Huawei Security Certification Training

HCIA-Security

Lab Guide

ISSUE: 4.0

HUAWEI TECHNOLOGIES CO., LTD

Trademarks and Permissions

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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

Huawei Certification System

Huawei Certification is an integral part of the company's Platform + Ecosystem strategy. It supports the development of ICT infrastructure that features Cloud-Pipe-Device synergy. Our certification is always evolving to reflect the latest trends in ICT development.

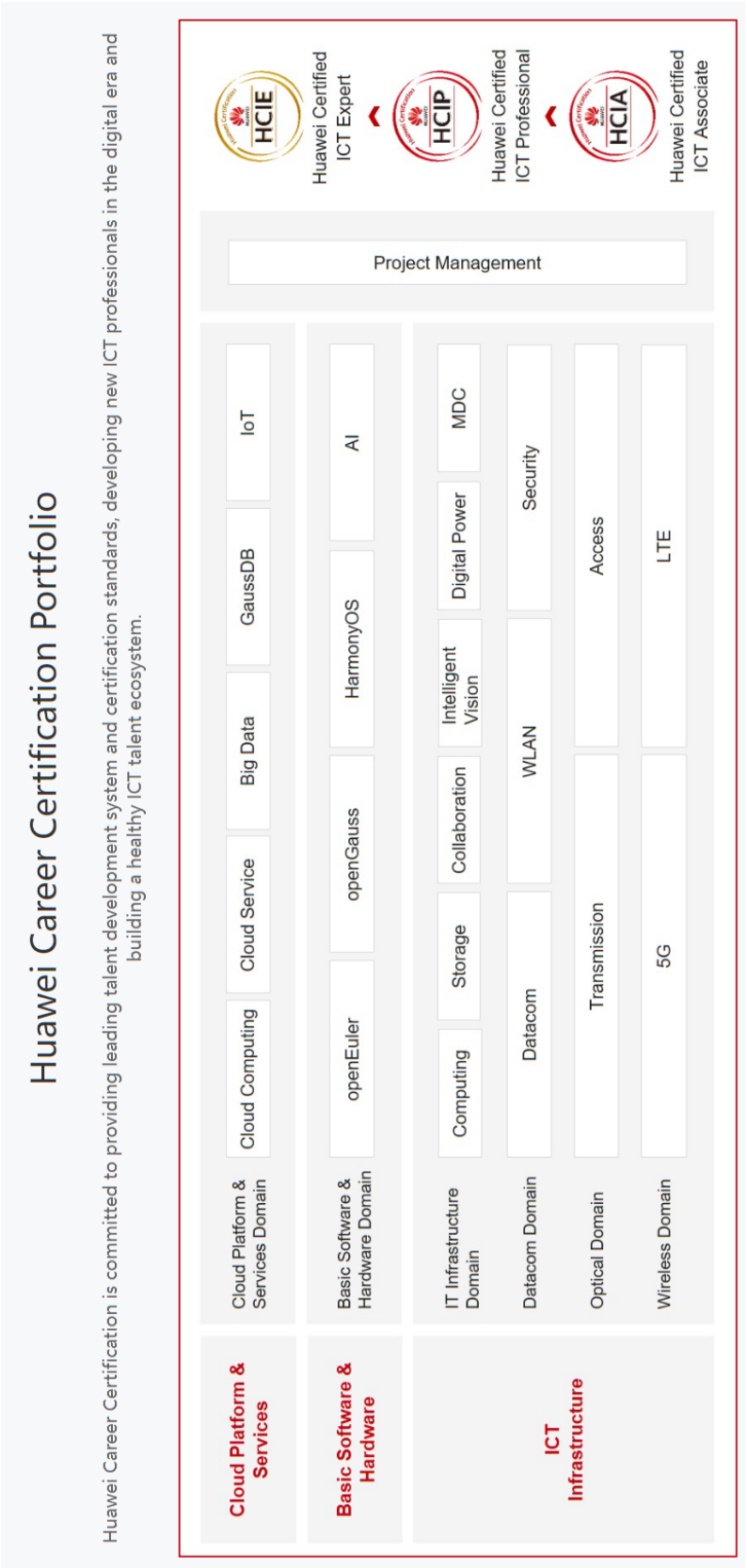
Huawei Certification consists of three categories: ICT Infrastructure Certification, Basic Software & Hardware Certification, and Cloud Platform & Services Certification, making it the most extensive technical certification program in the industry.

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

Our programs cover all ICT fields and follow the industry's trend of ICT convergence. With our leading talent development system and certification standards, we are committed to fostering new digital ICT talent and building a sound ICT talent ecosystem.

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

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


Huawei Career Certification Portfolio
Huawei Career Certification is committed to providing leading talent development system and certification standards, developing new ICT professionals in the digital era and building a healthy ICT talent ecosystem.
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate
Project Management
Cloud Platform & Services
Basic Software & Hardware
ICT Infrastructure
Cloud Platform & Services Domain
Cloud Computing
Cloud Service
Big Data
GaussDB
IoT
Basic Software & Hardware Domain
openEuler
openGauss
HarmonyOS
AI
IT Infrastructure Domain
Computing
Storage
Collaboration
Intelligent Vision
Digital Power
MDC
Datacom Domain
Datacom
WLAN
Security
Optical Domain
Transmission
Access
Wireless Domain
5G
LTE

About This Document

Overview

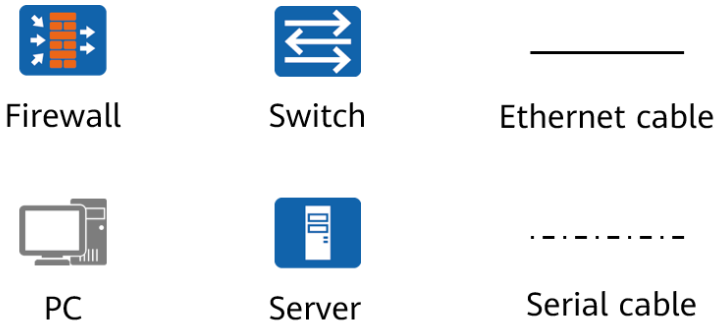
This document is an HCIA-Security certification training course and is intended for trainees who are going to take the HCIA-Security exam or readers want to understand the information security concepts and specifications, common cyber security threats and prevention, basic knowledge of cyber security,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

Background Knowledge Required

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

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

Common Icons



Experiment Environment Overview

This document is based on Huawei data communication simulator eNSP Pro. The datacom simulator provides a one-stop datacom simulator environment for users in the training, certification, and learning solutions of Huawei datacom product line.

Simulator Name	Software Version
eNSP Pro	eNSP Pro V100R001C10

You can click eNSP Pro to obtain the latest product version and product documentation.

You can also use eNSP Pro through the o3 community.

Note: eNSP Pro is for certified partners only. (ASP, Service Partner/Business Operation Partner, Sales Partner) This document is published on the enterprise business website. It is temporarily not open to registered sales partners, talent alliance partners, consulting and planning partners, solution development partners, investment and financing partners, industry partners, product customers, and common registered users. If your company is an ASP, service partner, business operation partner, or sales partner, after the company completes the authentication on the ePartner website, you can upgrade your account by referring to the link to the associated company.

Experimental Comparison with Real Machine Environment

Real machine environment	Data communication simulator
1. Firewall Login	Changed to the basic configuration of the YunShan OS.
2. Firewall Security Policy	Support
3. Firewall NAT Server and Source NAT	Support
4. Firewall Hot Standby	Support
5. User Management	Not supported
6. Site-to-Site IPSec VPN	Not supported
7. SSL VPN	Not supported

Contents

1 Firewall Login

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

By default, the eNSP simulator is connected to the console port. Therefore, you can directly log in to the device without manually connecting a serial cable when using the simulator to perform lab operations. If you need to manually connect a serial cable to the console to log in to the USG, see the HCIA-Security Experiment Manual.

1.2 Getting Familiar with Commands (Slightly)

1.2.1 Introduction

1.2.1.1 About This Lab

This exercise aims to understand and get familiar with basic operations of the Huawei Yunshan system by configuring Huawei devices.

1.2.1.2 Objectives

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

1.2.1.3 Networking Topology

The device models used in this lab is ENSP-USG.

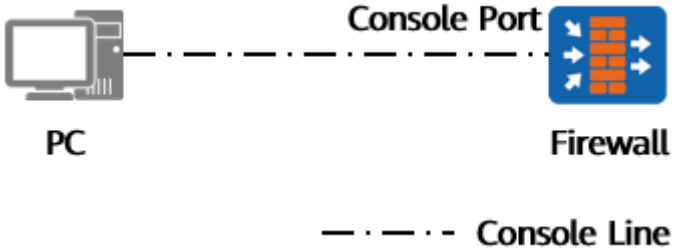


Figure 1-1 Topology for logging in to the device through the console port

1.2.1.4 Background

As shown in the networking diagram, the FW is a brand-new firewall without configuration. The network administrator needs to debug the firewall and learns the CLI operations of the firewall.

By default, the eNSP simulator is connected to the console port. Therefore, you can directly log in to the device without manually connecting a serial cable when using the simulator to perform lab operations.

1.2.2 Lab Configuration

1.2.2.1 Configuration Roadmap

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

1.2.2.2 Configuration Procedure

Step 1 Log in to the device through the console port. (Slightly)

Step 2 Enter the system view.

Set a password after the connection to the firewall is established. Most commands need to be configured in the system view. Therefore, you need to enter the system view from the user view before the configuration. The commands are as follows:

```
Please press "Enter" to start command line
---------------------------------------------
eNSP can only be used for practice.
This device is an emulator and does not reflect a physical device model.
Some functions and commands may not supported.
Please read the feature list carefully before using.
---------------------------------------------

User interface con0 is available


Please Press ENTER.


Please configure the login password (8-16)
Enter Password: Huawei@123
Confirm Password: Huawei@123
Info: Save the password now. Please wait for a moment.

*************************************************************
*                    Copyright (C) 20xx-20xx                *
*                  Huawei Technologies Co., Ltd.            *
*                       All rights reserved.                *
*              Without the owner's prior written consent,   *
*     no decompiling or reverse-engineering shall be allowed.*
*************************************************************
```

```
Info: The max number of VTY users is 21, the number of current VTY users online is 0, and total
number of terminal users online is 1.
        The current login time is 20xx-xx-xx 14:54:52.
<HUAWEI>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[HUAWEI]
```

Step 3 Modify the device name.

Run the sysname command in the system view to change the device name.

```
[HUAWEI]sysname FW
[FW]
```

Step 4 Enter the interface view.

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

```
[FW] interface GE 0/0/1
[FW-GE0/0/1]
```

Step 5 Get online help.

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

```
[FW] interface ?
  Eth-Trunk     Ethernet-Trunk interface
  GE            GE interface
  LoopBack      LoopBack interface
  MEth          MEth interface
  NULL          NULL interface
  Tunnel        Tunnel interface
  Virtual-if    Virtual interface
  Vlanif        VLAN interface
  range         Interface range command
```

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

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

Step 6 Quit the current view (go back to the previous view).

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

```
[FW-GE0/0/1] quit
[FW]
```

Step 7 Return to the user view.

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

```
[FW-GE0/0/1] return
<FW>
```

Step 8 Display the device version.

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

```
<FW> display version
2024-xx-xx 14:59:35.523
Huawei YunShan OS
Version 1.22.0.1 (USG6600F V100R022C00)
Copyright (C) 20xx-20xx Huawei Technologies Co., Ltd.
HUAWEI USG6655F uptime is 0 day, 0 hour, 5 minutes


MPU(Master) 0 : uptime is   0 day, 0 hour, 5 minutes
            StartupTime 20xx/xx/xx     14:53:56
Memory          Size       : 4096 M bytes
Flash           Size       : 0 M bytes
MPU version information:
1.PCB           Version : usg VER A
2.MAB           Version : 0
3.Board         Type       : usg
4.BIOS          Version : 000
5.CPLD1         Version : 000
  CPLD2         Version : 000
```

Step 9 Save configurations.

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

```
<FW> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
Now saving the current configuration to the slot 0
Info: Save the configuration successfully.
```

Step 10 Display configurations.

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

```
[FW-GE0/0/0] display this
2024-xx-xx 15:01:17.540
#
```

```
interface GE0/0/0
 ip address 192.168.0.1 255.255.255.0
 device transceiver 1000BASE-X
#
return
```

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

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

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

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

1.2.3 Quiz

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

Reference Answer:

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

1.3 Logging In to a Device Through Telnet (Slightly)

Remote login to the USG is not supported in the eNSP Pro simulation environment. If you want to remotely log in to the USG through the CLI, refer to the following link:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100301333&id=EN-US_TASK_0000001124848964

1.4 Logging In to the Device Through SSH (Slightly)

eNSP Pro 模拟环境中暂不支持通过 SSH 登录 USG 设备。若真机设备想通过命令行方式 SSH 登录 USG 设备，可参考以下链接中的指导步骤：

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100301333&id=EN-US_TASK_0000001171568591

2 Firewall Security Policy

2.1 Introduction

2.1.1 About This Lab

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

2.1.2 Objectives

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

2.1.3 Networking Topology

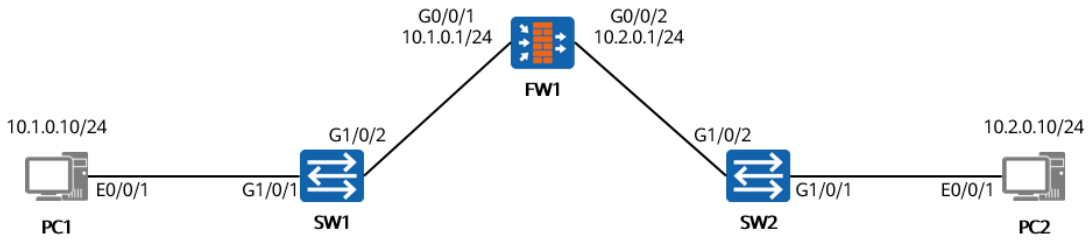


Figure 2-1 Topology for configuring firewall security policies

2.1.4 Lab Planning

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

Table 2-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW1	GE0/0/1	10.1.0.1/24	trust
	GE0/0/2	10.2.0.1/24	untrust

Device	Interface	IP Address	Security Zone
PC1	Eth0/0/1	10.1.0.10/24	trust
PC2	Eth0/0/1	10.2.0.10/24	untrust

2.2 Lab Configuration

2.2.1 Configuration Roadmap

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

2.2.2 Configuration Procedure on the CLI

Step 1 Configure interfaces and security zones.

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

```
<HUAWEI> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[HUAWEI] sysname FW1
[FW1] interface G0/0/1
[FW1-GE0/0/1] ip address 10.1.0.1 255.255.255.0
[FW1-GE0/0/1] quit
[FW1] interface G0/0/2
[FW1-GE0/0/2] ip address 10.2.0.1 255.255.255.0
[FW1-GE0/0/2] quit
[FW1] firewall zone trust
[FW1-zone-trust] add interface G0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface G0/0/2
[FW1-zone-untrust] quit
```

Step 2 Configure a forwarding policy.

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

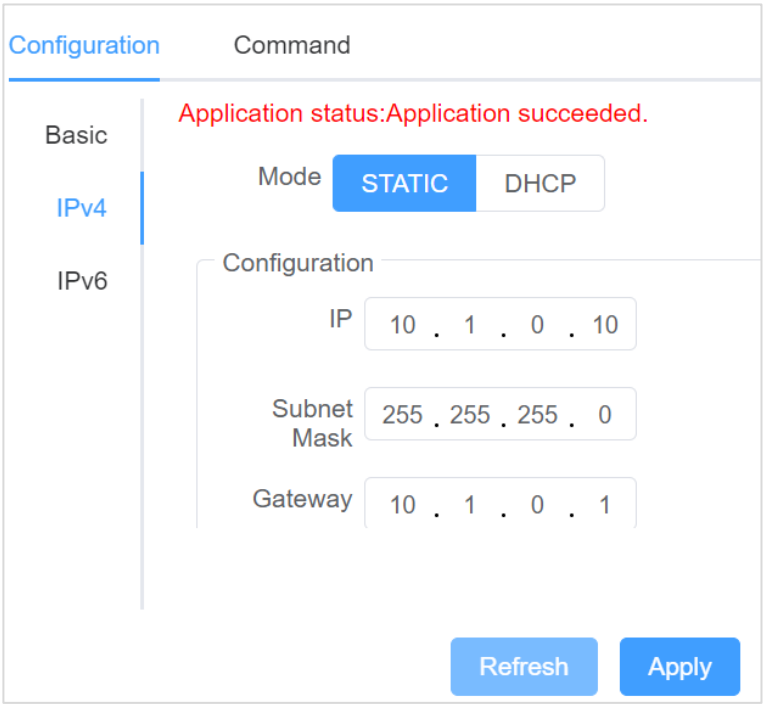
```
[FW1] security-policy
[FW1-policy-security] rule name policy_sec
[FW1-policy-security-rule-policy_sec] source-zone trust
[FW1-policy-security-rule-policy_sec] destination-zone untrust
[FW1-policy-security-rule-policy_sec] action permit
[FW1-policy-security-rule-policy_sec] quit
```

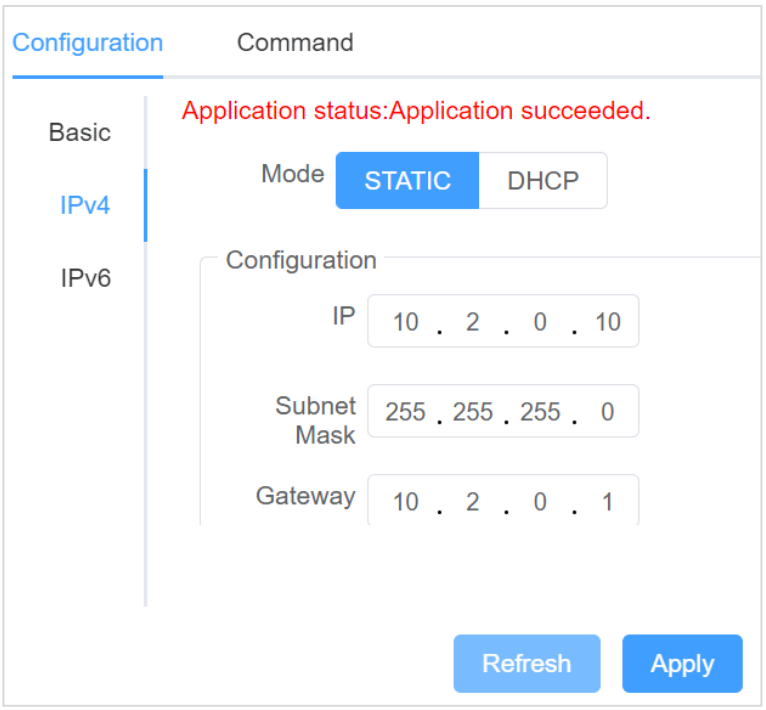
Step 3 Configure the switch.

Add the two interfaces of the two switches to the same VLAN. The default VLAN is used. By default, all service interfaces on the switch are added to the default VLAN. For details about how to configure additional service VLANs, see the product documentation of Huawei switches.

Step 4 Configure the PC.

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





2.3 Verification

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

```
PC> ping 10.2.0.10
PING 10.2.0.10 (10.2.0.10) 56(84) bytes of data.
64 bytes from 10.2.0.10: icmp_seq=1 ttl=63 time=32.5 ms
64 bytes from 10.2.0.10: icmp_seq=2 ttl=63 time=11.1 ms
64 bytes from 10.2.0.10: icmp_seq=3 ttl=63 time=7.83 ms
64 bytes from 10.2.0.10: icmp_seq=4 ttl=63 time=9.09 ms
64 bytes from 10.2.0.10: icmp_seq=5 ttl=63 time=9.11 ms
^C
--- 10.2.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 7.826/13.938/32.531/9.356 ms
PC>
```

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

```
[FW1] display firewall session table
20xx-xx-xx 01:51:18.519
  Current Total Sessions : 1
  Slot: 0 CPU: 0
  ICMP    VPN: public --> public    10.1.0.10:4 --> 10.2.0.10:2048
[FW1]
```

2.4 Quiz

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

Reference Answer:

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

3 Firewall NAT Server and Source NAT

3.1 Introduction

3.1.1 About This Lab

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

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

3.1.2 Objectives

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

3.1.3 Networking Topology

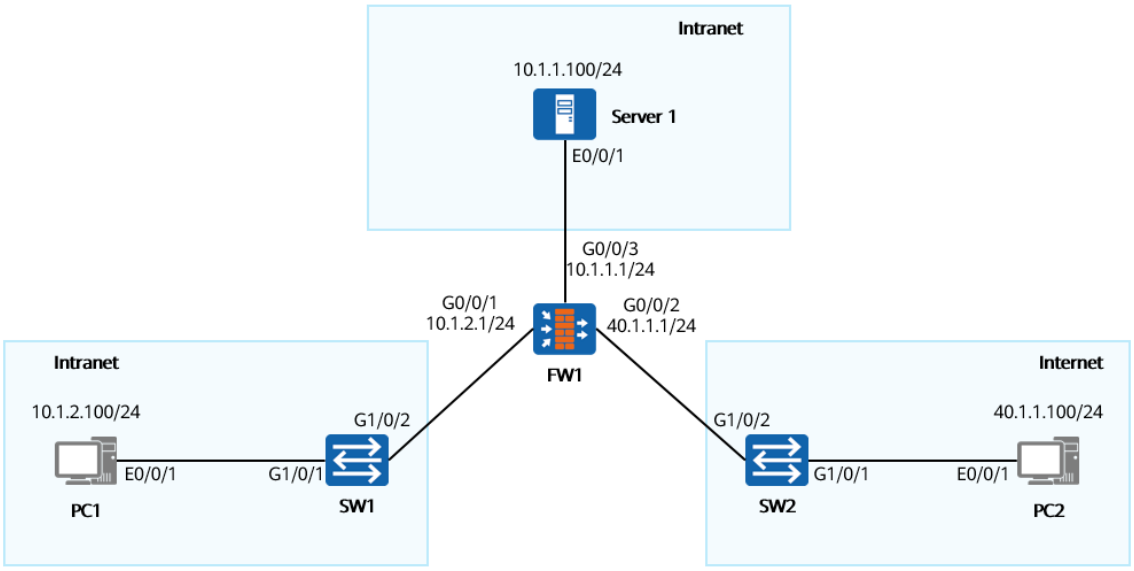


Figure 3-1 Topology for configuring the NAT Server and Source NAT for a firewall

3.1.4 Lab Planning

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

Table 3-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW1	GE0/0/1	10.1.2.1/24	trust
	GE0/0/2	40.1.1.1/24	untrust
	GE0/0/3	10.1.1.1/24	dmz
PC1	Eth0/0/1	10.1.2.100/24	trust
PC2	Eth0/0/1	40.1.1.100/24	untrust
Server 1	Eth0/0/1	10.1.1.100/24	dmz

3.2 Lab Configuration (Source NAT)

3.2.1 Configuration Roadmap

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

3.2.2 Configuration Procedure on the CLI

Step 1 Configure interfaces and security zones.

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

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

```
<HUAWEI> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[HUAWEI] sysname FW1
[FW1] interface G0/0/1
[FW1-GE0/0/1] ip address 10.1.2.1 255.255.255.0
[FW1-GE0/0/1] quit
[FW1] interface G0/0/2
[FW1-GE0/0/2] ip address 40.1.1.1 255.255.255.0
[FW1-GE0/0/2] quit
[FW1] interface G0/0/3
[FW1-GE0/0/3] ip address 10.1.1.1 255.255.255.0
[FW1-GE0/0/3] quit
```

Add the interfaces of FW1 to the corresponding security zones.

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface G0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface G0/0/2
[FW1-zone-untrust] quit
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface G0/0/3
[FW1-zone-dmz] quit
```

Step 2 Configure a forwarding policy.

Configure a forwarding policy between the Trust and Untrust zones.

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

Step 3 Configure a NAT address pool..

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

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

Step 4 Configure a NAT policy.

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

Step 5 Configure the switches.

Add the two interfaces of the two switches to the same VLAN. The default VLAN is used. By default, all service interfaces on the switch are added to the default VLAN. For details about how to configure additional service VLANs, see the product documentation of Huawei switches.

3.2.3 Verification

Ping PC2 from PC1.

```
PC> ping 40.1.1.100
PING 40.1.1.100 (40.1.1.100) 56(84) bytes of data.
64 bytes from 40.1.1.100: icmp_seq=1 ttl=63 time=12.1 ms
64 bytes from 40.1.1.100: icmp_seq=2 ttl=63 time=11.4 ms
```

```
64 bytes from 40.1.1.100: icmp_seq=3 ttl=63 time=10.0 ms
64 bytes from 40.1.1.100: icmp_seq=4 ttl=63 time=9.93 ms
64 bytes from 40.1.1.100: icmp_seq=5 ttl=63 time=10.1 ms
64 bytes from 40.1.1.100: icmp_seq=6 ttl=63 time=12.1 ms
^C
--- 40.1.1.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 9.932/10.929/12.107/0.963 ms
PC>
```

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

```
[FW1] display firewall session table
20xx-xx-xx 15:37:04.744
  Current Total Sessions : 1
  Slot: 0 CPU: 0
  ICMP    VPN: public --> public    10.1.2.100:2[2.2.2.5:2048] --> 40.1.1.100:2048
[FW1]
```

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

3.2.4 Quiz

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

Reference Answer:

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

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

3.3 Lab Configuration (NAT Server and Source NAT)

3.3.1 Configuration Roadmap

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

3.3.2 Configuration Procedure on the CLI

Step 1 Configure interfaces and security zones.

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

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

```
<HUAWEI> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[HUAWEI] sysname FW1
[FW1] interface GE0/0/1
[FW1-GE0/0/1] ip address 10.1.2.1 255.255.255.0
[FW1-GE0/0/1] quit
[FW1] interface GE0/0/2
[FW1-GE0/0/2] ip address 40.1.1.1 255.255.255.0
[FW1-GE0/0/2] quit
[FW1] interface GE0/0/3
[FW1-GE0/0/3] ip address 10.1.1.1 255.255.255.0
[FW1-GE0/0/3] quit
```

Add the interfaces of FW1 to the corresponding security zones.

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface GE0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GE0/0/2
[FW1-zone-untrust] quit
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface GE0/0/3
[FW1-zone-dmz] quit
```

Step 2 Configure a forwarding policy.

Configure a forwarding policy between the Untrust and DMZ zones.

```
[FW1] security-policy
[FW1-policy-security] rule name bidectinal_nat
[FW1-policy-security-rule-policy_sec] source-zone untrust
[FW1-policy-security-rule-policy_sec] destination-zone dmz
[FW1-policy-security-rule-policy_sec] action permit
[FW1-policy-security-rule-policy_sec] service ftp
Warning: You attempt to add the first service object for the policy. This will narrow down the policy
matching scope. Continue?Please select [Y/N]: y
[FW1-policy-security-rule-policy_sec] quit
```

Step 3 Configure a NAT server.

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

Step 4 Configure a NAT address pool.

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

Step 5 Configure the NAT ALG function.

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

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

Step 6 Create a NAT policy.

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

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

Step 7 Configure the switches.

Add the two interfaces of the two switches to the same VLAN. The default VLAN is used. By default, all service interfaces on the switch are added to the default VLAN. For details about how to configure additional service VLANs, see the product documentation of Huawei switches.

3.3.3 Verification

Check related information on the firewall.

```
[FW1] display nat server
2024-xx-xx 02:02:20.724
Server in private network information:
  Total     1 NAT server(s)
 server name     : ftpserver
 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                 zone               : ---
 protocol          : tcp                     vrrp              : ---
 no-reverse        : 0                       nat-disable       : 0
 route             : 0                       description       : ---
```

3.3.4 Quiz

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

Reference Answer:

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

4 Firewall Hot Standby

4.1 Introduction

4.1.1 About This Lab

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

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

4.1.2 Objectives

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

4.1.3 Networking Topology

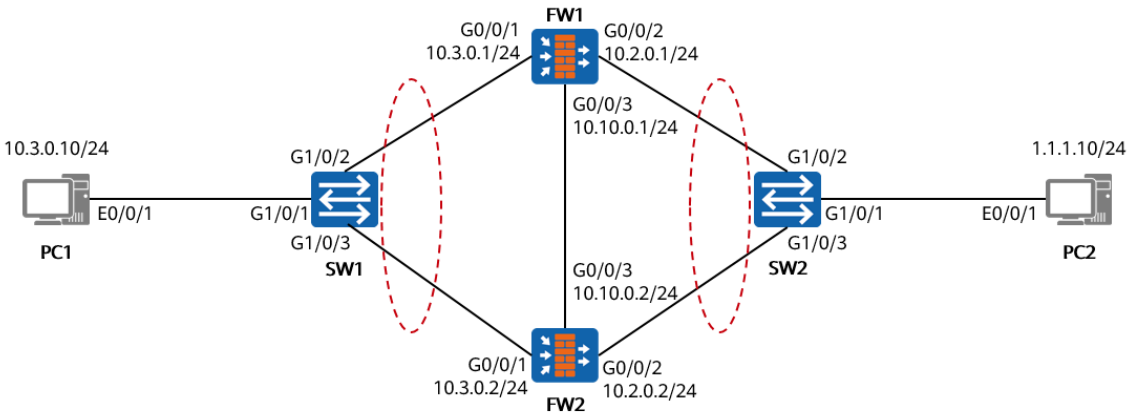


Figure 4-1 Networking topology for configuring firewall hot standby

4.1.4 Lab Planning

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

Table 4-1 Port address and zone planning

Device	Interface	IP Address	Security Zone
FW1	GE0/0/1	10.3.0.1/24	trust
	GE0/0/2	10.2.0.1/24	untrust
	GE0/0/3	10.10.0.1/24	dmz
FW2	GE0/0/1	10.3.0.2/24	trust
	GE0/0/2	10.2.0.2/24	untrust
	GE0/0/3	10.10.0.2/24	dmz
PC1	Eth0/0/1	10.3.0.10/24	trust
PC2	Eth0/0/1	1.1.1.10/24	untrust
SW1	GE1/0/1 GE1/0/2 GE1/0/3	Access	PVID: VLAN 10
SW2	GE1/0/1 GE1/0/2 GE1/0/3	Access	PVID: VLAN 10

4.2 Lab Configuration

4.2.1 Configuration Roadmap

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

4.2.2 Configuration Procedure on the CLI

Step 1 Configure interfaces and security zones.

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

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

```
<HUAWEI> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[HUAWEI] sysname FW1
```

```
[FW1] interface GE0/0/1
[FW1-GE0/0/1] ip address 10.3.0.1 255.255.255.0
[FW1-GE0/0/1] quit
[FW1] interface GE0/0/2
[FW1-GE0/0/2] ip address 10.2.0.1 255.255.255.0
[FW1-GE0/0/2] quit
```

Configure VRRP group 1 on GE0/0/1 of FW1 and add it to the VGMP group in the **Active** state.

```
[FW1] interface GE0/0/1
[FW1-GE0/0/1] vrrp vrid 1 virtual-ip 10.3.0.3 active
[FW1-GE0/0/1] quit
```

Configure VRRP group 2 on GE0/0/2 of FW1 and add it to the VGMP group in the **Active** state.

```
[FW1] interface GE0/0/2
[FW1-GE0/0/2] vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 active
[FW1-GE0/0/2] quit
```

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

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface GE0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GE0/0/2
[FW1-zone-untrust] quit
```

Configure the upstream and downstream service interfaces of FW2.

```
<HUAWEI> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[HUAWEI] sysname FW2
[FW2] interface GE0/0/1
[FW2-GE0/0/1] ip address 10.3.0.2 255.255.255.0
[FW2-GE0/0/1] quit
[FW2] interface GE0/0/2
[FW2-GE0/0/2] ip address 10.2.0.2 255.255.255.0
[FW2-GE0/0/2] quit
```

Configure VRRP group 1 on GE0/0/1 of FW2 and add it to the VGMP group in the **Standby** state. (**Note**: If the VRRP virtual IP address and the real IP address are in the same network segment, you do not need to add the mask parameter. If the VRRP virtual IP address and the real IP address are in different network segments, you need to add the mask parameter.)

```
[FW2] interface GE0/0/1
[FW2-GE0/0/1] vrrp vrid 1 virtual-ip 10.3.0.3 standby
[FW2-GE0/0/1] quit
```

Configure VRRP group 2 on GE0/0/2 of FW2 and add it to the VGMP group in the **Standby** state.

```
[FW2] interface GE0/0/2
[FW2-GE0/0/2] vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 standby
[FW2-GE0/0/2] quit
```

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

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

Configure default routes on FW1 and FW2 and set the next hop to 1.1.1.10 so that traffic from PC1 can be forwarded to PC2.

```
[FW1] ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
```

```
[FW2] ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
```

Step 2 Configure the heartbeat cables for FW1 and FW2.

Configure an IP address for the heartbeat interface GE0/0/3 of FW1.

```
[FW1] interface GE0/0/3
[FW1-GE0/0/3] ip address 10.10.0.1 255.255.255.0
[FW1-GE0/0/3] quit
```

Configure an IP address for the heartbeat interface GE0/0/3 of FW2.

```
[FW2] interface GE0/0/3
[FW2-GE0/0/3] ip address 10.10.0.2 255.255.255.0
[FW2-GE0/0/3] quit
```

Add the heartbeat interface GE0/0/3 of FW1 to the DMZ.

```
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface GE0/0/3
[FW1-zone-dmz] quit
```

Add the heartbeat interface GE0/0/3 of FW2 to the DMZ.

```
[FW2] firewall zone dmz
[FW2-zone-dmz] add interface GE0/0/3
[FW2-zone-dmz] quit
```

Configure an authentication key for the heartbeat interface on FW1, enable dual-system hot backup, and allow HRP packets to pass through. (**Note**: There are two ways to permit HRP packets. One is to cancel the filtering of basic protocol packets shown in this experiment manual, and the other is to configure a security policy.)

```
[FW1] hrp interface GE0/0/3 remote 10.10.0.2
[FW1] hrp authentication-key Admin@123
[FW1] hrp enable
[FW1] undo firewall packet-filter basic-protocol enable
```

Configure an authentication key for the heartbeat interface on FW1, enable dual-system hot backup, and allow HRP packets to pass through.

```
[FW2] hrp interface GE0/0/3 remote 10.10.0.1
[FW2] hrp authentication-key Admin@123
[FW2] hrp enable
[FW2] undo firewall packet-filter basic-protocol enable
```

Step 3 Configure a security policy.

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

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

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

Step 4 Configure a NAT policy.

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

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

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

Step 5 Configure the switches.

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

4.3 Verification

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

```
HRP_M[FW1] display vrrp verbose
20xx-xx-xx 03:30:20.471
GE0/0/1 | Virtual Router 1
State              : Master
Virtual IP         : 10.3.0.3
Master IP          : 10.3.0.1
PriorityRun        : 120
PriorityConfig : 100
MasterPriority : 120
Preempt            : YES     Delay Time : 0s     Remain : --
Hold Multiplier: 3
TimerRun           : 30s
TimerConfig        : 30s
Auth Type          : NONE
Virtual MAC        : 0000-5e00-0101
Check TTL          : YES
Config Type        : vgmp-vrrp
Create Time            : 20xx-xx-xx 01:17:00
Last Change Time   : 20xx-xx-xx 01:22:29

GE0/0/2 | Virtual Router 2
State              : Master
Virtual IP         : 1.1.1.1
Master IP          : 10.2.0.1
PriorityRun        : 120
PriorityConfig : 100
MasterPriority : 120
Preempt            : YES     Delay Time : 0s     Remain : --
Hold Multiplier: 3
TimerRun           : 30s
TimerConfig        : 30s
Auth Type          : NONE
Virtual MAC        : 0000-5e00-0102
Check TTL          : YES
Config Type        : vgmp-vrrp
Create Time            : 20xx-xx-xx 01:17:15
Last Change Time   : 20xx-xx-xx 01:22:29
```

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

```
HRP_S<FW2> display vrrp verbose
```

```
20xx-xx-xx 03:33:01.83
GE0/0/1 | Virtual Router 1
State             : Backup
Virtual IP        : 10.3.0.3
Master IP         : 10.3.0.1
PriorityRun       : 120
PriorityConfig : 100
MasterPriority : 120
Preempt           : YES     Delay Time : 0s     Remain : --
Hold Multiplier: 3
TimerRun          : 30s
TimerConfig       : 30s
Auth Type         : NONE
Virtual MAC       : 0000-5e00-0101
Check TTL         : YES
Config Type       : vgmp-vrrp
Create Time           : 20xx-xx-xx 01:19:11
Last Change Time   : 20xx-xx-xx 01:57:08

GE0/0/2 | Virtual Router 2
State             : Backup
Virtual IP        : 1.1.1.1
Master IP         : 10.2.0.1
PriorityRun       : 120
PriorityConfig : 100
MasterPriority : 120
Preempt           : YES     Delay Time : 0s     Remain : --
Hold Multiplier: 3
TimerRun          : 30s
TimerConfig       : 30s
Auth Type         : NONE
Virtual MAC       : 0000-5e00-0102
Check TTL         : YES
Config Type       : vgmp-vrrp
Create Time           : 20xx-xx-xx 01:19:34
Last Change Time   : 20xx-xx-xx 01:57:08
```

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

```
HRP_M[FW1] display hrp state verbose
20xx-xx-xx 03:34:12.3
  Local role: Active, Peer role: Standby
  Local priority: 0:2, Peer priority: 0:2
  Connection state: succeeded
  Stable time: 0 day, 1 hour, 37 minutes
  Last state change information: 20xx-xx-xx 09:57:08 The HRP link changes to up. Local device ID is fa-41-ba-c4-00-10. Peer device ID is fa-41-ba-c4-00-20.

  Configuration:
  Hello interval                  1000ms
  Preempt                           on
  Track trunk member                on
  Auto-Sync connection status       on
  Auto-Sync configuration           on
```

```
  Mirror configuration              off
  Mirror session                    off
  Adjust OSPF-Cost                   on
  Adjust OSPFv3-Cost                 on
  Adjust BGP-Cost                    on

  Module                          Fault             Robust
  Total                           0                 2
  Manual                           0                 0
  BFD                              0                 0
  Healthcheck                      0                 0
  Tracked interface                0                 0
  VRRP                             0                 0
  CPU                              0                 2
  Boot sync                        0                 0

  Detail-Information:
                                    ospf-cost: 0
                                  ospfv3-cost: 0
                                     bgp-cost: 0
                          GE0/0/1 vrrp vrid 1: active
                          GE0/0/2 vrrp vrid 2: active
```

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

```
HRP_S<FW2> display hrp state verbose
20xx-xx-xx 03:35:10.236
  Local role: Standby, Peer role: Active
  Local priority: 0:2, Peer priority: 0:2
  Connection state: succeeded
  Stable time: 0 day, 1 hour, 38 minutes
  Last state change information: 20xx-xx-xx 09:57:08 The HRP link changes to up. Local device ID is fa-
41-ba-c4-00-20. Peer device ID is fa-41-ba-c4-00-10.

  Configuration:
  Hello interval                  1000ms
  Preempt                           on
  Track trunk member                on
  Auto-Sync connection status      on
  Auto-Sync configuration          on
  Mirror configuration             off
  Mirror session                   off
  Adjust OSPF-Cost                  on
  Adjust OSPFv3-Cost                on
  Adjust BGP-Cost                   on

  Module                          Fault             Robust
  Total                           0                 2
  Manual                           0                 0
  BFD                              0                 0
  Healthcheck                      0                 0
  Tracked interface                0                 0
  VRRP                             0                 0
  CPU                              0                 2
```

```
Boot sync                       0                0

Detail-Information:
                                        ospf-cost: 65500
                                      ospfv3-cost: 65500
                                         bgp-cost: 100
                                GE0/0/1 vrrp vrid 1: standby
                                GE0/0/2 vrrp vrid 2: standby
```

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

```
HRP_M<FW1> display firewall session table
20xx-xx-xx 03:38:32.319
 Current Total Sessions : 4
 Slot: 0 CPU: 0
 udp    VPN: public --> public    10.10.0.2:16384 --> 10.10.0.1:18514
 udp    VPN: public --> public    10.10.0.2:49152 --> 10.10.0.1:18514
 udp    VPN: public --> public    10.10.0.1:49152 --> 10.10.0.2:18514
 ICMP    VPN: public --> public    10.3.0.10:2[1.1.1.4:2048] --> 1.1.1.10:2048
```

```
HRP_S<FW2> display firewall session table
20xx-xx-xx 03:38:12.208
 Current Total Sessions : 4
 Slot: 0 CPU: 0
 udp    VPN: public --> public    10.10.0.1:16384 --> 10.10.0.2:18514
 udp    VPN: public --> public    10.10.0.2:49152 --> 10.10.0.1:18514
 udp    VPN: public --> public    10.10.0.1:49152 --> 10.10.0.2:18514
 ICMP    VPN: public --> public    Remote 10.3.0.10:2[1.1.1.4:2048] --> 1.1.1.10:2048
```

4.4 Configuration Reference

4.4.1 Configuration of FW1

```
#
sysname FW1
#
 hrp enable
 hrp interface GE0/0/3 remote 10.10.0.2
 hrp authentication-key Admin@123
#
undo firewall packet-filter basic-protocol enable
#
 interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 active
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
```

```
 vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 active
#
interface GE0/0/3
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/3
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action source-nat address-group group1
#
```

4.4.2 Configuration of FW2

```
#
sysname FW2
#
 hrp enable
 hrp interface GE0/0/3 remote 10.10.0.1
 hrp authentication-key Admin@123
#
undo firewall packet-filter basic-protocol enable
#
 interface GE0/0/1
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 standby
#
interface GE0/0/2
 ip address 10.2.0.2 255.255.255.0
```

```
 vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 standby
#
interface GE0/0/3
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/3
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action source-nat address-group group1
#
```

4.5 Quiz

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

Reference Answer:

Whether HRP packets exchanged between heartbeat interfaces are controlled by security policies depends on the device model and version.

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

5 User Management (Slightly)

This manual applies only to the online eNSP Pro. You cannot log in to the USG through the web page. If the local eNSP Pro is used for web management, visit the following link: Configuring USG Web Login - eNSP Pro V100R001C10 Product Documentation - Huawei (huawei.com)

After the device is successfully bridged and logged in to the device in web mode, perform subsequent configurations by referring to the lab manual of the real device.

6 Site-to-Site IPSec VPN (Slightly)

This manual applies only to the online eNSP Pro. You cannot log in to the USG through the web page. If the local eNSP Pro is used for web management, visit the following link: Configuring USG Web Login - eNSP Pro V100R001C10 Product Documentation - Huawei (huawei.com)

After the device is successfully bridged and logged in to the device in web mode, perform subsequent configurations by referring to the lab manual of the real device.

7 SSL VPN (Slightly)

This manual applies only to the online eNSP Pro. You cannot log in to the USG through the web page. If the local eNSP Pro is used for web management, visit the following link: Configuring USG Web Login - eNSP Pro V100R001C10 Product Documentation - Huawei (huawei.com)

After the device is successfully bridged and logged in to the device in web mode, perform subsequent configurations by referring to the lab manual of the real device.