Huawei Security Certification Training

HCIA-Security

Lab Guide

Version: 4.0

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China

Website: https://e.huawei.com

Huawei Certification System

Huawei Certification is an integral part of the company's "Platform + Ecosystem" strategy, and it supports the ICT infrastructure featuring "Cloud-Pipe-Device". It evolves to reflect the latest trends of ICT development. Huawei Certification consists of two categories: ICT Infrastructure Certification, and Cloud Service & Platform Certification, making it the most extensive technical certification program in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Security (HCIA-Security) is designed for Huawei's frontline engineers and anyone who wants to understand Huawei's security products and cyber security. The HCIA-Security certification covers the overview of information security, basis of cyber security, encryption and decryption principles, as well as related application.

Huawei Certification introduces you to the industry and market, helps you in innovation, and enables you to stand out among your industry peers.


Huawei Certification
Huawei Certified ICT Expert
Huawei Certified ICT Professional
Huawei Certified ICT Associate
HCIE
HCIP
HCIA
Cloud Service & Platform
ICT Infrastructure
HarmonyOS
IoT
openGauss
GaussDB
openEuler
MDC
Big Data
Kunpeng Application Developer
AI
Cloud
Storage
Intelligent Computing
Enterprise Communication
Intelligent Vision
Datacom
WLAN
Security
SDN
Data Center
Transmission
Access
LTE
5G

About This Document

Introduction

This document is an HCIA-Security certification training course and is intended for trainees who are going to take the HCIA-Security exam or readers want to understand the information security concepts and specifications, common cyber security threats and prevention, basic knowledge of cyber security, firewall network security prevention technology, user management technology, encryption and decryption principles, as well as application of encryption technology.

Description

This document covers seven labs. Starting from basic device operation configuration, it describes the basic operations of logging in to the firewall, security policy, NAT, hot standby, user management, IPSec VPN, and SSL VPN.

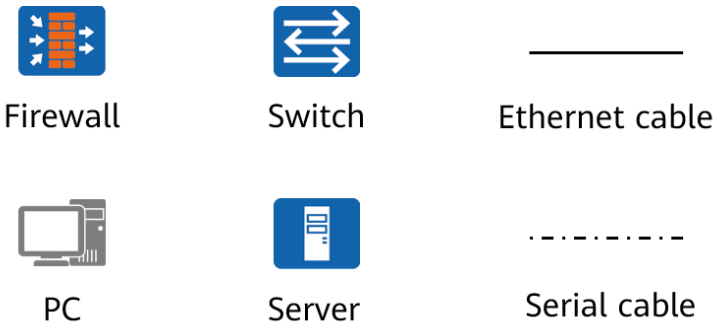
- Lab 1: firewall login. By introducing the common methods of logging in to the firewall, this lab helps readers to master the firewall management mode and the basic debugging skills.
- Lab 2: firewall security policy. Through basic networking configurations, this lab helps readers to master the key technologies such as firewall security zones and interzone forwarding control logic.
- Lab 3: NAT Server and Source NAT. Focusing on the source NAT and destination NAT technologies, this lab helps readers to master the firewall debugging method in NAT scenarios and to get familiar with the application scenarios of firewalls functioning as egress devices.
- Lab 4: firewall hot standby. This lab helps readers to master technologies such as how to use firewalls to implement service redundancy and how to ensure stable service operation when a single firewall is faulty.
- Lab 5: user management. This lab helps readers to master the authentication of users who use the firewall to access the Internet.
- Lab 6: site-to-site IPSec VPN. This lab helps readers to master the basic methods of communication between different networks over the Internet.
- Lab 7: SSL VPN. This lab enables mobile office users to access the enterprise intranet at any time on the Internet, helping readers to understand the SSL VPN principle and configuration.

Background Knowledge Required

This course is for Huawei's basic certification. To better understand this course, familiarize yourself with the following requirements:

- Have basic understanding of cyber security, and be familiar with Huawei security devices and basic security knowledge.

Symbol Conventions



Lab Environment

Network Description

This lab environment is intended for cyber security engineers who are preparing for the HCIA-Security exam. Each lab environment consists of two firewalls, two switches, and four PCs. In the lab environment, 4 trainees can perform hands-on labs at the same time.

Device Requirements

To meet the HCIA-Security lab requirements, it is recommended that each lab environment adopt the following configurations.

Mapping between device names, models, and versions

Device Name	Device Model	Software Version
Switch	S5735	V200R010C00SPC600
Firewall	USG6525E	V600R007C20SPC100

Note: The port information, output, and configuration information of all devices in this guide are provided based on the device models in the recommended topology. The actual information may vary according to the lab environment.

Preparing the Lab Environment

Checking Devices

Ensure that all items required in the labs are available. The following table lists the specific items.

Item	Quantity	Remarks
Switch (S5735)	2 for each group	
Firewall (USG6525E)	2 for each group	
Laptop or desktop	4 for each group	
Twisted pair	8 for each group	Length: at least 2 m
Console cable	1 for each group	

Clearing the Firewall Configuration

To avoid the residual configurations from impacting the lab, trainees are required to clear the configuration saved on the devices after the lab is complete and before the devices are shut down. Before starting the labs, ensure that the devices start from empty configurations. Otherwise, clear all configurations and restart the devices.

The user name and password for logging in to the firewall are **admin** and **Admin@123**, respectively. The operation methods on switches are the same. The following uses the firewall as an example:

```
Login authentication
Username:admin
Password:
<FW> reset saved-configuration
This will delete the configuration in the flash memory.
The device configurations will be erased to reconfigure.
Are you sure? (y/n)[n]:y
Clear the configuration in the device successfully.
```

To restart the firewall, run the following command:

```
<FW> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration.
Continue ? [y/n]:n
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

Contents

1 Firewall Login....10
1.1 Logging In to a Device Through the Console Port (PuTTY)....10
1.1.1 Introduction....10
1.1.2 Lab Configuration....11
1.1.3 Verification....12
1.1.4 Quiz....13
1.2 Getting Familiar with Commands (PuTTY)....13
1.2.1 Introduction....13
1.2.2 Lab Configuration....14
1.2.3 Quiz....17
1.3 Logging In to a Device Through Telnet....17
1.3.1 Introduction....17
1.3.2 Lab Configuration....18
1.3.3 Verification....23
1.3.4 Quiz....23
1.4 Logging In to the Device Through SSH....23
1.4.1 Introduction....23
1.4.2 Lab Configuration....24
1.4.3 Verification....26
1.4.4 Quiz....27
1.5 Logging In to the Device Through the Default Web UI....28
1.5.1 Introduction....28
1.5.2 Lab Configuration....28
1.5.3 Verification....29
1.5.4 Quiz....30
1.6 Logging In to the Device Through the Web UI....30
1.6.1 Introduction....30
1.6.2 Lab Configuration....31
1.6.3 Verification....35
1.6.4 Quiz....36
2 Firewall Security Policy....37
2.1 Introduction....37
2.1.1 About This Lab....37
2.1.2 Objectives....37

2.1.3 Networking Topology....37
2.1.4 Lab Planning....37
2.2 Lab Configuration....38
2.2.1 Configuration Roadmap....38
2.2.2 Configuration Procedure on the CLI....38
2.2.3 Configuration Procedure on the Web UI....39
2.3 Verification....40
2.4 Quiz....41
3 Firewall NAT Server and Source NAT....42
3.1 Introduction....42
3.1.1 About This Lab....42
3.1.2 Objectives....42
3.1.3 Networking Topology....42
3.1.4 Lab Planning....42
3.2 Lab Configuration (Source NAT)....43
3.2.1 Configuration Roadmap....43
3.2.2 Configuration Procedure on the CLI....43
3.2.3 Configuration Procedure on the Web UI....44
3.2.4 Verification....48
3.2.5 Quiz....49
3.3 Lab Configuration (NAT Server and Source NAT)....49
3.3.1 Configuration Roadmap....49
3.3.2 Configuration Procedure on the CLI....49
3.3.3 Configuration Procedure on the Web UI....50
3.3.4 Verification....54
3.3.5 Quiz....55
4 Firewall Hot Standby....56
4.1 Introduction....56
4.1.1 About This Lab....56
4.1.2 Objectives....56
4.1.3 Networking Topology....56
4.1.4 Lab Planning....56
4.2 Lab Configuration....57
4.2.1 Configuration Roadmap....57
4.2.2 Configuration Procedure on the CLI....57
4.2.3 Configuration Procedure on the Web UI....60
4.3 Verification....65
4.4 Configuration Reference....67
4.4.1 Configuration of FW1....67

4.4.2 Configuration of FW2 68
4.5 Quiz 69
5 User Management 71
5.1 Introduction 71
5.1.1 About This Lab 71
5.1.2 Objectives 71
5.1.3 Networking Topology 71
5.1.4 Lab Planning 71
5.2 Lab Configuration 72
5.2.1 Configuration Roadmap 72
5.2.2 Configuration Procedure on the Web UI 72
5.3 Verification 81
5.4 Quiz 82
6 Site-to-Site IPSec VPN 83
6.1 Introduction 83
6.1.1 About This Lab 83
6.1.2 Objectives 83
6.1.3 Networking Topology 83
6.1.4 Lab Planning 83
6.2 Lab Configuration 84
6.2.1 Configuration Roadmap 84
6.2.2 Configuration Procedure on the Web UI 84
6.3 Verification 89
6.4 Configuration Reference 89
6.4.1 Configuration of FW1 89
6.4.2 Configuration of FW2 91
6.5 Quiz 92
7 SSL VPN 94
7.1 Introduction 94
7.1.1 About This Lab 94
7.1.2 Objectives 94
7.1.3 Networking Topology 94
7.1.4 Lab Planning 94
7.2 Lab Configuration 95
7.2.1 Configuration Roadmap 95
7.2.2 Configuration Procedure on the Web UI 95
7.3 Verification 101
7.4 Configuration Reference 102

7.4.1 Firewall Configuration 102
7.5 Quiz 103

1 Firewall Login

1.1 Logging In to a Device Through the Console Port (PuTTY)

1.1.1 Introduction

1.1.1.1 About This Lab

In this lab, you will be familiar with the management and configuration of the device by logging in to an unconfigured firewall from a PC through the console port.

1.1.1.2 Objectives

- Learn how to log in to and manage a device from a PC through the console port.
- Learn common CLI–based configurations.
- Learn how to use the CLI online help.
- Learn how to undo a command.
- Learn how to use the CLI shortcut keys.

1.1.1.3 Networking Topology

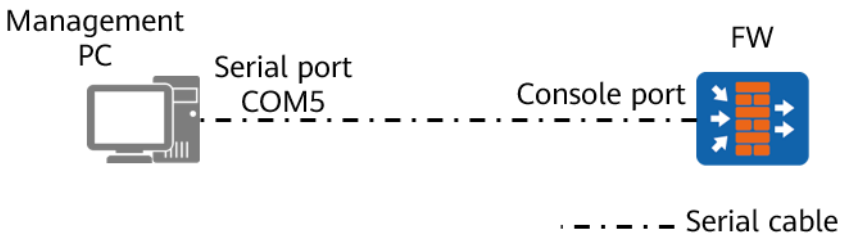


Figure 1-1 Topology for logging in to the device through the console port

1.1.1.4 Background

As shown in the networking diagram, the FW is a new firewall without any configurations. The PC is connected to the console port of the FW through a serial cable, so you need to perform initialization on the FW.

1.1.1.5 Lab Planning

The management PC uses a serial cable to connect to the console port of the device, and uses PuTTY to log in to the device.

Table 1-1 Device ports and parameters

Device	Port	Port Type	Description
Management PC	COM5	Serial port	The serial cable uses a USB port or serial port to connect to the management PC. You need to install a driver on the PC to check and use the corresponding port.
Firewall	Console	Console port	The console port on the device panel has a console port identifier.

1.1.2 Lab Configuration

1.1.2.1 Configuration Roadmap

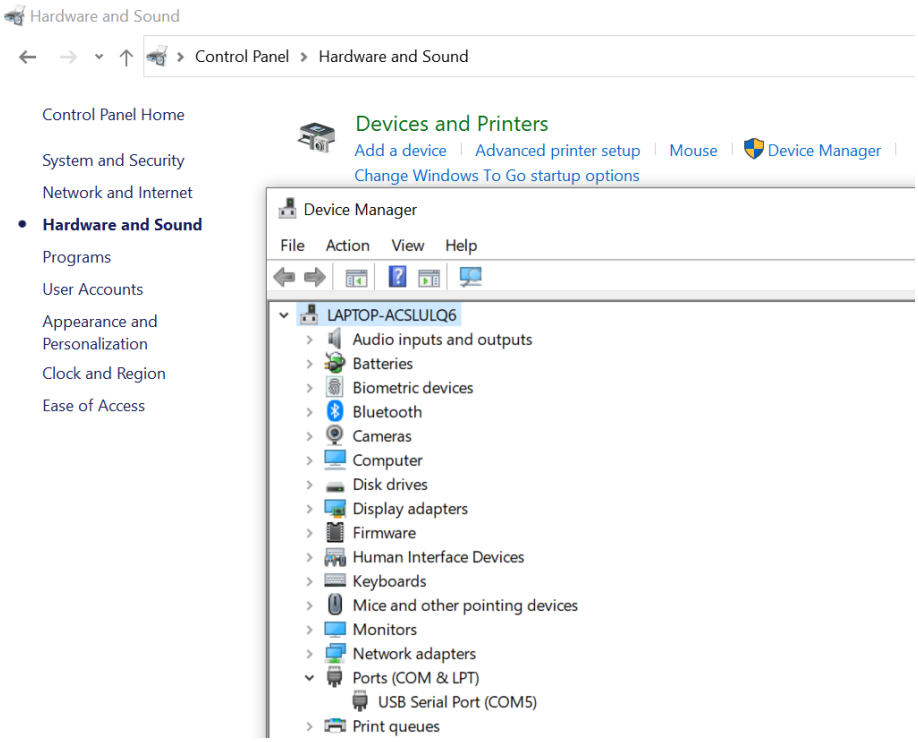
1. Use a serial cable to connect the serial port (or USB port) on the management PC and the console port on the device.
2. Set connection parameters in PuTTY on the management PC and log in to the device.

1.1.2.2 Configuration Procedure

Step 1 Establish the connection, power on all devices, and ensure that they run properly.

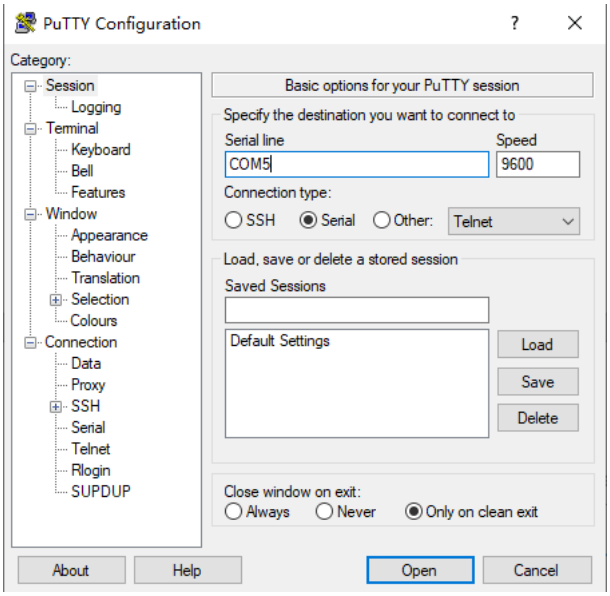
Step 2 Check the serial COM port number used by the management PC to connect to the device.

Choose **Control Panel** > **Hardware and Sound** > **Devices and Printers** > **Device Manager** > **Ports** and check the serial port number.



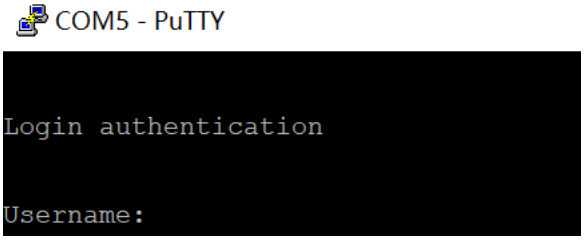
Step 3 Run PuTTY on the management PC and set parameters.

Click **Session**, set **Connection type** to **Serial**, set **Serial line** to **COM5** queried in the previous step, and set other parameters as shown in the following figure.



1.1.3 Verification

Press **Enter**. If the following information is displayed in PuTTY, the login to the device through the console port is successful.



1.1.4 Quiz

After the console cable is connected to the management PC, the serial port number is not displayed on the management PC by choosing **Control Panel** > **Hardware and Sound** > **Devices and Printers** > **Device Manager** > **Ports**. What are the possible causes? What corresponding solutions are there?

Reference Answer:

1. The console cable driver is not installed on the management PC. Scan and install the driver. Note that the driver that needs to be installed may vary according to console cable. You are advised to rule out driver installation problems first.
2. The console cable is faulty. Replace the console cable with another functioning one.
3. The PC port is in poor contact. Remove and insert the cable again or replace the cable with a new one.

1.2 Getting Familiar with Commands (PuTTY)

1.2.1 Introduction

1.2.1.1 About This Lab

You can use a PC to log in to a device that uses factory default settings through the console port and perform basic operations on the CLI.

1.2.1.2 Objectives

- Through this lab, you will be familiar with the basic operations of the CLI.

1.2.1.3 Networking Topology

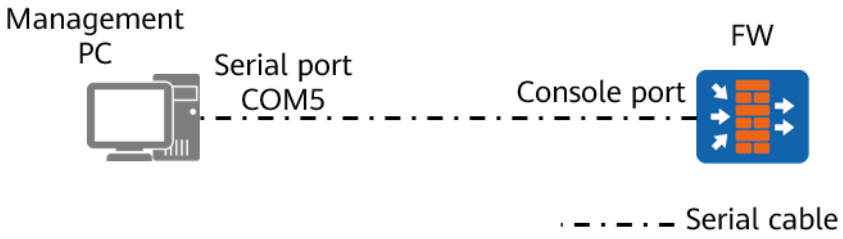


Figure 1-2 Topology for logging in to the device through the console port

1.2.1.4 Background

As shown in the networking diagram, the FW is a brand-new firewall without configuration. The network administrator needs to debug the firewall and learns the CLI operations of the firewall. Therefore, the network administrator needs to use a PC to connect to the console port of the firewall through a serial cable, then uses the PuTTY software to log in to the device, and performs initialization operations on the firewall.

1.2.1.5 Lab Planning

The management PC uses a serial cable to connect to the console port of the device, and uses PuTTY to log in to the device.

Table 1-2 Device ports and parameters

Device	Port	Port Type	Description
Management PC	COM5	Ethernet port	The serial cable uses a USB port or serial port to connect to the management PC. You need to install a driver on the PC to check and use the corresponding port.
Firewall	Console	Console port	The console port on the device panel has a console port identifier.

1.2.2 Lab Configuration

1.2.2.1 Configuration Roadmap

1. Log in to the device through the console port.
2. Perform basic command line configurations on the device.

1.2.2.2 Configuration Procedure

Step 1 Log in to the device through the console port.

Step 2 Enter the system view.

The CLI is divided into multiple command views. Every command is registered with one or multiple views, so a command can be run only in the specified view (or views). After a connection to a firewall is set up, you need to enter the user name and the initial password, and change the initial password. Most commands need to be configured in the system view, so you need to enter the system view from the user view before configuration. The commands are as follows:

```
Press ENTER to get started.
Login authentication
```

```
Username:admin
Password:
The password needs to be changed. Change now? [Y/N]: Y
Please enter old password:
Please enter new password:
Please confirm new password:

  Info: Your password has been changed. Save the change to survive a reboot.
******************************************************************************
*            Copyright (C) 2014-2020 Huawei Technologies Co., Ltd.           *
*                                All rights reserved.                        *
*                    Without the owner's prior written consent,              *
*           no decompiling or reverse-engineering shall be allowed.          *
******************************************************************************
<FW> system
[FW]
```

Step 3 Enter the interface view.

In the system view, you can run configuration commands to enter the views of protocols, interfaces, etc. To enter the view of an interface, run the following command:

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1]
```

Step 4 Get online help.

A question mark (?) is one of the online help methods provided by the VRP. If you enter a question mark (?) in the system view, the system will list the command parameters that can be configured in the system view. You can also type a space after a parameter and then enter a question mark (?) to obtain the list of parameters that can be used after this particular parameter. If you type a character string followed by a question mark (?), the system will list all the commands starting with this character string. For example:

```
[FW] interface ?
  Cellular              Cellular interface
  Dialer                Dialer interface
  Eth-Trunk             Ethernet-Trunk interface
  GigabitEthernet       GigabitEthernet interface
  LoopBack              LoopBack interface
  NULL                  NULL interface
  Nve                   Nve interface
  Tunnel                Tunnel interface
  Vbdif                 Vbdif interface
  Virtual-Template      Virtual-Template interface
```

The **Tab** key is another online help method provided by the VRP. If you enter the first few letters of a command keyword and press **Tab**, the complete keyword is displayed. You can switch between all the commands that have this keyword.

```
[FW] inter   //Press Tab.
[FW] interface
```

Step 5 Quit the current view (go back to the previous view).

To go back to the previous view, run the **quit** command. For example, to quit the current interface view, run the following command:

```
[FW-GigabitEthernet0/0/1] quit
[FW]
```

Step 6 Return to the user view.

To return to the user view from another view, run the **return** command. For example:

```
[FW-GigabitEthernet0/0/1] return
<FW>
```

Step 7 Display the device version.

In any view, run the **display version** command to display the device version. For example:

```
<FW> display version
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.170 (USG6500 V600R007C20)
Copyright (C) 2014-2020 Huawei Technologies Co., Ltd.
```

Step 8 Save configurations.

To save all the configurations of the device, run the **save** command in the user view.

```
<FW> save
The current configuration will be written to hda1:/fw2.zip.
Are you sure to continue?[Y/N]Y
Now saving the current configuration to the slot 0..
Jan 19 2022 10:13:19 FW %%01CFM/4/SAVE(s)[0]:The user chose Y when deciding whether to save
the configuration to the device.....
Save the configuration successfully.
```

Step 9 Display configurations.

In the current view, run the **display this** command to display the configuration of the view. An interface view is used as an example:

```
[FW-GigabitEthernet0/0/0] display this
#
interface GigabitEthernet0/0/0
undo shutdown
  ip address 192.168.0.1 255.255.255.0
#
Return
```

Run the following command in any view to display all the current configurations, including the configurations that have not been saved:

```
[FW] display current-configuration
```

Run the following command in any view to display the configurations that have been saved:

```
[FW] display saved-configuration
```

1.2.3 Quiz

After logging in to the device through PuTTY, garbled characters occasionally appear during the command configuration process. What should I do?

Reference Answer:

Check whether PuTTY uses UTF-8. If not, configure PuTTY to use UTF-8.

1.3 Logging In to a Device Through Telnet

1.3.1 Introduction

1.3.1.1 About This Lab

During network maintenance, network administrators often need to log in to multiple devices. It is difficult to log in to each device through the console port. The remote login function can be configured on the device to enable administrators to remotely log in to the device through Telnet. This facilitates device maintenance and commissioning.

1.3.1.2 Objectives

- Through this lab, you can get familiar with the basic method of configuring the Telnet-based remote login function.

1.3.1.3 Networking Topology

Figure 1-3 Topology for logging in to the device through Telnet

1.3.1.4 Lab Planning

The management PC uses a common Ethernet cable to connect to GE0/0/1 of the device, and uses PuTTY to remotely log in to the device.

Table 1-3 Device ports and parameters

Device	Port	Port Type	Address
Management PC	Ethernet port	Ethernet port	10.1.2.100/24
Firewall	GE0/0/1	Ethernet port	10.1.2.1/24

1.3.2 Lab Configuration

1.3.2.1 Configuration Roadmap

1. Log in to the device, for example, through the console port.
2. Configure Telnet on the device.
3. Log in to the device from the management PC through Telnet.

1.3.2.2 Configuration Procedure on the CLI

Step 1 Log in to the device through other methods. (For example, log in to the device through the console port. For details, see section 1.1 Logging In to a Device Through the Console Port (PuTTY).)

Step 2 Enable Telnet on the device.

```
<FW> system-view
[FW] telnet server enable
```

Step 3 Configure the port through which a Telnet user can log in to the device.

Configure the IP address of the port.

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1] ip address 10.1.2.1 24
```

Configure access control for the port.

```
[FW-GigabitEthernet0/0/1] service-manage enable
[FW-GigabitEthernet0/0/1] service-manage telnet permit
[FW-GigabitEthernet0/0/1] quit
```

Add the port to a security zone.

```
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet0/0/1
[FW-zone-trust] quit
```

Configure a security policy to allow the management PC to access GE0/0/1 of the firewall.

```
[FW] security-policy
[FW-policy-security] rule name trust-local
[FW-policy-security-rule-trust-local] source-zone trust
```

```
[FW-policy-security-rule-trust-local] destination-zone local
[FW-policy-security-rule-trust-local] action permit
```

Note: If the MGMT port of the firewall is used for remote login, skip this step.

Step 4 Configure an administrator.

Set the VTY administrator authentication mode to AAA.

```
[FW] user-interface vty 0 4
[FW-ui-vty0-4] authentication-mode aaa
[FW-ui-vty0-4] protocol inbound telnet
[FW-ui-vty0-4] user privilege level 3
[FW-ui-vty0-4] quit
```

Configure a Telnet administrator.

```
[FW] aaa
[FW-aaa] manager-user telnetuser
[FW-aaa-manager-use-telnetuser] password cipher (Enter password)
[FW-aaa-manager-use-telnetuser] service-type telnet
[FW-aaa-manager-use-telnetuser] level 3
[FW-aaa-manager-use-telnetuser] quit
```

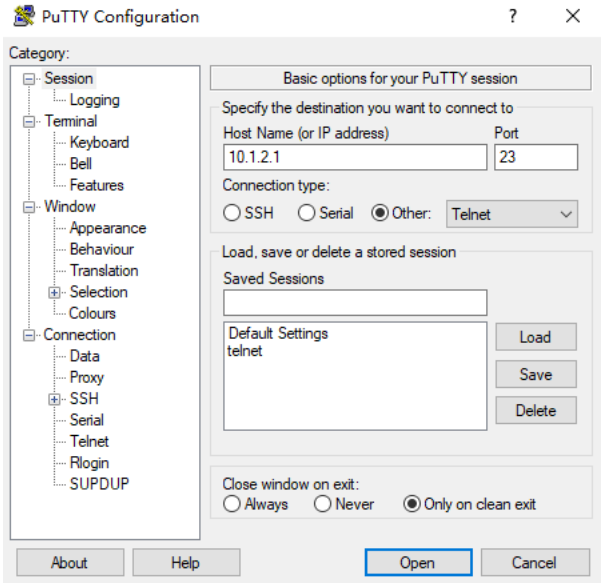
Bind a role to the administrator (optional, supported only by firewalls).

```
[FW-aaa] bind manager-user telnetuser role system-admin
```

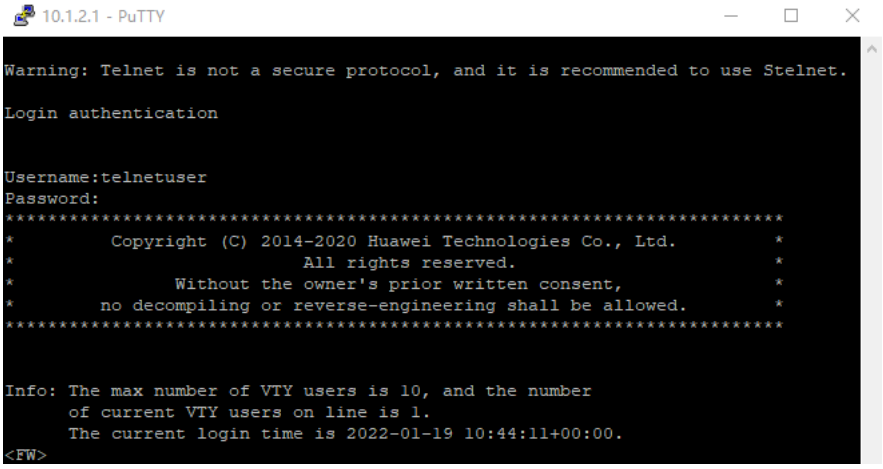
Step 5 Log in to the device.

On the management PC, set the address to **10.1.2.100/24**, run PuTTY, set Telnet parameters, and log in to the device.

Click **Session**, set **Connection type** to **Telnet** and **Host Name (or IP address)** to **10.1.2.1**, and set other parameters as shown in the following figure.



Click **Open** to establish a connection. If the following information is displayed, you have successfully logged in to the device by using Telnet.



1.3.2.3 Configuration Procedure on the Web UI (Supported only by Firewalls)

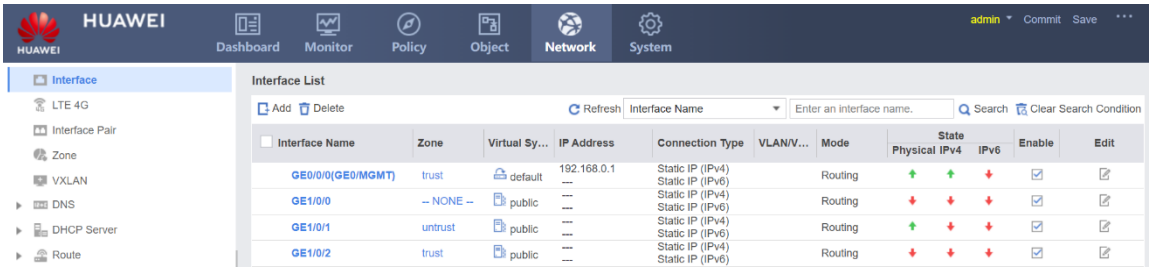
Step 1 Use the default web UI to log in to the device. For details, see section 1.5 "Logging In to the Device Through the Default Web UI."

Step 2 Enable the Telnet service.

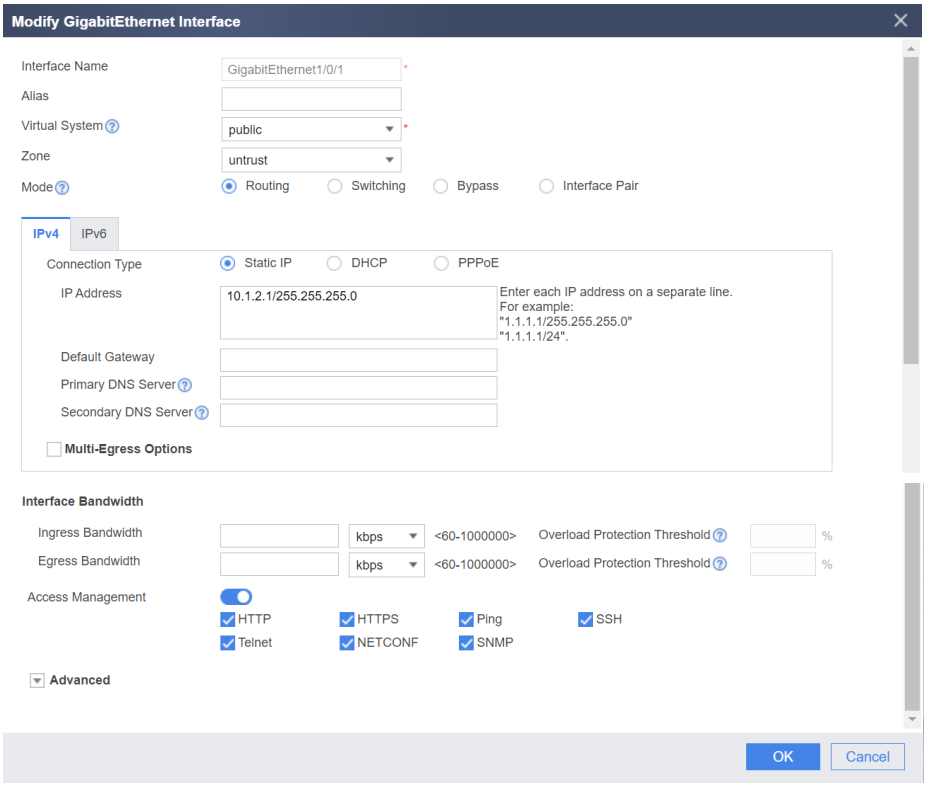
Choose **System** > **Administrator** > **Service Settings** and select the **Enable** check box of **Telnet Service**.

Step 3 Configure the login port.

Configure the port through which a Telnet user logs in to the device. Choose **Network** > **Interface** and click the **Edit** button on the line of GE0/0/1.



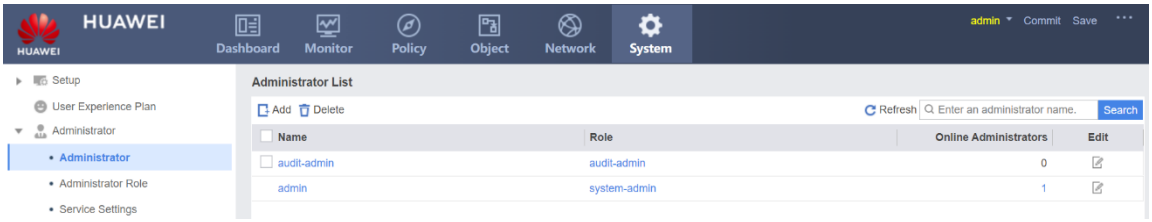
Configure the IP address, security zone, and access control functions of the port.



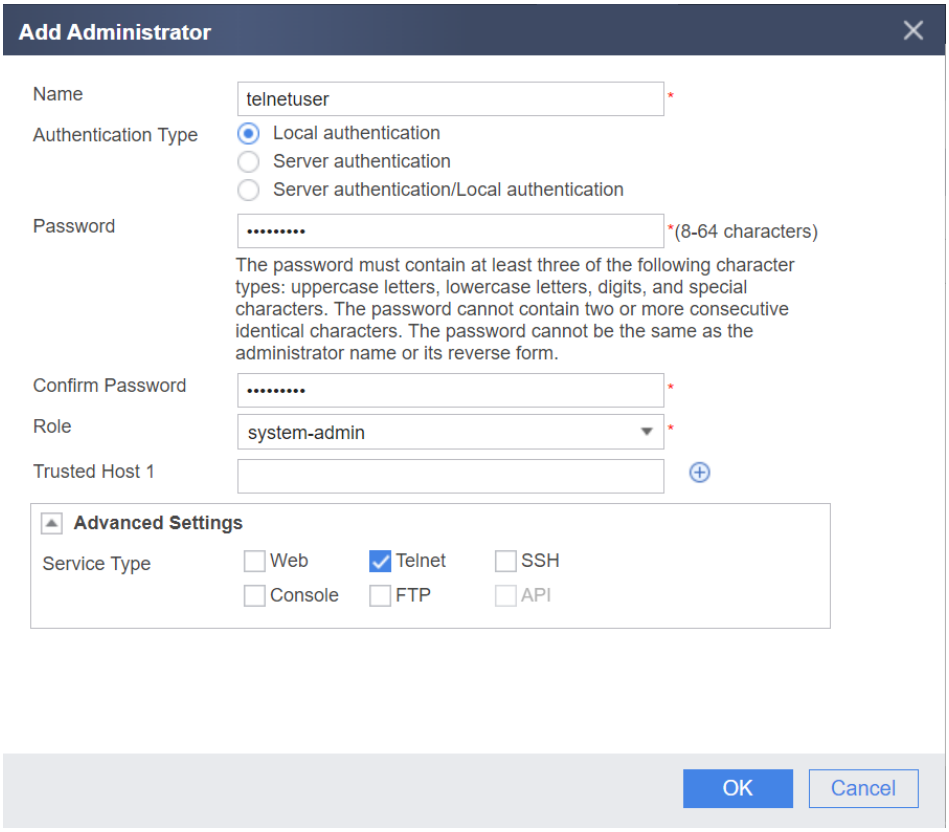
Note: If the MGMT port of the firewall is used for remote login, skip this step.

Step 4 Configure an administrator.

Choose **System** > **Administrator** > **Administrator** and click **Add**.



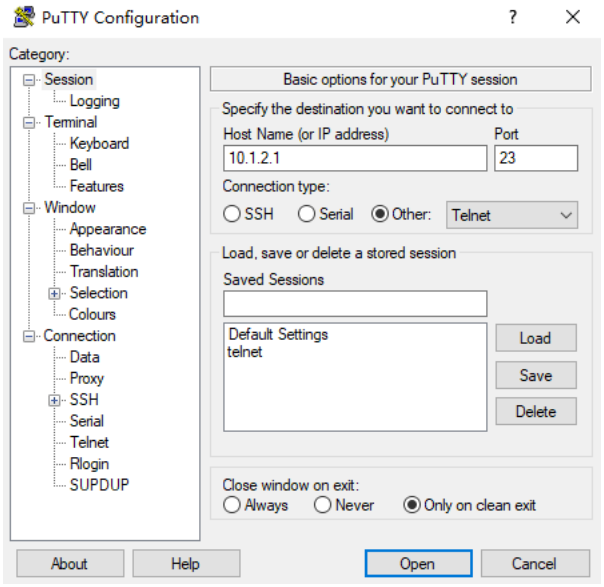
Set the Telnet user name to **telnetuser**, password to **Admin@123**, administrator role to **system-admin**, and service type to **Telnet**.



Step 5 Log in to the device.

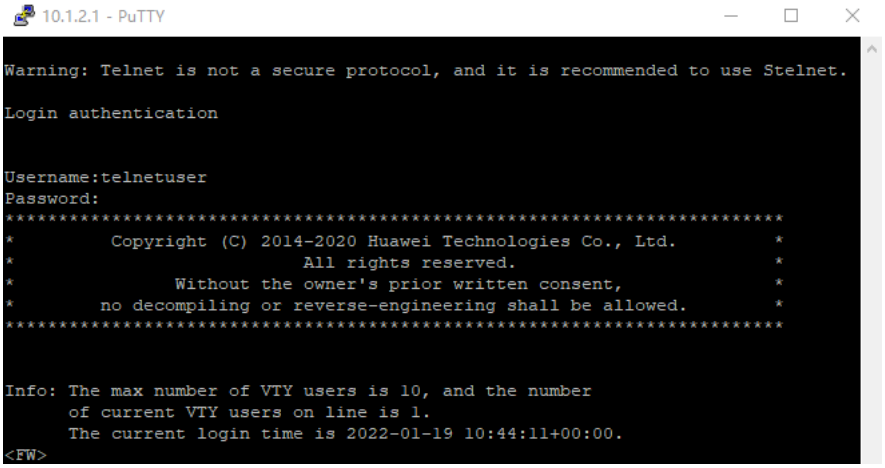
On the management PC, set the address to **10.1.2.100/24**, run PuTTY, set Telnet parameters, and log in to the device.

Click **Session**, set **Connection type** to **Telnet** and **Host Name (or IP address)** to **10.1.2.1**, and set other parameters as shown in the following figure.



1.3.3 Verification

Click **Open** inStep 5, press **Enter**, and enter the user name **telnetuser** and the password **Admin@123**. If the following information is displayed in PuTTY, the Telnet login is successful.



1.3.4 Quiz

TCP port 23 is used to log in to the device through Telnet. Can I change it to another port number? If so, what is the corresponding command? After the change, which command can I use to check the current port number for setting up a Telnet connection?

Reference Answer:

1. Run the **telnet server port** *port-number* command to set the listening port number of the Telnet server.
2. After the Telnet listening port number is changed, you can run the **display telnet server status** command to check the listening port number currently used by the Telnet server.

1.4 Logging In to the Device Through SSH

1.4.1 Introduction

1.4.1.1 About This Lab

During network maintenance, network administrators often need to log in to multiple devices. It is difficult to log in to each device through the console port. In addition, the Telnet remote login packets are in plain text. To enhance security, configure the SSH function on the device to enable administrators to remotely log in to the device through SSH for management.

1.4.1.2 Objectives

- Through this lab, you can get familiar with the basic method of configuring the SSH-based remote login function.

1.4.1.3 Networking Topology

Figure 1-4 Topology for logging in to a device through SSH

1.4.1.4 Lab Planning

The management PC uses a common Ethernet cable to connect to GE0/0/1 of the device, and uses PuTTY to remotely log in to the device.

Table 1-4 Device ports and parameters

Device	Port	Port Type	Address
Management PC	Computer network port	Ethernet port	10.1.2.100/24
Firewall	GE0/0/1	Ethernet port	10.1.2.1/24

1.4.2 Lab Configuration

1.4.2.1 Configuration Roadmap

1. Log in to the device, for example, through the console port.
2. Configure the SSH function on the device.
3. Log in to the device from the management PC through SSH.

1.4.2.2 Configuration Procedure on the CLI

Step 1 Log in to the device through other methods. (For example, log in to the device through the console port. For details, see section1.1 "Logging In to a Device Through the Console Port (PuTTY)".)

Step 2 Enable SSH on the device.

```
<FW> system-view
[FW] stelnet server enable
```

Step 3 Configure the login port.

Configure the IP address of the port for login.

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1] ip address 10.1.2.1 24
```

Configure access control for the port.

```
[FW-GigabitEthernet0/0/1] service-manage enable
[FW-GigabitEthernet0/0/1] service-manage ssh permit
[FW-GigabitEthernet0/0/1] quit
```

Add the port to a security zone.

```
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet0/0/1
[FW-zone-trust] quit
```

Configure a security policy to allow the management PC to access GE0/0/1 of the firewall.

```
[FW] security-policy
[FW-policy-security] rule name trust-local
[FW-policy-security-rule-trust-local] source-zone trust
[FW-policy-security-rule-trust-local] destination-zone local
[FW-policy-security-rule-trust-local] action permit
[FW-policy-security-rule-trust-local] quit
```

Note: If the MGMT port of the firewall is used for remote login, skip this step.

Step 4 Configure an administrator.

Set the VTY administrator authentication mode to AAA.

```
[FW] user-interface vty 0 4
[FW-ui-vty0-4] authentication-mode aaa
[FW-ui-vty0-4] protocol inbound ssh
[FW-ui-vty0-4] user privilege level 3
[FW-ui-vty0-4] quit
```

Create an SSH administrator account **sshuser**, and set the authentication method to **password**, password to **Admin@123**, and service mode to **SSH**.

```
[FW] aaa
[FW-aaa] manager-user sshuser
[FW-aaa-manager-use-sshuser] password cipher (Enter password)
[FW-aaa-manager-use-sshuser] service-type ssh
[FW-aaa-manager-use-sshuser] level 3
[FW-aaa-manager-use-sshuser] quit
```

Bind a role to the administrator (optional, supported only by firewalls).

```
[FW-aaa] bind manager-user sshuser role system-admin
```

Configure an SSH user.

```
[FW] ssh user sshuser
[FW] ssh user sshuser authentication-type password
[FW] ssh user sshuser service-type stelnet
```

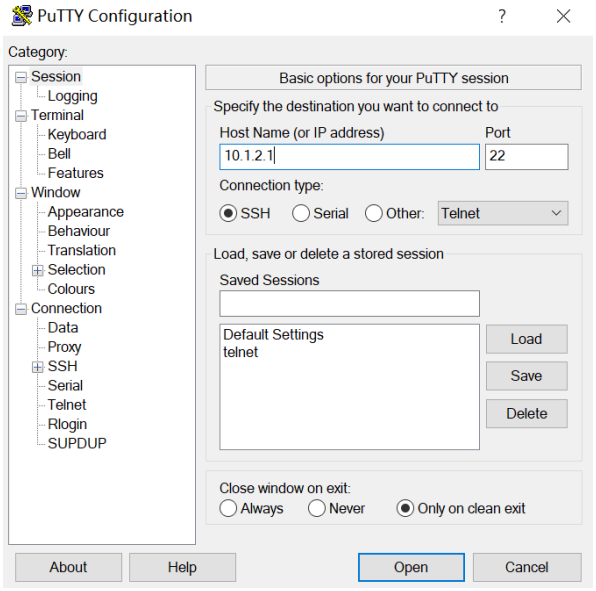
Step 5 Generate a local key pair.

```
[FW] rsa local-key-pair create
The key name will be: FW_Host
The range of public key size is (512 ~ 2048).
NOTES: A key shorter than 1024 bits may cause security risks.
        The generation of a key longer than 512 bits may take several minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
...++++++++
..++++++++
.....+++++++++
.....+++++++++
```

Step 6 Log in to the device.

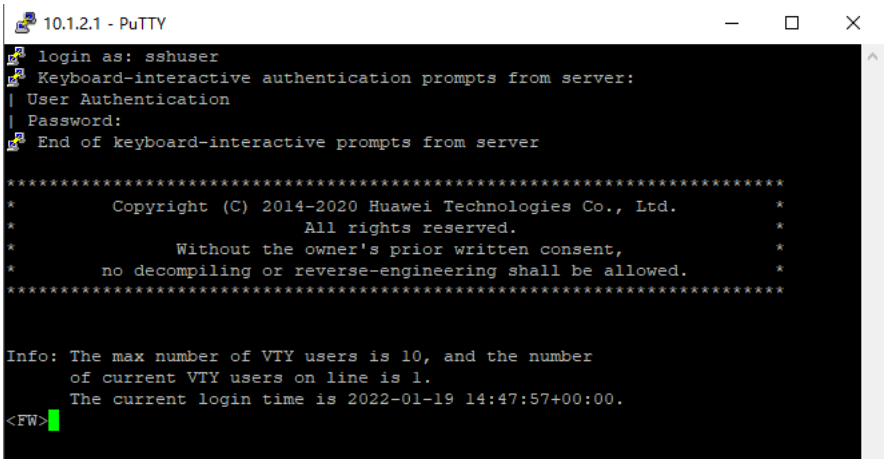
On the management PC, set the address to **10.1.2.100/24**, run PuTTY, set SSH parameters, and log in to the device.

Click **Session**, set **Connection type** to **SSH** and **Host Name (or IP address)** to **10.1.2.1**, and set other parameters as shown in the following figure.



1.4.3 Verification

Click **Open** in Step 6, press **Enter**, and enter the user name **sshuser** and the password **Admin@123**. If the following information is displayed in PuTTY, the SSH login is successful.



1.4.4 Quiz

What type of security verification mode does SSH login use in this lab? Is there any other SSH method for secure login? If so, please give examples and list the key verification steps for secure login.

Reference Answer:

1. This lab uses SSH password-based security verification.
2. SSH security verification falls into password-based security verification and key-based security verification.
3. Login procedure of password-based SSH security verification:
   a. A user initiates a login request.
   b. The remote host returns its public key to the requesting host.
   c. The requesting host uses the public key to encrypt the password entered by the user.
   d. The requesting host sends the encrypted password to the remote host.
   e. The remote host decrypts the password using the private key.
   f. The remote host checks whether the decrypted password is the same as the user password. If so, the login is successful.
4. Login procedure of key-based SSH security verification:
   a. A user host generates a key pair and imports the public key to the remote host.
   b. The user initiates a login request.
   c. The remote host returns a random character string to the user.
   d. The host where the user is located uses the private key to encrypt the random character string and returns the encrypted random string to the remote host.
   e. The remote host uses the imported public key to decrypt the encrypted random string. If the decryption succeeds, the user's login information is correct and the login is allowed.

1.5 Logging In to the Device Through the Default Web UI

1.5.1 Introduction

1.5.1.1 About This Lab

Engineers can commission new firewalls on the web UI. In the factory default settings, a PC can log in to the device through the MGMT port of the firewall, implementing device management and configuration.

1.5.1.2 Objectives

- Through this lab, you will be able to use a PC to log in to the firewall through the default web UI.

1.5.1.3 Networking Topology

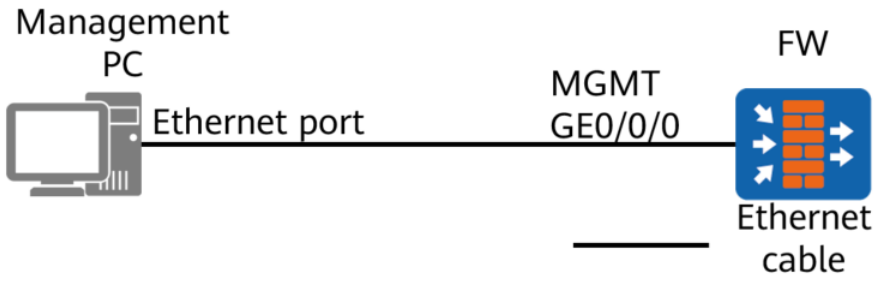


Figure 1-5 Topology for logging in to the device through the default web UI

1.5.1.4 Lab Planning

The PC uses an Ethernet cable to connect to the MGMT port of the device, and uses a web browser to log in to the device.

Table 1-5 Device ports and parameters

Device	Port	Port Type	IP Address
Management PC	Computer network port	Ethernet port	192.168.0.2/24
Firewall	GigabitEthernet0/0/0	Ethernet port	192.168.0.1/24

1.5.2 Lab Configuration

1.5.2.1 Configuration Roadmap

1. Use twisted pairs to connect the Ethernet port on the management PC to the MGMT port on the device.
2. Use a browser to access the firewall from the management PC.

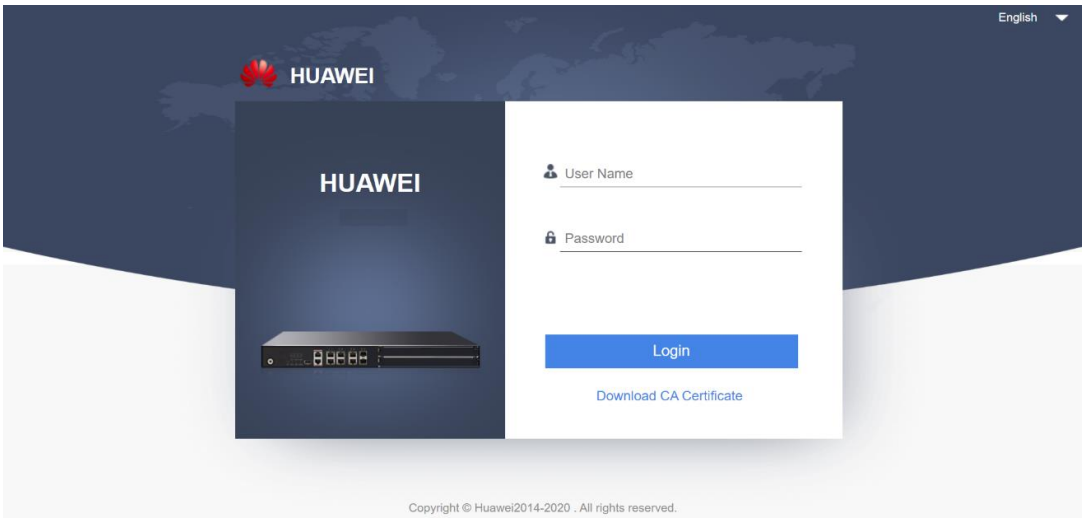
1.5.2.2 Configuration Procedure

Step 1 Establish the connection, power on all devices, and ensure that they run properly.

Step 2 Set the IP address to 192.168.0.2/24 on the management PC.

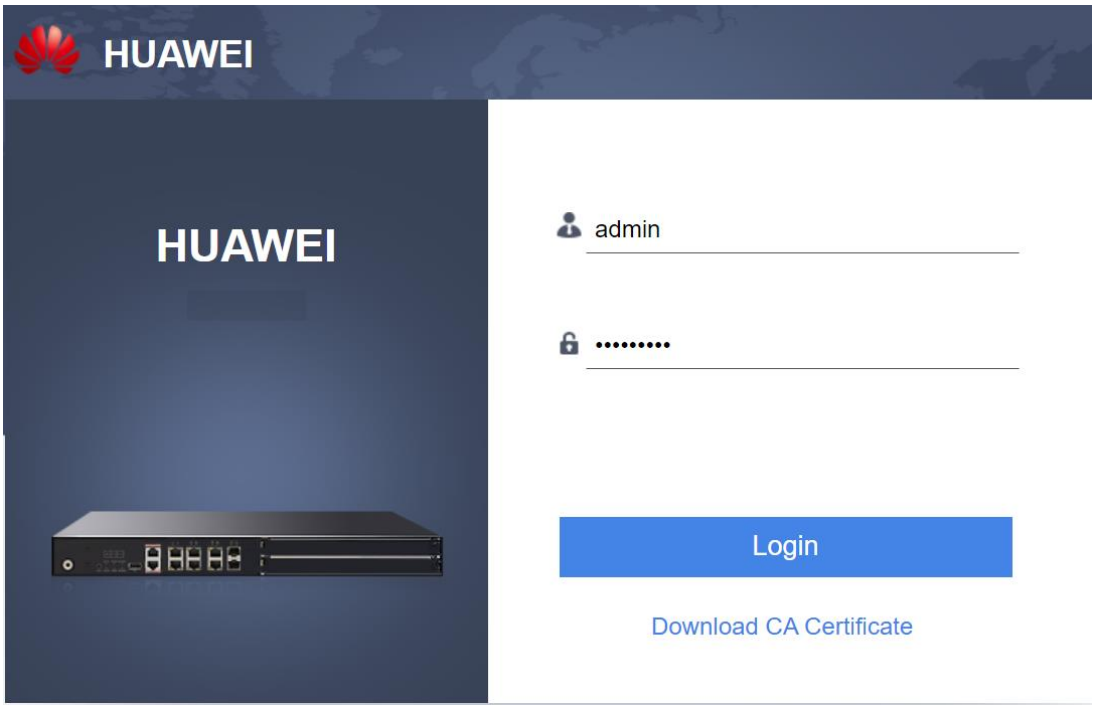
Step 3 Open a browser on the management PC and enter https://192.168.0.1:8443 (or http://192.168.0.1) in the address box.

(Note: By default, the IP address of GE0/0/0 is 192.168.0.1 and HTTPS management is enabled. You can log in to the system using the user name **admin** and password **Admin@123**.)

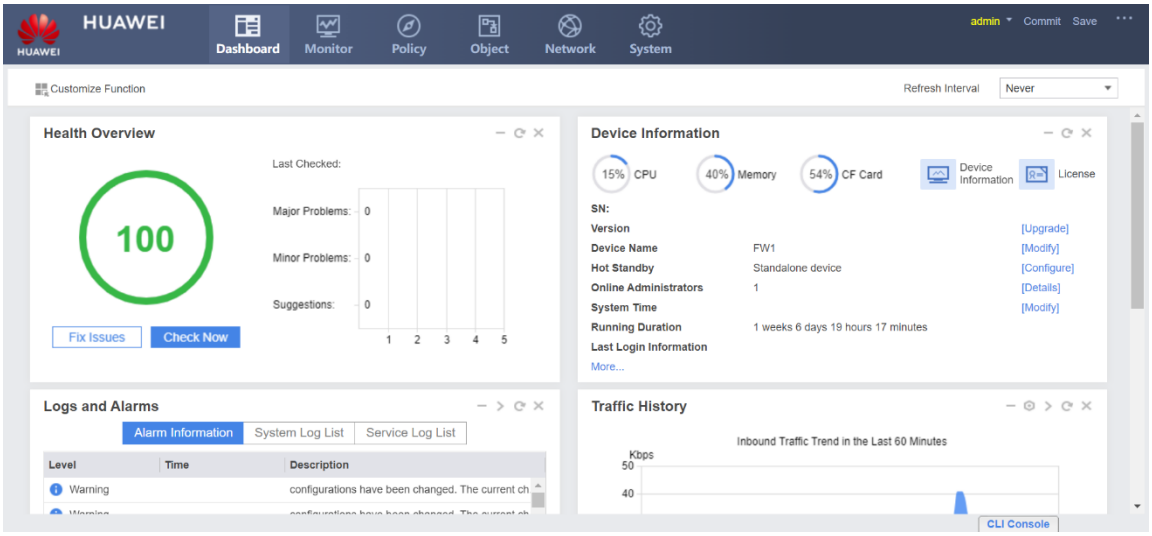


1.5.3 Verification

Enter the user name **admin** and its password **Admin@123**, and click **Login**.



If the following information is displayed in the browser, the login succeeds.



1.5.4 Quiz

By default, which interface is used for logging in to the device through the default web UI? Do you need to manually start the web service through the CLI?

Reference Answer:

By default, the interface for login through the web UI is GigabitEthernet0/0/0. You do not need to manually enable the web service or configure a security policy to allow traffic to pass through.

1.6 Logging In to the Device Through the Web UI

1.6.1 Introduction

1.6.1.1 About This Lab

After the firewall is added to the network, engineers want to log in to firewall management page through the management PC. In this case, the MGMT port is not connected to the network. The PC can log in to the device using the firewall service port through the web UI to manage and configure the device.

1.6.1.2 Objectives

- Through this lab, you will be able to use a PC to log in to the firewall through the web UI.

1.6.1.3 Networking Topology

Figure 1-6 Topology for logging in to a device through the web UI

1.6.1.4 Lab Planning

The PC uses an Ethernet cable to connect to GE0/0/1 of the device, and uses the web UI to log in to the device.

Table 1-6 Device ports and parameters

Device	Port	Port Type	IP Address	Description
Management PC	Network port	Ethernet port	10.1.2.100/24	
Firewall	GE0/0/1	Ethernet port	10.1.2.1/24	By default, the service port of the device does not support web login. Therefore, you need to enable the web function and configure the account and password for web login.

1.6.2 Lab Configuration

1.6.2.1 Configuration Roadmap

1. Use twisted pairs to connect the Ethernet port on the management PC to the service port on the device.
2. Configure the web login function of the device.
3. Log in to the device from the management PC through the web UI.

1.6.2.2 Configuration Procedure on the CLI

Step 1 Establish the connection, power on all devices, and ensure that they run properly.

Step 2 Log in to the device through other methods, for example, console, Telnet, and SSH. For details, see 1.1 Logging In to a Device Through the Console Port (PuTTY), 1.2 Getting Familiar with Commands (PuTTY), and 1.3 Logging In to a Device Through Telnet.

Step 3 Check whether the web server function is enabled. If not, run the following command to enable it:

```
[FW] web-manager security enable
```

Note: The **web-manager security enable** command enables HTTPS device management. If the **web-manager enable** command is used, HTTP device management is enabled. Do not use the same port for HTTPS and HTTP device management. Otherwise, port conflicts may occur.

Step 4 Configure the login port.

Configure an IP address and the access control function for the port.

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1] ip address 10.1.2.1 24
[FW-GigabitEthernet0/0/1] service-manage enable
[FW-GigabitEthernet0/0/1] service-manage https permit
[FW-GigabitEthernet0/0/1] quit
```

Add the port to a security zone.

```
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet 0/0/1
[FW-zone-trust] quit
```

Configure a security policy to allow the management PC to access GE0/0/1 of the firewall.

```
[FW] security-policy
[FW-policy-security] rule name trust-local
[FW-policy-security-rule-trust-local] source-zone trust
[FW-policy-security-rule-trust-local] destination-zone local
[FW-policy-security-rule-trust-local] action permit
```

Step 5 Configure an administrator.

```
[FW] aaa
[FW-aaa] manager-user webuser
[FW-aaa-manager-use-webuser] password cipher (Enter password)
[FW-aaa-manager-use-webuser] level 3
[FW-aaa-manager-use-webuser] service-type web
[FW-aaa-manager-use-webuser] quit
```

Bind a role to the administrator (optional, supported only by firewalls).

```
[FW-aaa] bind manager-user webuser role service-admin
```

Step 6 Set the IP address of the PC to 10.1.2.100/24. Visit https://10.1.2.1:8443 in the browser of the PC.

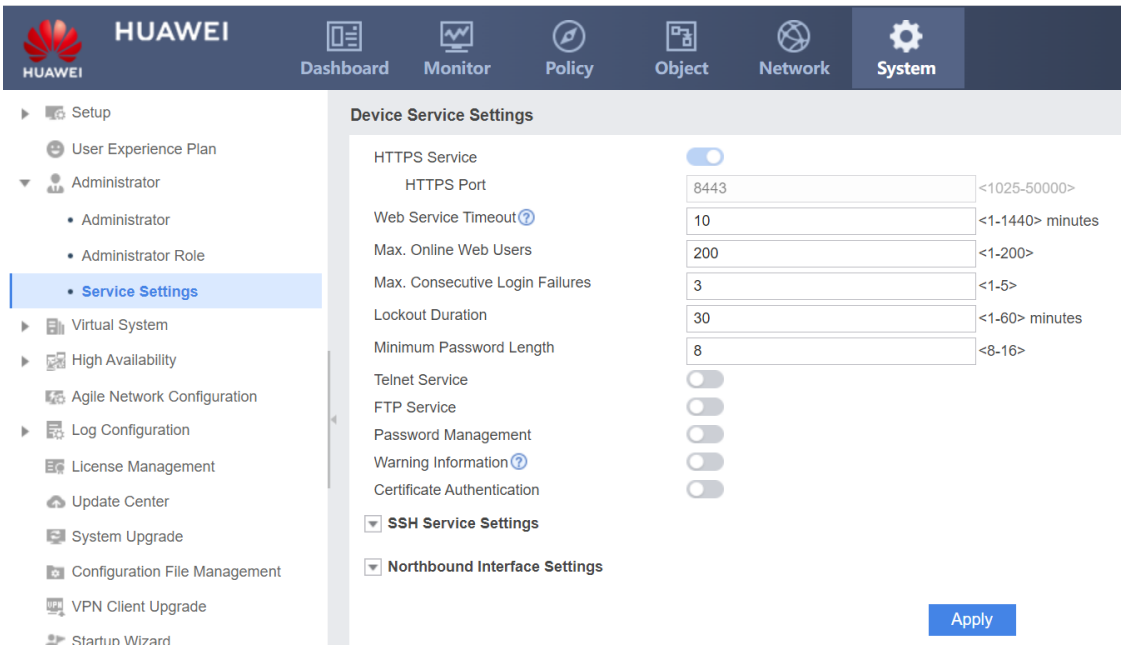
1.6.2.3 Configuration Procedure on the Web UI

Step 1 Establish the connection, power on all devices, and ensure that they run properly.

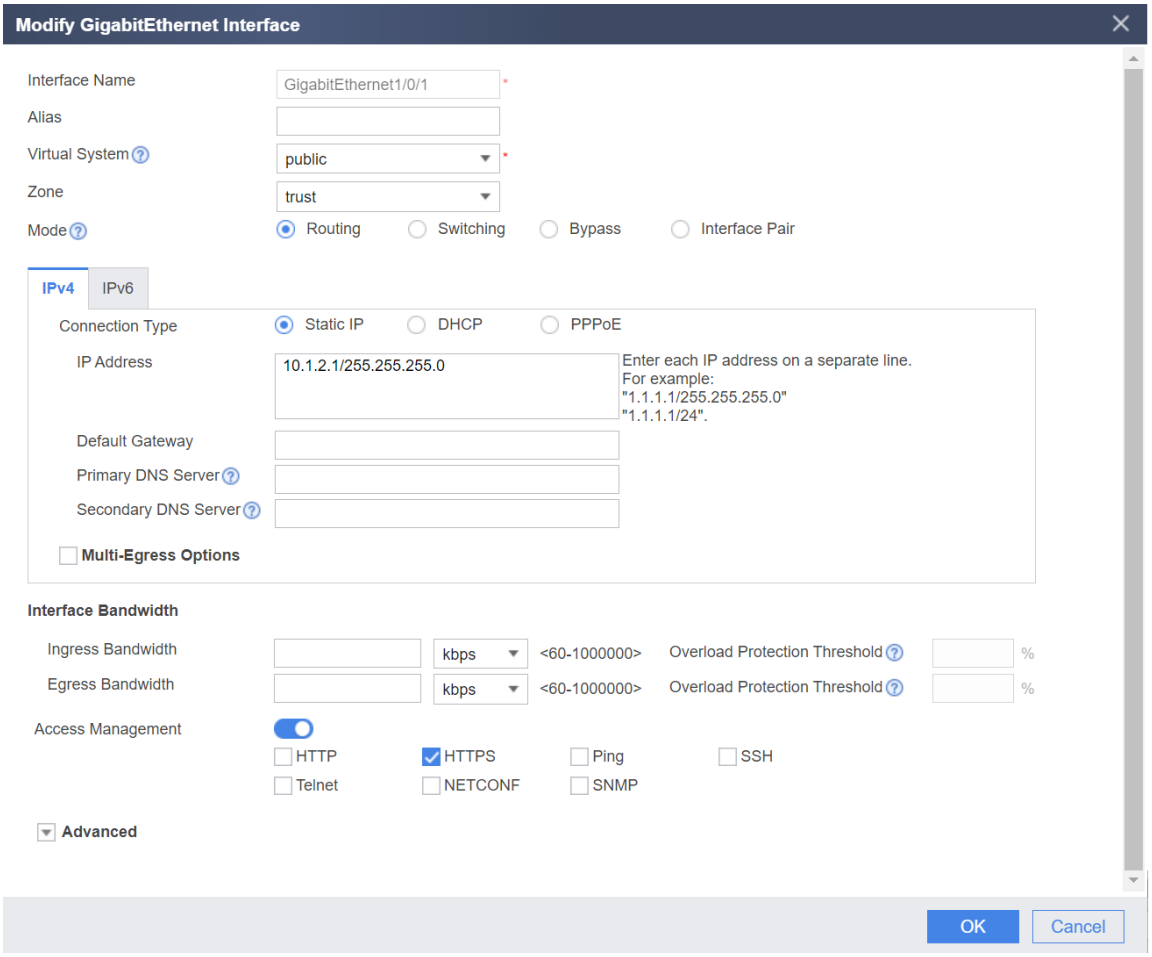
Step 2 Log in to the device in the default web mode. (For details, see 1.5 "Logging In to the Device Through the Default Web UI.")

Step 3 Enable the HTTPS service.

Choose **System** > **Administrator** > **Settings** and check whether the check box of the HTTPS service is enabled.

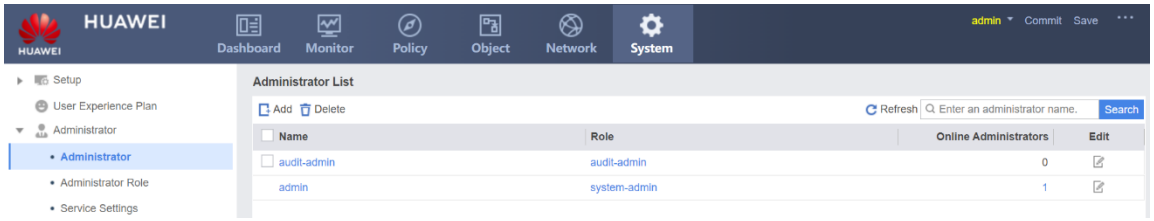


Configure the port used for login. Choose **Network** > **Interface** and click **Edit** on the line of GE0/0/1 to configure the IP address, security zone, and access control for the port.

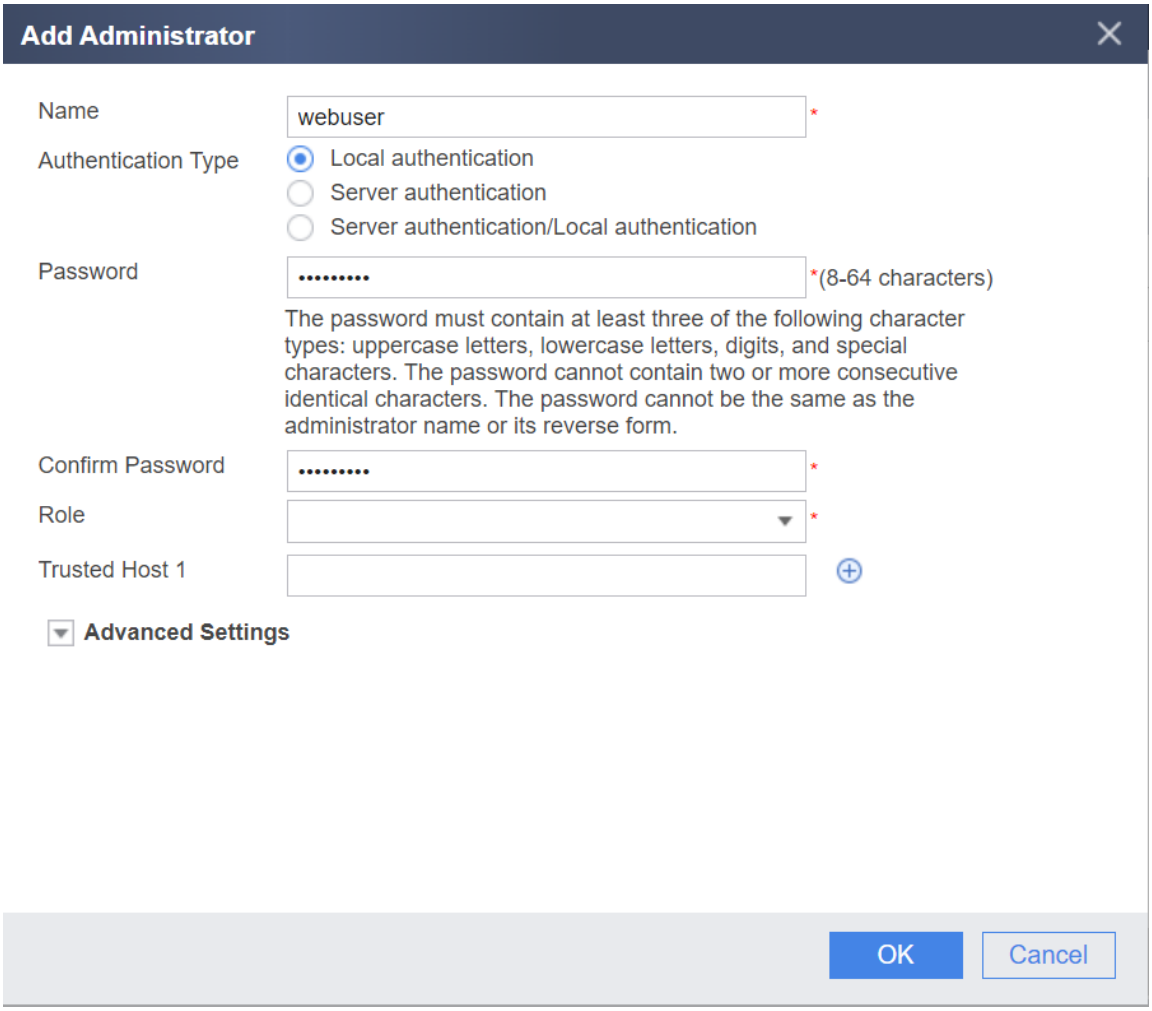


Configure an administrator.

Choose **System** > **Administrator** > **Administrator** and click **Add**.

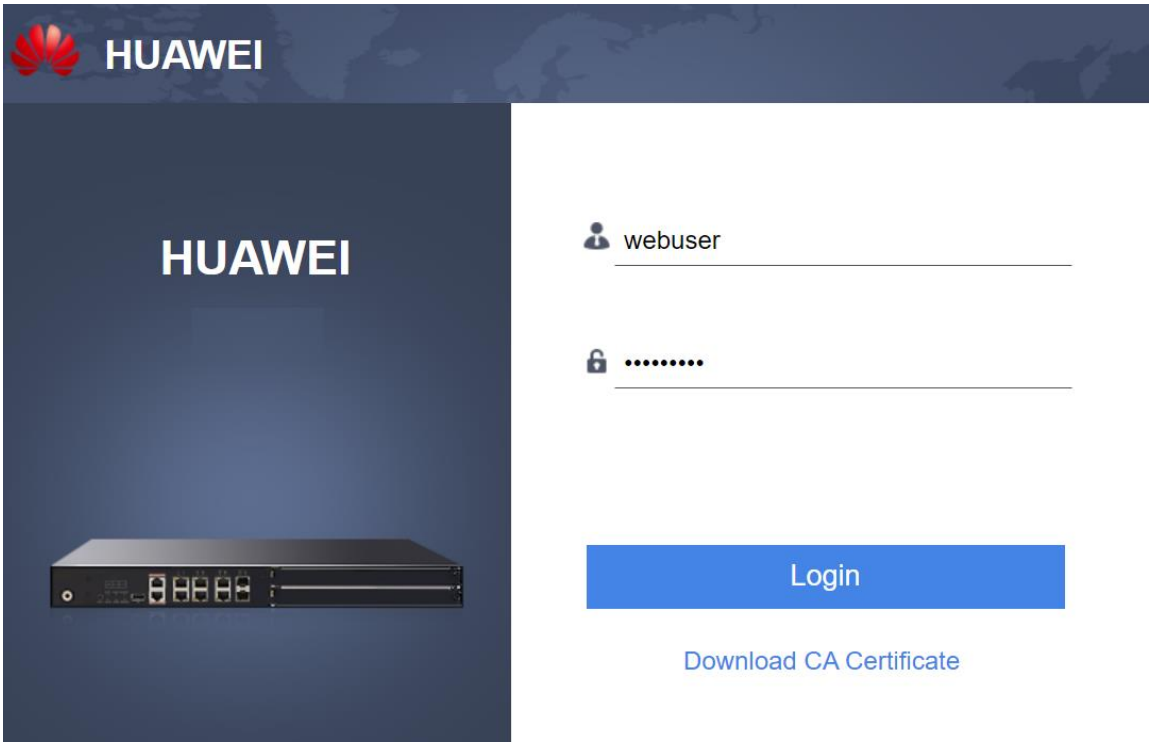


Set the web user name to **webuser**, password to **Admin@123**, and role to **system-admin**.

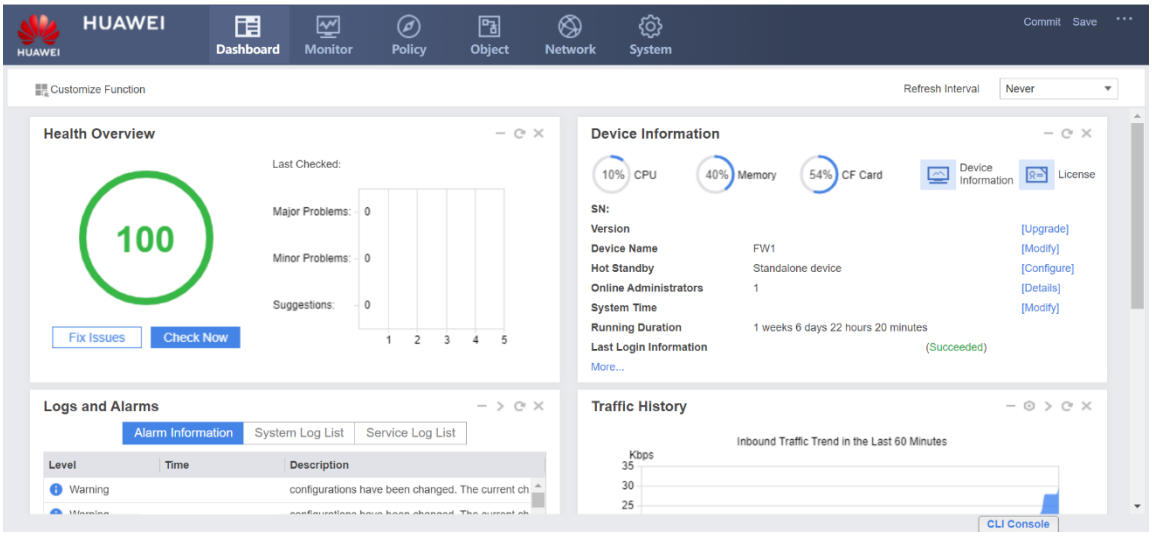


1.6.3 Verification

Access **https://10.1.2.1** in the browser on the PC, enter the user name **webuser** and password **Admin@123**, and click **Login**.



If the following information is displayed in the browser, the login succeeds.



1.6.4 Quiz

Which of the following key configurations are required for logging in to the device's web page through a non-management port?

Reference Answer:

1. The HTTPS access service must be enabled for the port.
2. The traffic policy needs to permit traffic from the security zone to which the port belongs to the local zone.
3. The HTTPS service needs to be enabled globally.

2 Firewall Security Policy

2.1 Introduction

2.1.1 About This Lab

During network deployment and maintenance, firewalls are required to protect the network. This lab introduces key concepts such as security zones and security policies. In this lab, security policies are deployed on firewalls to ensure that hosts in the trust zone can proactively access hosts in the untrust zone.

2.1.2 Objectives

- Understand the principles of security policies.
- Understand the relationship between different security zones.
- Configure firewall security policies using the CLI and web UI.

2.1.3 Networking Topology

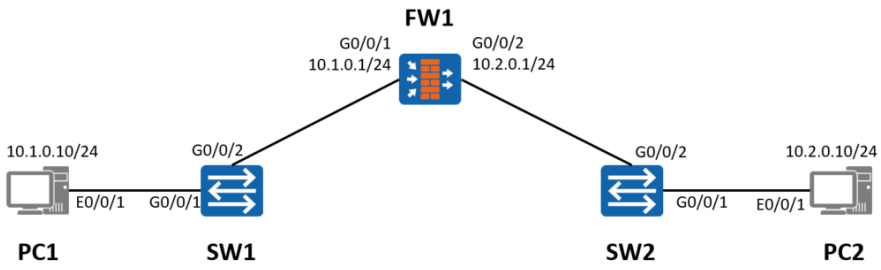


Figure 2-1 Topology for configuring firewall security policies

2.1.4 Lab Planning

FW1 is deployed between two networks. The upstream and downstream devices are switches, and the upstream and downstream service interfaces of FW1 work at Layer 3.

Table 2-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW1	GigabitEthernet0/0/1	10.1.0.1/24	trust
	GigabitEthernet0/0/2	10.2.0.1/24	untrust
PC1	Eth0/0/1	10.1.0.10/24	trust

Device	Interface	IP Address	Security Zone
PC2	Eth0/0/1	10.2.0.10/24	untrust

2.2 Lab Configuration

2.2.1 Configuration Roadmap

1. Configure basic IP addresses and security zones.
2. Configure an interzone security policy.
3. Configure the gateways of PC1 and PC2 to use IP addresses that are on the same network segment as those of the corresponding interfaces on the firewall.

2.2.2 Configuration Procedure on the CLI

Step 1 Complete the configurations of the upstream and downstream interfaces of FW1. Configure the IP addresses for interfaces and add them to security zones.

```
[FW1] interface G0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.1.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface G0/0/2
[FW1-GigabitEthernet0/0/2] ip address 10.2.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/2] quit
[FW1] firewall zone trust
[FW1-zone-trust] add interface G0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface G0/0/2
[FW1-zone-untrust] quit
```

Step 2 Configure a forwarding policy between the Trust zone and the Untrust zone.

```
[FW1] security-policy
[FW1-policy-security] rule name policy_sec
[FW1-policy-security-rule-policy_sec] source-zone trust
[FW1-policy-security-rule-policy_sec] destination-zone untrust
[FW1-policy-security-rule-policy_sec] action permit
[FW1-policy-security-rule-policy_sec] quit
```

Step 3 Configure the switch.

Add two interfaces of each switch to the default VLAN. For details, see the related switch document.

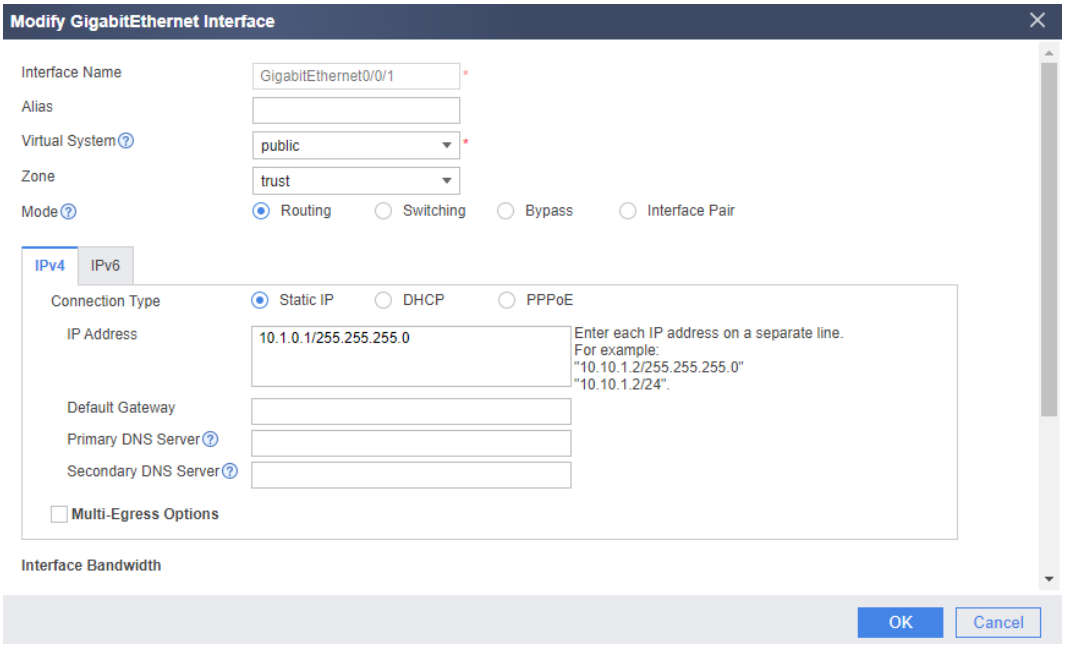
Step 4 Configure the PC.

Set the IP address of PC1 to **10.1.0.10/24** and that of the gateway to **10.1.0.1**. Set the IP address of PC2 to **10.2.0.10/24** and that of the gateway to **10.2.0.1**.

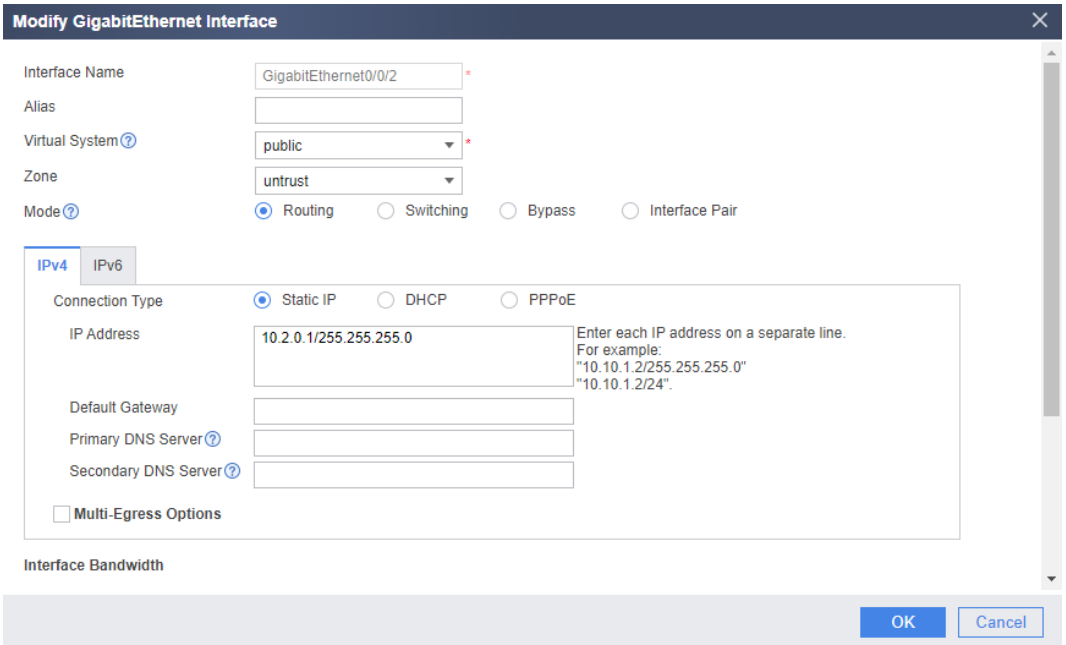
2.2.3 Configuration Procedure on the Web UI

Step 1 Complete the interface configuration on FW1.

Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/1, as shown in the following figure.

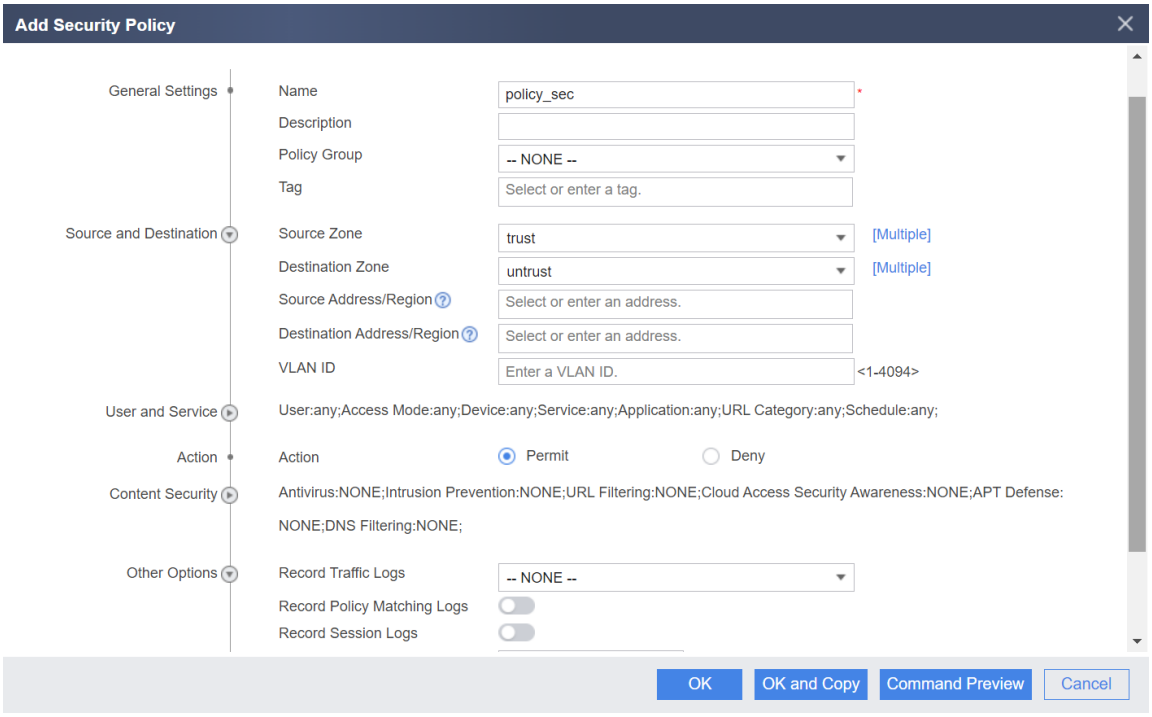


Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/2, as shown in the following figure.



Step 2 Configure an interzone forwarding policy on FW1.

Forwarding policy between **trust** and **untrust**: Choose **Policy** > **Security Policy** > **Security Policy**. In **Security Policy List**, click **Add**. Set or select each parameter in sequence. Click **OK**. The following figure shows the forwarding policy between the Trust and Untrust zones.



2.3 Verification

Ping **10.2.0.10** on the CLI from PC1 to check whether PC1 can ping PC2.

```
PC> ping 10.2.0.10
Ping 10.2.0.10: 32 data bytes, Press Ctrl_C to break
From 10.2.0.10: bytes=32 seq=1 ttl=127 time=16 ms
From 10.2.0.10: bytes=32 seq=2 ttl=127 time=16 ms
From 10.2.0.10: bytes=32 seq=3 ttl=127 time=15 ms
From 10.2.0.10: bytes=32 seq=4 ttl=127 time<1 ms
From 10.2.0.10: bytes=32 seq=5 ttl=127 time=16 ms
--- 10.2.0.10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 0/12/16 ms
```

Run the **display firewall session table** command to view the session table of the firewall.

```
[FW1] display firewall session table
Current Total Sessions : 1
icmp    VPN: public --> public    10.1.0.10:49569 --> 10.2.0.10:2048
```

2.4 Quiz

Based on the lab, ping PC1 from PC2, and explain why the ping operation fails.

Reference Answer:

The security policy in this lab only permits traffic from PC1 to PC2, but not from PC2 to PC1. Therefore, if PC2 initiates access to PC1, the packets will be discarded by the firewall's default security policy.

3 Firewall NAT Server and Source NAT

3.1 Introduction

3.1.1 About This Lab

An enterprise uses a firewall as the egress device. Employees in the enterprise need to access the Internet through the firewall, and one server in the enterprise network provides services for Internet users.

After NAT is configured on the egress firewall, multiple users on the intranet can access the Internet using a small number of public IP addresses, and extranet users can access the intranet server using specified IP addresses.

3.1.2 Objectives

- Understand the application scenarios and principles of Source NAT.
- Understand the application scenarios and principles of the NAT Server.
- Configure NAT Server and Source NAT commands through the CLI and web UI.

3.1.3 Networking Topology

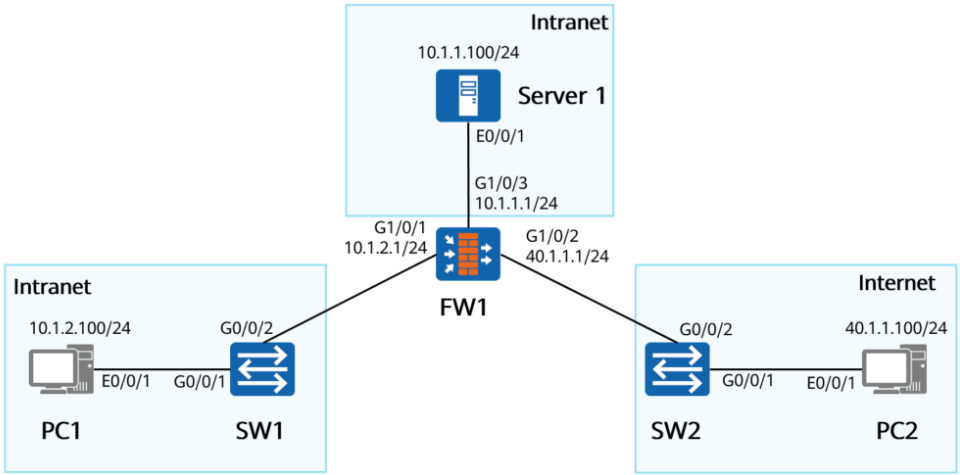


Figure 3-1 Topology for configuring the NAT Server and Source NAT for a firewall

3.1.4 Lab Planning

FW1 is deployed at the egress of the network. The upstream and downstream devices are switches.

Table 3-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW1	GigabitEthernet0/0/1	10.1.2.1/24	trust
	GigabitEthernet0/0/2	40.1.1.1/24	untrust
	GigabitEthernet0/0/3	10.1.1.1/24	dmz
PC1	Eth0/0/1	10.1.2.100/24	trust
PC2	Eth0/0/1	40.1.1.100/24	untrust
Server 1	Eth0/0/1	10.1.1.100/24	dmz

3.2 Lab Configuration (Source NAT)

3.2.1 Configuration Roadmap

1. Configure basic IP addresses, security zones, and security policies.
2. Configure a NAT address pool.
3. Configure a NAT policy.

3.2.2 Configuration Procedure on the CLI

Step 1 Configure the upstream and downstream service interfaces of FW1. Configure the IP addresses for interfaces and add them to security zones.

Configure IP addresses for the upstream and downstream service interfaces of FW1.

```
<FW1> system-view
[FW1] interface G0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.1.2.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface G0/0/2
[FW1-GigabitEthernet0/0/2] ip address 40.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/2] quit
[FW1] interface G0/0/3
[FW1-GigabitEthernet0/0/3] ip address 10.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/3] quit
```

Add the interfaces of FW1 to the corresponding security zones.

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface G0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface G0/0/2
[FW1-zone-untrust] quit
[FW1] firewall zone dmz
```

```
[FW1-zone-dmz] add interface G0/0/3
[FW1-zone-dmz] quit
```

Step 2 Configure a forwarding policy between the Trust and Untrust zones.

```
[FW1] security-policy
[FW1-policy-security] rule name policy_sec
[FW1-policy-security-rule-policy_sec] source-zone trust
[FW1-policy-security-rule-policy_sec] destination-zone untrust
[FW1-policy-security-rule-policy_sec] action permit
[FW1-policy-security-rule-policy_sec] quit
```

Step 3 Configure a NAT address pool and set the public IP address range from 2.2.2.2 to 2.2.2.5.

```
[FW1] nat address-group natpool
[FW1-address-group-natpool] section 2.2.2.2 2.2.2.5
```

Step 4 Configure a NAT policy.

```
[FW1] nat-policy
[FW1-policy-nat] rule name source_nat
[FW1-policy-nat-rule-source_nat] destination-zone untrust
[FW1-policy-nat-rule-source_nat] source-zone trust
[FW1-policy-nat-rule-source_nat] action source-nat address-group natpool
```

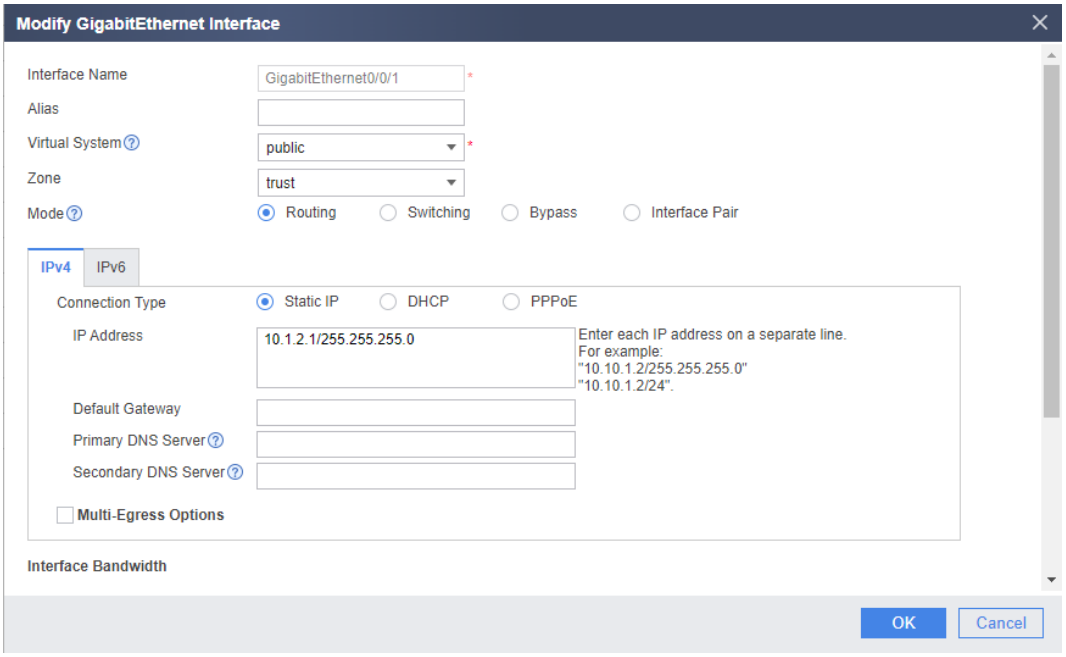
Step 5 Configure the switches.

Add two interfaces of each switch to the default VLAN. For details, see the related switch document.

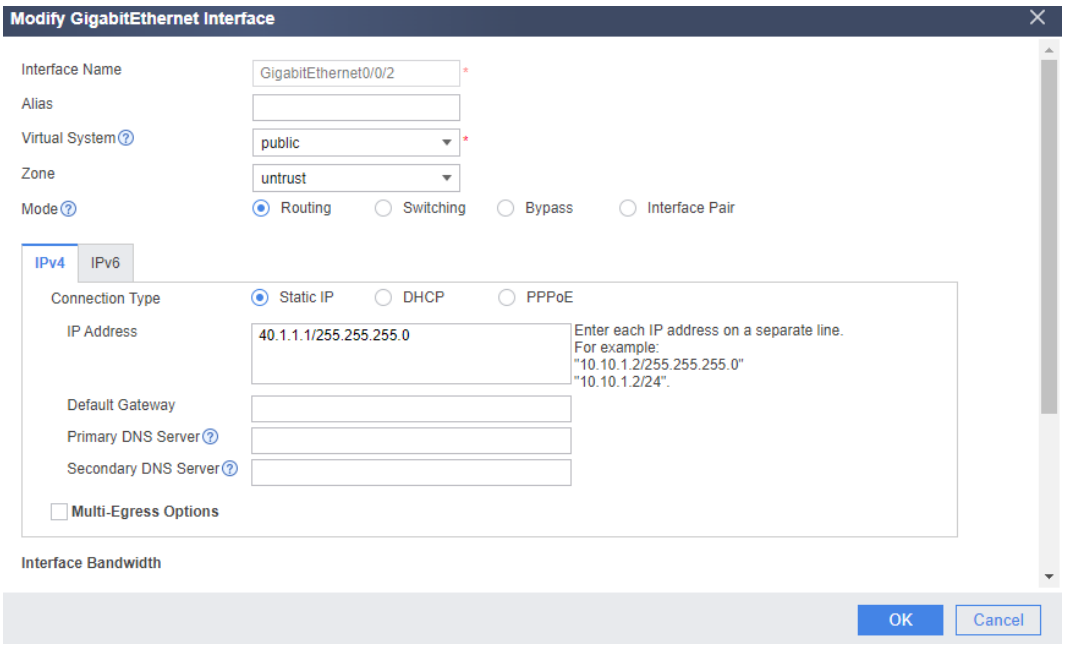
3.2.3 Configuration Procedure on the Web UI

Step 1 Configure interfaces on FW1.

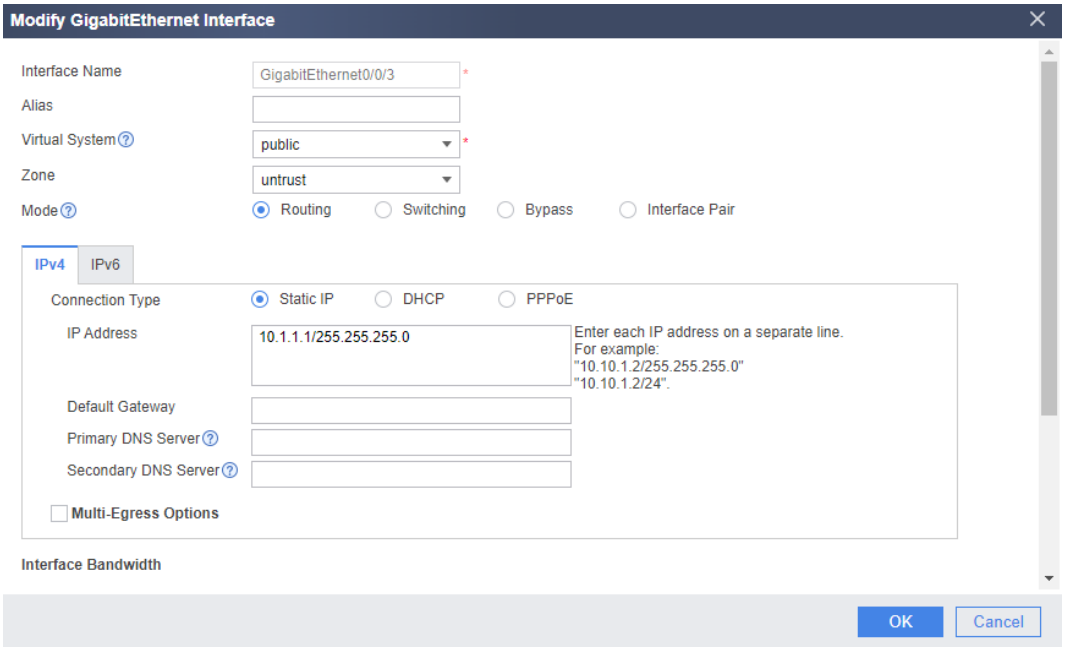
Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/1, as shown in the following figure.



Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/2, as shown in the following figure.

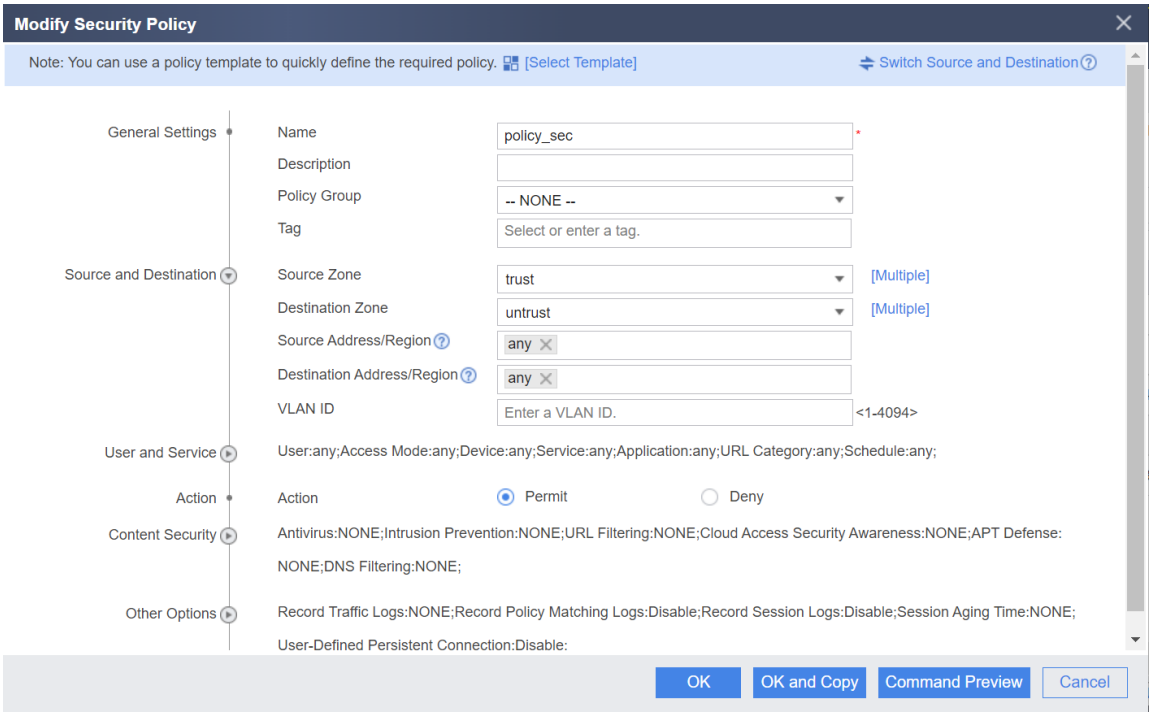


Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/3, as shown in the following figure.



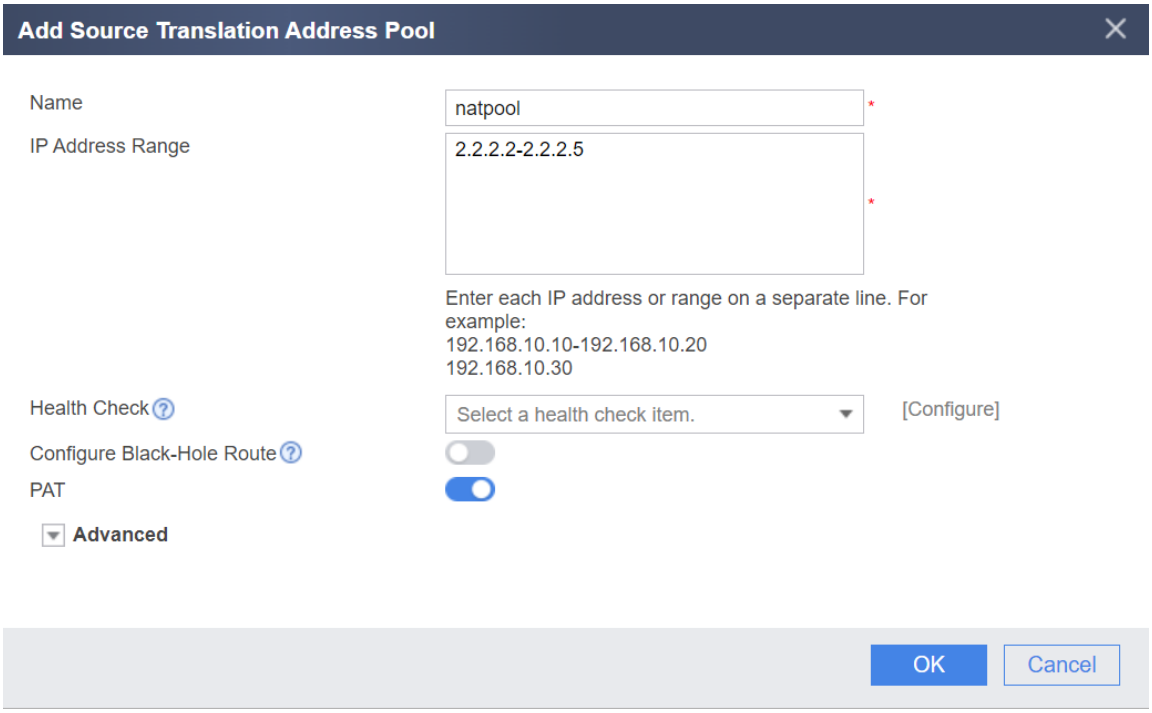
Step 2 Configure an interzone forwarding policy for FW1.

Choose **Policy** > **Security Policy** > **Security Policy**. In the **Security Policy List** area, click **Add**, set or select parameters, and click **OK**. Configure the interzone forwarding policy between the Trust and Untrust zones, as shown in the following figure.



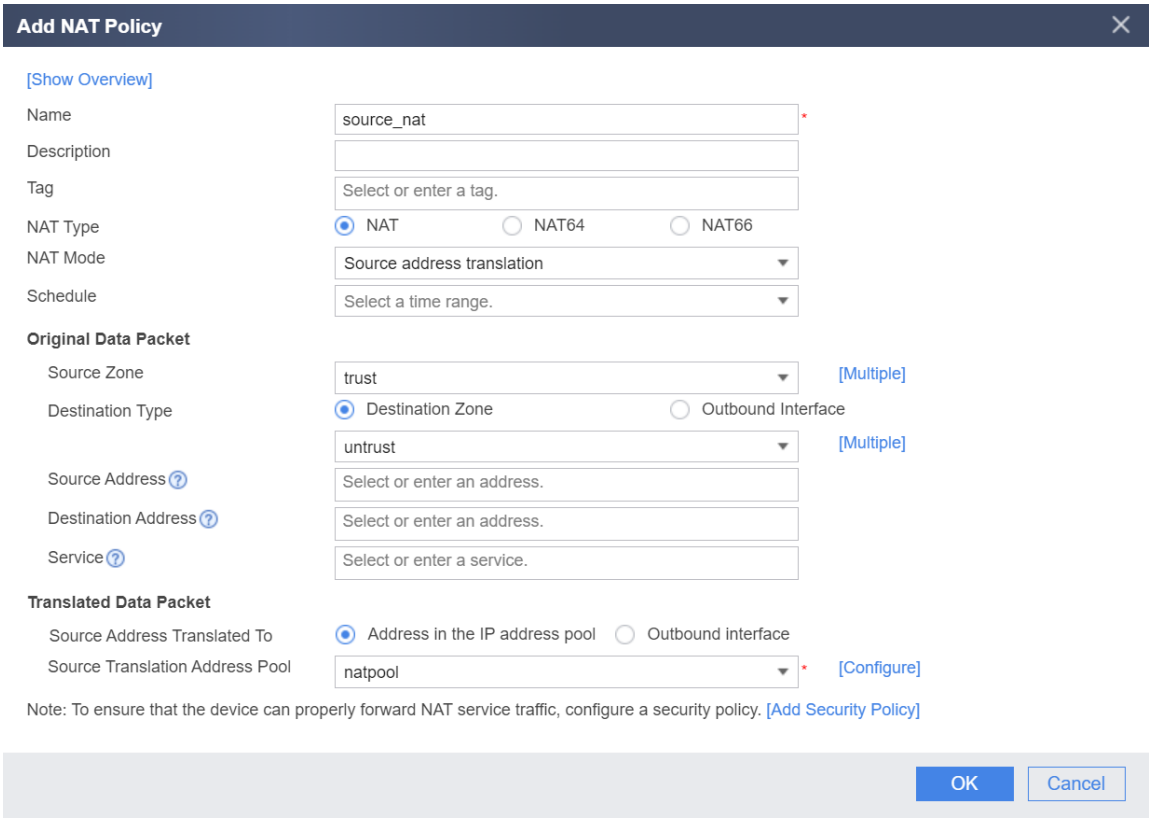
Step 3 Configure a NAT address pool. The public IP addresses range from 2.2.2.2 to 2.2.2.5.

Choose **Policy** > **NAT Policy**. Click the **Source Translation Address Pool** tab. In **Source Translation Address Pool**, click and create an address pool. Then, click **OK**. The following figure shows the detailed configurations.



Step 4 Configure a NAT policy.

Choose **Policy** > **NAT Policy**. Click the **NAT Policy** tab. In the **NAT Policy List** area, click and create a NAT policy. Then, click **OK**. The following figure shows the detailed configurations.



3.2.4 Verification

Ping PC2 from PC1.

```
PC> ping 40.1.1.100

Ping 40.1.1.100: 32 data bytes, Press Ctrl_C to break
From 40.1.1.100: bytes=32 seq=1 ttl=127 time=16 ms
From 40.1.1.100: bytes=32 seq=2 ttl=127 time=16 ms
From 40.1.1.100: bytes=32 seq=3 ttl=127 time<1 ms
From 40.1.1.100: bytes=32 seq=4 ttl=127 time=15 ms
From 40.1.1.100: bytes=32 seq=5 ttl=127 time=16 ms

--- 40.1.1.100 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 0/12/16 ms
```

Run the **display firewall session table** command on FW1 to check the session table.

```
[FW1] display firewall session table
 Current Total Sessions : 5
  icmp    VPN: public --> public    10.1.2.100:56279[2.2.2.5:2057] -->40.1.1.100:2048
  icmp    VPN: public --> public    10.1.2.100:55255[2.2.2.5:2053] -->40.1.1.100:2048
  icmp    VPN: public --> public    10.1.2.100:56023[2.2.2.5:2056] -->40.1.1.100:2048
  icmp    VPN: public --> public    10.1.2.100:55767[2.2.2.5:2055] -->40.1.1.100:2048
  icmp    VPN: public --> public    10.1.2.100:55511[2.2.2.5:2054] -->40.1.1.100:2048
```

You can see that the firewall translates the source address 10.1.2.100 into 2.2.2.5 in the NAT address pool to communicate with PC2.

3.2.5 Quiz

What are the differences between NAPT and NAT No-PAT in Source NAT? Which scenarios are they applicable to?

Reference Answer:

NAPT translates both IP addresses and ports. It enables multiple private IP addresses to share one or more public IP addresses to access the public network resources. NAPT applies to scenarios where only a small number of public addresses are available for many private network users to access the Internet.

NAT No-PAT translates only IP addresses but not ports. It translates private IP addresses to public IP addresses in a one-to-one relationship. NAT No-PAT applies to scenarios where there are a small number of Internet access users and the number of public IP addresses is the same as the number of concurrent Internet access users.

3.3 Lab Configuration (NAT Server and Source NAT)

3.3.1 Configuration Roadmap

1. Configure basic IP addresses, security zones, and security policies.
2. Configure a NAT server.
3. Configure a NAT address pool.
4. Configure a NAT policy.

3.3.2 Configuration Procedure on the CLI

Step 1 Configure the upstream and downstream service interfaces of FW1. Configure the IP addresses for interfaces and add them to security zones.

Configure IP addresses for the upstream and downstream service interfaces of FW1.

```
<FW1> system-view
[FW1] interface G0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.1.2.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface G0/0/2
[FW1-GigabitEthernet0/0/2] ip address 40.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/2] quit
[FW1] interface G0/0/3
[FW1-GigabitEthernet0/0/3] ip address 10.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/3] quit
```

Step 2 Configure a forwarding policy between the Untrust and DMZ zones.

```
[FW1] security-policy
```

```
[FW1-policy-security] rule name bidectinal_nat
[FW1-policy-security-rule-policy_sec] source-zone untrust
[FW1-policy-security-rule-policy_sec] destination-zone dmz
[FW1-policy-security-rule-policy_sec] action permit
[FW1-policy-security-rule-policy_sec] service ftp
[FW1-policy-security-rule-policy_sec] quit
```

Step 3 Configure a NAT server.

```
[FW1] nat server ftpserver protocol tcp global 40.1.1.2 ftp inside 10.1.1.100 ftp
```

Step 4 Configure a NAT address pool.

```
[FW1] nat address-group natpool2
[FW1-address-group-natpool] section 10.1.1.10 10.1.1.20
```

Step 5 Apply the NAT ALG function between the DMZ and Untrust zones, so that the server can provide the FTP service for external systems properly. By default, NAT ALG is enabled globally. You can skip this step.

```
[FW1] firewall interzone dmz untrust
[FW1-interzone-dmz-untrust] detect ftp
[FW1-interzone-dmz-untrust] quit
```

Step 6 Create the NAT policy between the DMZ and Untrust zones, define the range of source IP addresses for NAT, and bind the NAT policy to natpool2.

```
[FW1] nat-policy
[FW1-policy-nat] rule name source_nat
[FW1-policy-nat-rule-source_nat] destination-zone dmz
[FW1-policy-nat-rule-source_nat] source-zone untrust
[FW1-policy-nat-rule-source_nat] source-address 40.1.1.0 24
[FW1-policy-nat-rule-source_nat] action nat address-group natpool2
```

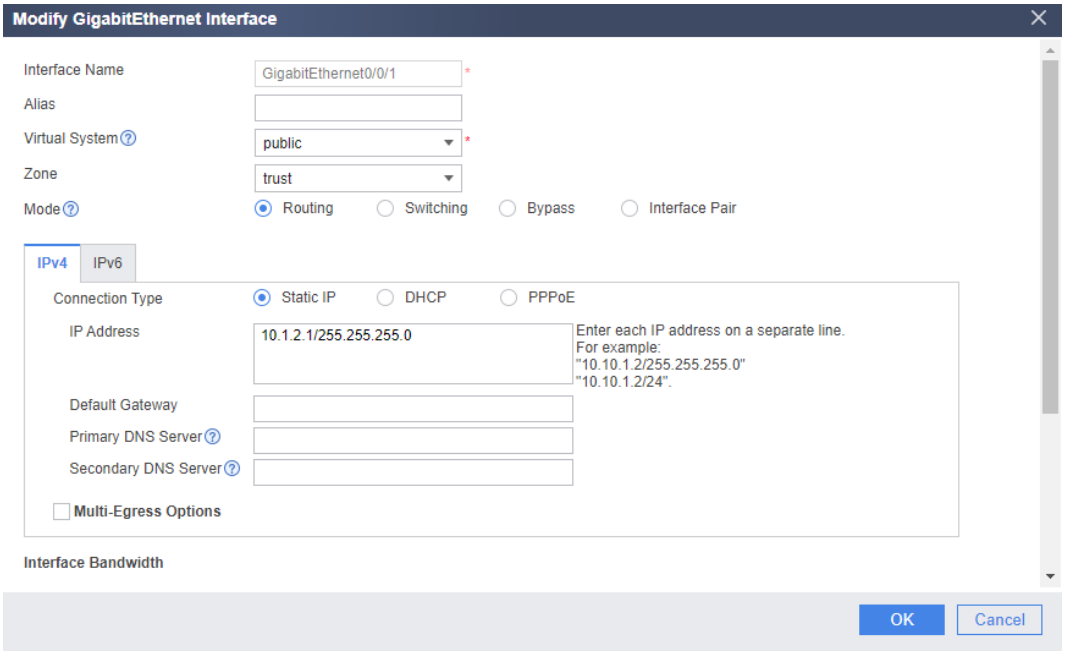
Step 7 Configure the switches.

Add two interfaces of each switch to the default VLAN. For details, see the related switch document.

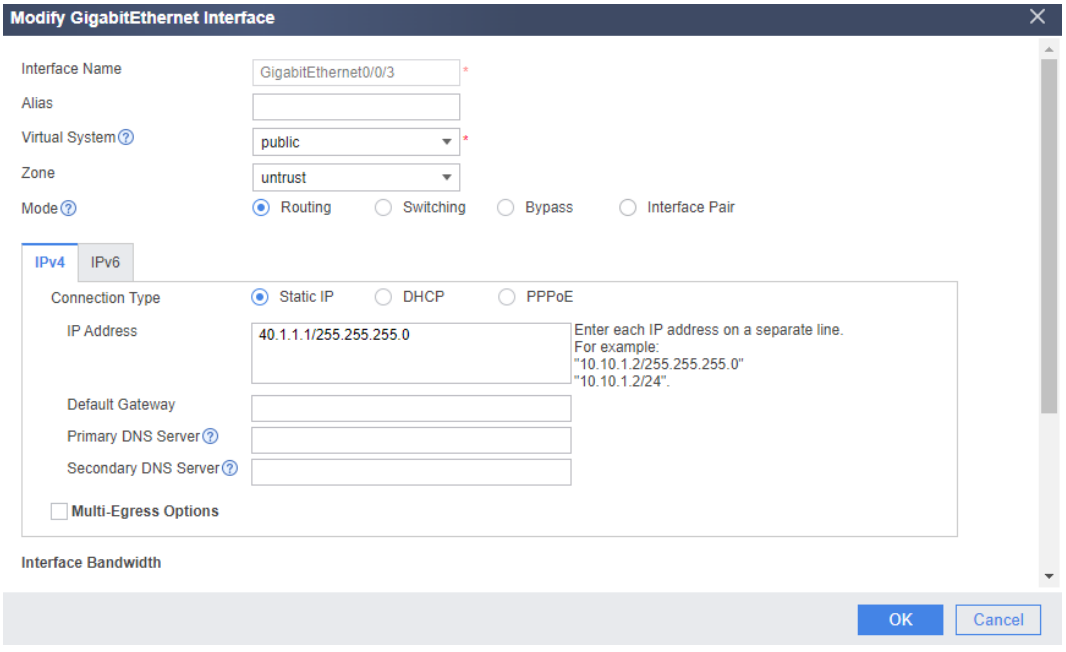
3.3.3 Configuration Procedure on the Web UI

Step 1 Configure interfaces on FW1.

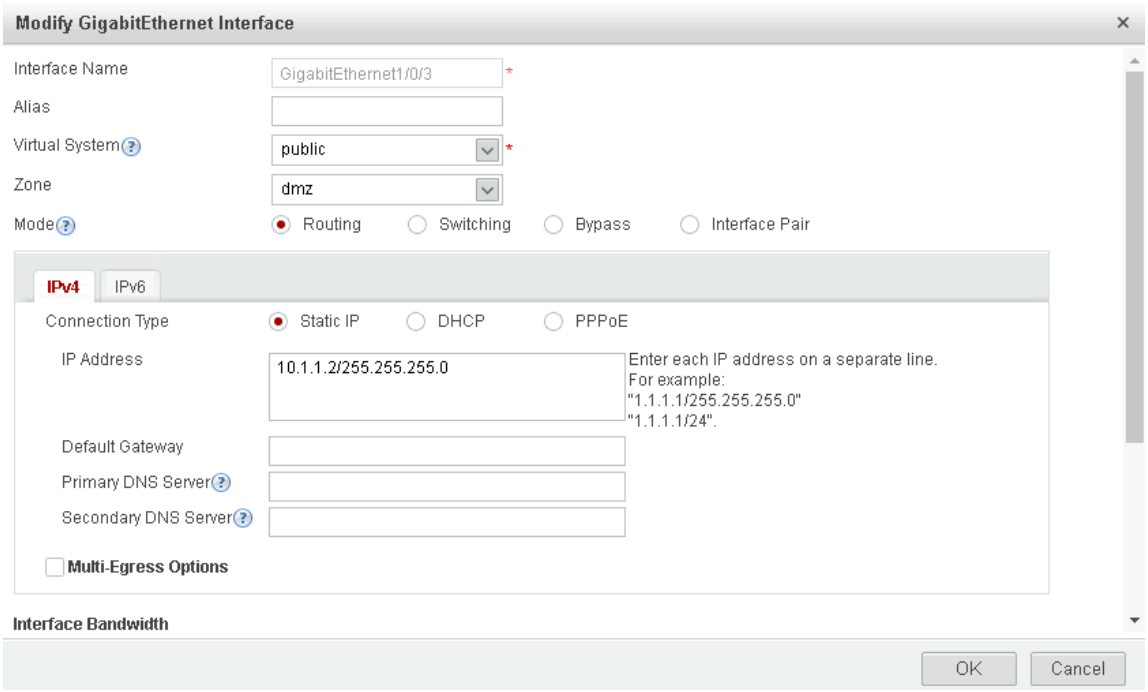
Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/1, as shown in the following figure.



Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/2, as shown in the following figure.

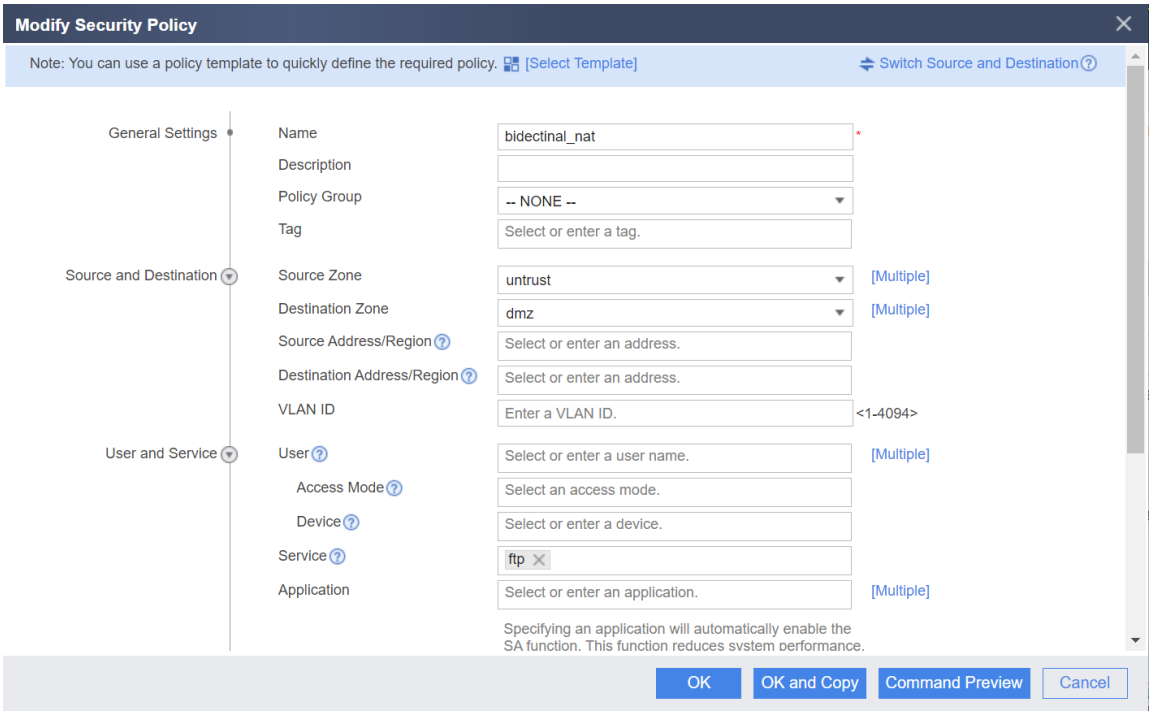


Choose **Network** > **Interface**, and click the button next to the interface to be configured. Select or set parameters and click **OK**. Configure the interface GigabitEthernet0/0/3, as shown in the following figure.



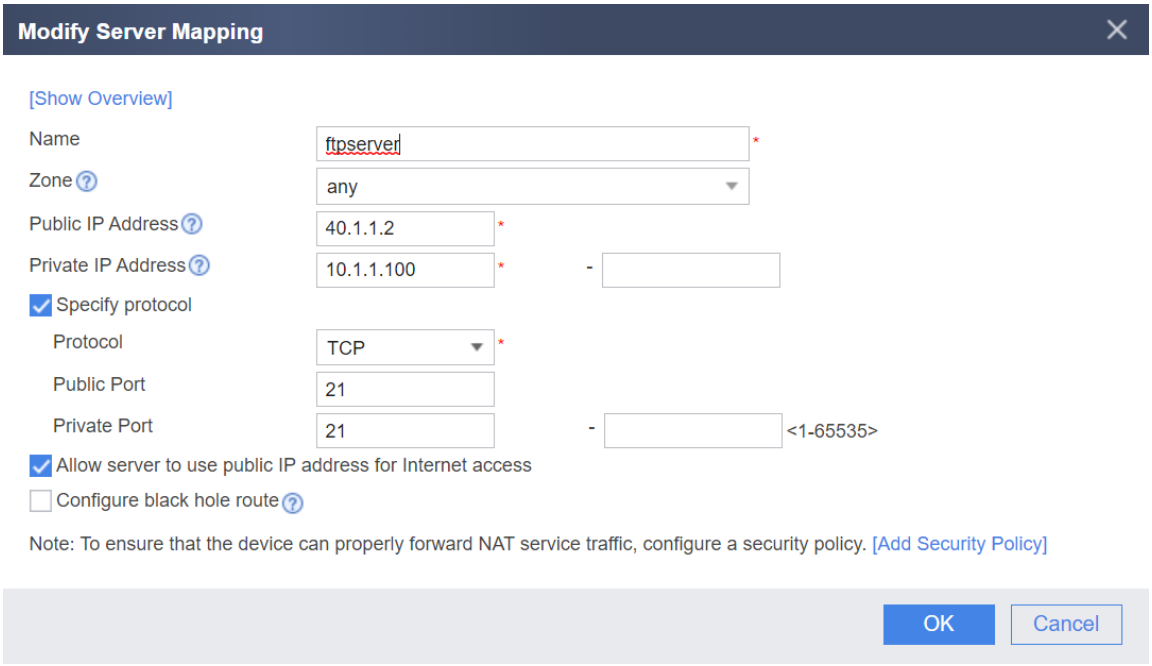
Step 2 Configure an interzone forwarding policy of FW1.

Choose **Policy** > **Security Policy** > **Security Policy**. In **Security Policy List**, click **Add**. Set or select each parameter in sequence. Click **OK**. Configure the forwarding policy between the Untrust and DMZ zones, as shown in the following figure.



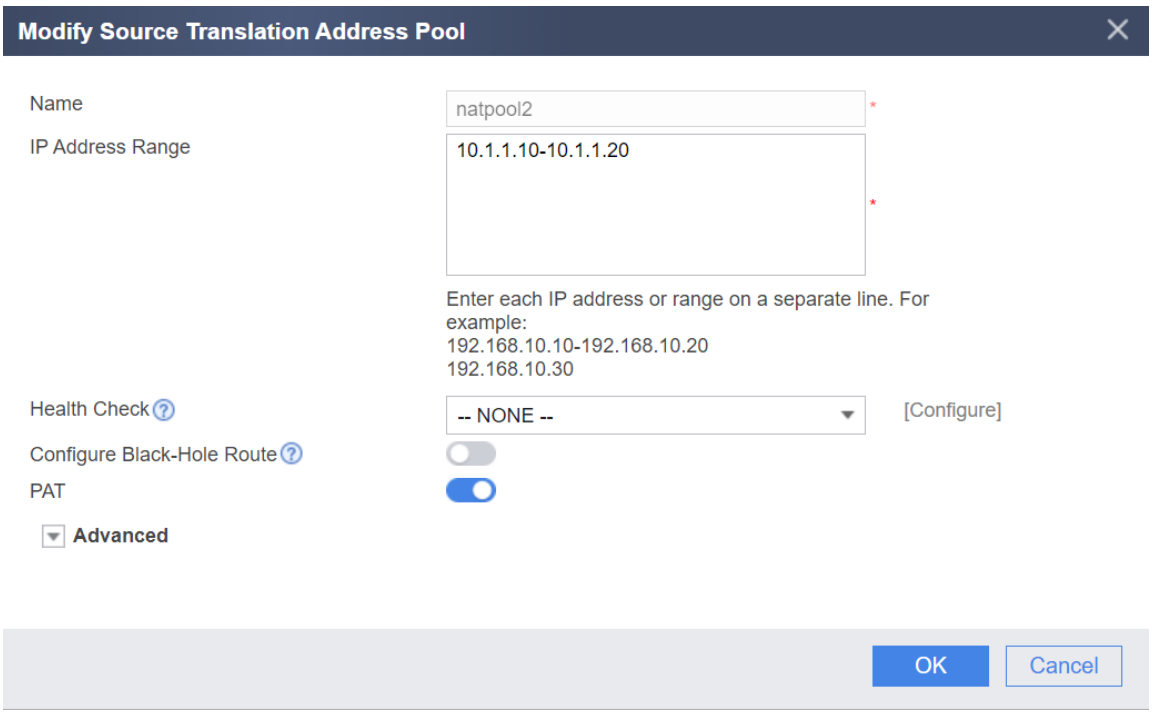
Step 3 Configure a NAT server.

Choose **Policy** > **NAT Policy** > **Server Mapping**. In **Server Mapping List**, click and configure a NAT server. Then, click **OK**. The following figure shows the detailed configurations.



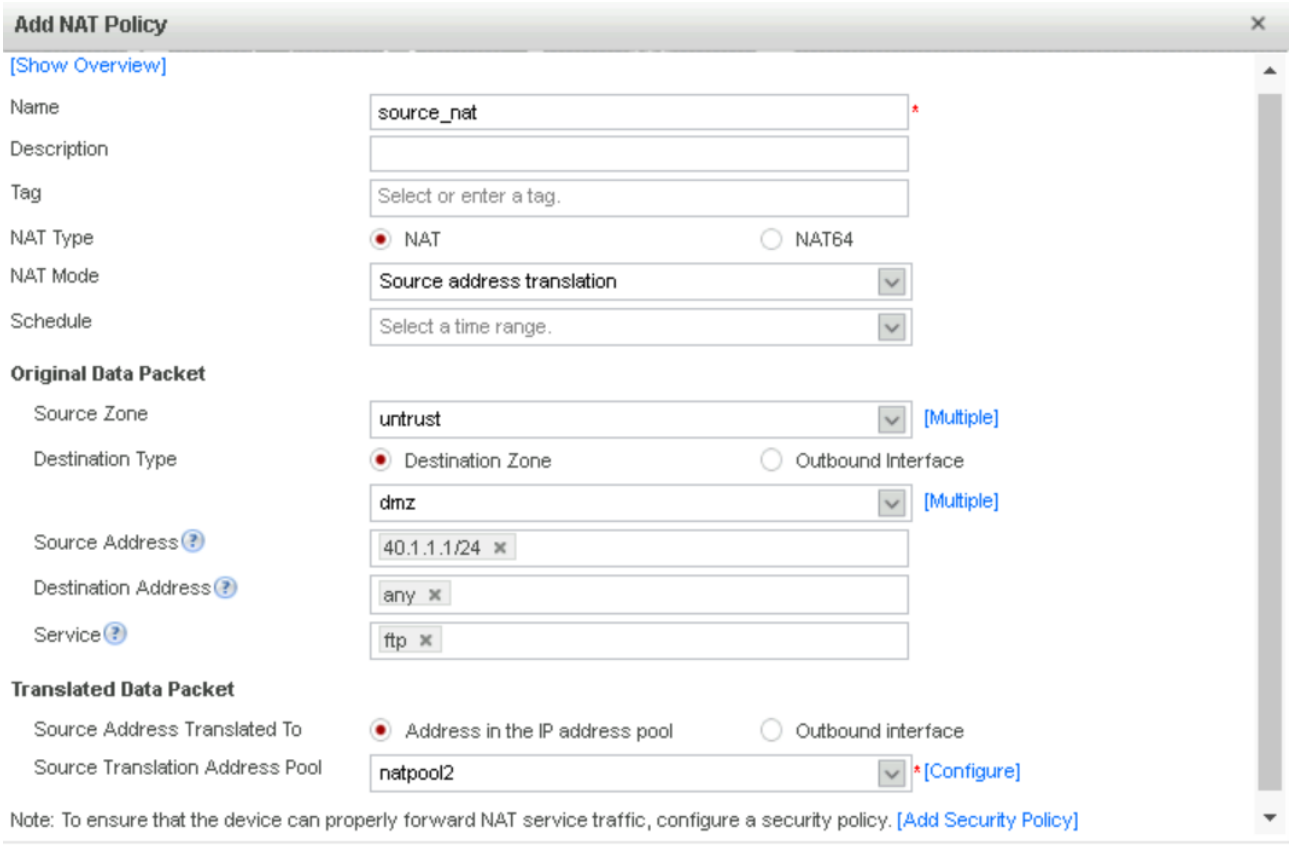
Step 4 Configure a NAT address pool.

Choose **Policy** > **NAT Policy**. Click the **Source Translation Address Pool** tab. In **Source Translation Address Pool**, click and create an address pool. Then, click **OK**. The following figure shows the detailed configurations.



Step 5 Configure a NAT policy.

Choose **Policy** > **NAT Policy**. Click the **NAT Policy** tab. In **NAT Policy List**, click and create a NAT policy. Then, click **OK**. The following figure shows the detailed configurations.



3.3.4 Verification

Check related information on the firewall.

```
[FW1] display nat server
Server in private network information:
  Total     1 NAT server(s)
 server name    : ftpserver
 id                  : 0                   zone              : ---
 global-start-addr   : 40.1.1.2            global-end-addr     : 40.1.1.2
 inside-start-addr     : 10.1.1.100          inside-end-addr     : 10.1.1.100
 global-start-port   : 21(ftp)             global-end-port     : 21
 inside-start-port   : 21(ftp)             inside-end-port     : 21
 globalvpn : public            insidevpn       : public
 vsys           : public                protocol        : tcp
 vrrp           : ---                   no-revers       : 0
 interface      : ---                   vrrp-bind-interface: ---
 unr-route : 1                          description     : ---
 nat-disable : 0
```

3.3.5 Quiz

When an external network user accesses the intranet server through a specific IP address, what are the processing steps for packets reaching the firewall?

Reference Answer:

1. The first packet arrives at the firewall.
2. The NAT server configuration is matched, and destination address translation is performed.
3. The routing table is searched.
4. The security policy is matched.
5. A session is created.

4 Firewall Hot Standby

4.1 Introduction

4.1.1 About This Lab

An enterprise needs to provide uninterrupted services. To avoid line interruption caused by network devices or other external factors, the enterprise wants to implement redundancy at the network egress to increase network reliability.

In this lab, two firewalls are deployed as gateways at the network egress to ensure smooth communication between the internal network and the external network in the case of a single-node fault.

4.1.2 Objectives

- Understand the basic principles of hot standby.
- Understand the VGMP and HRP protocols.
- Master the configuration of firewall hot standby using the CLI and web UI.

4.1.3 Networking Topology

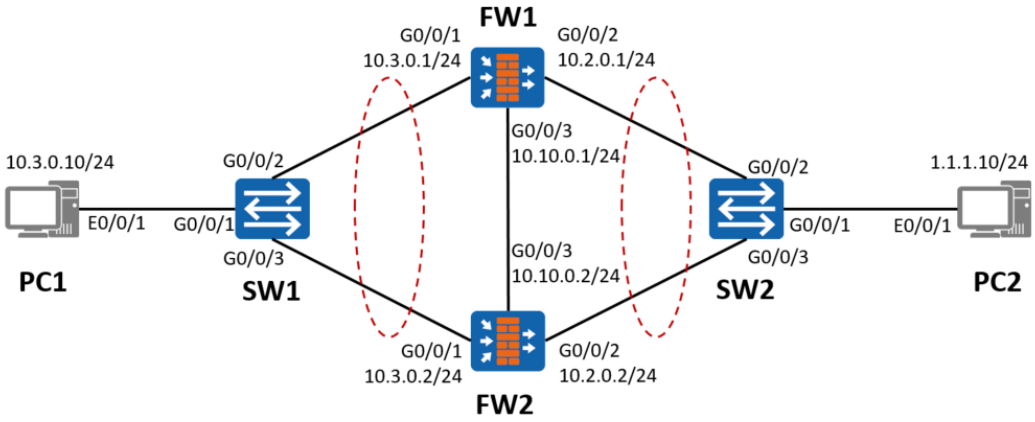


Figure 4-1 Networking topology for configuring firewall hot standby

4.1.4 Lab Planning

The firewalls are deployed as security devices at the network egress. The upstream and downstream devices are switches. FW1 and FW2 work in active/standby mode.

Table 4-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW1	GigabitEthernet0/0/1	10.3.0.1/24	trust
	GigabitEthernet0/0/2	10.2.0.1/24	untrust
	GigabitEthernet0/0/3	10.10.0.1/24	dmz
FW2	GigabitEthernet0/0/1	10.3.0.2/24	trust
	GigabitEthernet0/0/2	10.2.0.2/24	untrust
	GigabitEthernet0/0/3	10.10.0.2/24	dmz
PC1	Eth0/0/1	10.3.0.10/24	trust
PC2	Eth0/0/1	1.1.1.10/24	untrust
SW1	GigabitEthernet0/0/1 GigabitEthernet0/0/2 GigabitEthernet0/0/3	Access	PVID: VLAN 10
SW2	GigabitEthernet0/0/1 GigabitEthernet0/0/2 GigabitEthernet0/0/3	Access	PVID: VLAN 10

4.2 Lab Configuration

4.2.1 Configuration Roadmap

1. Configure the basic IP addresses and security zones on FW1 and FW2, and apply the relevant security policies.
2. Configure the hot standby. FW1 functions as the active node and FW2 functions as the standby node.

4.2.2 Configuration Procedure on the CLI

Step 1 Configure the upstream and downstream service interfaces of FW1 and FW2. Configure the IP addresses for interfaces and add them to security zones.

Configure IP addresses for the upstream and downstream service interfaces of FW1.

```
<FW1> system-view
[FW1] interface GigabitEthernet0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.3.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface GigabitEthernet0/0/2
[FW1-GigabitEthernet0/0/2] ip address 10.2.0.1 255.255.255.0
```

```
[FW1-GigabitEthernet0/0/2] quit
```

Configure VRRP group 1 on GigabitEthernet0/0/1 of FW1 and add it to the VGMP group in the **Active** state.

```
[FW1] interface GigabitEthernet0/0/1
[FW1-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 active
[FW1-GigabitEthernet0/0/1] quit
```

Configure VRRP group 2 on GigabitEthernet0/0/2 of FW1 and add it to the VGMP group in the **Active** state.

```
[FW1] interface GigabitEthernet0/0/2
[FW1-GigabitEthernet0/0/2] vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 active
[FW1-GigabitEthernet0/0/2] quit
```

Add the upstream and downstream service interfaces of FW1 to security zones.

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface GigabitEthernet0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GigabitEthernet0/0/2
[FW1-zone-untrust] quit
```

Configure the upstream and downstream service interfaces of FW2.

```
<FW2> system-view
[FW2] interface GigabitEthernet0/0/1
[FW2-GigabitEthernet0/0/1] ip address 10.3.0.2 255.255.255.0
[FW2-GigabitEthernet0/0/1] quit
[FW2] interface GigabitEthernet0/0/2
[FW2-GigabitEthernet0/0/2] ip address 10.2.0.2 255.255.255.0
[FW2-GigabitEthernet0/0/2] quit
```

Configure VRRP group 1 on GigabitEthernet0/0/1 of FW2 and add it to the VGMP group in the **Standby** state.

```
[FW2] interface GigabitEthernet0/0/1
[FW2-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 standby
[FW2-GigabitEthernet0/0/1] quit
```

Configure VRRP group 2 on GigabitEthernet0/0/2 of FW2 and add it to the VGMP group in the **Standby** state.

```
[FW2] interface GigabitEthernet0/0/2
[FW2-GigabitEthernet0/0/2] vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 standby
[FW2-GigabitEthernet0/0/2] quit
```

Add the upstream and downstream service interfaces of FW2 to security zones.

```
[FW2] firewall zone trust
```

```
[FW2-zone-trust] add interface GigabitEthernet 0/0/1
[FW2-zone-trust] quit
[FW2] firewall zone untrust
[FW2-zone-untrust] add interface GigabitEthernet 0/0/2
[FW2-zone-untrust] quit
```

Step 2 Configure the heartbeat cables for FW1 and FW2.

Configure an IP address for the heartbeat interface GigabitEthernet0/0/3 of FW1.

```
[FW1] interface GigabitEthernet0/0/3
[FW1-GigabitEthernet0/0/3] ip address 10.10.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/3] quit
```

Configure an IP address for the heartbeat interface GigabitEthernet0/0/3 of FW2.

```
[FW2] interface GigabitEthernet0/0/3
[FW2-GigabitEthernet0/0/3] ip address 10.10.0.2 255.255.255.0
[FW2-GigabitEthernet0/0/3] quit
```

Add the heartbeat interface GigabitEthernet0/0/3 of FW1 to the DMZ.

```
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface GigabitEthernet0/0/3
[FW1-zone-dmz] quit
```

Add the heartbeat interface GigabitEthernet0/0/3 of FW2 to the DMZ.

```
[FW2] firewall zone dmz
[FW2-zone-dmz] add interface GigabitEthernet0/0/3
[FW2-zone-dmz] quit
```

Configure the authentication key for the heartbeat interface of FW1 and enable the hot standby function.

```
[FW1] hrp interface GigabitEthernet0/0/3 remote 10.10.0.2
[FW1] hrp authentication-key Admin@123
[FW1] hrp enable
```

Configure the authentication key for the heartbeat interface of FW2 and enable the hot standby function.

```
[FW2] hrp interface GigabitEthernet0/0/3 remote 10.10.0.1
[FW2] hrp authentication-key Admin@123
[FW2] hrp enable
```

Step 3 Configure a security policy on FW1 to allow service packets to pass through. After hot standby is enabled, the security policy configured on FW1 will be automatically synchronized to FW2.

Configure a forwarding policy between the Trust and Untrust zones on FW1.

```
HRP_M[FW1] security-policy
HRP_M[FW1-policy-security] rule name trust_to_untrust
HRP_M[FW1-policy-security-rule-trust_to_untrust] source-zone trust
HRP_M[FW1-policy-security-rule-trust_to_untrust] destination-zone untrust
HRP_M[FW1-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
HRP_M[FW1-policy-security-rule-trust_to_untrust] action permit
HRP_M[FW1-policy-security-rule-trust_to_untrust] quit
HRP_M[FW1-policy-security] quit
```

Step 4 Configure a NAT policy on FW1. After hot standby is enabled, the NAT policy configured on FW1 will be automatically synchronized to FW2.

Configure a NAT policy to translate source addresses on subnet 10.3.0.0/24 to IP addresses in the NAT address pool (1.1.1.2 to 1.1.1.5) when intranet users access the Internet.

```
HRP_M[FW1] nat address-group group1
HRP_M[FW1-address-group-group1] section 0 1.1.1.2 1.1.1.5
HRP_M[FW1-address-group-group1] quit
HRP_M[FW1] nat-policy
HRP_M[FW1-policy-nat] rule name policy_nat1
HRP_M[FW1-policy-nat-rule-policy_nat1] source-zone trust
HRP_M[FW1-policy-nat-rule-policy_nat1] destination-zone untrust
HRP_M[FW1-policy-nat-rule-policy_nat1] source-address 10.3.0.0 24
HRP_M[FW1-policy-nat-rule-policy_nat1] action source-nat address-group group1
```

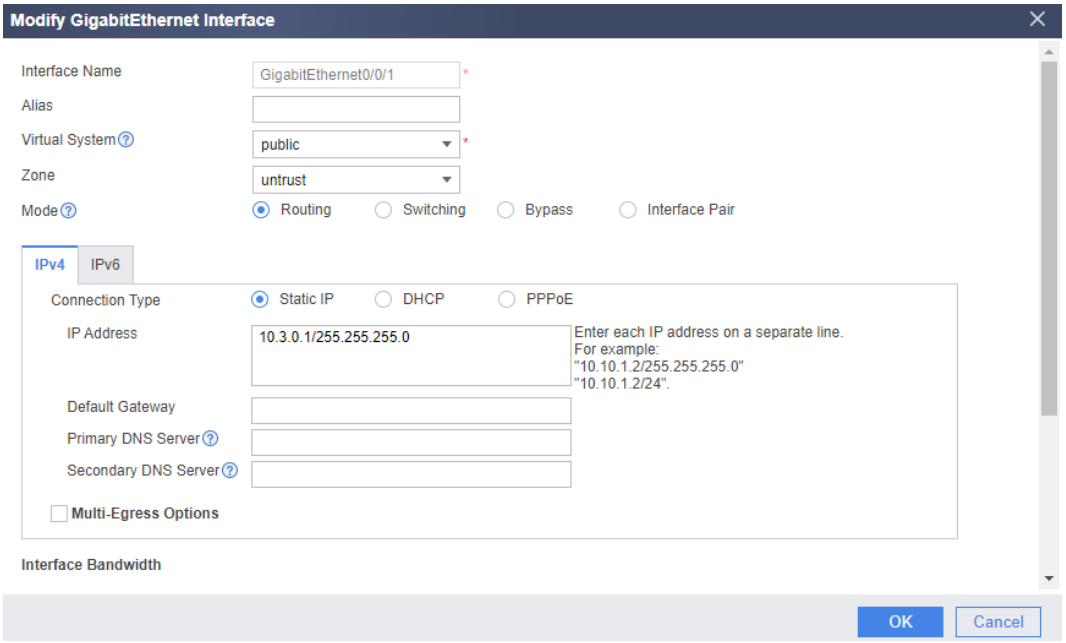
Step 5 Configure the switches.

Add the three interfaces of SW1 and SW2 to VLAN 10. For details, see the related switch document.

4.2.3 Configuration Procedure on the Web UI

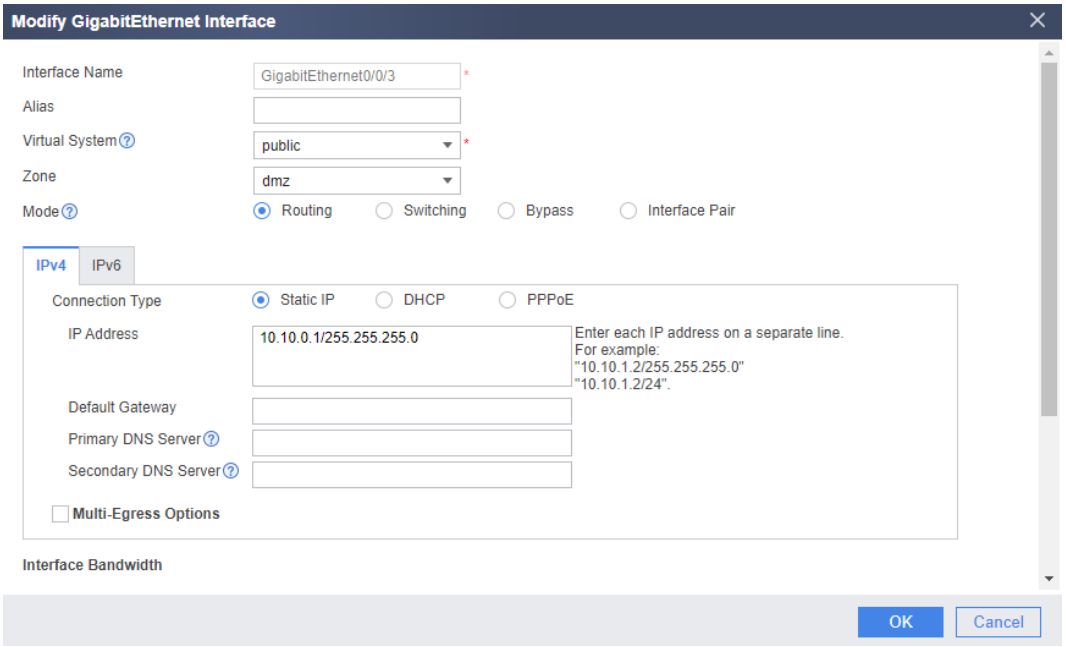
Step 1 Configure the upstream and downstream service interfaces of FW1 and FW2. Configure the IP addresses for interfaces and add them to security zones.

Configure the interfaces on FW1. Choose **Network** > **Interface** and click the button next to the interface to be configured. Set parameters, and then click **OK**. The following figure shows the configuration of the GigabitEthernet0/0/1 interface.



The configurations of GigabitEthernet0/0/2 and GigabitEthernet0/0/3 on FW1 and GigabitEthernet0/0/1, GigabitEthernet0/0/2, and GigabitEthernet0/0/3 on FW2 are similar.

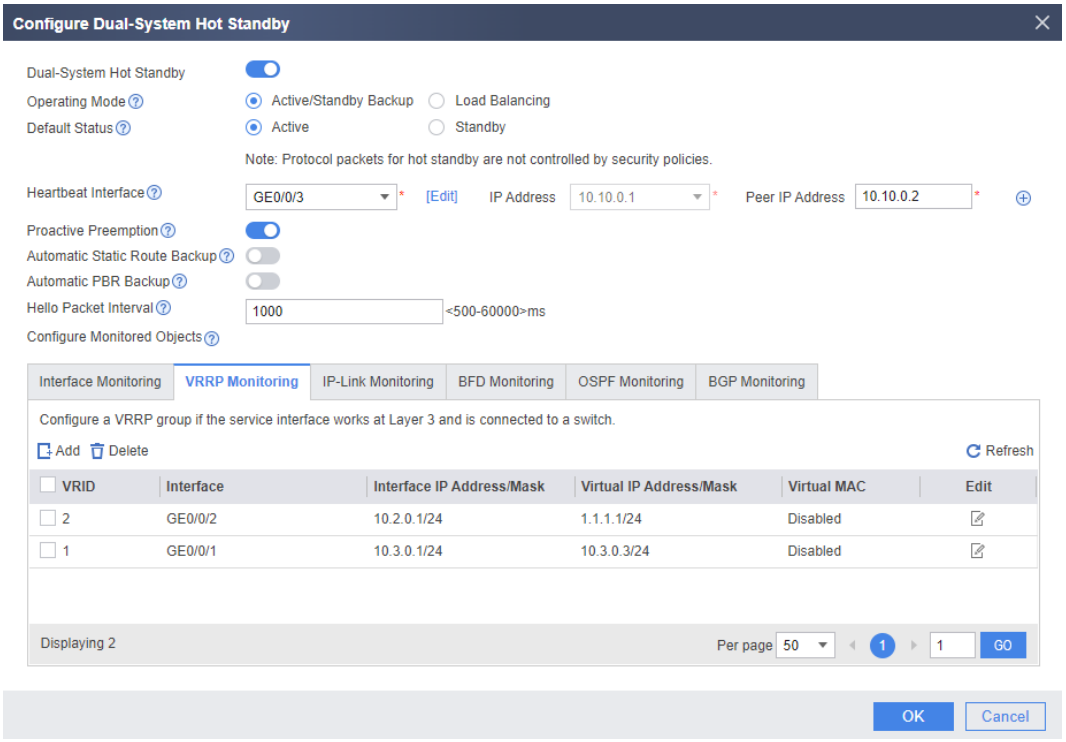
Step 2 Configure the heartbeat cables for FW1 and FW2.



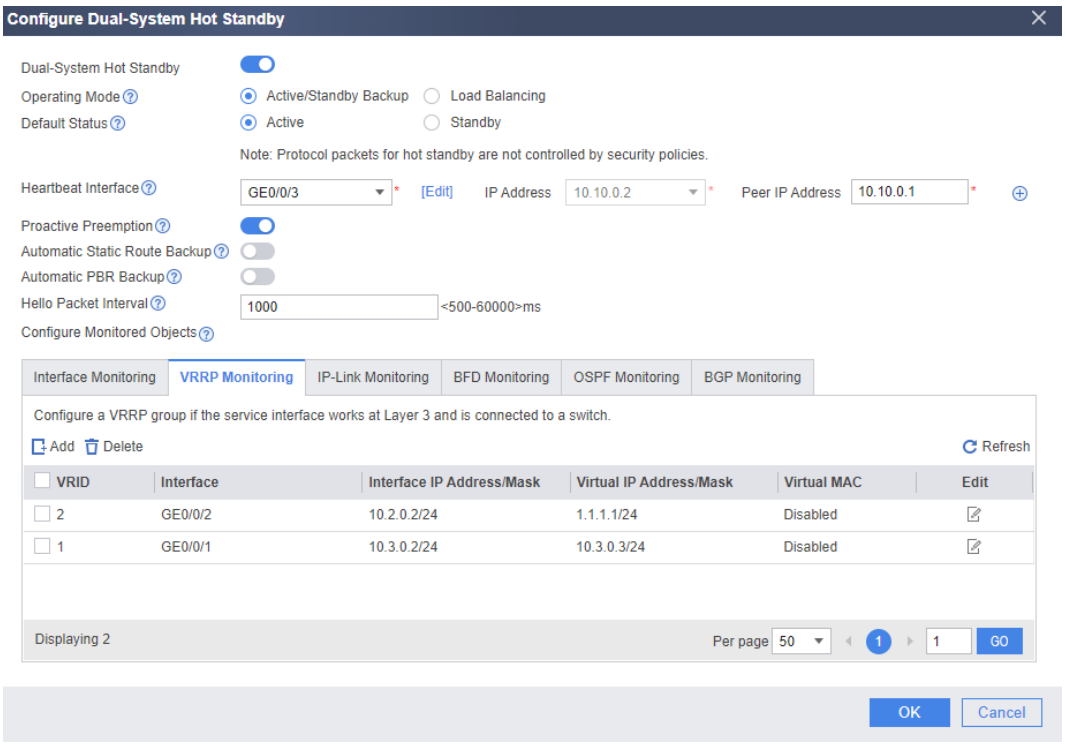
The configuration of GigabitEthernet0/0/3 on FW2 is similar.

Step 3 Configure hot standby on FW1 and FW2.

FW1:

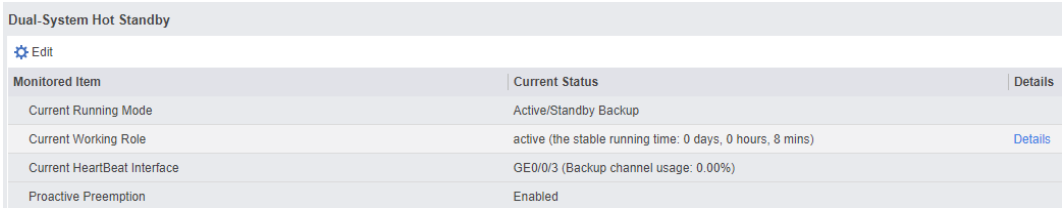


FW2:

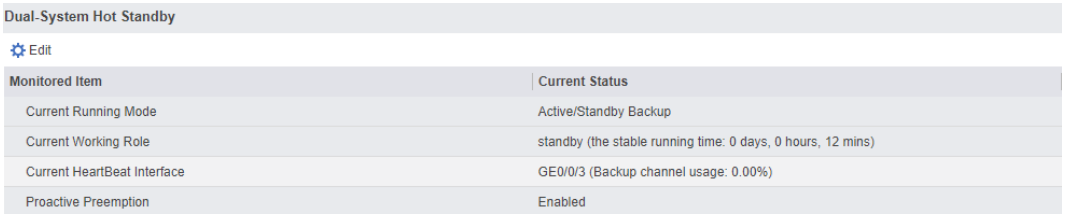


Step 4 On the **Dual-System Hot Standby** page, view the hot standby status.

Hot standby status of FW1:



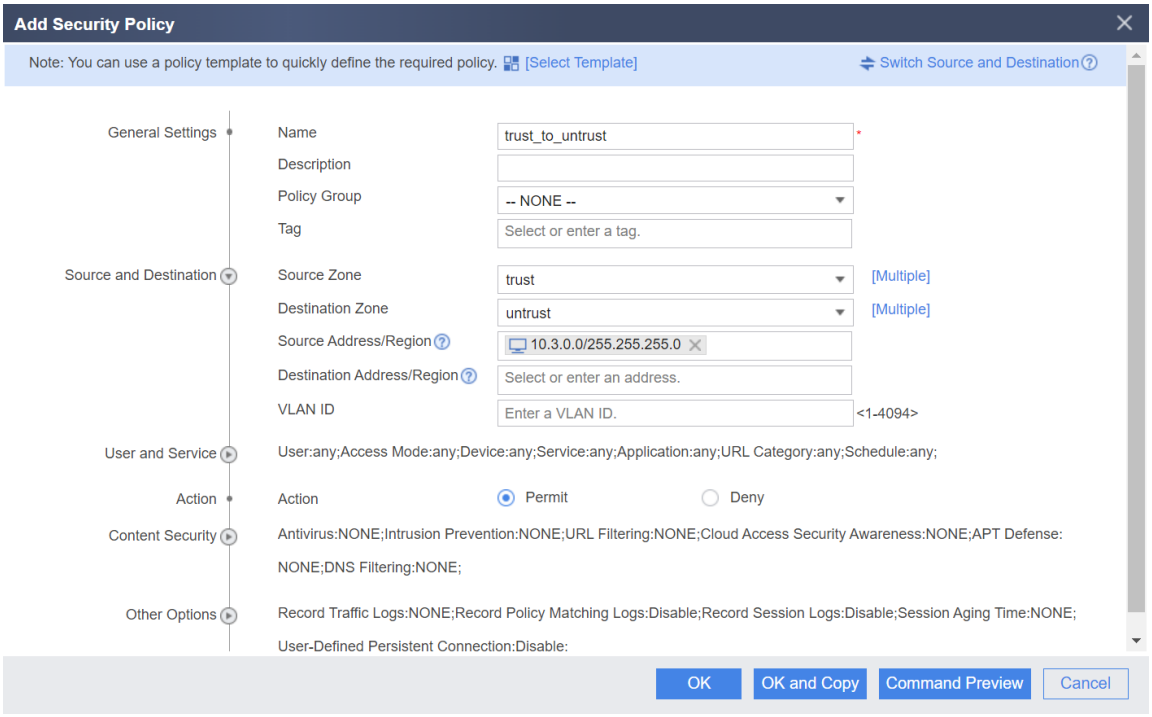
Hot standby status of FW2:



Step 5 Configure an interzone forwarding policy for FW1 and FW2.

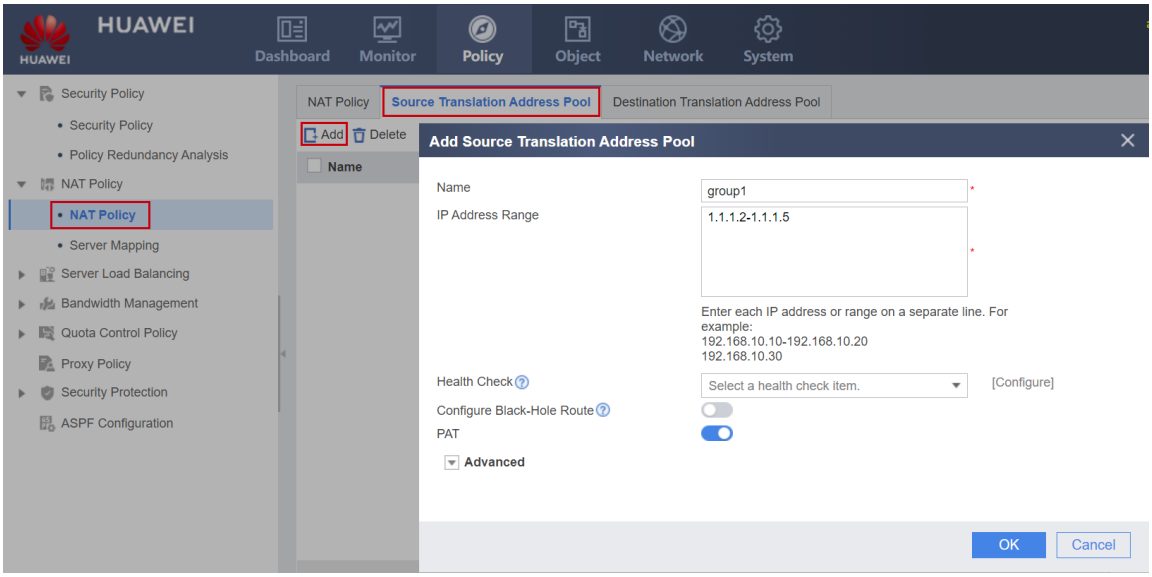
Configure a security policy on FW1 to allow service packets to pass through. After hot standby is enabled, the security policy configured on FW1 will be automatically synchronized to FW2.

Choose **Policy** > **Security Policy** > **Security Policy**. Click **Add** in **Security Policy List**, set or select parameters, and click **OK**. Configure a forwarding policy between the Trust and Untrust zones, as shown in the following figure.

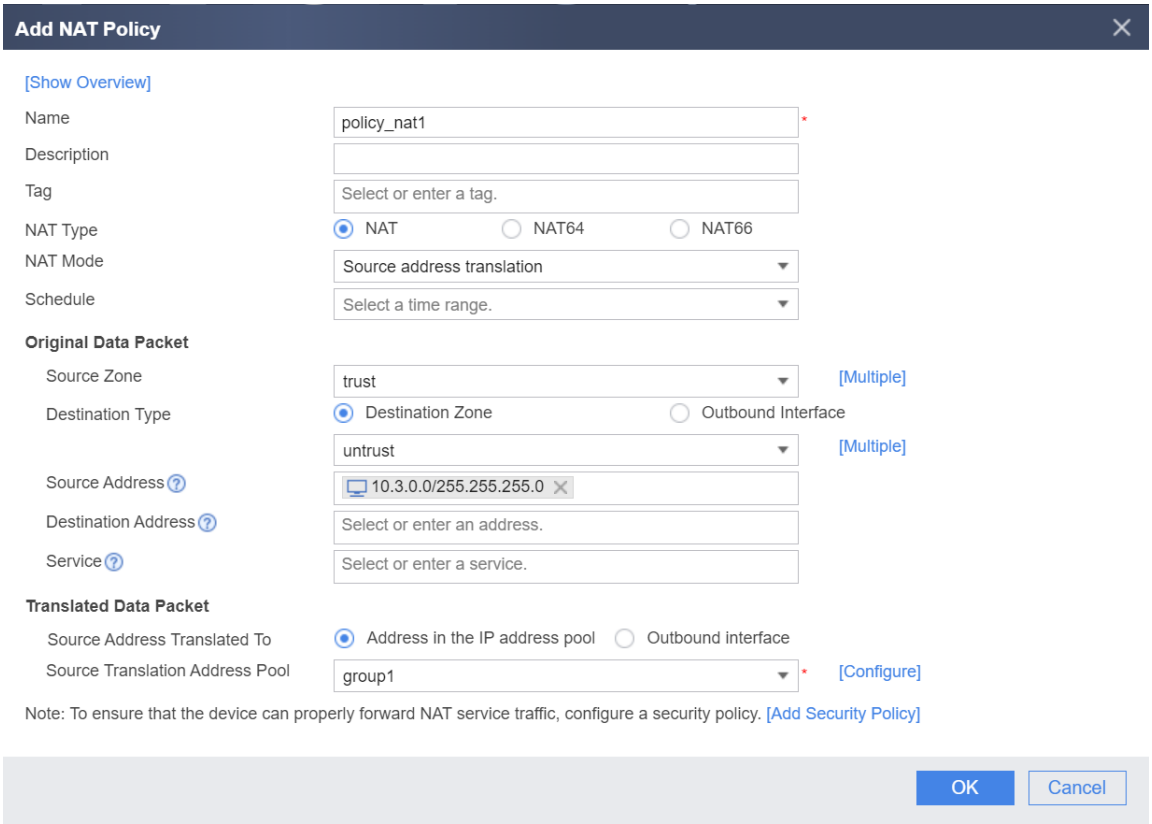


Step 6 Configure a NAT policy on FW1. After hot standby is enabled, the NAT policy configured on FW1 will be automatically synchronized to FW2.

Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool** and click **Add** to configure a NAT address pool.



Choose **Policy** > **NAT Policy** > **NAT Policy** and click **Add** to configure a NAT policy. When intranet users access the Internet, the source IP addresses on 10.3.0.0/24 will be translated into addresses in the address pool (1.1.1.2 to 1.1.1.5).



Step 7 Configure the switches.

Add the three interfaces of SW1 and SW2 to VLAN 10. For details, see the related switch document.

4.3 Verification

Run the **display vrrp** command on FW1 to check the status of interfaces in the VRRP group.

```
HRP_M<FW1> display vrrp
    GigabitEthernet0/0/1 | Virtual Router 1
      State : Master
      Virtual IP : 10.3.0.3
      Master IP : 10.3.0.1
      PriorityRun : 120
      PriorityConfig : 100
      MasterPriority : 120
      Preempt : YES     Delay Time : 0 s
      TimerRun : 60 s
      TimerConfig : 60 s
      Auth type : NONE
      Virtual MAC : 0000-5e00-0101
      Check TTL : YES
      Config type : vgmp-vrrp
      Backup-forward : disabled

    GigabitEthernet0/0/2 | Virtual Router 2
      State : Master
      Virtual IP : 1.1.1.1
      Master IP : 10.2.0.1
      PriorityRun : 120
      PriorityConfig : 100
      MasterPriority : 120
      Preempt : YES     Delay Time : 0 s
      TimerRun : 60 s
      TimerConfig : 60 s
      Auth type : NONE
      Virtual MAC : 0000-5e00-0102
      Check TTL : YES
      Config type : vgmp-vrrp
      Backup-forward : disabled
```

Run the **display vrrp** command on FW2 to check the status of interfaces in the VRRP group.

```
HRP_S<FW2>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
      State : Backup
      Virtual IP : 10.3.0.3
      Master IP : 10.3.0.1
      PriorityRun : 120
      PriorityConfig : 100
      MasterPriority : 120
      Preempt : YES     Delay Time : 0 s
      TimerRun : 60 s
      TimerConfig : 60 s
      Auth type : NONE
```

```
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : vgmp-vrrp
    Backup-forward : disabled

  GigabitEthernet0/0/2 | Virtual Router 2
    State : Backup
    Virtual IP : 1.1.1.1
    Master IP : 0.0.0.0
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 0
    Preempt : YES     Delay Time : 0 s
    TimerRun : 60 s
    TimerConfig : 60 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0102
    Check TTL : YES
    Config type : vgmp-vrrp
    Backup-forward : disabled
```

Run the **display hrp state verbose** command on FW1 to check the current status of the VGMP group.

```
HRP_M< FW1>display hrp state verbose
 Role: active, peer: standby
 Running priority: 45000, peer: 45000
 Backup channel usage: 0.00%
 Stable time: 0 days, 0 hours, 46 minutes
 Last state change information: 17:18:08 HRP core state changed, old_state = abnormal(active),
new_state = normal, local_priority = 45000, peer_priority = 45000.

 Configuration:
 hello interval:                 1000ms
 preempt:                          60s
 mirror configuration:           off
 mirror session:                 off
 track trunk member:               on
 auto-sync configuration:        on
 auto-sync connection-status: on
 adjust ospf-cost:               on
 adjust ospfv3-cost:             on
 adjust bgp-cost:                on
 nat resource:                   off

 Detail information:
             GigabitEthernet0/0/1 vrrp vrid 1: active
             GigabitEthernet0/0/2 vrrp vrid 2: active
                                        ospf-cost: +0
                                      ospfv3-cost: +0
                                        bgp-cost: +0
```

Run the **display hrp state verbose** command on FW2 to check the current status of the VGMP group.

```
HRP_S<FW2>display hrp state verbose
  Role: standby, peer: active
  Running priority: 45000, peer: 45000
  Backup channel usage: 0.00%
  Stable time: 0 days, 0 hours, 41 minutes
  Last state change information: 17:18:08 HRP core state changed, old_state = abnormal(standby),
new_state = normal, local_priority = 45000, peer_priority = 45000.

  Configuration:
  hello interval:                 1000ms
  preempt:                           60s
  mirror configuration:           off
  mirror session:                 off
  track trunk member:               on
  auto-sync configuration:        on
  auto-sync connection-status: on
  adjust ospf-cost:               on
  adjust ospfv3-cost:             on
  adjust bgp-cost:                on
  nat resource:                   off

  Detail information:
              GigabitEthernet0/0/1 vrrp vrid 1: standby
              GigabitEthernet0/0/2 vrrp vrid 2: standby
                                          ospf-cost: +65500
                                        ospfv3-cost: +65500
                                          bgp-cost: +100
```

Ping PC2 in the Untrust zone from PC1 in the Trust zone. Run the **display firewall session table** command on FW1 and FW2 to check sessions.

```
HRP_M<FW1> display firewall session table
  Current Total Sessions : 1
    icmp    VPN: public --> public    10.3.0.10:53419[1.1.1.4:2049] --> 1.1.1.10:2048
```

```
HRP_S<FW2> display firewall session table
  Current Total Sessions : 1
    icmp    VPN: public --> public    10.3.0.10:53419[1.1.1.4:2049] --> 1.1.1.10:2048
```

4.4 Configuration Reference

4.4.1 Configuration of FW1

```
#
sysname FW1
#
 hrp enable
 hrp interface GigabitEthernet0/0/3 remote 10.10.0.2
 hrp authentication-key Admin@123
```

```
#
 interface GigabitEthernet0/0/1
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 active
#
interface GigabitEthernet0/0/2
 ip address 10.2.0.1 255.255.255.0
 vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 active
#
interface GigabitEthernet0/0/3
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/2
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet0/0/3
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action source-nat address-group group1
#
```

4.4.2 Configuration of FW2

```
#
sysname FW2
#
 hrp enable
 hrp interface GigabitEthernet0/0/3 remote 10.10.0.1
 hrp authentication-key Admin@123
#
 interface GigabitEthernet0/0/1
```

```
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 standby
#
interface GigabitEthernet0/0/2
 ip address 10.2.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 standby
#
interface GigabitEthernet0/0/3
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/2
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet0/0/3
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action source-nat address-group group1
#
```

4.5 Quiz

Are HRP packets exchanged between the heartbeat interfaces controlled by security policies?

Reference Answer:

Whether HRP packets exchanged between heartbeat interfaces are controlled by security policies depends on the device model and version. In this lab environment, the HRP packets exchanged between heartbeat interfaces are not controlled by security policies.

In other versions, whether HRP packets are controlled by security policies depends on the configuration of the **firewall packet-filter basic-protocol enable** command. By default, the **firewall packet-filter basic-protocol enable** command is configured. That is, HRP packets are controlled by a security policy. In this case, you need to configure a security policy between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass through.

5 User Management

5.1 Introduction

5.1.1 About This Lab

A firewall functions as the egress of an enterprise, and the enterprise wants to authenticate internal users. Internal users need to be authenticated before they can access the Internet. No authentication is required for visitors.

In this lab, security devices are deployed at the network egress to implement local authentication or authentication exemption for users who attempt to access the Internet.

5.1.2 Objectives

- Understand the basic principles of user management.
- Master the method of configuring authentication exemption for users.
- Master the method of configuring password-based authentication for users.

5.1.3 Networking Topology

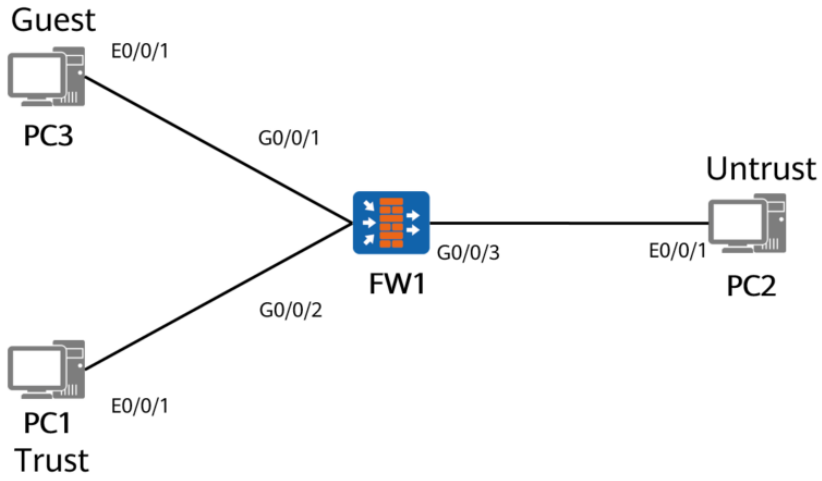


Figure 5-1 Networking topology for configuring user management

5.1.4 Lab Planning

FW1 is deployed at the gateway. PC3 and PC1 are used to simulate an authentication-free user and password-based authentication user, respectively, and access the Internet server (PC2).

Table 5-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW1	GigabitEthernet0/0/1	10.1.1.1/24	Guest
	GigabitEthernet0/0/2	10.1.2.1/24	trust
	GigabitEthernet0/0/3	40.1.1.1/24	untrust
PC1	Eth0/0/1	10.1.2.10/24	trust
PC2	Eth0/0/1	40.1.1.10/24	untrust
PC3	Eth0/0/1	10.1.1.10/24	Guest

5.2 Lab Configuration

5.2.1 Configuration Roadmap

1. Configure basic IP addresses and security zones.
2. Create a user group and formulate related user policies.

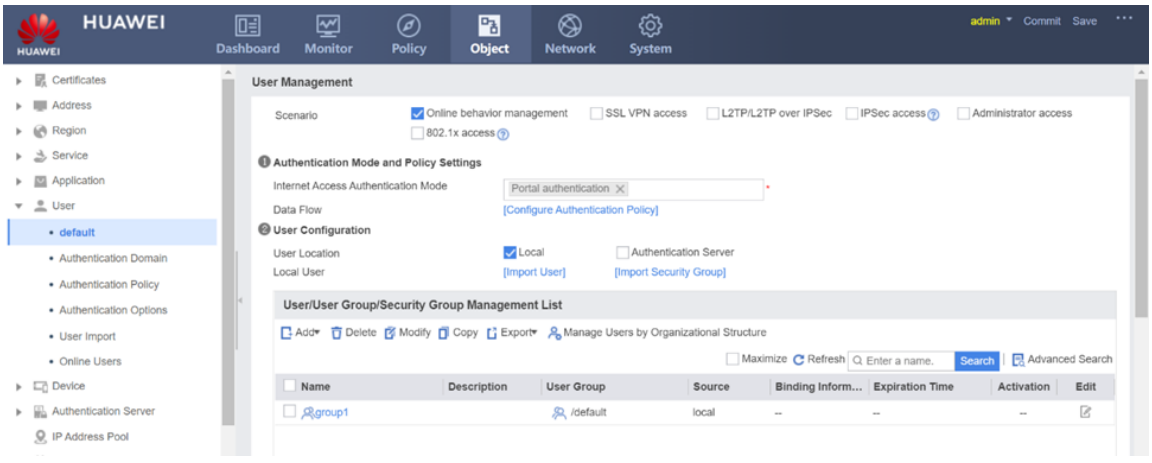
5.2.2 Configuration Procedure on the Web UI

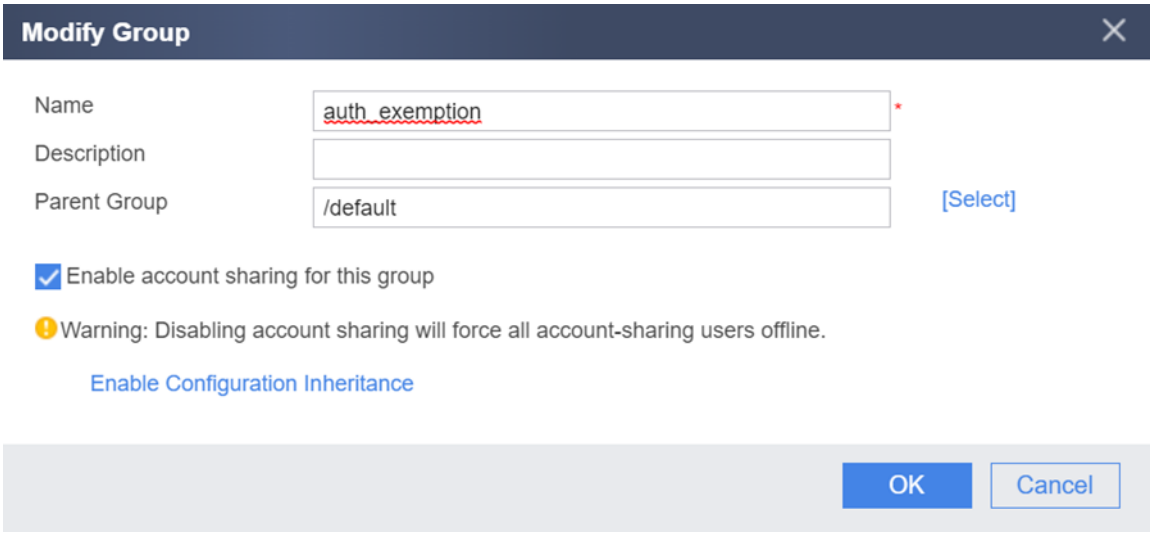
Step 1 Configure basic parameters for the interfaces of FW1 and add the interfaces to the related security zones.

Add G0/0/1 to the Guest zone. (The Guest zone is a new security zone whose security level is 40.) Add G0/0/2 to the Trust zone and G0/0/3 to the Untrust zone. Details are not provided.

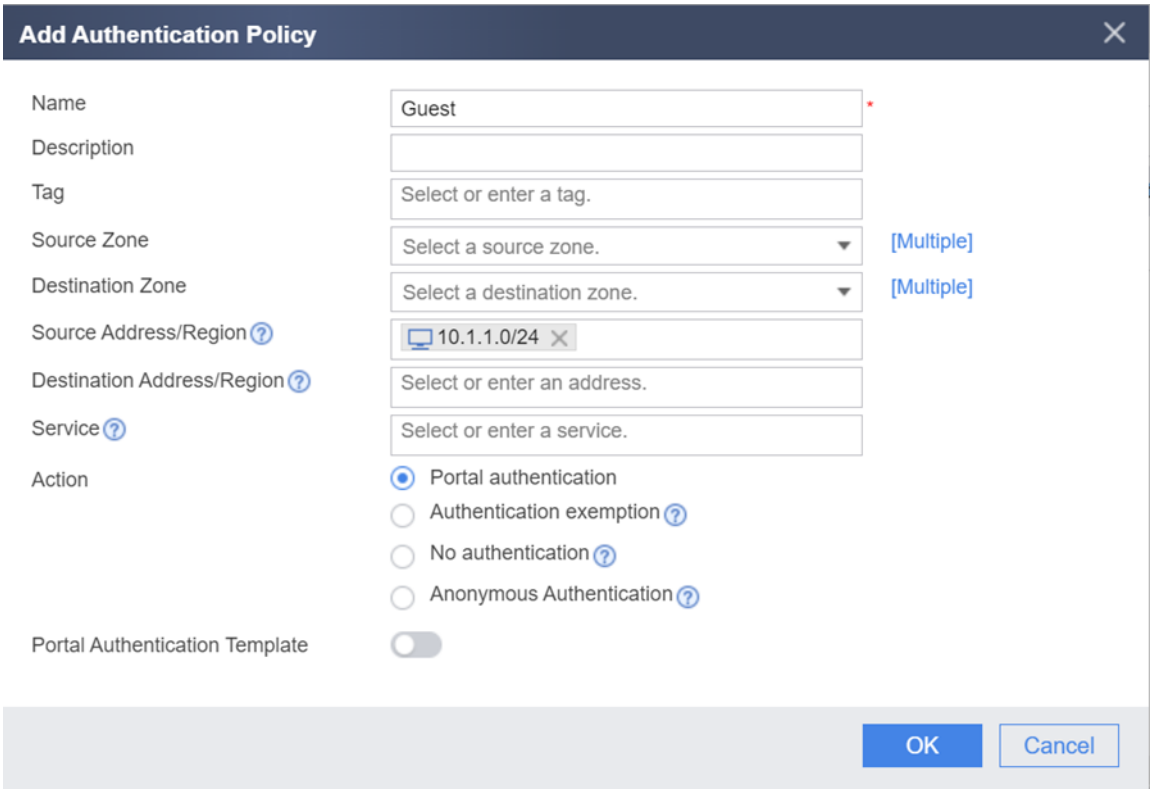
Step 2 Create an authentication–free user group.

Choose **Object** > **User** > **default**. In the **User/User Group/Security Group Management List** area, click **Add** and add a user group named **auth_exemption**.



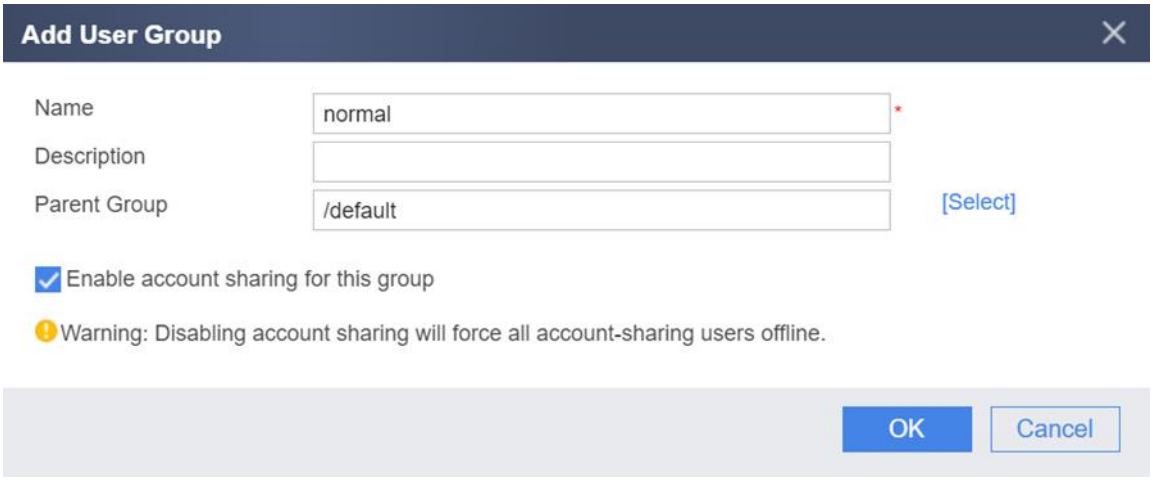


Step 3 Choose **Object** > **User** > **Authentication Policy**, click **Add**, and create a user authentication policy named **Guest** for network segment **10.1.1.0/24**.

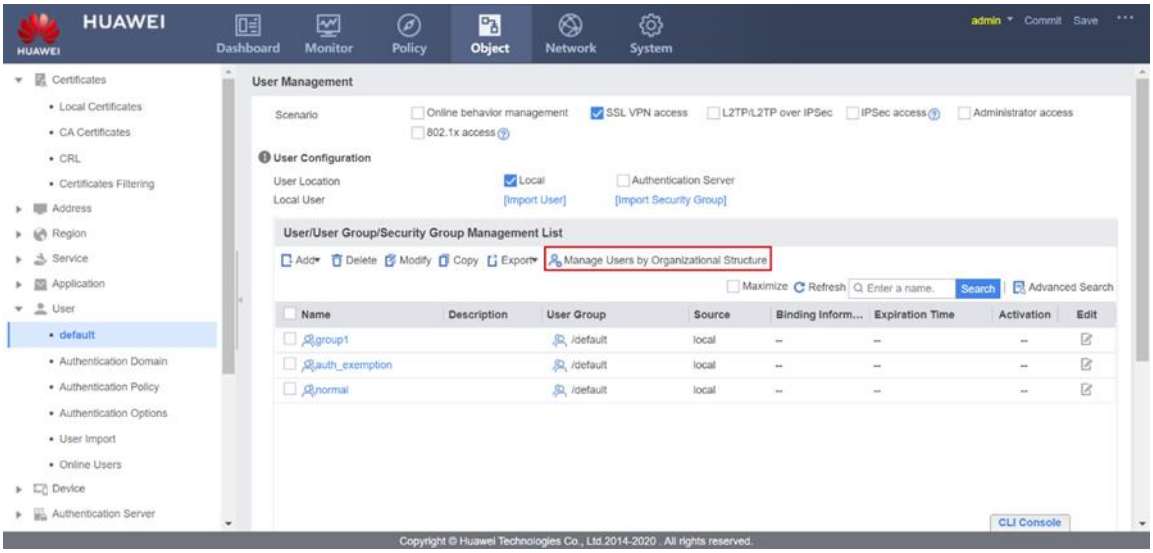


Step 4 Create a password-based authentication user group and user.

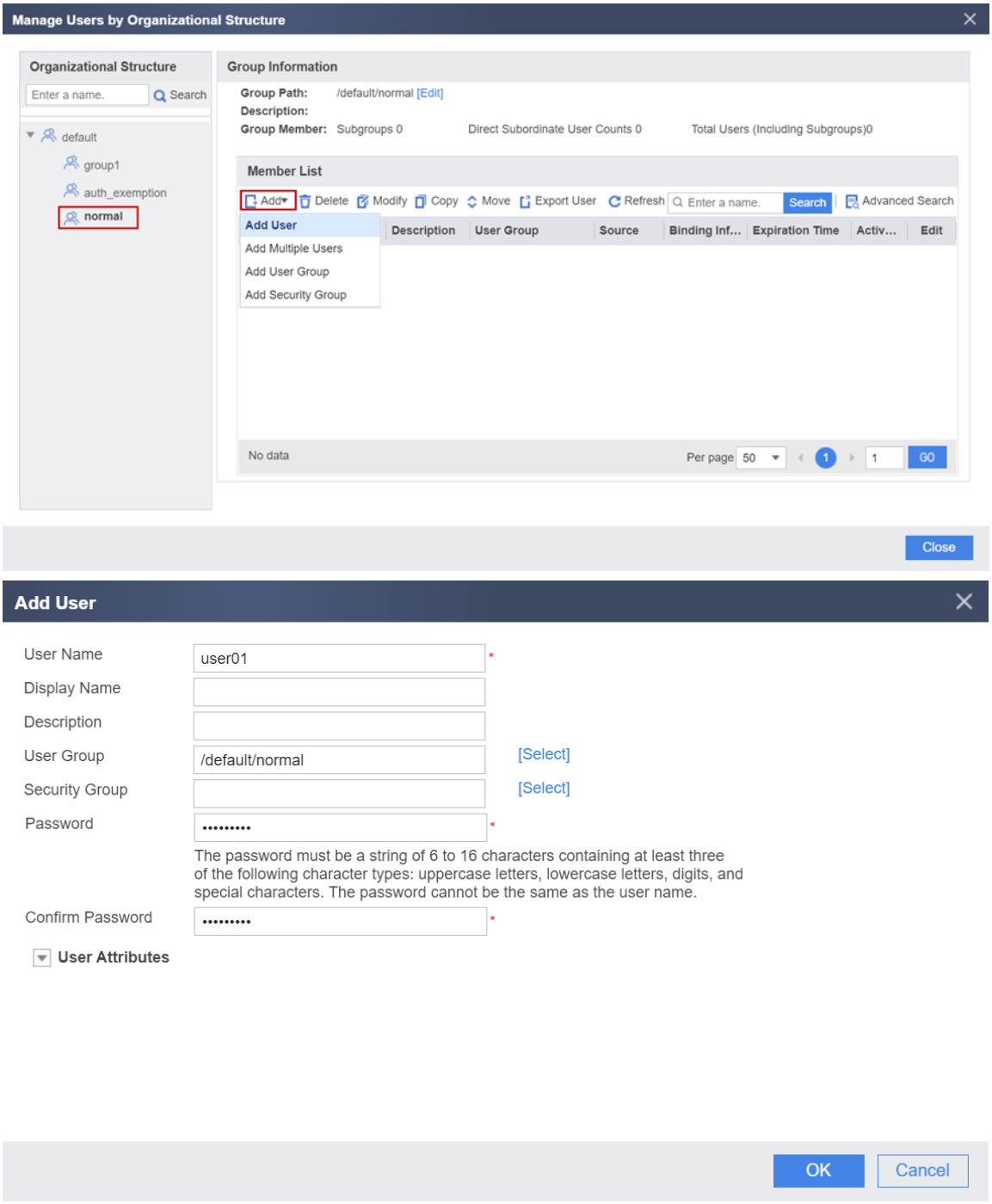
Choose **Object** > **User** > **default**. In the **User/User Group/Security Group Management List** area, click **Add** and add a user group named **normal**.



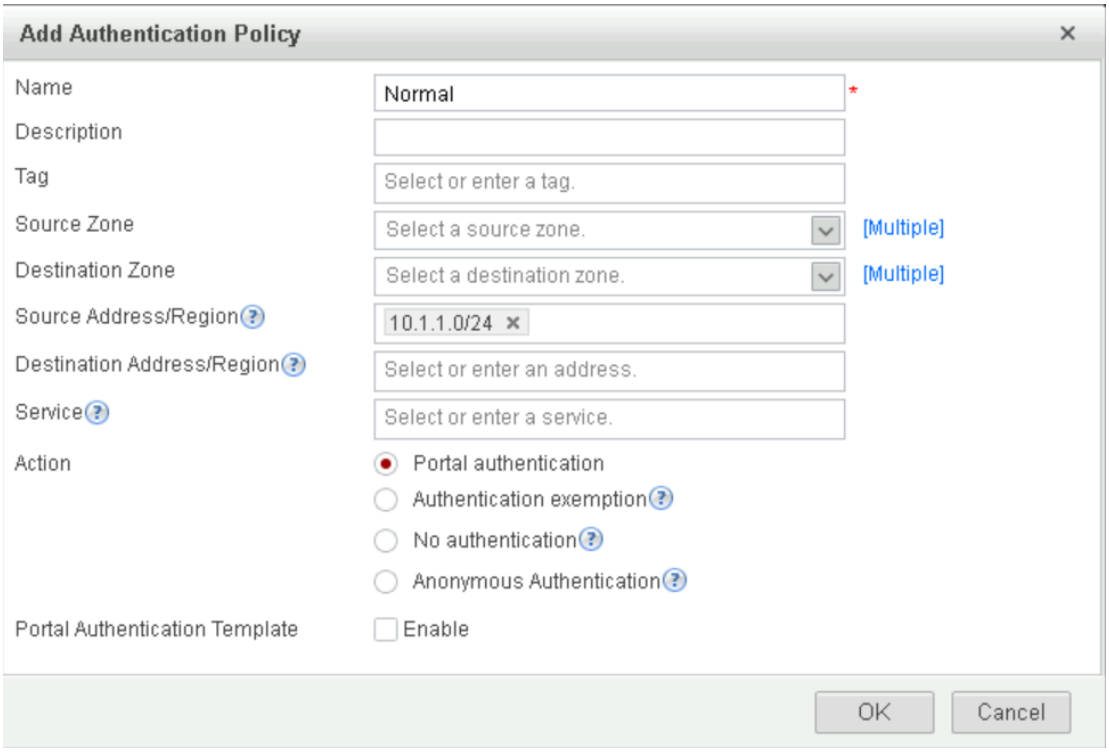
Choose **Object** > **User** > **default**. In the **User/User Group/Security Group Management List** area, click **Manage Users Based by Organizational Structure**.



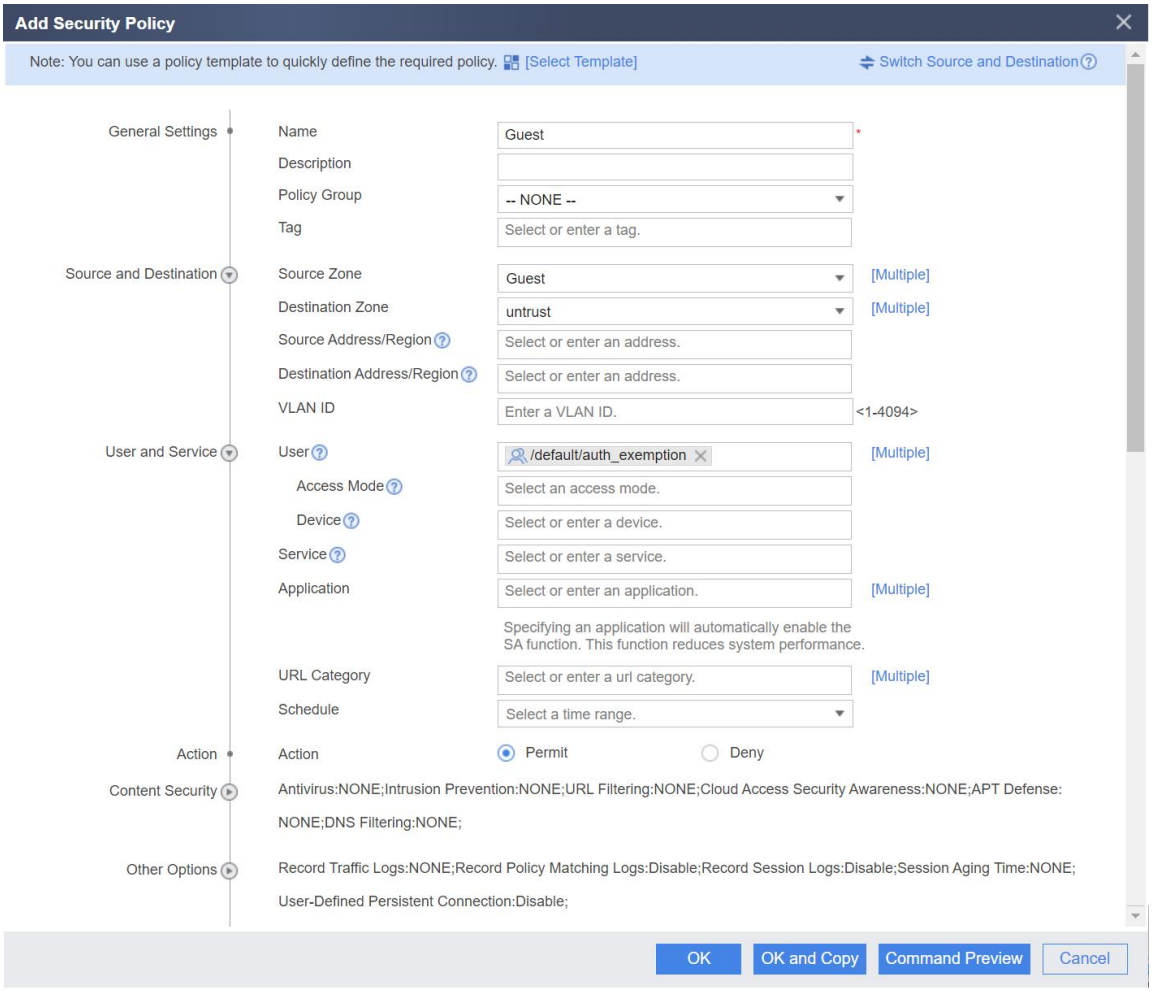
In the **Organizational Structure** area, click **normal**. In the **Member List** area, click **Add** and add the user whose user name is **user01** and password is **Admin@123**.



Step 5 Choose **Object > User > Authentication Policy**, click **Add**, and create a user authentication policy named **Normal** for network segment **10.1.2.0/24**.

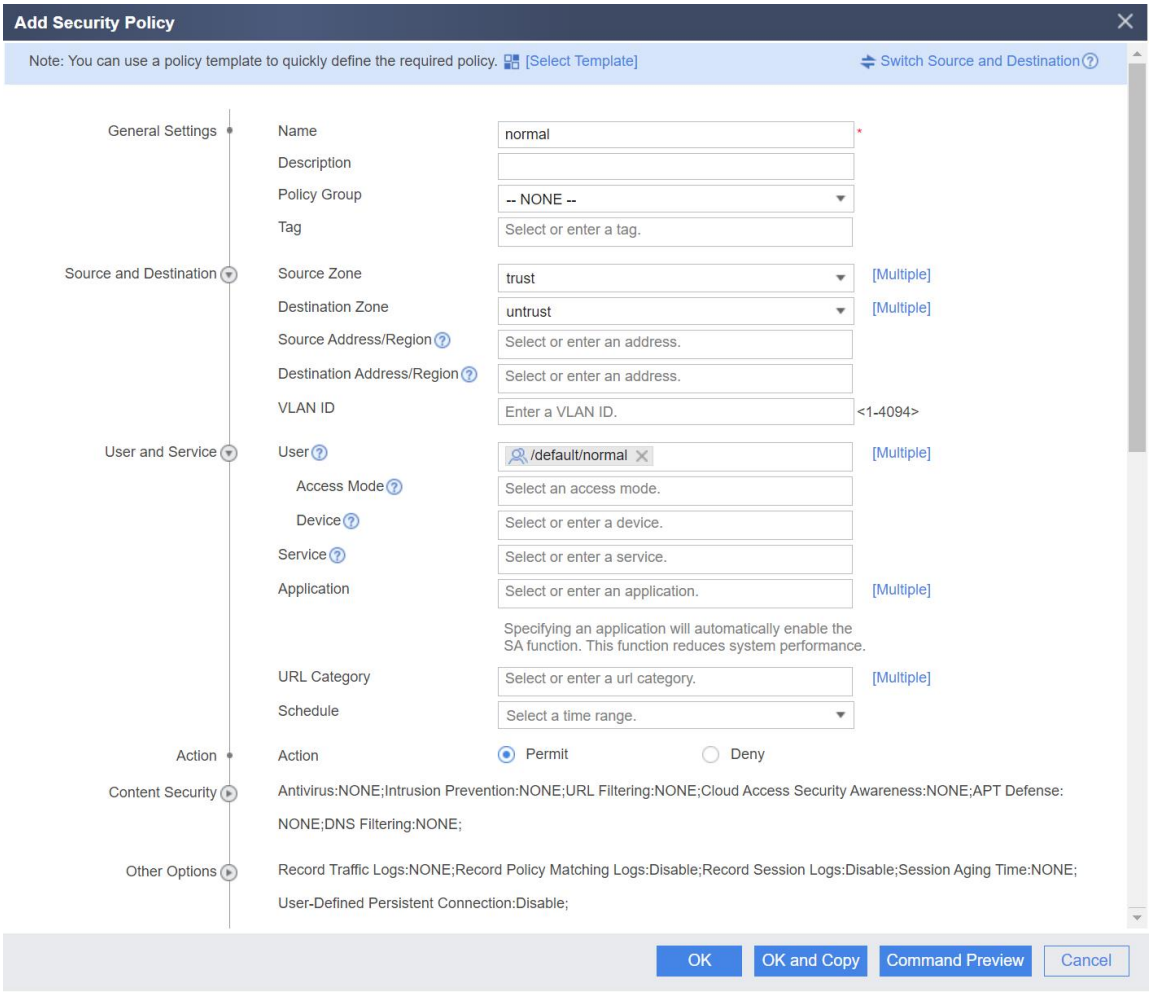


Step 6 Choose **Policy** > **Security Policy**, click **Add**, and create a forwarding policy for authentication-free users. Set the source security zone to Guest and destination security zone to Untrust, select the authentication-free user group **auth_exemption**, and set the action to Permit.

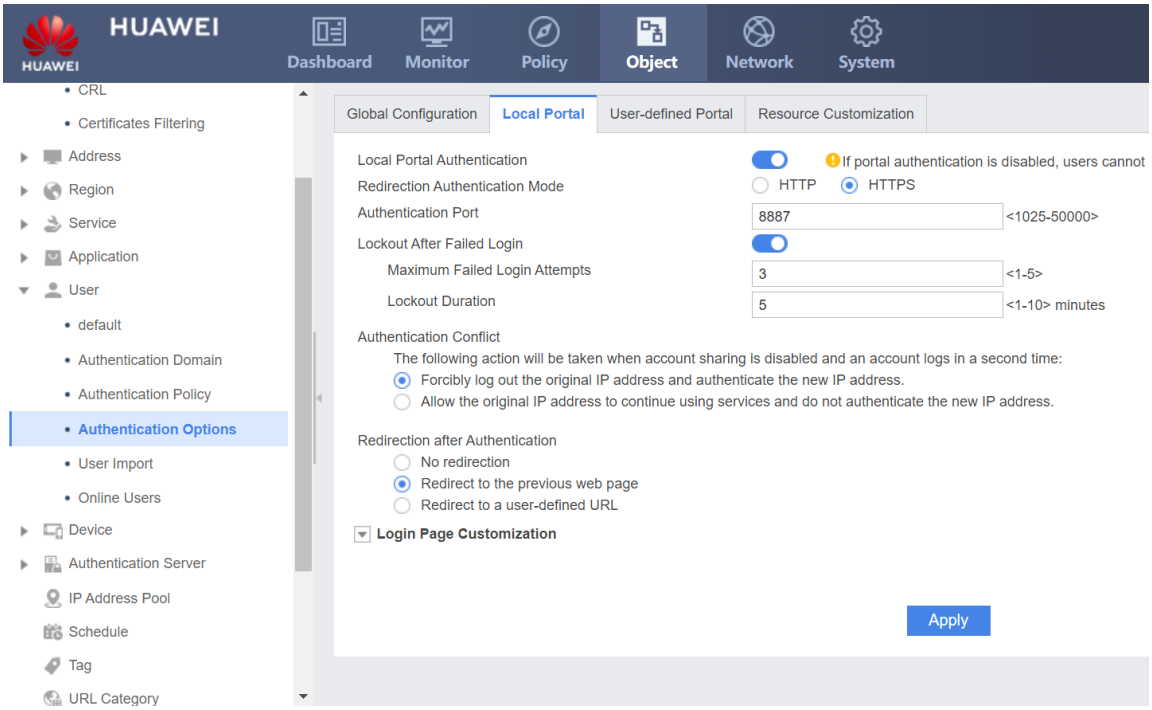


Step 7 Choose **Policy > Security Policy**, click **Add**, and create a forwarding policy for password-based authentication users.

Set the source security zone to Trust and destination security zone to Untrust, and select the password-based authentication user group **normal**, and set the action to Permit.

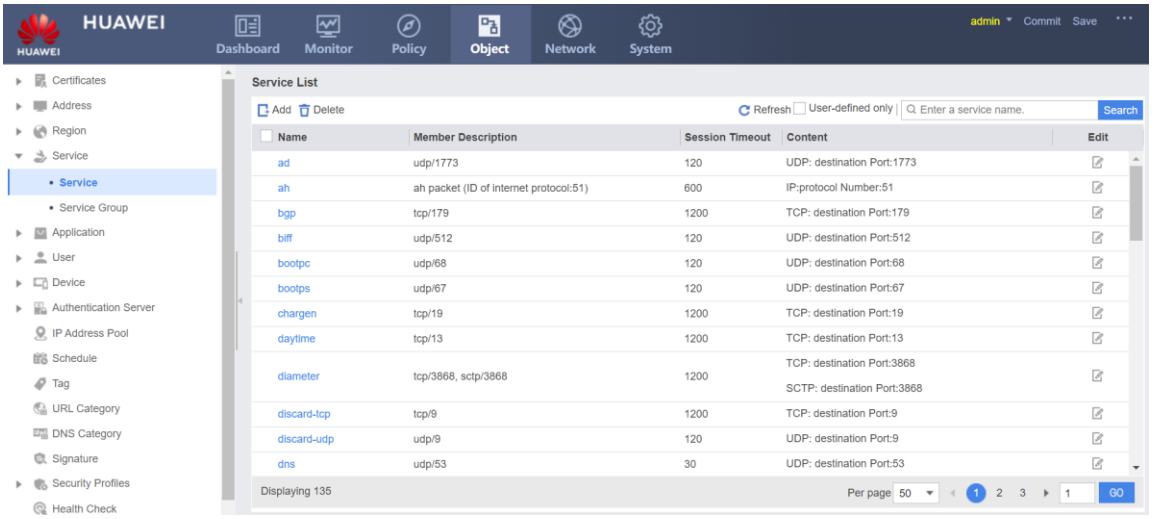


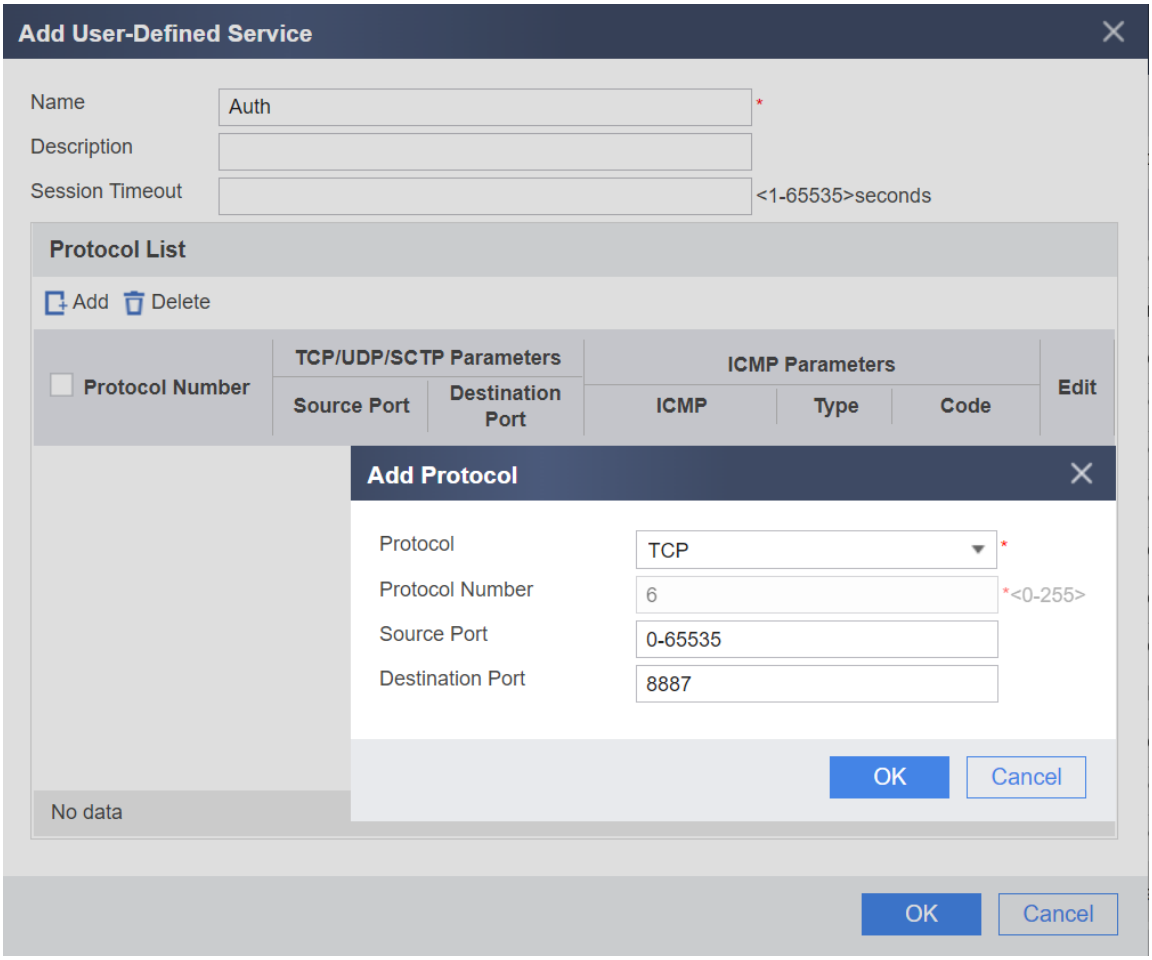
Step 8 Choose **Object** > **User** > **Authentication Options** > **Local Portal**, configure the page to be pushed upon Internet access authentication, and select **Redirect to the previous web page**.



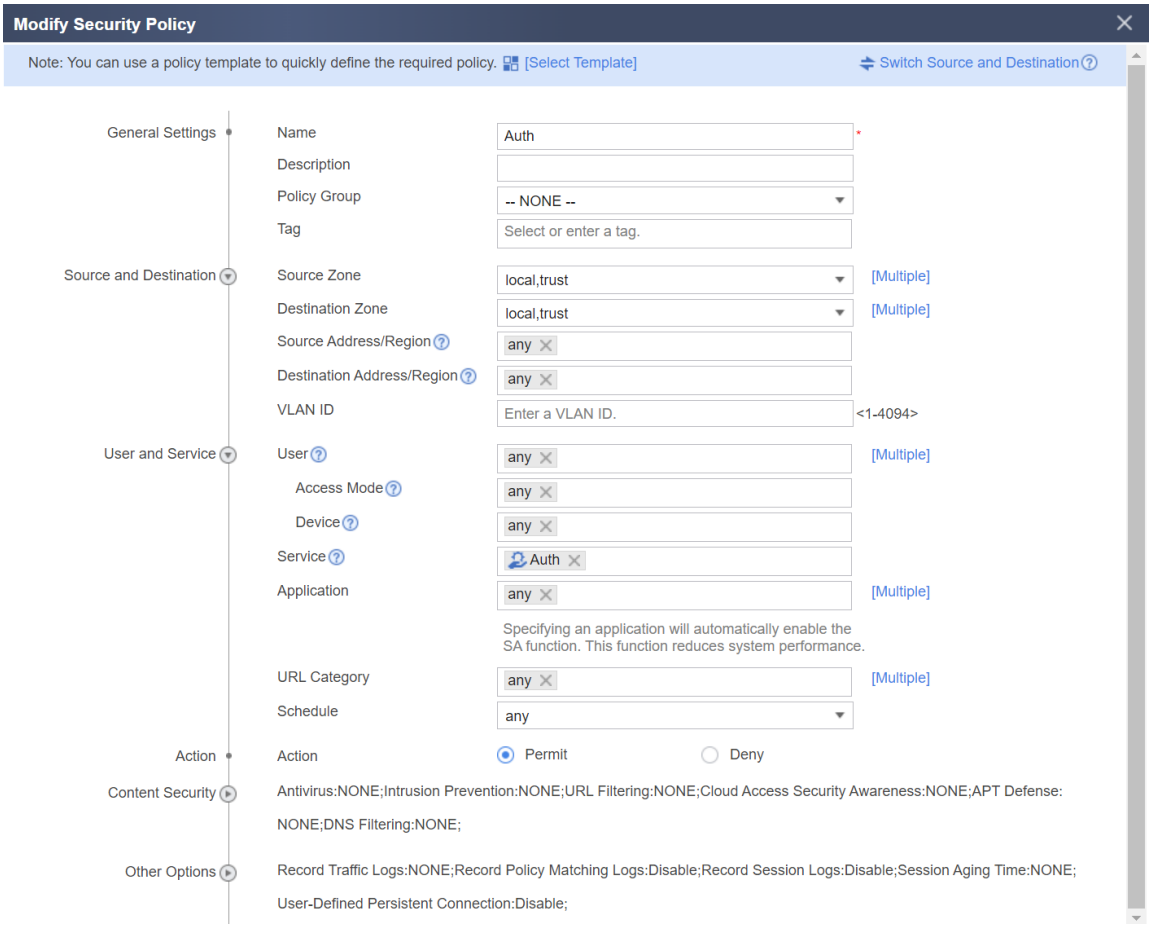
When a user accesses the Internet through HTTP, the user is redirected to the authentication page.

Step 9 Choose **Object > Service > Service** and click **Add** to create a customized service named **Auth**.

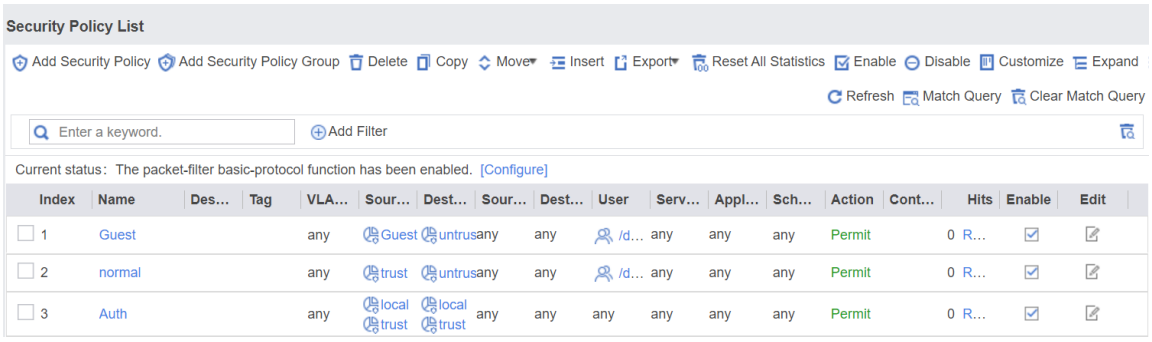




Step 10 Choose **Policy > Security Policy** and click **Add** to create a security policy that allows traffic from port 8887 in the Trust and Local zones to pass through the firewall. This ensures that the authentication page can be successfully pushed.



The following figure shows the configured security policies.



5.3 Verification

Temporary users can access the Internet without entering the user name and password.

When an employee accesses the Internet through HTTP, FW1 will push the user authentication page, and then prompt the user to enter the user name and password. The employee can access network resources only after entering the correct user name and password.

5.4 Quiz

What are the user categories?

Reference Answer:

Users are classified into administrators, Internet access users, and access users. Different authentication methods are used for different users to determine user identities and implement user management.

6 Site-to-Site IPSec VPN

6.1 Introduction

6.1.1 About This Lab

Enterprise A and enterprise B need to access services of each other over the Internet. The confidentiality of the enterprises' secrets needs to be guaranteed.

In this lab, network A and network B are used to simulate enterprise A and enterprise B. Network A and network B are connected to the Internet through FW1 and FW2, respectively. An IPSec tunnel in IKE mode is established between FW1 and FW2. Users on network A and network B can access each other through the IPSec tunnel. During the access, packets on the Internet are encrypted by the IPSec VPN to meet confidentiality requirements.

6.1.2 Objectives

- Understand the basic principles of IPSec VPN.
- Master the application scenario of the site-to-site IPSec VPN.

6.1.3 Networking Topology

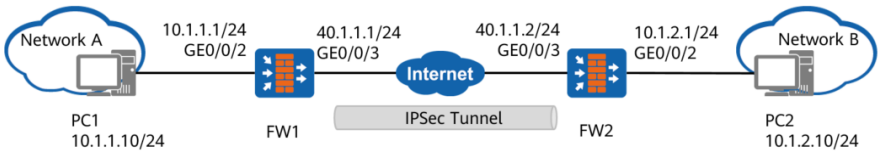


Figure 6-1 Networking topology for configuring site-to-site IPSec VPN

6.1.4 Lab Planning

Network A belongs to subnet **10.1.1.0/24**, PC1 is a host on network A, and FW1 is the gateway of network A.

Network B belongs to subnet **10.1.2.0/24**, PC2 is a host on network B, and FW2 is the gateway of network B.

FW1 and FW2 are connected to the Internet, have reachable routes to each other, and have established an IPSec tunnel between them.

Table 6-1 Port address and zone planning

Device	Interface	IP Address	Security Zone

FW1	GigabitEthernet0/0/3	40.1.1.1/24	untrust
	GigabitEthernet0/0/2	10.1.1.1/24	trust
FW2	GigabitEthernet0/0/3	40.1.1.2/24	untrust
	GigabitEthernet0/0/2	10.1.2.1/24	trust
PC1	Eth0/0/1	10.1.1.10/24	trust
PC2	Eth0/0/1	10.1.2.10/24	trust

6.2 Lab Configuration

6.2.1 Configuration Roadmap

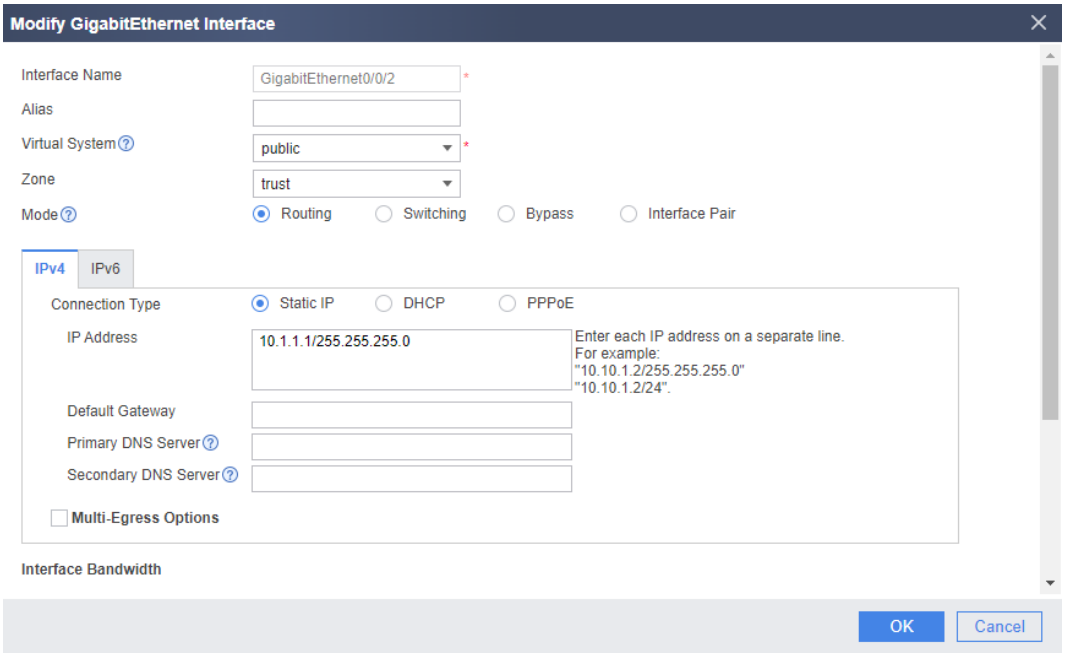
1. Configure IP addresses for interfaces.
2. Configure an interzone security policy.
3. Configure an IPsec/IKE proposal.
4. Configure and apply an IPSec policy.

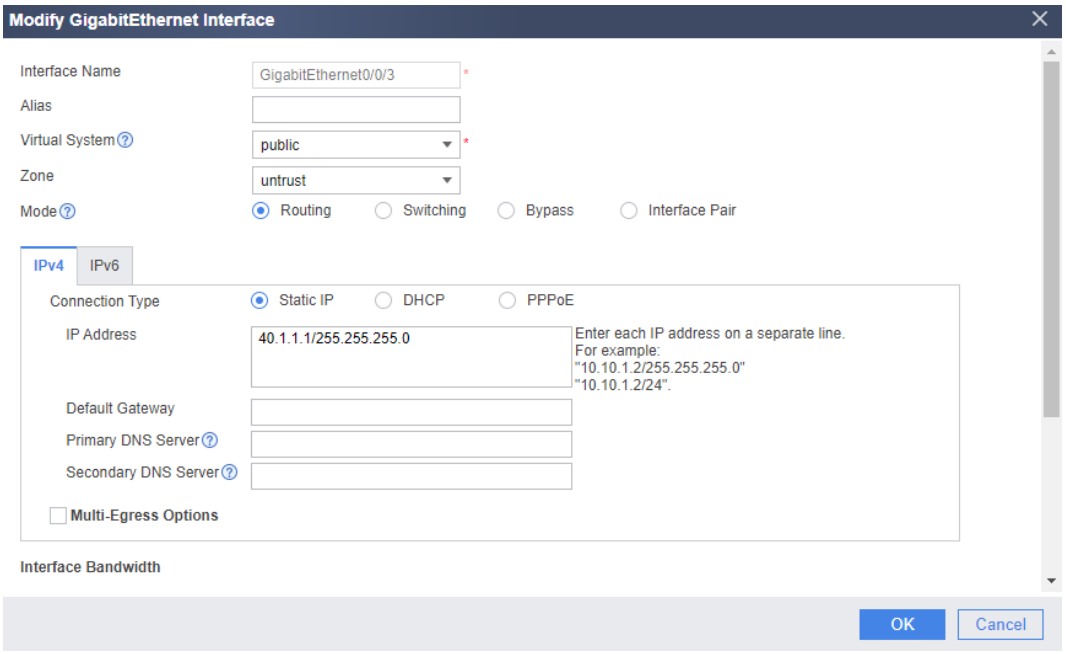
6.2.2 Configuration Procedure on the Web UI

Step 1 Configure IP addresses for interfaces.

Configure IP addresses for interfaces on the firewalls, and add the interfaces to security zones. FW1 is used as an example. The configuration of FW2 is similar to that of FW1.

On FW1, choose **Network** > **Interface**, click  next to GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3, and set the parameters.

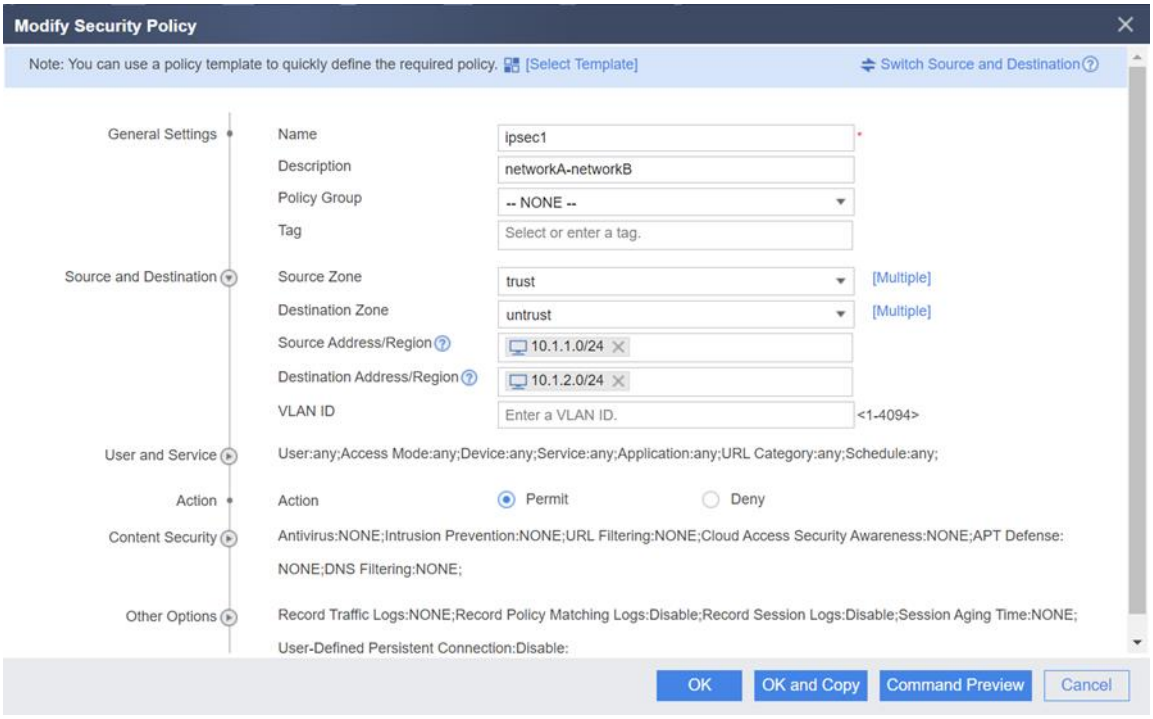


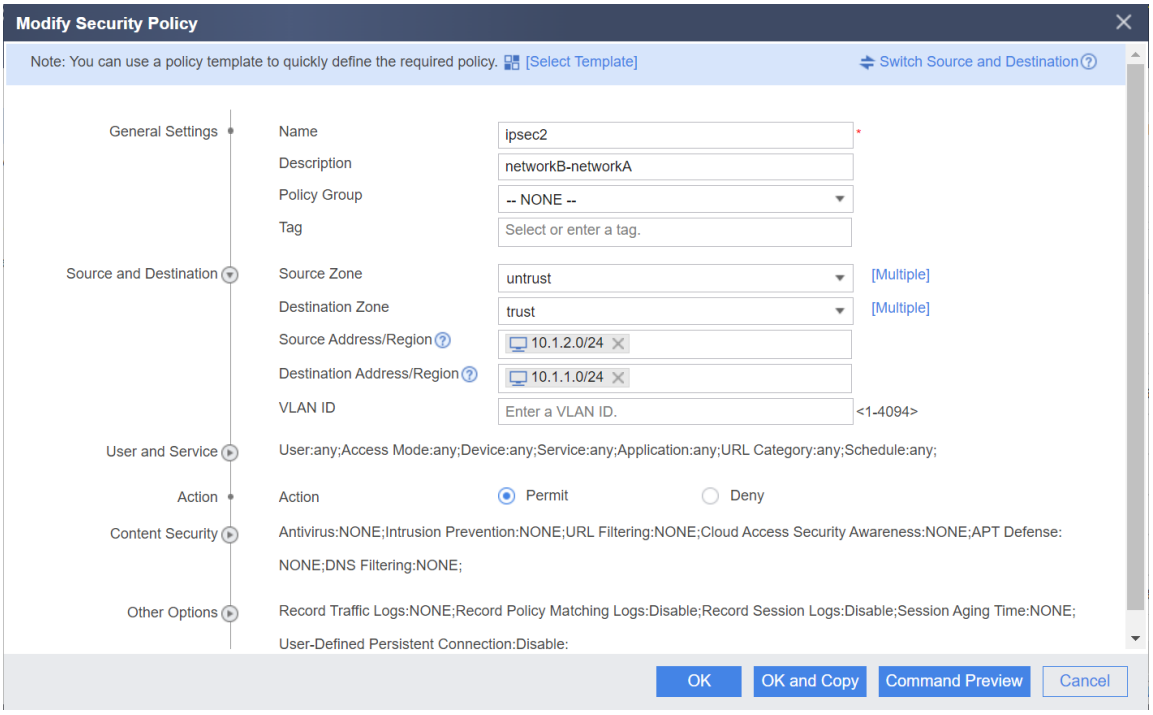


Step 2 Configure security policies on FW1 and FW2.

Configure security policies **ipsec1** and **ipsec2** on the firewall to allow networks A and B to access each other. The configuration of FW1 is used as an example. The configuration of FW2 is similar to that of FW1.

On FW1, choose **Policy > Security Policy > Security Policy**, and click **Add** to add a security policy that allows traffic between network segments 10.1.1.0/24 and 10.1.2.0/24.

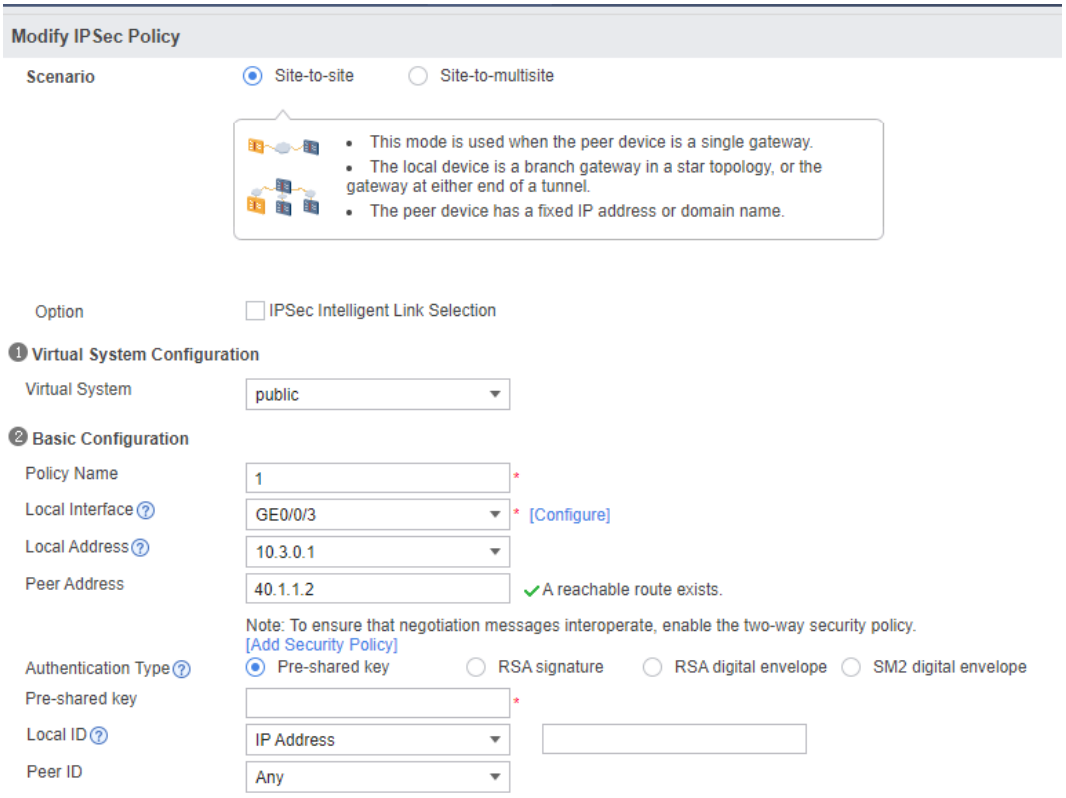




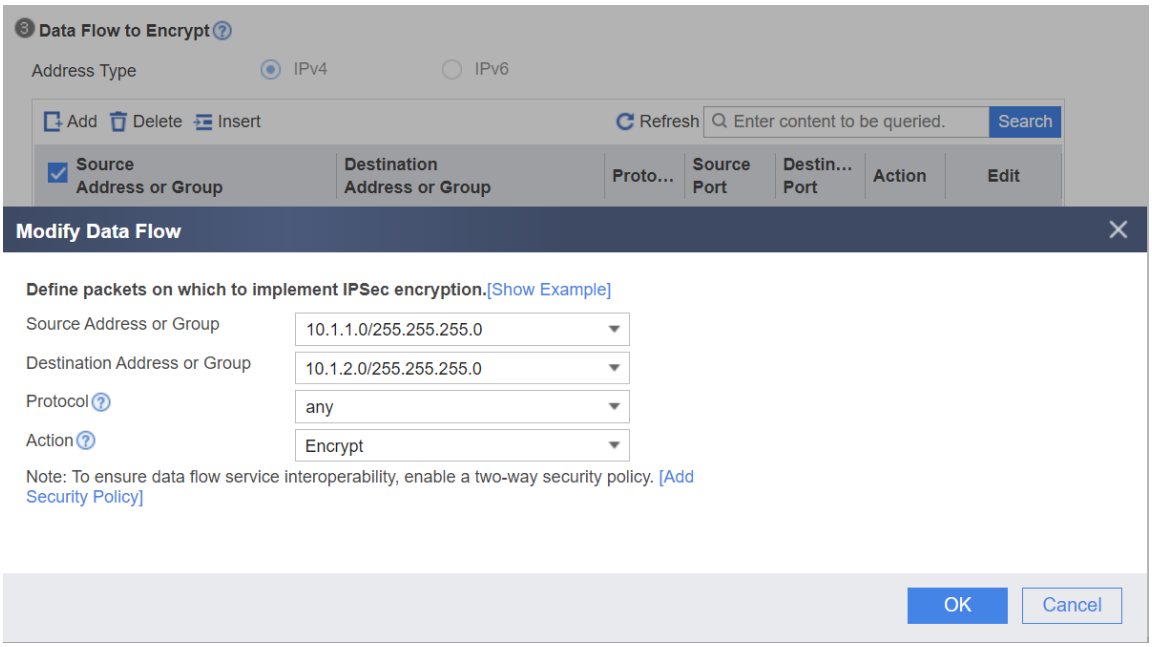
Step 3 Configure an IPSec policy.

On FW1, choose **Network** > **IPSec** > **IPSec**, click **Add**, and set **Scenario** to **Site-to-site**.

In the **Basic Configuration** area, set IPSec parameters, including the pre-shared key **Test!123** and the local and peer IP addresses.

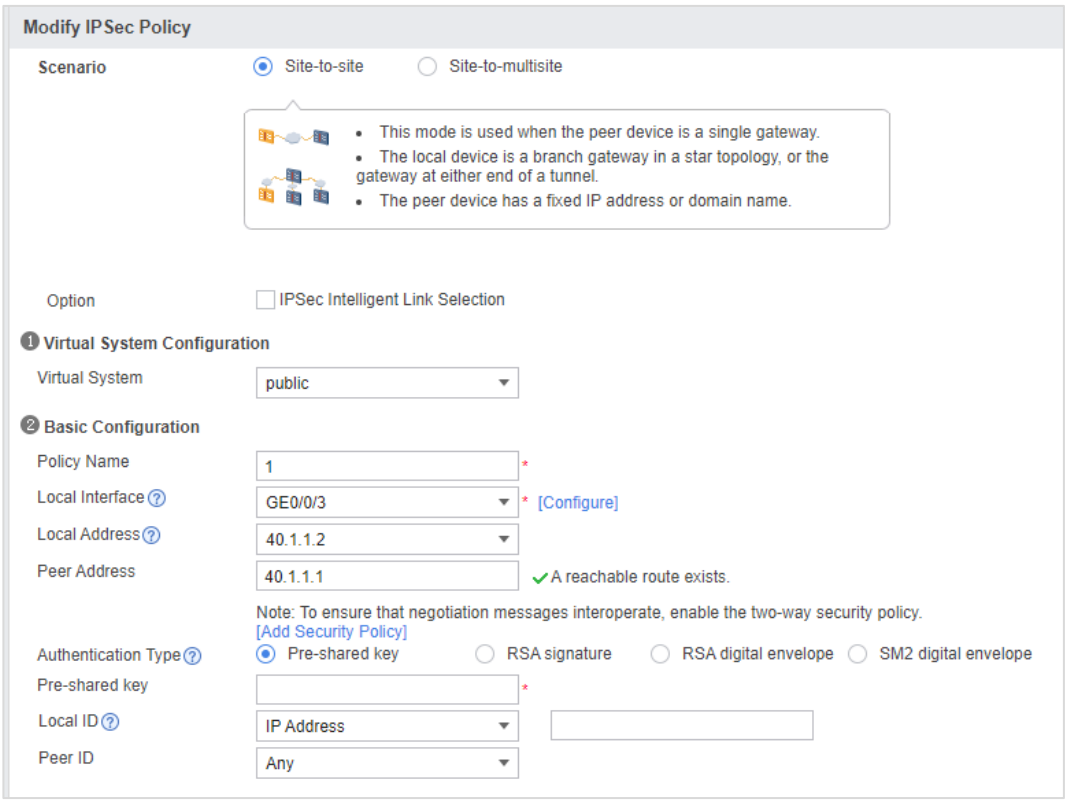


On FW1, click **Add** in **Data Flow to Encrypt** to encrypt the interested traffic.

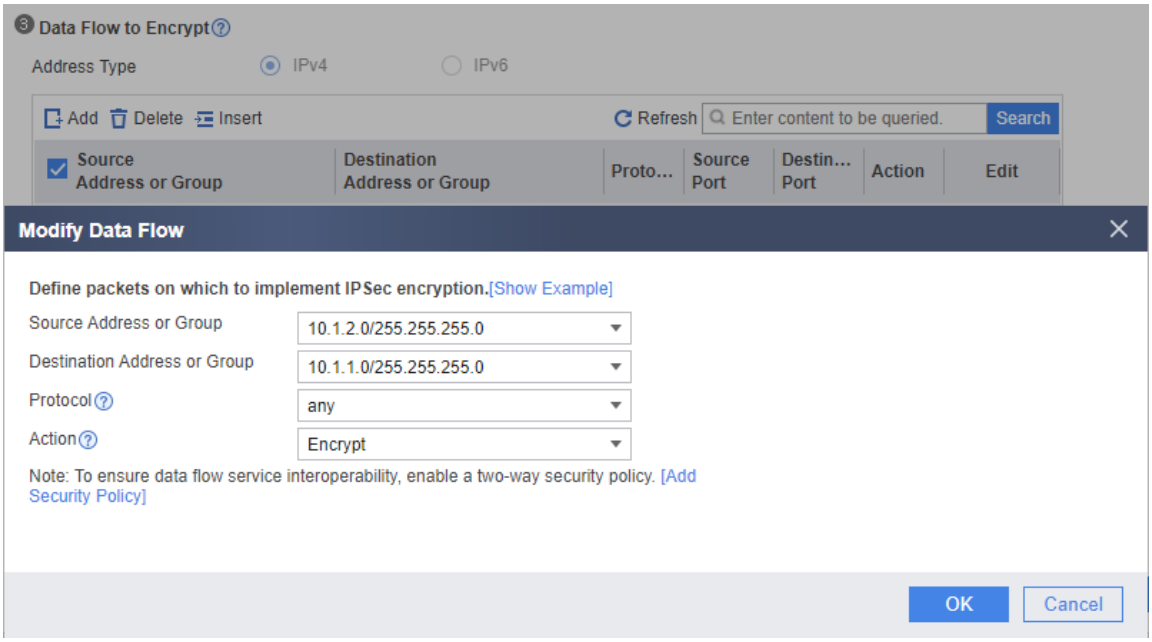


On FW2, choose **Network** > **IPSec** > **IPSec**, click **Add**, and set **Scenario** to **Site-to-site**.

In the **Basic Configuration** area, set IPSec parameters, including the pre-shared key **Test!123** and the local and peer IP addresses.



On FW2, click **Add** in **Data Flow to Encrypt** to encrypt the interested traffic.



Step 4 Apply the IPSec policy.

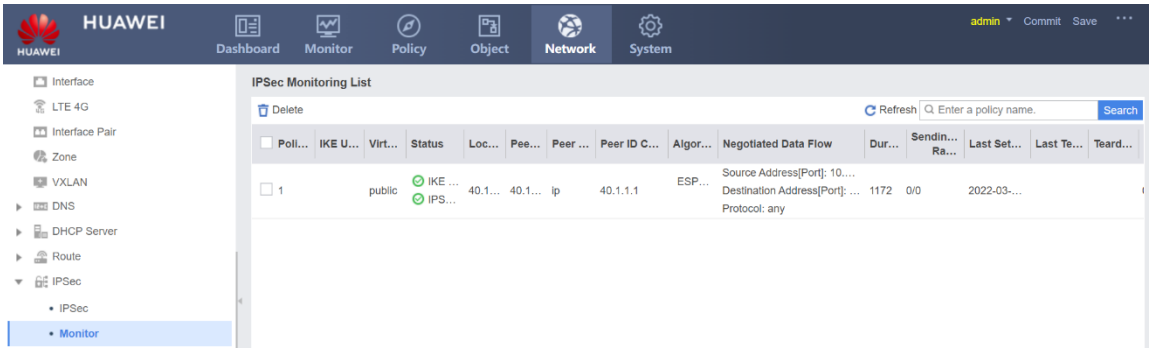
After the configuration is complete, click **Apply** to save and apply the IPSec policy.

6.3 Verification

Run the **ping** command on PC1 to test the connectivity of PC2.

```
C:\Users\admin>ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=2ms TTL=126
Reply from 10.1.1.10: bytes=32 time<1ms TTL=126
Reply from 10.1.1.10: bytes=32 time<1ms TTL=126
Reply from 10.1.1.10: bytes=32 time<1ms TTL=126
Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

On FW1 and FW2, choose **Network** > **IPSec** > **Monitor** and check the monitoring list. You can see the IPSec tunnel is established properly.



6.4 Configuration Reference

6.4.1 Configuration of FW1

```
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop16217151963
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike162171519631
```

```
 exchange-mode auto
 pre-shared-key %^%#Tw^J,\TJzTtF8tRRu6K#DD"zU-1`OI*(Em%lTb['%^%#
 ike-proposal 1
 remote-id-type none
 dpd type periodic
 remote-address 40.1.1.2
 rsa encryption-padding oaep
 rsa signature-padding pss
 local-id-preference certificate enable
 ikev2 authentication sign-hash sha2-256
#
ipsec policy ipsec1621715194 1 isakmp
 security acl 3000
 ike-peer ike162171519631
 proposal prop16217151963
 tunnel local applied-interface
 alias 1
 sa trigger-mode auto
 sa duration traffic-based 5242880
 sa duration time-based 3600
#
interface GigabitEthernet0/0/3
 undo shutdown
 ip address 40.1.1.1 255.255.255.0
 ipsec policy ipsec1621715194
#
interface GigabitEthernet0/0/2
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/2
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/3
#
ip route-static 0.0.0.0 0.0.0.0 40.1.1.2
#
ip address-set 10.1.1.0/24 type object
 description Address segment of network A
 address 0 10.1.1.0 mask 24
#
ip address-set 10.1.2.0/24 type object
 description Address segment of network B
 address 0 10.1.2.0 mask 24
#
security-policy
 rule name ipsec1
  description Network A-Network B
  source-zone trust
  destination-zone untrust
  source-address address-set 10.1.1.0/24
  destination-address address-set 10.1.2.0/24
```

```
  action permit
 rule name ipsec2
  description Network B-Network A
  source-zone untrust
  destination-zone trust
  source-address address-set 10.1.2.0/24
  destination-address address-set 10.1.1.0/24
  action permit
#
```

6.4.2 Configuration of FW2

```
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop16217202185
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike162172021857
 exchange-mode auto
 pre-shared-key %^%#-"i1,QFGvWsErbOB@ph98G-PW*QI_1W-{Z~58>0.%^%#
 ike-proposal 1
 remote-id-type none
 dpd type periodic
 remote-address 40.1.1.1
 rsa encryption-padding oaep
 rsa signature-padding pss
 local-id-preference certificate enable
 ikev2 authentication sign-hash sha2-256
#
ipsec policy ipsec1621720216 1 isakmp
 security acl 3000
 ike-peer ike162172021857
 proposal prop16217202185
 tunnel local applied-interface
 alias 1
 sa trigger-mode auto
 sa duration traffic-based 5242880
 sa duration time-based 3600
#
interface GigabitEthernet0/0/3
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
```

```
 ipsec policy ipsec1621720216
#
interface GigabitEthernet0/0/2
 undo shutdown
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/2
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/3
#
ip route-static 0.0.0.0 0.0.0.0 40.1.1.1
#
ip address-set 10.1.1.0/24 type object
 description Address segment of network A
 address 0 10.1.1.0 mask 24
#
ip address-set 10.1.2.0/24 type object
 description Address segment of network B
 address 0 10.1.2.0 mask 24
#
security-policy
 rule name ipsec1
  description Network A-Network B
  source-zone trust
  destination-zone untrust
  source-address address-set 10.1.1.0/24
  destination-address address-set 10.1.2.0/24
  action permit
 rule name ipsec2
  description Network B-Network A
  source-zone untrust
  destination-zone trust
  source-address address-set 10.1.2.0/24
  destination-address address-set 10.1.1.0/24
  action permit
#
```

6.5 Quiz

If the employees of enterprise A and enterprise B need to access the Internet, what precautions should be taken when configuring NAT on the firewall egress?

Reference Answer:

For traffic between enterprise A and enterprise B, the firewall searches for the route to determine the outbound interface. In this case, packets are matched against NAT first and then IPSec on the outbound interface. If NAT is configured on the WAN interfaces of firewalls, ensure that NAT is not performed on the traffic exchanged between enterprise A and enterprise B.

7 SSL VPN

7.1 Introduction

7.1.1 About This Lab

An enterprise wants to use local authentication to authenticate all employees on the firewall. Employees who pass the authentication can access the enterprise intranet, while those who do not pass the authentication cannot access the enterprise intranet.

The enterprise wants mobile office users in a certain group (group1) to be able to obtain an intranet IP address when they are on business trip and can access various intranet resources as if they were on a LAN. To enhance security, local authentication on both the user name and password is required for mobile office users.

7.1.2 Objectives

- Master the method of configuring an SSL VPN virtual gateway.
- Understand the SSL VPN application scenarios and network planning.

7.1.3 Networking Topology

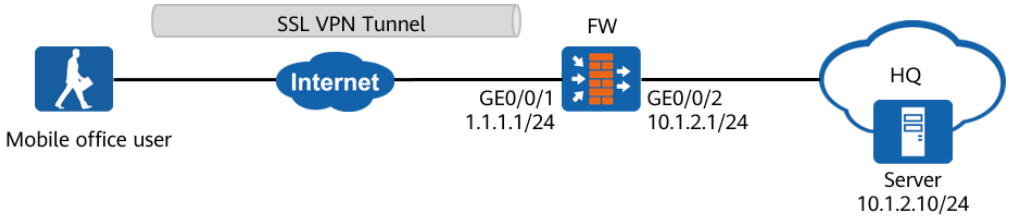


Figure 7-1 Networking topology for configuring SSL VPN

7.1.4 Lab Planning

Table 7-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW	GigabitEthernet0/0/1	1.1.1.1/24	untrust
	GigabitEthernet0/0/2	10.1.2.1/24	trust
Server	Eth0/0/1	10.1.2.10/24	trust
Mobile office	Eth0/0/1	Addresses that can	untrust

Device	Interface	IP Address	Security Zone
users		be used to access the public network	

7.2 Lab Configuration

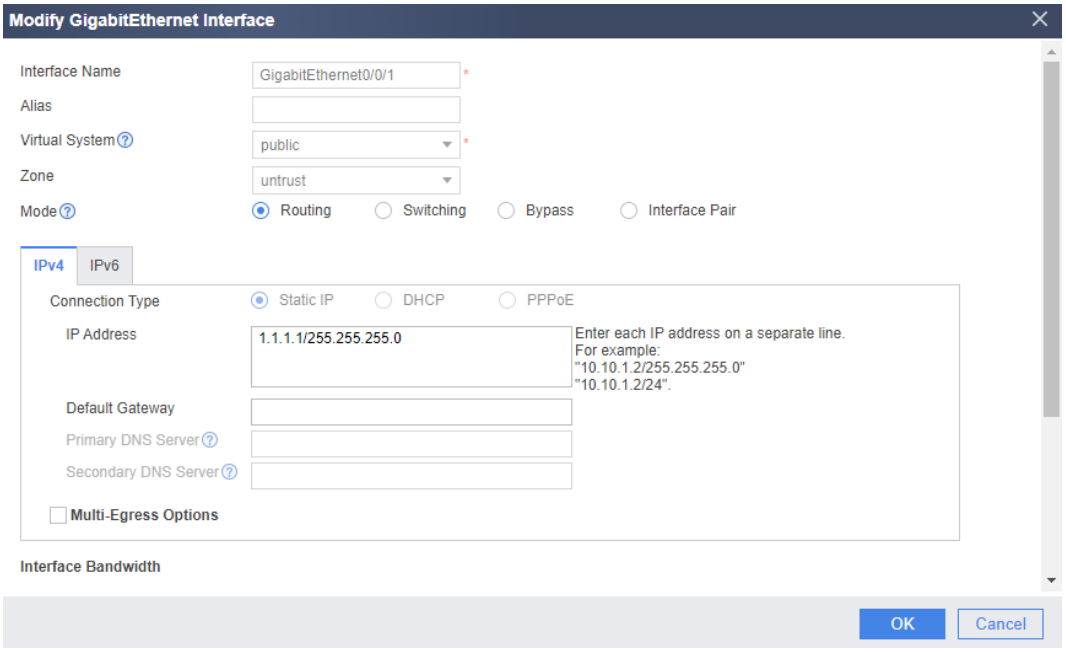
7.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces and add the interfaces to security zones.
2. Configure users and authentication.
3. Configure the SSL VPN gateway.
4. Configure the SSL protocol and other parameters.
5. Configure the security policies.

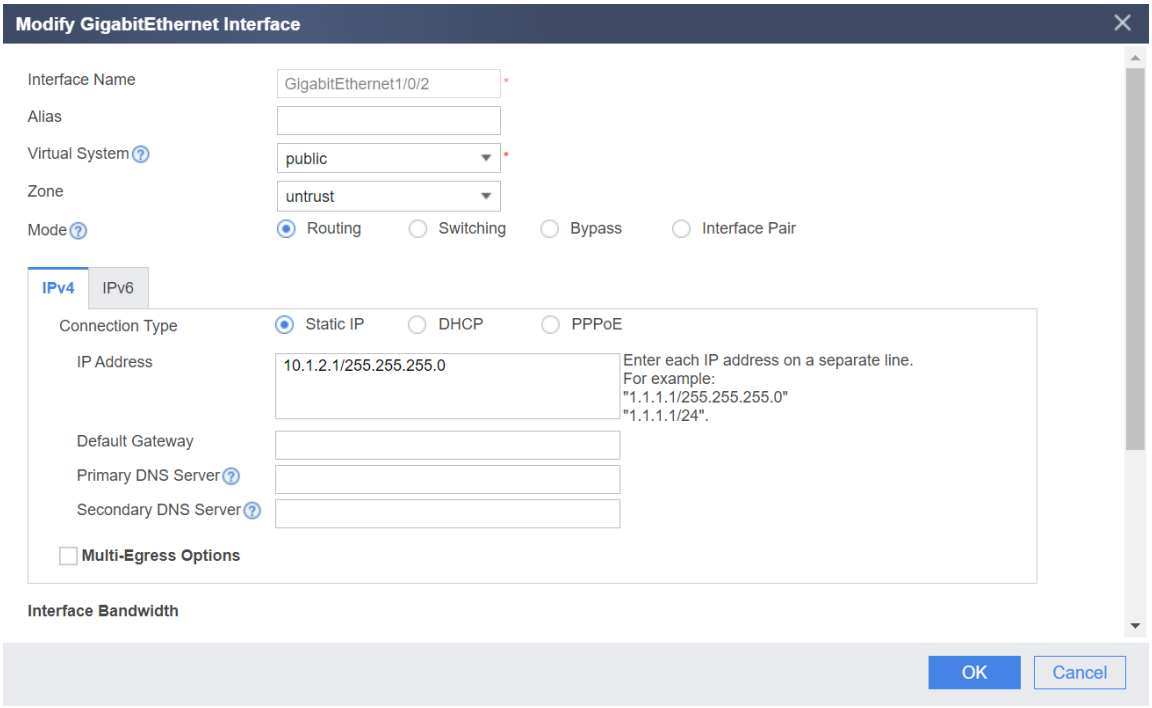
7.2.2 Configuration Procedure on the Web UI

Step 1 Configure interfaces.

On the FW, choose **Network** > **Interface**, click next to GigabitEthernet 0/0/1, and set the parameters as follows.



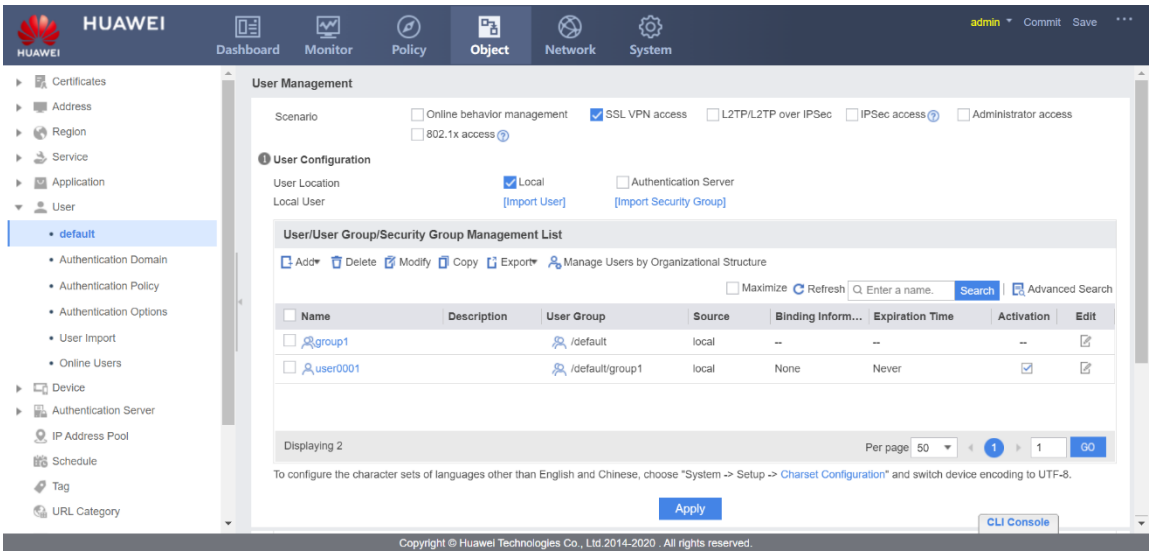
On the FW, choose **Network** > **Interface**, click next to GigabitEthernet 0/0/2, and set the parameters as follows.



Step 2 Configure user objects and authentication.

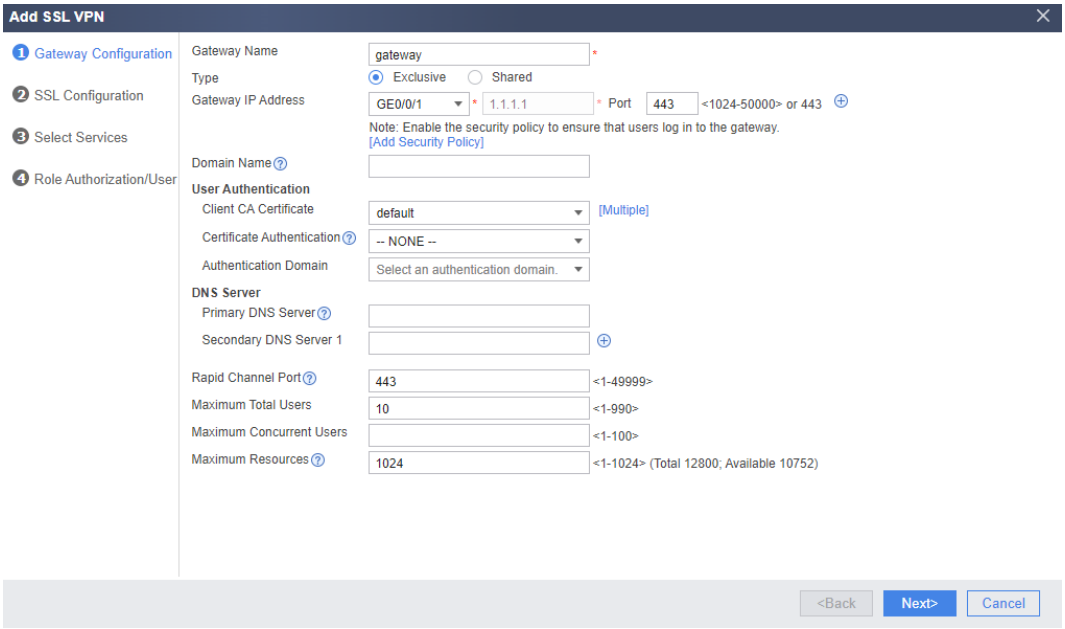
Choose **Object > User > default** and set the parameters as follows:

Set **User Group** of **user0001** to **/default/group1**, **Source** to **local**, and **Password** to **Password@123**. (Note: You need to create the user group **/default/group1** before creating the user **user0001**. In this way, you can select the created user group when creating the user.) Click **Apply**.



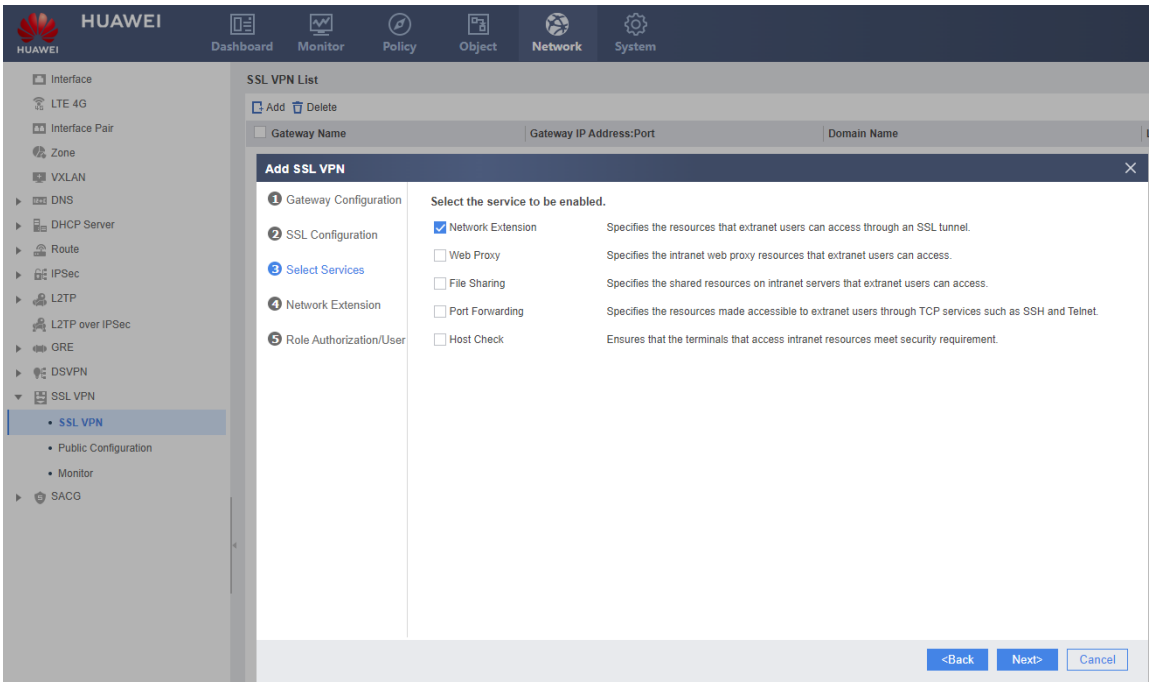
Step 3 Configure an SSL VPN gateway.

Choose **Network** > **SSL VPN** > **SSL VPN**, click **Add**, set parameters as follows, and click **Next>**.

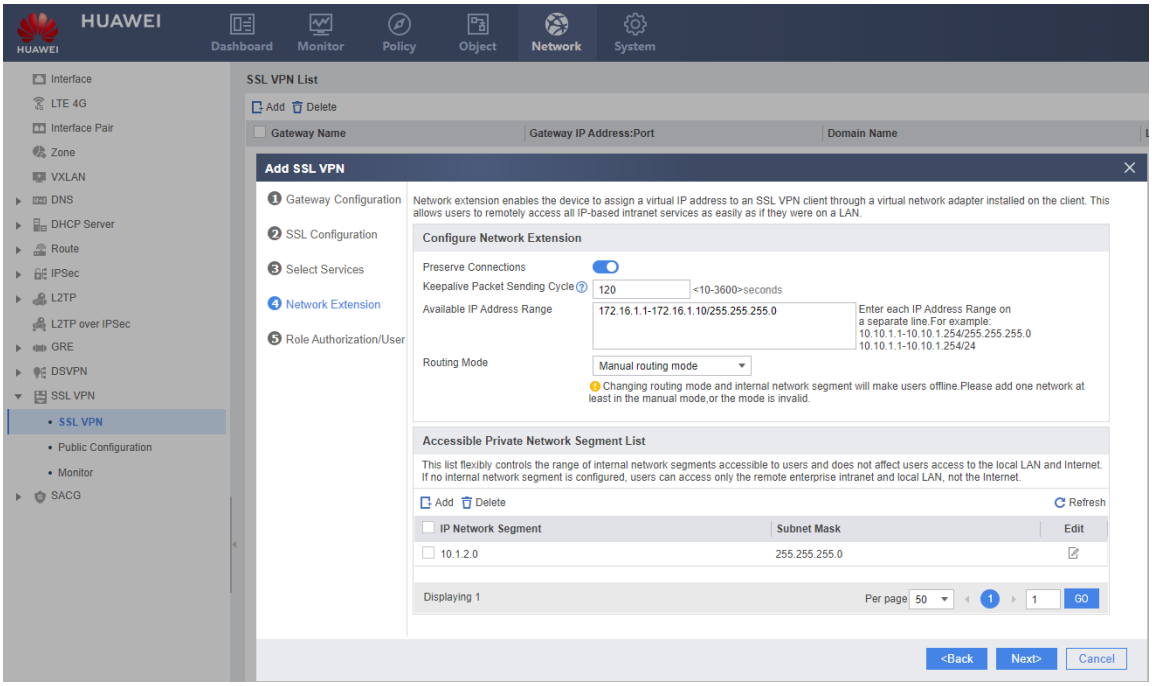


Configure the SSL version, encryption suite, session timeout period, and lifecycle. You can use the default value and click **Next>**.

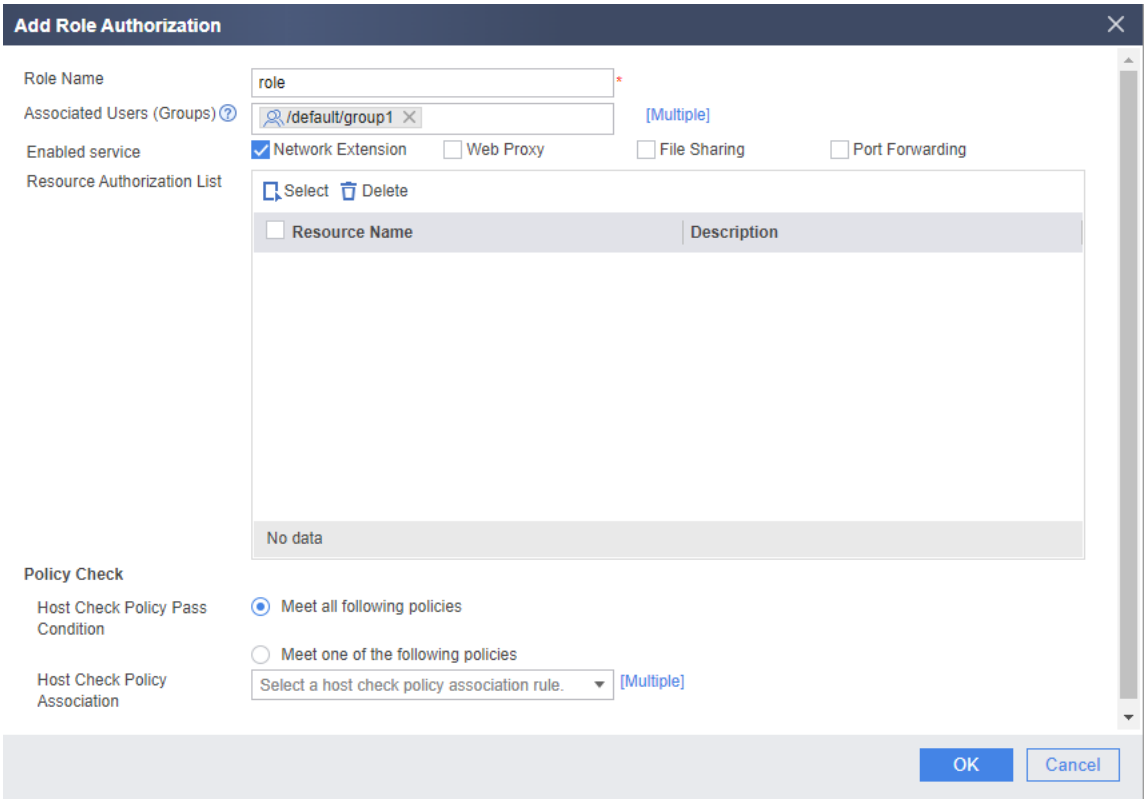
Select **Network Extension** and click **Next>**.



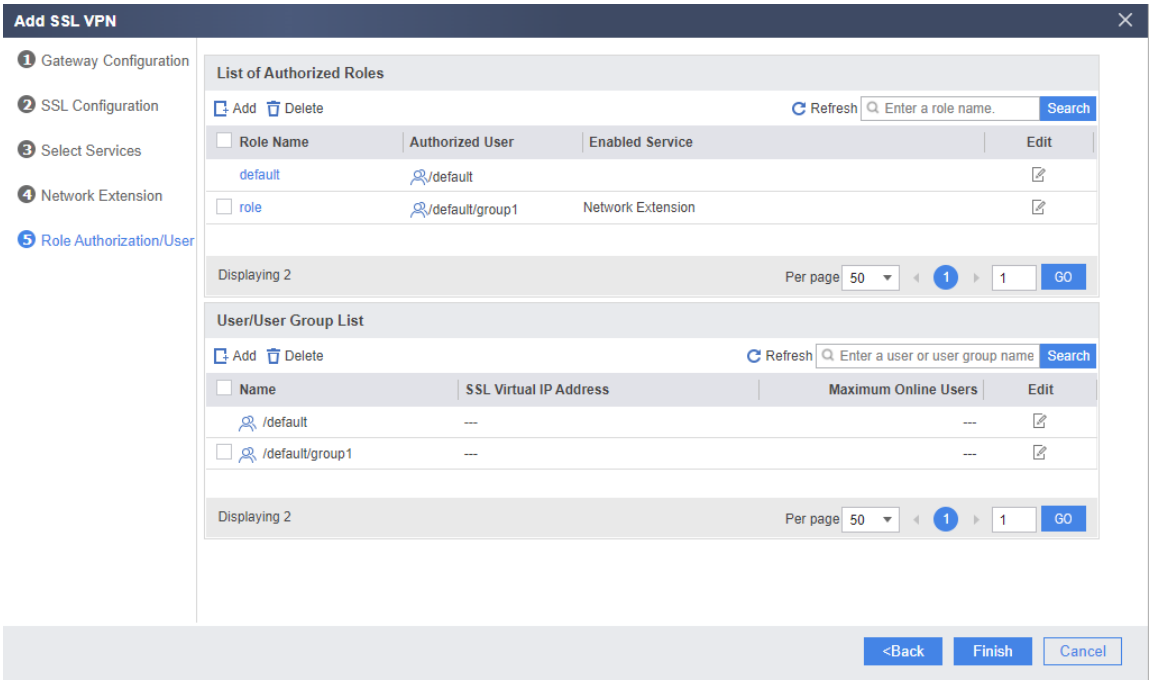
Set parameters on the **Network Extension** tab page and click **Next>**.



Configure SSL VPN role authorization/users. In **Role Authorization List**, click **Add**, and set the role authorization parameters as shown in the following figure. Click **OK**.

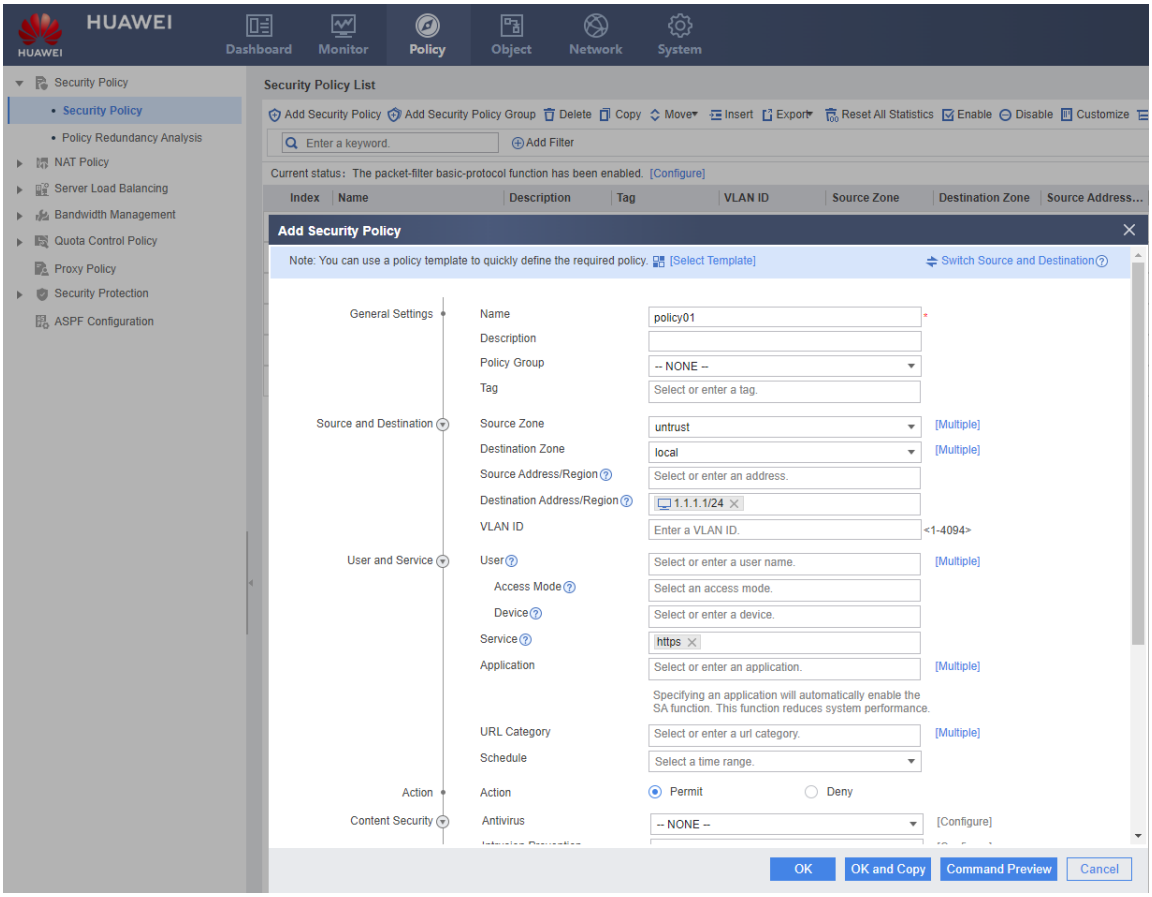


Return to the **Role Authorization/User** page, and click **Finish**.

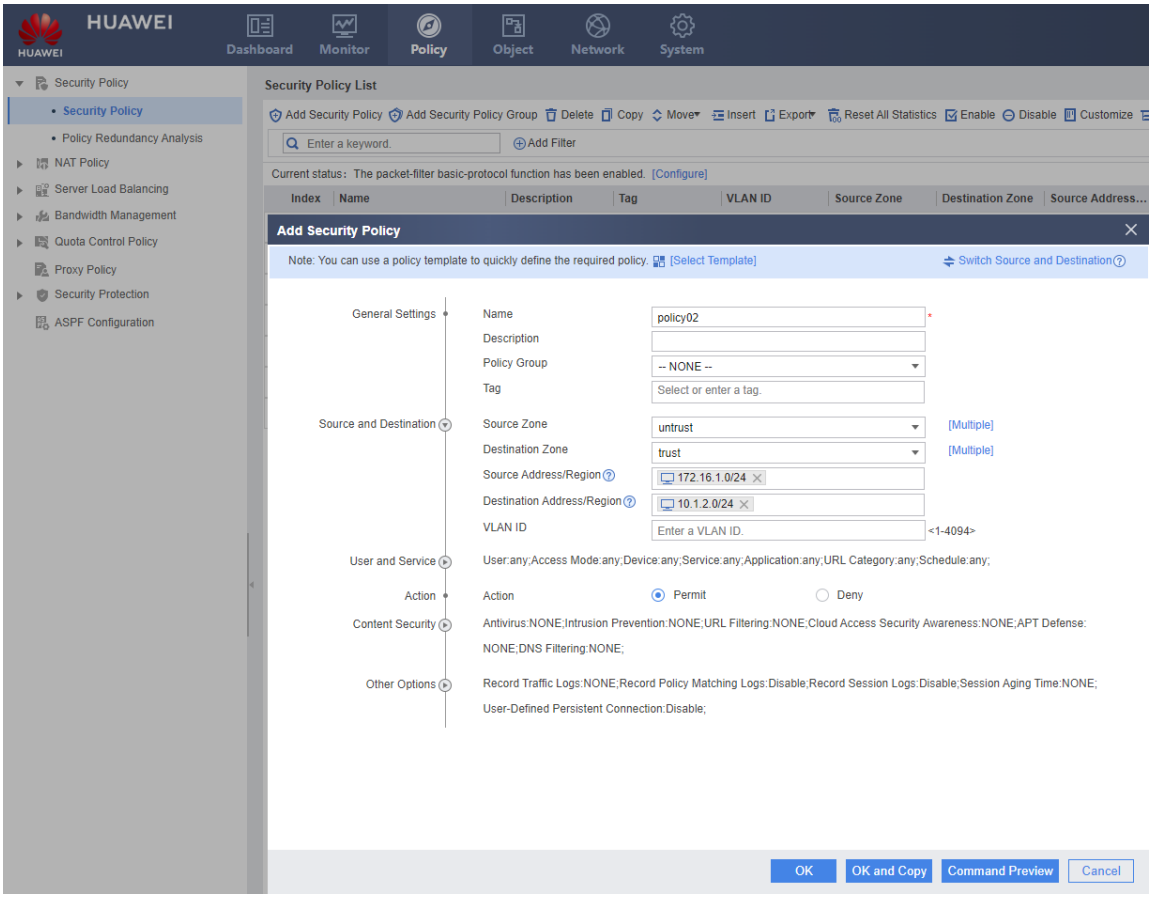


Step 4 Configure security policies.

Configure a security policy for traffic from the Internet to the firewall to allow employees on business trips to log in to the SSL VPN gateway. Choose **Policy** > **Security Policy** > **Security Policy**. Click **Add Security Policy** and configure security policy **policy01**, as shown in the following figure.



Configure a security policy for traffic from the firewall to the intranet to allow employees on business trip to access resources of HQ. Choose **Policy** > **Security Policy** > **Security Policy**. Click **Add Security Policy** and configure security policy **policy02**, as shown in the following figure.



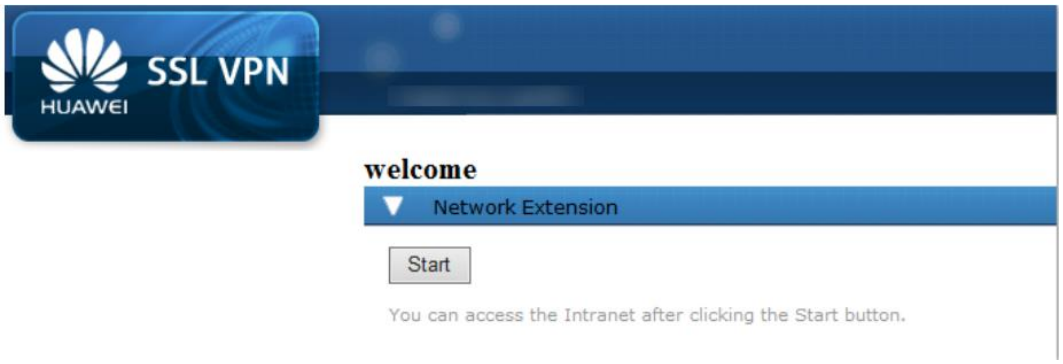
The IP address of the HQ server is **10.1.2.10/24** and that of the gateway is **10.1.2.1**. Detailed configurations are not provided.

7.3 Verification

Access **https://1.1.1.1:443** in the browser to access the SSL VPN login interface as an employee on business trip.

Install the control as prompted upon the first login.

In the login window, enter the user name and password, and then click **Login**. After the login is successful, click **Start** under **Network Extension**. Then you can access the servers on the enterprise intranet.



7.4 Configuration Reference

7.4.1 Firewall Configuration

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
  service-type ssl-vpn
  internet-access mode password
  reference user current-domain
 #
interface GigabitEthernet0/0/1
 undo shutdown
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 undo shutdown
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/2
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/1
#
 v-gateway gateway interface GigabitEthernet0/0/1 private
 v-gateway gateway alias gateway
#
#****BEGIN***gateway**1****#
v-gateway gateway
 basic
  ssl version tlsv12
  ssl timeout 5
  ssl lifecycle 1440
  ssl public-key algorithm rsa
  ssl ciphersuit custom aes256-sha non-des-cbc3-sha aes128-sha
 service
  network-extension enable
  network-extension keep-alive enable
  network-extension keep-alive interval 120
  network-extension netpool 172.16.1.1 172.16.1.10 255.255.255.0
  netpool 172.16.1.1 default
  network-extension mode manual
  network-extension manual-route 10.1.2.0 255.255.255.0
 security
  policy-default-action permit vt-src-ip
  certification cert-anonymous cert-field user-filter subject cn group-filter subject cn
  certification cert-anonymous filter-policy permit-all
  certification cert-challenge cert-field user-filter subject cn
```

```
   certification user-cert-filter key-usage any
   undo public-user enable
  hostchecker
  cachecleaner
  vpndb
   group /default
   group /default/group1
  role
  role default
   role default condition all
  role role
   role role condition all
   role role network-extension enable
#****END****
#
ip address-set 10.1.1.0/24 type object
 address 0 10.1.1.0 mask 24
#
ip address-set 10.1.2.0/24 type object
 address 0 10.1.1.0 mask 24
#
ip address-set 1.1.1.1/24 type object
 address 0 1.1.1.0 mask 24
#
ip address-set 172.16.1.0/24 type object
 address 0 172.16.1.0 mask 24
#
security-policy
 default action permit
 rule name policy01
  source-zone untrust
  destination-zone local
  destination-address address-set 1.1.1.1/24
  service https
  action permit
 rule name policy02
  source-zone untrust
  destination-zone trust
  source-address address-set 172.16.1.0/24
  destination-address address-set 10.1.2.0/24
  action permit
 rule name pass
  action permit
#
```

7.5 Quiz

During the verification, when you click **Start** under **Network Extension**, what will happen to the routing entries and IP address?

Reference Answer:

Run the **route print** command to view the IPv4 routing table. You can see the route destined to **10.1.2.0/24**.

Run the **ipconfig** command to view the information about the local NIC. You can see that the local NIC is assigned an IP address in the range from **172.16.1.1/24** to **172.16.1.10/24**.