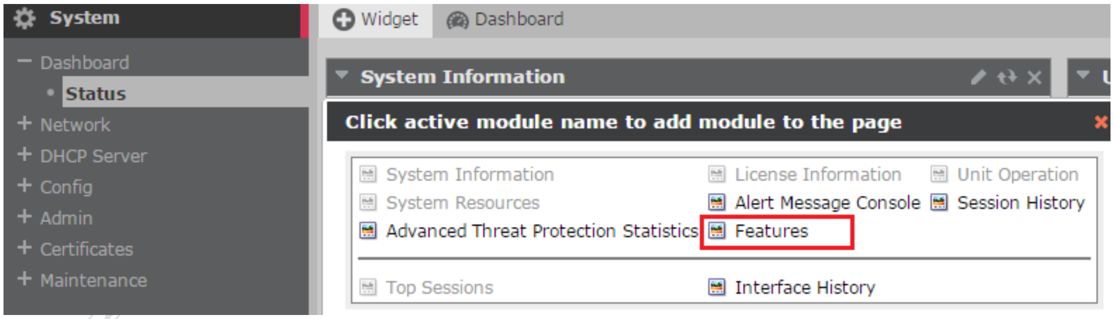
```
RG-WALL # diagnose netlink aggregate list
List of 802.3ad link aggregation interfaces:
 1  name lacp              status up    algorithm L3  lacp-mode static

RG-WALL # diagnose netlink  aggregate  name lacp
LACP flags: (A|P)(S|F)(A|I)(I|O)(E|D)(E|D)
(A|P) - LACP mode is Active or Passive
(S|F) - LACP speed is Slow or Fast
(A|I) - Aggregatable or Individual
```

```
(I|O) - Port In sync or Out of sync
(E|D) - Frame collection is Enabled or Disabled
(E|D) - Frame distribution is Enabled or Disabled

status: up
npu: y
flush: n
asic helper: y
oid: 135
ports: 2
ha: master
distribution algorithm: L4
LACP mode: active
LACP speed: slow
LACP HA: enable
aggregator ID: 1
actor key: 17
actor MAC address: 14:14:4b:7e:e1:69
partner key: 17
partner MAC address: 14:14:4b:7e:e1:67

slave: port13
  link status: up
  link failure count: 0
  permanent MAC addr: 14:14:4b:7e:e1:69
  LACP state: established
  actor state: ASAIEE                                   // Local status
  actor port number/key/priority: 1 17 255
  partner state: ASAIEE                                 // Peer status
  partner port number/key/priority: 1 17 255
  partner system: 65535 14:14:4b:7e:e1:67
  aggregator ID: 1
  speed/duplex: 1000 1
  RX state: CURRENT 6
  MUX state: COLLECTING_DISTRIBUTING 4

slave: port14
  link status: up
  link failure count: 0
  permanent MAC addr: 14:14:4b:7e:e1:68
  LACP state: established
  actor state: ASAIEE
  actor port number/key/priority: 2 17 255
  partner state: ASAIEE
  partner port number/key/priority: 2 17 255
  partner system: 65535 14:14:4b:7e:e1:67
  aggregator ID: 1
  speed/duplex: 1000 1
  RX state: CURRENT 6
MUX state: COLLECTING_DISTRIBUTING 4
```

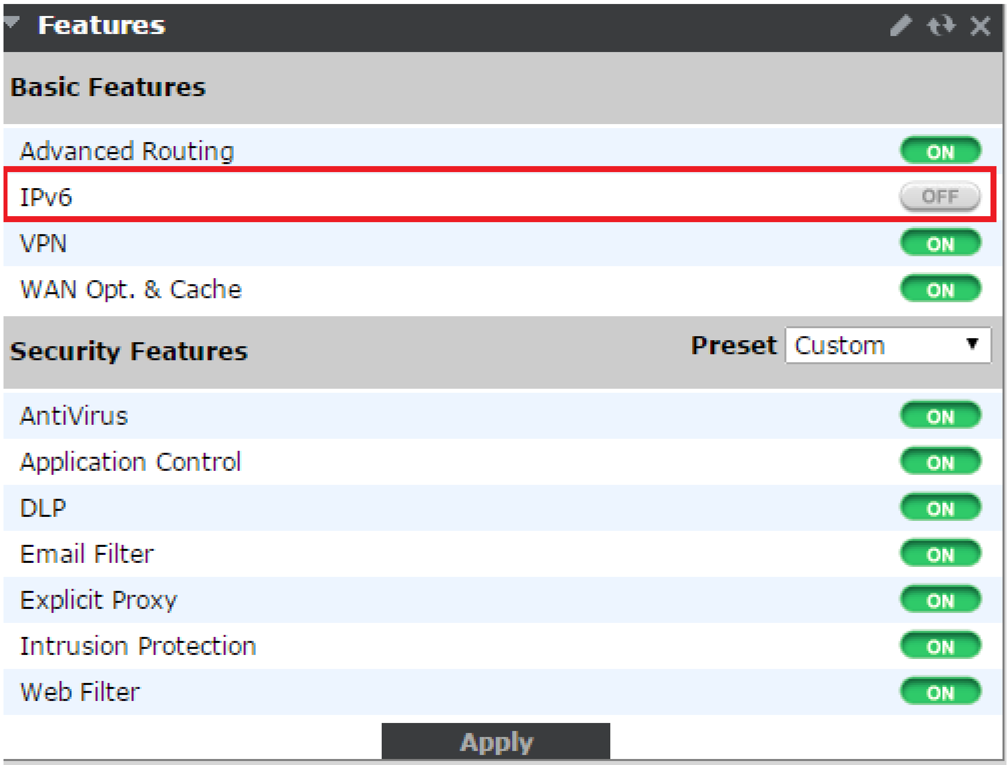
8 Configuring IPv6

8.1 Enabling IPv6 on the Web Page

Choose **System** > **Dashboard** > **Status**. Click **Widget**, and then click **Features**. See the following figure:



The following widgets of features are added. Click the button next to IPv6 to enable IPv6 configuration on the Web page. Click **Apply**.



Features

Basic Features

Advanced Routing	ON
IPv6	OFF
VPN	ON
WAN Opt. & Cache	ON

Security Features — Preset: Custom

AntiVirus	ON
Application Control	ON
DLP	ON
Email Filter	ON
Explicit Proxy	ON
Intrusion Protection	ON
Web Filter	ON

8.2 Configuring Internet Access

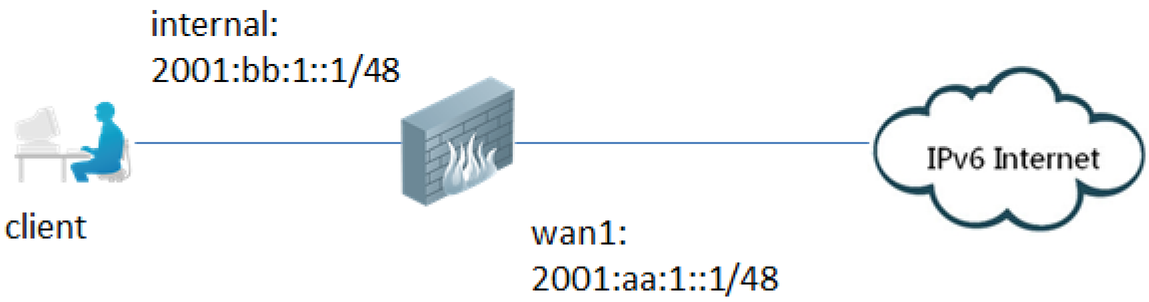
Networking Requirements

Intranet uses the IPv6 network. The RG-WALL firewall, as the Internet border access device of Intranet, enables Internet access.

The wan1 interface is connected to the Internet access service provider of IPv6 network.

The internal interface is connected to the IPv6 Intranet.

Network Topology

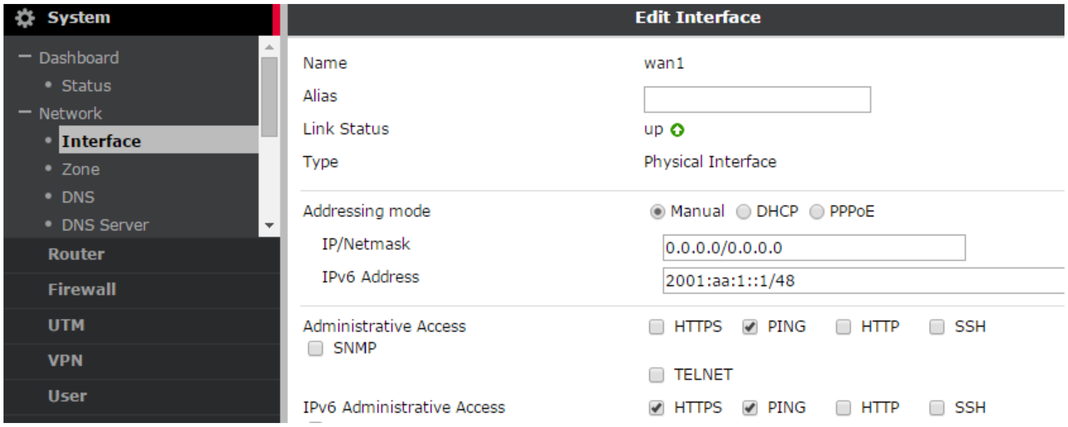


Configuration Tips

1. Configure IP addresses of interfaces.
2. Configure a route.
3. Configure the policy.
4. Configure UTM and flow control.

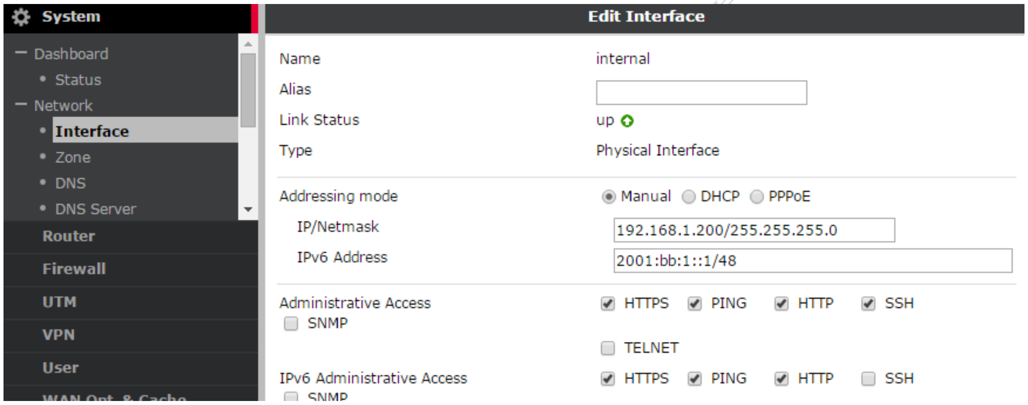
Configuration Steps

1. Configure IP addresses of interfaces.



Edit Interface

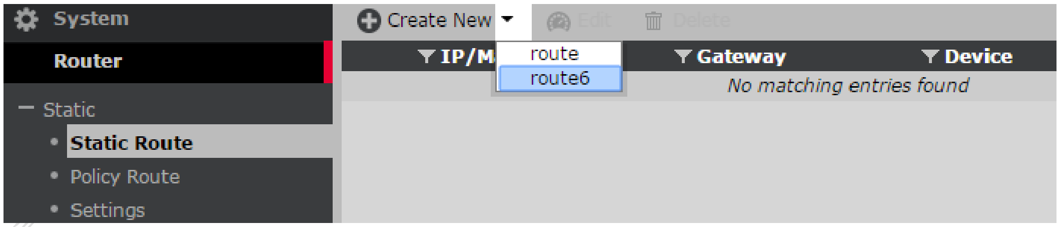
Name	wan1
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	0.0.0.0/0.0.0.0
IPv6 Address	2001:aa:1::1/48
Administrative Access □ SNMP	□ HTTPS ☑ PING □ HTTP □ SSH □ TELNET
IPv6 Administrative Access	☑ HTTPS ☑ PING □ HTTP □ SSH



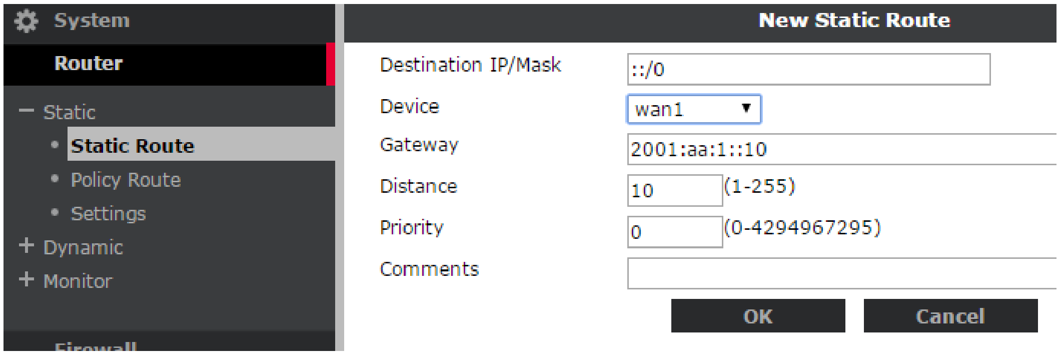
Edit Interface

Name	internal
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.1.200/255.255.255.0
IPv6 Address	2001:bb:1::1/48
Administrative Access	☑ HTTPS ☑ PING ☑ HTTP ☑ SSH □ SNMP □ TELNET
IPv6 Administrative Access	☑ HTTPS ☑ PING ☑ HTTP □ SSH □ SNMP

2. Configure a route.



No matching entries found



New Static Route

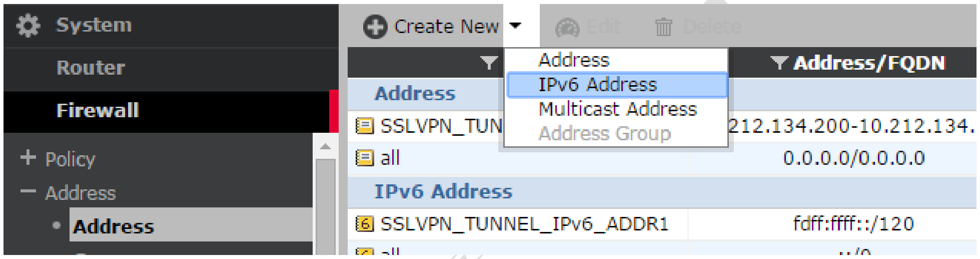
Destination IP/Mask	::/0
Device	wan1
Gateway	2001:aa:1::10
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

```
config router static6
    edit 1
        set gateway 2001:aa:1::10
        set device ″wan1″
    next
end
```

3. Configure the policy.

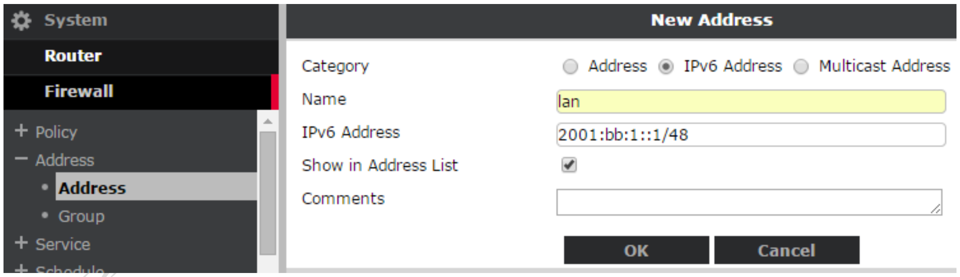
Define the IP address.

Choose **Firewall** > **Address** > **Address**, click **Create New**, and then choose **IPv6 Address**, as shown in the following figure:



	Address/FQDN
Address	
SSLVPN_TUN	212.134.200-10.212.134.
all	0.0.0.0/0.0.0.0
IPv6 Address	
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120

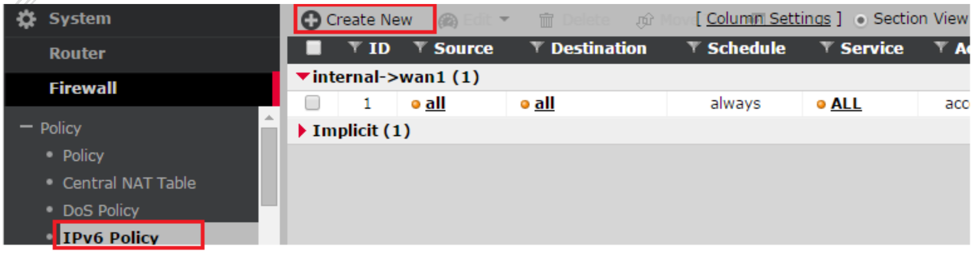
Edit address lan. The IPv6 address is 2001:bb:1::1/48. See the following figure:



New Address

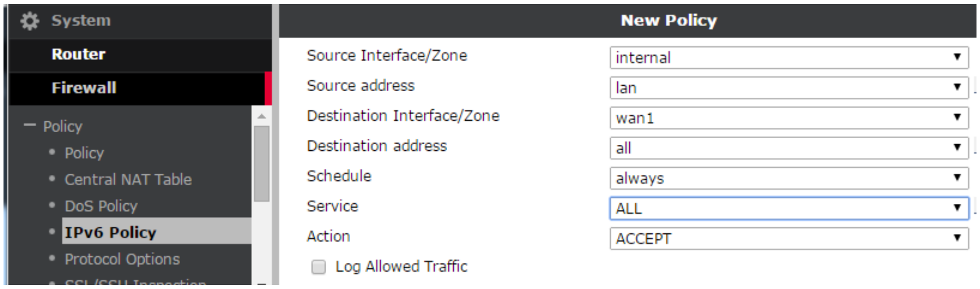
Category	○ Address ● IPv6 Address ○ Multicast Address
Name	lan
IPv6 Address	2001:bb:1::1/48
Show in Address List	☑
Comments	

Define the IPv6 policy.



	ID	Source	Destination	Schedule	Service	A
internal->wan1 (1)						
□	1	all	all	always	ALL	acc
Implicit (1)						

Define the policy to allow Intranet users to access the IPv6 network, as shown in the following figure:

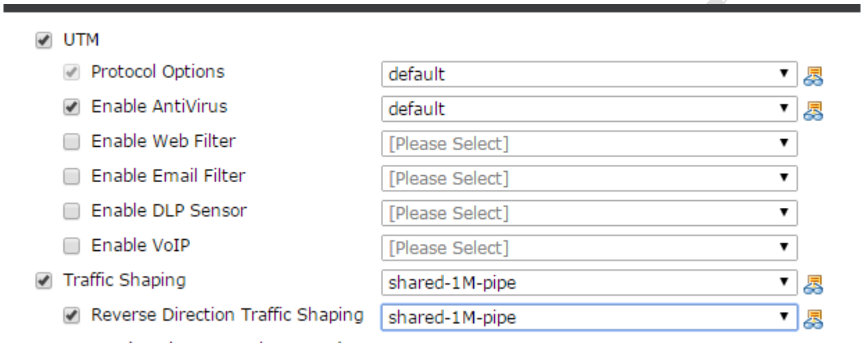


New Policy

Source Interface/Zone	internal
Source address	lan
Destination Interface/Zone	wan1
Destination address	all
Schedule	always
Service	ALL
Action	ACCEPT
□ Log Allowed Traffic	

4. Configure UTM and flow control.

Add UTM and flow control function to policy configuration. See the following figure:



☑ UTM

☑ Protocol Options: default ▼

☑ Enable AntiVirus: default ▼

□ Enable Web Filter: [Please Select] ▼

□ Enable Email Filter: [Please Select] ▼

□ Enable DLP Sensor: [Please Select] ▼

□ Enable VoIP: [Please Select] ▼

☑ Traffic Shaping: shared-1M-pipe ▼

☑ Reverse Direction Traffic Shaping: shared-1M-pipe ▼

Verification

The user can access the Internet successfully.

8.2.1 Configuring NAT64&DNS64

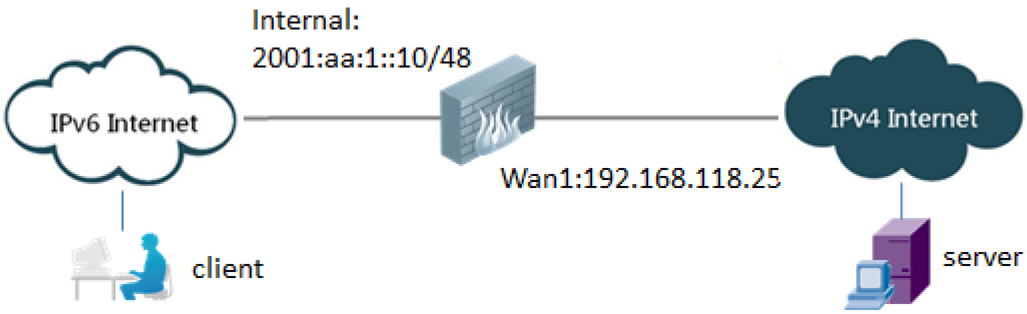
Networking Requirements

Intranet uses the IPv6 network. The RG-WALL firewall, as the Internet access border of Intranet, enables Internet access by NAT64.

The wan1 interface is connected to the Internet access service provider of IPv4 network.

The internal interface is connected to access the IPv6 Intranet.

Network Topology



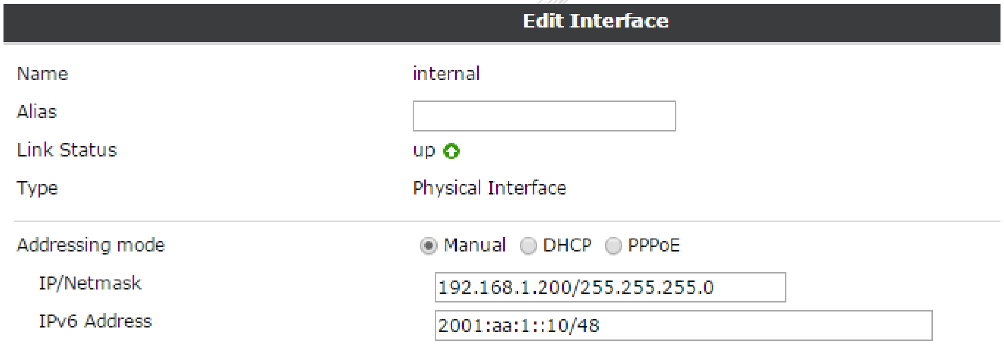
Configuration Tips

1. Configure IP addresses of interfaces.
2. Configure a route.
3. Configure the address pool.
4. Configure the policy.
5. Configure the DNS64.
6. Configure the PC.

Configuration Steps

1. Configure IP addresses of interfaces.

Choose **System** > **Network** > **Interface** > **Edit Interface**, as shown in the following figure:



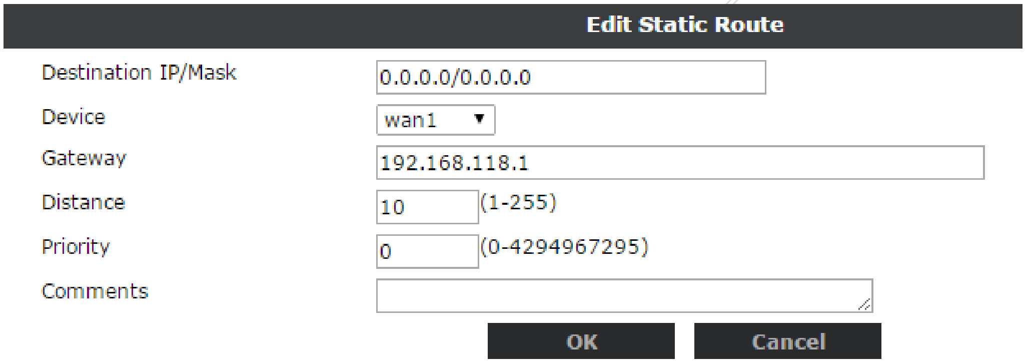
Edit Interface

Name	internal
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.1.200/255.255.255.0
IPv6 Address	2001:aa:1::10/48

```
config system interface
    edit ″internal″
        set vdom ″root″
set ip 192.168.1.200 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set description ″    ″
        set snmp-index 1
          config ipv6
        set ip6-address 2001:aa:1::10/48
        set ip6-send-adv enable
        config ip6-prefix-list
            edit 2001:db8:1::/48
                set autonomous-flag enable
                set onlink-flag enable
next
        end
end
Edit wan1 interface:
```

2. Configure a route.

Choose **Router** > **Static** > **Static Route**, and then click **Create New**, as shown in the following figure:



Edit Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan1 ▼
Gateway	192.168.118.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Destination IP/Mask: Keep the default value **0.0.0.0/0.0.0.0**.

Device: Choose **wan1**, which is associated with this route. It must be set correctly. Otherwise, the route cannot work.

Gateway: The IP address of the next hop, that is, the IP address of the peer carrier device.

Distance: The default value is 10. The route with a shorter distance will be written into the routing table.

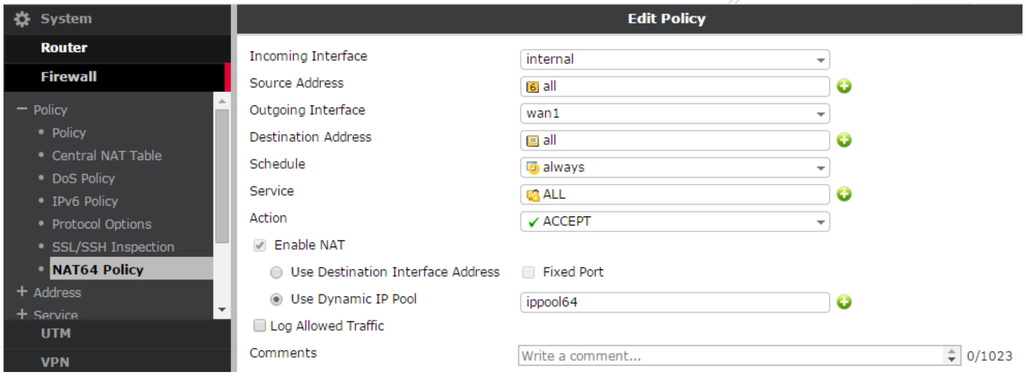
Priority: The default value is 0. The route with a smaller value is used preferably.

3. Configure the address pool.

```
         IPv4 address pool
config firewall ippool
    edit "ippool64"
        set startip 192.168.118.88
        set endip 192.168.118.90
    next
end

Configure the IPv6 address prefix in NAT64.
config system nat64
    set status enable
    set nat64-prefix 64:ff9b::/96
end
```

4. Configure the policy.

Choose **System** > **Firewall** > **Policy** > **NAT64 Policy**, as shown in the following figure:



Edit Policy

Incoming Interface	internal
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	✓ ACCEPT
☑ Enable NAT	
○ Use Destination Interface Address	□ Fixed Port
● Use Dynamic IP Pool	ippool64
□ Log Allowed Traffic	
Comments	Write a comment... 0/1023

CLI configuration is as follows:

```
config firewall policy64
    edit 1
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set ippool enable
        set poolname "ippool64"
    next
end
```

5. Configure the DNS64.

IPv6 Intranet users initiate AAAA record query. DNS64 (FGT) proxy server requests A record on the IPv4 network. After receiving the response of A record, DNS64 server converts A record to AAA, and then returns it to users.

```
config system nat64
    set status enable
    set nat64-prefix 64:ff9b::/96
set always-synthesize-aaaa-record enable  //Enabled by default.
end

config system dns-server           //Intranet interface is used as the DNS proxy.
    edit "internal"
        set mode forward-only
    next
end
config system dns                    //Set the DNS server for the system.
    set primary 8.8.8.8
end
```

6. **Configure the PC.**

DNS server address is the IP address of the internal interface. RG-WALL firewall acts as the DNS proxy server.

Verification

Ping the IP address 8.8.8.8. The prefix of NAT64 is 64:ff9b. Convert the IP4 address 8.8.8.8 into the hexadecimal IP address: 0808:0808.

```
C:\Users\Administrator>ping -6 64:ff9b::0808:0808
Pinging 64:ff9b::808:808 with 32 bytes of data:
Reply from 64:ff9b::808:808: Time = 63 ms
Reply from 64:ff9b::808:808: Time = 63 ms
```

Ping www.baidu.com.

```
C:\Users\Administrator>ping  -6 www.baidu.com
Pinging www.a.shifen.com [64:ff9b::774b:d96d] with 32 bytes of data:
Reply from 64:ff9b::774b:d96d: Time = 2 ms
Reply from 64:ff9b::774b:d96d: Time = 1 ms
```

Use a domain name to access IPv4 Internet through a browser.

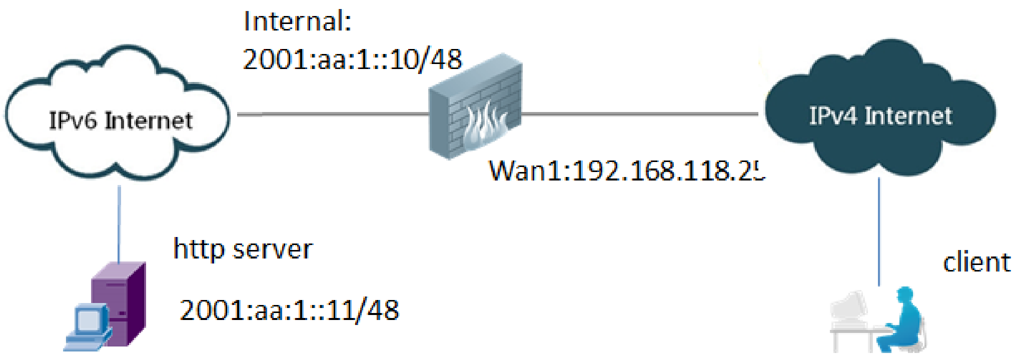
```
id=13 trace_id=142 msg=″vd-root received a packet(proto=58, 2001:bb:1::10:1->64:ff9b::808:808:128) from
internal.″
id=13 trace_id=142 msg=″vd-root received a packet(proto=58, 2001:bb:1::10:1->64:ff9b::808:808:128) from
internal.″
id=13 trace_id=142 msg=″allocate a new session-0000184e″
id=13 trace_id=142 msg=″find a route: gw-fe80::a5b:eff:fe6f:f7a6 via wan1 err 0 flags 00000003″
id=13 trace_id=142 msg=″Check policy between internal -> wan1″
id=13 trace_id=142 msg=″Allowed by Policy-1:″
id=13 trace_id=143 msg=″vd-root received a packet(proto=58, 64:ff9b::808:808:1->2001:bb:1::10:129) from wan1.″
id=13 trace_id=143 msg=″Find an existing session, id-0000184e, reply direction″
id=13 trace_id=143 msg=″vd-root received a packet(proto=58, 64:ff9b::808:808:1->2001:bb:1::10:129) from wan1.″
id=13 trace_id=143 msg=″Find an existing session, id-0000184e, reply direction″
```

8.2.2 Configuring VIP46 Mapping

Networking Requirements

Access the IPv6 internal server through the IPv4 network. Allow users to access the IPv6 internal server through 192.168.118.86.

Network Topology



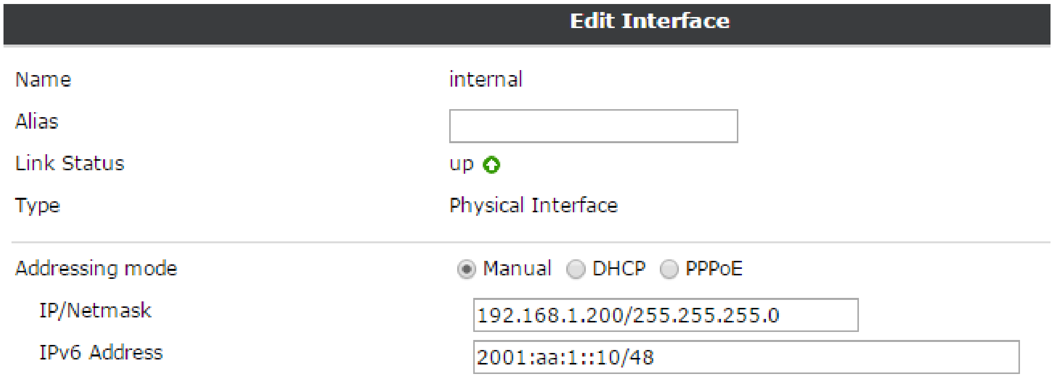
Configuration Tips

1. Basic configuration for Internet access
2. Configure the virtual IP address (DNAT).
3. Configure the security policy.
4. Enable NAT64.

Configuration Steps

1. Basic configuration

Choose **System** > **Network** > **Interface** > **Edit Interface**, as shown in the following figure:



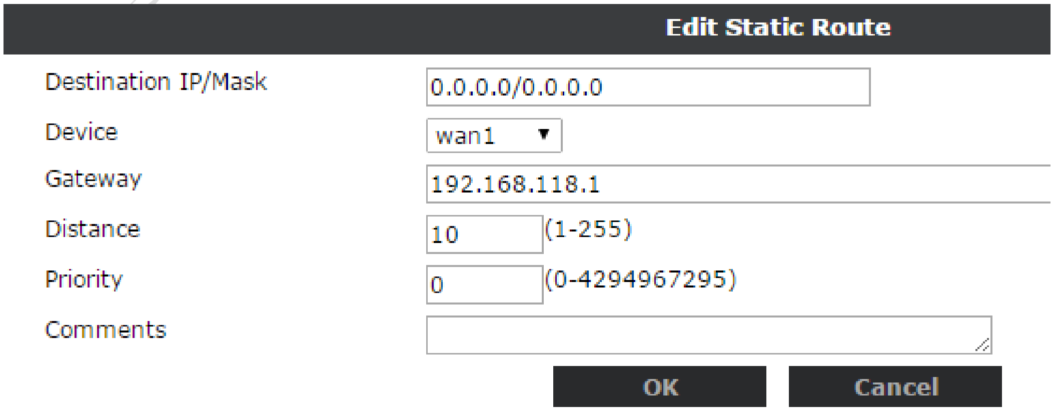
Edit Interface

Name	internal
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.1.200/255.255.255.0
IPv6 Address	2001:aa:1::10/48

```
config system interface
    edit ″internal″
        set vdom ″root″
        set ip 192.168.1.200 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set description ″    ″
        set snmp-index 1
          config ipv6
        set ip6-address 2001:aa:1::10/48
        set ip6-send-adv enable
        config ip6-prefix-list
            edit 2001:db8:1::/48
                set autonomous-flag enable
                set onlink-flag enable
next
        end
end
Edit wan1 interface:
```

2. **Configure a route.**

Choose **Router** > **Static** > **Static Route**, and then click **Create New**, as shown in the following figure:



Edit Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan1 ▼
Gateway	192.168.118.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Destination IP/Mask: Keep the default value **0.0.0.0/0.0.0.0**.

Device: Choose **wan1**, which is associated with this route. It must be set correctly. Otherwise, the route cannot work.

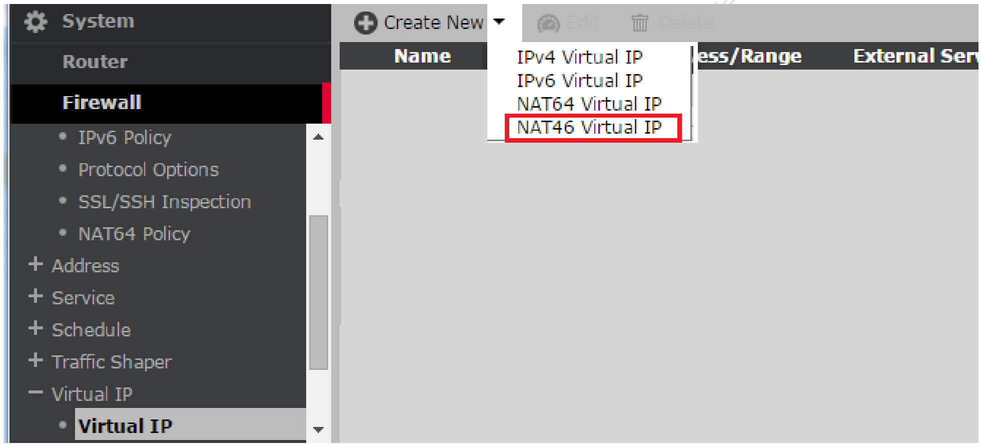
Gateway: The IP address of the next hop, that is, the IP address of the peer carrier device.

Distance: The default value is 10. The route with a shorter distance will be written into the routing table.

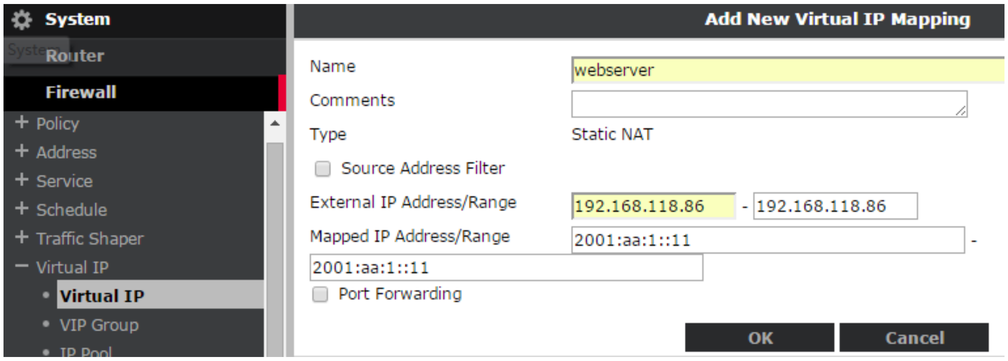
Priority: The default value is 0. The route with a smaller value is used preferably.

3. **Configure the virtual IP address (DNAT).**

   a) Choose **Firewall** > **Virtual IP** > **NAT46 Virtual IP**, as shown in the following figure:



b) Configure the virtual IP address, as shown in the following figure:



Name: webserver

Comments

Type: Static NAT

☐ Source Address Filter

External IP Address/Range: 192.168.118.86 - 192.168.118.86

Mapped IP Address/Range: 2001:aa:1::11 - 2001:aa:1::11

☐ Port Forwarding

```
config firewall vip46
    edit "webserver"
        set extip 192.168.118.86
        set mappedip 2001:aa:1::11
    next
end
```

4. Configure the policy.

```
config firewall policy46
    edit 1
        set srcintf "wan1"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "webserver"  // vip46
        set schedule "always"
        set service "all"
next
end
```

5. Enable NAT64.

```
config system nat64
    set status enable
end
```

Verification

The user can access https://192.168.118.86 successfully.

View the session:

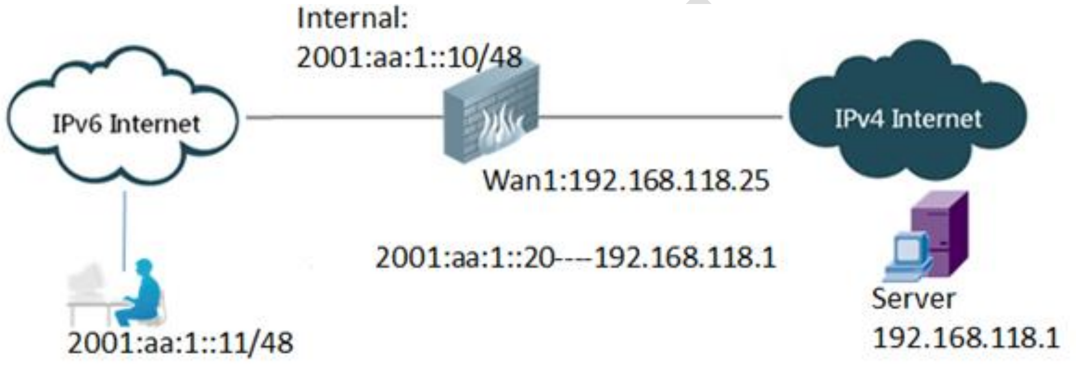
```
RG-WALL # diagnose  sys session  list
session info: proto=6 proto_state=05 duration=1 expire=0 timeout=3600 flags=00000000 sockflag=00000000
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty npu nlb
statistic(bytes/packets/allow_err): org=820/6/1 reply=389/6/1 tuples=2
orgin->sink: org pre->org, reply nataf->post dev=5->3/3->5 gwy=192.168.118.86/0.0.0.0
hook=pre dir=org act=dnat 10.10.69.80:55035->192.168.118.86:443(192.168.118.86:443)
hook=post dir=reply act=snat 192.168.118.86:443->10.10.69.80:55035(192.168.118.86:443)
hook=5 dir=org act=noop 64:ff9b::a0a:4550:55035 ->2001:aa:1::11:443(:::0)
hook=6 dir=reply act=noop 2001:aa:1::11:443 ->64:ff9b::a0a:4550:55035(:::0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=0000a00d tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
```

8.2.3 Configuring VIP64 Mapping

Networking Requirements

Map the server (IP address: 192.168.118.1) on the IPv4 network to 2001:aa:1::20 on the IPv6 network.

Network Topology



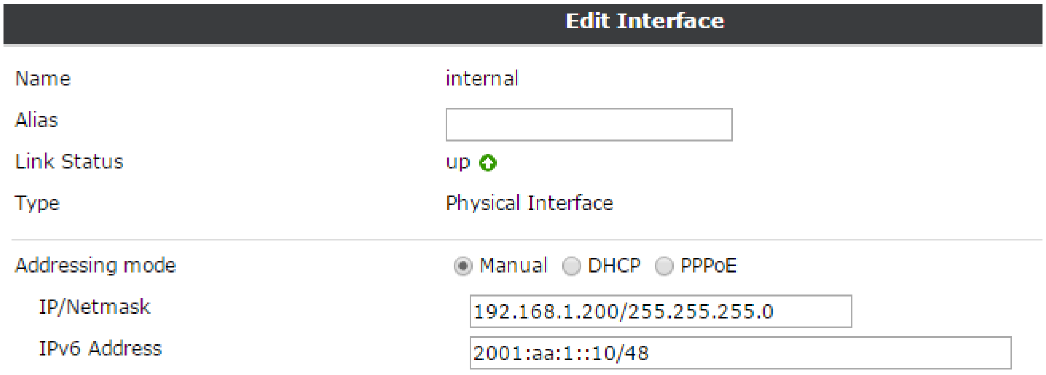
Configuration Tips

1. Basic configuration
2. Configure the virtual IP address (DNAT).
3. Configure the security policy.
4. Enable NAT64.

Configuration Steps

1. Basic configuration

Choose **System** > **Network** > **Interface** > **Edit Interface**, as shown in the following figure:



Edit Interface

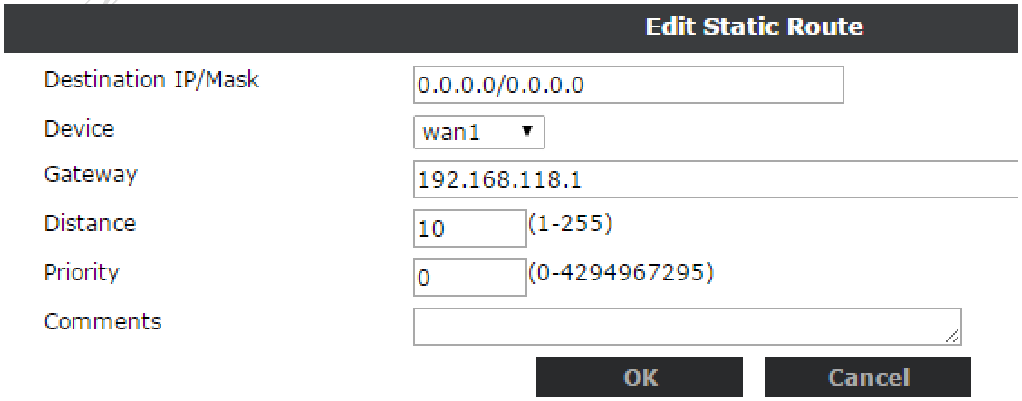
Name	internal
Alias	
Link Status	up
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Netmask	192.168.1.200/255.255.255.0
IPv6 Address	2001:aa:1::10/48

```
config system interface
    edit ″internal″
        set vdom ″root″
        set ip 192.168.1.200 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set description ″    ″
        set snmp-index 1
```

```
          config ipv6
        set ip6-address 2001:aa:1::10/48
        set ip6-send-adv enable
        config ip6-prefix-list
            edit 2001:db8:1::/48
                set autonomous-flag enable
                set onlink-flag enable
next
        end
end
Edit wan1 interface:
```

2. **Configure a route.**

Choose **Router** > **Static** > **Static Route**, and then click **Create New**, as shown in the following figure:



Edit Static Route

Destination IP/Mask: 0.0.0.0/0.0.0.0

Device: wan1

Gateway: 192.168.118.1

Distance: 10 (1-255)

Priority: 0 (0-4294967295)

Comments:

Destination IP/Mask: Keep the default value 0.0.0.0/0.0.0.0.

Device: Choose wan1, which is associated with this route. It must be set correctly. Otherwise, the route cannot work.

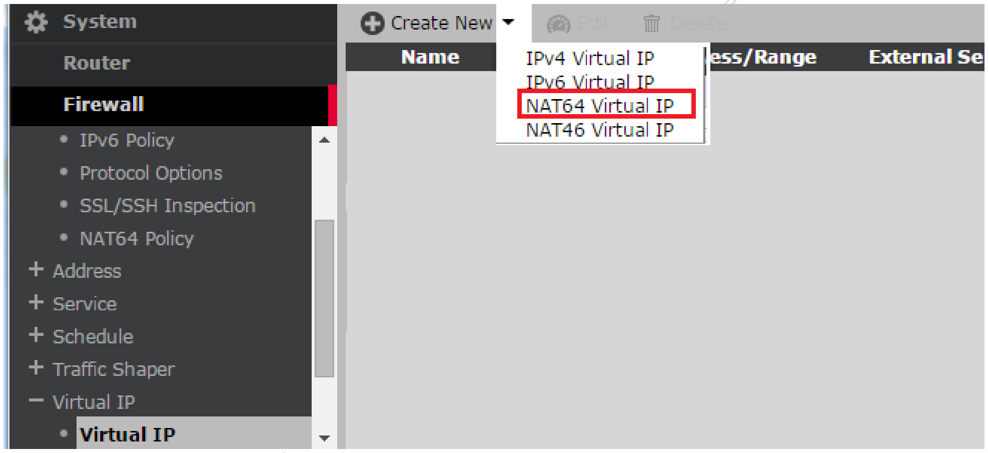
Gateway: The IP address of the next hop, that is, the IP address of the peer carrier device.

Distance: The default value is 10. The route with a shorter distance will be written into the routing table.

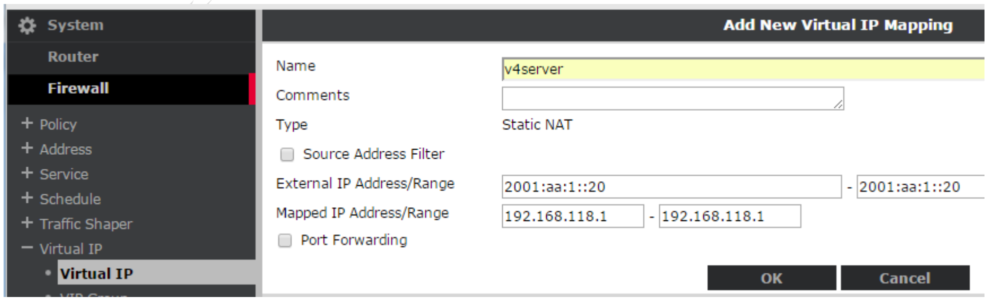
Priority: The default value is 0. The route with a smaller value is used preferably.

3. **Configure the virtual IP address (DNAT).**

    a) Choose **Firewall** > **Virtual IP** > **NAT46 Virtual IP**, as shown in the following figure:



b) Configure the virtual IP address, as shown in the following figure:



Add New Virtual IP Mapping

Name: v4server

Comments:

Type: Static NAT

□ Source Address Filter

External IP Address/Range: 2001:aa:1::20 - 2001:aa:1::20

Mapped IP Address/Range: 192.168.118.1 - 192.168.118.1

□ Port Forwarding

OK Cancel

```
config firewall vip64
    edit "v4server"
        set extip 2001:aa:1::20
        set mappedip 192.168.118.1
    next
end
```

4. **Configure the policy.**

```
config firewall policy64
    edit 2
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "v4server"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

5. **Enable NAT64.**

```
config system nat64
    set status enable
end
```

Verification

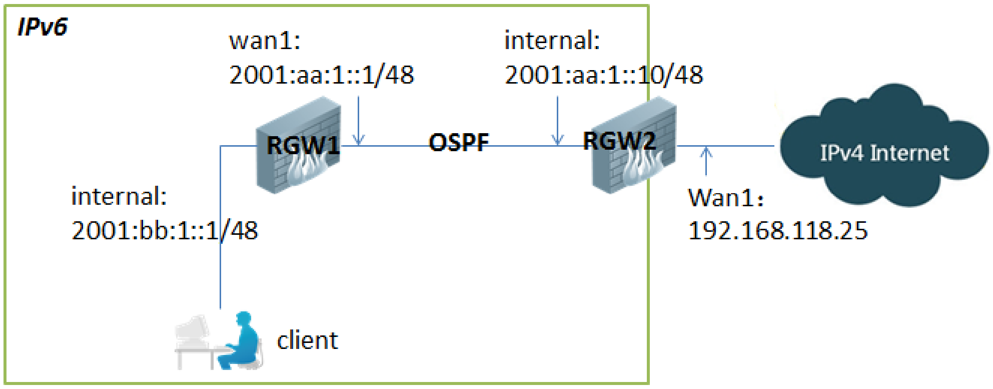
```
Telnet 2001:aa:1::20.
View the session:
RG-WALL # diagnose  sys session  list
session info: proto=6 proto_state=01 duration=2 expire=3598 timeout=3600 flags=00000000 sockflag=00000000
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=npu
statistic(bytes/packets/allow_err): org=510/11/1 reply=669/15/1 tuples=2
orgin->sink: org nataf->post, reply pre->org dev=16->5/5->16 gwy=0.0.0.0/192.168.118.25
hook=5 dir=org act=noop 192.168.118.25:59531->192.168.118.1:23(0.0.0.0:0)
hook=6 dir=reply act=noop 192.168.118.1:23->192.168.118.25:59531(0.0.0.0:0)
hook=pre dir=org act=dnat 2001:aa:1::1:55303 ->2001:aa:1::20:23(64:ff9b::c0a8:7601:23)
hook=post dir=reply act=snat 64:ff9b::c0a8:7601:23 ->2001:aa:1::1:55303(2001:aa:1::20:23)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=0000b2d2 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
```

8.2.4 Configuring OSPFv3

Networking Requirements

Use OSPFv3 on the IPv6 network.

Network Topology



Configuration Tips

RGW1

1) Configure the basic Internet access function.

2) Configure OSPFv3.

RGW2

1) Configure Internet access through NAT64.

2) Configure OSPF.

Configuration Steps

RGW1

Configure basic Internet access function. See section 1.1.2 “Internet Access Configuration” in section 6.1 “IPv6 Configuration”.

```
config system interface
         edit "internal"
                    config ipv6
                set ip6-allowaccess ping https http
set ip6-address 2001:bb:1::1/48
        next
     edit "wan1"
            config ipv6
                set ip6-allowaccess ping https
                set ip6-address 2001:aa:1::1/48
      next
   end
```

Configure OSPFv3.

```
RG-WALL # show router ospf6
config router ospf6
```

```
    set router-id 192.168.1.200              //Specify route ID.
        config area
            edit 0.0.0.0                                //Configure area 0.
            next
        end
        config ospf6-interface
            edit "wan1"                               //The interface name can be self-defined.
                set interface "wan1"             //Enable OSPFv3 for the wan1 interface.
            next
        end
        config redistribute "connected"    //Redistribute the directly connected route.
            set status enable
        end
        config redistribute "static"
     end
```

RGW2

Configure NAT64 Internet access function. For details, see section 6.1.3 “NAT64&DNS64” in section 6.1 “IPv6 Configuration”.

```
config system interface
    edit "internal"
            config ipv6
                set ip6-allowaccess ping https telnet
                set ip6-address 2001:aa:1::10/48
    next
    edit "wan1"
        set vdom "root"
        set ip 192.168.118.25 255.255.255.0
        set allowaccess ping https
        set type physical
        set description "         "
        set snmp-index 2
    next
end
```

Configure OSPFv3.

```
config router ospf6
    set default-information-originate always                        //Distribute a default route to the OSPF
neighbor RGW1.
    set router-id 192.168.1.99                 //Set route ID.
        config area                                  //Configure area 0.0.0.0.
            edit 0.0.0.0
            next
        end
        config ospf6-interface                    //Enable OSPF for the internal interface.
            edit "internal"                            //The interface name can be self-defined.
                set interface "internal"
            next
        end
end
```

Verification

View OSPF neighbors.

```
RG-WALL # get router info6   ospf  neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time    Interface  Instance ID
192.168.1.99      1   Full/Backup     00:00:34    wan1       0
```

View the routing table of RGW1.

```
RG-WALL # get  router  info6   routing-table
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, B - BGP
       * - candidate default
Timers: Uptime
O*E2    ::/0 [110/1] via fe80::a5b:eff:fe6f:f7a6, wan1, 00:20:29                                    //Learned
default route.
C       ::1/128 via ::, root, 02:21:41
C       2001:aa:1::/48 via ::, wan1, 02:13:38
C       2001:bb:1::/48 via ::, internal, 01:58:51
```

RGW1 can access IPv4 Internet through RGW2.

8.2.5 Common Commands

Commands for reference:

```
RG-WALL # diag sni p any 'host 2001:aa:1::10' 4      //Based on IPv6 address
interfaces=[any]
filters=[host 2001:aa:1::10]
1.389573 internal in 2001:bb:1::10 -> 2001:aa:1::10: icmp6: echo request seq 415
1.389692 wan1 out 2001:bb:1::10 -> 2001:aa:1::10: icmp6: echo request seq 415
1.389912 wan1 in 2001:aa:1::10 -> 2001:bb:1::10: icmp6: echo reply seq 415
```

```
1.389983 internal out 2001:aa:1::10 -> 2001:bb:1::10: icmp6: echo reply seq 415
2.391299 internal in 2001:bb:1::10 -> 2001:aa:1::10: icmp6: echo request seq 416
2.391426 wan1 out 2001:bb:1::10 -> 2001:aa:1::10: icmp6: echo request seq 416
2.391671 wan1 in 2001:aa:1::10 -> 2001:bb:1::10: icmp6: echo reply seq 416
2.391735 internal out 2001:aa:1::10 -> 2001:bb:1::10: icmp6: echo reply seq 416
8 packets received by filter
0 packets dropped by kernel
RG-WALL # diag sni p any icmp6 4 2                 //Based on ICMPv6
interfaces=[any]
filters=[icmp6]
1.410860 internal in 2001:bb:1::10 -> 2001:aa:1::10: icmp6: echo request seq 431
1.410986 wan1 out 2001:bb:1::10 -> 2001:aa:1::10: icmp6: echo request seq 431
RG-WALL # diagnose sys  session6 list
session6 info: proto=17 proto_state=01 duration=0 expire=179 timeout=0 flags=00000000 sockport=0 sockflag=0
use=3
origin-shaper=shared-1M-pipe prio=2  guarantee 0Bps  max 131072Bps  traffic 787Bps)
reply-shaper=shared-1M-pipe prio=2  guarantee 0Bps  max 131072Bps traffic 787Bps)
per_ip_shaper=
ha_id=0
policy_dir=0 tunnel=/
state=may_dirty os rs
statistic(bytes/packets/allow_err): org=83/1/0 reply=276/1/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3
hook=pre dir=org act=noop 2001:bb:1::10:57194 ->2001:aa:1::10:53(:::0)
hook=post dir=reply act=noop 2001:aa:1::10:53 ->2001:bb:1::10:57194(:::0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0 serial=000003f1
npu_state=00000000
RG-WALL # diagnose sys  session6 full-stat
session table:          table_size=131072 max_depth=1 used=188
misc info:       session_count=94 setup_rate=20 exp_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/0 removeable=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         19 in ESTABLISHED state
```

debug flow command

- diagnose debug enable
- diagnose deb flow **filter6** proto 1
- diagnose deb flow show con en
- diagnose deb flow show con enable

- dia deb flow trace **start6** 10

9 Troubleshooting

9.1 Debug Flow Command

Overview

When the firewall is deployed, the firewall often receives data packets, but does not forward them. You can run the **diagnose debug flow** command to track the processing procedure of data packets. Specifically, you can clearly view the processing procedure of data packets in each functional module, thus judging how the data packets are forwarded or discarded.

Command Description

diagnose debug enable Enable the debugging function

diagnose debug flow show console enable Begin to output the flow

diagnose debug flow filter add 119.253.62.131 Customize the filters, support diverse filtering modes; you can add multiple combinations of filters

diagnose debug flow filter View the filter configurations

diagnose debug flow trace start 6 Define the number of data packets to be tracked

Filtering Parameters

```
RG-WALL# diagnose deb flow filter
addr IP address.   // IP address
clear    Clear filter. // Clear the filter
daddr    Destination IP address. // Destination address
dport    Destination port.  // Destination port
negate   Inverse filter.        // Reverse filtering
port port // Interface, for example, port1
proto    Protocol number.   // Protocol, for example, 6 (TCP), 17 (UDP), and 1 (ICMP)
saddr    Source IP address. // Source address
sport    Source port.  // Source port
vd   Index of virtual domain.    // vdom
```

Analysis Examples

```
RG-WALL# id=36871 trace_id=1 msg="vd-root received a packet(proto=6, 192.168.
1.110:51661->119.253.62.131:80) from internal."id=36871 trace_id=1 msg="allocate a new session-00016920"  //
The internal interface receives data, and a new session is set up.
id=36871 trace_id=1 msg="find a route: gw-192.168.118.1 via wan1"         // Find the routing table
id=36871 trace_id=1 msg="find SNAT: IP-192.168.118.28, port-43333"// Detect the NAT configurations
id=36871 trace_id=1 msg="Allowed by Policy-1: SNAT"                    // Matching policy, ID1
id=36871 trace_id=1 msg="SNAT 192.168.1.110->192.168.118.28:43333"          // Conduct NAT
id=36871 trace_id=3 msg="vd-root received a packet(proto=6, 119.253.62.131:80->1
92.168.118.28:43333) from wan1."                         // The Wan1 port receives the returned data packets.
id=36871 trace_id=3 msg="Find an existing session, id-00016920, reply direction"  // The data packet matches
the session ID 0001692.
id=36871 trace_id=3 msg="DNAT 192.168.118.28:43333->192.168.1.110:51661"                 // Conduct reverse
DNAT
id=36871 trace_id=3 msg="find a route: gw-192.168.1.110 via internal"                                // Find
routes, and sent them to the internal interface
id=36871 trace_id=5 msg="vd-root received a packet(proto=6, 192.168.1.110:51661-
>119.253.62.131:80) from internal."                      // The internal interface receives subsequent data
packets.
id=36871 trace_id=5 msg="Find an existing session, id-00016920, original direction"              // Match the
session ID 0001692
id=36871 trace_id=5 msg="enter fast path"                    // Direct forwarding
id=36871 trace_id=5 msg="SNAT 192.168.1.110->192.168.118.28:43333"           // NAT
```

Example: The policy denies the access

```
RG-WALL#id=36871 trace_id=23 msg="vd-root received a packet(proto=6, 192.168
.1.110:51768->119.253.62.131:80) from internal."
id=36871 trace_id=23 msg="allocate a new session-00017537"
id=36871 trace_id=23 msg="find a route: gw-192.168.118.1 via wan1"
id=36871 trace_id=23 msg="Denied by forward policy check"            // The data packet is directly denied by
the policy; check the policy configurations.
```

Common debug flow results:

This policy is not available, or does not match the data packet; the data packet is discarded: msg="iprope_in_check() check failed, drop"

The data packet is denied by the policy, or hits the implicit policy; the data packet is denied: msg="Denied by forward policy check"

Reverse path check failed, and the data packet is discarded: msg="reverse path check fail, drop"

The session is processed via session-helper: msg="run helper-ftp(dir=original)"